

[Open in app](#) ↗[Sign up](#)[Sign in](#)**Medium** SearchPrinu_17 · [Follow](#)

3 min read · Dec 22, 2024

 Listen Share

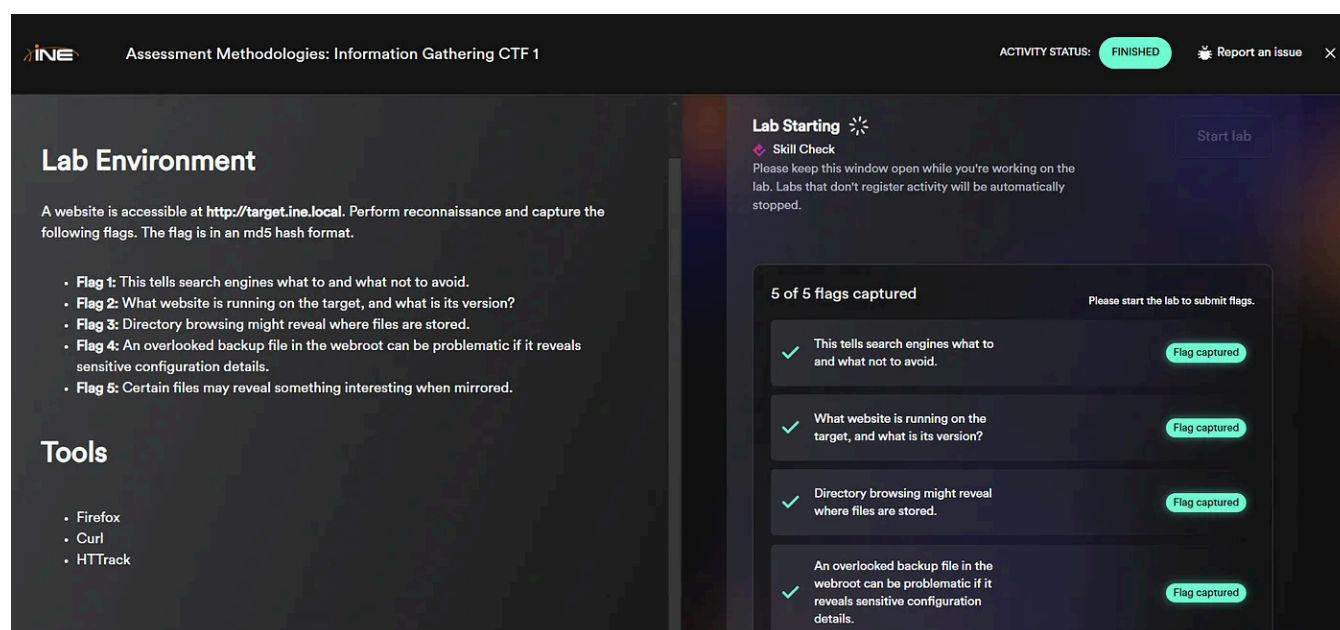
Assessment Methodologies: Information Gathering CTF 1 (EJPT INE)

Hii all!!

I'm excited to share the write-up of my recently purchased EJPT CTF, and I'm glad to walk you through the solution.

Let's get started!

Time to dive into our first lab!



Lab Environment

A website is accessible at <http://target.ine.local>. Perform reconnaissance and capture the following flags. The flag is in an md5 hash format.

- **Flag 1:** This tells search engines what to and what not to avoid.
- **Flag 2:** What website is running on the target, and what is its version?
- **Flag 3:** Directory browsing might reveal where files are stored.
- **Flag 4:** An overlooked backup file in the webroot can be problematic if it reveals sensitive configuration details.
- **Flag 5:** Certain files may reveal something interesting when mirrored.

Tools

- Firefox
- Curl
- HTTrack

Lab Starting ✨

💡 **Skill Check**

Please keep this window open while you're working on the lab. Labs that don't register activity will be automatically stopped.

