

# EJPT Skill Check Lab – Information Gathering (CTF 1)

## Ciel:

Získať 5 flagov prostredníctvom prieskumu cieľovej webovej aplikácie (<http://target.ine.local>) a aplikovaním znalostí zo zberu informácií.

## Lab Environment

A website is accessible at <http://target.ine.local>. Perform reconnaissance and capture the following flags.

- **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

### **Použité nástroje:**

→ [Mozilla Firefox](#)

→ [gobuster](#)

→ [wget](#)

→ [curl](#)

→ [whatweb](#)

→ [HTTrack](#)

→ [DIRB](#)

→ [grep](#)

→ [md5sum](#)

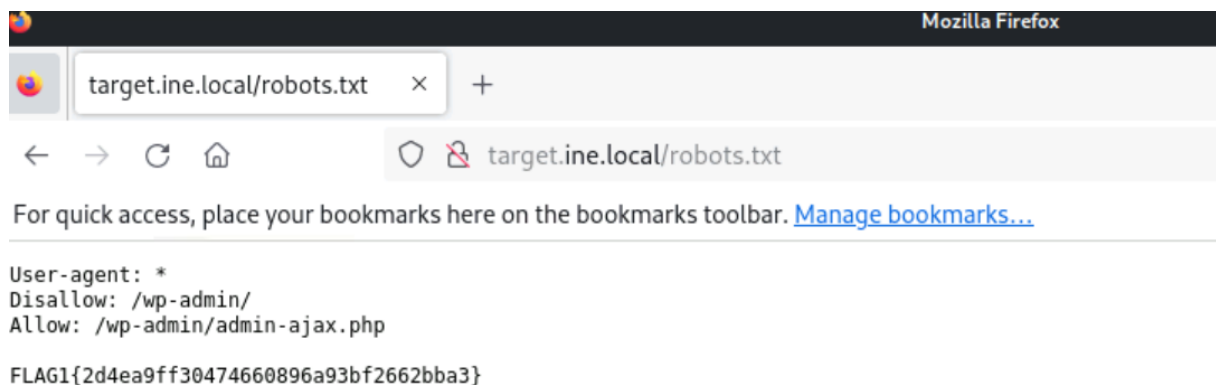
### **Flag 1 – robots.txt:**

**Task: „This tells search engines what to and what not to avoid“**

URL: <http://target.ine.local/robots.txt>

Obsah: **FLAG1{2d4ea9ff30474660896a93bf2662bba3}**

→ výsledný hash pre EJPT: **2d4ea9ff30474660896a93bf2662bba3**



**4 of 5 flags captured**

Please start the lab to submit flags.



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

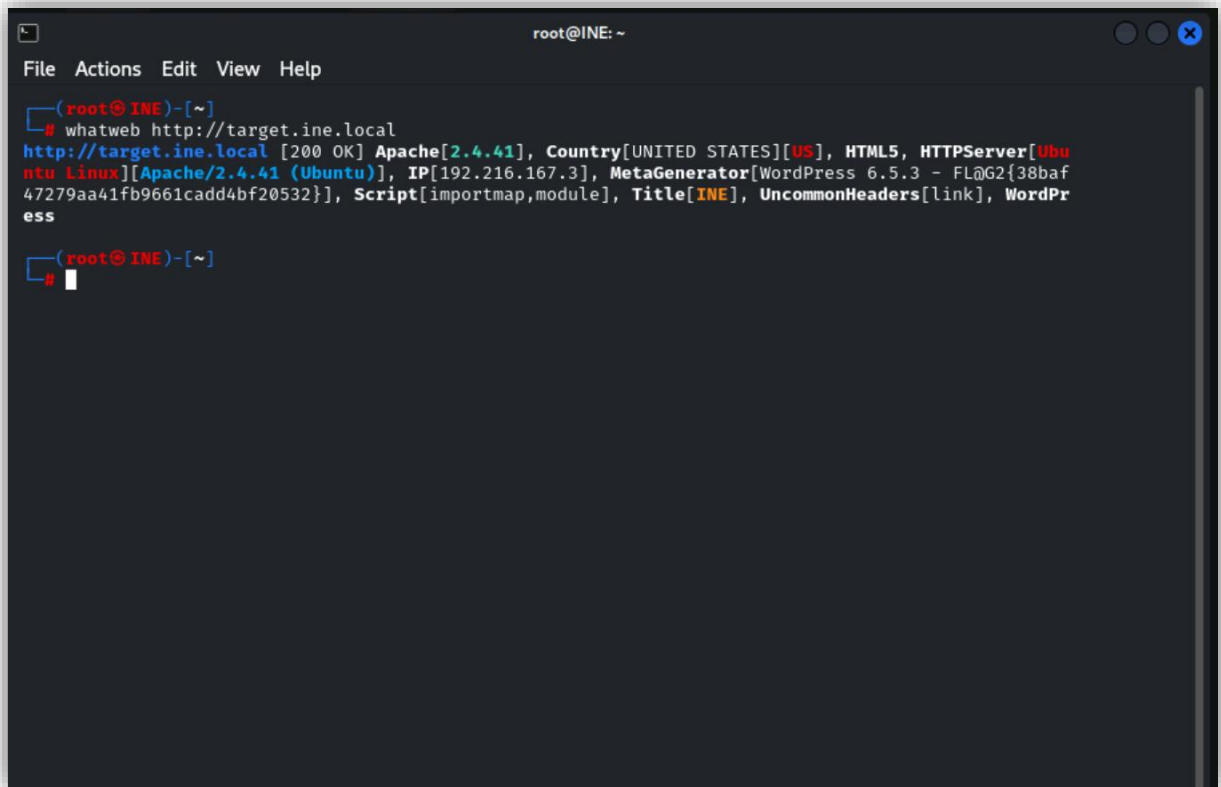
Flag captured

## Flag 2 – Webový server a verzia

Task: „What website is running on the target, and what is its version?“

Príkaz:

