location identification and framing accuracy. In the established structure, online parking offers several advantages, including time savings, environmental preservation, increased revenue, and enhanced safety and traffic security. The system is primarily based on the Python programming language and is structured in terms of architecture. Overall, it retains the functions of traffic monitoring and management at the state level and in the broader market.

Reference

[1]. Max Tegmark ," Life 3.0 Being Human in the Age of Artificial Intelligence"
[2]. Peter Norvig and Stuart Russel," Artificial Intelligence- A Modern Approach (3rd edition)"
[3]. Denis Rothmanl," Artificial Intelligence By Example-2nd edition"
[4]. James V Stone," Artificial Intelligence Engines: A Tutorial Introduction to the Mathematics of Deep Learning"
[5]. Vinod Chandra," Artificial Intelligence and Machine Learning 1st Edition"
[6]. Deepak Khemani," A First Course in Artificial Intelligence"
[7]. John Paul Mueller and Luca Massaron," Machine Learning (in Python and R) For Dummies"
[8]. Adelyn Zhou and Marlene Jia," Applied Artificial Intelligence: A handbook for business leaders"
[9]. https://www.mathworks.com/discovery/object-detection.html
[10]. https://www.analyticsvidhya.com/blog/2022/03/a-basic-introduction-to-object-detection/
[11]. https://solutions.innodata.com/image-video-sensor-annotation/?dyn_keyword=Object+Detection&utm_term=object%20detection&utm_campaign=Image,+Video,+and+Sensor+Data+Annotation&utm_source=adwords&utm_medium=ppc&hsa_acc=4015251027&hsa_cam=18859846770&hsa_grp=146896640801&hsa_ad=554037122604&hsa_src=g&hsa
[12]. https://www.section.io/engineering-education/introduction-to-yolo-algorithm-for-object-detection

SAYTLARA ZİYAN VERƏN XSS HÜCUMLARININ NÖVLƏRİ

Əliyeva Nailə
Əliyeva Yeganə
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə

Məqalədə XSS hücumları anlayışı haqqında ətraflı araşdırmalar aparılmış, geniş şəkildə yayılmış XSS hücumlarının növləri qeyd olunmuşdur. İstifadəçilərin və proqramçıların məruz qaldığı bu hücumun növlərinin ayrı-ayrılıqda fərqləri izah olunmuşdur. Həmçinin XSS hücumlarının yaranma səbəbləri və onlardan qorunma yolları müəyyənləşdirilmişdir. Əlavə olaraq XSS hücumlarının yaratdığı zərərlərə əsasən veb tətbiq növləri araşdırılmışdır. Bu hücumlar tətbiqlərə göstərdiyi ziyanların nəticəsində tətbiqlərdə baş vermiş dəyişikliklər təhlil edilmişdir. Qeyd olunan dəyişikliklərlə bağlı araşdırmalar aparılmış və onların aradan qaldırılması üçün müəyyən tədbirlər görülmüşdür.

Açar sözlər: Cross Site Scripting (XSS), Document Object Model, zərərli hərəkətlər, Reflective XSS, hücum növləri, Stored XSS

Giriş. Son günlər Azərbaycanda bəzi saytlara qarşı hücumlar intensivləşib. Hücumlar xarici ölkələrdən həyata keçirilsə də sifarişçilər adətən rəqiblər və yaxud digər maraqlı şəxslər olur. Veb saytın hazırlanmasında ən mühüm məsələ o saytın təhlükəsizliyidir. Dağıdıla bilməyən veb sayt yoxdur. Hər saytın zəif cəhəti ola bilər. Sadəcə, onu dağıtmaq və ya müdaxilə etmək istəyən hakerin gücündən çox şey asılıdır. Haker nə qədər güclüdürsə, veb sayt bir o qədər zəifdir. Ümumiyyətlə, informasiya təhlükəsizliyi elə bir problemdir ki, onun qarşısını tam şəkildə almaq mümkün deyil. Cross Site Scripting **(**XSS), təcavüzkar veb tətbiqini istifadəçinin brauzerinin icra edə biləcəyi formada məlumat göndərmək

