

Лабораторна робота 14

Мельника Олеся

Мета: знайти SQL та XSS вразливість

Результат:

1. Використовуючи програму OWASP ZAP я знайшов декілька SQL Injection на сайті <http://testphp.vulnweb.com/>

Приклади декілька з них:

The image displays three screenshots of the OWASP ZAP (Zed Attack Proxy) interface, showing the results of security scans for SQL Injection vulnerabilities. Each screenshot provides detailed information about a specific vulnerability found on the website <http://testphp.vulnweb.com/>.

First Screenshot:

- SQL Injection**
- URL-адреса: <http://testphp.vulnweb.com/artists.php?artist=5-2>
- Ризик: High
- Надійність: Medium
- Параметр: artist
- Атака: 5-2
- Докази: CWE ID: 89, WASC ID: 19
- Джерело: Активно (40018 - SQL Injection)
- Опис: SQL injection may be possible.

Second Screenshot:

- SQL Injection**
- URL-адреса: <http://testphp.vulnweb.com/listproducts.php?artist=3+AND+1%3D1+--+>
- Ризик: High
- Надійність: Medium
- Параметр: artist
- Атака: 3 OR 1=1 --
- Докази: CWE ID: 89, WASC ID: 19
- Джерело: Активно (40018 - SQL Injection)
- Опис: SQL injection may be possible.

Third Screenshot:

- SQL Injection**
- URL-адреса: <http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+>
- Ризик: High
- Надійність: Medium
- Параметр: cat
- Атака: 4 OR 1=1 --
- Докази: CWE ID: 89, WASC ID: 19
- Джерело: Активно (40018 - SQL Injection)
- Опис: SQL injection may be possible.

SQL Injection
URL-адреса: http://testphp.vulnweb.com/product.php?pic=8-2
Ризик: High
Надійність: Medium
Параметр: pic
Атака: 8-2
Докази:
CWE ID: 89
WASC ID: 19
Джерело: Активно (40018 - SQL Injection)
Опис:
SQL injection may be possible.

Current Scans 0 0 0 0 1 0 0 0 0 0

SQL Injection
URL-адреса: http://testphp.vulnweb.com/secured/newuser.php
Ризик: High
Надійність: Medium
Параметр: username
Атака: ZAP' OR '1'='1' --
Докази:
CWE ID: 89
WASC ID: 19
Джерело: Активно (40018 - SQL Injection)
Опис:
SQL injection may be possible.

Current Scans 0 0 0 0 1 0 0 0 0 0

2. Також було знайдено XSS вразливості

Cross Site Scripting (Reflected)
URL-адреса: http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
Ризик: High
Надійність: Low
Параметр: file
Атака: <script>alert(1);</script>
Докази: <script>alert(1);</script>
CWE ID: 79
WASC ID: 8
Джерело: Активно (40012 - Cross Site Scripting (Reflected))
Опис:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is

Cross Site Scripting (Reflected)
URL-адреса: http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%281%29%3B
Ризик: High
Надійність: Medium
Параметр: pp
Атака: javascript:alert(1);
Докази: javascript:alert(1);
CWE ID: 79
WASC ID: 8
Джерело: Активно (40012 - Cross Site Scripting (Reflected))
Опис:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is

Висновок: на даному сайті можна знайти багато різних вразливостей, чим можуть скористатись зломисники, але оскільки це тестовий сайт, це не грає дуже велику роль.