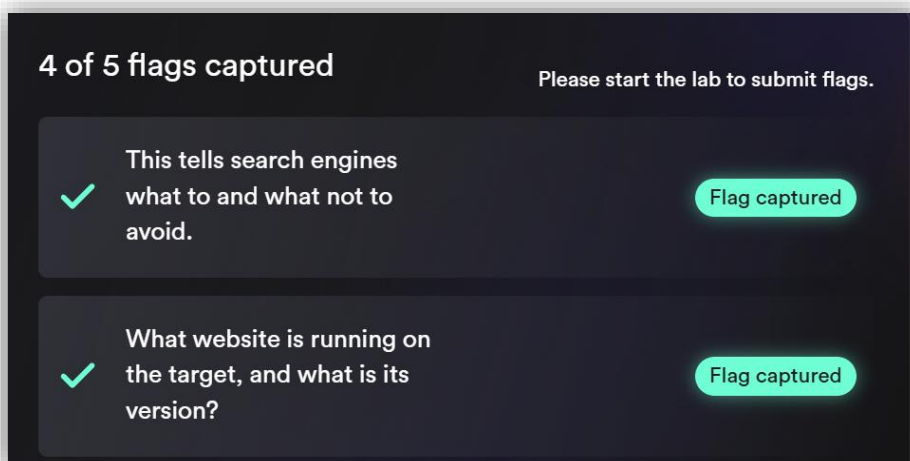
**whatweb** http://target.ine.local



```
root@INE: ~  
File Actions Edit View Help  
(root@INE)~[~]  
# whatweb http://target.ine.local  
http://target.ine.local [200 OK] Apache[2.4.41], Country[UNITED STATES][US], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.216.167.3], MetaGenerator[WordPress 6.5.3 - FL@G2{38baf47279aa41fb9661cadd4bf20532}], Script[importmap,module], Title[INE], UncommonHeaders[link], WordPress  
(root@INE)~[~]  
#
```

Výsledok:

- Apache/2.4.41 (Ubuntu), WordPress 6.5.3
- MetaGenerator[WordPress 6.5.3 → FL@G2{...}]
- FL@G2{38baf47279aa41fb9661cadd4bf20532}
- výsledný hash pre EJPT: 38baf47279aa41fb9661cadd4bf20532



4 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

## Flag 3 – Directory Browsing

Task: „Directory browsing might reveal where files are stored“

Príkaz:

`dirb http://target.ine.local`

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

____
DIRB v2.22
By The Dark Raver
____

START_TIME: Sun Apr 20 20:01:49 2025
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)
=> DIRECTORY: http://target.ine.local/wp-admin/css/
=> DIRECTORY: http://target.ine.local/wp-admin/images/
=> DIRECTORY: http://target.ine.local/wp-admin/includes/
+ http://target.ine.local/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://target.ine.local/wp-admin/js/
=> DIRECTORY: http://target.ine.local/wp-admin/maint/
=> DIRECTORY: http://target.ine.local/wp-admin/network/
=> DIRECTORY: http://target.ine.local/wp-admin/user/

--- 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/
```

```
—— Entering directory: http://target.ine.local/wp-includes/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/css/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/images/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/includes/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/js/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/maint/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://target.ine.local/wp-admin/network/ ——  
+ http://target.ine.local/wp-admin/network/admin.php (CODE:302|SIZE:0)  
+ http://target.ine.local/wp-admin/network/index.php (CODE:302|SIZE:0)  
  
--- Entering directory: http://target.ine.local/wp-admin/user/ ——  
+ http://target.ine.local/wp-admin/user/admin.php (CODE:302|SIZE:0)  
+ http://target.ine.local/wp-admin/user/index.php (CODE:302|SIZE:0)  
  
--- Entering directory: http://target.ine.local/wp-content/plugins/ ——  
+ http://target.ine.local/wp-content/plugins/index.php (CODE:200|SIZE:0)  
  
--- Entering directory: http://target.ine.local/wp-content/themes/ ——  
+ http://target.ine.local/wp-content/themes/index.php (CODE:200|SIZE:0)  
  
—— Entering directory: http://target.ine.local/wp-content/uploads/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)
```

```
—— Entering directory: http://target.ine.local/wp-admin/js/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/maint/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
—— Entering directory: http://target.ine.local/wp-admin/network/ ——  
+ http://target.ine.local/wp-admin/network/admin.php (CODE:302|SIZE:0)  
+ http://target.ine.local/wp-admin/network/index.php (CODE:302|SIZE:0)  
  
—— Entering directory: http://target.ine.local/wp-admin/user/ ——  
+ http://target.ine.local/wp-admin/user/admin.php (CODE:302|SIZE:0)  
+ http://target.ine.local/wp-admin/user/index.php (CODE:302|SIZE:0)  
  
—— Entering directory: http://target.ine.local/wp-content/plugins/ ——  
+ http://target.ine.local/wp-content/plugins/index.php (CODE:200|SIZE:0)  
  
—— Entering directory: http://target.ine.local/wp-content/themes/ ——  
+ http://target.ine.local/wp-content/themes/index.php (CODE:200|SIZE:0)  
  
