

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

Tool used: Kali-Linux, Firefox

Solution/walkthrough:

Question 1

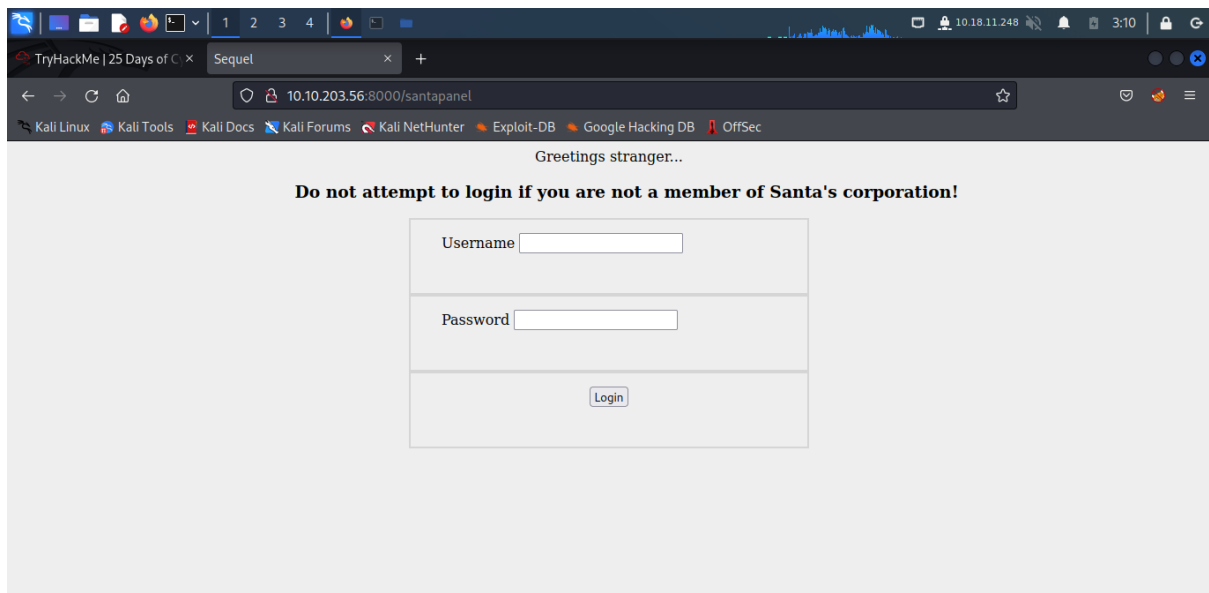
port 1433

If enabled, the default instance of the SQL Server Database Engine listens on **TCP port 1433**. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports.

11 Mar 2022

Research and find the answer.

Question 2

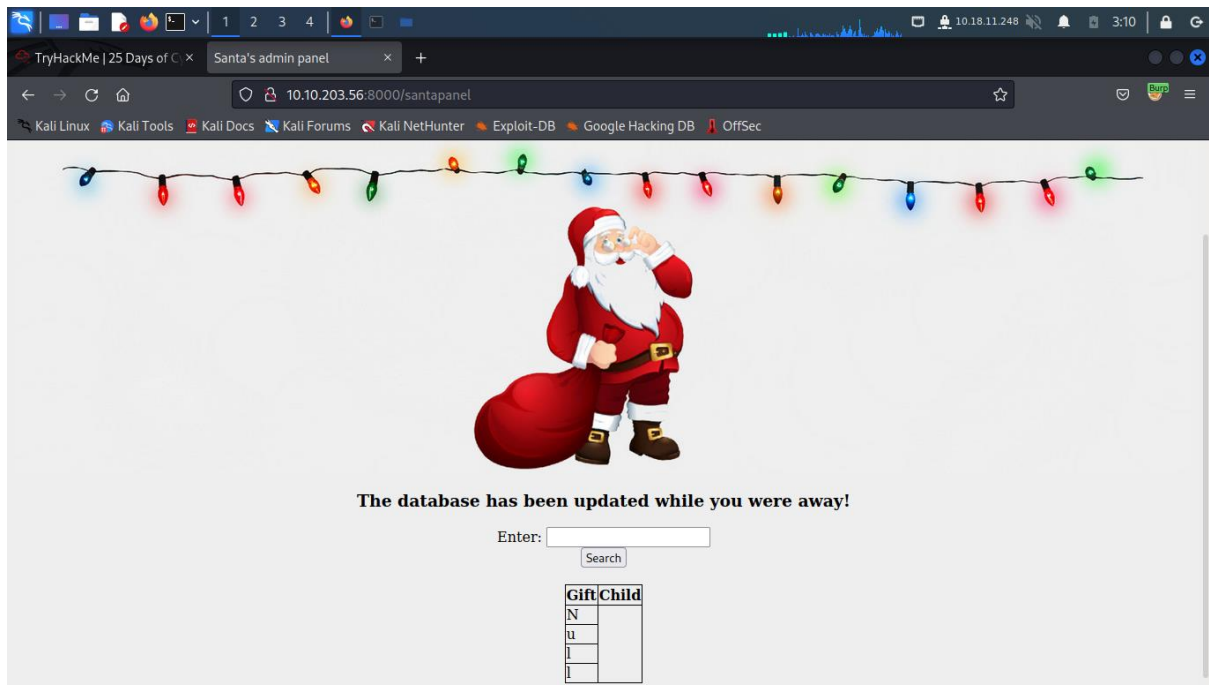


Random guessing.

