

Задание выполнил студент группы 2345 Романенко Кирилл Д.

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.

HTTP Parameter Pollution – Расщепление запроса

ugs Change Password Create User Set Security Level Re

/ HTTP Parameter Pollution /

In order to vote for your favorite movie, your name must be entered:

Проверил

/ HTTP Parame

In order to vote for your favorite movie, yo

Вывод:

<http://192.168.56.11/bwapp/hpp-2.php?name=123&action=vote>

192.168.56.11/bwapp/hpp-2.php?name=123&action=vote

Index of / — <http://192.168.56.11>

Wikipedia — wikipedia.org








Challenges/Web - Server : HTML - Source code [Root Me : Hacking and

Burp Suite Community Edition — <http://burp>

YouTube — youtube.com

avito — avito.ru

aliexpress — aliexpress.com

This time, search with:       

an extreme

Change Password

/ HTTP P

Hello 123, please vote for

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

Это голосование. Нажал vote у фильма Iron Man

<http://192.168.56.11/bwapp/hpp-3.php?movie=2&name=123&action=vote>

192.168.56.11/bwapp/hpp-3.php?movie=2&name=123&action=vote

Index of / — <http://192.168.56.11>

Wikipedia — wikipedia.org








Challenges/Web - Server : HTML - Source code [Root Me : Hacking and I

Burp Suite Community Edition — <http://burp>

YouTube — youtube.com

avito — avito.ru

aliexpress — aliexpress.com

This time, search with:       