—— Entering directory: http://target.ine.local/wp-content/uploads/ ——  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)
```

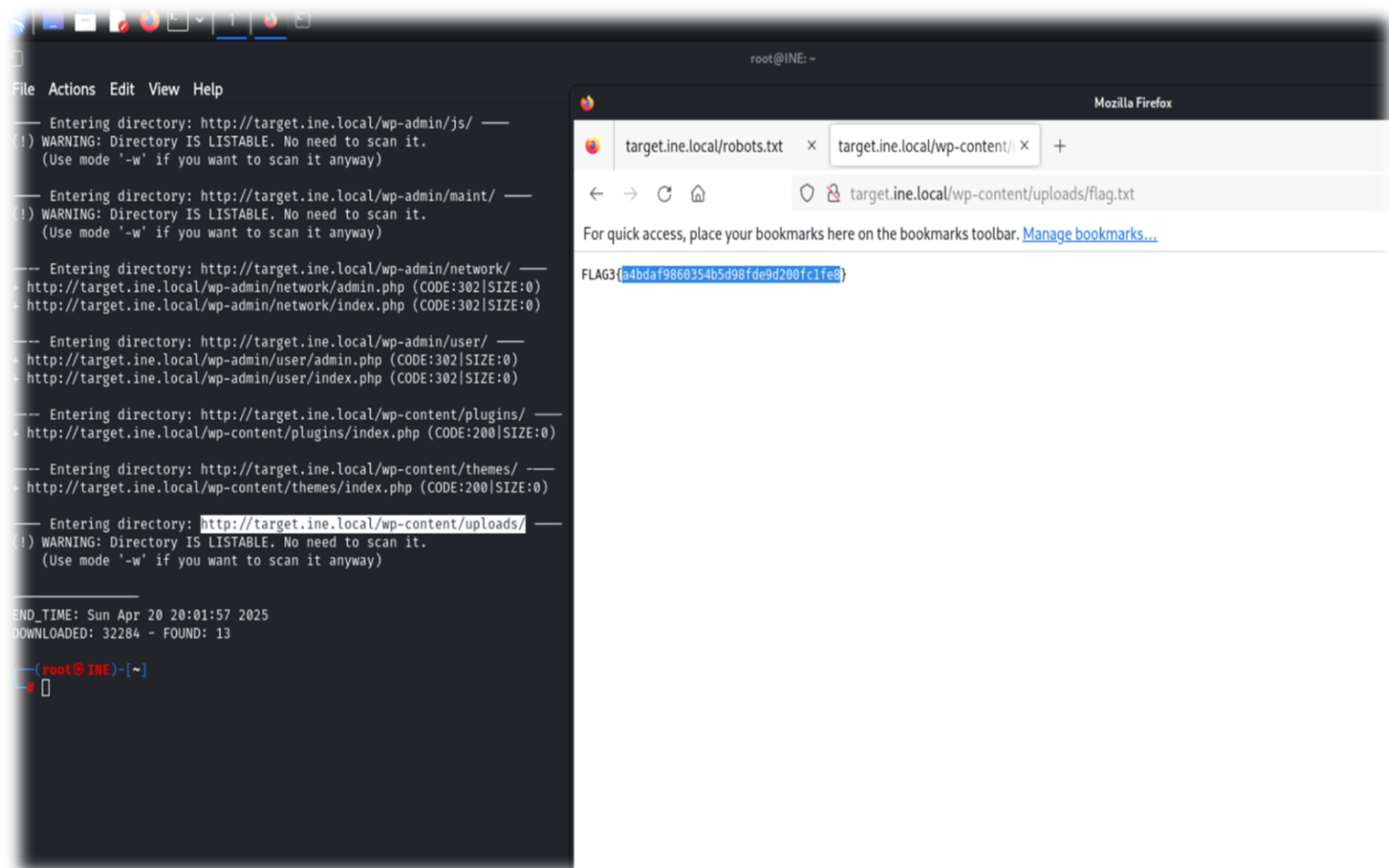
---

