PROJECT REPORT ON

"INTRODUCTION TO CYBER SECURITY"

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

TOPICS:

Hacking Wireless Networks

Hacking Web Servers

Hacking Web Applications

SQL Injection

Submitted By-

Vivek Arora-101715178

Sudhanshu Mahajan-101706171

Suman Saurav -101706173

Suneet Gupta-101706176

Submitted To-

Ms. Swati Kumari

HACKING WIRELESS NETWORKS

AIM - Disconnecting a device from a network using Aircrack-ng

OS USED – Ubuntu

THEORY-

Hacking Wireless Network-

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

Wireless networks have some excellent advantages like connectivity beyond walls, wireless connection, easy to access internet even in areas where laying cables is difficult, speed and sharing. But, wireless networks have a few disadvantages, the major issue being- the questionable security.

Important Terms:-

1. **Access Point**: The point where the mobile device, computers connect to the wireless network.
2. **SSID**: Service Set Identifier identifies the access point, it is a human-readable text which when broadcasted leads to the identification of an access point.
3. **BSSID:** Mac address of the Access point.
4. **Bandwidth**: Amount of information that can be transferred over the connection.

SOFTWARES / WEB APPLICATIONS USED –

1. Aircrack-ng

Aircrack-ng is a complete suite of tools to assess WiFi network security.Aircrack-ng is a fork of the original Aircrack project. It can be found as a preinstalled tool in many Linux distributions such as Kali Linux or Parrot, which share common attributes as they are developed under the same project.

It focuses on different areas of WiFi security:

1. Monitoring: Packet capture and export of data to text files for further processing by third party tools
2. Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
3. Testing: Checking WiFi cards and driver capabilities (capture and injection)
4. Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are a command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris ,etc.

PROCEDURE/EXPLANATION-

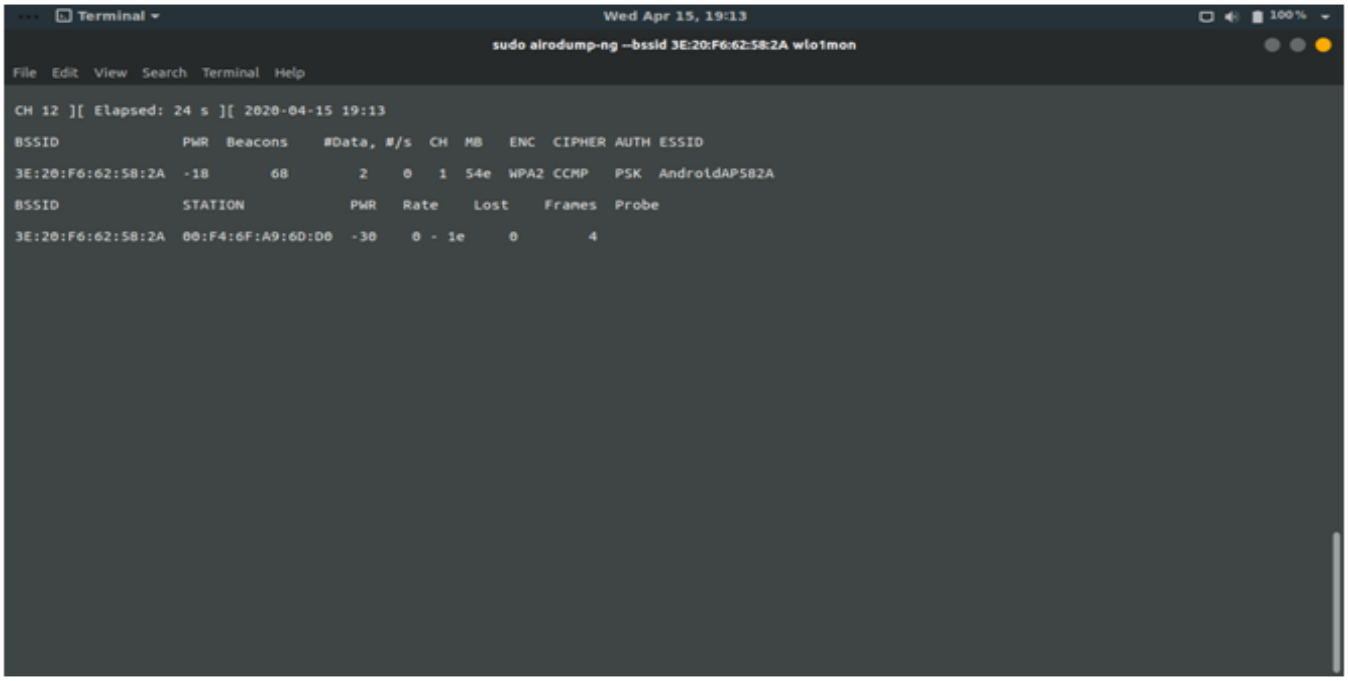
In this experiment, I have used aircrack-ng to lock a phone out of a wireless network .