bwapp

an extreme

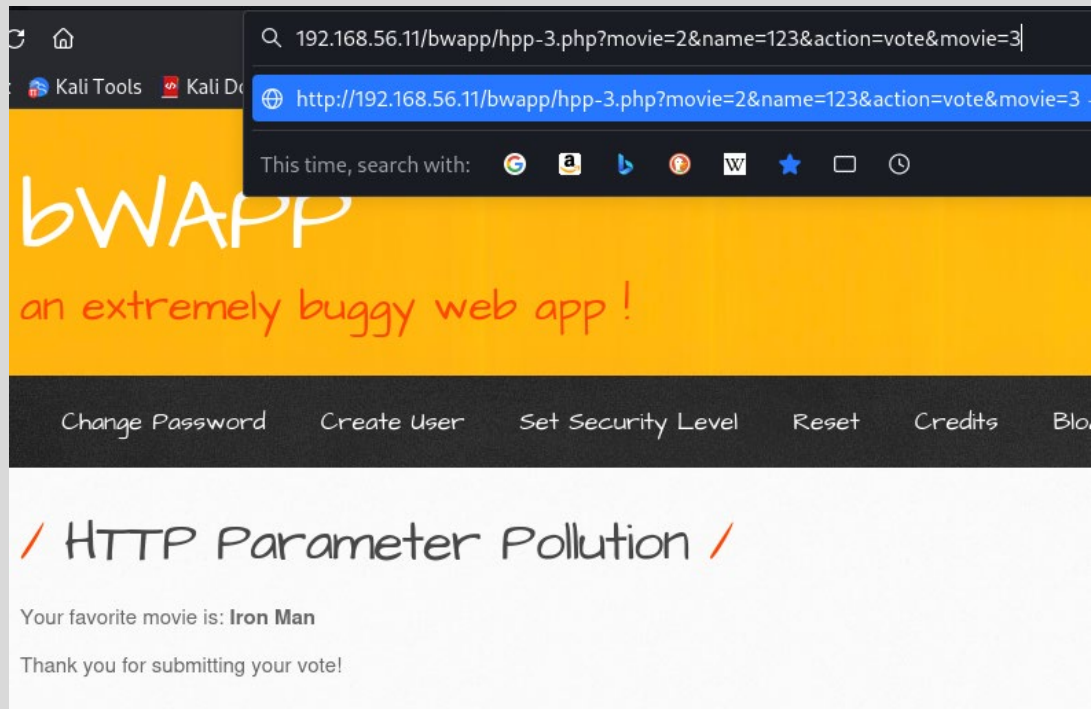
Change Password

/ HTTP Parameter Pollution /

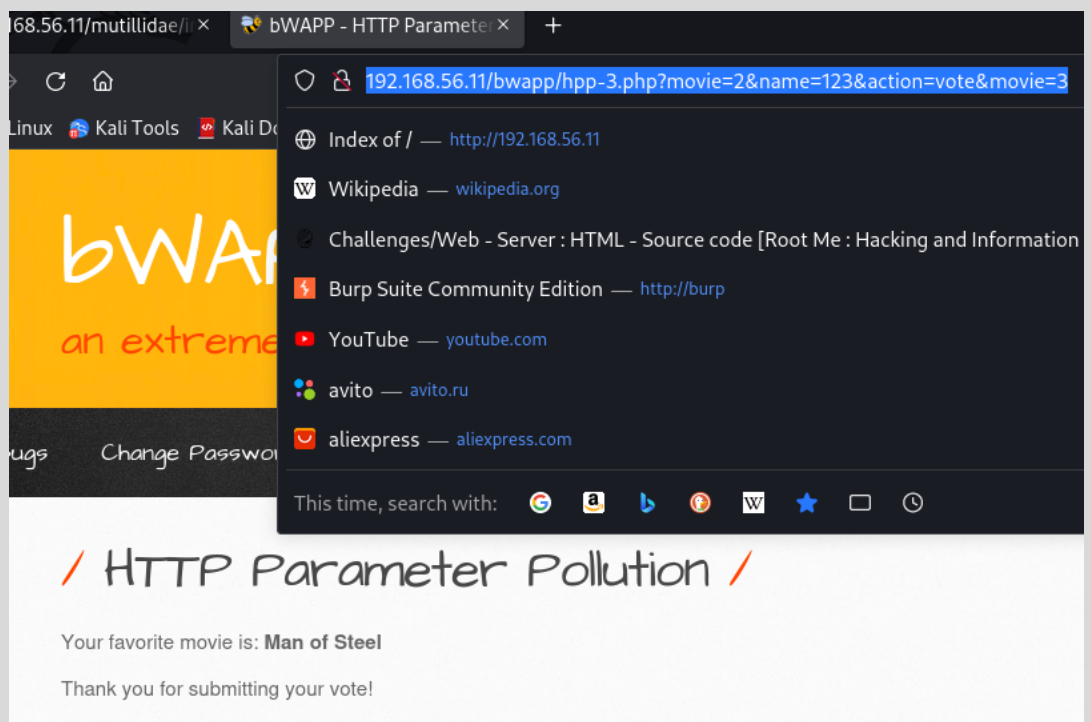
Your favorite movie is: **Iron Man**

Thank you for submitting your vote!

Подставляю в конец запроса новый параметр



Результат



Фильм заменился.

В запросе учитывается только последнее значение параметра.

Благодаря этому можно подменить ссылку, которая обрабатывает при нажатии клавиши vote на этапе голосования.

Пользователь будет голосовать за фильм №2, а сервер обработает запрос и приме голос на счёт фильма №3

Это можно использовать в любого рода голосованиях, в пользу конкретного варианта

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.

Открыл страницу

Изучил код в браузере. Форма работает через метод GET

```
<legend>Document Viewer</legend>
▼<form id="idDocumentForm" action="index.php" method="GET" enctype="application/x-www-form-urlencoded">
  <input type="hidden" name="page" value="document-viewer.php">
```

То есть параметры передаются прямо в запросе строки браузера

Выбрал 1 вариант, нажал на кнопку.

Вывод в строке: <http://192.168.56.11/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation%2Fchange-log.html&document-viewer-php-submit-button=View+Document>

Выбрал 2 вариант, нажал на кнопку

<http://192.168.56.11/mutillidae/index.php?page=document-viewer.php&PathToDocument=robots.txt&document-viewer-php-submit-button=View+Document>

Подставил параметр **PathToDocument=robots.txt** в конец запроса к варианту №1

<http://192.168.56.11/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation%2Fchange-log.html&document-viewer-php-submit-button=View+Document&PathToDocument=robots.txt>

В ответ на выбранный №1 сервер дал ответ решив, что я выбрал вариант №2

Пример атаки: Это можно использовать в любого рода голосованиях, в пользу конкретного варианта

3. Изучите пример 3 на практике. Составьте отчет о рассматриваемой уязвимости.

В момент добавления товара в корзину есть возможность положить его, изменив стоимость. Далее к оплате будет выставлен счёт на ту сумму, которую указал злоумышленник.

Где найдена уязвимость

Уязвимость расположена по адресу

[<Ссылка на сайт>](#)

Наименование продукта: <Имя онлайн-магазина>.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, проанализировав историю запросов, которые появляются на пути от добавления товара в корзину до этапа оплаты

Выводы и рекомендации по устранению

Уязвимость позволяет изменить стоимость любого товара. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Установить проверку входящего параметра price и id

Используемое программное обеспечение

- Браузер Firefox browser 102.5.0esr (64-bit)
- BurpSuite