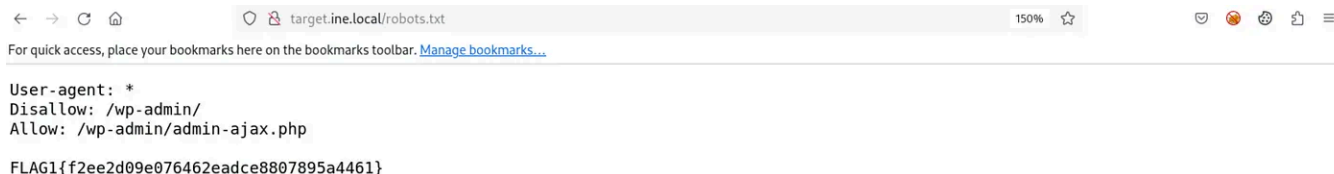
[Start lab](#)

5 of 5 flags captured Please start the lab to submit flags.

- ✓ This tells search engines what to and what not to avoid. [Flag captured](#)
- ✓ What website is running on the target, and what is its version? [Flag captured](#)
- ✓ Directory browsing might reveal where files are stored. [Flag captured](#)
- ✓ An overlooked backup file in the webroot can be problematic if it reveals sensitive configuration details. [Flag captured](#)

Q.1 This tells search engines what to and what not to avoid.

As we know, the robots.txt file tells search engines what to crawl and what to avoid. Let's take a look at the robots.txt file, and here we find our first flag.



```
target.ine.local/robots.txt
150% ☆
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

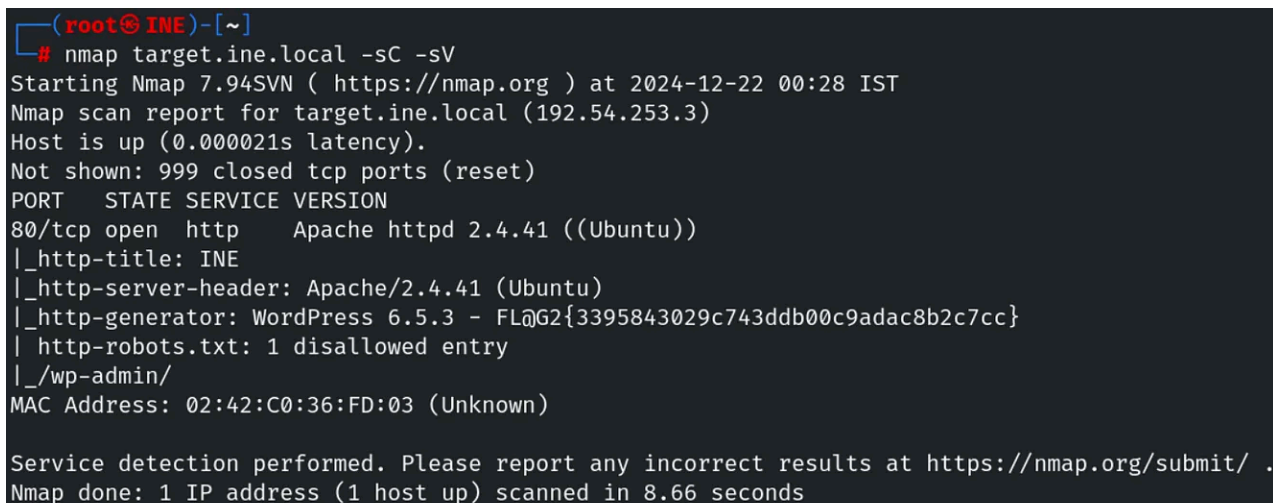
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

FLAG1{f2ee2d09e076462eadce8807895a4461}
```

FLAG 1: f2ee2d09e076462eadce8807895a4461

Q.2 What website is running on the target, and what is its version?

To determine the version of the website, we can use Nmap to identify the server and its version. Run the following command in the terminal: “*nmap target.ine.local -sC -sV*”



```
(root@INE)-[~]
# nmap target.ine.local -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-22 00:28 IST
Nmap scan report for target.ine.local (192.54.253.3)
Host is up (0.000021s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-title: INE
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 6.5.3 - FL@G2{3395843029c743ddb00c9adac8b2c7cc}
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
MAC Address: 02:42:C0:36:FD:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.66 seconds
```

And here we find our second flag, which is:

FLAG 2: 3395843029c743ddb00c9adac8b2c7cc

Q.3 Directory browsing might reveal where files are stored.