In first pic we have used command "**sudo airodump-ng wlo1mon**" to look for all the wireless devices around me in first pic .We were able to see the wireless host "**ANDROIDAP 582A"** and also a device connected to it which is a phone.

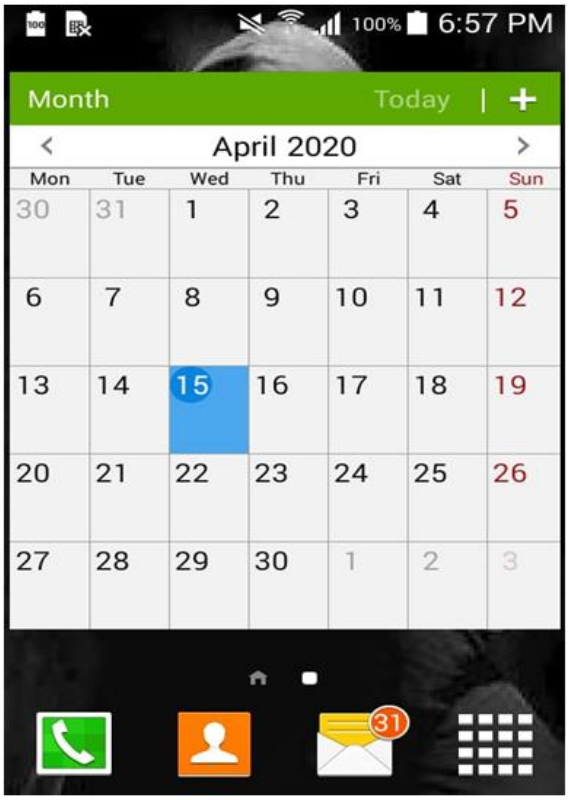
We were able to see the mac addresses of both the device which is sending hotspot signals and that of the phone .

We used those mac addresses in second command which you can see in the third pic to send deauth signal to the phone 2000 times which resulted in the phone disconnecting to the wifi.

