AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

Seyfullayev İbrahim Əli oğlu

Həsənov Fərid Asəf oğlu

Xıdırova Sevda Elman qızı

Həsənov Kənan Zahid oğlu

Əliyev Yasin Aydın oğlu

VEB-SAYTLARDA BOŞLUQLARIN VƏ TƏHDİTLƏRİN AŞKARLANMASI VƏ QARŞISININ ALINMASI ÜSULLARI

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: **060632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

İxtisaslaşma**:** **"Kibertəhlükəsizlik (SABAH)"**

Elmi rəhbər: T.f.d. Babək Nəbiyev

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

“Veb-saytlarda boşluqların və təhditlərin aşkarlanması və qarşısının alınması üsulları” mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Yasin Əliyev

Fərid Həsənov

Kənan Həsənov

Sevda Xıdırova

İbrahim Seyfullayev

Tarix

XÜLASƏ

İşin adı: Veb-Saytlarda Boşluqların Və Təhditlərin Aşkarlanması Və Qarşısının Alınması Üsulları

Bu magistr dissertasiya işində veb-saytlarda boşluqların və təhditlərin aşkarlanması və qarşısının alınması üsulları ilə bağlı məsələlər müzakirə olunmuşdur və əsas diqqət veb-saytlardakı boşluqların və təhditlərin aşkarlanması və qarşısının alınması modellərin yaradılmasına yetrilir. İşdə qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

- Veb-sayt və veb əsaslı platformalar analiz edilmişdir.
- Veb-saytlarda və platformalarda kibertəhlükəsiz konsepsiyası analizi edilmişdir.
- Vebdə mövcud boşluqlar və təhdidlərin analizi aparılmışdır.
- Vebdə mövcud boşluqlar və təhdidlərin aşkarlama metodları araşdırılmışdır.
- Aşkarlama alətlərinin analizi ,müqayisəli təhlili və qiymətləndirilməsi aparılmışdır.
- Veb təhditlərin qarşısının alınması üçün kompleks yanaşma işlənib hazırlanmışdır.

SUMMARY

Title od work: Methods for Detecting and Preventing Vulnerabilities and Threats in Websites

In this master's thesis, issues related to methods of detection and prevention of vulnerabilities and threats in websites are discussed, and the main focus is on creating models for detection and prevention of vulnerabilities and threats in websites. Researches were carried out in the direction of several issues and concluded with the following results:

- Website and web based platforms were analyzed.
- Analyzed the concept of cyber security on websites and platforms.
- An analysis of existing web gaps and threats was carried out.
- Methods of detection of vulnerabilities and threats on the web were investigated.
- The analysis, comparative analysis and evaluation of detection tools was carried out.
- A comprehensive approach has been developed to prevent web threats.

MÜNDƏRİCAT

İXTİSARLARIN SİYAHISI

SQL	Structured Query Language – *Struklaşdırılmış sorğu dili*
DDoS	Distributed Denial of Service – *Paylanmış xidmətdən imtina*
WWW	World Wide Web - *Ümumdünya şəbəkəsi*
OWASP	Open Web Application Security Project - *Açıq veb tətbiq təhlükəsizliyi layihəsi*
LDAP	Lightweight Directory Access Protocol - *Sadələşdirilmiş kataloq giriş protokolu*
API	Application Programming Interface - *tətbiq proqramlaşdırma interfeysi*
CRLF	Carriage Return and Line Feed
HTTP	HyperText Transfer Protocol – *Hiper mətinlərin ötürülməsi protokolu*
HTML	HyperText Markup Language – *Hiper mətin işarələnmə dili*
SSRF	Server-Side Request Forgery - *Server tərəfində sorğuların saxtalaşdırılması*
XSS	Cross-Site Scripting – *Saytlararası skript*
CSRF	Cross-Site Request Forgery - *Saytlararası sorğuların saxtalaşdırılması*
XML	Extensible Markup Language - *Genişləndirilə bilən işarələmə dili*
URFDS	Unvalidated Redirects and Forwards Detection System - *Etibarsız yönləndirmə və aşkarlama sistemi*
URL	Uniform Resource Locator
IDP	İntrusion Detection and Prevention - *Müdaxilənin aşkarlanması və qarşısının alınması*
IDS	İntrusion Detection Systems - *Müdaxilənin aşkarlanması sistemləri*
FAR	Fuzzy Association Rule-based - *Qeyri-səlis assosiativ qaydalara əsaslanmış*
VAPT	Vulnerability Assessment & Penetration Testing - *Zəifliklərin qiymətləndirilməsi və nüfuz testi*

DAST	Dynamic Application Security Testing – *Dinamik proqram təhlükəsizliyi testi*
WAVSEP	Web Application Vulnerability Scanner Evaluation Project - *Veb tətbiq zəifliklərinin skanerinin qiymətləndirilməsi layihəsi*
CLF	Common Log Format - *Ümumi jurnal formatı*
DNS	Domain Name System - *Domen adı sistemi*
SAD	Session Anomaly Detection - *Sessiya anomaliyalarının aşkarlanması*
CRS	Core Rule Set - *Əsas qaydalar dəsti*

GİRİŞ

Mövzunun aktuallığı. Veb-saytlardan istifadənin geniş yayılması və informasiya texnologiyalarının sürətli inkişafı ilə birlikdə,saytlardakı təhlükəsizlik açıqları və potensial təhditlərin artması, bu sahədə aparılan tədqiqatların və həll təkliflərinin əhəmiyyətini artırır. Bu məqamda, veb saytlarda mövcud olan təhlükəsizlik boşluqlarının müəyyən edilməsi və onların effektiv şəkildə həll edilməsi, aktual bir tədqiqat mövzusu kimi özünü göstərir. Bu proses, internetdə məlumat mübadiləsinin və digər fəaliyyətlərin artması ilə birləşərək, təhlükəsizlik prinsiplərinin və texnologiyalarının davamlı olaraq yenilənməsini və inkişaf etdirilməsini tələb edir.

Tədqiqatın məqsədi və məsələləri. Tədqiqatın məqsədi, veb-saytlar və veb əsaslı platformaların kibertəhlükəsizlik risklərinin araşdırılması, mövcud boşluqların müəyyənləşdirilməsi və kibertəhlükələrin qarşısını almaq üçün effektiv həllər təklif etməkdir. Bu məqsədə nail olmaq üçün qarşıya aşağıdakı məsələlər qoyulmuşdur:

1. Veb-saytlar və veb əsaslı platformaların texnoloji prinsiplərinin araşdırılması;
2. Veb əsaslı platformaların təhlükəsizlik analizinin aparılması;
3. Veb-saytlar və platformaları əhatə edən mümkün hücum ssenarilərinin və təhdidlərin analizi;
4. Kibertəhlükələrin qarşısının alınması üçün müasir müdafiə mexanizmlərinin işlənməsi;
5. Veb hücumların qarşısının alınması üçün öyənmə modellərinin analizi;

Tədqiqatın obyekti və metodikası. Bu dissertasiya işindəki tədqiqat, veb-saytlar və veb əsaslı platformalar üzərində mövcud olan kibertəhlükəsizlik problemlərinin araşdırılması ilə bağlı təkmilləşdirilmiş bir analitik perspektiv təmin edir. Tədqiqatın məqsədi, bu platformaların məlumat təhlükəsizliyi ilə əlaqədar potensial zəiflikləri və təhlükələri müəyyənləşdirmək və daha sonra bu təhlükələrin səviyyəsini qiymətləndirməkdir. Bu məqsədə nail olmaq üçün, tədqiqatda SQL

inyeksiya (ing. injection), Command inyeksiya və zərəli kod yeritmə texnikaları kimi müxtəlif metodlar istifadə olunmuşdur.

Tədqiqatın elmi yeniliyi və praktik əhəmiyyəti. Bu dissertasiya işi, veb-saytlar və veb əsaslı platformalarda informasiya təhlükəsizliyinin yaxşılaşdırılmasında istifadə edilə bilər. Təklif olunan həllər və metodlar praktiki olaraq tətbiq edilərək kibertəhlükəsizlik səviyyəsinin artırılmasına kömək edə bilər.

Dissertasiya işinin strukturu: Dissertasiya işi giriş, dörd fəsil, nəticə və 32 ədəbiyyat mənbəyindən ibarət olmaqla 80 səhifədə təşkil olunmuşdur.

Birinci fəsildə, veb-saytlar və veb əsaslı platformaların strukturu, funksionallığı və kibertəhlükəsizlik anlayışı araşdırılmışdır.

İkinci fəsildə, veb-saytlar və platformalarda mövcud olan zəifliklər və təhdidlər analiz edilmiş,veb hücum metodlarının növlərinə geniş aspektdə nəzər salınmışdır. Kritik infrastrukturları əhatə edən hücumlar və onların təsirləri elmi əsaslarla təhlil edilmişdir.

Üçüncü fəsildə, kiber təhdidlərin qarşısının alınması üsulları müzakirə olunmuşdur. Bu bölmə, müxtəlif təhlükəsizlik tədbirləri və strategiyaların təsvirini təqdim edərək, kiber hücumların aşkar edilməsi üçün effektiv həll yollarını göstərəcəkdir.

Magistrantların dissertasiyada gördüyü işlər: Dissertasiya işinin birinci fəsli ümumi olaraq, Veb saytlarda və platformalarda kibertəhlükəsizlik anlayışından ibarətdir. **Seyfullayev İbrahim Əli oğlu** tərəfindən yazılmışdır.

Dissertasiya işinin ikinci fəsli Veb-saytlardakı, platformalardakı boşluqlar və təhditlərin araşdırılmasından ibarətdir. **Həsənov Fərid Asəf oğlu** tərəfindən yazılmışdır.

Dissertasiya işinin üçüncü fəsli Veb-saytlarda, platformalarda mövcud olan boşluqların və təhditlərin aşkarlanması üsullarından ibarətdir. **Həsənov Kənan Zahid oğlu,Xıdırova Sevda Elman qızı** tərəfindən yazılmışdır.

Dissertasiya işinin dördüncü fəsli Mövcud Boşluqların və Təhditlərin Qarşısının alınması Modeli haqqındadır. **Əliyev Yasin Aydın oğlu** tərəfindən yazılmışdır.

FƏSİL I. VEB-SAYTLARDA KİBERTƏHLÜKƏSİZLİYİN TƏMİN OLUNMASI SAHƏSİNDƏ AKTUAL MƏSƏLƏLƏR

1.1 Veb-sayt və veb əsaslı platformalar

"Veb-sayt" hər hansı bir müəssəsinin kimliyinin əks etdirilməsi və təqdimat fəaliyyətlərinin reallaşması məqsədi ilə milli və beynəlxalq şəbəkə mühitində nəşr olunan onlayn sistemlərə veb-sayt (və ya veb səhifəsi) deyilir. Veb-sayt, internet üçün nəzərdə tutulmuş, ən azı bir hiperkeçidə malik olan, xüsusi format olunmuş və özündə mətn,qrafika, istinadları və animasiyaları göstərən sənəddir. Veb-sayt yalnız internet üzərində işləyən bir servisdir. Hər bir sayt ən azı bir serverdə yerləşdirilmiş faylların bir-biri ilə əlaqələndirilməsindən yaradılmış bir qovluqdur. Saytlara internet şəbəkəsi vasitəsilə baxmaq imkanı yaradılır və beləliklə informasiya mübadələsini qat-qat asanlaşdırılmış olur (Benson V, Saridakis G, Tennakoon H, Ezingeard JN ,2015).

Dinamiklik və interaktivlik artırıldıqca saytlar virtual ofis, media mərkəz, onlayn mağaza kimi bir çox funksiyaları özündə cəmləməyə başladı. Müasir həyatımızda demək olar ki, nə qədər biznes növü varsa o qədər də sayt var. İndi təkcə hər bir şirkət deyil, hər kəs özünün şəxsi saytının (blog) olmasına çalışır. Saytlar informasiya mübadiləsində yeni, eyni zamanda əvəz olunmaz texnologiyaya çevrilmişdir. Saytları internet üzərindən həftənin 7 gün 24 saat fasiləsiz olaraq ziyarət etmək mümkündür. Eyni zamanda mağaza, ofis, satıcı və s. kimi saymaqla bitməyən bir çox funksiyaları yerinə yetirərkən bir dəfə düzgün hazırlanmış iş sayəsində,illərlə səhvsiz çalışma bacarığı vardır. "Veb-sayt" daha çox onlayn dünya ilə yeni tanış olan şəxslərin internetdə axtarış etdiyi mövzulardandır.

Bütün bu üstünlüklərə baxmayaraq hazırlanması və işlədilməsi qat-qat az maliyyə dəstəyi tələb edir ki, bu da saytları hər kəs üçün əlçatan bir alətə çevirir. Bundan əlavə veb-sayt ən səmərəli və asan reklam növüdür. Sayt sizin şirkətinizin və ya biznesinizin bütün dünyaya çıxışını təmin edir. Veb-sayt sizin həm peşəkarlığınızın həm də biznesinizin göstəricisidir.

İnternetin müasir həyatın ayrılmaz hissəsi olduğu inkar edilməzdir. İnternet istifadəçiləri olaraq 197,6 milyon e-mail göndərir, onlayn olaraq 1,6 milyon dollar

xərcləyir və hər dəqiqə demək olar ki, 415,000 proqram yükləyirik. Lakin internetdən artan istifadəmiz bizə sonsuz ünsiyyət, öyrənmə və texnoloji imkanlar təqdim etsə də, bu, bizi çoxlu sayda veb əsaslı təhlükələrlə üz-üzə qoyur. Veb-saytlarda və platformalarda kibertəhlükəsizlik bu rəqəmsal aktivləri kiber təhdidlərdən və hücumlardan qorumaq üçün görülən təcrübə və tədbirlərə aiddir. Bu veb-saytlar və platformalar vasitəsilə saxlanılan, emal edilən və ya ötürülən məlumatların məxfiliyinin, bütövlüyünün və əlçatanlığının qorunmasını əhatə edir.

1.2Veb-saytlarda və platformalarda kibertəhlükəsizlik

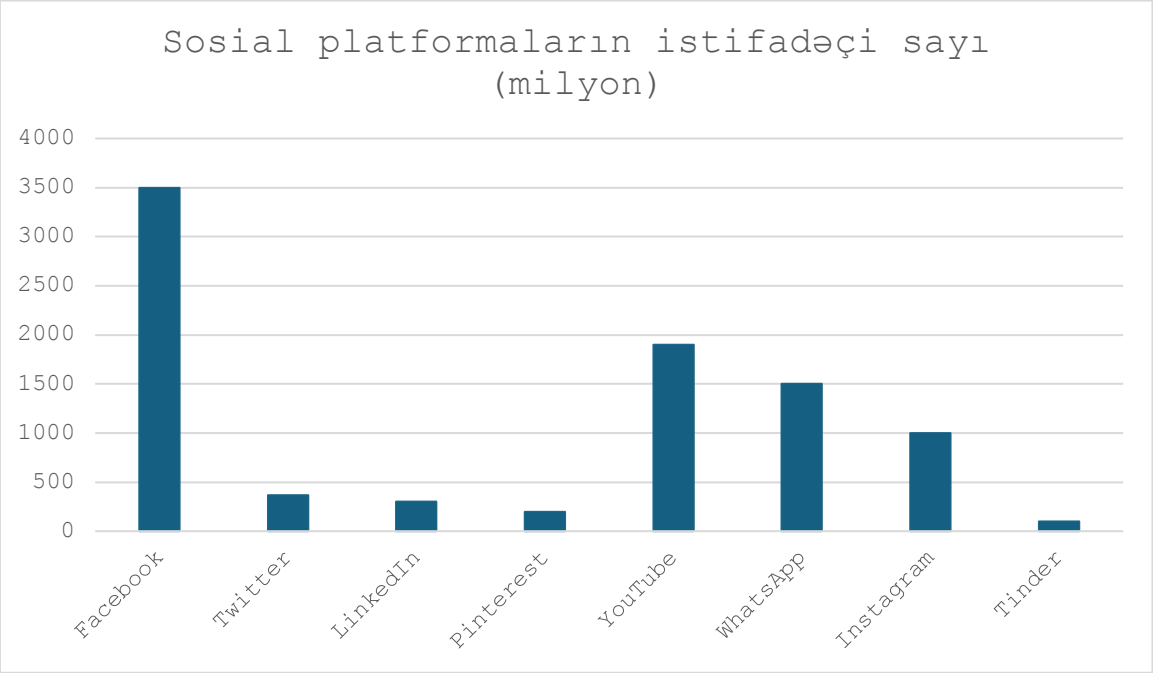
Veb platformalar istifadəçilərə internet üzərindən bir-biri ilə və ya müəssisələrlə qarşılıqlı əlaqə qurmağa və əməkdaşlıq etməyə imkan verən proqram sistemləri və ya xidmətlərdir. Bu platformalar sosial şəbəkə, e-ticarət, məzmunun idarə edilməsi və s. kimi müxtəlif məqsədlərə xidmət edə bilər (Gregory Terzian 2023). Aşağıdakı bəzi veb platforma növlərini nəzərdən keçirək:

1. Sosial Media Platformaları
2. Elektron Ticarət Platformaları

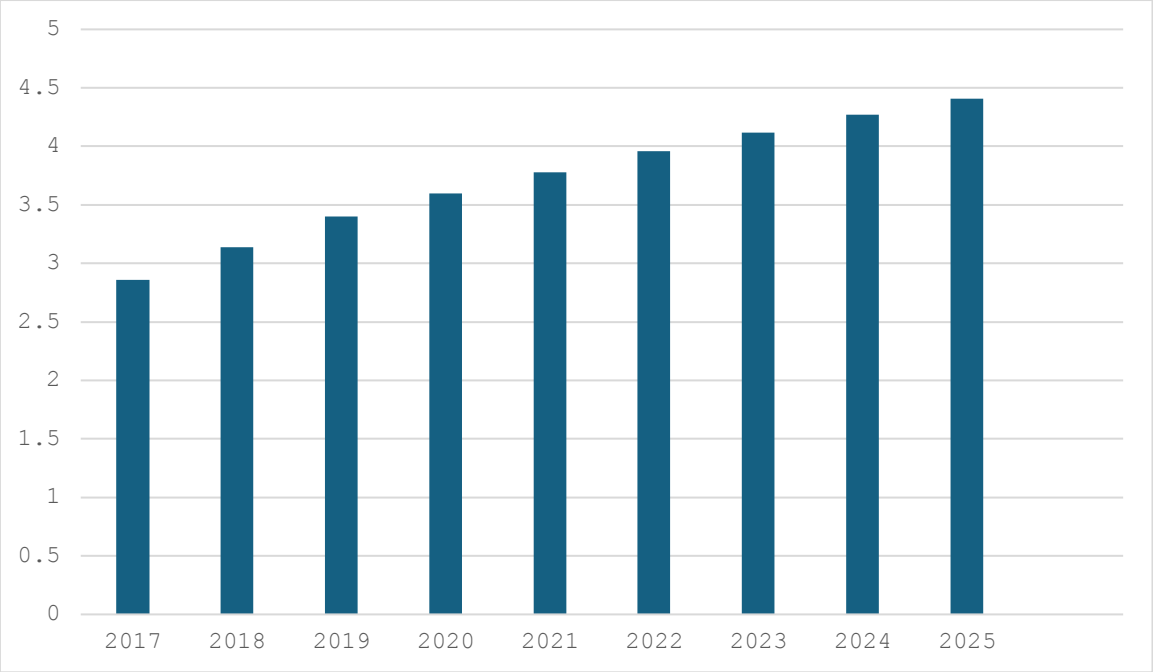
Sosial Media Platformaları 1990-cı illərin ortalarında internet populyarlaşdıqca, əvəllər paylaşılması mümkün olmayan məlumatları,asan bir şəkildə paylaşmağa imkan yaratdı. Daha sonra, 2000-ci illərin əvvəllərində kütlələr tərəfindən sosial şəbəkə və veb-saytlarda qəbul edilən onlayn məlumat mübadiləsinə üstünlük verildi. Bu Facebook, Twitter, Instagram, LinkedIn kimi sosial media platformaları vasitəsilə digər şəxslərlə ünsiyyətini genişləndirmək artıq hər zaman olduğundan daha asan bir hala çevrildi. Həm şəxsi, həm də kommersiya məqsədləri üçün istifadə edilməyə başlanıldı.Sosial media platformaları,insanları danışmaq, fikir və maraqları bölüşmək və yeni dostlar qazanmaq üçün bir araya gətirdi. Əsasən, müxtəlif coğrafi bölgələrdən olan insanlara əməkdaşlıq etməyə , komanda şəklində işləməyə kömək etdi. Sosial şəbəkə platformalarının istifadəsi həmişə asan olmuşdur. Buna görə də sosial media saytlarının populyarlığı və sayları eksponent olaraq artır.Bədii ədəbiyyatdan göründüyü kimi, sosial şəbəkələr əyləncə, iş imkanları yaratmaq, karyera qurmaq, sosial bacarıqlarını təkmilləşdirmək və digər şəxslərlə münasibət qurmaq

üçün istifadə edilə bilər. Facebook və Myspace ən çox seçilən sosial şəbəkə saytları arasındadır.Onlayn əhalinin böyük bir hissəsi sosial media platformasından istifadə etdiyi üçün bu, biznesin təşviqi, maarifləndirmə kampaniyası üçün mühüm vasitəyə çevrilib (Sahoo SR, Gupta BB 2020). İnternetin onlayn məkanında təxminən 4 milyard istifadəçi var. 30 dekabr 2020-ci il tarixinə, ümumi internet istifadəçilərinin 2,7 milyardı Facebook, 330 milyon Twitter aktiv istifadəçisi və 320 milyon Pinterest aktiv istifadəçisidir. Şəkil1.1 müxtəlif sosial media platformalarında istifadəçilərin sayını göstərir. Zephoria-nın hesabatına görə, Facebook-un aylıq aktiv istifadəçilərinin sayı əvvəlki ilə nisbətən 16% artıb. Hər saniyədə yeddi yeni profil yaradılır. İstifadəçilər gündə cəmi 350 milyon foto yükləyirlər. Orta hesabla hər 60 saniyədə Facebook-da 510.000 şərh yerləşdirilir, 298.000 status yenilənir və 136.000 foto yüklənir. Facebook-da çox sayda məlumat yükləndiyindən təhlükəsizlik təhdidlərinin baş vermə ehtimalı yüksəkdir.

Şəkil.1.2-də göstərilən məlumatlara görə, sosial media saytlarının istifadəsi günü-gündən böyük sürətlə artmaqdadır, buna görə də bu saytlardan çox sayda məlumat və informasiya əldə edilə bilər, bu da məlumat sızması riski , məlumatların ələ keçirilməsi, məxfiliyə nəzarət, müəllif hüquqlarının pozulması və informasiya saxtakarlığı kimi bir sıra kibercinayətlərə qapı açmaqdadır. Twitter kimi bəzi iş sosial media saytları şəxsi məlumatların istifadəçilərə açıqlanmasına icazə verməsə də, bəzi təcrübəli kibercinayətkarlar istifadəçilərin yazılarını və onlayn paylaşdıqları məlumatları təhlil edərək həssas məlumatlar əldə edə bilərlər. İnternetdə paylaşdığımız şəxsi məlumatlar kibercinayətkarlara e-mail və şifrələrimizə daxil olmaq üçün kifayət qədər məlumat verə bilər.



Şəkil 1.1 Sosial şəbəkə platformalarının istifadəçi sayları



Şəkil.1.3 Dünyada sosial şəbəkə istifadəçilərinin illərə görə sayı

Elektron Ticarət Platformaları - sadə sözlə desək, e-ticarət termini tamamilə internet vasitəsilə həyata keçirilən alış-verişi, satışı və ödənişləri əhatə edir. Belə bir biznes demək olar ki, bütün ölkələrdə inkişafa təsir edən nəhəng bir sistemə çevrilib və buna görə də qlobal iqtisadiyyatın ayrıca bir hissəsini formalaşdırır.

Onlayn ticarət sizə internet üzərindən sahibkarlıq fəaliyyətini həyata keçirməyə imkan verməklə yanaşı həmçinin, təchizatçıların və alıcıların axtarışı, hesabların ödənilməsi, müqavilələrin tərtib olunması kimi prosesləri həyata keçirməyə şərait yaradır. Təbii ki, bunun üçün xüsusi qaydalar hazırlanır, unikal proqram təminatı yaradılır.

1.3 Veb-saytlarda və platformalarda kibertəhlükəsiz konsepsiyasının analizi

İnternetin qlobal kommunikasiya, ticarət və qarşılıqlı əlaqənin onurğa sütunu olduğu bir dövrdə kibertəhlükəsizlik əvəzolunmaz hala gəldi. Veb tətbiqləri və platformalarının əlavə edilməsi ilə rəqəmsal aktivlərin zərərli hücumlara qarşı gücləndirilməsi zərurəti heç vaxt bu qədər kritik olmamışdır. Veb tərtibatçıları rəqəmsal təhlükəsizlik sahəsində baş rolda çıxış edərək bu davam edən kiber döyüşdə əsas rol oynayırlar. İnternet şəxsi və peşəkar həyatımızın təməl daşıdır. Bu rəqəmsal mühitdə veb inkişafı gündəlik olaraq qarşılıqlı əlaqədə olduğumuz veb-saytları formalaşdırmaq və saxlamaq üçün əsas amildir. Lakin rəqəmsal məkan inkişaf etdikcə onun dərinliklərində görünən təhlükələr də artır. İnternet milyardlarla gündəlik mübadilə və əməliyyatları asanlaşdırır və qlobal miqyasda ən mürəkkəb bir-biri ilə əlaqəli sistemlərdən birini yaradır. Lakin bu geniş yayılmış əlaqə interneti veb-saytlarda və tətbiqlərdə zəiflik axtaran kibercinayətkarlar üçün də əsas hədəfə çevirib. Uğurlu kiberhücum maliyyə itkilərindən tutmuş həssas məlumatlara və zədələnmiş nüfuza qədər dağıdıcı nəticələrə gətirib çıxara bilər (H. Tabrizchi and M. K. Rafsanjani,2020).

Kiber təhdidlər sadə lakin güclü fişinq hücumlarından mürəkkəb zərərli proqram inyeksiyalarına və DDoS hücumlarına qədər müxtəlif formalarda olur. Bu təhdidlər həssas məlumatları ələ keçirə, xidmətləri poza və reputasiyaya xələl gətirə bilər. Veb inkişafında zəifliklər səhv kod, səhv konfiqurasiya edilmiş serverlər və ya qeyri-adekvat şifrələmə protokollarından yaranır. Kibertəhlükəsizlik kompüter sistemlərinin, şəbəkələrinin, cihazların və məlumatların icazəsiz girişdən, kiberhücumlardan və digər rəqəmsal təhlükələrdən qorunmasıdır. Buraya rəqəmsal aktivləri qorumaq, məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək və zərərli

aktorların yaratdığı riskləri azaltmaq üçün nəzərdə tutulmuş tədbirlər, texnologiyalar və protokollar kompleksi daxildir. Kibertəhlükəsizlik insanların, təşkilatların və hökumətlərin rəqəmsal məkanda təhlükəsiz işləyə biləcəyi təhlükəsiz hesablama mühiti yaradır. Buraya güclü autentifikasiya mexanizmlərinin tətbiqi, məlumatların şifrələnməsi, şübhəli fəaliyyətə görə şəbəkə trafikinin monitorinqi və məlum zəifliklərin aradan qaldırılması üçün proqram təminatının müntəzəm olaraq yenilənməsi kimi proaktiv tədbirlər daxildir. Bundan əlavə, kibertəhlükəsizlik istifadəçiləri rəqəmsal təhlükəsizliyi qorumaq və baş verən təhlükəsizlik insidentlərinə cavab vermək üçün ən yaxşı təcrübələr haqqında öyrətməyi əhatə edir.

