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

Tool used: Kali-Linux, Firefox

Solution/walkthrough:

Question 1

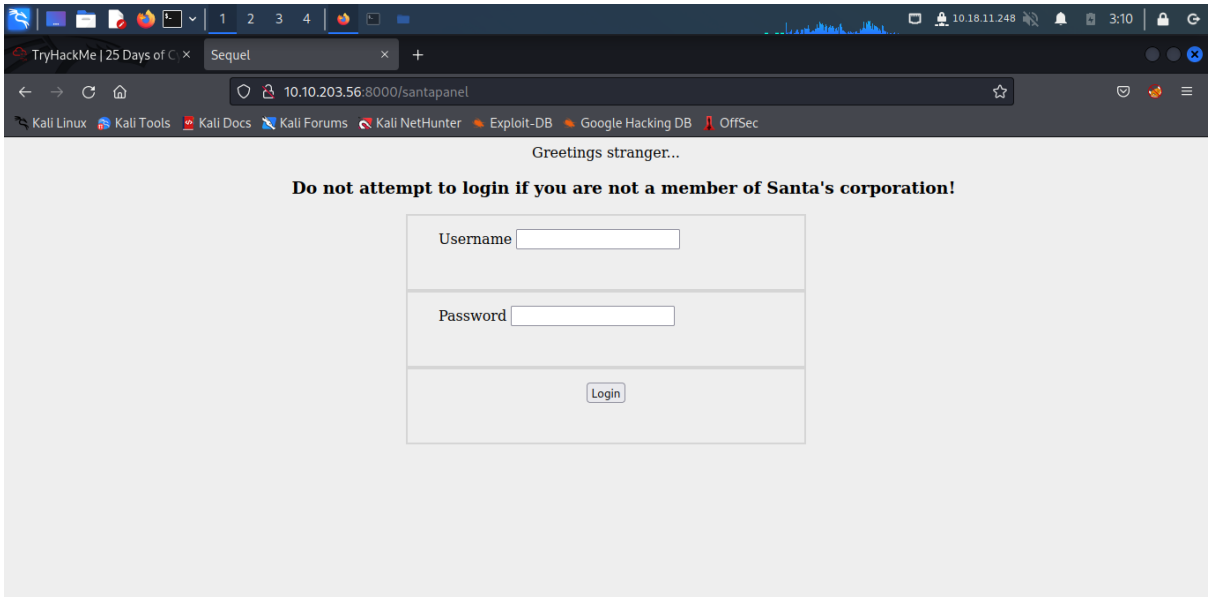
port 1433

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

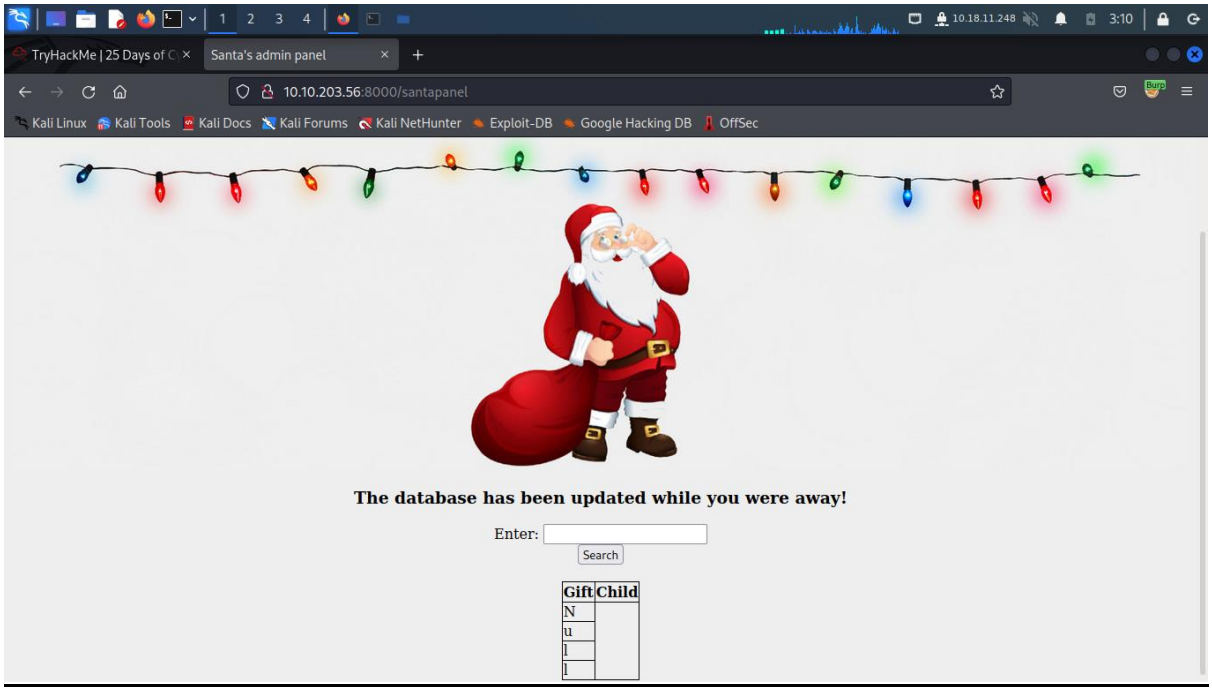


Random guessing.