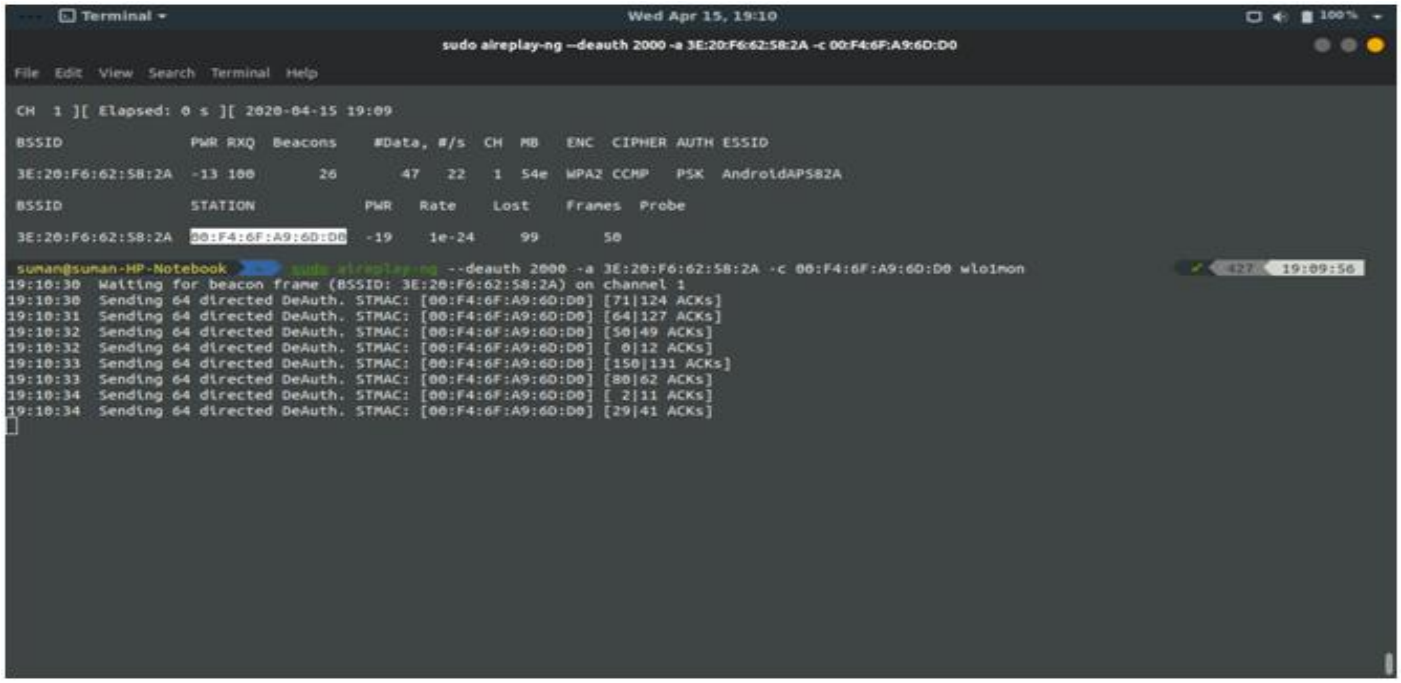
OUTPUT/SCREENSHOTS-



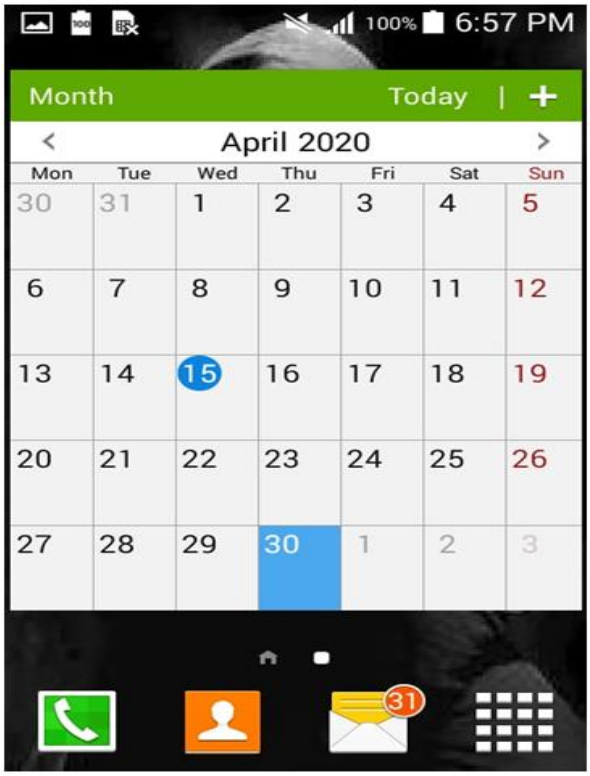
We used the command "**sudo airodump-ng wlo1mon"** to look for all the wireless devices around us**.** We saw the wireless host "**ANDROIDAP 582A"** and also a device connected to it which is a phone. We also saw the MAC addresses of both devices.



This is Device "**See the Wi-Fi Signals-Network Connected**"



Here we are Sending the deauth signals 2000 times to the device using command "**sudo aireplay -ng -- deauth 2000 -a (ssid) -c (mac address of the device)**".