Bu gün bir-biri ilə əlaqəli dünyada kibertəhlükəsizliyin "zəruriliyi şişirdilmişdir" düşüncəsi tamamilə yanlışdır. Rəqəmsal əsrimizdə maliyyə və şəxsi məlumatlar daxil olmaqla həssas məlumatların böyük bir hissəsi onlayn olaraq saxlanılır və ötürülür. Adekvat kibertəhlükəsizlik tədbirləri olmadan bu məlumatlar kibercinayətkarlar tərəfindən oğurluğa, istismara və sui-istifadəyə qarşı həssas olur. Məsələn, bir maliyyə institutunda məlumatların pozulması milyonlarla müştərinin maliyyə qeydlərini poza bilər və bu, şəxsi məlumat oğurluğuna həmçinin bu hadisədən zərərçəkənlər üçün maliyyə itkisinə səbəb ola bilər. Eynilə, səhiyyə müəssisəsindəki pozuntu xəstələrin tibbi sənədlərinin ifşa olunması, onların məxfiliyinin pozulması və sağlamlıqlarına potensial təhlükə ilə nəticələnə bilər.

Müasir cəmiyyətlər səmərəli fəaliyyət göstərmək üçün bir-biri ilə əlaqəli rəqəmsal infrastruktura çox etibar edirlər. Buraya elektrik şəbəkələri, nəqliyyat sistemləri, rabitə şəbəkələri, əsas səhiyyə və fövqəladə hallara cavab xidmətləri daxildir. Kritik infrastrukturu hədəf alan kiberhücumlar həyati əhəmiyyətli xidmətləri sıradan çıxara, geniş yayılmış xaosa, iqtisadi itkilərə və hətta insanların həyatı üçün təhlükə yarada bilər. Məsələn, elektrik şəbəkəsinə edilən kiberhücum uzunmüddətli fasilələrə, gündəlik həyatın pozulmasına, biznesin pozulmasına və ictimai təhlükəsizlik üçün əhəmiyyətli risklərə səbəb ola bilər. Eynilə, nəqliyyat sisteminə kiberhücum səyahəti poza, logistik fəsadlara və iqtisadi nəticələrə səbəb ola bilər. Kibercinayətkarlarla yanaşı, dövlətlər və dövlət tərəfindən maliyyələşdirilən aktyorlar strateji üstünlüklər əldə etmək, düşmənlərin əməliyyatlarını pozmaq və həssas məlumatları oğurlamaq

üçün kibermüharibə və casusluqla məşğul olurlar. Dövlət qurumlarını, hərbi qurumları və müdafiə podratçılarını hədəf alan kiberhücumlar milli təhlükəsizliyə təhlükə yaratmaq, diplomatik münasibətləri pozmaq və geosiyasi mənzərəni destabilləşdirmək də daxil olmaqla, geniş nəticələrə səbəb ola bilər. Məxfi hərbi kəşfiyyat məlumatlarını oğurlamaq və ya hökumətin kritik funksiyalarını pozmaq məqsədi daşıyan dövlət tərəfindən maliyyələşdirilən kiberhücumlar ölkələr arasında gərginliyi artıra, geosiyasi böhranlara gətirib çıxara və potensial olaraq ənənəvi müharibələrə səbəb ola bilər.

Veb inkişafı və kibertəhlükəsizlik bəzi ümumi zəminləri bölüşür, lakin onlar əhəmiyyətli dərəcədə fərqlənirlər. Hər iki sahə müxtəlif məqsədlər üçün olsa da, kodlaşdırma anlayışını tələb edir.Veb tərtibatçılarının işi veb səhifələri hazırlamaq, dizayn etmək eyni zamanda qüsurları və səhvləri də həll etməkdir. Bunun əksinə olaraq, kibertəhlükəsizlik mütəxəssisləri veb-saytları gücləndirmək üçün autentifikasiya protokolları və firewall kimi təhlükəsizlik tədbirlərinin işlənib hazırlanmasında ixtisaslaşırlar. Hər ikisi veb-saytın baxımını tələb etsə də, fərqli cəhətlərə üstünlük verirlər. Veb tərtibatçıları kibertəhlükəsizliyi və zəiflikləri nəzərə alırlar, lakin əsas diqqəti vebsaytların yaradılmasına, qurulmasına və saxlanmasına yönəldirlər. Bunun əksinə olaraq, kibertəhlükəsizlik mütəxəssisləri vebsaytın müdafiəsini təkmilləşdirməyə və autentifikasiya və digər alətlər vasitəsilə saytın təhlükəsizlik statusunu fəal şəkildə izləməyə diqqət yetirirlər. Davam edən kibertəhlükəsizlik və veb inkişafı müzakirələrində bu 2 qrupun əməkdaşlığı real qalib hesab edilə bilər. Fərqlərə diqqət yetirməkdənsə, onların tərəfdaşlığı müştərilər üçün ən yüksək səviyyədə təhlükəsizliyi təmin etmək məqsədi daşıyır (Sodagudi, S., Kotha, S.K., David Raju,2019). Onlar birlikdə necə işləyirlər:

1. **İlkin yaradılma və planlaşdırılma**:Veb tərtibatçıları dizayn zamanı optimal veb-sayt təhlükəsizliyi üçün frontend və backend həlləri inteqrasiya etmək üçün kibertəhlükəsizlik mütəxəssislərinə etibar edirlər.

2. **Təhlükəsizlik testi:Kibertəhlükəsizlik**:Mütəxəssisləri veb-saytların güclü qorunmasını təmin etmək üçün sınaq keçirməyə kömək edir.

3. **Təhdidlərin təxmin edilməsi**:Hər iki komanda verilənlər bazası müdafiəsini gücləndirmək üçün potensial təhlükələri modelləşdirir.

4. **Yamaqlar və monitorinq**:Davamlı monitorinq və sistem yeniləmələri haker cəhdlərinin qarşısını almaq üçün çox vacibdir.

5. **Hadisəyə cavab planı**:Kibertəhlükəsizlik pozuntu halında zərərli proqram təminatının müəyyən edilməsinə, təhlilinə və aradan qaldırılmasına gətirib çıxarır, veb tərtibatçıları isə məlumatı qoruyur və veb-sayt təhlükəsizliyini bərpa edir.

Veb inkişafı və kibertəhlükəsizlik bir-biri ilə sıx bağlıdır və hər birinin funkisayaları digərinə əsaslı şəkildə təsir edir və onu tamamlayır. Onların əlaqəsini başa düşmək üçün aşağıdakı məqamları nəzərdən keçirək:

Veb-saytların yaradılması və saxlanması kodun yazılmasını, serverlərin konfiqurasiyasını və verilənlər bazalarının idarə edilməsini əhatə edir.Bütün bunlar təhlükəsizlik şərtləri daxilində yerinə yetirilmədikdə təhlükəsizlik zəifliyinə səbəb ola bilər. İstifadəçi daxiletməsini sanitarlaşdırmamaq və ya proqram təminatını məlum təhlükəsizlik yamaqları ilə yeniləməyə məhəl qoymamaq kimi etibarsız kodlaşdırma təcrübələri kibercinayətkarların istifadə edə biləcəyi giriş nöqtələri yaradır. Buna görə də proqramçılar veb inkişaf proqramlarının təhlükəsizlik vəziyyətini yaxşılaşdırmaqla, təşkilatlar təhlükəsizlik pozuntusu ehtimalını və potensial riskləri azalda bilər.

Onlayn məxfilik və məlumat təhlükəsizliyinin istifadəçilər üçün əsas narahatlıq doğurduğu bir dövrdə, veb tətbiqlərinə inam yaratmaq üçün güclü kibertəhlükəsizlik tədbirlərinin həyata keçirilməsi vacibdir. İstifadəçilər veb-saytların öz həssas məlumatlarını və məxfiliyini qorumasını gözləyirlər və hər hansı bir təhlükəsizlik çatışmazlığı etibarı sarsıda və nüfuzun zədələnməsinə səbəb ola bilər. Veb inkişafında kibertəhlükəsizliyə üstünlük verməklə təşkilatlar istifadəçi məlumatlarını qorumaq və etibarı artırmaq öhdəliyini nümayiş etdirirlər.

Veb inkişafının həyat dövrü boyunca ilk olaraq təhlükəsizlik yanaşmasını qəbul etmək, davamlı və təhlükəsiz veb tətbiqləri yaratmaq üçün çox vacibdir. Kibertəhlükəsizlik təcrübələrinin inteqrasiyası təhlükəsizlik mülahizələrinin ilkin dizayndan tutmuş yerləşdirmə və texniki xidmətə qədər inkişaf prosesinin hər mərhələsində daxil edilməsini təmin edir. Buraya müntəzəm təhlükəsizlik qiymətləndirmələrinin aparılması, təhlükəsiz kodlaşdırma standartlarının tətbiqi və autentifikasiya, avtorizasiya, şifrələmə və girişə nəzarət üçün informasiya

təhlükəsizliyinin ən yaxşı təcrübələrinə riayət edilməsi daxildir. Kibertəhlükəsizliyi veb inkişafının strukturuna daxil etməklə, təşkilatlar təhlükəsizlik risklərini fəal şəkildə müəyyən edə və azalda bilər və bununla da veb tətbiqlərinin ümumi təhlükəsizlik vəziyyətini yaxşılaşdıra bilərlər. Veb inkişafı və kibertəhlükəsizlik ayrı-ayrı qurumlar deyil, təhlükəsiz və etibarlı veb proqramları yaratmaq üçün birlikdə işləyən bir-biri ilə əlaqəli müasir texnologiyanın elm sahələridir. Bu iki sahə arasında simbiotik əlaqəni tanımaqla və təhlükəsizliyə vahid yanaşma ilə təşkilatlar kibertəhlükələri effektiv şəkildə azaldan və istifadəçilərə təhlükəsiz, davamlı veb proqramlar inkişaf etdirə bilər. Veb mühitdə kibertəhlükəsizlik saytların yaradılmasının inkişaf mərhələsindən başlayır. Tərtibatçılar təhlükəsizlik tədbirlərini öz iş axınlarına inteqrasiya etmək üçün proaktiv yanaşma nümayiş etdirməlidirlər.

Veb-saytların və platformaların günümüzdə nə qədər faydalı olduğunu nümayiş etdirə biləcək nüansları nəzərdən keçirmiş olduq, və günümüzdə həyatımızın niyə ayrılmaz parçasına çevrildiyini bir daha dərindən analiz etdik. Bütün bu xüsusiyyətlərin və yenilikçi sistemlərin, eyni zamanda həyatımızda çox ciddi problemlərə yol açа biləcəyini də bilmək vacibdir.Elmi işimizin növbəti fəslində sözü gedən təhlükələrin nə olduğu və istifadəçilərə verə biləcəyi ziyanların analizi aparılmışdır.

FƏSİL II VEB MÜHİTDƏ MÖVCUD BOŞLUQLARIN VƏ TƏHDİTLƏRİN ANALİZİ.

2.1 Vebdə mövcud boşluqlar və təhdidlər

7 milyon veb-saytın təhlilinə əsaslanaraq, "SiteLock" bildirir ki, veb-saytlar hazırda hər gün orta hesabla 94 hücuma məruz qalır və həftədə təxminən 2608 dəfə botlar tərəfindən avtomatlaşdırılmış rejimdə yoxlanılır. Orta hesabla 4,45 milyon dollara başa gələn məlumat pozuntuları ilə veb-sayt təhlükəsizliyi təhdidlərinin ciddiliyini nəzərə almamaq olmaz.

Bu hücumlar müştəri itkisi, saytların əlçatanlığının pozulması və dayanma müddəti səbəbindən maliyyə itkilərinə səbəb olur və müştərilərin etibarını sarsıdır.Veb-sayt təhlükəsizliyinə təhdidlərin sayının artması, artan miqyası, mürəkkəbliyi və təsiri təhditlərin proaktiv qarşısının alınması tədbirlərinə ehtiyacı vurğulayır.Bütün sistem müdaxilələrinin 70%-dən çoxu zərərli proqramla (malware) bağlıdır və bütün zərərli proqramların 32%-i internet vasitəsilə yayılır. Zərərli URL-ləri saxlayan saytların əsas kateqoriyaları bunlardır:

- İstehsalat (19,87% zərərli URL ehtiva edir)
- Shareware/torrents (11.84%)
- Sosial şəbəkə (8,71%)
- Əyləncə (8,63%)
- Tibb (7,66%)
- URL keçid dəyişdiricisi (5,81%)
- Digər (28,06%)

Aparılan araşdırmalar nəticəsində belə bir qənaətə gəlmək olar ki, internetdən istifadə edən hər kəs təhlükə altındadır. Və bu elmi iş internet istifadəçilərinin internetdən təhlükəsiz bir şəkildə istifadə edə bilmələri üçün sözü gedən təhditlərin araşdırılması və qarşısının alınması üsullarının öyrənilməsini özündə ehtiva edir.

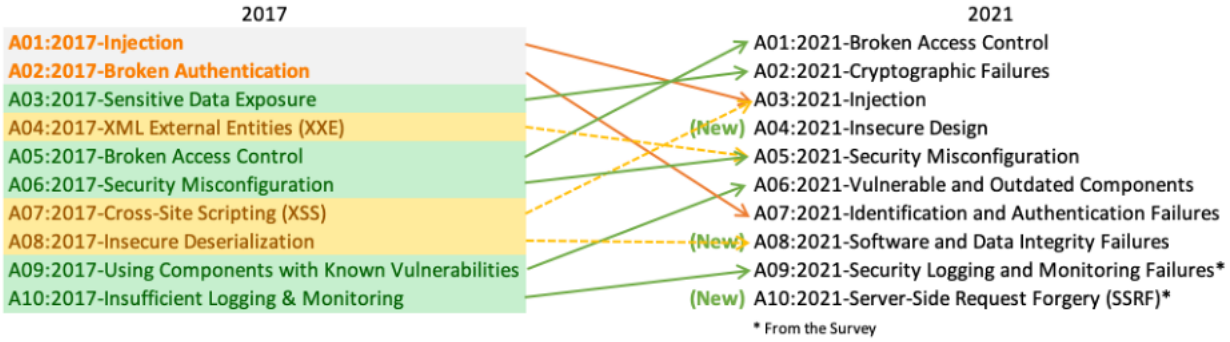
Ümumdünya Şəbəkəsi , aşkar edilmiş zəifliklərin və bildirilən təhlükəsizlik insidentlərinin sayında müvafiq artıma, eləcə də boşluqların sayının artmasına səbəb

olan, getdikcə daha çox həssas məlumatların təqdim edildiyi veb proqramlar vasitəsilə güclü informasiya paylaşma platformasına çevrilmişdir. Veb tətbiqi funksiyalarının genişləndirilməsi proqramların daha effektiv və sürətli cavab vermə qabiliyyətini artırdı. Bu, inkişafın ilkin mərhələlərində və proqram təminatının inkişaf dövrü boyunca təhlükəsizlik yoxlama nöqtələrinin və texnikalarının tətbiqi ilə təhlükəsiz veb proqramların inkişafının təkmilləşdirilməsinin çox güclü səbəbinə çevrilmişdir. Vebin populyarlığının artması və veb tətbiqlərinin genişlənməsi və demək olar ki, hər bir əsas sistemin hazırda veb texnologiyasından asılılığı səbəbindən veb tətbiqlərindəki zəifliklər vebi kiber cinəyatkarların əksəriyyəti üçün əsas diqqət mərkəzinə çevirmiş, buna görə də vebin hədəflənməsi əsas məsələ halına gəlmişdir (Peder Jungck, and Simon S.Y. Shim,2004).

Səhv kodlaşdırma, yanlış konfiqurasiya edilmiş veb serverlər, proqram dizayn qüsurları və ya formaların təsdiq edilməməsi nəticəsində yaranan sistem qüsurları da daxil olmaqla, müxtəlif səbəblərdən veb proqramlar hücuma məruz qala bilər. İstənilən veb tətbiqində hakerlərin daha yüksək səviyyədə istifadə edə biləcəyi ən azı bir boşluq var .

Resursların proqnozlaşdırıla bilən yeri, strukturlaşdırılmış sorğu dilivə kod tətbiqi üç əsas təhlükəsizlik pozuntusu idi və bütün veb tətbiq və tətbiq proqramlaşdırma interfeysi hücumlarının 64%-ni təşkil edirdi. 2023-cü ildə veb tətbiqetmələrə paylanmış xidmətdən imtina hücumu hücumlarının sayı 2022-ci illə müqayisədə 33% azalsa da, veb tətbiqetmələrində düşmən əməliyyatların tezliyi eksponent olaraq artaraq 500% oldu. Hal-hazırda hücumçular onlayn tətbiqetmələrə və onların infrastrukturuna daha çox diqqət yetirirlər və Xidmətdən imtina hücumları hücumları veb tətbiqləri hədəf alan daha mürəkkəb hücumlara keçir. Kibercinayətkarlar sındırılmış saytlardan zərərli proqramların yayılması, məxfi məlumatların oğurlanması kimi məqsədlər üçün istifadə edirlər. Bütün bunlar təşkilatın işini və nüfuzunu təhdid edir. Beləliklə, proqramı qorumaq və veb tətbiqindəki bütün potensial zəifliklərı aradan qaldırmaq yalnız bir seçim deyil, 2024-cü ildə təcili bir zərurətdir.

Açıq mənbə icması olan Açıq Veb Tətbiq Təhlükəsizliyi ən çox yayılmış veb tətbiqi zəifliklərinin icmalını yaratmaq və onları azaltmaq üçün sənayedə ən yaxşı təcrübələri təqdim etməklə interneti istifadəçilər üçün ən təhlükəsiz etmək məqsədi daşıyır.OWASP Top 10 sadəcə veb proqram zəiflikləri siyahısı deyil. O, OWASP riskin qiymətləndirilməsi (ing.Risk Rating)metodologiyasından istifadə edərək hər bir zəiflik sinfini qiymətləndirir və hər bir risk üçün nümunələr, hücumların qarşısının alınması tövsiyələri və bağlantılar təqdim edir. OWASP-in ən yaxşı 10 veb tətbiqi zəifliyini araşdıraraq,proqram tərtibatçıları zərərli hücumlara gəldikdə istifadəçilərin təhlükəsizliyini qorumağa kömək edəcək daha təhlükəsiz proqram yaratmaq üçün konkret addımlar ata bilər. Şəkil.2.1 OWASP siyahısındakı 2017-ci ildən 2021-ci ilə qədər olan dəyişiklikləri görə bilərsiniz.



Şəkil.2.1 OWASP 2017-2021 müqayisəsi

Qırılmış giriş nəzarəti (ing.Broken Access Control)

Qırılmış giriş nəzarəti, veb təhlükəsizlik üçün vacib olan bir kiber təhlükədir. Bu, bir sayt və ya tətbiq proqramında düzgün şəkildə idarə olunmayan giriş imkanlarının istifadə edilməsi nəticəsində məxfilik və məhdudiyyətlərə əməl edilməyən məlumatların əldə edilə biləcəyi bir təhlükədir. Müəyyən bir sənəd, məlumat və ya funksiyanın ancaq müəyyən istifadəçilər tərəfindən çatdırılması təmin edilmir, bu da potensial istismara və məlumatların qeyri-müvafiq ələ keçirilməsinə gətirib çıxara bilər. Bu, nümunələrə icazəsi olmayan şəxslərə yetki verilməsi, istifadəçi sessiyalarının düzgün şəkildə idarə edilməməsi və ya səhifənin URL parametrlərinin dəyişdirilməsi ilə baş verə bilər (Butler W. Lampson,2004).

Kriptoqrafik Uğursuzluqlar (ing.Cryptographic failures)

Kriptoqrafik uğursuzluqlar, kriptoqrafiya tətbiqlərində görünən boşluq və zəifliklərdir. Bu uğursuzluqların arxasında, məlumatların qorunmasında istifadə olunan kriptoqrafik protokolların və alqoritmlərin düzgün şəkildə tətbiq edilməməsi, anlaşılmazlıq və ya əksikliklər yatır. Bu uğursuzluqların əsasında bir sıra problemlər ola bilər:

- Müasir hesablama gücü ilə asanlıqla qırıla bilən zəif və ya köhnəlmiş şifrələmə alqoritmlərindən istifadə.
- Hətta güclü şifrələmə alqoritmləri düzgün tətbiq edilmədikdə uğursuz ola bilər. Ümumi səhvlərə defolt və ya sərt kodlu şifrələmə açarlarından istifadə, açarların düzgün saxlanmaması və ya ötürülmə və ya saxlama zamanı məlumatların açıqda qalmasına səbəb olan şifrələmə/deşifrləmə prosesindəki səhvlər daxildir.
- Açarların birdən çox sistemdə təkrar istifadəsi və ya açarların vaxtaşırı yenilənməməsi kimi zəif açar idarəetmə təcrübələri.
- Kriptoqrafik kitabxanalarda zəifliklər.Bir çox veb proqramlar şifrələmə tapşırıqları üçün üçüncü tərəfin kriptoqrafik kitabxanalarına etibar edir. Bu kitabxanalardakı veb tətbiqi zəiflikləri kriptoqrafik nasazlıqlara səbəb ola bilər, xüsusən də məlum problemlərin aradan qaldırılması üçün onlar müntəzəm olaraq yenilənmirsə.

Biz parollar, e-mail ünvanları, xəstənin sağlamlıq qeydləri, mülkiyyət biznes sirləri, kredit kartı məlumatı və s. haqqında danışırıq. Proqram avtomatik verilənlər bazası şifrələməsindən istifadə edərək kredit kartı məlumatlarını səylə şifrələyir. Bura kimi hər şey yaxşıdır, ancaq bu məlumat əldə edildikdə, dərhal şifrəsi açılır. Veb tətbiqlərindəki bu təhlükəsizlik zəifliyi, kredit kartı məlumatlarını açıq mətndən çıxarmaq üçün SQL inyeksiyasının uğursuzluğuna yol açır – biz buna həmçinin gözləyən hər hansı bir hücumçu üçün hazır fürsət də deyə bilərik.

İnyeksiya

İnyeksiya qüsuru veb proqramlardakı boşluqlardan biridir ki, bu da kiber hücumçuya proqram vasitəsilə zərərli kodu başqa bir sistemə ötürməyə imkan verir. Bu inyeksiyalar müxtəlif forma və ölçülərdə olur, o cümlədən SQL, CRLF, LDAP inyeksiyaları və s. həssas proqramlarda olan digər müştəriləri təhlükə altına almaqla

geniş təsirə malikdirlər. Əslində, kod inyeksiyası (14%) və SQL inyeksiyası (11%) hücumları birlikdə bütün veb proqram hücumlarının dörddə birini təşkil edir [7].

Təhlükəli Dizayn (ing.Insecure Design)

OWASP Top 10 zəiflik siyahısına yeni daxil edilmiş bu kateqoriya təhlükəsizlik təhdidlərinin artmasına yol açan dizayn və memarlıq qüsurlarına diqqət yetirir. Təsəvvür edin ki, təhlükəsizlik nəzarətinin mükəmməl şəkildə həyata keçirilməsi və risklərin azaldılması üçün sərf olunan zəhmətli səylər yalnız təməl dizayn qüsurları ilə məhv edilir. Əsas struktur qüsurlu olarsa, hətta ən təcrübəli təhlükəsizlik tədbirləri belə hücumlara qarşı tab gətirə bilməz. Şübhəsiz ki, bacarıqlı hücumçular gec-tez bu veb proqram zəifliklərini araşdırıb taparaq istifadə edəcəkdir.

İdentifikasiya və Doğrulama Uğursuzluqları (ing.Identification and Authentification Flaws)

Getdikcə mürəkkəbləşən rəqəmsal dünyada autentifikasiya uğursuzluqları veb tətbiqlərində nisbətən ümumi təhlükəsizlik zəifliyidir. Veb tətbiqinizin istifadəçi identifikasiyası, autentifikasiyası və ya sessiyanın idarə edilməsi funksiyaları dəqiq yerinə yetirilmirsə və ya lazımi şəkildə qorunmursa, bu öz növbəsində böyük təhditlərlə bizi üz-üzə qoya bilər.

Proqram təminatı və məlumatların tamlığı ilə bağlı nasazlıqlar (ing.Software and Data Integrity Failures)

Proqram təminatı və məlumatların tamlığı ilə bağlı nasazlıqlar, proqramlarda və sistemlərdə məlumatların düzgün şəkildə saxlanması, işlənməsi və ötürülməsi ilə bağlı yaranan problemləri ifadə edir. Bu cür nasazlıqlar, məlumatlarda yaradılan dəyişikliklərin proqram təminatı tərəfindən doğrulanması və ya proqram təminatının təhlükəsizliyinin zəif olduğu halları əhatə edir

Təhlükəsizlik Qeydiyyatı və Monitorinq Uğursuzluqları (ing.Security Logging and Monitoring Flaws)

Veb tətbiqi zəifliklərinizi izləmək üçün düzgün alətlər olmadan, mahiyyətcə statik naviqasiya edirsiniz. Beləliklə, qeydlər və monitorinq əsas hesabatlılığı təmin edir, sizə baş verənlər barədə aydın fikir verir, insident xəbərdarlığını işə salır və məhkəmə-tibbi araşdırmalar üçün mühüm yardım rolunu oynayır. Bu sistemlər

uğursuz olarsa, bu, gəminin radarını söndürməyə bənzəyir - pozuntuları aşkar etmək və onlara reaksiya vermək qabiliyyətiniz ciddi şəkildə pozulur.

Server tərəfində sorğu saxtakarlığı (ing.Server Site Request Forgery,SSRF)

Bu, veb tətbiqini aldadan, gözlənilməz yerə saxta sorğu göndərən aldadıcı kiber boşluqdur. SSRF zamanı, hücumçu HTTP istəklərini, adətən serverin daxili və ya təyin edilmiş mövqelərində icra etmək üçün dəyişir. SSRF, hücumçunun şəbəkəyə daxil olmasına, yerli və ya xarici resurslara müraciət etməsinə və ya istifadəçilərə təsir etməsinə imkan verir. Bu, müvafiq qorunma tədbirləri olmadan serverlərdə ciddi təhlükələr yarada bilər. SSRF nümunələri arasında daxili serverlərə nəzarət və məlumatların əldə edilməsi, şəbəkəyə daxil olmaq və daxili servislərə hücum nümunələri yer alır.

Təhlükəsizliyin Yanlış Konfiqurasiyası (ing.Security missconfiguration)

Bu, təhlükəsizlik protokollarınız düzgün qurulmadıqda və ya səhvlər etdikdə baş verir. Bu o qədər də aşkar olmayan səhvlər proqramınızı, onun dəyərli məlumatlarını, bütün təşkilatınızı təhlükəli kiberhücum və ya haker istismarına məruz qoyaraq açıq təhlükəsizlik boşluqlarını ortaya qoyur. Bu veb proqram zəiflikləri kibercinayətkarlar üçün asan hədəflər halına çevrilmiş olur.

Zəif və köhnəlmiş komponentlər (ing.Vulnerable and Outdated Conponenets)

Əksər onlayn proqramlar üçüncü tərəf çərçivələrindən istifadə etməklə qurulur. Beləliklə, tətbiqinizdə vurğuya nəzarət pozuntuları, icazəsiz giriş, SQL inyeksiyaları və digər təhlükələr kimi gözlənilməz hadisələrin baş verməsinə səbəb ola biləcək naməlum kodlar ola bilər.