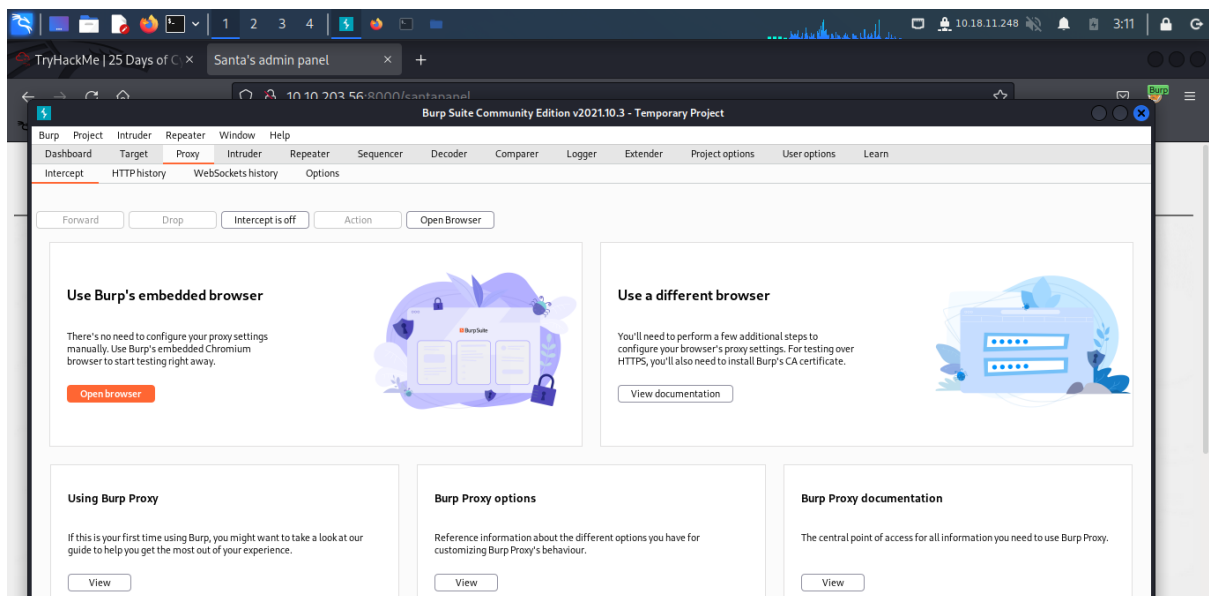
Question 3

Santa TODO: Look at alternative database systems that are than sqlite.

