[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

sorğulamağa imkan verir. SQL istifadəçiləri nəticələrin filtrlənməsi, çeşidlənməsi və məhdudlaşdırılması kimi üsullar vasitəsilə geniş verilənlər bazalarından lazım olan dəqiq məlumatları əldə edə bilərlər.[3]
Məlumatların manipulyasiyası: SQL təkcə məlumat axtarışı ilə deyil, həm də verilənləri manipulyasiya etmək üçün istifadə edilir. INSERT, UPDATE və DELETE əməliyyatları istifadəçilərə verilənlər bazasını lazım olduqda formalaşdırmağa imkan verir. SQL məlumatların bütövlüyünü və ardıcıllığını, əlaqəli verilənlər bazalarının həmişə dəqiq və etibarlı məlumat anbarları olaraq qalmasını təmin edir.[4]
Bundan əlavə, SQL cədvəllər, görünüşlər və indekslər kimi verilənlər bazası obyektləri anlayışını təqdim edir, cədvəllər və sütunlar arasında əlaqələrin əhəmiyyətini vurğulayır. SQL-də saxlanılan prosedurlar ümumi əməliyyatları sadələşdirir, tərtibatçılar və idarəçilər üçün məlumatların manipulyasiyasını sadələşdirir. Qabaqcıl SQL üsulları əsas sorğulardan kənara çıxır, dublikat dəyərlərin müəyyən edilməsi, cədvəllərin səmərəli idarə edilməsi və mürəkkəb verilənlərin manipulyasiyası üçün müntəzəm ifadələrin gücündən istifadə kimi tapşırıqlara diqqət yetirir. Bu üsullar SQL funksiyalarının daha dərindən başa düşülməsini təmin etmək, istifadəçilərə məlumatların bütövlüyünü optimallaşdırmaq, verilənlər bazası idarəçiliyini asanlaşdırmaq və daha mürəkkəb məlumatların təhlili üçün qabaqcıl nümunə uyğunluğunu həyata keçirmək üçün səlahiyyət vermək məqsədi daşıyır.
SQL İnyeksiyası: Çoxsaylı üstünlüklərinə baxmayaraq, SQL-in də öz çətinlikləri var. Zərərli istifadəçilər verilənlər bazalarını pozmaq üçün ümumi təhlükəsizlik zəifliyi olan SQL inyeksiyasından istifadə edə bilərlər. Komandalar bu cür hücumların qarşısını almaq üçün girişin doğrulanması və parametrləşdirilmiş sorğular kimi təhlükəsizlik tədbirlərini həyata keçirməlidir.[5]
Verilənlər bazası administratorları performansını qorumaq və məlumatların bütövlüyünü təmin etmək üçün verilənlər bazasını daim izləməli və optimallaşdırmalıdırlar. Bu, indeksləşdirmə, sorğuların optimallaşdırılması, server, aparat və proqram təminatının yenilənməsi kimi tapşırıqları əhatə edir.
Böyük paylaşılan məlumat bazalarını idarə etmək çətin ola bilər, xüsusən də birdən çox komandanın eyni məlumatlara çıxışa ehtiyacı olduğu bir şirkətdə. Fərqli komandaların tələblərini balanslaşdırmaq, məlumatların ardıcıllığını təmin etmək və səmərəli girişi təmin etmək mürəkkəb ola bilər, bunun üçün dəqiq müəyyən edilmiş məlumat strategiyası tələb olunur.
Güclü bir vasitə olsa da, SQL hər bir məlumat idarəetmə ssenarisi üçün ideal həll olmaya bilər. Bəzi hallarda, xüsusi ehtiyacları qarşılamaq üçün hibrid yanaşmalar və ya alternativ məlumat idarəetmə vasitələri lazım ola bilər. Şirkətlər öz tələblərini diqqətlə qiymətləndirməli və müvafiq alətlər və texnologiyalar seçməlidirlər. SQL inyeksiyası (SQLi) zərərli SQL ifadələrini yerinə yetirməyə imkan verən inyeksiya hücumunun bir növüdür.[6] Bu ifadələr veb proqram arxasında verilənlər bazası serverinə nəzarət edir. Təcavüzkarlar tətbiqin təhlükəsizlik tədbirlərindən yan keçmək üçün SQL inyeksiya boşluqlarından istifadə edə bilərlər. Onlar veb səhifənin və ya veb tətbiqinin autentifikasiyası və avtorizasiyası ətrafında gəzə və bütün SQL verilənlər bazasının məzmununu əldə edə bilərlər. Onlar həmçinin verilənlər bazasında qeydləri əlavə etmək, dəyişdirmək və silmək üçün SQL inyeksiyasından istifadə edə bilərlər.[7] SQL inyeksiya zəifliyi MySQL, Oracle, SQL Server və ya başqaları kimi SQL verilənlər bazasından istifadə edən hər hansı vebsayt və ya veb proqrama təsir göstərə bilər. Cinayətkarlar ondan həssas məlumatlarınıza icazəsiz giriş əldə etmək üçün istifadə edə bilər: müştəri məlumatları, şəxsi məlumatlar, ticarət sirləri, əqli mülkiyyət və s. SQL inyeksiya hücumları ən qədim, ən çox yayılmış və ən təhlükəli veb proqram zəifliklərindən biridir. OWASP təşkilatı (Açıq Veb Tətbiqi Təhlükəsizliyi Layihəsi) OWASP Top 10 2017 sənədində inyeksiyaları veb tətbiqi təhlükəsizliyinə bir nömrəli təhlükə kimi qeyd edir.[8]
SQL inyeksiya hücumu etmək üçün təcavüzkar əvvəlcə veb səhifə və ya veb proqram daxilində həssas istifadəçi girişlərini tapmalıdır. SQL inyeksiya zəifliyi olan veb səhifə və ya veb tətbiqi bu cür istifadəçi girişindən birbaşa SQL sorğusunda istifadə edir. Təcavüzkar giriş məzmunu yarada bilər. Bu cür məzmun tez-tez zərərli yük adlanır və hücumun əsas hissəsidir. Təcavüzkar bu məzmunu göndərdikdən sonra verilənlər bazasında zərərli SQL əmrləri yerinə yetirilir.[9] SQL, əlaqəli verilənlər bazalarında saxlanılan məlumatları idarə etmək üçün nəzərdə tutulmuş sorğu dilidir. Məlumata daxil olmaq, dəyişdirmək və

