DOI: https://doi.org/10.36719/2789-6919/45/176-179

Nurvin Rəhimov
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəçilik Akademiyası
magistrant
https://orcid.org/0009-0001-8633-9608
ragimovnurvin1@gmail.com

SQLMAP və SQL INJECTION hücumlarının avtomatlaşdırılmış aşkarlanması

Xülasə

Bu məqalə SQL injection hücumlarının avtomatlaşdırılmış aşkarlanması üçün istifadə olunan SQLMap alətinin ətraflı təhlilinə həsr edilmişdir. SQL injection, kibercinayətkarların veb tətbiqlərin zəifliklərindən istifadə edərək məlumat bazalarına icazəsiz giriş əldə etdiyi geniş yayılmış hücum növüdür. Bu cür hücumlar çox vaxt ciddi nəticələrə, o cümlədən məxfi məlumatların sızmasına, məlumat bazalarının məhv edilməsinə və sistemlərin fəaliyyətinin pozulmasına gətirib çıxarır. Məlumat bazalarının təhlükəsizliyini təmin etmək üçün güclü və effektiv həll yolları tələb olunur. SQL injection (SQLi) hücumlarının avtomatlaşdırılmış aşkarlanması məqsədilə geniş istifadə olunan SQLMap alətinin funksional imkanlarının və tətbiq mexanizmlərinin dərin təhlilinə həsr olunmuşdur. SQL injection hücumları, veb əsaslı məlumat bazalarına qarşı yönəlmiş ən təhlükəli və geniş yayılmış təhlükəsizlik təhdidlərindən biridir. Bu hücum növü vasitəsilə kibercinayətkarlar məlumat sorğularını manipulyasiya edərək, sistemə icazəsiz giriş əldə edir, mövcud məlumatları dəyişdirir, silir və ya məxfi məlumatları sızdırırlar. Məqalədə qeyd olunur ki, bu cür hücumlar nəticəsində təkcə fərdi və kommersiya məlumatlarının ifşası deyil, həm də dövlət qurumları və kritik infrastruktur sistemləri üçün ciddi təhlükə yaranır. Beləliklə, SQL injection hücumlarının vaxtında aşkarlanması və qarşısının alınması informasiya təhlükəsizliyinin əsas prioritetlərindən biri kimi dəyərləndirilir. Bu kontekstdə SQLMap aləti təhlükəsizlik üzrə mütəxəssislər üçün əvəzolunmaz bir vasitə kimi çıxış edir. Alət açıq mənbə kodlu olub, müxtəlif növ SQL injection zəifliklərini aşkar etmək, onları avtomatik şəkildə istismar etmək və nəticələri analiz etmək üçün geniş imkanlar təqdim edir. SQLMap, istifadəçinin bir neçə komanda sətrindən istifadə etməklə məlumat bazasının strukturu, istifadəçi səlahiyyətləri, saxlanılan məlumatlar və digər mühüm göstəricilər barədə ətraflı informasiya əldə etməsinə şərait yaradır.

Açar sözlər: *SQL injection, SQLMap, avtomatlaşdırılmış aşkarlama, məlumat bazası təhlükəsizliyi, zəifliklərin analizi, hücum simulyasiyası, veb tətbiq təhlükəsizliyi*

Nurvin Rahimov
Academy of Public Administration under
the President of the Republic of Azerbaijan
Master student
https://orcid.org/0009-0001-8633-9608
ragimovnurvin1@gmail.com

Automated Detection of SQLMAP and SQL INJECTION Attacks

Abstract

This article is dedicated to a comprehensive analysis of the SQLMap tool, which is widely used for the automated detection of SQL injection attacks. SQL injection is a common type of cyberattack in which cybercriminals exploit vulnerabilities in web applications to gain unauthorized access to databases. Such attacks often lead to severe consequences, including the leakage of confidential data, destruction of databases, and disruption of system operations. Ensuring the security of databases requires robust and effective solutions. The paper focuses on the functional capabilities and application mechanisms of SQLMap, a popular tool for the automated detection of SQL injection

(SQLi) vulnerabilities. SQL injection attacks are among the most dangerous and widespread security threats targeting web-based databases. By manipulating data queries, attackers gain unauthorized access, alter existing information, delete data, or extract sensitive records. The article notes that these attacks pose a serious threat not only to personal and commercial data but also to government agencies and critical infrastructure systems. Therefore, the timely detection and prevention of SQL injection attacks are considered one of the main priorities in information security. In this context, SQLMap stands out as an indispensable tool for security specialists. It is open-source and offers extensive features for identifying various types of SQL injection vulnerabilities, exploiting them automatically, and analyzing the outcomes. SQLMap enables users to retrieve detailed information about the database structure, user privileges, stored data, and other critical components with just a few command-line inputs.