2.2. Veb əsaslı təhdidlərin analizi

Veb əsaslı təhdidlər və ya onlayn təhdidlər internet üzərindən arzuolunmaz hadisə və ya hərəkətə səbəb ola biləcək kibertəhlükəsizlik riskləri kateqoriyasıdır.Veb təhdidləri son istifadəçi zəifliklər, veb-xidmət tərtibatçıları/operatorları və ya veb xidmətlərinin özləri tərəfindən yarana bilər. Məqsəd və səbəbdən asılı olmayaraq, veb

təhlükəsinin nəticələri həm fərdlərə, həm də təşkilatlara zərər verə bilər.Veb əsaslı təhdidlər geniş şəkildə bir çox növə bölünür:

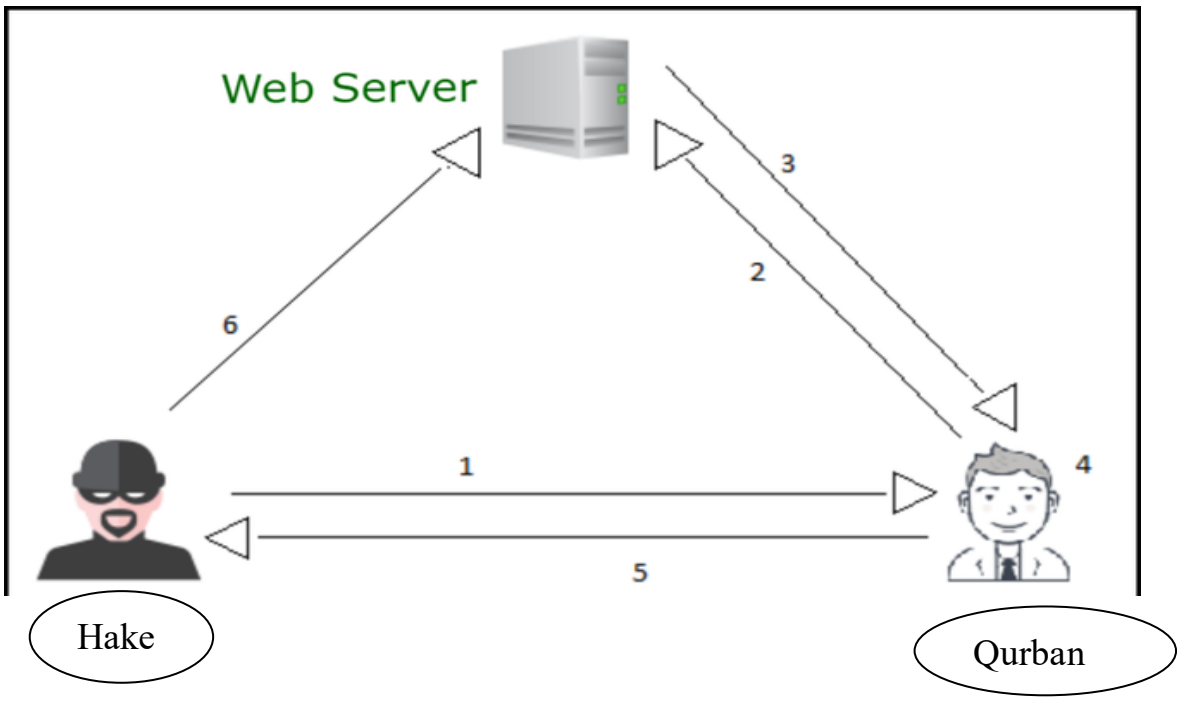
Saytlararası Skript (ing.Cross-Site Scripting, XSS)

XSS zəifliyi veb zəifliklər arasında geniş yayılmış bir zəiflikdir. XSS zəifliklərindən istifadə bir çox ciddi problemə səbəb ola bilər.Hücumçu müştəri skriptini veb səhifələrə və ya serverə və veb tətbiq plaginlərinə yerləşdirə bilər. Bu hücumlardan istifadə edərək saytda istifadəçilər üçün əlçatan olacaq zərərli məzmun yerləşdirə bilər. Viral məzmunu tətbiq etməklə hücumçu həssas səhifə məlumatlarına, sessiya məlumatlarına və brauzerin idarə etdiyi digər vacib məlumatlara səlahiyyətli giriş əldə edə bilər Şəkil.2.2. Beləliklə, verilən hücum koddan istifadə edilən hücuma aiddir.Nümunə kimi qeyd etmək olar ki, 2006-cı ildə Beantovn haker Təşkilatı 2 milyon aktiv istifadəçisi olan bir onlayn platforma olan LiveJournal da XSS zəifliklərini aşkar etdilər (Rahul Johari and Pankaj Sharma,2012). Hücumçu zərərli kodu ehtiva edən çox sayda URL yaratdı və istifadəçiləri onlara keçməyə məcbur etdi. Qurbanlar bu URL-lərə daxil olduqları zaman, hücumçu istifadəçilərin kukilərini oğurlayıb qurbanların hesablarına daxil olmaq üçün istifadə edə bilirdi.

XSS Zəifliklərinin Təsnifatı

Əvvəlcə iki əsas XSS növü müəyyən edilmişdir: Saxlanılan XSS (ing.Stored XSS) və Qalıcı olmayan XSS (ing.Reflected XSS).Stored XSS, məlumatların serverdə saxlanılması zamanı hücum etdiyi XSS növüdür. Burada, hücumçu serverə pis niyyətlə işlədiləcək kod yerləşdirir və istifadəçilər o məlumatı oxuduğu zaman hücum edilir.Reflected XSS, URL-dəki parametrlər vasitəsilə hücum etdiyi XSS növüdür.Hücumçu, pis niyyətlə hazırlanmış bir URL vasitəsilə məlumatı göndərir və server tərəfindən qaytarılan cavabda bu məlumatlar göstərildiyi zaman hücum edilir.2005-ci ildə Amit Klein üçüncü növ XSS-növünü təyin etdi və bu yeni hücum növü Sənəd obyekti modeli (Document Object Model, DOM) əsaslı XSS olaraq adlandırıldı. DOM əsaslı XSS həmçinin tip-0 XSS kimi də tanınır. DOM əsaslı XSS, JavaScript kodunun istifadəçi tərəfindən dəyişdirilmiş məlumatlarla manipulyasiya edilməsi zamanı aktivləşir. Burada, hücumçu, səhifədə olan JavaScript kodunu pis

niyyətlə hazırlanmış məlumatlarla dəyişdirir, bu da brauzerdə pis niyyətlə işlənə biləcək kodların işləməsinə səbəb olur. XSS boşluqları kuki məlumatlarının oğurlanmasına, DOS, DDOS, fişinq hücumlarına səbəb ola bilər.



Şəkil.2.2 XSS hücumu

Addım 1 : Hücumçu URL yaradır və qurbana göndərir.

Addım 2 : Qurban linkə daxil olur və serverə sorğu daxil olur.

Addım 3 : Serverin cavabı "hard kod"-lu JavaScript kodu olur.

Addım 4 : Hücumçuın URL-si hard kod olunmuş JavaScript ilə işlənir.

Addım 5 : Qurbanın brauzerində saxlanan məlumatlar göndərir.

Saytlararası Sorğu Saxtakarlığı (ing. Cross-Site Request Forgery, CSRF)

CSRF, istifadəçinin istifadə etdiyi bir veb səhifəsindən yararlanan hücumçunun istifadəçinin adına avtomatik olaraq HTTP istəkləri göndərməsinə imkan verən bir təhlükədir. Bu istəklər onun adı ilə serverə göndərilir. Bu, həm istifadəçi hesabları, həm də müvafiq brauzer istifadə olunaraq edilə bilər. CSRF əsasən o zaman istifadə olunur ki, "cinayətkar" öz qurbanının adından veb-sayt üzərindən şifrəsinin dəyişdirsin, şifrənin bərpası üçün istifadə olunan məxfi sözü əldə etsin, saytda istifadəçi hüquqlarını dəyişsin və s. Həmçinin CSRF-in köməyi ilə müxtəlif refleksiv (reflected) XSS

hücümları həyata keçirə bilər.Uğurlu bir CSRF hücumu üçün qurbanın veb tətbiqində yaxşı bir sessiyaya sahib olması lazımdır. CSRF hücumunda, hücumçu, həssas veb-sayt GET metodundan istifadə edərsə, tələb olunan URL ilə HTML etiketindən istifadə edə bilər. Post metodundan istifadə edən sorğular üçün hücumçu JavaScript XML,HttpRequest və ya əvvəlcədən təyin edilmiş giriş formasını payload kimi istifadə edə bilər. Qurban daha sonra CSRF məlumatlarını ehtiva edən zərərli bir veb-saytına cəlb olunur. Qurban sayta daxil olduqda, qurbanın sessiyası haqqında məlumat olan əvvəlcədən təyin edilmiş sorğular avtomatik olaraq veb-sayta göndərilir və sorğular müvafiq olaraq işlənir. Qurban, özü də bilmədən, bütün bu sorğulara hücumçunun saytında cavab verir,nəticədə özünü təhlükəyə atmış olur.

Bugcrowd kiber təhlükəsizlik platformasının 2021-ci ildə apardığı bir araşdırmaya görə, CSRF zəifliyi platformanın ən çox yayılmış səhvləri siyahısında 8-ci yerdədir.Bununla birlikdə, bu hücum hələ də bir çox veb tətbiq developeri tərəfindən tez-tez nəzərə alınmır və elmi ədəbiyyatda nadir hallarda müzakirə olunur.Bu hücum, eyni zamanda qurbana pul köçürmək, parol dəyişdirmək və həssas məlumatları dəyişdirmək kimi bir çox zərərlər verə bilər.

Bu müdafiələri veb tətbiqlərə tətbiq etməzdən əvvəl hücumları təhlil etmək və müəyyənləşdirmək çox vacibdir. CSRF-nin aşkarlanması və istifadəsi digər böyük hücumlarla müqayisədə nisbətən asandır. İstifadəçi bu hücumun harada və necə edildiyini bilirsə, qarşısını almaq da nisbətən asanlaşır.

SQL inyeksiyası (ing.Structured Query Language Injection, SQLI)

Müasir veb-saytların və tətbiqlərin əksəriyyəti Strukturlaşdırılmış Sorğu dili (SQL) istifadə edərək proqramlaşdırılmış verilənlər bazalarına qoşulur. SQL inyeksiyası, tətbiqlərin verilənlər bazasına sorğular gedən zaman soğunun pozulması ilə hücumçuın istifadə etdiyi bir üsuldur. Bu hücum hücumçuın veb məlumatlarını icazəsiz oxumaq və ya yazmaq imkanı verir. Bu hücumla hücumçu şəxsiyyəti dəyişdirə, verilənlər bazasındakı mövcud məlumatları dəyişdirə, etibarlılıq problemlərini aradan qaldıra, bütün məlumatların açıqlanmasına, məlumatlara zərər verə, ziyarətçilər üçün əlçatmaz edə və server zərərli hala gətirə bilər. SQL sorğularının

tətbiqi ilə əlaqəli zəifliklər veb-saytdakı sorğulara qeyri-adekvat baxdıqda, filtrlədikdə, nəzarət edilmədikdə baş verir, bu da hücumçuların məlumat almaq üçün verilənlər bazası sorğularına SQL kod parçalarını daxil etməyə imkan verir. SQL inyeksiyasının bəzi növləri vardır:

Daxili SQLi (ing.İn-band SQLi): Bu, hücumçuların SQL Injection hücumlarını eyni kanal vasitəsi ilə yerinə yetirdikləri ən geniş yayılmış SQL Injection növüdür. Hücumçular, məlumat bazasına hücum etmək üçün istifadəçi daxil sahələrinə zərərli SQL kodlarını yerləşdirirlər və nəticələri əldə etmək üçün eyni HTTP responsundan istifadə edirlər.

Səhv əsaslı SQLI (ing.Error-based SQLI): Bu növ SQL Injection, hücumçuların məlumat bazasından xəbərdarlıq xəbərləri əldə etmək üçün səhv mesajlarından istifadə etməsinə əsaslanır. Səhv mesajlarının detallarından yararlanan hücumçular, məlumat bazasının strukturunu və informasiyanın nəticələrini öyrənməyə çalışırlar.

Birləşmə əsaslı SQLI (ing.UNION-based SQLi): Bu, hücumçuların məlumat bazasından bir HTTP responsunu geri qaytarmaq üçün UNION SQL operatorundan istifadə etdikləri bir SQL Injection növüdür. Hücumçular, responsu qiymətləndirərək məlumat bazasının məzmunu barədə ipuclarını qiymətləndirə bilərlər.

Məntiqi (kor) SQLI (ing. Inferential (Blind) SQLI): Bu növ SQL Injection, hücumçuların məlumat bazasını sorğulamaq və serverin davranışını izləyərək məlumat bazasının strukturunu öyrənmək üçün istifadə olunur. Bu tip hücumlar daha yavaş olsa da, digər SQL Injection növləri kimi məlum informasiya aşkarlamaqda istifadə olunur.

Məntiqi (ing. Boolean): Bu, Blind SQL Injection üçün bir alt növ olaraq həyata keçirilir. Hücumçular, məlumat bazasına istədikləri sorğuları yerinə yetirmək üçün boolean (true/false) cavablarını qiymətləndirirlər. HTTP responsunun dəyişdirilməsi və ya dəyişilməməsi ilə nəticənin doğruluğunu qiymətləndirərək məlumatlar əldə edirlər.

Zaman əsaslı (ing. Time-based): Bu, digər bir Blind SQL Injection alt növüdür. Hücumçular, məlumat bazasına göndərilən sorğuların nəticələrinin müəyyən vaxtda (saniyələr şəklində) cavablanmasını gözləyərək məlumatlar əldə edirlər.

Xarici interfeysli SQLI (ing. Out-of-band SQLI): Bu növ SQL Injection, eyni HTTP kanalını istifadə etmədən məlumat bazasına hücum etməyə imkan verir. Hücumçular, ayrı bir kanal vasitəsilə məlumat bazasına sorğular göndərərək informasiya əldə edirlər.

Spam hücumu.

Spam istənməyən kütləvi elektron mesajlar üçün istifadə olunan termindir. Elektron poçt spamın yayılmasının ənənəvi üsulu olsa da, sosial şəbəkə platforması spamın yayılmasında daha uğurludur (Xiaowei Li and Yuan Xue, 2011). Qanuni istifadəçilərin ünsiyyət detallarını asanlıqla şirkət saytlarından, bloqlardan və xəbər qrupundan əldə etmək olar. Hədəfə alınmış müştərini spam mesajlarını oxumağa və bu mesajların təhlükəsiz olduğuna inandırmaq çətin deyil. Spamların əksəriyyəti kommersiya reklamlarıdır, lakin istifadəçilərdən həssas məlumatlar toplamaq üçün də istifadə edilə bilər və ya viruslar, zərərli proqramlar və ya saxta fəaliyyətlər kimidə qarşımıza çıxa bilər.

Fişinq hücumu (ing.Phising attack)

Fişinq hücumları onlayn əməliyyatlarda və xidmətlərdə iştirak edən çoxlu sayda təşkilatlara görə ən çətin sosial mühəndislik kiberhücumlarından biridir. Bu hücumlarda cinayətkarlar orijinal veb-saytın surətini çıxaran və məlumatları zərərli serverə göndərən giriş forması vasitəsilə istifadəçiləri etimadnamələrini və ya həssas məlumatlarını çıxarmaq üçün aldadırlar. Fişinq hücumu, hücumçunun istifadəçi adı, şifrə və istifadəçinin kredit kartı məlumatları kimi həssas məlumatları saxta veb-saytlar və real görünən e-poçtlar vasitəsilə əldə edə biləcəyi bir növ sosial mühəndislik hücumudur. Hücumçu orijinal istifadəçini təqlid edə bilər və şəxsi məlumatı saxta URL ehtiva edən sosial şəbəkə platforması vasitəsilə digər istifadəçilərə saxta mesajlar göndərmək üçün istifadə edə bilər.Bu məqsədə çatmaq üçün hücumçu müxtəlif sosial mühəndislik metodlarından istifadə edir. Məsələn, istifadəçiyə "Bu veb-sayt şəxsi şəkillərinizi istifadə edir , zəhmət olmasa yoxlayın.

Bir çox fişinq hücum vektorlarında veb-sayta işarə edən URL olduğundan, biz veb-saytları hücumların son nöqtəsi kimi müəyyən edə bilərik. Anti-Fişinq İşçi Qrupu (ing. Anti-Phishing Working Group , APWG) 2020-ci ilin son rübündə 611 877 unikal fişinq saytı aşkar edib. Bu hücumların əsas hədəfləri maliyyə institutları (24,9%), sonra sosial media (23,6%), Xidmət kimi proqram (ing.Software as a Service, SAAS) və veb-email xidmətləri (19,6%) və ödəniş platformaları (8,5%) olmuşdur(Steve Petite,2001). Fişinq kampaniyaları nəzərəçarpacaq təsirə malikdir, çünki açıqlanan şəxsi məlumatlar şirkətlərə 411 milyon ABŞ dollarından çox və istifadəçilərə milyonlarla ABŞ dolları dəyərində olan iqtisadi itkilərinə səbəb olmuşdur.

Bəzi nümunələr nəzər salsaq görərik ki,məsələn, adnsu.edu.az saytından saxta e-poçt mümkün qədər çox fakültə üzvünə kütləvi şəkildə paylanır. E-poçt istifadəçinin parolunun bitmək üzrə olduğunu iddia edir. Şifrəni 24 saat ərzində yeniləmək üçün adnsu.edu.az/reset_password saytına daxil olmaq üçün göstərişlər verilir. Şəkil.2.3 ümumi fişinq fırıldaqçılıq cəhdini göstərir:

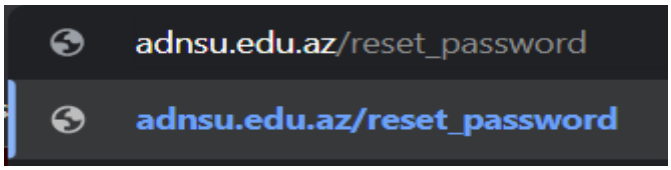
Şəkil.2.3 Fişinq nümunəsi

Linkə klikləməklə bir neçə şey baş verə bilər.Məsələn,istifadəçi myuniversity.edurenewal.com-a yönləndirilir,amma bu səhifə həm yeni, həm də mövcud parolların tələb olunduğu əsl yeniləmə səhifəsi kimi görünən saxta səhifədir. Səhifəni izləyən hücumçu universitet şəbəkəsindəki təhlükəsiz ərazilərə daxil olmaq üçün orijinal parolu oğurlayır.İstifadəçi faktiki parol yeniləmə səhifəsinə göndərilir.

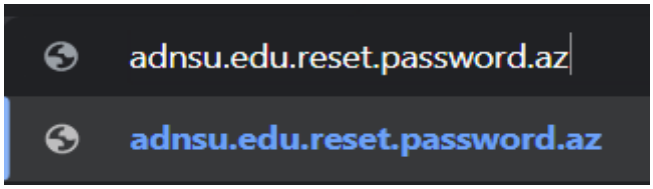
Bununla belə, yönləndirilərkən zərərli skript istifadəçinin sessiya kukisini oğurlamaq üçün arxa planda aktivləşir. Bu, cinayətkarın universitet şəbəkəsinə imtiyazlı giriş imkanı verən əks olunan XSS hücumu ilə nəticələnir.

E-poçt fişinqi

E-poçt fişinqi söz oyunudur. Minlərlə saxta mesaj göndərən bədiyyətli şəxslər, alıcıların yalnız kiçik bir faizi tələyə düşsə belə, əhəmiyyətli məlumat və külli miqdarda pul əldə edə bilər. Yuxarıda göründüyü kimi, bədniyyətli şəxslərin müvəffəqiyyət nisbətlərini artırmaq üçün istifadə etdiyi bəzi üsullar var.Birincisi, onlar saxta təşkilatdan gələn faktiki e-poçtları təqlid etmək üçün fişinq mesajlarının hazırlanmasında çox səy göstərirlər. Eyni ifadələrdən, şriftlərdən, loqolardan və imzalardan istifadə mesajların qanuni görünməsinə səbəb olur.Şəkil.2.4 və şəkil.2.5-dəki nümunədə adnsu.edu.az/reset_password URL-si adnsu.edu.reset.password.az olaraq dəyişdirildi. İki ünvan arasındakı oxşarlıqlar təhlükəsiz bir əlaqə təəssüratı yaradır, bu da alıcının hücumun baş verdiyindən xəbərdar olması ehtimalını azaldır.



Şəkil.2.4



Şəkil.2.5

Spear fişinqi (ing. Spear phishing)

Spear phishing, təsadüfi tətbiq istifadəçilərindən fərqli olaraq, müəyyən bir şəxsi və ya müəssisəni hədəf alır. Bu, təşkilat, o cümlədən onun güc strukturu haqqında xüsusi bilik tələb edən fişinqin daha dərin versiyasıdır.

Asanlıqla oğurlana bilən şəxsi məlumatlara aşağıdakılar daxildir:

1. Sosial təminat nömrəsi
2. Bank hesab nömrəsi

3. Kredit kartı məlumatları
4. E-poçt ünvanı
5. Tibbi qeydlər
6. Telefon nömrəsi

Profil klonlaşdırma hücumu (ing. Attack Of The Profile Clones)

Bu hücum zamanı hücumçu əvvəlcədən haqqında məlumatlı olduğu istifadəçinin profilini klonlayır. Hücumçu bu klonlanmış profili ya eyni, ya da başqa bir sosial şəbəkə iş platformasında həqiqi istifadəçinin dostları ilə etibarlı əlaqələr yaratmaq üçün istifadə edə bilər (David Watson, 2007). Bağlantı qurulduqdan sonra hücumçu qurbanın dostlarını saxta profilin etibarlılığına inandırmaq üçün aldadır və ictimai profillərində dərc olunmayan həssas məlumatları uğurla əldə edir. Bu hücum kiber zorakılıq, kiber təcavüz və şantaj kimi digər kiber cinayətlər törətmək üçün də istifadə edilə bilər. Profilin klonlaşdırılması əhəmiyyətli kibertəhlükəsizlik riski yaradır, çünki o, nisbətən sadə, lakin effektivdir. Profil klonlamasını həyata keçirmək üçün lazım olan hər şey sosial mühəndislik taktikasıdır. İstənilən istifadəçi etibar və tanışlıq kimi insan təbiətindən faydalanmağa əsaslanan bu cür saxtakarlıq fəaliyyətlərinin qurbanı ola bilər. Profilin klonlaşdırılmasının təsiri səth səviyyəsində görünəndən çox ciddi ola bilər. Potensial olaraq qanuni profil kimi qəbul edilə bilən klonlaşdırılmış profil bir sıra kibertəhlükəsizlik pozuntularına səbəb ola bilər. Bu saxta profillərdən göndərilən mesajlar məxfi məlumatların topdansatış oğurlanmasına gətirib çıxara bilər ki, bu da fərdlərə və ya qurumlara zərər verə bilər. Bir çox hallarda bu, reputasiyanın zədələnməsinə, şəxsi həyatın toxunulmazlığına və klonlaşdırılmış profillərin qurbanlarının ağır psixi gərginlik kimi hallarla qarşılaşmasına səbəb olur.

Yanlış yönləndirmə hücumu (ing. Hijacking attack)

Hijacking sizi daxil olmaq istədiyiniz saytın əvəzinə başqa bir veb-sayta aparan üsula verilən addır. Hijacking və ya Domen adı Sistemi (ing.Domain Name System, DNS) Hijacking adlanan bu üsula əsasən hakerlər, nadir hallarda isə dövlət adamları tərəfindən məcburi vəziyyətlərdə istifadə etmək üçün üstünlük verilir.

Nəticə çıxarma hücumu (ing.İnference attack)

Nəticə hücumu, əsas məlumatların bir qisminin müxtəlif taktikalarla qanunsuz şəkildə əldə olunmasından sonra bu məlumatlardan əsas məxfi informasiyanın əldə olunması hücumudur . Hücumçu böyük miqdarda məlumatı təhlil edərək, verilənlər bazasına və ya onun məzmununa faktiki daxil olmadan qeyri-qanuni şəkildə məlumat əldə edə bilər. Məlumat yalnız ondan heç nə çıxarmaq mümkün olmadıqda əhəmiyyətsiz sayılır. Bununla belə, hücumçu daha yüksək səviyyədə qorunmalı olan qiymətli məlumatları birləşdirə bilsə, nəticə çıxarma hücumu uğurlu sayılır.

Sibil hücumu (ing.Sybil attack)

Sibil hücumu, peer-to-peer şəbəkəsində bir çox aktiv saxta identifikatoru eyni vaxtda istifadə etmək üçün tək bir node istifadə edir. Bu tip hücum, şəbəkədəki təsirlərin əksəriyyətini əldə edərək nüfuzlu bir sistemdəki nüfuzu və ya gücü pozmağı hədəfləyir. Saxta şəxsiyyət vəsiqələri bu cür təsiri təmin etməyə xidmət edir.Uğurlu Sybil hücumu hücumçulara sistemdə icazəsiz hərəkətlər etmək imkanı verir. Məsələn, kompüter kimi bir obyektə istifadəçi hesabları və IP əsaslı hesablar kimi birdən çox şəxs yaratmaq və istifadə etmək imkanı verir. Bütün bu saxta şəxsiyyət vəsiqələri, izləmə sistemləri və istifadəçilər onları real kimi qəbul edirlər.Bu hücumun adı 1973-cü ildə "dissosiativ şəxsiyyət pozğunluğu" diaqnozu qoyulmuş bir qadından bəhs edən "Sybil" kitabından ilhamlanıb.Hücumlar kontekstində bu termin əvvəlcə Brian Zill tərəfindən təqdim edilmiş və əvvəlcə Microsoft Research-dən John R. Douceur-in məqaləsində müzakirə edilmişdir.

Klikləmə hücumu (ing.Clickjacking attack)

Clickjacking, İstifadəçinin görünməz və ya başqa bir element kimi gizlənmiş bir veb səhifə elementini fərqində olmadan klikləmək hücumdur. Bu, istəmədən zərərli proqramların yüklənməsinə, zərərli veb səhifələrə daxil olmasına, etimadnamələrin və ya həssas məlumatların verilməsinə, pul köçürməsinə və ya malların onlayn alınmasına səbəb ola bilər .

Ümumiyyətlə, tıklama, İstifadəçinin gördüyü səhifənin üstündə iframe içərisində görünməz bir səhifə və ya HTML elementi göstərməklə həyata keçirilir. İstifadəçi görünən səhifəni vurduğuna inanır, amma əslində üstündə yerləşən əlavə səhifədəki görünməz elementi vurur.Bilinməyən bir səhifə zərərli bir səhifə və ya

istifadəçinin ziyarət etmək istəmədiyi qanuni bir səhifə ola bilər, məsələn, istifadəçinin bank saytındakı pul köçürməsinə icazə verən bir səhifədə istifadəçinin müəyyən köçürtmələr etməsinə və daha sonra bu məbləğin hücumçu tərəfindən mənəsinilməsinə səbəb ola bilər.Klikləmə hücumu üçün bir neçə seçim var, məsələn:

Likejacking hücumu istifadəçilərin Facebook-da "bəyəndim" düyməsini manipulyasiya edərək istifadəçiləri həqiqətən bəyənməməli olduqları bir səhifəni "bəyənməyə" məcbur edən bir üsuldur.

Cursorjacking hücumu hücumçuın qurbanın siçan kursorunu idarə etdiyi və qurbanın kompüterində zərərli hərəkətlər etmək üçün manipulyasiya etdiyi kiber hücum növüdür. Cursorjacking, qurbanın ziyarət etdiyi veb-sayta və ya reklama zərərli kodu yeritməklə işləyir. Daha sonra kod zərərçəkmişin siçan kursorunu zərərli proqram quraşdıra və ya həssas məlumatları oğurlaya bilən gizli düymələrə və ya keçidlərə klikləməyə yönəldir.