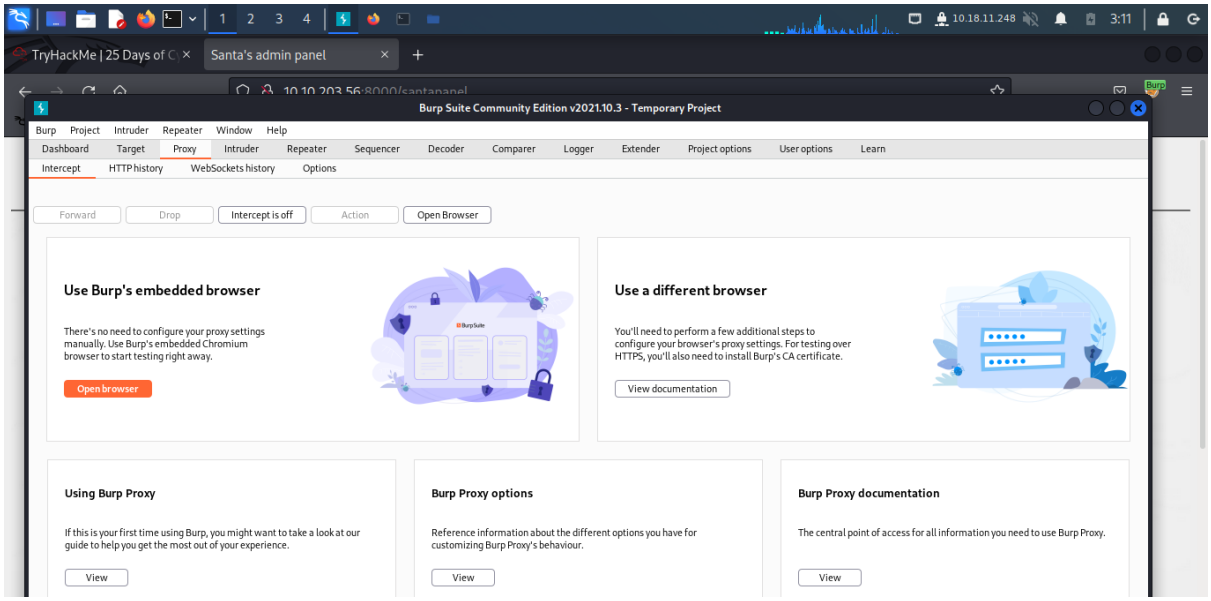
Question 3

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

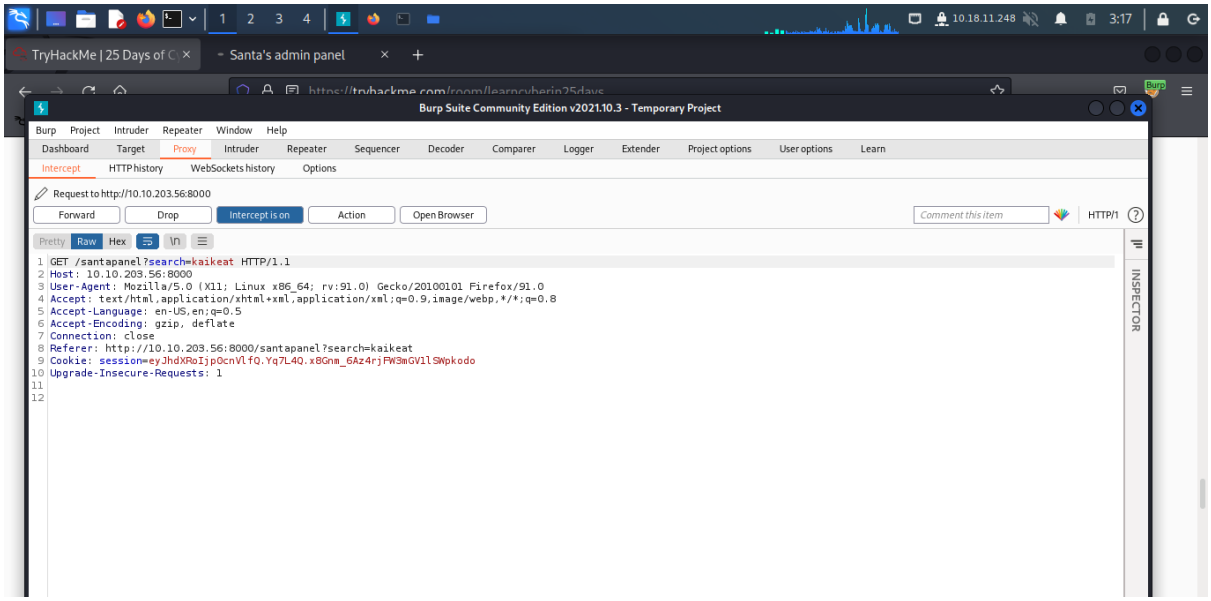
Question 4, 5, 6, 7, 8



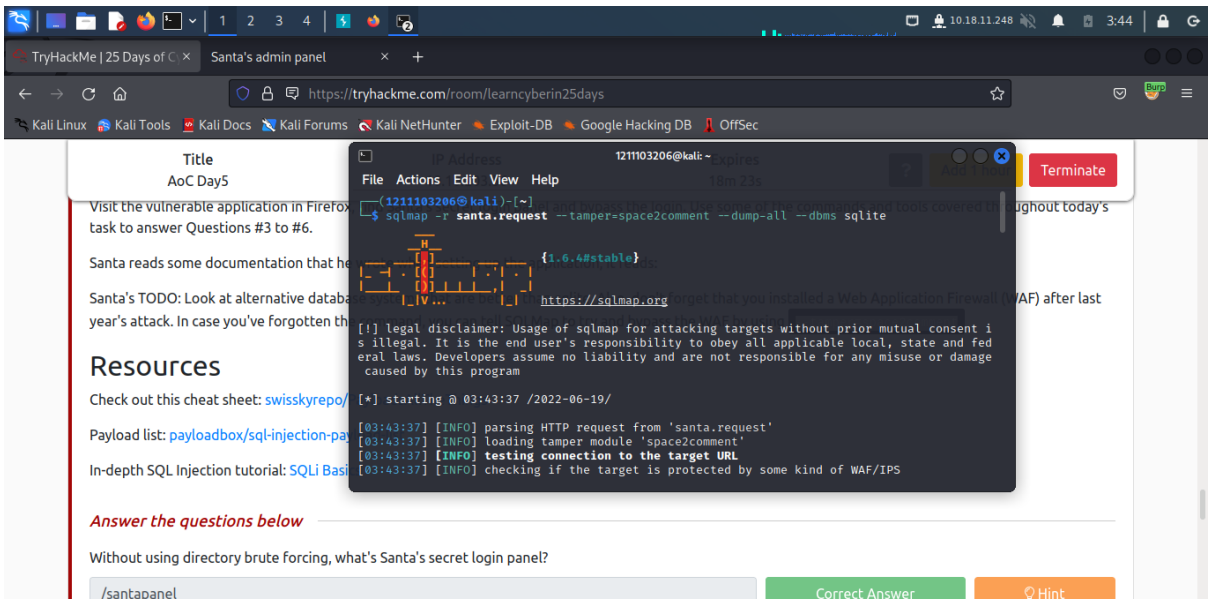
Bypass the login using SQLI.