```
END_TIME: Sun Apr 20 20:01:57 2025
```

```
DOWNLOADED: 32284 - FOUND: 13
```

```
(root@INE)-[~]  
# █
```





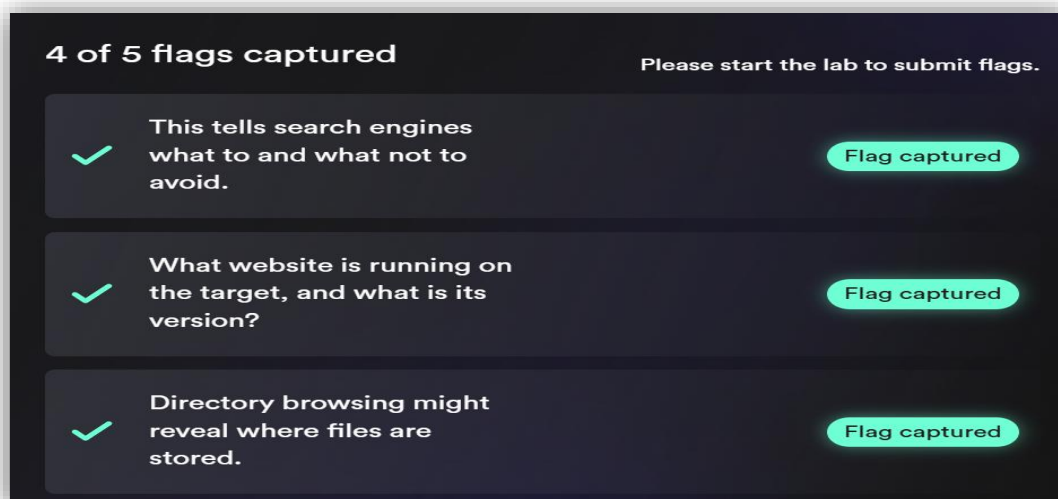
## Výsledok:

→ **/wp-content/uploads/flag.txt**

→ **WARNING:** Directory is **LISTABLE**, no need to scan it

Obsah: **FLAG3{a4bda9f806354b5d98fde9d200fc1fe8}**

→ potrebný hash pre EJPT: **a4bda9f806354b5d98fde9d200fc1fe8**



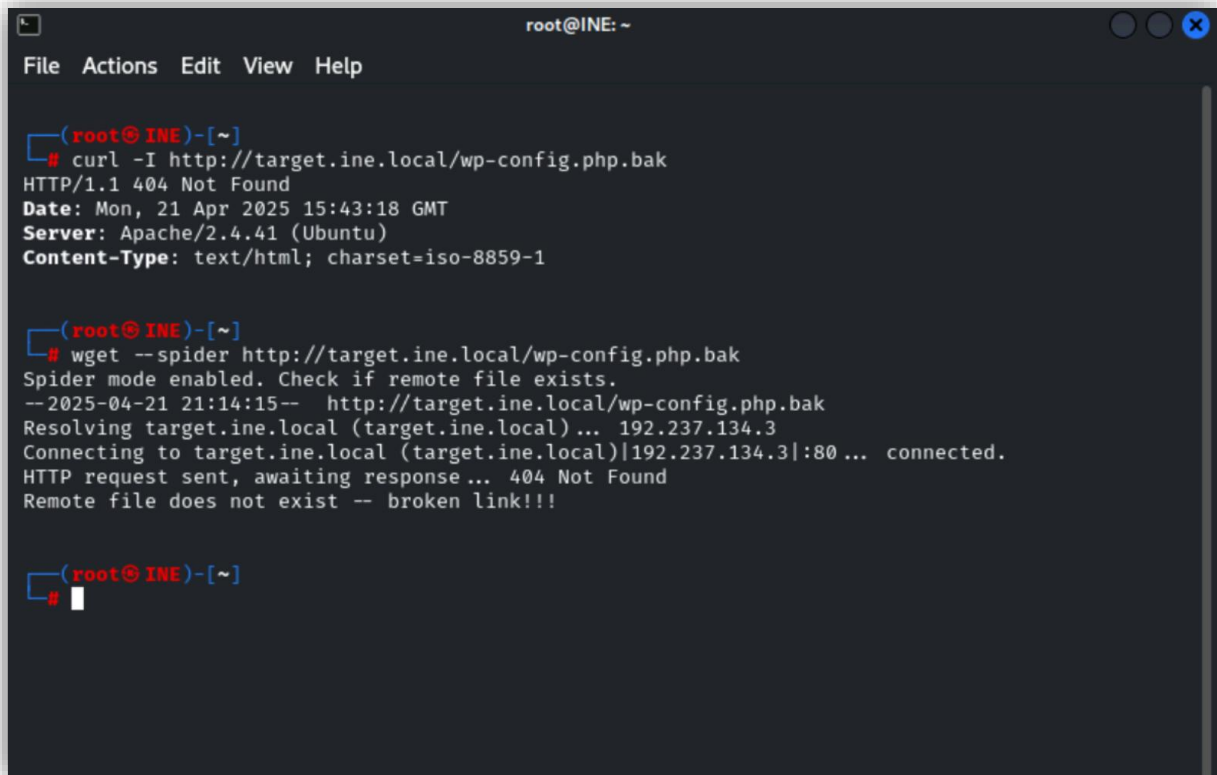
## Flag 4 – Backup file v root adresári (neúspešný)

### Príkazy:

**curl -I** <http://target.ine.local/wp-config.php.bak>

**wget --spider** <http://target.ine.local/wp-config.php.bak>

**gobuster** + vlastný wordlist s backup názvami



```
root@INE: ~  
File Actions Edit View Help  
  
(root@INE)-[~]  
# curl -I http://target.ine.local/wp-config.php.bak  
HTTP/1.1 404 Not Found  
Date: Mon, 21 Apr 2025 15:43:18 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Content-Type: text/html; charset=iso-8859-1  
  
(root@INE)-[~]  
# wget --spider http://target.ine.local/wp-config.php.bak  
Spider mode enabled. Check if remote file exists.  
--2025-04-21 21:14:15-- http://target.ine.local/wp-config.php.bak  
Resolving target.ine.local (target.ine.local) ... 192.237.134.3  
Connecting to target.ine.local (target.ine.local)|192.237.134.3|:80 ... connected.  
HTTP request sent, awaiting response ... 404 Not Found  
Remote file does not exist -- broken link!!!  
  
(root@INE)-[~]  
#
```

### Výsledok:

→ HTTP/1.1 404 Not Found

→ Remote file does not exist – broken link!!!

Výsledky hovoria, že súbor, **wp-config.php.bak**, reálne na tomto serveri neexistuje...

Ideme ďalej...



Skúsil som **gobuster**:

```
(root@INE)-[~]
# gobuster dir -u http://target.ine.local -w <(echo -e "wp-config.php.bak\nwp-config.php~\nwp-config.old\n.htac
cess.bak\n.htpasswd\nbackup.zip\ndb.sql") -x php,bak,zip,sql,~ --no-error

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                http://target.ine.local
[+] Method:             GET
[+] Threads:            10
[+] Wordlist:            /dev/fd/63
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Extensions:        sql,~,php,bak,zip
[+] Timeout:            10s

Starting gobuster in directory enumeration mode

Progress: 0 / 48 (0.00%)
Error: error on running gobuster: failed to rewind wordlist: seek /dev/fd/63: illegal seek

(root@INE)-[~]
#
```

### **Chyba:**

**Error on running gobuster: failed to rewind wordlist: seek /dev/fd/63: illegal seek**

→ ide o klasickú chybu, keď sa použije **process substitution** <(>) ako wordlist, pretože gobuster reálne potrebuje seekable file, aby mohol wordlist zresetovať, či pri /dev/fd/XX nefunguje...

Takže som skúsil toto:

**Zápis wordlistu do dočasného súboru → backups.txt:**

```
echo -e "wp-config.php.bak\nwp-config.php~\nwp-config.old\n.htaccess.bak\n.htpasswd\nbackup.zip\nndb.sql" > /tmp/backups.txt
```