Anonimləşdirmə hücumu (ing. De-anonymization attack)

Anonimləşdirmə şifrələnmiş və ya dəyişdirilmiş məlumatları yenidən müəyyən etməyə cəhd etmək və məlumatların əldə edilməsində istifadə edilən bir texnikadır. Məlumatların yenidən identifikasiyası adlanan anonimləşdirmə fərdi, qrup və ya əməliyyatı müəyyən etmək üçün digər mövcud məlumatlarla çarpaz istinad etmək üçün anonimləşdirilmiş məlumatdan istifadə edir. Anonimləşdirmə şifrələnmiş və ya başqa şəkildə gizlədilmiş məlumatlarda saxlanılan şəxsi məlumatın yenidən qurulması təcrübəsidir. Anonimləşdirilmiş məlumatlar hər yerdə onlayn və maliyyə əməliyyatlarında, həmçinin sosial mediada və elektron mesajlaşma və ünsiyyətin digər formalarında istifadə olunur. Anonimləşdirilmiş məlumatların yenidən identifikasiyası qeyri-qanuni məqsədlər üçün şəxsi şəxsiyyəti və maliyyə təhlükəsizliyini poza bilər,həmçinin istehlakçı inamını sarsıda bilər. Texnologiyadan pis niyyətli istifadə dövrü iqtisadiyyatın müxtəlif sektorlarında ənənəvi biznesin aparılması üsulunu sürətlə pozur(Mina Askari, Reihaneh Safavi-Naini, and Ken Barker, 2012). Bu innovativ məhsullar maliyyə inklüzivliyini təşviq edərək, daha çox istehlakçıya ənənəvi maliyyə institutlarının icazə verdiyindən daha az xərclə maliyyə məhsulları və xidmətlərinə çıxış əldə etməyə imkan verib. Texnologiyanın tətbiqinin artması məlumatların toplanması, saxlanması və istifadəsində də artıma səbəb olub. Sosial media platformaları, rəqəmsal ödəniş platformaları və smartfon texnologiyaları kimi texnoloji alətlər müxtəlif şirkətlərin istehlakçılarla qarşılıqlı əlaqələrini yaxşılaşdırmaq üçün istifadə etdiyi tonla məlumat emal edir.

Kiber güc hücumu (ing.Cyberbullying attack)

Kiber zorakılıq, bir insanı qorxutmaq üçün e-poçt, söhbət, telefon danışıqları və onlayn sosial media kimi elektron medianın istifadəsidir. Ənənəvi zorakılıqdan fərqli olaraq, kiber zorakılıq davamlı bir prosesdir. Sosial şəbəkələr vasitəsilə daim dəstəklənir. Hücumçu müntəzəm olaraq qorxuducu xarakterli mesajlar, cinsi xarakterli ifadələr, şayiələr və bəzən də bir insanı qorxutmaq üçün utanc verici şəkillər və ya videolar göndərir. Qurban haqqında şəxsi məlumatları da utandıraraq və ya alçaltmaqla dərc edə bilər. Kiber zorakılıq da təsadüfən baş verə bilər. Mətn mesajları, ani

yazışmalar və e-poçt e-poçtlarında göndərənin tonunu təyin etmək çox çətindir. Ancaq bu cür e-poçtlarda, mətn mesajlarında və onlayn nəşrlərdə təkrarlanan nümunələr nadir hallarda təsadüfi olur.

Məntiq hücumları

Tətbiqin məntiqi hər hansı bir prossesi etmək üçün tərtibatçı tərəfindən hazırlanır. Tətbiq düzgün yoxlanılmama səbəbindən bu cür məntiq xətaları aşkar olunmaya bilər. Məntiq xətalarından istifadə edərək hücum həyata keçirilir. Və bu hücum tətbiqin icrası ardıcılllığını dəyişdirə bilər.

Genişlənən işarələmə dili (ing. Extensible Markup Language, XML) əsaslı proqramlar əsasən XML inyeksiyası hücumlarının üç növünə məruz qalır

XML yol inyeksiyası (ing. XPath injection)

XPath inyeksiyası bir hücum növüdür. Bu, XML path (XML path) sorğularından istifadə edərək hazırlanmış bir tətbiqə zərər verir. Bu dil XML sənədlərindən qovşaqları seçə bilər. Bu tip hücum, məlumatların alınması üçün XPath sorğusu istifadəçinin veb-saytında verdiyi məlumatlardan istifadə edərək hazırlandıqda baş verir. Hücumçu sadəcə veb-sayta pozulmuş məlumatları asanlıqla əlavə edə və XML məlumatlarının quruluşunu əldə edə və onlara daxil ola bilər.

XML sorğu inyeksiyası (ing.XQuery injection)

XQuery funksional proqramlaşdırma dilidir. Toplanmış məlumatları XML formatına çevirir. Bu hücum məlumat zərərli mənbə tərəfindən daxil edildikdə baş verir. XQuery Injection XML XQuery Dilinə qarşı klassik SQL inyeksiya hücumunun variantıdır. XQuery Injection, XQuery əmrlərinə ötürülən düzgün olmayan təsdiqlənmiş məlumatlardan istifadə edir. Bu qayıdış, hücumçu adından XQuery rutinlərinin daxil ola biləcəyi əmrləri yerinə yetirəcək. XQuery inyeksiyası qurbanın mühitindəki elementləri sadalamaq, yerli hosta əmrlər yeritmək və ya uzaq fayllar və məlumat mənbələrinə sorğuları yerinə yetirmək üçün istifadə edilə bilər. SQL inyeksiya hücumları kimi, hücumçu resurs giriş qatını hədəfləmək üçün proqram giriş nöqtəsi üzərindən keçir.

XSS inyeksiyası

XML Saytlararası Skriptləmə auditi XML məlumatlarında mümkün saytlararası skript hücumları üçün istifadəçi sorğularını yoxlayır. Mümkün saytlararası skript hücumu aşkar edərsə, sorğunu bloklayır. Qorunan veb xidmətlərinizdəki skriptlərin veb xidmətlərinizin təhlükəsizliyini pozmaq üçün sui-istifadə edilməsinin qarşısını almaq üçün XML Saytlararası Skript nəzarəti eyni mənşə qaydasını pozan skriptləri bloklayır, bu da skriptlərin başqa serverlərdəki məzmuna daxil olmaması və ya dəyişdirilməməsi lazım olduğunu bildirir. Eyni mənşə qaydasını pozan hər hansı bir skript saytlar arası skript adlanır və ya başqa serverdə məzmuna daxil olmaq və dəyişdirmək üçün skriptlərdən istifadə praktikası saytlar arası skript adlanır.

Link İzləmə (ing. Link Traversal)

Hücumçular müəyyən veb-saytlarının URL-larını izləyərək artıq mövcud olmayan və ya mövcud olan bəzi linkləri və URL-ləri öyrənirlər. Bu linklər hələ də veb tətbiqdən silinməmiş dəyərli məlumatlara çatmağa imkan verə bilər.Link Traversal hücumçuların veb-sayt serverindəki məhdud fayllara və qovluqlara icazəsiz giriş əldə etməsinə imkan verən bir kiberhücum növüdür. Bu, Şəxsi məlumatlar, Giriş etimadnaməsi və maliyyə məlumatları kimi həssas məlumatlara icazəsiz girişə və e-mail və sosial media kimi onlayn hesabların güzəştə getməsinə səbəb ola bilər.Uğurlu bir veb kataloqu hücumunun nəticələri şəxsi məlumat oğurluğu, maliyyə saxtakarlığı və istifadəçinin onlayn nüfuzuna xələl gətirmək də daxil olmaqla ciddi fəsadlara səbəb ola bilər. İnternet və onlayn xidmətlərdən istifadənin artması ilə istifadəçilər üçün bu təhlükədən xəbərdar olmaq və özünümüdafiə üçün tədbirlər görmək çox vacibdir. Effektiv tədbirlərdən biri, Trend Micro Home məhsulları kimi zərərli trafiki aşkarlaya və bloklaya bilən və veb-kataloqlardan və digər kibertəhlükələrdən yan keçməkdən real vaxt rejimində qorunma təmin edən təhlükəsizlik proqramlarından istifadə etməkdir. Hücumçularlar veb-sayt serverindəki zəifliklərdən istifadə etmək üçün məhdud qovluqlara daxil olmaq üçün URL-də xüsusi simvollardan istifadə etmək kimi müxtəlif üsullardan istifadə edirlər. Buna kataloq bypass və ya bypass deyilir. Veb-kataloq bypass hücumunda hücumçu məhdudlaşdırılmış fayllara və qovluqlara daxil olmaq üçün veb-sayt serverindəki zəiflikdən istifadə edir. Hücumçu paylaşmaq üçün nəzərdə tutulmayan fayllara və qovluqlara daxil olmaq üçün xüsusi simvolları olan URL-dən

istifadə edir. Bu, ona həssas məlumatlara daxil olmağa və onlayn hesablar üçün təhlükə yaratmağa imkan verə bilər.

Link Traversal necə işləyir ?

Link Traversal hücumunu həyata keçirmək üçün hücumçular ümumiyyətlə veb-saytları zəifliklər üçün axtaran avtomatlaşdırılmış vasitələrdən istifadə edirlər. Bu vasitələr həssas veb-saytları tez bir zamanda müəyyənləşdirməyə və bir neçə saniyə ərzində istifadə etməyə imkan verir. Hücumçu veb-sayta daxil olduqdan sonra faylları yükləyə və ya silə, zərərli proqram quraşdıra və ya həssas məlumatları oğurlaya bilər. Buna görə veb-sayt sahibləri və administratorları üçün veb-saytlarını veb qovluq bypass hücumlarından qorumaq üçün addımlar atmaq vacibdir. Buraya düzəlişlərin və proqram yeniləmələrinin vaxtında tətbiqi, etibarlı giriş nəzarəti və identifikasiya mexanizmlərinin istifadəsi və şübhəli fəaliyyət üçün veb-saytların mütəmadi olaraq izlənməsi daxil ola bilər. Fərdlər üçün Trend Micro Home məhsulları kimi təhlükəsizlik proqramlarından istifadə veb-kataloqlardan və digər kibertəhlükələrdən yan keçməkdən əlavə qorunma qatını təmin edə bilər.

Rəqəmsal çağımızda veb-kataloqlara baxmaq kimi kibertəhlükələrin yaratdığı risklərdən xəbərdar olmaq həmişəkindən daha vacibdir. Özünüzü və cihazlarınızı qorumağın təsirli yollarından biri Trend Micro Home məhsulları kimi təhlükəsizlik proqramlarından istifadə etməkdir. Trend Micro Home məhsulları, zərərli trafikin aşkarlanması və bloklanması, bilinən və ortaya çıxan təhdidlərə qarşı real vaxt qorunması və phishing və zərərli proqramlardan qorunma kimi bir sıra inkişaf etmiş təhlükəsizlik xüsusiyyətləri təklif etməklə veb hücumlarının və digər kiber təhlükələrin qarşısını almağa kömək edə bilər.

Yanlış yönləndirmə (ing.Path Truncation)

Yanlış yönləndirmə hücumu veb proqram və ya xidmətdə URL-lərin (Uniform Resource Locator) yollarını manipulyasiya etməklə həyata keçirilən hücum növüdür. Bu hücumda təcavüzkar URL-in yol hissəsini dəyişdirərək tətbiqdə tələb olunanlardan başqa müxtəlif fayl və ya səhifələrə daxil olmağa çalışır.

Məsələn, veb proqramdakı fayllara daxil olmaq üçün istifadə edilən URL-lər adətən `http://example.com/files/document.pdf`-dir. Təcavüzkar belə URL yaratmaq üçün bu

URL-i manipulyasiya edə bilər: `http://example.com/files/../admin/secrets.txt`. Burada `..` işarəsi daha yüksək qovluğa keçidi bildirir. Belə bir URL ilə təcavüzkar adətən daxil ola bilməyəcəyi fayllara daxil olmağa çalışır.

Bu cür hücumlar tez-tez server tərəfindəki zəifliklərdən, məsələn, qeyri-adekvat giriş nəzarəti və ya düzgün yolun təsdiq edilməməsi nəticəsində yaranır. Yolun kəsilməsi hücumları təcavüzkarın həssas məlumatlara və ya sistemə giriş əldə etməsinə və vacib məlumatlara zərər verməsinə imkan yarada bilər.

Sessiyanın oğurlanması (ing.Session Hijacking)

Sessiyanın oğurlanması (çərəz tutma olaraq da bilinir), hücumcuya qurbanın veb seanslarına giriş imkanı verə biləcək "ortadakı adam (MİTM)" tipli hücumlardan biridir. Bu həm də, o deməkdir ki, hücumçu İstifadəçinin sessiyasının bir hissəsinə nəzarət edə bilər. Bu proses ona şəxsi və maliyyə məlumatları kimi həssas məlumatlara giriş imkanı verəcək ki, çox vaxt bu məlumatların parolla qorunmasına baxmayaraq sessiyanın ələ keçirilməsi hücumçunun mövcud əlaqənin yoxlayaraq hər cür təhlükəsizlik tədbirindən yan keçməsinə imkan yaratmış olacaq.

Sessiya fiksasiyası (ing. Session fixation).

Bu tip hücumda hücumçular sessiya identifikatoru yaradır və istifadəçi aldadıldıqdan sonra həmin sessiya identifikatorundan istifadə edir. Sessiya identifikatoru hücumçuın veb-saytına aparan URL və ya e-poçt formaları ilə təyin edilə bilər. İstifadəçi daxil olduqdan sonra hücumçu İstifadəçinin məlumatlarına daxil olur.

Kobud güc hücumu (ing.Brute force)

Bu, əsasən veb-sayt və ya hədəf istifadəçi, hücumçuın onları təxmin etməsi və hücumu həyata keçirməsi lazım olduqda proqnozlaşdırılan sessiya identifikatorlarından istifadə edərsə işləyir. Başqa bir ssenari, hücumçuın zəif təhlükəsizlik tədbirləri olan bir veb-saytdan sessiya identifikatorlarının siyahısına daxil olmasıdır.

FƏSİL III VEB-SAYTLARDA MÖVCUD OLAN BOŞLUQLARIN VƏ TƏHDİTLƏRİN AŞKARLANMASI VASİTƏLƏRİ VƏ ÜSULLARI

3.1 Aşkarlama metodlarının analizi

Bu fəsil, veb-saytlarda və platformalarda mövcud olan boşluqların və təhditlərin aşkarlanması üsullarının metodologiyasını təqdim edir. Veb-saytlarının və platformaların artan kompleksliyi, onların məxfilik, təhlükəsizlik və funksional keyfiyyətinin əsas məqamlarından biri halına gəlmişdir. Bu səbəblə, bu iş, veb-saytlarının və platformaların təhlükəsizliyini təmin etmək və onları potensial təhlükələrə qarşı qorumaq üçün vacibdir.

Bu fəsilin məqsədi, veb-saytlarda və platformalarda mövcud olan boşluqların və təhditlərin aşkarlanması prosesinə geniş bir baxış verməkdir. Bu, mövcud metodologiyaların və texnologiyaların təhlükəsizliyin təmin edilməsi üçün nə qədər effektiv olduğunu və necə tətbiq edilə biləcəyini araşdırır. Fəsil, əsasən aşkarlama metodlarının analizini hədəfləyir və bu metodlar veb-saytlarının və platformalarının müdafiəsinin mühüm hissələrindən birini təşkil edir.

Hücumların aşkar olunması üçün klassik yanaşmalar.

1. İmza əsaslı aşkar edilmə:Bu cür aşkarlama üsulları artıq aşkar edilmiş hücumları aşkar etmək üçün effektivdir. Bu üsullar hər yeni gələn paketi artıq aşkarlanmış məlum hücumların siyahısı ilə təsdiqləyir. Bu üsul bir çox hücum növünə qarşı effektiv təsir göstərsə də 0-gün hücumlarını (ing. zero-day attacks) aşkar edə bilmir. O, proqram səhvlərini yəni “false positive”–ləri müəyyən edə bilər. Bu aşkarlama üsulu virus proqram təminatı satıcıları tərəfindən istifadə edilir.

2. Bilik əsaslı aşkarlama:Bu tip hücum aşkarlama sistemi sistem zəiflikləri və əvvəlki hücumların təsviri haqqında məlumatları özündə saxlayır və şübhəli istifadəçi davranışlarını aşkar edə bilir. İstifadəçi davranışları normal və anormal olmaqla iki sinifdən ibarətdir. Normal davranış istifadəçi profili kimi müəyyən edilir, digər sinif isə kibercinəyətkarın anormal davranışını ehtiva edir.

3. Statistikaya əsaslanan aşkarlama:Bu texnika şəbəkənin normal fəaliyyətini müəyyənləşdirir. Əgər bəzi fəaliyyətlər normal fəaliyyətlərin əhatə dairəsini keçərsə, bu, zərərli fəaliyyət kimi qiymətləndiriləcəkdir. Bu sistem daha dəqiq nəticələr əldə

etmək üçün şəbəkədəki trafik sxemlərinə davamlı olaraq nəzarət edir. Sonra bu sistemlər mürəkkəb statistik alqoritmdən istifadə edərək trafiki təhlil edir və sonra trafik nümunələrində hücumları müəyyənləşdirir. Bu texnika bir hədd dəyərindən istifadə edir və hər paket üçün anomaliya hesabını yaradır. Paketin anomaliya xalı həddən artıq böyükdürsə, paket zərərli hadisə kimi qəbul edilir və xəbərdarlıq mesajı verir.

4. Davranış əsaslı aşkarlama:Həm adi, həm də zərərli proqramların davranışı kod tələblərindən asılıdır. Bu, bayt ardıcıllığının yoxlanılmasını tələb etməyən hücumların vacib xüsusiyyətlərini müəyyən etməyə imkan verir. Bu davranışa əsaslanan hücum aşkarlama metodunun əsas məqsədi veb tətbiq serverinin gələcək davranışını müəyyənləşdirməkdir. Bu metod şəbəkə trafik axınının proqnozlaşdırma qabiliyyətindən asılıdır.

5. Hibrid əsaslı aşkarlama:Yuxarıda göstərilən bütün metodların üstünlükləri və mənfi cəhətləri var. Hibrid metodlar statistika, bilik, imza və davranışa əsaslanan metodları birləşdirir. Bütün metodların üstünlüklərini birləşdirir, çatışmazlıqları aradan qaldırır və daha yaxşı nəticələr verir. Bu hibrid metod veb tətbiqləri sıfır gün hücumlarından uğurla qorumağa nail olur.

Hücumların aşkarlanması üçün hazırlanmış üsullar:

Etibarsız yönləndirmə və aşkarlama sistemi metodu

Ashish Kumar altı maşın öyrənmə təsnifat alqoritmlərini, yəni qərar ağacı (ing. decision tree), təsadüfi meşə (ing. random forest), ADA gücləndirmə (ing. Adaptive Boosting), dəstək vektor maşını (ing. support vector machine), xətti reqressiya (ing. linear regression) və neyron şəbəkəsini tədqiq etmişdir (Kumar, D. Garg and P. S. Rana, 2015). Performansa əsasən, ansambl modelini təkmilləşdirmək üçün üç alqoritm seçilir. Bu ansambl modeli təklif olunan sistemlərdə profil hücumlarını aşkar etmək üçün istifadə olunan neyron şəbəkəsi, SVM və təsadüfi meşə alqoritmindən ibarətdir. Model 10 oK film verilənlər bazası[1] ilə sınaqdan keçirilib.

[1] https://movielens.org/movies/2959

Etibarsız yönləndirmə aşkarlama sistemi (ing. Unvalidated Redirects and Forwards Detection System URFDS) qara qutu (black box) skan etmə texnikasından istifadə etməklə Linux-da həyata keçirilən ilk təhlükəsizlik texnikasıdır. Etibarlı olmayan yönləndirmə və irəliyönləndirmələri aşkar etmək üçün bir sistemdir. Bu, tipik olaraq veb tətbiqlərində mövcud olan və saytların mənimsədiyi potensial təhlükələri azaldan bir təhlükəsizlik mənbəyidir. URFDS, hücumların növünü, tipini və mənbəyini aşkar etmək üçün müxtəlif alqoritmlər və texnologiyalar istifadə edir.

URFDS-in arxitekturu aşağıdakı əsas komponentlərdən ibarətdir:

Log məlumatları toplama: Sistem, hücumları aşkar etmək üçün əvvəlcədən müəyyən edilmiş alqoritmlərə əsaslanan log məlumatları toplayır. Bu loglar, hücumların müəyyən edilməsində kritik önəmə malikdir.

Verilənlərin analiz edilməsi: Toplanan log məlumatları, alqoritmlər tərəfindən müvafiq formata çevrilir və analiz edilir. Bu analizlər, etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını təyin etməyə kömək edir.

Hücumların aşkar edilməsi: URFDS, verilənlərin əsasında etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını aşkar etmək üçün fərqli alqoritmlər və metodologiyalar istifadə edir. Bu alqoritmlər, hücumların növünə və mənbəsinə görə müxtəlif təhlillər aparır.

Nəticələrin qiymətləndirilməsi: Alqoritmlərin işləməsindən sonra əldə edilən nəticələr, hücumların növünü və şiddətini qiymətləndirmək üçün nəzarət edilir və dəyərləndirilir.

Zərərli yönləndirmə hallarının bloklandırılması: Nəticələrə əsasən, sistem etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını bloklamaq üçün müvafiq tədbirlər götürür.

URFDS adlı sistemimiz, web tətbiqlərində URF təhlükəsizliyini aşkar etmək üçün dörd əsas komponentdən ibarətdir: bir spider, bir analizator, bir modifikator və bir filter. Sistemin ümumi arxitekturu Şəkil.3.1-də verilmişdir.

Sistem, məntiqi düzgünlüyünü test edərək və 142,522,691 unikal linkdə hücumları taparaq doğruluğunu sübut etmişdir. Bu sistem, əvvəlki sistemlər tərəfindən

tanımlanmayan bəzi hücumları da tapmışdır (Jing Wang , Hongjun Wu “URFDS” 2015).

"Spider" komponenti, URFDS sisteminin bir hissəsidir və veb səhifələrindən məlumat toplamaq üçün istifadə olunur. Bu komponentin iş prinsipi aşağıdakı kimi işləyir:

1. Veb səhifələrinin toplanması: Spider, əsasən, bir axtarış motoru kimi davranır və verilmiş URL-ləri istifadə edərək veb səhifələrini toplayır.
2. Linklərin çıxarılması: Spider, alınan veb səhifələrindən linkləri tapır və onları ayrıca yaddaşa alır.
3. Yeniləmələr: Spider, əvvəlcədən yaddaşa alınmış linkləri də yeniləyə bilər. Yeniləmə prosesi, yeni məlumatların əldə edilməsi və mövcud olan linklərin dəyişdirilməsi ilə bağlı olaraq fərqli olabilir.
4. Yaddaş: Spider, alınan veb səhifələrindən əldə edilmiş məlumatları yaddaşda saxlayır. Bu, digər komponentlər üçün linklərin və səhifə məlumatlarının əlçatanlığına imkan verir.

Bu prinsip əsasında, spider, URFDS sistemi üçün əsas məlumat toplama və işləmə proseslərində mühüm bir rol oynayır.

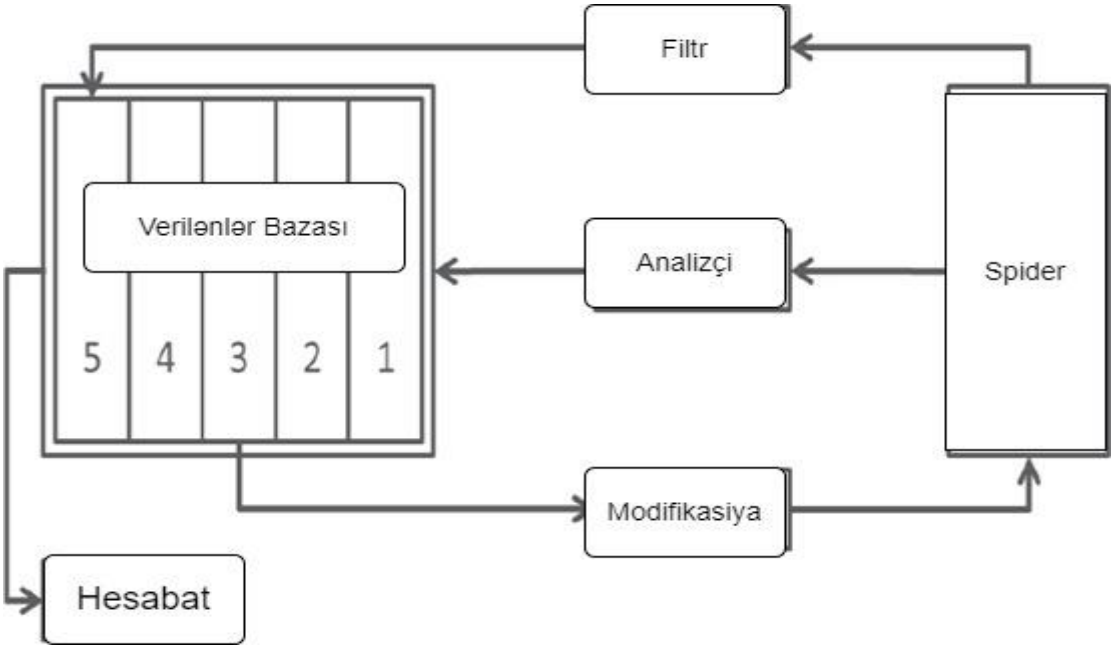
Analizator, URFDS sisteminin bir hissəsidir və linklərin strukturunu təyin etmək üçün istifadə olunur. İş prinsipi aşağıdakı kimi işləyir:

1. Parametrlərin və HTTP prefixlərin yoxlanılması

2. Linklərin strukturunun təyini

3. Məlumatların bazada saxlanılması

4. Təhlükəli linklərin aşkar edilməsi



Şəkil.3.1 URFDS sistem arxitekturası

Analizator, URFDS sisteminin təhlükəli linkləri aşkar etmək üçün əsas mexanizmlərindən biridir.

Modifier, URFDS sisteminin bir hissəsidir və linkləri dəyişdirərək yeni testlər üçün yeni linklər yaradır. İş prinsipi aşağıdakı kimi işləyir:

1. Yaddaşdakı linklərin dəyişdirilməsi

2. Yeni linklərin yaradılması
3. Təhlükəli linklərin aşkar edilməsi

Modifier, URFDS sisteminin linkləri dəyişdirərək yeni testlər və yeni linklər yaratmaq üçün əsas funksionallığı icra edir.

Filter, Unvalidated Redirects and Forwards Detection System (URFDS) sisteminin bir hissəsidir və yönləndirmə URL-inin təsdiqlənib-təsdiqlənmədiyini yoxlayır. İş prinsipi aşağıdakı kimi işləyir:

1) Yönləndirmə URL-lərinin yoxlanılması
2) Təhlükəsizlik təsdiqləməsi
3) Məlumatın təsdiqlənməsi

Filter, URFDS sisteminin təhlükəli linkləri filtrləmək və təhlükəsiz linkləri təsdiqləmək üçün əsas funksionallığı icra edir. URFDS, veb tətbiqlərinə hücumların

qarşısını almaq üçün vacib sayılan alətlər sırasındadır və bu sistem hücumların aşkar edilməsi və məhdudiyyətlənməsi üçün təhlükəsizlik həllərini özündə ehtiva edir. Şəkil.3.2 də URFDS üçün kod nümunəsi nəzərdən keçirərək sistemin işləmə prinsipi yaxından analiz etmək olar.

```python
import urllib.parse

def is_valid_url(url):
    # Yönləndirmə URL-lərinin təhlükəsizliyini yoxlamaq üçün əlavə təhlükəsizlik yoxlamaları edilə bilər
    # Bu nümunədə, sadə bir yoxlama üçün URL-də "http" və "https" prefixlərinin olub-olmadığı yoxlanılır
    if url.startswith("http://") or url.startswith("https://"):
        return True
    return False

# Nümunə üçün, URL-lərin siyahısını göstərir
urls = [
    "http://www.example.com",
    "https://www.example.com",
    "ftp://www.example.com",
    "http://www.example.com/redirect?url=https://www.example.com/redirected",
    "https://www.example.com/redirect?url=https://www.example.com/redirected"
]

for url in urls:
    if is_valid_url(url):
        print(f"{url} - Təhlükəsiz")
    else:
        print(f"{url} - Təhlükəsiz deyil")
```

Şəkil.3.2 URFDS üçün kod nümunəsi

FAR IDP metodu

Qeyri-səlis assosiasiya qaydasına əsaslanan müdaxilənin aşkarlanması və qarşısının alınması sistemi, e-ticarət veb aplikasiyalarında müdaxilə üçün assosiasiya qaydalarının təyin edilməsi və istifadə edilməsi ilə əlaqədardir. Bu sistem, müxtəlif məhsulların satın alınması ilə bağlı məlumatları təhlil edir və bu məlumatlar əsasında assosiasiya qaydaları yaradır. Məsələn, müştərilərin birgə alıb-satmağa meyilli olduğu məhsullar təyin edilir və bununla bağlı qaydalar qurulur (Gaik-Yee Chana, Fang-Fang Chuaa and Chien-Sing Leeb, 2015).