silmək üçün ondan istifadə edə bilərsiniz. Bir çox veb proqramlar və veb saytlar bütün məlumatları SQL verilənlər bazasında saxlayır. Bəzi hallarda əməliyyat sistemi əmrlərini yerinə yetirmək üçün SQL əmrlərindən də istifadə edə bilərsiniz. Buna görə uğurlu SQL Injection hücumu çox ciddi nəticələrə səbəb ola bilər.

Təcavüzkarlar verilənlər bazasında digər istifadəçilərin etimadnaməsini tapmaq üçün SQL inyeksiyalarından istifadə edə bilərlər. Daha sonra bu istifadəçiləri təqlid edə bilərlər. Təqdim olunan istifadəçi bütün verilənlər bazası imtiyazlarına malik verilənlər bazası administratoru ola bilər.

SQL verilənlər bazasından məlumatları seçmək və çıxarmaq imkanı verir. SQL inyeksiya zəifliyi təcavüzkara verilənlər bazası serverindəki bütün məlumatlara tam giriş əldə etməyə imkan verə bilər. SQL həmçinin verilənlər bazasındakı məlumatları dəyişməyə və yeni məlumatlar əlavə etməyə imkan verir. Məsələn, maliyyə proqramında təcavüzkar balansları dəyişdirmək, əməliyyatları ləğv etmək və ya hesabına pul köçürmək üçün SQL inyeksiya istifadə edə bilər. Siz verilənlər bazasından qeydləri silmək üçün SQL-dən istifadə edə bilərsiniz. İnzibatçı verilənlər bazasının ehtiyat nüsxəsini çıxarsa belə, verilənlər bazası bərpa olunana qədər məlumatların silinməsi proqramların mövcudluğuna təsir göstərə bilər. Həmçinin, ehtiyat nüsxələr ən son məlumatları əhatə etməyə bilər.

