**Урок 8. Non-RCE vulnerabilities**

Задание 1:

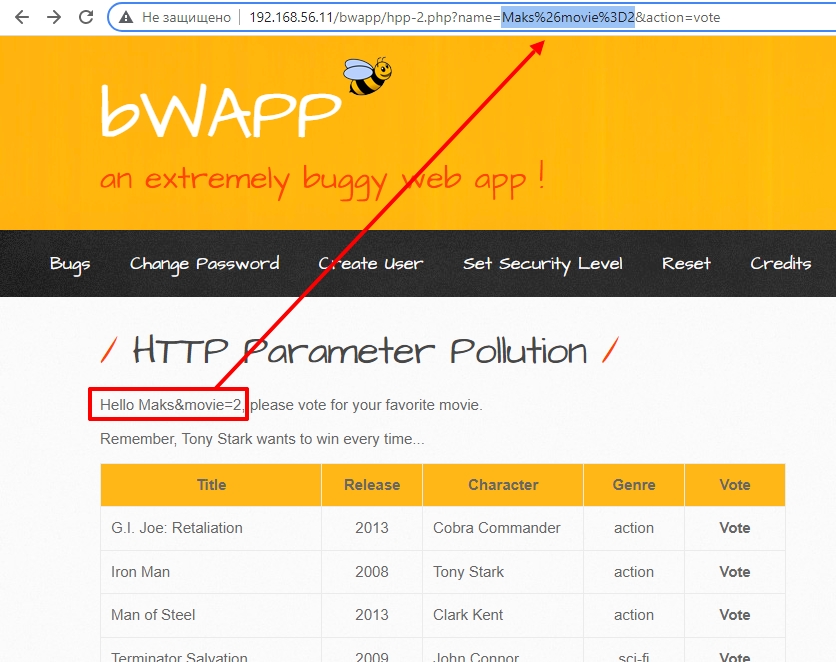
Изучите пример уязвимости HPP со страницы [**http://192.168.56.11/bwapp/hpp-1.php**](http://192.168.56.11/bwapp/hpp-1.php).  
 В ответе укажите уязвимый параметр, сценарий и последствия от эксплуатации уязвимости.

Решение:

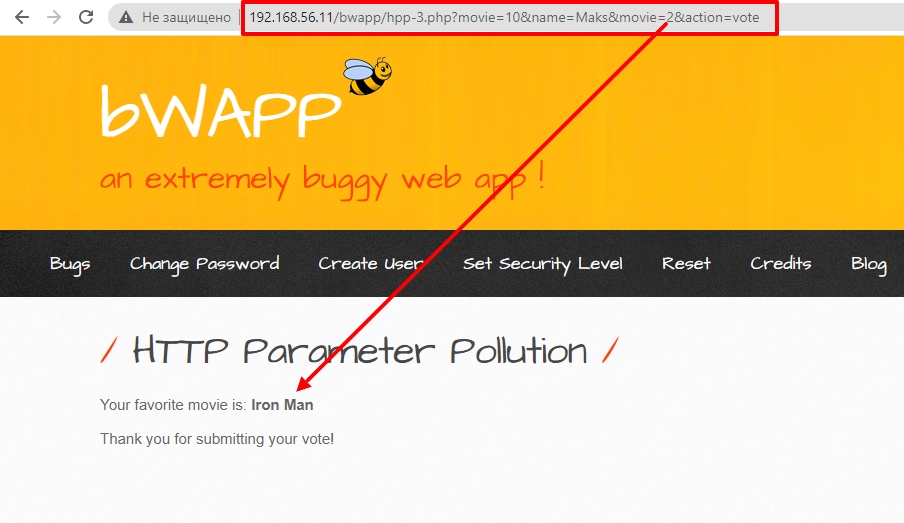
**Уязвимый параметр**: movie

**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**](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:



* 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 скомпрометированаи не является легитимной. Доверять результатам голосования нельзя.

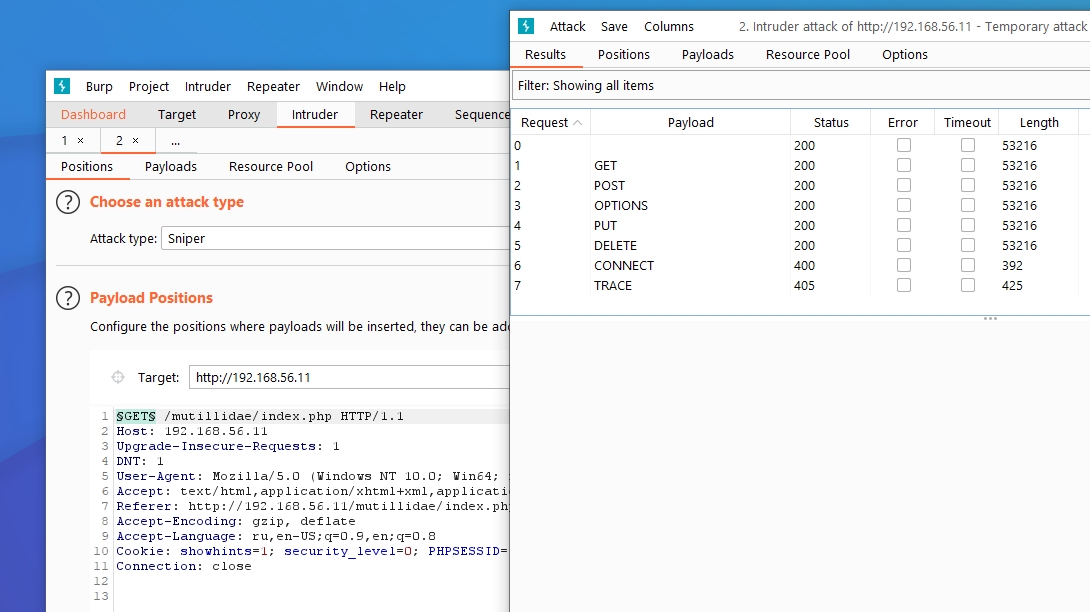
Задание 2:

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:



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.