Bu qaydalar vasitəsilə, sistemin normal fəaliyyətlərə uyğunluğu qiymətləndirilir və normadan fərqli olan zərərli fəaliyyətlər aşkar edilir. Bu təhlil prosesi, sistemin qaydaların ətraflı təhlilinə əsaslanmasını təmin edir və zərərli fəaliyyətlərin müəyyən edilməsində kömək edir.

Müəyyən edilmiş zərərli fəaliyyətlərə cavab olaraq, sistemin müdaxilə prosesi işə salınır. Bu proses, müştərilərlə əlaqə saxlanılması, şübhəli fəaliyyətlərin səbəblərinin təyin edilməsi və qarşının alınması kimi addımları özündə saxlayır.

FAR IDP sistemi, e-ticarət veb aplikasiyalarında istifadə olunan və assosiasiya qaydalarına əsaslanan bir müdaxilə sistemi və alqoritmidir Şəkil.4. Bu sistem, müəyyən qaydalara əsaslanan bir alqoritm ilə təhlükəli fəaliyyətləri aşkar etməyə və qarşısını almağa kömək edir. İş prinsipi aşağıdakı kimi işləyir:

1.Assosiasiya qaydalarının təyin edilməsi

2. Müdaxilənin aşkar edilməsi

3. Fəaliyyətin qarşısının alınması

4.Yenilənə bilən sistem

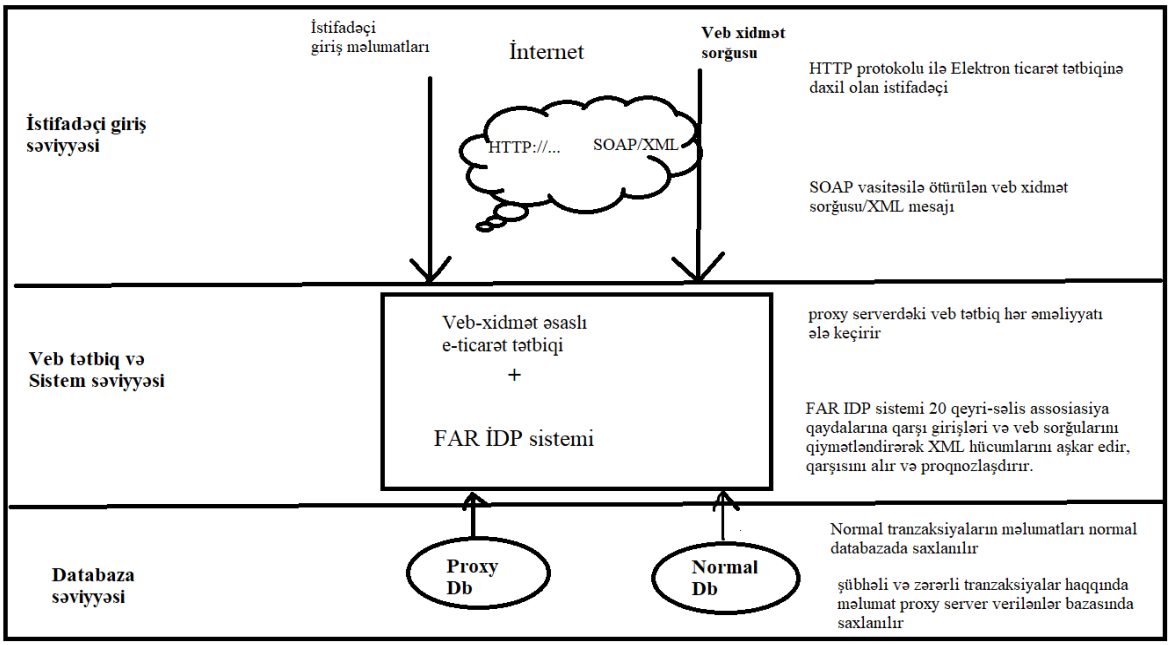
Şəkil.3 də, "mlxtnd" kitabxana funksiyası ilə assosiasiya qaydalarının təyin edilməsi və təhlili üçün tətbiq edilən bir python kodu var. Bu kod, məlumat setindən assosiasiya qaydalarını təyin etmək üçün Apriori alqoritmini istifadə edir və sonra zərərli fəaliyyətlərin aşkarlanması, qarşısının alınması və müdaxilə etmək üçün nəzərdə tutulmuş bir hissədən ibarətdir.

```python
# Məlumatların yaradılması
data = [
    {'mehsul': 'X', 'musteri': 'A'},
    {'mehsul': 'Y', 'musteri': 'A'},
    {'mehsul': 'X', 'musteri': 'B'},
    {'mehsul': 'Z', 'musteri': 'B'},
    # Digər məlumatlar ...
]

# Assosiasiya qaydalarının təyin edilməsi
from mlxtend.frequent_patterns import apriori
from mlxtend.frequent_patterns import association_rules

df = pd.DataFrame(data)
hot_encoded_df = df.groupby(['musteri', 'mehsul']).size().unstack().fillna(0)
frequent_itemsets = apriori(hot_encoded_df, min_support=0.2, use_colnames=True)

# Assosiasiya qaydalarının təhlili
rules = association_rules(frequent_itemsets, metric="lift", min_threshold=1)

# Zərərli fəaliyyətlərin aşkarlanması və qarşısının alınması
for index, row in rules.iterrows():
    if row['lift'] > 1:  # Təhlükəli qaydaları təyin etmək üçün müəyyən bir metrik istifadə edilə bilər
        print("Təhlükəli assosiasiya:", row['antecedents'], "->", row['consequents'])
        # Zərərli fəaliyyətə qarşı addımlar atılması

```

Şəkil.3.3

FAR IDP sistemi, süni intellekt alqoritmlərindən və assosiasiya qaydalarının tətbiqindən istifadə edir. Bu, e-ticarət veb aplikasiyalarında zərərli fəaliyyətlərin aşkarlanması və qarşısının alınması üçün effektiv bir yanaşmadır. Honeypot sistemi ilə FP-growth və Hidden Markov Modellərindən istifadə etməklə təklif olunan veb tətbiqlərində zərərli fəaliyyətin aşkarlanması həyata keçirir. Veb server tərəfində

təcavüzkarın davranışını aşkar edir və proqnozlaşdırır. Bu, server və müştərilər arasında keçmiş qarşılıqlı əlaqə davranışına əsaslanır.



Şəkil.3.4 FAR IDP sistem arxitekturası

Joza metodu

Hiper-mətnli preprosessor (Hipertext preprocessor ,PHP) əsaslı proqramlarda SQL inyeksiya hücumlarını aşkar etmək üçün *Joza* metodu həyata keçirilir. Joza, mənfi və müsbət nəticə çıxarmağın üstünlüklərini birləşdirən hibrid yanaşmadır. Joza-nın təhlükəsizliyi WP-SQLI-LAB test üsulundan istifadə etməklə qiymətləndirilir. Bu metod SQL inyeksiya hücumlarının aşkarlanması üçün dəqiqdir. Joza metodikası, SQL inyeksiyası kimi yayılmış veb tətbiqləri üzərindəki zərərli fəaliyyətləri aşkar etmək və müdafiə etmək üçün inkişaf etdirilmiş bir təsir müəyyən etmə metodikasıdır. Bu metodika, hibrid bir təsir müəyyən etmə metodikasıdır və təhlükəli girişləri aşkar etmək üçün müxtəlif məlumatlardan istifadə edir (Naderi-Afooshteh, Anh Nguyen-Tuong, M. Bagheri-Marzijarani, J. D. Hiser and J. W. Davidson, 2015).

Joza metodikasının əsas mərhələləri aşağıdakılardır:

1. Verilənlərin izlənməsi: Joza, veb tətbiqinin girişlərini izləyərək bu girişləri təhlil edir. Bu, təhlükəli girişləri aşkar etməyə kömək edir.

2. Təsirli təhlil: Joza, izlədiyi girişləri hibrid təsir müəyyən etmə ilə təhlil edir. Bu metodika, məlumatın nəzarət dövrünü izləmək və məlumatların necə dəyişdirildiyini anlamaq üçün zərərli girişlərin təhlilindən istifadə edir.

3. Nəticələrin təhlili: Joza, təhlükəli girişlərin nəticələrini təhlil edir və hücumun məqsədini və potensial ziyanını qiymətləndirir.

4. Mühafizə tədbirlərinin tətbiqi: Joza, təhlükəli girişlərin aşkar edilməsindən sonra mövcud olan təhlükəni aşmaq üçün mühafizə tədbirləri tətbiq edir.

Joza metodikası, veb tətbiqlərinin mühafizəsini artırmaq və SQL injection kimi yayılmış təhlükələrə qarşı mübarizədə müvəffəqiyyətlə tətbiq edilmiş bir təsir müəyyən etmə metodikasıdır.

Onlayn sosial şəbəkələrdə XSS, SQL kimi hücumları aşkarlaya bilən yeni sistem təklif edilmişdir. Bu sistem Alternativ qərar ağacı (Alternating Decision, AD) təsnifatı və təkmilləşdirilmiş n-qram modelinin hibrid formada birləşdirilməsi ilə həyata keçirilir. Təsnifatdan istifadə edərək sistem veb-səhifələrin xüsusiyyətlərinin sayını müəyyən edir və hücumların aşkarlanması üçün təsnifatlandırıcı yaradır. Sonra veb-səhifələri təsnif etmək üçün artıq çıxarılan xüsusiyyətlərdən n-qram modeli hazırlanır. N-gram modeli, bir mətnin ardıcıl sözlər, hərflər və ya simvollar dəsti arasında müəyyən bir sıxılığın müşahidə edilməsində istifadə olunan bir təhlil metodikasıdır. N-gram modeli, bir mətni n sayda ardıcıl hissəyə (n-grama) bölərək hər bir hissənin neçə dəfə təkrarlandığını və bu hissələrin növünü müəyyənləşdirir. Əsasən, 2-gram (bi-gram), 3-gram (tri-gram) və s. olmaqla istifadə olunur.

N-gram modelinin əsas prinsipi, bir mətnin ardıcıl hissələrindəki çoxluğu və sıxlığı analiz etməkdən ibarətdir. Bu, mətnin strukturunu, dil xüsusiyyətlərini və məzmununu anlamağa kömək edir. N-gram modelləri dil modelləşdirmə və mətn sinifləndirmə kimi mətn işləmə tətbiqlərində geniş miqyasda istifadə olunur. Şəkil.3.5-dəki sadə nümunə də SQL inyeksiyasının qarşısının alınması üçün Python-da n-qram və AD ağac modelinin işləmə prinsipi öz əksini tapır, lakin real dünya tətbiqlərində istifadə olunan üsullar daha mürəkkəbdir.

```python
from flask import Flask, request

app = Flask(__name__)

# SQL inyeksiyasının yoxlama funksiyası
def process_query(query):
    # Gelen sorguda təhlükəli ola biləcək ifadələrin yoxlanılması
    if "DROP" in query.upper() or "DELETE" in query.upper() or "UPDATE" in query.upper():
        return "Təhlükəli sorgu"
    # Təhlükəli ifadə yoxdursa sorgu işlənir
    # Burada verilənlər bazasına qoşularaq sorgu işlədilə bilər
    return "Sorgu uğurla işləndi"

@app.route('/')
def home():
    return 'SQL inyeksiyasının yoxlanması Nümunəsi'

@app.route('/query', methods=['POST'])
def query():
    # POST istəyindən gələn SQL sorgusu alınır
    query = request.form['query']
    # SQL sorgusu işlənir
    result = process_query(query)
    return result

if __name__ == '__main__':
    app.run(debug=True)
```

Şəkil.3.5 N-gram ilə SQL sorğularının yoxlanılması

N-gram modelləri hər bir n-gramın çoxluğuna və ardıcıl hissələrin sıxlığına əsaslanaraq mətnin xarakteristikalarını qiymətləndirir. Bu, mətnlərdəki hər hansı bir üstünlükləri, tipik olmayan strukturları müəyyən etməyə və hücumları aşkar etməyə kömək edə bilər. Nəhayət, onlayn sosial şəbəkələrdə XSS hücumlarını müəyyən etmək üçün hər iki yanaşmanı birləşdirildi. Sistem sübut edir ki, klassifikatorun və n-gram modelinin birləşdirilməsi bu iki metodun birlikdə işləyərək daha effektiv bir nəticə verməsinə səbəb oldu.

Honey cyber metodu

Honey cyber metodologiyası, kiber təhlükəsizlik sahəsində istifadə olunan bir taktikadır. Bu metod, potensial hücumçuları cəlb etmək və onların hücum niyyətlərini müəyyən etmək üçün əlverişli bir mühit yaradır. Həqiqi sistemlərdə yerləşdirilmiş, lakin həqiqi istifadəçilər tərəfindən işlədilməyən "bal" və ya "honey pot" adlanan mənbələri istifadə edirlər. Bu mənbələr, normal şəbəkə cihazlarına oxşar görünən hədəfləri təmsil edir, lakin əslində onlar yalnız hücumçuların marağına səbəb olmaq məqsədi daşıyır. Hücumçular bu honey pot sistemlərinə cəlb olunur və onlarla interaksiya etdikcə, təhlükəli niyyətlərini ortaya qoyurlar. Böyük şirkətlər və orqanizasiyalar, bu metod vasitəsilə mövcud olan təhlükələri müəyyən etməyə, nail

olur və lazımı tədbirləri həyata keçirmək fürsətləri yaranır.Məsələn, bir şirkət, bir honey potqura bilər ki, bu server şirkətin mövcud web serverinə oxşar görünə, lakin aslında yalnız hücumçulara məxsus olan bir web server olsun. Bu honey pot serverinə giriş etməyə çalışan hücumçuların IP ünvanları və hücum metodları qeydə alınaraq, şirkətin təhlükəsizlik tədbirləri daha da gücləndirilə bilər. Başqa bir nümunə kimi, şirkət, hücumçuları cəlb etmək üçün bir honey pot e-poçt adresi yarada bilər. Bu e-poçt adresi, yalnız hücumçuların əlaqə saxladığı və hücum niyyətlərini açıq şəkildə ortaya qoyduğu bir e-poçt adresi ola bilər. Bu yolla, şirkətin təhlükəsizlik ekspertləri cari hücumların qarşısını almaq üçün uyğun tədbirləri hazırlaya bilərlər (R. Shukla and M. Singh,2014).

Honey Monkey metodu

Honey Monkey metodologiyası, potensial təhlükəsizlik boşluqlarını aşkarlamaq üçün internetdə avtomatik axtarış aparır və fərqli veb səhifələrindən saytları, faylları və digər resursları yükləyən köməkli bir avtomatlaşdırılmış fəaliyyət qurğusunu (honeyclient) istifadə edir. Microsoft tərəfindən təklif edilmiş bu metodun əsas məqsədi, internetdə mövcud olan potensial təhlükəsizlik boşluqlarını aşkarlamaqdır. Bu, saytları və faylları yükləmək, onların davranışını müşahidə etmək və potensial təhlükəsizlik boşluqlarını təyin etmək üçün avtomatik bir təhlükəsizlik yoxlama sistemi təşkil edir.Bu metod, avtomatik cədvələrin yaradılmasını, saytların avtomatik yüklənməsini və davranışlarının izlənməsini tələb edir. Əgər bir saytda və ya faylda təhlükəsizlik boşluğu müşahidə edilsə, bu boşluq qeydə alınır və təhlükəsizlik tədbirlərinin artırılması üçün qabaqcıl addımlar atılır.Bu metod, internetdəki potensial təhlükəsizlik açıqlarını müəyyən etmək və qarşısını almaq üçün effektiv bir yoldur (R. Shukla and M. Singh, 2014).

Cədvəl.3.1 araşdırılan metodların müqayisəli təhlili özündə saxlayır və bu təhlil metodların arasındakı fərqləri daha aydın şəkildə əks etdirir.

Aşkar edilmiş hücum	İstifadə edilən məlumat	Istifadə edilən yanaşma	Dəqiqlik/əticə
Profil inyeksiyası Hücum	**Film obyektiv məlumat toplusu**	Ansambl yanaşması SVM, NN ilə, Təsadüfi meşə təsnifatçı.	Dəqiqlik 90%-dən çoxdur
URF zəifliklər	Sistem 142,522,691 unikal link ilə sınaqdan keçirildi	URFDS	0-gün hücumu və "false positive" kimi boşluqları müəyyən edir
SQL enjeksiyonu, XML inyeksiyası, SOAP, XML, DoS hücumları	366 qeyri-səlis assosiativ nümunələr (FAP)	FAR IDP Sistemi	Bilinən mövcud hücumların aşkarlanması və qarşısının alınması və yeni hücumların proqnozlaşdırılması. Dəqiqlik 99%. Əməliyyat müddəti 0,25 ms daha azdır.
Müştəri tərəfdə zərərli aktivlik aşkar edildi.	116 ümumi saytsa Capture-HPC log fayllar	HMM, FP artımı və Honeypot əsasında Proqnozlaşdırma sistemi	90% dəqiqlik
SQL inyeksiyası hücumları	WP-SQLI-LAB, və açıq mənbə təhlükəsizliyi	Joza- hibrid problem çıxarış yanaşması müsbət və mənfi nəticə çıxarma alqoritmi	PHP-yə əsaslanan tətbiqləri avtomatik qoruyur. "false positive" nəticə vermir, aşağı performanslıdır (4%), və quraşdırmaq asandır.
Saytlararası script (XSS)	33,843 veb səhifə kimi Yaxşı xasiyyətli nümunələr DMOZ-dan əldə edilmişdir verilənlər bazası və 18,700 veb-səhifələri zərərli hesab edir -dən alınan nümunələr XSSed verilənlər bazasından və Real saytlardan 3300 veb səhifə.	ADTree klassifikasiyası ilə N-gram modelinin təkmilləşdirilməsi	Effektiv XSS aşkarlanması. Yaxşı performans dəqiqlik və geri çağırma
Sıfır gün, polimorfik **qurdlar**	Honeynet arxitekturasından asılı olan sınaq mühiti	İkiqat honeynet sistemi – avtomatik imza generasiyası	Yanlış həyəcan siqnalının azaldılması və polimorf qurdlar üçün yüksək keyfiyyətli imzalar yaratmaq
Zərərli veb URL-ləri	Veb URL **crawler** üçün istifadə ediləm veb səhifələrin URL-ləri (100 url üçün veb səhifə)	Python Honey Monkey sistemi	Müxtəlif əməliyyat sistemlərinin zəifliklərini və onların standart veb-sörf proqram təminatını işə salan IP ünvanlarının siyahısını yönləndirən URL siyahısı olan qara siyahı faylı.
XSS, SQL inyeksiyası hücumları	Simvolik soket	CRAXweb	Geniş miqyaslı açıq mənbəli veb proqramlardakı zəifliklərı uğurla müəyyən edir və hücum xəttini yaradır.

Cədvəl.3.1 Veb tətbiqlərindəki müxtəlif hücum aşkarlama sistemlərinin müqayisəli təhlili

3.2 Aşkarlama alətlərinin analizi ,müqayisəli təhlili və qiymətləndirilməsi

Nüfuzetmə testi ilə veb tətbiq skan edilir və zəifliklər aşkar edilir. Veb zəifliyi skanerlərinin yayılmasını nəzərə alaraq, onların effektivliyini qiymətləndirmək lazımdır. Bunun üçün istifadə olunan üsullardan biri də müqayisəli təhlildir. Veb zəifliyi skanerləri müxtəlif meyarlardan istifadə etməklə qiymətləndirilmişdir. Biz ilk növbədə OWASP etalonundan istifadə edərək dörd tanınmış veb skaneri (Nessus Vulnerability Scanner, OpenVAS, Wapiti və Burp Suite) qiymətləndirir və müqayisə edirik. Biz həmçinin OWASP etalonunda bu dörd proqramın performans nəticələrini onların WAVSEP etalonunda əvvəlki nəticələri ilə müqayisə edərək, bu üç etalonun imkanları arasındakı fərqləri əldə edirik. İnformasiya texnologiyaları sahəsində ən populyar sektorlardan biri öyrənmənin idarə edilməsidir. Veb tətbiqlərin nüfuz sınağı üçün vebsayta baxılır (Shebli, H.M.Z.A.; Beheshti, B.D. 2018).

Məqsəd:

1) Qüsurların müəyyən edilməsi
2) Təhlükəsizlik vəziyyətini müəyyən edin
3) Risk Prioritetlərinin Müəyyən edilməsi
4) Təhlükəsizlik Risklərini Azaldılması
5) Məlumatların pozulmasının qarşısının alınması

Mburano, veb tətbiqi təhlükəsizlik alətlərinin işini qiymətləndirmək üçün standartlaşdırılmış və hərtərəfli test nümunələri dəsti olan Açıq Veb Tətbiqi Təhlükəsizliyi Layihəsindən (OWASP Benchmark) istifadə edərək veb zəifliyi skanerlərinin effektivliyini qiymətləndirdi. Müəlliflər OWASP Benchmark-dan istifadə edərək veb zəiflik skanerlərini, Acunetix, AppScan, Burp Suite və Netsparker-i qiymətləndiriblər. Qiymətləndirmə ölçülərinə əhatə dairəsi, aşkarlama dəqiqliyi və yanlış müsbət dərəcələr daxildir. Nəticələr göstərir ki, hər bir brauzerin performans baxımından özünəməxsus güclü və zəif tərəfləri var. OWASP belə nəticəyə gəldi ki, Benchmark müxtəlif veb zəiflik skanerlərinin performansını qiymətləndirmək və müqayisə etmək üçün faydalı alət ola bilər və istifadəçilərə xüsusi ehtiyac və tələblərinə əsaslanaraq ən uyğun aləti seçməkdə kömək edə bilər (Mburano, B.; Si, W. 2018) .

Qutam, A. Tiwari, V. yanaşmanın effektivliyini nümayiş etdirmək üçün veb proqramında yerinə yetirilən VAPT - ın ətraflı nümunəsini təqdim etdi. Müəlliflər VAPT prosesində iştirak edən müxtəlif addımları, o cümlədən kəşf, zəifliyin müəyyən edilməsi, istismar və hesabat verməyi təsvir edirlər. Onlar həmçinin Nmap, Burp Suite, Metasploit və SQL Map kimi test zamanı istifadə olunan alətlər və texnikaları müzakirə edirlər. Məqalə veb proqramların təhlükəsizliyinin təmin edilməsində VAPT-nin əhəmiyyətini və inkişaf edən təhlükə mənzərəsi ilə ayaqlaşmaq üçün müntəzəm sınaqlara ehtiyacı vurğulamaqla yekunlaşır. Müəlliflər təşkilatlara VAPT-ni kibertəhlükəsizlik strategiyasının bir hissəsi kimi daxil etməyi və ondan veb proqramlardakı zəiflikləri müəyyən etmək və azaltmaq üçün istifadə etməyi tövsiyə edirlər (Arvind Goutam , Vijay Tiwari, 2020).

S., Kotha, S.K., David Raju veb proqramlarda kiberhücumları aşkar etmək və qarşısını almaq üçün yeni üsullar təqdim etdilər. Birinci mərhələdə, istifadəçi davranışı, şəbəkə trafiki və sistem qeydləri kimi xüsusiyyətlərə əsasən mümkün hücumların aşkarlanması. İkinci mərhələdə, aşkar edilmiş hücumların baş verməsinin qarşısının alınması. Bu qaydalar tətbiqin xüsusi ehtiyaclarına uyğunlaşdırıla və yeni təhlükələr üçün yenilənə bilər. Onlar tapdılar ki, onların metodu geniş spektrli hücumları, o cümlədən SQL inyeksiyası, saytlararası skriptlər və kataloqlar arası hücumları müəyyən edib qarşısını ala bilər. Ümumilikdə, məqalə maşın öyrənməsi və qaydalara əsaslanan metodlardan istifadə edərək veb tətbiqlərində kiberhücumların müəyyən edilməsi və qarşısının alınması üçün perspektivli yanaşma təqdim edir. Bu, veb tətbiqlərinin təhlükəsizliyini artırmaq və məlumat pozuntularının qarşısını almaq istəyən təşkilatlar üçün faydalı ola bilər (S., Kotha, S.K., David Raju 2019).