For this, we need to brute-force the directories, and we can use the simple `dirb` command. Once we run the scan, we will need to manually search for the flag.

```
(root@INE)~[~]
# dirb http://target.ine.local

DIRB v2.22
By The Dark Raver

START_TIME: Sun Dec 22 00:35:09 2024
URL_BASE: http://target.ine.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt




GENERATED WORDS: 4612

— Scanning URL: http://target.ine.local/ —
+ http://target.ine.local/index.php (CODE:301|SIZE:0)
+ http://target.ine.local/robots.txt (CODE:200|SIZE:108)
+ http://target.ine.local/server-status (CODE:403|SIZE:281)
=> DIRECTORY: http://target.ine.local/wp-admin/
=> DIRECTORY: http://target.ine.local/wp-content/
=> DIRECTORY: http://target.ine.local/wp-includes/
+ http://target.ine.local/xmlrpc.php (CODE:405|SIZE:42)

— Entering directory: http://target.ine.local/wp-admin/ —
+ http://target.ine.local/wp-admin/admin.php (CODE:302|SIZE:0)
```




```
— Entering directory: http://target.ine.local/wp-content/ —
+ http://target.ine.local/wp-content/index.php (CODE:200|SIZE:0)
=> DIRECTORY: http://target.ine.local/wp-content/plugins/
=> DIRECTORY: http://target.ine.local/wp-content/themes/
=> DIRECTORY: http://target.ine.local/wp-content/uploads/
```

The flag is located in the `wp-content/uploads` directory.

  target.ine.local/wp-content/uploads/

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

Index of /wp-content/uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 2024/	2024-05-27 08:46	-	
 flag.txt	2024-12-22 05:31	40	

Apache/2.4.41 (Ubuntu) Server at target.ine.local Port 80

FLAG 3: ccca869e58f54c02b0fa4f9b5a1ee84f

Q.4 An overlooked backup file in the webroot can be problematic if it reveals sensitive configuration details.

To find the backup files, we need to use the `-x` option in the command to specify the file extensions. The most common backup file extensions are: `.bak`, `.tar.gz`, `.zip`, `.sql`, and `.bak.zip`.

Run the following command in Terminal: “`dirb http://target.ine.local -w /usr/share/dirb/wordlists/big.txt -X .bak,.tar.gz,.zip,.sql,.bak.zip`”

```
(root@INE) ~
# dirb http://target.ine.local -w /usr/share/dirb/wordlists/big.txt -X .bak,.tar.gz,.zip,.sql,.bak.zip

DIRB v2.22
By The Dark Raver

START_TIME: Sun Dec 22 11:05:53 2024
URL_BASE: http://target.ine.local/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
EXTENSIONS_LIST: (.bak,.tar.gz,.zip,.sql,.bak.zip) | (.bak)(.tar.gz)(.zip)(.sql)(.bak.zip) [NUM = 5]

GENERATED WORDS: 4612

— Scanning URL: http://target.ine.local/ —
+ http://target.ine.local/wp-config.bak (CODE:200|SIZE:3438)
```

We can use the `curl` command to read its contents. And here, we find our fourth flag, which is:

```
curl http://target.ine.local/wp-config.bak
```

```

* Authentication unique keys and salts.
*
* Change these to different unique phrases! You can generate these using
* the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
*
* You can change these at any point in time to invalidate all existing cookies.
* This will force all users to have to log in again.
*
* @since 2.6.0
*/
define('AUTH_KEY',          'Mq^#|v{n0fQ6Vn[tr 6e4glzi:OVs/9(IQ .7f^dp3ym4,th-0$Qx.])|2+(t(sE');
define('SECURE_AUTH_KEY',   'S_LKQ#*}p*U}kdX[GNNVM2*0YISNQ&zrFl jEUNq5T}0Zg|,s0|yB68^|N*1nS-p');
define('LOGGED_IN_KEY',     '`tz-Uz9IXka,5z0J BD0l/zfU|r2|;9BGL5l~A1RQtZMwh=JftaU$2)$FI%v};|E');
define('NONCE_KEY',        'D>ZN961k>aHWJ*R8#&x+rR>3g|<[:G 8B+rqPH WrWet1SC60+ LL/S+=[G-6g7)');
define('AUTH_SALT',        '+<2l=;osCL(L)zV[=uvr[]}2^j-16(gFq18V<m|fP<R{7DV`^0&bb3fxY+Jf|~;C');
define('SECURE_AUTH_SALT', 'HG6/Q/ceR-;$;?jCL}<cL4@LKzDjv,M=K-gR<]iHiAqcHQ0+rXcWn/jMt0#K,uWq%');
define('LOGGED_IN_SALT',    'REsFv+0sL*qd=yV<oPaAXeYj@f)A[/Wm5-?|_4d::(;dXcps`rgJf]t4B0Q3)RcH');
define('NONCE_SALT',       'Q.:0=pFDTA-LNB&ekjJu(mp7$cQrF|IZ _hOWDA&Q18w6CL(<{+1$a-ZJ~<(!_');

/** FLAG4{de9e6050a6de44daa74e91e87b3112f3} */