See the device "**No Wi-Fi Signal - Network Disconnected** "

RESULT-

We understood how to hack wireless networks. We were able to disconnect a device from a network using Aircrack-ng.

HACKING WEB SERVERS

AIM- To get the webserver footprint.

OS USED- Ubuntu (Linux)

SOFTWARE USED- Zen-map

WEBSITE SCANNED- scanme.nmap.org

THEORY-

Footprinting-

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.
It allows a hacker to gain information about the target system or network. This information can be used to carry out attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed in order to get a complete and successful resolution of the attack. Footprinting is also used by ethical hackers and penetration testers to find security flaws and vulnerabilities within their own company's network before a malicious hacker does.

Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain

access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

Zenmap-

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

PROCEDURE/EXPLANATION-

We used intensive scanning to scan the website scanme.nmap.org.
You can see in both pictures (both are of same scan) the ports of servers, the os used by them, the name of severs, tcp sequence , ip address , etc.

OUTPUT/SCREENSHOTS-

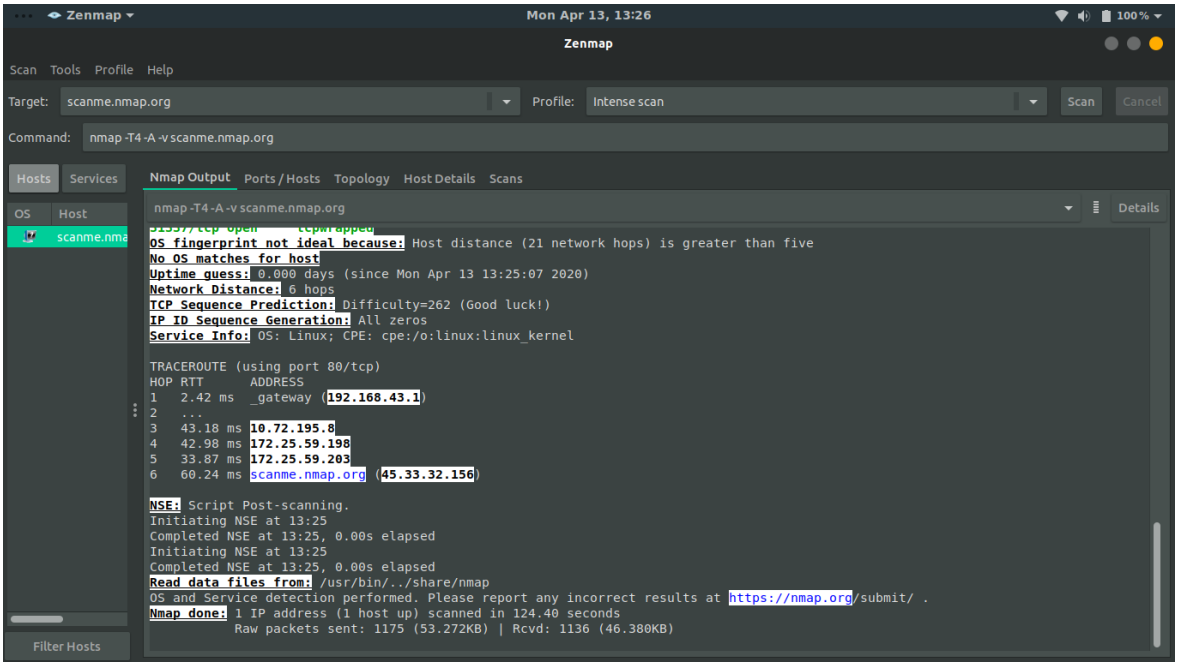


Fig: Details of servers

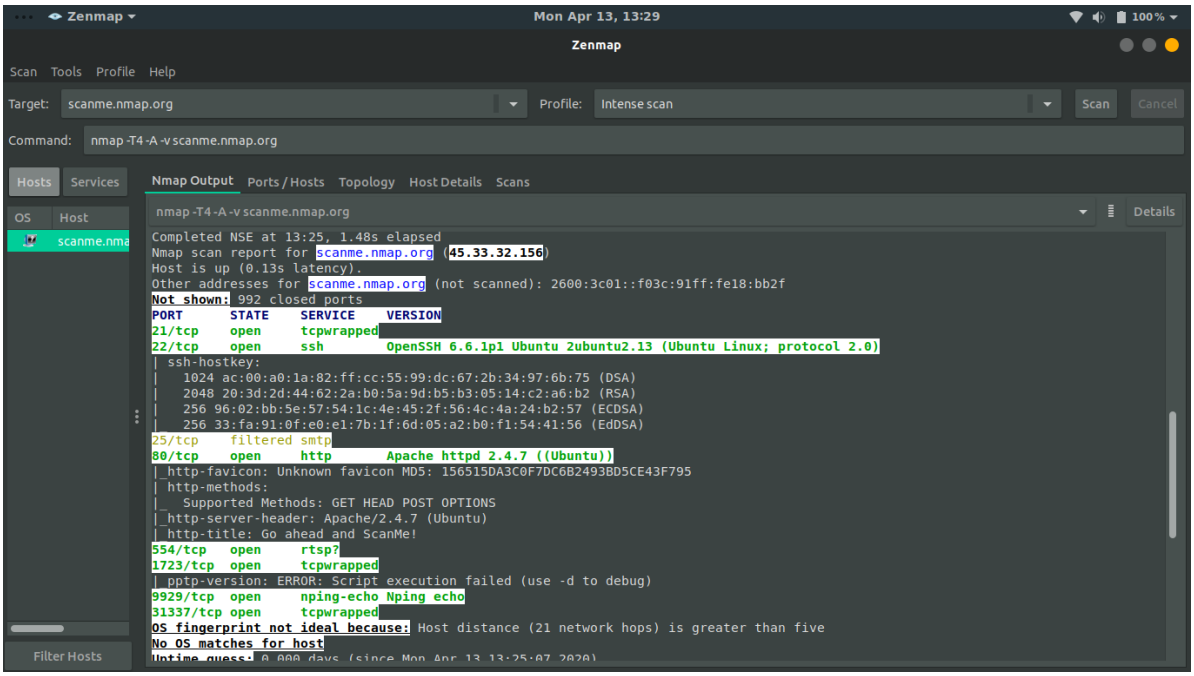


Fig: Details of servers

RESULT- We understood how footprinting is very useful for web server hacking. We got to know about the ports of servers, the os used by them, the name of severs, tcp sequence, ip address, etc.

HACKING WEB APPLICATIONS

AIM- To execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