üçün aldatdığı zaman baş verir. Çox vaxt bu, təcavüzkar tərəfindən təmin edilən HTML və XSS birləşməsidir, lakin XSS zərərli yükləmələri və media məzmununu çatdırmaq üçün də istifadə oluna bilər. Veb tətbiqi etibarsız mənbədən verilənlərin düzgün şəkildə qaçırılmadan istifadəçilərə göstərilməsinə icazə verdikdə təcavüzkar veb tətbiqini bu şəkildə aldada bilər. [1]

XSS-in əsas anlayışları aşağıdakılardır:

- XSS həssas veb proqramlar üzərində həyata keçirilən veb əsaslı hücumdur.
- XSS hücumlarında qurban proqram deyil, istifadəçi hesab olunur.
- XSS hücumlarında zərərli məzmun JavaScript vasitəsilə istifadəçilərə çatdırılır.

XSS hücumlarının növləri.

Reflective XSS hücumu: Hakerin zərərli skripti həssas veb proqrama çatdırdığı zaman baş verir və server daha sonra HTTP cavabında qaytarır. Qurbanın brauzeri HTTP cavabının bir hissəsi kimi zərərli skripti icra edir, beləliklə qanuni istifadəçini təhlükə altına alır və şəxsi məlumatları hakerə geri göndərir. Reflective XSS hücumları adətən səhv mesajlarını və ya axtarış motorunun nəticə səhifələrini hədəf alır, çünki bir çox istifadəçinin klik edəcəyi linklə zərərli e-poçt göndərmək asandır. İstifadəçi linki kliklədikdə, server zərərli skripti ehtiva edən sorğunu alır və o, saxlanmadığı üçün istifadəçiyə geri kod göndərməklə cavab verir.

Reflected XSS nümunəsində axtarış formasının daxil edilməsi axtarış açarının nə olduğunu göstərmək üçün səhifədə əks olunur. Təcavüzkar zərərli kodu ehtiva edən URL yarada və e-poçt və ya sosial mediadan istifadə edərək URL-i yaya bilər. Bu keçidi seçən istifadəçi veb tətbiqini açır və o, brauzerdə zərərli kodu işə salır.

- Skript veb proqramda saxlanmır
- Zərərli kod yalnız bir istifadəçiyə göstərilir
- Linki açan istifadəçilər proqram açıldıqda skripti icra edirlər
- Skript və hücum server tərəfində mütləq görünmür.[2]

XSS hücumlarına qarşı ilk müdafiə xətti məzmunu süzgəcdən keçirmək və istifadəçi daxiletmələrini yoxlamaqdır. Riskli məlumat nümunələrini rədd etmək üçün skript təchizatçılarının təhlükəsiz siyahılarından və blok siyahılarından istifadə etmək lazımdır. Əlavə olaraq, əks olunan XSS hücumlarının riskini azaltmaq üçün Content Security Policy (CSP) tətbiq olunur. CSP skriptlərə və onların yüklənə və işə salına biləcəyi veb səhifə yerlərinə nəzarət imkanı verir.[3]

Stored XSS: Bu hücumda zərərli skript istifadəçi girişini hədəf serverə saxlayır. Serverdə həyata keçirilən Reflective XSS hücumundan fərqli olaraq, Stored XSS hücumu istifadəçinin brauzerində həyata keçirilir. Təcavüzkarlar daha sonra zərərli skriptləri brauzerdə daimi saxlamaq üçün adətən HTML verilənlər bazalarından istifadə edən müasir HTML5 proqramlarından istifadə edirlər.