Boşluqların aşkarlanması

1)HTTP cavabı daxilində brauzer tərəfindən icra edilə bilən kod daxil edildikdəbu kodun nəticəsi brauzerdə əks olunursa bu boşluq XSS boşluğu sayılır. Əlavə edilmiş hücum daimi deyil və yalnız zərərli şəkildə hazırlanmış linki klikləyən və ya üçüncü tərəfin veb saytına daxil olan istifadəçilərə təsir edir; Tətbiqin özündə saxlanmır. Hücum sətri, tətbiqin səhv emal etdiyi və qurbana geri göndərdiyi hazırlanmış URI və

ya HTTP parametrlərinin bir hissəsidir. Bu tip hücumlara qarşı həssas olan veb tətbiqi sorğular vasitəsilə qəbul edilən təsdiqlənməmiş girişi müştəriyə geri göndərəcək. Hücum adətən üç addımı izləyir: Dizayn, burada təcavüzkar zərərli URL yaradır və sınaqdan keçirir; qurbanlarını URL-ni brauzerlərinə yükləməyə inandırdığı sosial mühəndislik; icra isə qurbanın brauzeri vasitəsilə zərərli kodun icrasıdır. Hər Giriş Sahəsində XSS-in yoxlanılması üçün addımlar

1. Giriş vektorlarını izləyin.
2. Giriş vektorlarını yoxlayın

2)Nəticənin veb tətbiqinin təhlükəsizliyinə zərər gətirə biləcək zəifliyi göstərib-göstərmədiyini görmək üçün əvvəlki turda cəhd edilmiş hər bir test girişini araşdırdıq. Bunu etmək üçün yaradılan veb-səhifənin HTML-ni nəzərdən keçirməli və test girişini axtarmalısınız. Xüsusi simvol aşkar edildikdə, tester düzgün kodlaşdırılmamış, dəyişdirilmiş və ya süzülmüş simvolları tapır. Məqsəd bütün HTML xüsusi simvollarını HTML obyektləri ilə əvəz etməkdir. Tanımaq üçün vacib HTML obyektləri bunlardır

1) >(böyükdür)

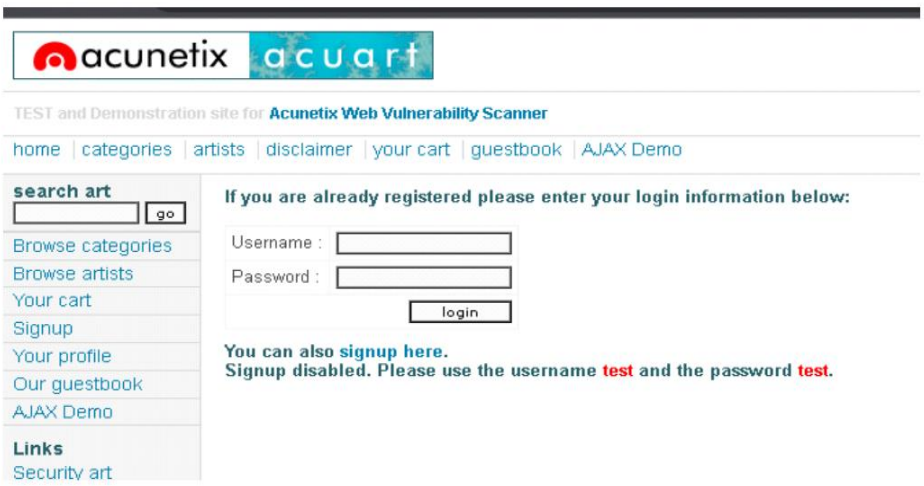
2) <(kiçikdir)

3) & (ampersand)

4)' (apostrof və ya tək dırnaq)

5)"(cüt dırnaq)

XSS-in testi məqsədi ilə istifadə olunan bu veb-saytı nəzərdən keçirək

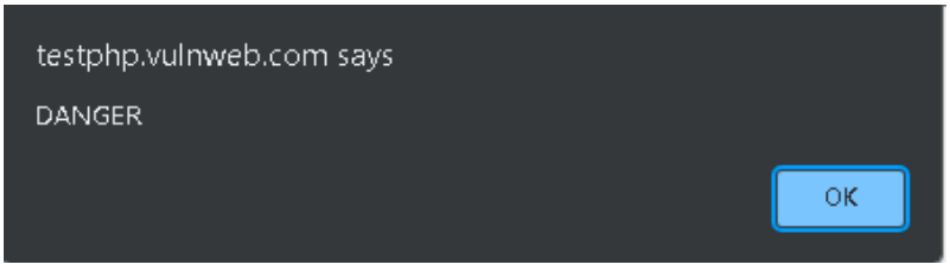


Şəkil.3.6 Acunetix veb zəiflik skaneri

Acunetix Veb Zəiflik Skaneri Şəkil.3.6-da göstərilmişdir. Testerin fikrincə, hər bir məlumat giriş nöqtəsi XSS hücumu ehtimalını artırmalıdır. Tester istifadəçi dəyişənini sınayacaq və onu təhlil etmək üçün zəiflikdən istifadə etməyə çalışacaq.

http://example.com/index.php?user=<script>alert("Danger")</script>

XSS Nəticəsi Şəkil.3.7-də göstərilmişdir. Bu, XSS zəifliyinin mövcud olduğunu göstərir və əgər kimsə testerin linkinə klik edərsə, tester potensial olaraq istənilən brauzerdə istənilən kodu işlədə bilər.



Şəkil.3.7 XSS-in nəticəsi

2) Sessiyanın fiksasiyası zəifliyi

Sessiyanın fiksasiyası hücumçuya etibarlı istifadəçi sessiyasını oğurlamağa imkan verən hücumdur. Hücum veb tətbiqinin sessiya ID-sini, xüsusən də həssas veb tətbiqini idarə etməsinə imkan yardacaq məhdudiyyəti araşdırır. O, istifadəçinin autentifikasiyası zamanı yeni sessiya identifikatoru təyin etmir və mövcud sessiya ID-dən istifadə etməyə imkan verir. Hücum etibarlı sessiya identifikatorunun əldə edilməsindən (məsələn, proqrama qoşulmaqla), istifadəçini həmin sessiya ID-si ilə autentifikasiya etməyə sövq etməkdən və sonra istifadə edilən sessiya ID-si haqqında məlumatı olan istifadəçi tərəfindən autentifikasiya edilmiş sessiyanı qaçırmaqdan ibarətdir. Təcavüzkar qanuni Veb tətbiqi sessiya identifikatorunu təqdim etməli və qurbanın brauzerinə ondan istifadə etməyə imkan verməlidir.

3) Veb Server Parolun Avtomatik Tamamlanmasına İcazə Verməsi

4) Veb proqram kukiləri HTTPOnly kimi qeyd olunmaması

5) Veb əks etdirmə zəifliyi

OWASP onlayn proqram təhlükəsizliyi sahəsində tanınmış və hörmətli bir təşkilatdır. O, inkişaf etdiricilərə və təşkilatlara zəiflikləri müəyyən etmək və

azaltmaqda kömək etmək üçün resurslar, alətlər və tövsiyələr təqdim etməklə proqram təminatı və veb tətbiqlərini daha təhlükəsiz etmək məqsədi daşıyır. Tövsiyə olunan üsul sızma testi üçün istifadə edilən standart üsuldur. Bu metodologiya Zəifliyin növünü və Baqların təsir gücünü təsnif etməyə kömək edir. Metod zəifliklərin müəyyən edilməsində dəqiq və düzgün tətbiq axınını təmin edən bir neçə addımdan ibarətdir.

1) Kəşfiyyat: Hədəf sistemin potensial zəifliklərini və hücum səthini anlamaq üçün kəşfiyyat lazımdır. Bu, uğurlu bir zəiflik qiymətləndirməsinin əsasını təşkil edir.

2) Skan etmə: Skan etmə, açıq portları, xidmətləri və bilinən zəiflikləri təyin edərək sistemin potensial zəif sahələrini başlanğıc üçün anlamağı təmin edir.

3) Qiymətləndirmə: Qiymətləndirmə, zəiflikləri ciddilik və potensial təsirlərinə görə sinifləndirmək, onları prioritetləndirmək və məqsədəuyğun tövsiyələri təmin etmək üçün əhəmiyyətlidir.

4) Açıqlanma və Analiz: Qiymətləndirmə, zəiflikləri ciddilik və potensial təsirlərinə görə sinifləndirmək, onları prioritetləndirmək və məqsədəuyğun tövsiyələri təmin etmək üçün əhəmiyyətlidir.

5) Hesabat və Yamaq: Qiymətləndirmənin nəticələrinə əsaslanaraq sistemi təmir etmək və qorumaq üçün son mərhələ, aşkar olunan məlumatları dokumentləşdirmək və zəifliklər yamamaqdan ibarətdir.

Metodologiya

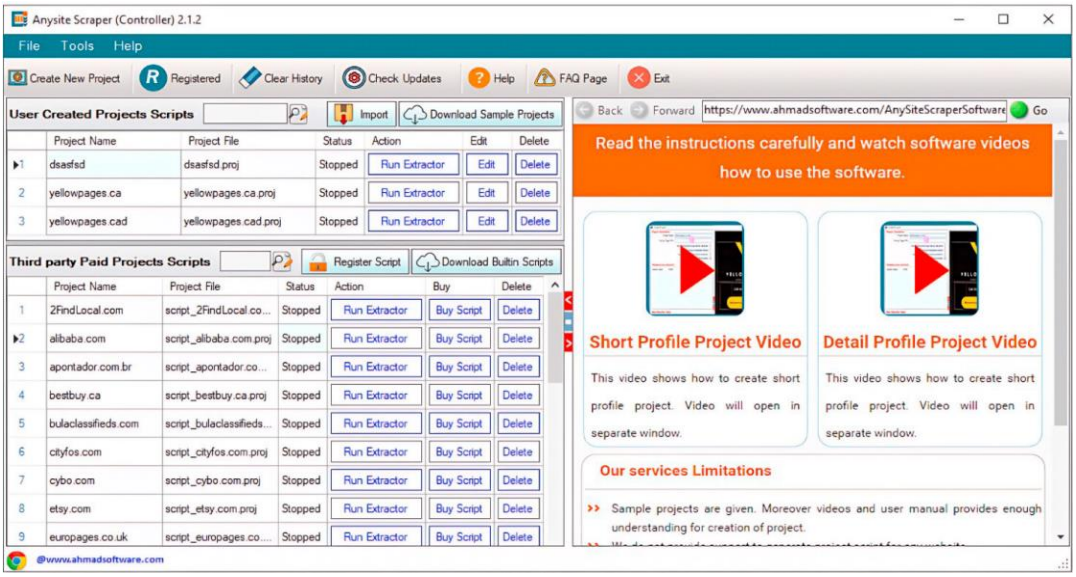
Veb Tətbiqinin Təhlükəsizliyi Testi üçün Test Metodologiyası beş mərhələyə bölünür:

1. Kəşfiyyat
2. Skanlama
3. Qiymətləndirmə
4. Kəşf və Təhlil
5. Hesabat və yamaq

Kəşfiyyat Bu mərhələ hədəf vebsayt, sistem, proqram və s. haqqında məlumatların toplandığı zəifliklərin qiymətləndirilməsi və nüfuzetmə testində məlumat toplama mərhələsidir. id's,.kəşfiyyatın məqsədi mümkün qədər çox potensial təhlükəni, yəni hədəflər Veb Tətbiqində mövcud olan zəiflikləri müəyyən etməkdir. Google

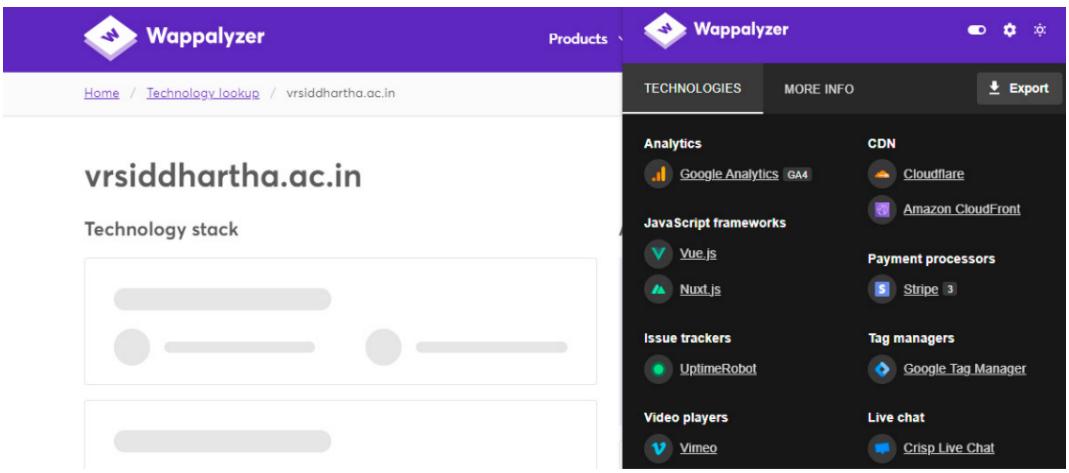
Dorking: Google Dorks, adətən axtarış motorları tərəfindən indeksləşdirilməyən məlumatları axtarmaq üçün qabaqcıl operatorlardan istifadə edən axtarış texnikasıdır. Bu yazıda Google Dorking Hədəf Veb Tətbiqinin Məlumat Toplama Texnikası (Kəşfiyyat) üçün istifadə olunur.

Bu elmi-işdə biz veb-proqramın ayaq izlərini (foot printing) üçün istifadə olunan Vebdata Extractor alətindən istifadə etdik. Tətbiq veb-saytın IP ünvanının bütün statik və dinamik səhifələri haqqında bütün məlumatları verir. Webdata Extractor Şəkil 8-də göstərilmişdir.



Şəkil.3.8 Vebdata Extractor

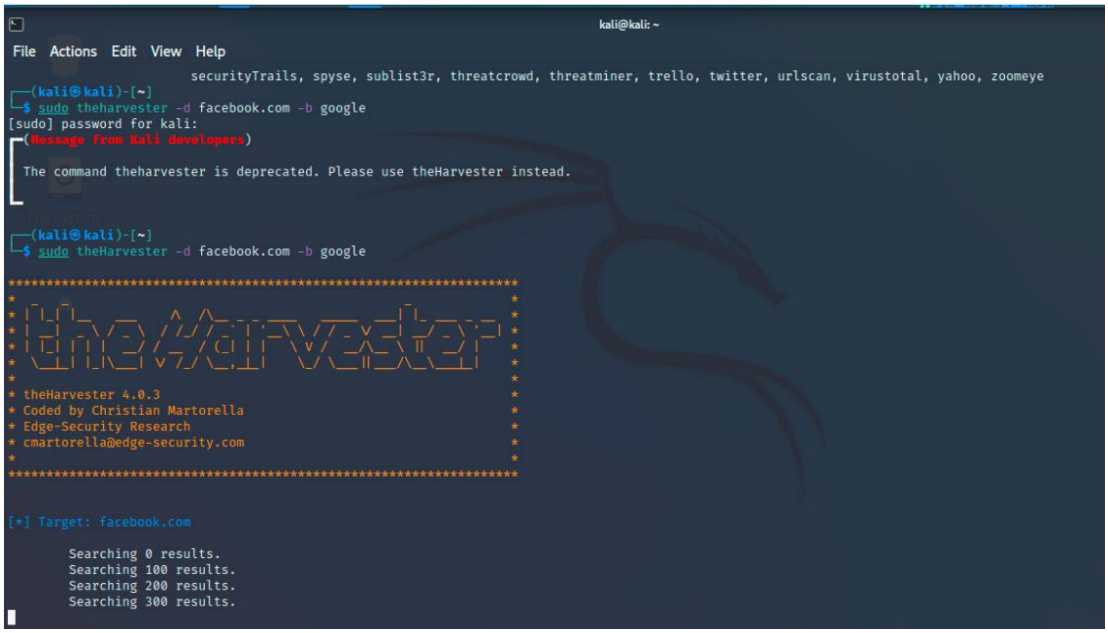
Həmçinin proqramın hazırlanması üçün istifadə olunan Texnologiyaları (Server tərəfi ƏS, FrontEnd, BackEnd, DataBase, IPAddress, UI Frame işləri, Veb serverləri) müəyyən etmək üçün istifadə edilən Wappalyzer Genişlənməsindən istifadə edilir. Wappalyzer Şəkil.3.9-da göstərilmişdir.



Şəkil.3.9 Wappalyzer

Araşdırma zamanı alt domen adlarını və qeydiyyatdan keçmiş e-poçt ünvanlarını müəyyənləşdirmək üçün Harvester alətindən istifadə edilib.

Harvester Aləti yuxarıdakı şəkil.3.10-da göstərilmişdir. Və enumeration prosesi üçün biz hədəf veb tətbiqinin bütün giriş səhifələrini və Admin giriş səhifələrini toplamaq üçün foot printing çapında əsas addım olan GOOGLE DORKING-dən istifadə etdik.



Şəkil.3.10 Harvester Tool

Skanlama

Skanlama Veb Tətbiqinin Zəifliyin Qiymətləndirilməsi və Penetrasiya Texnikasının ən mühüm mərhələsidir. Bu mərhələdə biz istənilən Tətbiqin son nöqtələri adlanan potensial giriş nöqtələrini və portları və zəiflikləri müəyyən etmək üçün hədəf Veb Tətbiqini skan edirik. Bu o deməkdir ki, bura Port daxildir. Veb Tətbiqindəki zəifliyi aşkar etmək üçün skan, Şəbəkə Skanı və siyahıyaalma. Məqaləmiz daha çox Veb Tətbiqi üçün əsas təhlükələr olan açıq Veb Tətbiq Təhlükəsizliyi Layihəsi (OWASP) İstismarlarına, yəni səhvlərə (Zəifliklərə) yönəlmişdir.

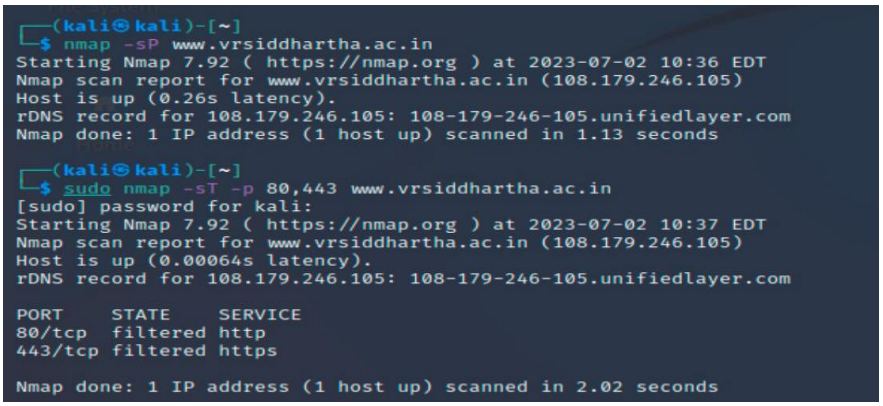
Nmap (Network Mapper) şəbəkənin skan edilməsi və xəritələşdirilməsi üçün istifadə edilən məşhur və güclü açıq mənbə alətidir. O, təhlükəsizlik mütəxəssislərinə

hostları kəşf etməyə, açıq portları müəyyən etməyə və şəbəkə xidmətləri və əməliyyat sistemləri haqqında məlumat toplamağa imkan verir.

1) Host kəşfi

2) Port Skanı

3) Xidmət və versiyanın aşkarlanması



Şəkil.3.11 Nmap skanlama

• AngryIP Scanner: Angry IP Scanner və o, həmçinin IPScan kimi tanınır, şəbəkədəki IP ünvanlarını və əlaqəli portları aşkar etmək və skan etmək üçün istifadə edilən məşhur açıq mənbəli şəbəkə skan alətidir. O, istifadəçilərə şəbəkədəki hostlar haqqında məlumatları tez bir zamanda skan etməyə və toplamağa imkan verən sadə və intuitiv interfeys təqdim edir.

1) IP Ünvanı və Port Skanı
2) Host Məlumatı
3) Qiymətləndirmə
4) Kəşf və Təhlil
5) Hesabat və Yamaq

Wapiti

Wapiti, defolt olaraq kali linux-da əvvəlcədən quraşdırılmış zəifliklərin qiymətləndirilməsi üçün ən yaxşı açıq mənbə alətlərindən biridir. Hədəflənmiş veb Tətbiqinin nüfuz sınağı üçün istifadə olunur. Wapiti, açıq Veb Tətbiqi Təhlükəsizliyi Layihəsi (OWASP) boşluqlarını müəyyən edə biləcəyimiz wapiti alətindən istifadə edərək veb tətbiqi ilə qarşılıqlı əlaqə qurmağın ən yaxşı və sürətli yolu olan komanda xətti interfeysidir.

- Backup faylı
- Blind SQL Injection
- Zəif etimadnamələr
- CRLF inyeksiaysı
- Məzmun Təhlükəsizlik Siyasəti Konfiqurasiyası
- Saytlararası Sorğu Saxtakarlığı
- Potensial təhlükəli fayl
- Komandanın icrası
- Path Traversal
- Htaccess Bypass
- HTTP Təhlükəsiz Başlıqlar
- HttpOnly Flag kukisi
- Open Redirect
- Təhlükəsiz Bayraq kukisi
- SQL injection
- Server tərəfində sorğu saxtakarlığı
- Cross Site Scripting
- XML Xarici Müəssisə
- Daxili Server Xətası
- Resurs istehlakı
- Barmaq izi veb texnologiyası

OpenVAS

OpenVAS zəifliyin hərtərəfli qiymətləndirilməsi və idarə edilməsi üçün güclü açıq mənbəli vasitədir. O, kompüter sistemləri və şəbəkələrində zəiflikləri aşkar etmək və idarə etmək üçün geniş imkanlar təqdim edir. OpenVAS və onun imkanlarının icmalı budur: OpenVAS zəifliyin qiymətləndirilməsini və idarə olunmasını asanlaşdıran məşhur açıq mənbə alətidir. O, təhlükəsizlik zəifliklərini müəyyən etmək və azaltmaq üçün möhkəm funksiyalar dəsti təklif edir. Bu yazıda biz OpenVAS və onun imkanlarını araşdırırıq. onun təhlükəsizlik ekosistemindəki rolu. OpenVAS skaner, menecer və müxtəlif plaginlər daxil olmaqla bir neçə əsas komponentdən

ibarətdir. Arxitektura zəifliklərin səmərəli və dəqiq skan edilməsinə və idarə edilməsi proseslərinə imkan verir. Digər təhlükəsizlik alətləri və çərçivələri ilə inteqrasiya OpenVAS-ın imkanlarını artırır.OpenVAS aktivlərin aşkarlanması və hədəf seçimindən başlayaraq zəifliyin skan edilməsinə sistematik yanaşma tətbiq edir. Skanlar xüsusi tələblərə uyğun olaraq konfiqurasiya edilə və planlaşdırıla bilər. Alət hədəf mühitdə zəiflikləri aşkar etmək üçün müxtəlif skan üsullarından istifadə edir.

Zəifliyin aşkarlanması və qiymətləndirilməsi: OpenVAS geniş spektrli zəifllikləri əhatə edir, o cümlədən, lakin bunlarla məhdudlaşmır:

• Ehtiyat fayl boşluqları
• Blind SQL Injection zəifllikləri
• Zəif etimadnamə zəifllikləri
• CRLF Injection zəifllikləri
• Məzmun Təhlükəsizlik Siyasəti Konfiqurasiya zəifllikləri
• Saytlararası Tələb Saxtalanma zəifllikləri
• Potensial təhlükəli fayl zəifllikləri
• Komandanın icrası ilə bağlı zəifliklər
• Path Traversal zəifllikləri
• HTTP Secure Headers zəifllikləri
• SQL Injection zəifllikləri
• Server Side Request Forgery zəifllikləri
• Saytlararası Skriptləmə zəifllikləri

Bu işdə OpenVas açıq mənbə aləti olan zəifliklərin qiymətləndirilməsi üçün istifadə edilən ikinci alətdir. Aləti istifadə etdikdən sonra şəxsi skan edilmiş hesabatlar üçün giriş etimadnamələri yaradılacaq, biz Veb Tətbiqin Domen adı və ya IP ünvanından istifadə edə bilərik. Openvas aləti skan edildikdən sonra, zəifliklərin şiddətinə görə təsnifatlara görə avtomatik hesabat verir. Və iş performansını verir, veb tətbiqinin tam statistikası yalnız openvas aləti tərəfindən yaradılacaqdır.

Nessus Zəiflik Skaneri: Kompleks Şəbəkə Təhlükəsizliyinin qiymətləndirilməsi aləti şəbəkə təhlükəsizliyinin qiymətləndirilməsi kompleks İT mühitlərində zəifliklərin müəyyən edilməsində və risklərin azaldılmasında mühüm rol

oynayır. Geniş istifadə olunan zəiflik skaneri olan Nessus şəbəkə təhlükəsizliyinin hərtərəfli qiymətləndirilməsi üçün geniş funksiyalar dəsti təklif edir. Bu sənəddə Nessusun arxitekturası, skan etmə metodologiyaları və şəbəkə zəifliklərini aşkar etmək və qiymətləndirmək qabiliyyəti daxil olmaqla, onun dərin tədqiqi təqdim olunur. Bundan əlavə, biz Nessusun təhlükəsizlik zəifliklərinin müəyyən edilməsi və aradan qaldırılmasında praktik tətbiqlərini müzakirə edirik.

1)Giriş:

• Şəbəkə təhlükəsizliyinin qiymətləndirilməsinin əhəmiyyəti

• Nessusun icmalı və onun şəbəkə təhlükəsizliyi mənzərəsindəki əhəmiyyəti

• Digər zəifliklərin skan edilməsi alətləri ilə müqayisə

• Digər təhlükəsizlik alətləri və çərçivələri ilə inteqrasiya

2) Skanlama Metodologiyaları:

• Aktiv və passiv skanlama yanaşmaları

• Şəbəkə skanları üçün fərdiləşdirmə seçimləri

• Zəifliyin aşkarlanması və qiymətləndirilməsi.

3) Nessusun müxtəlif şəbəkə zəifliklərini aşkar etmək və qiymətləndirmək bacarığı, o cümlədən:

• Yanlış konfiqurasiya edilmiş şəbəkə cihazları

• Zəif və ya standart etimadnamələr

• Açıq portlar və xidmətlər

• Köhnəlmiş proqram təminatı və çatışmayan yamalar.

Zəifliklərin təsnifatı: Skanlama addımından sonra aşkar edilmiş boşluqlar Nessus Zəiflik Skaneri tərəfindən hazırlanmış hesabata uyğun olaraq sıralanır.

1) Kritik

2) Yüksək

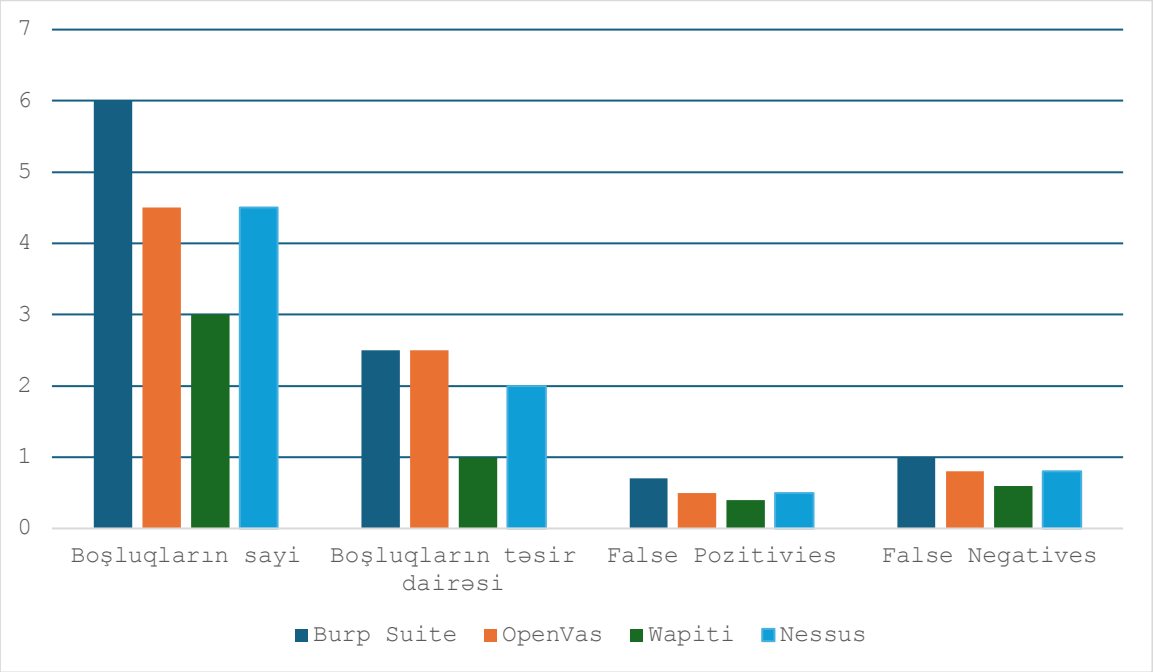
3) Orta

4) Aşağı

Bu işdə hədəf veb-saytda mövcud olan baqların müəyyən edilməsi üçün Nessus zəiflik skanerindən istifadə etdirik. Nessus veb tətbiqi zəifliklərinin qiymətləndirilməsi üçün istifadə olunan açıq mənbə zəiflik skaneridir (Zərərli proqramların aşkarlanması,

Ransomware aşkarlanması, Şəbəkə Skanı, Host Kəşfi.). Nesus aləti quraşdırıldıqdan sonra biz aləti bütün portları və protokolları skan etmək üçün konfiqurasiya etdik. Konfiqurasiyadan sonra biz Veb Tətbiqin istifadə olunan domen adları skan edildikdən sonra zəifliklərin şiddətinə görə təsnifat əsasında hesabat hazırlandı.