OS USED- Ubuntu (Linux)

Web-App Used- bWAPP

THEORY-

Cross-site Scripting-

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Types of Cross-Site Scripting:

- Server XSS
- Client XSS

Server XSS

Server XSS occurs when untrusted user supplied data is included in an HTML response generated by the server. The source of this data could be from the request, or from a stored location. As such, you can have both Reflected Server XSS and Stored Server XSS.

In this case, the entire vulnerability is in server-side code, and the browser is simply rendering the response and executing any valid script embedded in it.

Client XSS

Client XSS occurs when untrusted user supplied data is used to update the DOM with an unsafe JavaScript call. A JavaScript call is considered unsafe if it can be used to introduce valid JavaScript into the DOM. This source of this data could be from the DOM, or it could have been sent by the server (via an AJAX call, or a page load). The ultimate source of the data could have been from a request, or from a stored location on the client or the server. As such, you can have both Reflected Client XSS and Stored Client XSS.

Buggy Web App (bWAPP)-

Buggy web application (bWAPP) is a free and open source deliberately insecure web application. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with

WAMP / XAMPP or download the *bee-box*, a custom Linux VM pre-installed with bWAPP.

It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. It has over 100 web vulnerabilities that make it so unique.It covers all major known web bugs, including all risks from the OWASP Top 10 project.

PROCEDURE/EXPLANATION-

(Experment-I)

We searched a name using the form provided by website.