Saxlanılan XSS nümunəsində skript kifayət qədər doğrulama aparmayan və skripti davamlı olaraq verilənlər bazasında saxlayan veb serverə giriş sahəsindən istifadə etməklə təqdim edilmiş ola bilər. Nəticə ola bilər ki, bu skript indi veb proqrama daxil olan bütün istifadəçilərə çatdırılır və məsələn, istifadəçi sessiyası kukilərinə giriş əldə edir.

- Skript davamlı olaraq veb proqramında saxlanılır
- İnfeksiyadan sonra proqramı ziyarət edən istifadəçilər skripti geri alırlar
- Zərərli kod veb proqramdakı qüsurlardan istifadə edir
- Skript və hücum server tərəfində görünür.

Stored XSS hücumunda istifadəçi vebsayta hər dəfə daxil olduqda skript saxlanılır və serverdə icra olunur. Stored XSS hücumları, həmçinin təlim keçməmiş istifadəçilər doğrulama tədbirləri görmədən proqram təminatından məlumat çıxarmağa cəhd etdikdə də baş verə bilər.

Stored XSS hücumları zərərli skripti istifadəçiyə əks etdirmək məqsədi daşıyır, buna görə də onların qarşısını almağın ən asan yolu istifadəçi məlumatlarını təmizləmək və girişləri diqqətlə idarə etməkdir.

XSS hücumunun aşkarlanması və təsirinin azaldılması üçün Web Application Firewalls (WAFs) istifadə olunur.[4]

Document Object Model (DOM) hücumu: DOM interfeysi HTML və XML sənədlərini oxumaq və dəyişdirməklə veb səhifənin məzmununu emal etməyə və manipulyasiya etməyə imkan verir. DOM əsaslı XSS hücumları qurbanın brauzerinin DOM kontekstində zərərli dəyişikliklər təqdim edir və müştəri tərəfi kodunun gözlənilməz şəkildə icrasına səbəb olur.

DOM əsaslı XSS hücumu hətta serverin veb-brauzerdə icra edilən JavaScript-dəki qüsurdan istifadə edərək veb-səhifəyə heç bir zərərli kodu daxil etmədikdə belə uğurla həyata keçirilə bilər. Məsələn, müştəri saytı JavaScript giriş sahəsinə və ya GET parametrinə əsaslanaraq veb-səhifənin DOM ağacını girişi təsdiq etmədən dəyişdirərsə, zərərli kod icra oluna bilər.

- Skript veb proqramda saxlanmır
- Zərərli kod yalnız bir istifadəçiyə göstərilir
- Zərərli kod istifadəçi tərəfindəki brauzerdəki qüsurlardan istifadə edir
- Skript və hücum server tərəfində mütləq görünmür.[5]

DOM əsaslı XSS hücumları Reflective və Stored XSS hücumlarından fərqli olaraq zərərli skripti saxlamır və ya serverə çatdırmır. Bu hücumda qurbanın brauzeri yeganə zəiflikdir. Digər kateqoriyalara nisbətən onları başa düşmək daha çətin olduğundan, DOM əsaslı zəifliklər qeyri-adi, mürəkkəb və aradan qaldırılması çətin olur. Bu tip hücumlardan müdafiə olunmaq üçün etibarlı növlərdən istifadə edilməlidir. Bu, DOM-un bütün riskli hissələrinin yalnız əvvəlcədən müəyyən edilmiş siyasətdən keçmiş məlumatlar tərəfindən istifadə edilməsini təmin edən brauzer təhlükəsizlik mexanizmidir. Bu brauzerə kod və məlumat arasında fərq qoymağa kömək edir - əsas zəiflik mənbəyini aradan qaldırır.[6]

Zərərli hərəkətlər XSS zəifliklərindən istifadə etməklə təcavüzkar zərərli hərəkətlər edə bilər, məsələn:

- Hesabı oğurlamaq
- Veb qurdlarını yaymaq
- Brauzer tarixçəsinə və mübadilə buferinin məzmununa daxil olmaq
- Brauzeri uzaqdan idarə etmək
- İntranet cihazlarını və proqramlarını skan etmək və istismarını həyata keçirmək.