Keywords*: SQL injection, SQLMap, automated detection, database security, vulnerability analysis, attack simulation, web application security*

Giriş

Müasir texnologiyalar dövründə veb tətbiqlərin geniş yayılması ilə paralel olaraq, kibertəhlükəsizlik sahəsində yeni təhlükələr və çağırışlar ortaya çıxmaqdadır. Bu təhlükələr arasında SQL injection hücumları, veb tətbiqlərin zəifliklərindən istifadə edərək məlumat bazalarına qanunsuz giriş əldə etmək üçün ən geniş istifadə olunan və təsir gücü yüksək olan metodlardan biridir (AlAzzawi, 2024). Bu hücumların əsas məqsədi sistemlərdə saxlanılan həssas məlumatları əldə etmək, dəyişdirmək və ya məhv etməkdir. Təhlükəsizlik baxımından zəif veb tətbiqlər bu cür hücumların başlıca hədəfi olur və nəticədə həm texniki, həm də maliyyə baxımından ciddi problemlər ortaya çıxır (Mui, Frankl, 2010).

SQL injection hücumlarının təsirləri yalnız məlumatların oğurlanması və ya dəyişdirilməsi ilə məhdudlaşmır. Bu hücumlar şirkətlərin nüfuzuna xələl gətirir, istifadəçi məlumatlarının məxfiliyini pozur və təşkilatları ciddi hüquqi və maliyyə sanksiyaları ilə üz-üzə qoya bilər (Anley, Heasman, Grindlay, 2007). Buna görə də, SQL injection hücumlarının vaxtında aşkarlanması və qarşısının alınması kibertəhlükəsizlik sahəsində prioritet məsələlərdən biridir (Kharche, Patil, Gohad, Ambetkar, 2015). Ənənəvi yanaşmalar bu təhlükələrlə mübarizədə çox vaxt kifayət qədər effektiv olmur, çünki hücum metodları daim yenilənir və mürəkkəbləşir.

Tədqiqat

SQLMap: İlkin Quraşdırma və Ümumi Anlayışlar. SQL injection hücumlarını aşkarlamaq və onlara qarşı müvafiq tədbirlər görmək çox vacibdir. Bu məqsədlə, müxtəlif alətlərdən istifadə olunur, bunlardan ən effektiv təsiri olan isə SQLMap-dır. SQLMap, SQL injection zəifliklərini avtomatik olaraq aşkarlamağa və təsdiq etməyə kömək edən güclü bir açıq mənbə alətidir (Oudah, Marhusin, 2024). Bu alət, həmçinin müxtəlif SQL injection növlərini istifadə edərək məlumat bazalarına istismar etmə qabiliyyətinə malikdir (Mui, Frankl, 2010). SQLMap, mütəxəssislərin və kibertəhlükəsizlik peşəkarlarının işini asanlaşdırır, çünki o bütün bu əməliyyatları avtomatik şəkildə yerinə yetirir və təhlükəsizlik testlərinin sürətini artırır. SQLMap-ın quraşdırılması sadədir və müxtəlif əməliyyat sistemlərində (Linux, macOS, Windows) həyata keçirilə bilər. Rəsmi github səhifəsindən aşağıdakı standart git clone əmri ilə kompüterimizə yükləyə bilərik (Singh, 2016).

SQLMap hal-hazırda sql açıqlarının avtomatik şəkildə aşkarlanması üçün istifədə olunan ən güclü alətdir və özündə 100-dən çox metodu birləşdirir (Singh, 2016, s.34). Quraşdırmadan dərhal sonra proqram haqqında məlumatları Cədvəl 1-də göstərilmiş komandalar ilə əldə edə bilərik.

Cədvəl 1*. SQLMap: baza əmrlər*

COMMAND	DESCRIPTION
-h, --help	Əsas kömək mesajını göstərir
-hh	Ətraflı kömək mesajını göstərir
-version	Proqramın versiyasını göstərir
-v VERBOSE	Təfsilat səviyyəsi: 0-6

SQLMap açıq mənbəli layihə olduğundan daima dəstəklənir və məlum olan bütün sql açıqlarının avtomatlaşdırımış şəkildə test edilməsi üçün inkşaf etdirilir. Bu alət bizi aşağıdakı geniş imkanlarla təmin edir və bu sahədə işimizin məhsuldarlığını xeyli artırır:

- Məlumat çıxarılması – burada biz məlumat bazası adlarını (--dbs), cədvəl adlarını (--tables), sütun adlarını (--columns), cədvəl məlumatlarını (--dump) və müəyyən bir sütundakı məlumatları (--dump -C column_name) əldə edə bilərik;
- Məlumat bazası haqqında məlumatın çıxarılması - VBİS versiyası və növü (--banner), VBİS istifadəçi adları (--users), VBİS istifadəçilərinin parol hash-ləri (--passwords), VBİS -də işləyən proseslər (--threads);
- Məlumatların manipulyasiyası - yeni cədvəl yaratmaq, mövcud məlumatları dəyişmək və ya silmək, xüsusi SQL sorğularını icra etmək (--sql-query);
- Təhlükəsizlik istismarı - Hədəf sistemdə komanda icra etmək (--os-shell), faylların oxunması və dəyişdirilməsi (--file-read və --file-write);
- Şəbəkə və sessiya manipulyasiyası - Cookie təhlili və istifadə (--cookie), HTTP başlıqlarının dəyişdirilməsi (--headers);
- Avtomatlaşdırılmış hücumlar - şifrə hash-lərini açmaq üçün (--crack), Union-based, Error-based və Time-based hücumları avtomatik tətbiq etmək, Hədəf URL-də avtomatik injection növü təyin etmək;
- Testlərin dərinləşdirilməsi - Xüsusi istifadəçi-agent göndərmək (--user-agent), Xüsusi HTTP parametrləri göndərmək (--data), Müxtəlif HTTP metodlarından istifadə etmək (GET, POST, PUT və s.).
- Xüsusi təhlükəsizlik testləri - SQL injeksiyanın olduğu parametrləri aşkar etmək, Web application firewall bypass metodlarını sınamaq (--tamper), JSON, XML və Base64 kodlaşdırılmış məlumatlar üzərində injection testləri.

Müasir dövrdə bütün sistemlərdə, veb tətbiqlərdə və.s sql injection və digər potensial təhdidlər nəzərə alınaraq müxtəlif təhlükəsizlik tədbirləri həyata keçirilir (Anley, Heasman, Grindlay, 2007). Bu zaman aparılan testlər xüsusi tələblərə cavab verməli və sistemimizdə olan potensial sql açıqları gözdən qaçırmamalıdır. Mütləq şəkildə WAF(Web Application Firewall) və digər bizim əməliyyatlarımızı bloklaya biləcək sistemləri nəzərə alaraq hücumu onlar tərəfindən bloklanmayacaq şəkildə həyata keçirməliyik (Singh, 2016). Çünki, bizim məqsədimiz sistemin tam şəkilli analizi və mümkün zəiflikləri hücumdan öncə müəyyən etmək və aradaq qaldırmaqdır. SQLMap aləti bu istiqamətdə avtomatlaşdırılmış slq injection testləri zamanı prosesi tam ələ almağa imkan verir. Biz hücum zamanı bir çox parametrlərdən istifadə edərək təhlükəsizlik sistemlərindən yayına bilərik. Bununla yanaşı, SQLMap aləti istifadəçiyə xüsusi "tamper" skriptləri və təkmilləşdirilmiş konfiqurasiya imkanları təqdim edərək, WAF və digər qoruyucu sistemlərə qarşı daha çevik yanaşma tətbiq etməyə şərait yaradır (Stuttard, Pinto, 2011). Bu, SQL injection testlərinin daha effektiv və real ssenarilərə uyğun aparılmasına imkan verir. Məsələn, istəyə uyğun olaraq HTTP başlıqlarının dəyişdirilməsi, fərqli payload kombinasiyalarının seçilməsi və ya sorğuların gecikdirilməsi kimi üsullarla SQLMap təhlükəsizlik divarlarını aşaraq zəiflikləri müəyyən edə bilir (Jahanshahi, Doupé, Egele, 2020; Tajpour, Ibrahim, Sharifi, 2014).

Eyni zamanda, alətin “enumeration” funksionallığı vasitəsilə, sadəcə zəifliyin olub-olmadığını deyil, onun nə qədər təhlükəli olduğunu da analiz etmək mümkündür (Howard, LeBlanc, 2003). Bu verilənlər bazasının strukturu, istifadəçi icazələri, parolların şifrələmə vəziyyəti və digər həssas məlumatlar haqqında ətraflı məlumat toplamağa imkan verir (Kazmi, 2019). Beləliklə, yalnız aşkarlama deyil, eyni zamanda təsirliliyin ölçülməsi və risklərin prioritetləşdirilməsi də həyata keçirilmiş olur (Tajpour, Masrom, Heydari, Ibrahim, 2010). Ümumiyyətlə, müasir təhlükəsizlik testlərində təkcə zəifliklərin texniki aşkarlanması kifayət deyil. Hücum səviyyəsində həyata keçirilən avtomatlaşdırılmış testlər, həm də sistemin təhlükəsizlik arxitekturasını, monitorinq səviyyəsini və cavab mexanizmlərini qiymətləndirmək üçün mühüm vasitədir (Baklizi, Atoum, Abdullah, Al-Wesabi, Otoom, Hasan, 2022). SQLMap kimi vasitələrin düzgün tətbiqi, təhlükəsizlik komandalarının daha hazırlıqlı və strateji yanaşmalar formalaşdırmasına kömək edir.