```
root@INE: ~  
File Actions Edit View Help  
  
(root@INE)-[~]  
# echo -e "wp-config.php.bak\nwp-config.php~\nwp-config.old\n.htaccess.bak\n.htpasswd\nbackup.zip\nndb.sql" > /tmp/backups.txt  
  
(root@INE)-[~]  
# gobuster dir -u http://target.ine.local/ -w /tmp/backups.txt -x php,bak,zip,sql,~ --no-error  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Url: http://target.ine.local/  
[+] Method: GET  
[+] Threads: 10  
[+] Wordlist: /tmp/backups.txt  
[+] Negative Status codes: 404  
[+] User Agent: gobuster/3.6  
[+] Extensions: zip,sql,~,php,bak  
[+] Timeout: 10s  
  
Starting gobuster in directory enumeration mode  
  
/.htaccess.bak (Status: 403) [Size: 281]  
/.htaccess.bak~ (Status: 403) [Size: 281]  
/.htaccess.bak.bak (Status: 403) [Size: 281]  
/.htaccess.bak.php (Status: 403) [Size: 281]  
/.htaccess.bak.zip (Status: 403) [Size: 281]  
/.htaccess.bak.sql (Status: 403) [Size: 281]  
/.htpasswd (Status: 403) [Size: 281]  
/.htpasswd.php (Status: 403) [Size: 281]  
/.htpasswd.bak (Status: 403) [Size: 281]  
/.htpasswd.zip (Status: 403) [Size: 281]  
/.htpasswd.sql (Status: 403) [Size: 281]  
/.htpasswd~ (Status: 403) [Size: 281]  
Progress: 42 / 48 (87.50%)  
  
Finished  
  
(root@INE)-[~]  
#
```

### **Výsledok:**

Všetky files sú tam, ale sú **Status: 403 (Forbidden)**, čo znamená, že súbory sú na serveru ale server blokuje k nim priamy prístup.

Skúsil som ešte k ním prísť cez **curl -I príkaz...** alebo otvoriť ich priamo v prehliadači:

```
(root@INE)-[~]
# curl -I http://target.ine.local/.htaccess.bak.php
HTTP/1.1 403 Forbidden
Date: Mon, 21 Apr 2025 15:57:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
```

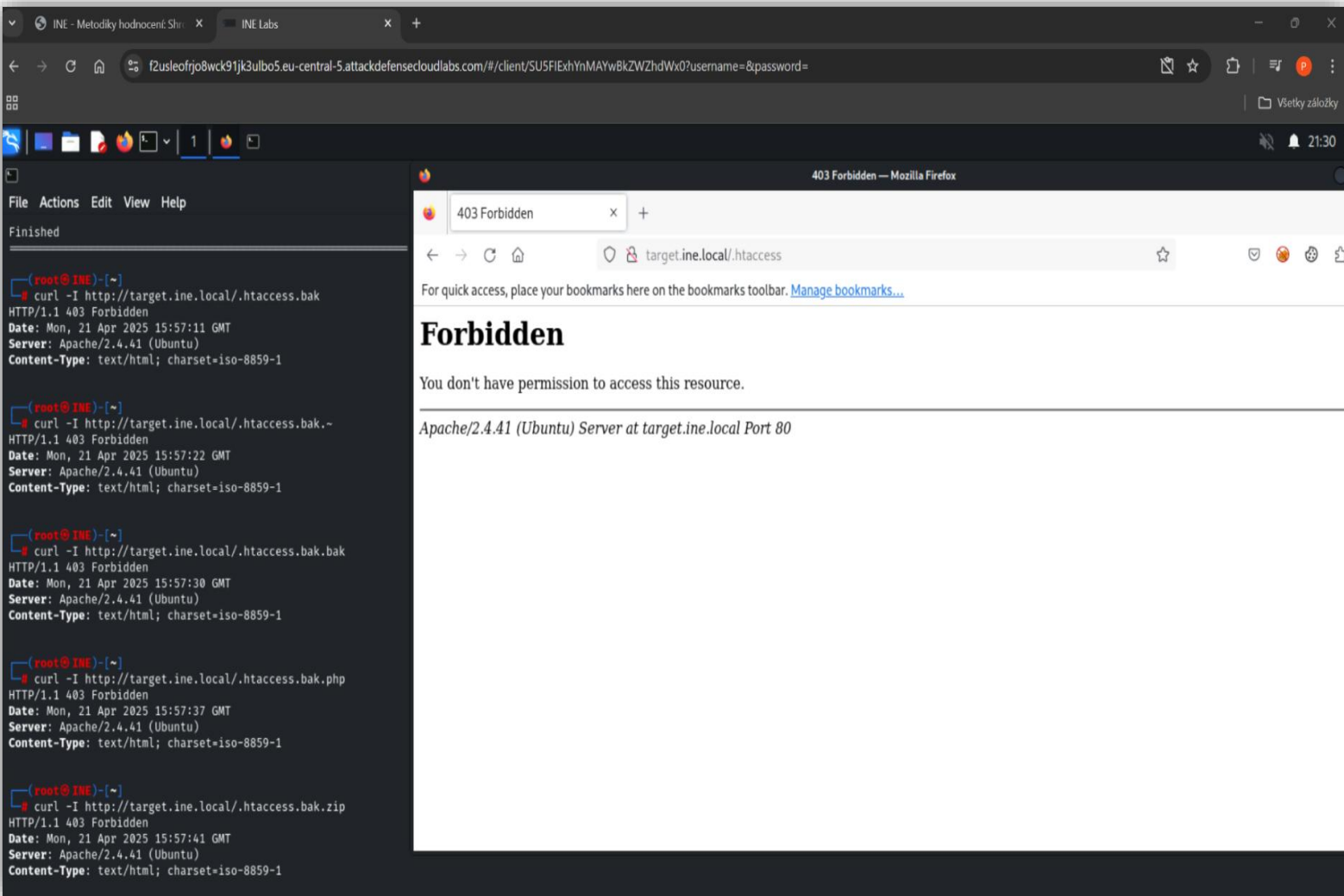
```
(root@INE)-[~]
# curl -I http://target.ine.local/.htaccess.bak.zip
HTTP/1.1 403 Forbidden
Date: Mon, 21 Apr 2025 15:57:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
```