Cross Site Scripting (XSS) işləmə xüsusiyyəti aşağıdakı kimidir:

XSS, təcavüzkarın həssas veb saytı manipulyasiya etdiyi zaman zərərli skriptləri istifadəçiyə qaytarır. Bu proses adətən JavaScript-i əhatə edir, lakin təcavüzkar istənilən istifadəçi dilindən istifadə edə bilər. Cross Site Scripting, dilin bir çox brauzerlə inteqrasiyası səbəbindən ilk növbədə JavaScript-i hədəfləyir.

XSS hücumlarının baş verməsinə imkan yaradan zəif cəhətlər geniş yayılmışdır. XSS hücumları müxtəlif proqramlaşdırma mühitlərindəki zəif cəhətlərdən istifadə edə bilər – məsələn, Flash, VBScript, JavaScript və ActiveX bura daxildir. Geniş istifadə olunan platformalardan istifadə etmək qabiliyyəti XSS hücumlarını ciddi təhlükəyə çevirir.[7]

XSS hücumlarının yaranma səbəbləri. XSS hücumunun baş verməsinin müxtəlif yolları bunlardır:

- İstifadəçi səhifəni yüklədikdə və ya müəyyən səhifə elementlərinin, o cümlədən hiperlinklərin üzərinə getdikdə icranı avtomatik olaraq işə sala bilər.
- Təcavüzkarlar XSS-i birbaşa, məsələn, zərərli keçid olan e-poçt mesajı vasitəsilə həyata keçirə bilər.
- Bəzi XSS hücumlarının xüsusi bir hədəfi yoxdur. Əksinə, təcavüzkar təsadüfi qurbanları hədəf alan sayt və ya proqramdakı zəiflikdən istifadə edir.
- Hücumun miqyasından asılı olaraq, təcavüzkarlar istifadəçi hesablarını ələ keçirə, troyan atı proqramlarını aktivləşdirə və səhifə məzmununu tamamilə dəyişdirə, istifadəçiləri öz həssas məlumatlarını paylaşmağa yönəldə bilər.
- Təcavüzkarlar session cookies haqqında məlumat əldə edə bilər, beləliklə, onlar həqiqi istifadəçiləri təqlid edə və şəxsi hesablarını ələ keçirə bilərlər.[8]

XSS hücumlarının təsir etdiyi veb tətbiq növləri

XSS zəifliyinin təsiri tətbiqin növündən asılıdır. Bir XSS hücumunun üç növ veb tətbiqinə necə təsir edəcəyi aşağıda verilmişdir:

Statik məzmun: Heç bir giriş funksiyası olmayan xəbər saytı kimi statik məzmunlu veb proqramda XSS minimal təsir göstərəcək, çünki bütün istifadəçilər anonimdir və məlumatlar ictimaiyyətə açıqdır.

Həssas məlumatlar: Tətbiq maliyyə və ya sağlamlıq xidmətləri kimi həssas istifadəçi məlumatlarını saxlayırsa, XSS böyük zərər verə bilər, çünki bu, təcavüzkarlara istifadəçi hesablarını ələ keçirməyə imkan verə bilər.[9]

İmtiyazlı istifadəçilər: Təcavüzkar XSS-dən veb proqram administratoru kimi imtiyazlı istifadəçinin sessiyasını ələ keçirmək üçün istifadə edə bilərsə, onlar proqram üzərində tam nəzarət əldə edə və onun bütün məlumatlarını ələ keçirə bilərlər. Saytlararası skript boşluqları adətən vebsaytın və ya veb tətbiqinin istifadəçilərin öz məlumatlarını yerləşdirə və ya yükləyə biləcəyi hissələrində, məsələn, bloqun şərhlər bölməsində baş verir.[10]

Saytlararası skript hücumlarının qarşısının alınması üsulları Saytlararası skript hücumlarının çoxsaylı variantları ilə təşkilatlar özlərini adekvat şəkildə qorumaq və gələcək problemlərin qarşısını almaq yollarını bilməlidirlər. Veb saytlar mürəkkəbləşdikləri üçün onlara ciddi şəkildə nəzarət etmək əvvəlkindən daha çətin olmağa başlayır. Zaman keçdikcə hücumların tezliyi artmağa davam edir.