Bəzi verilənlər bazası serverlərində verilənlər bazası serverindən istifadə edərək əməliyyat sisteminə daxil ola bilərsiniz. Bu qəsdən və ya təsadüfi ola bilər. Belə halda, təcavüzkar ilkin vektor kimi SQL inyeksiyasından istifadə edə, sonra isə firewall arxasında daxili şəbəkəyə hücum edə bilər.

SQL inyeksiya hücumlarının bir neçə növü var: diapazondaxili SQLi (in-band SQLi -verilənlər bazası xətalarından və ya UNION əmrlərindən istifadə etməklə), kor SQLi (Blind SQL Injection) və diapazondan kənar SQLi (out-of-band SQLi). SQL inyeksiya hücumlarının qarşısını almağın yeganə əmin yolu daxiletmənin yoxlanılması və hazırlanmış bəyanatlar daxil olmaqla parametrləşdirilmiş sorğulardır. Tətbiq kodu heç vaxt girişdən birbaşa istifadə edilməməlidir. Tərtibatçı yalnız giriş formaları kimi veb forması daxiletmələrini deyil, bütün daxiletmələri təmizləməlidir. Onlar tək dırnaqlar kimi potensial zərərli kod elementlərini silməlidirlər. İstehsal saytlarınızda verilənlər bazası səhvlərinin görünməsini söndürmək də yaxşı bir fikirdir. Verilənlər bazası səhvləri verilənlər bazanız haqqında məlumat əldə etmək üçün SQL inyeksiya ilə istifadə edilə bilər.[10]

SQL inyeksiya zəifliyini aşkar etsəniz, məsələn, Acunetix skanından istifadə etməklə, onu dərhal düzəldə bilməyəcəksiniz. Məsələn, boşluq açıq mənbə kodunda ola bilər. Belə hallarda, girişinizi müvəqqəti olaraq təmizləmək üçün veb tətbiqi təhlükəsizlik divarından istifadə edə bilərsiniz. SQL inyeksiya zəifliklərinin qarşısını almaq asan deyil. Xüsusi qarşısının alınması üsulları SQLi zəifliyinin alt növündən, SQL verilənlər bazası mühərrikindən və proqramlaşdırma dilindən asılıdır. Bununla belə, veb tətbiqinizi təhlükəsiz saxlamaq üçün riayət etməli olduğunuz müəyyən ümumi strateji prinsiplər var.

Addım 1: Maarifləndirməni öyrədin və qoruyun. Veb tətbiqinizi təhlükəsiz saxlamaq üçün veb proqramın yaradılmasında iştirak edən hər kəs SQL inyeksiyaları ilə bağlı risklərdən xəbərdar olmalıdır. Siz bütün tərtibatçılarınıza, QA işçilərinə, DevOps və SysAdmins-ə uyğun təhlükəsizlik təlimi verməlisiniz. Onları bu səhifəyə istinad etməklə başlaya bilərsiniz.

Addım 2: Heç bir istifadəçi girişinə etibar etməyin. Bütün istifadəçi daxiletmələrini etibarsız hesab edin. SQL sorğusunda istifadə edilən hər hansı istifadəçi girişi SQL inyeksiya riskini yaradır. Təsdiqlənmiş və ya daxili istifadəçilərin daxiletmələrinə ictimai daxiletmə ilə eyni şəkildə davranın.

Addım 3: Qara siyahıları deyil, ağ siyahıları istifadə edin. İstifadəçi daxiletmələrini qara siyahılar əsasında filtrləməyin. Ağıllı bir təcavüzkar, demək olar ki, həmişə qara siyahınızdan yan keçməyin bir yolunu tapacaqdır. Mümkünsə, yalnız ciddi ağ siyahılardan istifadə edərək istifadəçi daxiletməsini yoxlayın və filtrləyin.

Addım 4: Ən son texnologiyaları mənimsəyin. Köhnə veb inkişaf texnologiyaları SQLi qorunmasına malik deyil. İnkişaf mühitinin və dilin ən son versiyasını və həmin mühit/dillə əlaqəli ən son texnologiyalardan istifadə edin. Məsələn, PHP-də MySQLi əvəzinə PDO istifadə edin.