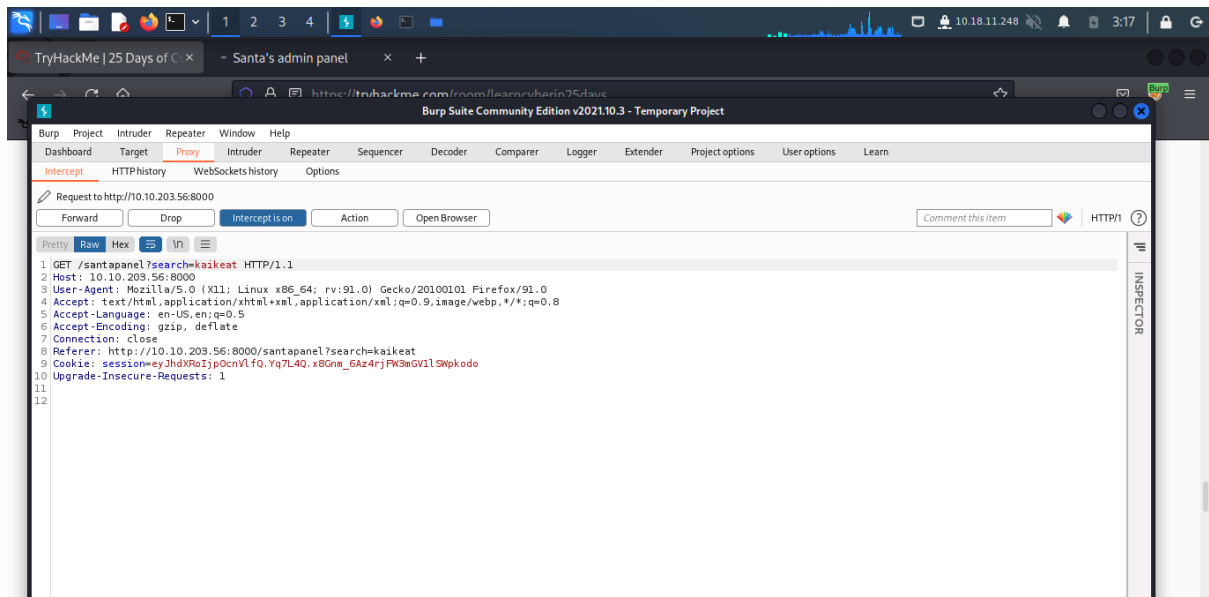
Question 4, 5, 6, 7, 8



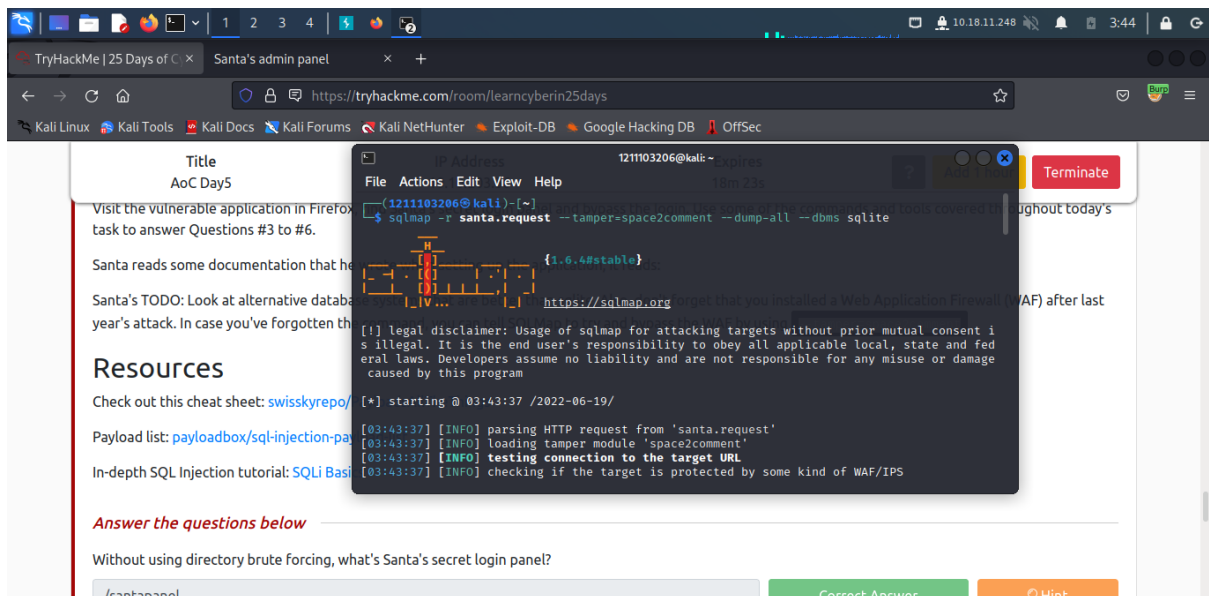
Bypass the login using SQLi.



After login, active the foxyproxy and open burp suite. Then, put an input for it. The burp suite will send a request.



Right click and save item.



The saved item is named santa.request.

```
File Actions Edit View Help
+-----+
| flag   |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+

[03:44:37] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/121110320
6/.local/share/sqlmap/output/10.10.203.56/dump/SQLite_masterdb/hidden_table.csv'
[03:44:37] [INFO] fetching columns for table 'sequels'
[03:44:37] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
+-----+-----+-----+
| kid   | age | title                |
+-----+-----+-----+
| James | 8   | shoes                |
| John  | 4   | skateboard           |
| Robert| 17  | iphone               |
| Michael| 5   | playstation          |
| William| 6   | xbox                 |
| David | 6   | candy                |
| Richard| 9   | books                |
| Joseph| 7   | socks                |
| Thomas| 10  | 10 McDonalds meals  |
| Charles| 3   | toy car              |
| Christopher| 8 | air hockey table     |
| Daniel| 12  | lego star wars       |
| Matthew| 15  | bike                 |
| Anthony| 3   | table tennis         |
| Donald| 4   | fazer chocolate      |
| Mark  | 17  | wii                  |
| Paul  | 9   | github ownership     |
| James | 8   | finnish-english dictionary |
| Steven| 11  | laptop               |
+-----+-----+-----+

The database has been updated while you were away!

Enter: name
Search
[03:44:37]
```

4) 22 entries

5) James' age = 8

6) Paul ask for github ownership

7) The flag is shown. thmfox{All_I_Want_for_Christmas_Is_You}

8) admin password = EhCNSWzzFP6sc7gB