Aşağıda göstərilmiş təkliflər istifadəçilərin XSS hücumlarından qorunmasına kömək edə bilər:

- İstifadəçi girişini təmizləmək
- Potensial zərərli istifadəçi tərəfindən təmin edilən daxiletməni doğrulamaq.
- Potensial olaraq zərərli istifadəçi tərəfindən təmin edilən məlumatların brauzer tərəfindən avtomatik yükləmə və icra davranışının işə salmasının qarşısını almaq üçün çıxışı kodlamaq.
- İstifadəçi tərəfindən verilən məlumatların istifadəsini məhdudlaşdırmaq və yalnız lazım olduğu yerdə istifadə etmək.
- Məzmun Təhlükəsizliyi Siyasətindən istifadə etmək: XSS cəhdlərinə qarşı əlavə qorunma səviyyələrinin azaldılmasını təmin edir.[11]

Nəticə

XSS (Cross-Site Scripting) hücumları hazırda bir çox veb saytlar və veb tətbiqlərdə bir təhlükə kimi mövcuddur. Bu cür hücumlar istifadəçilərin ziyana məruz qalmış platformalarda rahat işləməsinə çətinlik yaradır. Digər tərəfdən isə bu növ hücumların qarşısını almaq üçün bir çox məhdudiyyətlər və təhlükəsizlik tədbirləri mövcuddur. Brauzerlər və veb platformaları istifadəçiləri XSS hücumlarından qorumaq üçün daha güclü təhlükəsizlik funksiyaları təklif etməlidir. Bu potensial XSS mənbələrinin daha effektiv şəkildə aşkar edilməsinə və bloklanmasına imkan verəcək. Protokolların daha güclü şifrələnməsi və daha müxtəlif autentifikasiya metodları, istifadəçi məlumatlarının qorunmasına kömək etmiş olacaq.

Ədəbiyyat

[1] Grossman J. X (2021). SS Attacks: Cross Site Scripting Exploits and Defense. Brazil, page 110-125.

[2] Brij B.Gupta,(2020).Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures.İndia,page 95-112.

[3] Marcus P.(2022). The Web Application Hacker's Handbook:Finding and Exploiting Security Flaws 2nd Edition.England,page 88-96.

[4] Gürel A.(2019). Siber Güvenlik.Turkiye,page 65-87.

[5] Tarık K. (2022).Kişisel Verilerin Güvenliği ve Uyum.Turkiye,page 70-94.

[6] Salmanova K.(2019). İnformasiya Təhlükəsizliyi.Bakı,səh. 160-184.

[7] https://www.rapid7.com/fundamentals/cross-site-scripting/

[8] https://www.kaspersky.com/resource-center/definitions/what-is-a-cross-site-scripting-attack

[9] https://www.stackhawk.com/blog/what-is-cross-site-scripting-xss/

[10] https://aardwolfsecurity.com/types-of-cross-site-scripting-xss-attacks/
[11] https://www.imperva.com/learn/application-security/reflected-xss-attacks/