Addım 5: Təsdiqlənmiş mexanizmlərdən istifadə edin. SQLi müdafiəsini sıfırdan qurmağa çalışmayın. Müasir inkişaf texnologiyalarının əksəriyyəti sizə SQLi-dən qorunmaq üçün mexanizmlər təklif edə bilər. Təkəri yenidən ixtira etmək əvəzinə bu cür mexanizmlərdən istifadə edin. Məsələn, parametrləşdirilmiş sorğulardan və ya saxlanılan prosedurlardan istifadə edin.
Addım 6: Müntəzəm olaraq skan edin (Acunetix ilə). SQL inyeksiyaları tərtibatçılarınız tərəfindən və ya xarici kitabxanalar/modullar/proqram təminatı vasitəsilə təqdim oluna bilər. Siz Acunetix kimi veb zəiflik skaneri istifadə edərək müntəzəm olaraq veb proqramlarınızı skan etməlisiniz. Jenkins istifadə edirsinizsə, hər quruluşu avtomatik skan etmək üçün Acunetix plaginini quraşdırmalısınız.[11]

Nəticə

Bir çox veb sayt və proqramlar hazırda SQL İnyeksiya hücumlarına qarşı həssasdır. Bu cür hücumlar təhlükəsi olan platformalarda istifadəçilərin rahat işləməyi çətinləşir. Bununla belə, bu cür hücumları dayandırmaq üçün çoxsaylı məhdudiyyətlər və təhlükəsizlik tədbirləri mövcuddur.İstehlakçıları SQL İnyeksiya hücumlarından qorumaq üçün veb brauzerlər və sistemlər daha möhkəm təhlükəsizlik tədbirləri təmin etməlidir. Bu, mümkün SQL İnyeksiya mənbələrini daha uğurla müəyyən etməyə və dayandırmağa imkan verəcəkdir. İstifadəçi məlumatları daha güclü protokol şifrələməsi və daha geniş çeşidli autentifikasiya üsulları ilə daha yaxşı qorunacaq.

Ədəbiyyat

[1] Debarros, A. (2018), Practical SQL: A Beginner's Guide to Storytelling with Data, New York: No Starch Press, 392 s.
[2] Clarke-Salt, J. (2012), SQL Injection Attacks and Defense 2nd Edition, Oxford: Syngress, 576 s.
[3] Randolph, W., William A., Elizabeth N., Meagan L., Joseph D. A. (2023), SQL Server 2022 Administration Inside Out, United States: Pearson Education, 1593 s.
[4] Thirumalesh, (2022), The Complete Ethical Hacking Book, Hindistan: OrangeBooks Publication, 124 s.
[5] Richie M. (2022), Cybersecurity Design Principles: 2 Books In 1, Richie Miller, 210 s.
[6] Nathan C. , Steven F. (2022), Human Aspects of Information Security and Assurance, New York: Springer International Publishing, 329 s.
[7] https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/
[8] https://medium.com/@sevda_kh/sql-injection-4e959849f59d
[9] https://www.acunetix.com/websitesecurity/sql-injection2/
[10] https://www.knowledgehut.com/blog/security/sql-injection-and-prevention
[11] https://pentest-tools.com/blog/sql-injection-attacks

BAZAR MÜNASIBƏTLƏRI ŞƏRAITINDƏ INFORMASIYA TƏHLÜKƏSIZLIYININ BƏZI AKTUAL MƏSƏLƏLƏRI

Zamirə İbrahimli
Azərbaycan dövlət Neft və Sənaye Universiteti

Xülasə

Məqalədə müasir insan cəmiyyətinə yeni çağırışlar və təhdidlər kimi informasiya təhlükəsizliyindən bəhs edilir. İnformasiya təhlükəsizliyinin əsas pozucuları kimi hakerlərin elektron hücumları üsulları, spamlar, korporativ viruslar, korporativ şəbəkələr tərəfindən zərərli və təsadüfi hərəkətlər, təbii təhlükələr sadalanır. Müasir cəmiyyətdə informasiya təhlükəsizliyinin təmin edilməsi təcrübəsinin təkmilləşdirilməsində qanunvericilik bazasının gücləndirilməsi, İKT (informasiya-kommunikasiya texnologiyaları) sahəsində kadr hazırlığı sisteminin təkmilləşdirilməsi və bütün internet istifadəçilərinin