Nəticə

Məqalədə SQL injection hücumlarının avtomatlaşdırılmış aşkarlanması və təhlili üçün SQLMap alətinin önəmi və funksionallığı geniş şəkildə araşdırılmışdır. Bu növ hücumlar, müasir kibertəhlükəsizlik mühitində ən geniş yayılan və təhlükəli hücum növlərindən biridir. SQLMap, açıq mənbəli və çoxfunksiyalı bir alət olaraq, SQL injection zəifliklərini müəyyən etmək və bu zəifliklərdən istifadə yollarını simulyasiya etmək üçün mütəxəssislərə geniş imkanlar təqdim edir.

Nəticə olaraq qeyd etmək olar ki, SQL injection hücumlarına qarşı müasir müdafiə metodlarının inkişafı kibertəhlükəsizliyin təmin edilməsində prioritet məsələdir. SQLMap kimi vasitələrin düzgün tətbiqi və mütəmadi istifadə olunması, veb tətbiqlərin və məlumat bazalarının daha təhlükəsiz olmasını təmin edə bilər. SQLMap, açıq mənbəli və çoxfunksiyalı bir alət olaraq, SQL injection zəifliklərini müəyyən etmək və bu zəifliklərdən istifadə yollarını simulyasiya etmək üçün mütəxəssislərə geniş imkanlar təqdim edir (TryHackMe – SQLMap, n.d.). Onun avtomatlaşdırılmış funksiyaları, müxtəlif SQL injection texnikalarını dəstəkləməsi və geniş verilənlər bazası sistemləri ilə uyğunluğu, onu kibertəhlükəsizlik sahəsində əvəzolunmaz bir vasitə halına gətirir.

Ədəbiyyat

1. AlAzzashi, A. (2024). SQL injection detection using RNN deep learning model. *Journal of Applied Engineering and Technological Science*, 5(1).
2. Anley, C., Heasman, J., Grindlay, B. (2007). *The Shellcoder's Handbook: Discovering and Exploiting Security Holes*. Shiley.
3. Baklizi, M., Atoum, I., Abdullah, N., Al-Shesabi, O.A., Otoom, A.A., Hasan, M.A. (2022). A technical review of SQL injection tools and methods: A case study of SQLMap. *International Journal of Intelligent Systems and Applications in Engineering*, 10(3), pp.75–85.
4. Howard, M., LeBlanc, D. (2003). *Writing Secure Code*. Microsoft .
5. Jahanshahi, R., Doupé, A., Egele, M. (2020). *You shall not pass: Mitigating SQL injection attacks on legacy web applications*. arXiv preprint
6. Kazmi, M.A.N. (2019). *SQL injection detection and exploitation framework for penetration testing*. London Metropolitan University.
7. Kharche, S., Patil, J., Gohad, K., Ambetkar, B. (2015). *Preventing SQL injection attack using pattern matching algorithm*. arXiv preprint
8. Mui, R., Frankl, P. (2010). *Preventing SQL injection through automatic query sanitization with ASSIST*. arXiv preprint arXiv:1009.3712.
9. Oudah, M.A.M., Marhusin, M.F. (2024). SQL injection detection using machine learning: A review. *Malaysian Journal of Science Health & Technology*, 10(1), pp.39–49.
10. Singh, J. P. (2016). *Analysis of SQL injection detection techniques*. arXiv preprint arXiv:1605.02796.
11. Stuttard, D., Pinto, M. (2011). *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*. Shiley.
12. *SQLMap Documentation. SQLMap User Guide*. https:github.com/sqlmapproject.sqlmap.wiki.
13. *SQLMap Cheat Sheet: Flags & Commands for SQL Injection.* https:highon.coffee.blog.sqlmap-cheat-sheet/#sqlmap-optimisation.
14. Tajpour, A., Masrom, M., Heydari, M. Z., Ibrahim, S. (2010). SQL injection detection and prevention tools assessment. *In 2010 3rd IEEE International Conference on Computer Science and Information Technology* (Vol. 9, pp. 1–5). IEEE.
15. Tajpour, A., Ibrahim, S., Sharifi, M. (2014). *Web application security by SQL injection detection tools*. ResearchGate.
16. *TryHackMe - SQLMap*: The Basics. https://tryhackme.com/room/sqlmapthebasics

Daxil oldu: 04.02.2025
Qəbul edildi: 19.05.2025