SQL İNYEKSİYA HÜCUMLARI

Şirinova Şəbnəm
Əliyeva Yeganə
Azərbaycan Dövlət Neft və Sənaye Universiteti

Xülasə
Məqalədə SQL İnyeksiya hücumlarının bir çox növləri müzakirə edilmiş və onlar haqqında hərtərəfli araşdırmalar edilmişdir. Proqramçıların və istifadəçilərin həssas olduğu bu hücumun müxtəlif formaları ayrı-ayrılıqda izah edilmişdir. Bundan əlavə, SQL İnyeksiya hücumlarının arxasında duran səbəblər və onların qarşısını almaq üçün strategiyalar müəyyən edilmişdir. SQL İnyeksiya hücumlarına qarşı həssas olan onlayn proqram növləri və onların vura biləcəyi zərərlərlə bağlı hərtərəfli araşdırmalar aparılmışdır. Bu hücumların yaratdığı zərər nəticəsində tətbiqlərdə edilən dəyişikliklər araşdırılmışdır. Qeyd olunan dəyişikliklər araşdırma obyekti olub və onlardan xilas olmaq üçün tədbirlər görülmüşdür.
Açar sözlər: Structured Query Language (SQL), SQL injection (SQLi), In-band SQLi, Blind SQLi, Out-of-band SQLi, Acunetix

Giriş

Son günlərdə artan saytlara qarşı hücumları araşdırdıqda görünür ki, bu hücumlar çox vaxt xarici ölkələrdən həyata keçirilir. Lakin bu hücumların sifarişçiləri ya rəqib şirkətlər, ya da digər maraqları olan şəxslər olur. Hazırda Azərbaycanda da belə hücumların sayı heç də az deyildir. İstənilən veb sayt yaradılarkən ilk öncə onun təhlükəsizliyi nəzərə alınmalıdır. Hər bir saytın zəif yanları ola bilər, lakin ona kənar şəxslərin müdaxiləsi xakerlərin gücündən asılıdır. Çünki xakerin güclü olması veb saytın təhlükəsizliyinin zəifliyindən xəbər verir. SQL İnyeksiyası rəqiblərə veb tətbiqinin verilənlər bazası sorğularına etdiyi sorğulara ixtiyari SQL əmrləri daxil etməyə imkan verən bir texnikadır. O, MySQL, Oracle və ya MS SQL kimi backend verilənlər bazasından istifadə edən həssas veb səhifələrdə və proqramlarda işləyir. Bu, pisniyyətli aktyorların başqa cür əldə edə bilməyəcəkləri məxfi məlumatları əldə etmələrinin ümumi üsuludur.[1]

SQLi hücumları təhdid iştirakçılarına bu məlumatı əlavə etmək, yeniləmək və ya silmək imkanı verir, tətbiqin davranışını daimi olaraq dəyişdirir. Bu, həmçinin xidmətdən imtinaya və ya əsas serverin və ya digər backend infrastrukturunun pozulmasına səbəb ola bilər.

Strukturlaşdırılmış Sorğu Dili (SQL).

Structured Query Language qısaldılmış və tez-tez "esqüel" kimi tələffüz edilən SQL müasir məlumatların idarə edilməsinin əsasını təşkil edir. SQL əlaqəli verilənlər bazası idarəetmə sistemləri (RDBMS) ilə qarşılıqlı əlaqə üçün istifadə olunan standartlaşdırılmış proqramlaşdırma dilidir.[2] SQL istifadəçilərə məlumatları strukturlaşdırılmış və səmərəli şəkildə saxlamaq, əldə etmək, dəyişdirmək və təhlil etmək imkanı verir. Strukturlaşdırılmış Sorğu Dili (SQL) verilənlər bazası idarəetməsinin mürəkkəb və kompleks strukturunda birləşdirici bir elementdir. SQL Server, MySQL, Oracle və MS SQL Server daxil olmaqla müxtəlif verilənlər bazası sistemləri tərəfindən istifadə edilən ümumi dildir. SQL verilənlərlə ona ehtiyacı olan insanlar arasında körpüdür. SQL-in əsas əmrləri aşağıdakılardır:

Məlumatların alınması: SELECT ifadəsi məlumatların axtarışı üçün qapıdır. Bu bəyanat istifadəçilərə sətirlərdən və ya bütün verilənlər dəstlərindən xüsusi məlumatları əldə etmək üçün cədvəlləri