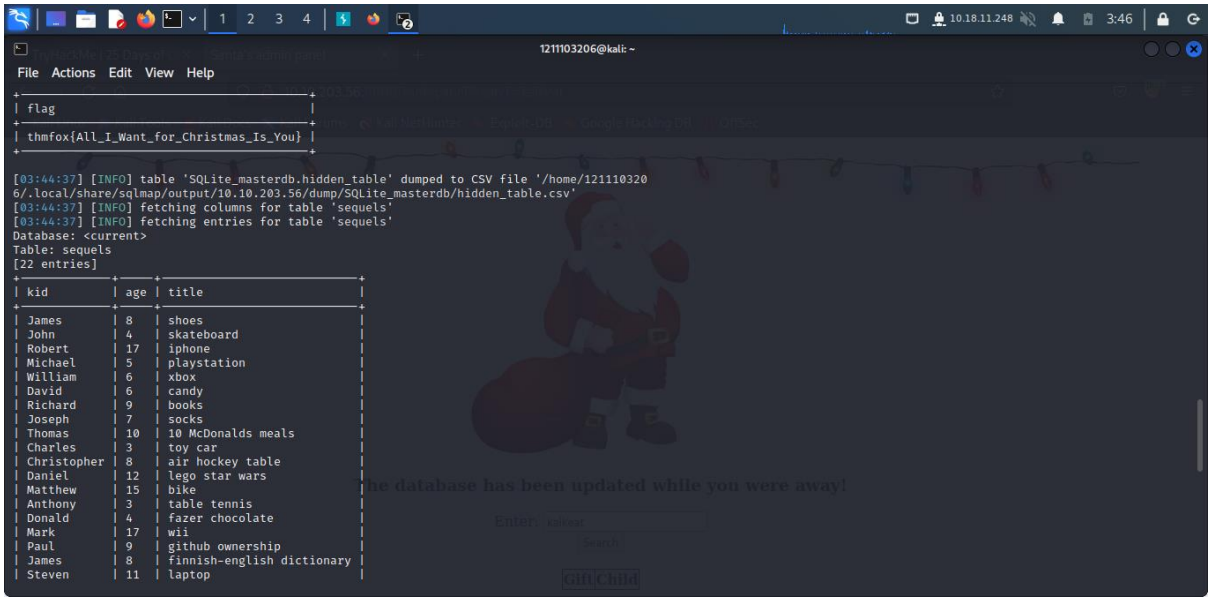
After login, active the foxyproxy and open burp suite. Then, put an input for it. The burp suite will send a request.



Right click and save item.



The saved item is named santa.request.



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