```
(root@INE)-[~]
# curl -I http://target.ine.local/.htaccess.bak.sql
HTTP/1.1 403 Forbidden
Date: Mon, 21 Apr 2025 15:57:48 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
```

```
(root@INE)-[~]
# curl -I http://target.ine.local/.htpasswd
HTTP/1.1 403 Forbidden
Date: Mon, 21 Apr 2025 15:57:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
```

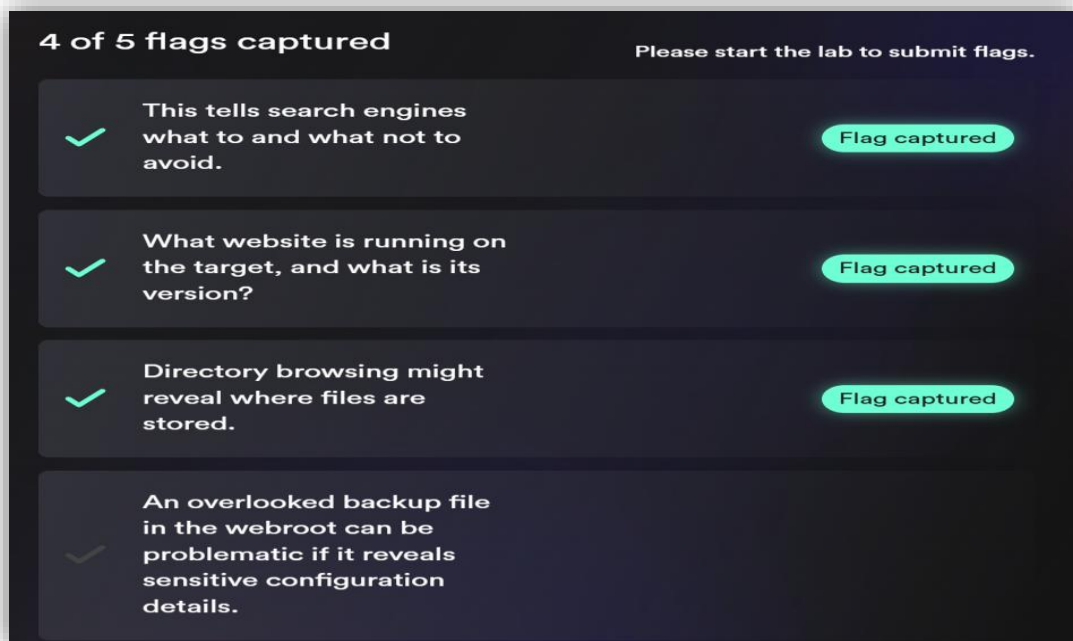
```
(root@INE)-[~]
# curl -I http://target.ine.local/.htpasswd.~
HTTP/1.1 403 Forbidden
Date: Mon, 21 Apr 2025 15:58:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
```

```
(root@INE)-[~]
#
```



## Výsledok:

- Všetky súbory z terminálu sú Forbidden
- Súbory som síce našiel, ale nemám oprávnenie ich otvárať...
- Tým pádom som **FLAG nemohol získať**, ale našiel som aspoň citlivé súbory



## Flag 5 – Mirrorovanie a zaujímavý súbor

Task: „Certain files may reveal something interesting when mirrored“

Príkazy:

**httrack** <http://target.ine.local> -O /root/httmirror -v

**wget** --mirror <http://target.ine.local>

```
(root@INE)~# httrack http://target.ine.local -O /root/httmirror -v
WARNING! You are running this program as root!
It might be a good idea to run as a different user
HTTrack3.49-5 launched on Mon, 21 Apr 2025 21:33:53 at http://target.ine.local
(httrack http://target.ine.local -O /root/httmirror -v )

Information, Warnings and Errors reported for this mirror:
note:  the hts-log.txt file, and hts-cache folder, may contain sensitive information,
      such as username/password authentication for websites mirrored in this project
      do not share these files/folders if you want these information to remain private

Mirror launched on Mon, 21 Apr 2025 21:33:53 by HTTrack Website Copier/3.49-5 [XR6C0'2014]
mirroring http://target.ine.local with the wizard help..
21:33:53get.ine.Error: o"Unable to get server's address: Temporary failure in name resolution" (-5) after 2 retries at link target.ine.local/robots.txt (from primary/primary)
21:33:53get.ine.Warning:  bytes)Retry after error -5 (Unable to get server's address: unknown error) at link target.ine.local/ (from primary/primary)
21:33:53get.ine.Warning:  bytes)Retry after error -5 (Unable to get server's address: unknown error) at link target.ine.local/ (from primary/primary)
21:33:53get.ine.Error: ("Unable to get server's address: unknown error" (-5) after 2 retries at link target.ine.local/ (from primary/primary)
21:33:53      Warning:      No data seems to have been transferred during this session! : restoring previous one!
Done.
Thanks for using HTTrack!
```

```
(root@INE)-[~]
# wget --mirror http://target.ine.local
--2025-04-21 21:34:31-- http://target.ine.local/
Resolving target.ine.local (target.ine.local)... 192.237.134.3
Connecting to target.ine.local (target.ine.local)|192.237.134.3|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'target.ine.local/index.html'

target.ine.local/index.html          [=====>] 82.90K --.-KB/s  in 0.001

Last-modified header missing -- time-stamps turned off.
2025-04-21 21:34:31 (87.7 MB/s) - 'target.ine.local/index.html' saved [84892]