```

FLAG 4: de9e6050a6de44daa74e91e87b3112f3

Q.5 Certain files may reveal something interesting when mirrored.

As the question suggests, we need to mirror the website to find this flag. To mirror the website, we can use the `httrack` command:

```
httrack http://target.ine.local -O target.html
```

```

(root@INE)~$ httrack http://target.ine.local -O target.html
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Sun, 22 Dec 2024 11:17:34 by HTTrack Website Copier/3.49-5 [XR6C0'2014]
mirroring http://target.ine.local with the wizard help..
* target.ine.local/index.php/wp-json/oembed/1.0/embed?url=http%3A%2F%2Ftarget.ine.local%2Findex.php%2F2024%2F05%2F27%2FHello-world%2F (2116 bytes) -
32/38: target.ine.local/index.php/wp-json/oembed/1.0/embed?url=http%3A%2F%2Ftarget.ine.local%2Findex.php%2F2024%2F05%2F27%2FHello-world%2F (0 bytes)
* target.ine.local/wp-admin/load-scripts.php?c=0&load%5Bchunk_0%5D=jquery-core,jquery-migrate,zxcvbn-async,wp-polyfill-inert,regenerator-runtime,wp-p
40/52: target.ine.local/wp-admin/load-scripts.php?c=0&load%5Bchunk_0%5D=jquery-core,jquery-migrate,zxcvbn-async,wp-polyfill-inert,regenerator-runtime
Done.: target.ine.local/wp-login.php (4105 bytes) - OK
Thanks for using HTTrack!

```

Once the mirroring is complete, navigate to the directory where the website was saved. The flag is located in the file `xmlrpc0db0.php`.

```

(root@INE)~/target.html/target.ine.local$ cat xmlrpc0db0.php
<?xml version="1.0" encoding="UTF-8"?><rsd version="1.0" xmlns="http://archipelago.phrasewise.com/rsd">
  <service>
    <engineName>WordPress</engineName>
    <engineLink>https://wordpress.org/</engineLink>
    <homePageLink>http://target.ine.local/</homePageLink>
    <apis>
      <api name="WordPress" blogID="1" preferred="true" apiLink="http://target.ine.local/xmlrpc.php" />
      <api name="Movable Type" blogID="1" preferred="false" apiLink="http://target.ine.local/xmlrpc.php" />
      <api name="MetaWeblog" blogID="1" preferred="false" apiLink="http://target.ine.local/xmlrpc.php" />
      <api name="Blogger" blogID="1" preferred="false" apiLink="http://target.ine.local/xmlrpc.php" />
      <api name="FLAG5{e79d9c81cc384cdd91bbc563fd61b7ee}" blogID="1" preferred="false" apiLink="http://target.ine.local/xmlrpc.php" />
    </apis>
    <api name="WP-API" blogID="1" preferred="false" apiLink="http://target.ine.local/index.php/wp-json/" />
  </service>
</rsd>

```

FLAG 5: e79d9c81cc384cdd91bbc563fd61b7ee

Thank you for reading!
See you all in the next CTF.

Happy Hacking!

Information Gathering

Assessment Methodologies

Ejpt

Ctf Walkthrough

Ctf Writeup



Follow



Written by Prinu_17

34 Followers · 1 Following

Responses (2)



What are your thoughts?

Respond



Hello World

Dec 24, 2024



Pretty useful 👍