ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ СУЧАСНИХ ВЕБ-РЕСУРСІВ

Д'якова Н.Є., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З кожним роком кількість веб-ресурсів та кількість конфіденційної інформації з якою вони взаємодіють стає все більшою. За рахунок цього розвивається велика кількість нових кіберзагроз. Тому безпека веб-ресурсів займає дедалі більшу нішу в сучасності. Тестування допомагає у пошуку вразливостей, запобіганню загроз та забезпеченню безпеки веб-ресурсів [1].

Метою доповіді є дослідження вразливостей веб-ресурсів, що найчастіше використовуються.

В результаті дослідження було розглянуто найбільші ризики для безпеки веб-ресурсів, такі як Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components тощо [2]. В доповіді розглянута одна з найпоширеніших вразливість - Injection, що включає в себе ін'єкції різних типів (SQL, LDAP, XPath, OS commands). Реалізовані на практиці SQL-ін'єкції.

В роботі було проведено тестування на можливість SQL-ін'єкцій [3]. Також розглянуті різні програми для тестування [4, 5]:

SQL Injection Fuzz Strings (з інструменту wfuzz) – Fuzzdb;

Bernardo Damele AG: sqlmap, інструмент автоматичного впровадження SQL(підтримка великої кількості баз даних, підтримка Linux і Windows);

Muhaimin Dzulfakar: MySqloit, MySql Injection takeover tool (підтримка Linux).

Проведений аналіз показав, що для тестування найбільше підходить SQL Injection Fuzz Strings [5]. Вона підтримується в операційних системах Windows, Unix і Linux, має багатий функціонал, видає результат у реальному часі. Головним недоліком MySqloit є відсутність структурованої документації.

Усі програми тестування дозволяють підвищити безпеку веб-додатків шляхом знаходження його вразливостей у вигляді SQL-ін'єкцій.

Список літератури

1. Поддубний В.О., Сєвєрінов О.В. Менеджмент вразливостей як складова частина системи управління інформаційної безпеки. – НТУ «ХПІ», 2020.

2. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 03.10.2022).

3. Gupta S. SQL injection attacks. Berkeley, CA : Apress, 2020. URL: https://doi.org/10.1007/978-1-4842-6505-5 (дата звернення: 04.10.2022).

4. Sqlmap: automatic SQL injection and database takeover tool. sqlmap: automatic SQL injection and database takeover tool. URL: http://sqlmap.org/ (дата звернення: 06.11.2022).

5. GitHub - dtrip/mysqloit: Mysqloit v0.2. GitHub. URL: https://github.com/dtrip/mysqloit (дата звернення: 06.11.2022).