Loading robots.txt; please ignore errors.
--2025-04-21 21:34:31-- http://target.ine.local/robots.txt
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 108 [text/plain]
Saving to: 'target.ine.local/robots.txt'

target.ine.local/robots.txt          100%[=====>] 108 --.-KB/s  in 0s

2025-04-21 21:34:31 (20.6 MB/s) - 'target.ine.local/robots.txt' saved [108/108]

--2025-04-21 21:34:31-- http://target.ine.local/index.php/feed/
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 1728 (1.7K) [application/rss+xml]
Saving to: 'target.ine.local/index.php/feed/index.html'

target.ine.local/index.php/feed/index.html 100%[=====>] 1.69K --.-KB/s  in 0s

2025-04-21 21:34:31 (286 MB/s) - 'target.ine.local/index.php/feed/index.html' saved [1728/1728]

--2025-04-21 21:34:31-- http://target.ine.local/index.php/comments/feed/
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 1689 (1.6K) [application/rss+xml]
Saving to: 'target.ine.local/index.php/comments/feed/index.html'

target.ine.local/index.php/comments/feed/index.html 100%[=====>] 1.65K --.-KB/s  in 0s

Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 326628 (319K) [font/woff2]
Saving to: 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/inter/Inter-VariableFont_slnt,wght.woff2'

target.ine.local/wp-content/themes/twentytwentyfour 100%[=====>] 318.97K --.-KB/s  in 0s

2025-04-21 21:34:31 (1.14 GB/s) - 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/inter/Inter-VariableFont_slnt,wght.woff2' saved [326628/326628]

--2025-04-21 21:34:31-- http://target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_400.woff2
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 146060 (143K) [font/woff2]
Saving to: 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_400.woff2'

target.ine.local/wp-content/themes/twentytwentyfour 100%[=====>] 142.64K --.-KB/s  in 0s

2025-04-21 21:34:31 (989 MB/s) - 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_400.woff2' saved [146060/146060]

--2025-04-21 21:34:31-- http://target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_italic_400.woff2
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 105184 (103K) [font/woff2]
Saving to: 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_italic_400.woff2'

target.ine.local/wp-content/themes/twentytwentyfour 100%[=====>] 102.72K --.-KB/s  in 0s

2025-04-21 21:34:31 (1.04 GB/s) - 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_italic_400.woff2' saved [105184/105184]

--2025-04-21 21:34:31-- http://target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_700.woff2
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 132564 (129K) [font/woff2]
Saving to: 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_700.woff2'

target.ine.local/wp-content/themes/twentytwentyfour 100%[=====>] 129.46K --.-KB/s  in 0s

2025-04-21 21:34:31 (774 MB/s) - 'target.ine.local/wp-content/themes/twentytwentyfour/assets/fonts/cardo/cardo_normal_700.woff2' saved [132564/132564]

--2025-04-21 21:34:31-- http://target.ine.local/index.php/sample-page/
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
```



```
File Actions Edit View Help

target.ine.local/index.php/2024/05/27/hello-world/1 [ ⇌ ] 75.36K --.-KB/s in 0.001s

Last-modified header missing -- time-stamps turned off.
2025-04-21 21:34:32 (61.9 MB/s) - 'target.ine.local/index.php/2024/05/27/hello-world/index.html?replytocom=1' saved [77165]

--2025-04-21 21:34:32-- http://target.ine.local/wp-includes/js/comment-reply.min.js?ver=6.5.3
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 2981 (2.9K) [application/javascript]
Saving to: 'target.ine.local/wp-includes/js/comment-reply.min.js?ver=6.5.3'

target.ine.local/wp-includes/js/comment-reply.min.j 100%[=====→] 2.91K --.-KB/s in 0s

2025-04-21 21:34:32 (492 MB/s) - 'target.ine.local/wp-includes/js/comment-reply.min.js?ver=6.5.3' saved [2981/2981]

--2025-04-21 21:34:32-- http://target.ine.local/index.php/author/admin/feed/
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 1755 (1.7K) [application/rss+xml]
Saving to: 'target.ine.local/index.php/author/admin/feed/index.html'

target.ine.local/index.php/author/admin/feed/index. 100%[=====→] 1.71K --.-KB/s in 0s

2025-04-21 21:34:32 (322 MB/s) - 'target.ine.local/index.php/author/admin/feed/index.html' saved [1755/1755]

--2025-04-21 21:34:32-- http://target.ine.local/index.php/wp-json/wp/v2/users/1
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 621 [application/json]
Saving to: 'target.ine.local/index.php/wp-json/wp/v2/users/1'

target.ine.local/index.php/wp-json/wp/v2/users/1 100%[=====→] 621 --.-KB/s in 0s

Last-modified header missing -- time-stamps turned off.
2025-04-21 21:34:32 (112 MB/s) - 'target.ine.local/index.php/wp-json/wp/v2/users/1' saved [621/621]

FINISHED --2025-04-21 21:34:32--
Total wall clock time: 0.6s
Downloaded: 34 files, 1.8M in 0.01s (178 MB/s)

(root@INE)~#
```

## Výsledok:

→ Zrkadlený: **target.ine.local/index.php/wp-json/wp/v2/users/1**

→ WordPress REST API, z ktorého vieme získať usernames

→ tak by sme vedeli aj zistiť admin účet pre budúci BruteForce útok

Tu som skontroloval obsah súboru **users/1** cez príkaz:

**cat target.ine.local/index.php/wp-json/wp/v2/users/1**