Nəticə və Müzakirə: Şəkil.3.12 davamlı zəifliyin qiymətləndirilməsi üçün istifadə edilən müxtəlif hibrid platformaları müqayisə edir. Zəifliyin skan edilməsinin nəticələrinə əsasən, Burp Suit Professional aləti zəifliyin aşkarlanması baxımından ən yaxşısını göstərmişdir. Veb proqramlarının təhlükəsizliyini qiymətləndirmək üçün güclü və effektiv vasitə kimi Burp Suite Professional seçilir. Onun uyğunlaşdırıla bilən skan etmə xüsusiyyətləri, interaktiv əl testi üçün dəstək, autentifikasiya və sessiyaların effektiv idarə edilməsi, proksi kimi real vaxt rejimində sınaq funksiyaları və güclü istifadəçi icması tərəfindən dəstəklənən davamlı yeniləmələr, hamısı onu müxtəlif proqramları tapmaqda ,zəifliklər və veb proqram təhlükəsizliyində dəyişən problemlərin həllini effektiv etmək üçün birlikdə işləyir. O, həm Windows, həm də Linux mühitlərində geniş spektrli boşluqları yoxlaya bilər. Alətlərin Performans göstəricilərinin müqayisəsi aşağıdakı cədvəl.2-də göstərilmişdir.



Şəkil.3.12 Skanlama alətlərin müqayisəsi

Dizaynerlər real məlumatlardan istifadə etməklə müxtəlif zəifliyin qiymətləndirilməsi üsullarının müqayisəsini təqdim ediblər (Windows -Nessus və Burp Suite Professional,

həmçinin saytlararası skript zəifliyi və kali Linux - Wapiti daxildir). Bu sənəddə tətbiq edilən təklif olunan çərçivə digər faktiki zəiflik mühitləri üçün etalon kimi istifadə oluna bilən Açıq Veb Tətbiqi Təhlükəsizliyi Layihəsi (OWASP) çərçivəsidir. Zəiflik skanımızın nəticələrinə əsasən, Burp Suit Professional aləti zəifliyin aşkarlanması baxımından ən yaxşısını həyata keçirir, çünki o, veb proqramında mövcud ola biləcək bütün növ zəifliklər skan edə bilir və həm Windows, həm də Linux üçün əlçatandır.

Alətlər	Nessus	OpenVas	Wapiti
Tapılmış boşluqların növləri	TLS versiyası 1.0 Protokol aşkarlama	Backdoor tapılması	Backup faylı
	TLS versiyası 1.0 Protokol aşkarlama	X Server	Blind SQL inyeksiyası
	Nessus SYN skanlama	Remote kod inyeksiyası boşluğu	Zəif verilənlər
	SSL/TLS versiyası	PostgreSql boşluqları	CLRF inyeksiyası
	SSL sertifkatlaşdırma	PostgreSql zəif şifrləmə	CSRF
	SSL imzalı sertifikatın zəif heş alqoritmi istifadəsi	phpMyAdmin konfuqrasiya faylına PHP kod inyeksiyası	Potensial təhlükəli fayıllar
	SSL Blok şifrləmə dəstəklənməsi	Phpinfo() çıxış məlumatlarının əlçatanlıq	Command execution
	SSL root sertifikatı	PostgreSql boşluqları	Path Traversal
	SSL /TLS son istifadə edilmiş şifrələr	PostgreSql “bitsubstr” Bufer daşması boşluğu	HTTP headeHTTPOnly kuki
	Xidmətlərin aşkarlanması	PostgreSql “intarray” Bufer daşması boşluğu	Təhlükəsiz kuki flag
	TLS next protokol dəstəklənməsi		SQL injection
	TLS versiyası 1.1 Protokol aşkarlama		XSS

Cədvəl.3.2 Alətlərin Performans göstəricilərinin müqayisəsi

Hər bir alətin də öz üstünlükləri və mənfi cəhətləri var. Nessusun bir çatışmazlığı onun ".org" domen adlarını qəbul etməməsidir, lakin Windows-da işlədiyi üçün istifadəsi sadədir. Buna baxmayaraq, Wapiti-də ona yalnız Kali Linux vasitəsilə daxil olmaq mümkündür.

FƏSİL IV Mövcud Boşluqların və Təhditlərin Qarşısının alınması Modeli

4.1 Veb təhditlərin qarşısının alınması üçün kompleks yanaşma

Veb proqramları internet üzərindən təqdim olunan bir çox xidmətlər üçün əsas interfeys rolunu oynayan qurumların mühüm aspektinə çevrilmişdir. Nəticə etibarilə, bu xidmətlərin artan nüfuzu ilə əlaqədar olaraq veb proqramlara qarşı hücumlar artır. Təhlükəsizliyə marağın olmaması, qeyri-kafi məlumatlılıq və təhlükəsiz proqram təminatının inkişaf etdirilməsi üsullarından istifadə edilməməsi də daxil olmaqla bir neçə faktor səbəbindən veb tətbiqləri hücumların əsas hədəfinə çevrilib. Veb əsaslı hücumların təxminən 70%-nin uğurlu olduğu təxmin edilir. Ənənəvi firewalllar şəbəkə qatının hücumlarının qarşısını almaqda təsirli olsa da, veb proqramları hədəf alan hücumlardan müdafiədə zəif olur. Buna görə də, mahiyyət etibarilə etibarsız mühit olan internetdə veb proqramları qorumaq, həssas məlumatları qorumaq və zəifl ikləri azaltmaq üçün gücləndirilmiş təhlükəsizlik tədbirlərinə ciddi ehtiyac var.

Veb tətbiqləri bir çox hücumların vektoru olan hiper mətinlərin ötürülməsi protokolu üzərində işləyir. Çoxsaylı tədqiqatlar zərərli HTTP trafikinin aşkarlanmasına və anormal sorğuların müəyyən edilməsinə yönəlmişdir. Veb Tətbiq Təhlükəsizliyi Konsorsiumu (ing. Web application security consortium) kimi təşkilatlar Ümumdünya Şəbəkə üçün təhlükəsizlik standartlarının işlənib hazırlanmasında mühüm rol oynayıblar. Digər diqqətə layiq təşəbbüs, imza əsaslı aşkarlamanı həyata keçirən Apache veb serveri üçün açıq mənbə modulu olan Thinking Stone-un ModSecurity - dir. ModSecurity məlum hücum növlərinə qarşı effektiv olsa da, sıfır gün hücumlarını aşkar etməkdə zəifdir.

Almgren, Debar və Dacier tərəfindən təklif olunan diqqətə layiq sistem veb serverlərdə Ümumi Giriş Formatından (ing. common log format, CLF) istifadə edərək hücumların davamlı olaraq araşdırılmasına və təhlilinə yönəlib. Bu yanaşma HTTP sorğularını təhlil etmək üçün qeydləri qeyd etmək üçün bir sıra anomaliya aşkarlama proseslərini tətbiq etməyi nəzərdə tutur. Bununla belə, bu metodologiya HTTP sorğuları və cavablarının əhatə dairəsi ilə məhdudlaşır.

Valeur və başqaları. veb proqramların kritik və qeyri-kritik kateqoriyalara diferensiallaşdırılmasını nəzərdən keçirərək, proxy prosesinə bənzər şəkildə fəaliyyət

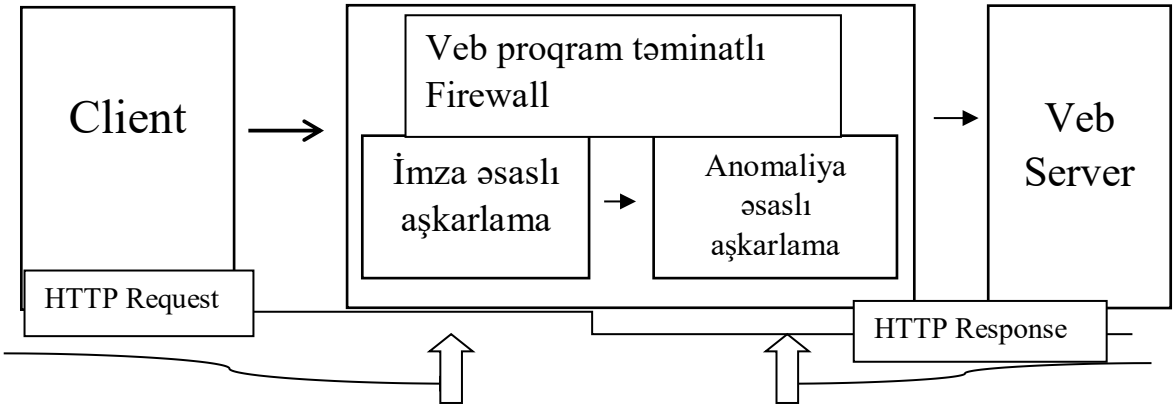
göstərən bir struktur təklif etdi. Bu struktur HTTP sorğularını normal və ya anomal kimi təyin edilmiş müxtəlif veb serverlərə yönləndirir. Veb serverlərə yalnız kritik olmayan proqramları işlətməyə icazə verməklə, potensial hücumların təsiri azaldıldı.

Valeur, Mutz və Vigna anomal sorğuları müəyyən etməklə SQL inyeksiya hücumlarının qarşısını almaq məqsədi ilə SQL sətirlərini daxil etmək üçün MySQL-də libmysqlclient kitabxanasından istifadə edirdilər. Onlar bu cür anomaliyaları aşkar etmək üçün nəzərdə tutulmuş LibAnomaly adlı alət hazırlayıblar. LibAnomaly alətindən istifadə edərək, onlar log faylında qeydə alınmış SQL sətirlərinin təhlili vasitəsilə hücumları müəyyən edə bildilər.

Kruegel sorğu növü, sorğunun uzunluğu və yük bölgüsü kimi parametrlər əsasında anomaliya balı əldə etmişdir. Onların yanaşması bildirir ki, əgər sorğunun uzunluğu orta sorğu uzunluğundan çox olarsa, sorğunun hücum olma ehtimalı yüksəkdir. Onlar həm HTTP, həm də DNS trafikini təhlil edərək DNS hücumlarını aşkar etmək üçün prototip hazırlayıblar.

Veb-hücumların aşkarlanmasının digər yanaşmalarından biri Kruegel və Vigna tərəfindən ifadə edilən xarakter paylama üsuludur (ing. character distribution method) ki, bu da hücum sorğularının xarakter paylanmasının normal sorğuların xarakter paylanmasından fərqli olduğunu göstərir. Tədqiqatda məlumat mənbəyi kimi sorğu parametrlərindən istifadə edilmişdir. Sessiya anomaliyasının aşkarlanması anomaliya aşkarlanması ilə bağlı Cho və Cha tərəfindən aparılan başqa bir araşdırmadır. İstifadəçilər tərəfindən axtarılan veb səhifə sessiyalarının oxşar xüsusiyyətlərə malik olduğu hesab edilmişdir. SAD log qeydlərindən veb sessiyaları aşkar edir, müəyyən sorğu sifarişləri üçün profillər tərtib edir və hesablamalar aparır. Bu tədqiqatda HTTP sorğuları, imza əsaslı aşkarlama və anomaliya aşkarlanması ilə hibrid metod təklif olunur. İmza əsaslı aşkarlama ümumi hücum növlərinə qarşı imza qara siyahısından istifadə etməklə hücumlar da daxil olmaqla sorğuların qarşısını alır. Anomaliya sorğunun aşkarlanması standart HTTP sorğu standartına uyğun olmayan sorğuların aşkarlanmasıdır. HTTP sorğularında imza əsaslı aşkarlama və anomaliya aşkarlanmasından istifadə etməklə aşkarlama prosesi həyata keçirilə bilər. Anomaliya sorğusunun aşkarlanması sıfır gün hücumları üçün effektiv olsa da, bu üsul digər

üsullardan daha yavaş işləyir. Bu işdə, imza əsaslı aşkarlama və anomaliya aşkarlama modellərindən istifadə edərək, daha sürətli işləyən hibrid üsul hazırlanmışdır. Anomaliya sorğunun aşkarlanması sorğunun uzunluğuna, sorğuların sayına və məktub tezliyinin təhlilinə əsasən həyata keçirilib. Təklif olunan modelin blok diaqramı Şəkil.4.1.1-də verilmişdir.



Şəkil.4.1.1

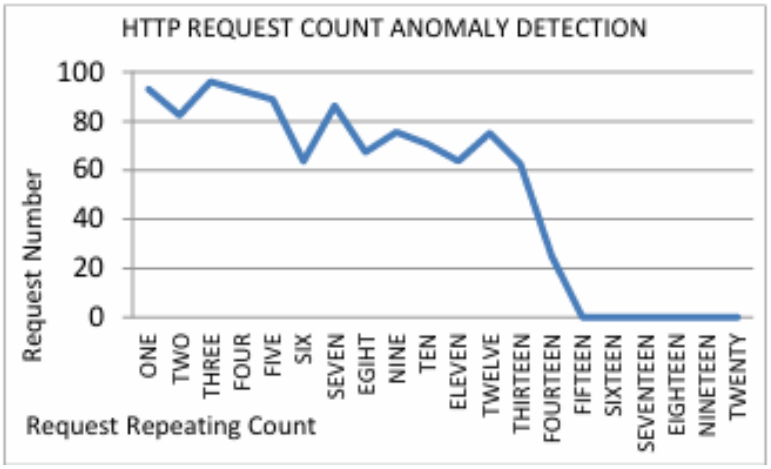
Şəkil.4.1.1-də göstərildiyi kimi, müştəri tərəfindən göndərilən HTTP sorğusu veb serverə çatmazdan əvvəl müvafiq olaraq imza əsaslı aşkarlama və anomaliya aşkarlama prosesləri tətbiq edilir. Hər şey normal görünəndə sorğu icra olunur və ya hücum kimi aşkar edilərsə bloklanır. Sorğunun aşkarlanması mərhələləri aşağıda göstərilmişdir.

Anomaliyaların aşkarlanması

Anomaliyaların aşkarlanmasında veb tətbiqinin normal davranışı ümumiyyətlə statistik metodların köməyi ilə əldə edilir. Bundan əlavə, anomaliya əsaslı aşkarlama metodlarında mühüm məlumat olan anomaliya balından istifadə edilir. Anomaliya hesablama parametrləri düzgün seçildikdə sistemin müvəffəqiyyət nisbəti artır. Anomaliyaların aşkarlanmasında aşağıdakılar istifadə edilmişdir: sorğu sayının təhlili, sorğu uzunluğunun təhlili və sorğu tezliyi metodlarının təhlili.

Sorğu Sayının Təhlili: Fərqli istifadəçilər müxtəlif yerlərdən eyni sorğu göndərə bildiyi üçün normal sorğular internet saytının ziyarət sayına görə davamlı olaraq təkrarlanır. Hücum sorğularının təkrarlanma ehtimalı normal sorğulardan daha aşağıdır. 20-yə qədər təkrarlanan sorğuların sayları Şəkil.4.1.2-də verilmişdir. Şəkil.4.1.2-ə əsasən, hücumun az sayda təkrarlanma ehtimalı çox sayda təkrarlanan

hücumdan daha yüksəkdir. Hazırlanmış tətbiqə görə, 15-dən çox təkrarlanan sorğular hücum deyil.



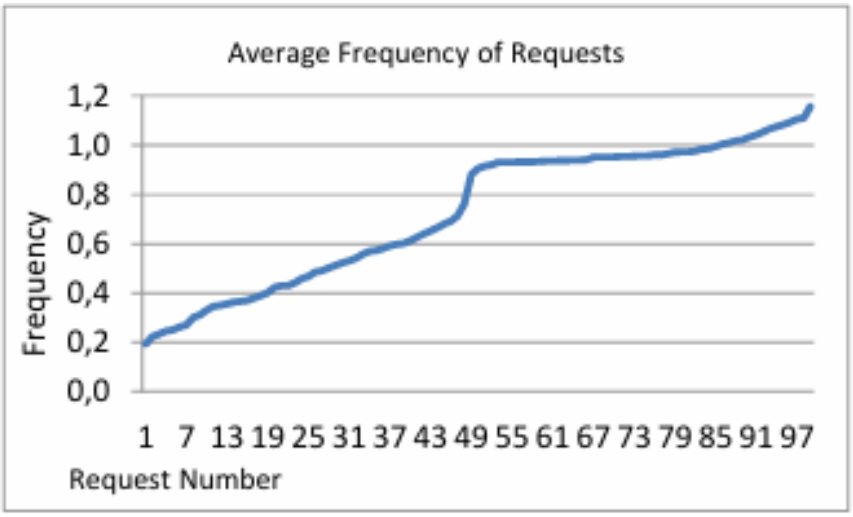
Şəkil.4.1.2

Sorğunun Uzunluğunun Təhlili : Veb tətbiqi tərəfindən qəbul edilən sorğuların strukturu onun əsas arxitekturasından təsirlənir. Anomaliyaların aşkarlanması üçün istifadə edilən xarakterik xüsusiyyətlərdən biri sorğunun uzunluğudur. Yaddaşın daşması və saytlararası skript hücumları ilə əlaqəli sorğular adətən normal sorğularla müqayisədə daha böyük uzunluğa malikdir. Bu yanaşma anormal sorğuların uzunluğuna görə müəyyən edilməsinə imkan verir, yaddaşın daşması və saytlar arası skript kimi potensial hücumların aşkarlanmasını asanlaşdırır.

Veb proqramlarının təhlükəsizlik ehtiyaclarını təmin etmək üçün bir çox tədqiqatlar aparılır. Bu işdə imza əsaslı aşkarlama və anomaliya sorğularının aşkarlanmasından istifadə etməklə hibrid sistem hazırlanmışdır. Bu inkişaf etdirilən sistemdə həm imza əsaslı aşkarlama, həm də anomaliya sorğularının aşkarlanması metodlarından istifadə edildiyi üçün iki metodun çatışmazlıqları aradan qaldırıldı. İmza əsaslı aşkarlama daha sürətli işləyir, lakin sıfır gün hücumlarına qarşı effektiv deyil. Digər tərəfdən anomaliya aşkarlama metodu sıfır günə hücumlara qarşı təsirlidir.

Sorğu Tezliyinin Təhlili: Sorğuların simvol tezliyi qiymətləri xarakter paylama modelinin köməyi ilə müəyyən edilir. Veb tətbiqinə gələn normal sorğuları təşkil edən simvolların hərf tezliyi qiymətləri anomaliya sorğularının hərf tezliyi qiymətlərindən

yüksəkdir. Simvolların paylanmasında ASCII simvollarından istifadə olunur. Hərf tezliyi təhlili ümumiyyətlə kriptoanaliz metodlarında istifadə olunan bir texnikadır. Bu araşdırmada hər bir simvolun ümumi sayını sorğulardan və orta dəyərdən aşkar etmək üçün hərf tezliyi təhlili aparılmışdır. index.php?secim=9&mid=50 kimi sorğu istifadə olunarsa, bu ifadənin hərflərinin tezliyi və orta qiymətləri alınır. Tezlik dəyərləri bütün sorğular üçün hər hərfin sayını göstərdiyi halda, orta qiymətlər hər simvolun ümumi dəyərlərini sorğu sayına bölmək yolu ilə tapılır. Veb tətbiqinə göndərilən 100 sorğunun tezlik qiymətləri kiçikdən böyüyə sıralandıqda, orta tezlik qiymətləri 0,9-dan kiçik olan sorğular anomaliya kimi müəyyən edilir. Qiymətləndirilmiş sorğuların orta tezlik qiymətləri Şəkil.4.1.3 -də göstərilmişdir.



Şəkil.4.1.3

İmza əsaslı aşkarlama

İmza əsaslı aşkarlama, həmçinin sui-istifadənin aşkarlanması kimi tanınan, əvvəlcədən təyin edilmiş imzalara və ya məlum hücumların nümunələrinə əsaslanır. Bu sistemlər adətən daha sürətli işləyir, lakin yalnız verilənlər bazasındakı mövcud imzalara uyğun gələn hücumlara qarşı effektivdir. Müdaxilənin aşkarlanması sistemləri (IDS) və antivirus proqramları adətən imza əsaslı aşkarlamadan istifadə edir. İmza aşkarlanması ilə SQL inyeksiyası, XSS, CSRF və Bot hücumlarının qarşısı alına bilər. SQL inyeksiyası, XSS, CSRF-nin qarşısının alınması etibarlı olmayan məlumatların aktiv brauzer məzmunundan ayrılmasını tələb edir.

Veb proqramlarının təhlükəsizlik ehtiyaclarını təmin etmək üçün bir çox tədqiqatlar aparılır. Bu işdə imza əsaslı aşkarlama və anomaliya sorğularının aşkarlanmasından istifadə etməklə hibrid sistem hazırlanmışdır. Bu inkişaf etdirilən sistemdə həm imza əsaslı aşkarlama, həm də anomaliya sorğularının aşkarlanması metodlarından istifadə edildiyi üçün iki metodun çatışmazlıqları aradan qaldırıldı. İmza əsaslı aşkarlama daha sürətli işləyir, lakin sıfır gün hücumlarına qarşı effektiv deyil. Digər tərəfdən anomaliya aşkarlama metodu sıfır günə hücumlara qarşı təsirlidir.

4.2Anomaliyaların aşkarlanması vasitəsilə Veb Tətbiq Firewalllarının təkmilləşdirilməsi

Ən çox yayılmış zəifliklər aradan qaldırmaq üçün MODSECURİTY, əsas qayda dəsti (OSP CRS) olaraq bilinən bir sıra standart qaydalar təklif edir.Bununla birlikdə, yalnız qaydalara əsaslanan yanaşmanın bəzi çatışmazlıqları var: Qaydalar təbiətdə statik və sərtdir, buna görə də OSP CRS ümumiyyətlə bəzi hallarda 40% - ə çata biləcək yüksək saxta pozitiv faiz verir. MODSECURİTY hücumların qarşısını almaq üçün nəzərdə tutulduğundan, bu qədər yüksək saxta pozitivlik potensial olaraq tətbiqin xidmətdən imtina etməsinə (DoS) səbəb ola bilər.

Bununla birlikdə, qaydaların qurulması hər bir xüsusi veb tətbiqi üçün əl ilə yerinə yetirilməli olan vaxt aparan və səhvlərə meylli bir işdir. Ənənəvi şəbəkə təhlükəsizlik divarlarında və IDS-də qaydalara əsaslanan yanaşma daha yüksək səviyyədə rahatlıq və uyğunlaşma təmin edən digər maşın öyrənmə vasitələri ilə uğurla tamamlandı. Bu yanaşmalar, normal istifadədən (anomaliyalardan) kənara çıxan və mövcud hücumlara uyğun ola biləcək şübhəli vəziyyətləri aşkar etmək üçün normal veb tətbiqetmə davranışının öyrənilə biləcəyi nümunə məlumatlarından faydalanır. Bu yazıda təqdim etdiyimiz iş, bu cür anomaliya aşkarlama üsulları ilə MODSECURİTY aşkarlama imkanlarının yaxşılaşdırılmasına kömək edir.

Məqalənin qalan hissəsinin strukturu aşağıdakı kimidir: II Bölmə bəzi məlumatlar təqdim edir və maşın öyrənmə üsullarından istifadə edərək MODSECURITY -ni artırmaq üçün təklifimizi irəli sürür. III bölmə statistik WAF-ı əsaslandırmaq üçün istifadə etdiyimiz iki tamamlayıcı öyrənmə modelini təqdim edir.

Sonra IV Bölmə eksperimentlərin nəticələrini təsvir edir və müzakirə edir. V bölmə əlaqədar işləri nəzərdən keçirir. Əlavə iş və nəticələr VI Bölmədə təqdim olunur.

OWASP CRS (ing. open web application security project, OWASP, core rule set, CRS) qaydalarından istifadə etməklə konfiqurasiya edilmiş MODSECURITY -nin aşkarlama və dəqiqlik imkanlarını artırmaq üçün biz əvvəlcə bir sinif təsnifatı birləşdirən mexanizmlə sınaqdan keçirdik. Bu, sorğunu təsnif etmək üçün mütəxəssisi birləşdirir. Hər iki ekspert razılaşdıqda (hər ikisi etibarlı və ya hücum deyir), nəticə sadədir. Bir sinifli yanaşma sorğunu hücum kimi təsnif etdiyi halda, OWASP CRS qaydalarının hücumlara dair nou-hauları təcəssüm etdirdiyini nəzərə alaraq ModSecurity cavabını prioritetləşdiririk (C. Folini. 2016) .

Bu inteqrasiya qərarı həm də yanlış pozitiv aşkar etdiyimiz halda WAF-ımızı tənzimləmək üçün ən yaxşı mexanizmə malik olmağa imkan verir: bu sorğunun hücum olmadığını müəyyən edən ModSecurity qaydalarına dəyişiklik etməliyik. Bu qaydanın tənzimləməsi bu gün OWASP CRS ilə istifadə edilənlə eynidir.

Nəhayət, bir sinif sorğunu etibarlı, ModSecurity isə hücum kimi təsnif etdiyi halda biz bir sinfə üstünlük veririk, çünki OWASP CRS-in yüksək yanlış müsbət göstəricilərə malik olduğu bilinir. Bu yanaşma, tətbiq üçün xüsusi təlim verilənlər toplusunun mövcud olmadığı ssenariyə kifayət qədər yaxşı uyğunlaşdığını göstərdi. Biz bir sinifli klassifikatoru bir neçə verilənlər toplusundan istifadə edərək öyrədirik və nəticədə əldə edilən təsnifat modeli müxtəlif veb tətbiqlərini qorumaq üçün istifadə edilə bilər. Əsas üstünlüyü ondan ibarətdir ki, onun yerləşdirilməsi asandır və veb proqramdakı dəyişikliklərə uyğunlaşa bilir.

Bununla belə, oneclass yanaşmasının təmin etdiyi aşkarlama imkanları həm sıfır gün hücumlarının, həm də tətbiqin xüsusi zəifliklərindən, xüsusən də şübhəli daxilolmalardan istifadə edən hücumların qarşısını almaq üçün o qədər də yaxşı uyğunlaşmır. Buna görə də araşdırdığımız ikinci yanaşma veb tətbiqi üçün gözlənilən (etibarlı) giriş dəyərlərini xarakterizə etməyə və ona verilən hər hansı anormal girişi potensial hücum kimi təsnif etməyə yönəlmişdir. Bundan əlavə, bu müsbət xarakteristikaya yanaşma WAF-ı öyrətmək üçün yalnız düzgün istifadəçilər tərəfindən istehsal edilən etiketlənməmiş HTTP sorğularının toplusunu tələb edir.

Bu ikinci yanaşma üçün tətbiq girişlərindəki n-gram tezliklərinin bəzi n-lərə qədər təhlili ilə sınaqdan keçirdik. Bununla belə, bu daha yüksək çeviklik və performans üçün ödəməli olan qiymət ondan ibarətdir ki, n-qram modelini öyrətmək üçün etibarlı sorğu ilə xüsusi proqram üçün məlumat dəsti tələb olunur. Bir veb tətbiqetmənin müsbət xüsusiyyətinin ikinci dezavantajı, bəzi hallarda bəzi giriş parçaları üçün gözlənilən davranışın olmamasıdır. Məsələn, istifadəçinin parol dəyərlərində gözlənilən səhv olmamalıdır. Belə hallarda simmetrik bir yanaşma tətbiq etmək və mövcud texnika səviyyəsinə uyğun olaraq parol hücum imzalarını axtarmaq lazımdır. Bu, etiketli bir təlim məlumat dəstindən çıxarılan və təhlükəsizlik mütəxəssisinin cari hücum vektorları haqqında biliklərini bir sinif təsnifat yanaşmasında olduğu kimi təqdim edən diqqətlə seçilmiş tokenlər tapmaq üçün gəlir. Bu metod, əvvəlki təlimə görə hücum kimi tanınmadığı təqdirdə, HTTP sorğusunu etibarlı olaraq tanıyır. Girişin işlənməsinin bu üsulu təhlilə one-class və n-qram yanaşmaları arasında ikinci bir tamamlama səviyyəsini təmin edir.