```
(root@INE)~# cat target.ine.local/index.php/wp-json/wp/v2/users/1
{"id":1,"name":"admin","url":"http://target.ine.local","description":"","link":"http://target.ine.local/index.php/author/admin/","slug":"admin","avatar_urls":{"24":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=24&mm6r=g","48":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=48&mm6r=g","96":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=96&mm6r=g"},"meta":{"_links":{"self":[{"href":"http://target.ine.local/index.php/wp-json/wp/v2/users/1"}],"collection":[{"href":"http://target.ine.local/index.php/wp-json/wp/v2/users"}]}}
```

Výsledok príkazu:

→ „slug“: admin

A teraz už iba stačí:

**echo -n „admin“ | md5sum**

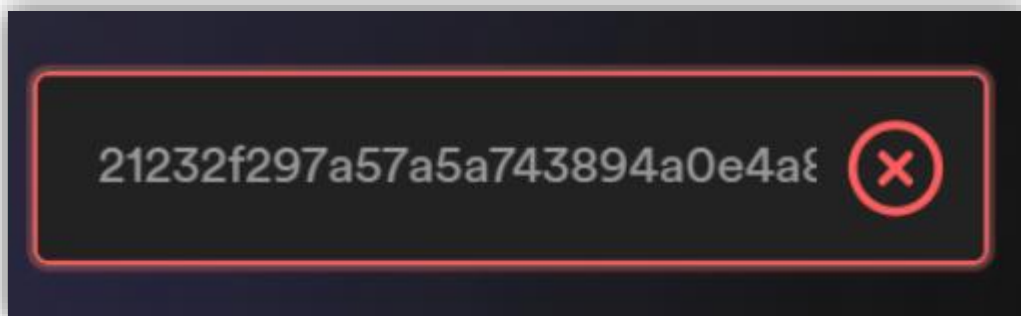
```
File Actions Edit View Help
Saving to: 'target.ine.local/wp-includes/js/comment-reply.min.js?ver=6.5.3'
target.ine.local/wp-includes/js/comment-reply.min.j 100%[=====] 2.91K --KB/s in 0s
2025-04-21 21:34:32 (492 MB/s) - 'target.ine.local/wp-includes/js/comment-reply.min.js?ver=6.5.3' saved [2981/2981]
--2025-04-21 21:34:32-- http://target.ine.local/index.php/author/admin/feed/
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 1755 (1.7K) [application/rss+xml]
Saving to: 'target.ine.local/index.php/author/admin/feed/index.html'
target.ine.local/index.php/author/admin/feed/index. 100%[=====] 1.71K --KB/s in 0s
2025-04-21 21:34:32 (322 MB/s) - 'target.ine.local/index.php/author/admin/feed/index.html' saved [1755/1755]
--2025-04-21 21:34:32-- http://target.ine.local/index.php/wp-json/wp/v2/users/1
Reusing existing connection to target.ine.local:80.
HTTP request sent, awaiting response... 200 OK
Length: 621 [application/json]
Saving to: 'target.ine.local/index.php/wp-json/wp/v2/users/1'
target.ine.local/index.php/wp-json/wp/v2/users/1 100%[=====] 621 --KB/s in 0s
Last-modified header missing -- time-stamps turned off.
2025-04-21 21:34:32 (112 MB/s) - 'target.ine.local/index.php/wp-json/wp/v2/users/1' saved [621/621]
FINISHED --2025-04-21 21:34:32--
Total wall clock time: 0.6s
Downloaded: 34 files, 1.8M in 0.01s (178 MB/s)

(root@INE)-[~]
$ cat target.ine.local/index.php/wp-json/wp/v2/users/1
{"id":1,"name":"admin","url":"http://target.ine.local","description":"","link":"http://target.ine.local/index.php/author/admin/","slug":"admin","avatar_urls":{"24":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=24&mm6r=g","48":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=48&mm6r=g","96":"http://0.gravatar.com/avatar/6b2413e8b8acc4cf371be562057ad94c?s=96&mm6r=g"},"meta":[],"_links":{"self":[{"href":"http://target.ine.local/index.php/wp-json/wp/v2/users/1"}],"collection":[{"href":"http://target.ine.local/index.php/wp-json/wp/v2/users"}]}}
(root@INE)-[~]
$ echo -n "admin" | md5sum
21232f297a57a5a743894a0e4a801fc3 -

(root@INE)-[~]
```

Výsledok:

→ HASH: 21232f297a57a5a743894a0e4a801fc3



Ups, oni nehashujú iba admina, ale celý jeho obsah... čiže nesprávny hash... okej, skúsím ešte niečo:


**grep -ir FLAG5 target.ine.local:**

```
(root@INE)-[~]
# grep -ir FLAG5 target.ine.local
target.ine.local/xmlrpc.php:rsd: <api name="FLAG5{55574431357347bb84d13db2ddea9328}" blogID="1" preferred="false" apiLink="http://target.ine.local/xmlrpc.php" />

(root@INE)-[~]
```


BUM! Máme **FLAG5{55574431357347bb843db2ddea9328}**

→ Našli sme ho v súbore xmlrpc.php cez grep, kde sa objavil priamo v API tagu




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.



Certain files may reveal something interesting when mirrored.

Flag captured

## **Záver:**

- Niektoré FLAGS boli detegované cez GET požiadavky, iné cez priečinky alebo JSON API
- Chyby ako 403 boli zaznamenané, ale považujem ich za dôveryhodné záložné súbory
- grep a md5sum pomohli identifikovať & zahashovať obsah tam, kde nebolo jasné riešenie

Tento report bol vytvorený v rámci eJPT prípravy ako praktické precvičenie info gathering fázy. Cieľom bolo demonštrovať schopnosť logicky uvažovať, použiť viacero nástrojov a adaptovať sa pri problémoch v reálnom labovom prostredí.