Xülasə, xüsusi verilənlər bazası olmadan və ya veb tətbiqi daim dəyişmədən (məsələn, məzmun meneceri tərəfindən dəstəklənən ictimai veb-sayt) veb tətbiqini qorumaq üçün WAF-ı tez yerləşdirməyə ehtiyacımız varsa, biz one-class yanaşmasından istifadə etməyi təklif edirik. Bu halda (Senari I) biz aşağıdakı sualı həll etmək istərdik: Digər veb proqramlarından toplanmış təlim məlumatlarından öyrənilən hücumun aşkarlanması sistemini qurmaq mümkündürmü? Bu ssenaridə ikinci sual MODSECURITY ilə bağlıdır: Anomaliya aşkarlama metodlarından istifadə edərək MODSECURITY nəticələrini təkmilləşdirə bilərikmi?

Yəni MODSECURITY tərəfindən yaradılan yanlış pozitivlərin (FP) sayını azalda bilərikmi? Yüksək səviyyəli təhlükəsizlik tələb olunduğu və tətbiqin dəyişikliklərinin idarə olunduğu kritik veb tətbiqini qorumalı olduğumuz ssenaridə biz n-qram yanaşmasını tətbiq edə bilərik. Bu ikinci halda (Ssenari II), tətbiqin hər yeni tətbiqindən əvvəl proqram təminatının sınaq mərhələsindən sahib keçməsi tələb olunur, beləliklə, xüsusi təlim məlumatları mövcud olacaqdır. Bu sonuncu ssenaridə biz MODSECURITY ilə müqayisədə anomaliya aşkarlama metodlarının əldə edilə bilən performansını anlamaq istərdik.

Öyrənmə Modelləri

Anomaliyaları aşkar etmək üçün təklif olunan modellər, HTTP sorğusunun əvvəlcədən işlənməsi, işarələrin vurğulanması və T təlim dəstindən istifadə edərək modelin öyrədilməsinin standart ardıcıllığını izləyir . Birincisi, sorğular onlarda olan məlumatları deşifrə etmək üçün əvvəlcədən işlənir. Sonra sorğuda bir sıra alt sətirlərin və ya işarələrin görünməsi ilə əlaqəli bir sıra xüsusiyyətlər çıxarılır. Model, yeni sorğunu məqbul və ya anormal olaraq təsnif etmək üçün jeton görünüşlərinin paylanmasını araşdırır. Bu təsnifat ilə birlikdə model normallığı qiymətləndirir. Bu hissənin qalan hissəsi iki fərqli modelin təsvirinə həsr edilmişdir: one-class yanaşması və n-qram analizi.

A. One-class yanaşması

Bu yanaşmada, əvvəlcədən emal mərhələsində dekodifikasiya istifadəçi-agent və server arasında kontekstual məlumat mübadiləsi üçün istifadə olunan sorğu başlıqlarının filtrasiyası ilə birlikdə həyata keçirilir. Kukilər, proksilər və İP kimi, istifadəçi davranışını təmsil etməyən və tətbiqin davranışını təxmin etmək kimi qəbul edilməməli olan protokola xas olan başlıqlarda olan bütün məlumatlar süzgəcdən keçrilir. [6] dan sonra biz tanınmış veb proqram hücumlarının xassələrini ələ keçirən xüsusiyyətləri müəyyən etmək üçün təhlükəsizlik mütəxəssisinin təcrübəsinə istinad etdik. Müəyyən edilmiş xüsusiyyətlərə simvollar (p.e. <, =, |) və tokenlər (p.e. seçin, passwd) daxildir. Biz “a bag-of-words” modelini tətbiq edirik, burada hər bir sənəd (bizim vəziyyətimizdə hər sorğu) həmin sözlərdən ibarət çanta kimi təmsil olunur. Etibarlı sinfi modelləşdirdiyimiz üçün hər sorğuda bu sözlərin bir neçəsinin olacağını gözləyirik (C. Raıssi, J. Brissaud, G. Dray, P. Poncelet, M. Roche, and M. Teisseire, 2007).

B. n-gram yanaşmasından istifadə edərək anomaly aşkarlama

İkinci yanaşmamıza baxdığımızda, hər bir tətbiqin normal davranışını müsbət şəkildə xarakterləndirmək üçün n-gramları token kimi istifadə etməyə çalışırıq.

Bir mətnin dilini təyin etmək üçün geniş tanınan bir texniki n-gram adlanan mətn istifadə olunan hər bir n ardıcı tokenın nisbi tezliyini ölçməkdir. Bu n-gramlar müxtəlif elementləri təmsil edə bilər, məsələn, ASCII simvolları, sözlər və s.

Bu tokenləşdirmə proseduru dil və ya mətn strukturu fərqlənməsindən asılı olmadan bərabər şəkildə tətbiq oluna bilər.

Biz HTTP strukturundan geniş istifadə etməyi nəzərə alaraq, hər bir CGI parametr və HTTP başlığı (daha sonra sahələr adlanır) üçün müəyyən bir n-gram tezliyinin hesablanması ilə yanaşmağı həyata keçiririk. Bu tezliyə hər bir sahənin dil imzası təqdim edirik. Belirli bir uzunluğa (n) qədər n-gramları nəzərə alır və mətni kiçik hərflərə çevirərək, aksentləri silərək və rəqəmləri böyük hərf "N" ilə əvəzləyərək mətni normalizləyərək onları sayırıq. Əlavə olaraq, model, hər bir sahənin (x) uzunluğu olaraq adlandırılan əlavə bir xüsusiyyətlə genişləndirilir. Bu əlavə xüsusiyyət kodun daxil olması ilə bağlıdır, çünki onlar çoxlu gözlənilən sahə uzunluğuna səbəb olur.

Məlumatlar M olmaqla hər bir sahə x üçün hesablanmış n-gram tezliklərinin dağılımını göstərir, bunlar təlim dəsti T-dən hesablanır. Verilmiş bir HTTP sorğusu r-ni test etmək üçün, Veb Tətbiqetmə Firewall (WAF) hər bir sahə rx-in hər bir n-gram z-nin tezliyini fr(x.z) hesablayır. Əgər x model M-də təyin edilməmişdirsə, onda r rədd edilir. Əks təqdirdə, n-gram müstəqil olma gərəkliliyi ilə aşağıdakı Mahalanobis məsafəsinin versiyasını istifadə edərək hər bir sahə x üçün sr.x = Σi=1..n distx_i(r, M) hesablanır:

Burada \(|T_{xi}| \) model sahəsi x üçün i-gramların sayını təmsil edir. Səbətə sıfır tezliyə malik n-gramlar üçün sıfıra bölmədən qorunmaq üçün konstant \(\frac{1}{|T_{xi}|} \) məqəmə əlavə olunur.

Bir hesab qəbul edilən hesablama olaraq dəyərlərinin T-dən çəkilmiş hesab distributivsı ds tərəfindən çəkilən minimum və maksimum dəyərlər arasında düşdüyü zaman hesab olunur, hər bir müəyyən təlim sorğusunun hesabını qiymətləndirərək hesablanır. Əgər əldə edilən hesab x sahəsi üçün min-max intervalında deyilsə, bütün sorğu anormal (potensial olaraq hücumu göstərə bilər) kimi kateqoriyalanır.

Əgər x sahəsinin müəyyən n-gramı M-də təyin edilməyibsə, x sahəsinin məzmununun öncədən təyin edilmiş bir dağılımı onun gözlənilən tezliyini hesablamaq üçün istifadə edilir. Bəzi CGI parametrlərini öncədən təyin etməklə, yanlış müsbət nisbətlər azaldılır. Hər bir sahə x üçün xüsusi öncələri, n-gram uzunluqları və digər

model parametrləri, hər bir veb tətbiqinin model tənzimləməsinin bir hissəsi olaraq konfiqurasiya edilir.

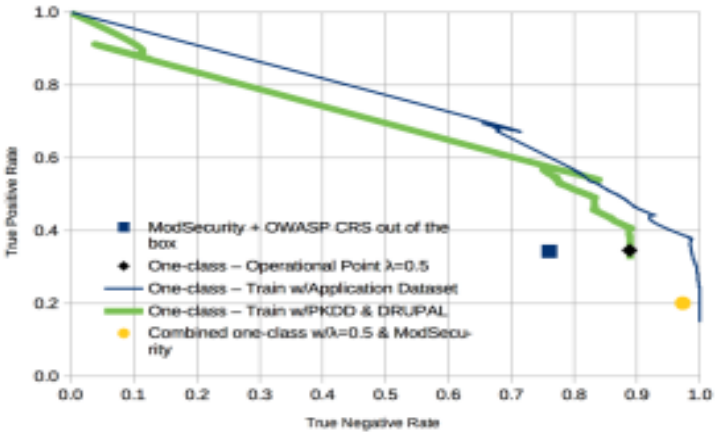
Təklif olunan modelləri CSIC2010 məlumat dəsti və universitetin veb serverinə (Drupal dataset) HTTP trafikindən əldə edilən məlumat dəsti əsasında qiymətləndirdik. Bundan əlavə, pkdd2007 challenge - dən alınan bir məlumat dəstində sinif yanaşması ilə sınaqdan keçirdik. Bununla birlikdə, PKDD2007 verilənlər bazası, URL-ləri, parametr adlarını və dəyərlərini təsadüfi məlumatlarla əvəz edən inkişaf etdiricilər tərəfindən qarışdırıldığı üçün n-g yanaşması ilə təcrübə üçün uyğun deyildi (M. Exbrayat ,2007).

Hər bir məlumat dəsti, bir təlim məlumat dəstinə və etibarlı və anormal trafik ehtiva edən iki test məlumat dəstinə bölünmüş bir sıra tam HTTP sorğularını (başlıq və gövdə) ehtiva edir. Daha əvvəl də qeyd edildiyi kimi, modellərimiz normal trafikdən yalnız təlim üçün istifadə edir, etiketli hücumlar isə yalnız test məqsədləri üçün nəzərə alınır. Modelin qiymətləndirilməsi həqiqi müsbət tezliyə (TPR) və həqiqi mənfi tezliyə (TNR) əsaslanırdı, burada TPR hücumlar kimi düzgün tanınan anormal sorğuların faizini, TNR isə normal trafik kimi düzgün müəyyən edilmiş etibarlı sorğuların faizini təmsil edir.

Modellərimizin davranışlarını, "qutudan kənar" versiyası 2.2.9 ilə konfiqurasiya edilmiş MODSECURİTY istifadə edərək əldə edilən əsas məlumatlarla müqayisə etdik.

Bir sinif təsnifatında təsnifatçının əsas parametri klasterlərin ölçüsünü təyin edən eşikdir. Bu ölçü, dəyərləri 0 ilə 1 arasında dəyişən bir parametr ilə tənzimlənir, hər bir dəyər təsnifatçının işləmə nöqtəsini təyin edir.

	Train (Valid)	Test (Valid)	Test (Attack)
CSIC	36000	36000	25065
Drupal	45907	19675	1287



Şəkil.4.2.1

Qrafikdə mavi incə xətt, bir-sinif sinifləndiricisinin qurulması üçün xüsusi məlumatlar istifadə olunduğu zaman əldə edilən kurvanı təmsil edir, burada λ dəyərləri (0, 1] aralığında dəyişir. Bu kurva sinifləndirici üçün ideal nəticə hesab edilə bilər, çünki tətbiq üzrə xüsusi təlim datasetindən istifadə edir.

Yaşıl qalın xətt, digər veb tətbiqlərindən məlumat istifadə edilərək təlim alınmış bir-sinif sinifləndiricisi üçün əldə edilən kurvanı təmsil edir (Senariya I). Siyahı üzərinə yerləşdirilmiş qara mümkün olan əməliyyat nöqtəsini göstərir, λ = 0.5 dəyəri ilə əldə edilən standart əməliyyat nöqtəsini göstərir. Xüsusilə təlimat verilmiş məlumatların mövcud olmadığı Senarioda, əməliyyat nöqtəsinin dəqiqliyini tənzimləmək mümkün deyil. Beləliklə, bu nöqtə təlim dəstinin yanlış müsbət nisbətlərinin sayına əsaslanaraq sabitləşdirildi (Betarte, G., Gimenez, E., Martinez, R., & Pardo, A. 2018).

Mavi kvadrat, OWASP CRS-ni qutudan çıxarılma yolu ilə istifadə edən MODSECURITY -nin nəticələrini təmsil edir. Nəhayət, sarı top, İİ bölməsində müzakirə olunan birləşmə strategiyasını izləyərək bir-sinifləndirici ilə MODSECURITY -nin performansını əks etdirir.

N-gram analiz yanaşmasına gəlincə, model parametrləri tokenləşdirmə metodunu, öncədən təyin edilmiş dağılımları və hər bir xüsusi sahəyə təyin edilmiş n-gram uzunluğu məhdudiyyətini daxil edir. Bu parametrlər dəqiqli qiymətlərin siyahı yerinə, bir kurva əvəzinə bir cədvəl istifadə edərək n = 1-dən 5-ə qədər olan n-gram uzunluğu məhdudiyyətləri üçün nəticələri göstərir.

A. 2010 CSIC məlumat dəsti

Bu məlumat dəsti, onlayn alış-veriş funksiyalarını asanlaşdıran bir veb tətbiqi üçün adi və xüsusi HTTP istəkləri toplusunu ehtiva edir. Parametr qutularında (yazı səhvləri) nadir simvolları ehtiva edən hücumlar və icazə verilən sorğuların birləşməsini ehtiva edən 25.000 anormal test sorğusunu ehtiva edir. Təəssüf ki, hücumlar və nadir dəyərlər arasında bölüşdürmə göstərilmir, baxmayaraq ki, hücumlar əsasən veb tətbiqetmə seçimlərini hədəf alır.

		CSIC2010		DRUPAL	
Method		**TNR**	**TPR**	**TNR**	**TPR**
ModSecurity		76,1	34,3	61,1	72,2
One-class: $\lambda = 0,5$		88,9	34,6	93,3	86,2
Combined OC-MS		97,3	20,1	99,1	63,0
N-grams	n=1	99,9	93,0	93,9	95,9
	n=2	99,9	94,8	94,4	97,6
	n=3	99,5	96,1	92,0	97,5
	n=4	96,2	96,8	90,7	98,8
	n=5	90,9	97,5	89,4	98,9

Şəkil.4.2.1

ROC əyrisi ModSecurity -dən (mavi kvadrat) üstün olan bir neçə nöqtəni göstərir. Bundan əlavə, tətbiqə məxsus təlim dəsti (mavi əyri) istifadə edərək əldə edilən nəticələrin müqayisəsi göstərir ki, performans eyni veb tətbiqindəki məlumatlardan istifadə edərək bir sinif təsnifatçısının öyrədilməsi ilə əldə edilən mükəmməlliyə yaxındır. Nəhayət, sarı top vahid sinif və MODSECURİTY birləşdirən modelin performansını göstərir. Bu birləşmə TNR-ni artırsa da, TPR-ni azaldır. Bunun səbəbi, əsas məqsədimiz MODSECURİTY - nin saxta pozitivlərinin sayını azaltmaqdır, buna görə birləşdirilmiş alqoritm sorğunu yalnız hər iki mütəxəssis tərəfindən təsnif edildiyi təqdirdə hücum kimi müəyyənləşdirir. Beləliklə, tək sinif modeli daxilində hücumlar kimi qeyd olunan bəzi sorğular MODSECURİTY-nin etibarlı olduğu və əksinə hesab olunur.

Nəticələri əsas məlumatlarımızla müqayisə edərək, eyni TNR üçün MODSECURİTY hücumların 34% - ni, sinif yanaşması isə 56% - ni aşkarlayır. Bu məlumat dəstində ModSecurity qaydalarının sinif yanaşması ilə inteqrasiyası yalnız

sinif yanaşması ilə TPR nəticələrini yaxşılaşdırmır, lakin yanlış pozitivlərin sayını nəzərəçarpacaq dərəcədə azaldır (yəni TNR dəyəri 1-ə yaxındır). Ətraflı nəticələr cədvəl II-də verilmişdir.

İndi bu məlumat dəsti üçün n-gram modelini müzakirə edək. N-gram analiz alətimizi müəyyən sahələrdə müəyyən hərəkətləri yerinə yetirmək üçün tənzimləyərək incə bir tənzimləmə etdik. URI sahələri, giriş kimliyi, Milli müştəri kimliyi və şifrə yalnız monoqram analizi üçündür, çünki bu sahələrin yeganə qeyri-dəqiq tərəfi icazə verilən simvollar toplusudur və daha yüksək səviyyəli n-g analizini saxta pozitivlərə meylli edir. Bundan əlavə, Bölmə III-B-də təsvir olunan metodologiyadan sonra əvvəlcədən paylanmasını göstərdik n-g ispan dilində yazılmış Vikipediya məqalələri kolleksiyasından götürülmüş bəzi veb tətbiqetmə parametrləri (müştəri adı, şəhər və İspaniyadakı ünvan) üçün. Bu sahələr üçün ilkin qiymətləndirmələrin istifadəsi trigramların saxta pozitiv tezliyini 3% azaldıb. Nəticələr cədvəl II-də verilmişdir. Yanlış pozitivlərin sayına ən əhəmiyyətli təsir n = 3-də müşahidə olunur, burada hücumların 96% - ə qədəri 0,1% - dən az saxta pozitivlərlə aşkar edilir və bu, bütün digər üsulları açıq şəkildə üstələyir.

B. Drupal məlumat dəsti

CSIC2010 verilənlər bazası süni şəkildə yaradılmışdır. Həqiqi sorğulara və hücumlara əsaslanan real dünya tətbiqetmələrinə yanaşmamızı qiymətləndirmək üçün universitetin ictimai veb saytında üç günlük daxil olan trafiki qeyd edərək bir sıra məlumatlar topladıq. Bu məlumat dəstinə tətbiq olunan yeganə sonrakı emal sorğularda parol dəyərlərinin aşınması idi.

Sorğular real trafikdən gəldiyindən, bu məlumat dəsti daha az balanslaşdırılmışdır. Yaranan problemlərdən biri qeydə alınmış sorğuların icazə verilən və hücum olunanlara təsnif edilməsidir. Universitetin veb saytı, təhlükəsizlik mütəxəssisləri qrupu tərəfindən bir neçə ildir yekunlaşdırılan ModSecurity modulunu dəstəkləyir. Beləliklə, ModSecurity -ni etiketləmə vasitəsi kimi istifadə etdik: MODSECURİTY tərəfindən qəbul edilən sorğular etibarlı, MODSECURİTY tərəfindən rədd edilən sorğular isə hücum kimi qeyd edildi. Şəkil 2 Drupal məlumat dəsti üçün nəticələri göstərir. Onların CSIC2010 üçün alınanlara bənzədiyini görürük.

I skriptini qiymətləndirmək üçün istifadə olunan digər veb tətbiqlərdən (yaşıl əyri) məlumatlar əsasında öyrədilmiş bir sinif təsnifatçısı, müəyyən bir tətbiqlə əlaqəli məlumatlar əsasında öyrədilmiş bir sinif təsnifatçısı ilə yaradılan ROC-u təmsil edən Mavi əyriyə çox bənzəyir. Varsayılan İş nöqtəsi (Qara diamond) MODSECURİTY-dən üstündür və əvvəlki əyrilərdəki bir neçə nöqtə MODSECURİTY-dən üstündür. Nəhayət, one-class və MODSECURİTY (sarı top) birləşdirən modelin nəticələri TNR-də yaxşılaşma, lakin TPR-də azalma olduğunu göstərir. Bunun səbəbi, əsas məqsədimiz MODSECURİTY - nin saxta pozitivlərinin sayını azaltmaqdır, buna görə birləşdirilmiş alqoritm sorğunu yalnız hər iki sistem onu belə təsnif etdikdə hücum kimi qeyd edir. Buna görə də, bir sinif modeli daxilində hücumlar kimi müəyyən edilən bəzi sorğular MODSECURİTY-nin etibarlı hesab olunur və əksinə.

N-gram modelinə gəldikdə, həyata keçirilən yeganə parametr URI-nin analizdən çıxarılması idi, çünki bu model sahəsinin yüksək dəyişməsi çox yalan pozitivlərə səbəb oldu. Nəticələr cədvəl II-də verilmişdir. Monoqramlara və bigramlara sinif yanaşması ilə eyni aşkarlama sürətini təmin edirlər. Yenə də bu yanaşma TPR-də digərlərindən üstündür.

NƏTİCƏ

Magistr dissertasiya mövzusu əlaqədar veb-sayt və platformaların analizi ilə başlamış, qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

- Veb-sayt və platformaların konsepsiyasının arxitektur-texnoloji prinsipləri araşdırılmış;
- Veb mühitində olan kritik kodlaşdırma təhlil olunmuş;
- Kritik kodlaşdırmanı əhatə edən mümkün hücum ssenariləri, təhdidləri və boşluqları göstərilmiş;
- Təhdidlərin aşkarlanması üçün vasitələr və alətlər haqqında məlumat verilmiş;
- Platformalarda olan hücumların statistikası çıxarılmış;
- Veb-saytlara olan hücumların, təhdidlərin qarşısının alınması üçün tədbirlər, mexanizmlər işlənmiş;
- Veb təhdid növlərindən istifadə edərək kritik informasiya strukturunda müxtəlif konfidensial məlumatların əldə edilməsinin eksperimenti aparılmış;
- Həssas məlumatların oğurlanmasının qarşısının alınması üçün müxtəlif öyrənmə metodları göstərilmiş;
- Hücumlara məruz qalmamaq üçün istifadəçi maarifləndirilməsinin aparılması haqqında məlumat verilmişdir.

ƏDƏBİYYAT SİYAHISI

Tək müəllifli jurnal məqaləsi : *Butler W. Lampson, "Computer security in the real world". IEEE Computer 37, 6 (June 2004), pp. 37-46. DOI:10.1109/MC.2004.17*

David Watson, " Web App Attacks: Web application attacks" Network Security, Volume 2007 Issue 10, October 2007, Pages 10-14.https://www.academia.edu/52676511/Survey_of_Web_Application_and_Internet_Security_Threats.

Gregory Terzian "The Web Platform Explanied" Mar 27,2023 https://medium.com/the-web-platform-explained/introducing-theweb-platform-da6b98c52ead

Kevin Spett, "SQL Injection", Whitepaper, 2002 SPI Dynamic Inc. https://repo.zenksecurity.com/Techniques%20d.attaques%20%20.%20%20Failles/SQL%20Injection.pdf

Steve Petite, "ANATOMY OF A WEB APPLICATION: Security Considerations", White Paper, Sanctum Inc., July, 2001. https://www.giac.org/paper/gsec/2298/mitigating-web-application-risks-security-code-review-appscan/103975

Çox müəllifli jurnal məqaləsi : *Benson V, Saridakis G, Tennakoon H, Ezingeard JN (2015) The role of security notices and online consumer behaviour: an empirical study of social networking users. Int J Hum Comput Stud 80:36–44. https://www.researchgate.net/publication/275634525_The_role_of_security_notices_and_online_consumer_behaviour_an_empirical_study_of_social_networking_users*

"Analyzing web traffic: Ecml/pkdd 2007 discovery challenge," http://www.lirmm.fr/pkdd2007-challenge/.

Arvind Goutam , Vijay Tiwari "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application" 16 March 2020.

DOI: *10.1109/ISCON47742.2019.9036175*

B. Gallagher and T. Eliassi-Rad, "Classification of http attacks: a study on the ecml/pkdd 2007 discovery challenge," Lawrence Livermore National Laboratory (LLNL), Livermore, CA, Tech. Rep., July 2009.

Betarte, G., Gimenez, E., Martinez, R., & Pardo, A. (2018). Improving Web Application Firewalls through Anomaly Detection. 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). ***DOI:*** *10.1109/ICMLA.2018.00124*

C. Folini. (2016) Handling false positives with the owasp modsecurity core rule set. [Online]. Available:https://www.netnea.com/cms/apache-tutorial-8handling-false-positives-modsecurity-core-rule-set/

C. Raıssi, J. Brissaud, G. Dray, P. Poncelet, M. Roche, and M. Teisseire, "Web analyzing traffic challenge: description and results," in Proceedings of the ECML/PKDD, 2007, pp. 47–52.

Gaik-Yee Chana, Fang-Fang Chuaa and Chien-Sing Leeb, "Fuzzy association rules vs fuzzy associative patterns in defending against web service attacks", 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, 2015, pp. 524-529. https://doi.org/10.3233/JIFS-169007

H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," Journal of Supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020. DOI:10.1007/s11227-020-03213-1

https://www.isis.vanderbilt.edu/sites/isis.vanderbilt.edu/files/bibcite_files/main_0_0.pdf

Jing Wang , Hongjun Wu "URFDS: Systematic discovery of Unvalidated Redirects and Forwards in web applications" 07 December 2015. DOI: 10.1109/CNS.2015.7346891

K. Pachopoulos, D. Valsamou, D. Mavroeidis, and M. Vazirgiannis, "Feature extraction from web traffic data for the application of data mining algorithms in attack identification." Citeseer, 2007.

Kumar, D. Garg and P. S. Rana, "Ensemble approach to detect profile injection attack in recommender system", International Conference on Advances in Computing, Communications and Informatics (ICACCI), , Kochi, 2015, pp. 1734-1740. DOI: 10.1109/ICACCI.2015.7275575

M. Exbrayat, "Ecml/pkdd challenge: analyzing web traffic a boundaries signature approach," 2007, p. 53.

Marjan Korosec and Joze Duhovnik, "Identification and optimization of key process parameters in noncontact laser scanning for reverse engineering", Journal of ComputerAided Design , Volume 42 Issue 8, August, 2010 , pages 744-748. https://www.academia.edu/52676511/Survey_of_Web_Application_and_Internet_Security_Threats

Mburano, B.; Si, W. Evaluation of web vulnerability scanners based on owasp benchmark. In Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng), Sydney, NSW, Australia, 18–20 December 2018; pp. 1–6. https://doi.org/10.1109/ICSENG.2018.8638176

Mina Askari, Reihaneh Safavi-Naini, and Ken Barker, "An information theoretic privacy and utility measure for data sanitization mechanisms", Proceedings of the second ACM conference on Data and Application Security and Privacy (CODASPY), 2012 ACM. https://doi.org/10.1145/2133601.2133637

Naderi-Afooshteh, Anh Nguyen-Tuong, M. Bagheri-Marzijarani, J. D. Hiser and J. W. Davidson, "Joza: Hybrid Taint Inference for Defeating Web Application SQL Injection Attacks", 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Rio de Janeiro, 2015, pp. 172-183. ***DOI:*** *10.1109/DSN.2015.13*

Novel approaches to identify and prevent cyber attacks in web Sodagudi, S., Kotha, S.K., David Raju, M.Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019, 2019, pp.1099-1101, 8819822. ***DOI:*** *10.1109/ICCMC.2019.8819822*

Novel approaches to identify and prevent cyber attacks in webSodagudi, S., Kotha, S.K., David Raju, M.Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019, 2019, pp.1099-1101, 8819822

OWASP. Owasp modsecurity core rule set project. [Online]. Available: https://www.owasp.org/index.php/

Pandiaraja, P., and J. Manikandan, "Web proxy based detection and protection mechanisms against client based HTTP attacks", IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2015. ***DOI:*** *10.1109/ICCPCT.2015.7159344*

Peder Jungck, and Simon S.Y. Shim, "Issues in High Speed Internet Security", Computing Practices published by the IEEE Computer Society, 2004 IEEE.

R. Shukla and M. Singh, "PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems", 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, 2014, pp. 1-5. ***DOI:*** *10.1109/MC.2004.58*

Rahul Johari and Pankaj Sharma, "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation, Proceedings of the 2012 International Conference on Communication Systems and Network Technologies Pages. DOI: 10.1109/CSNT.2012.104

Sahoo SR, Gupta BB (2020) Fake profle detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3):303–331. https://doi.org/10.1504/IJICS.2020.105181

Shebli, H.M.Z.A.; Beheshti, B.D. A study on penetration testing process and tools. In Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4 May 2018. DOI:10.1109/LISAT.2018.8378035

Xiaowei Li and Yuan Xue, "A Survey on Web Application Security", Technical report, Vanderbilt University, 2011.