Then, we changed the querry string and after changing it, we were able to change the search results without even searching.

OUTPUT/SCREENSHOTS-

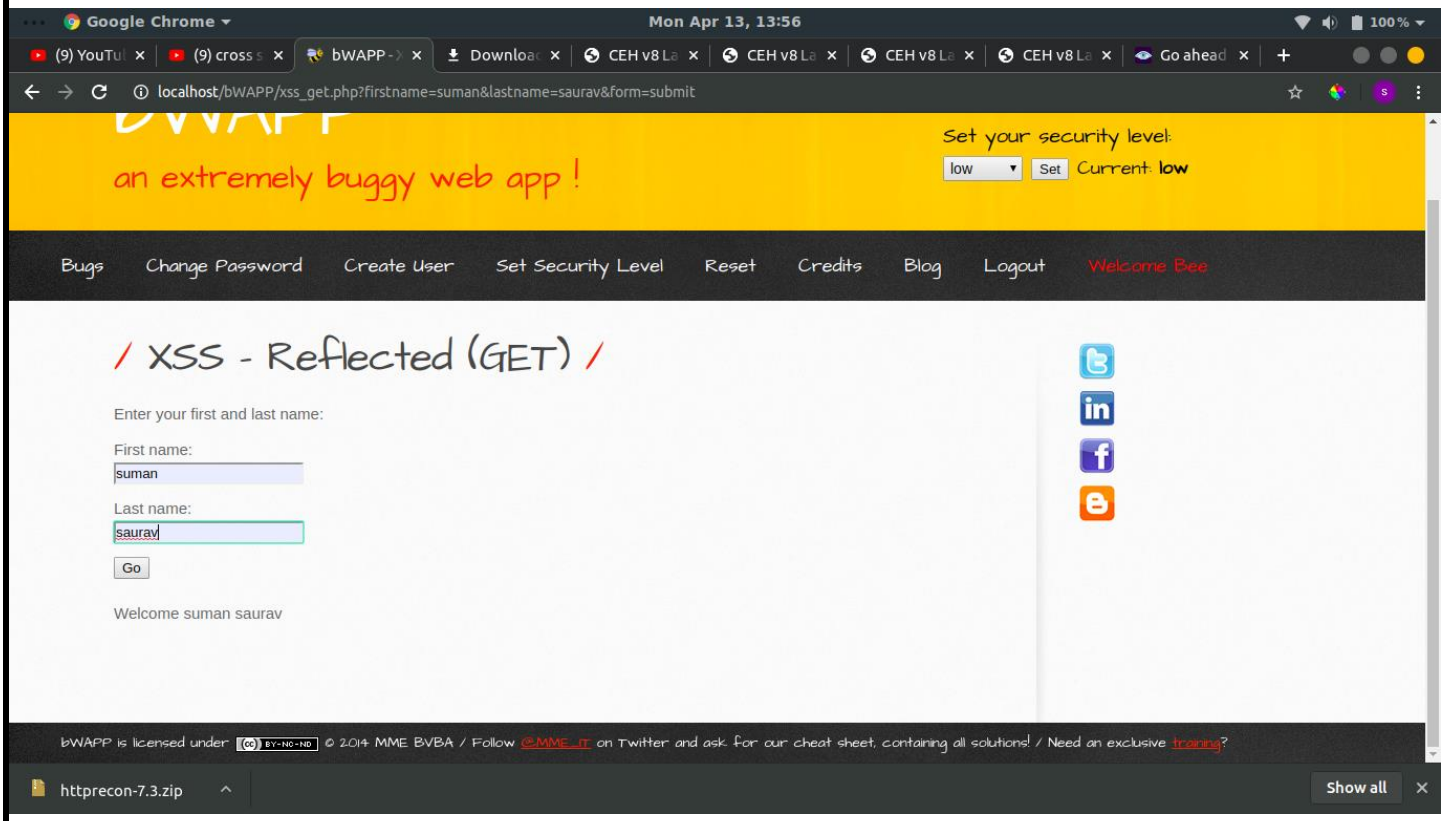


Fig: Searching a Name

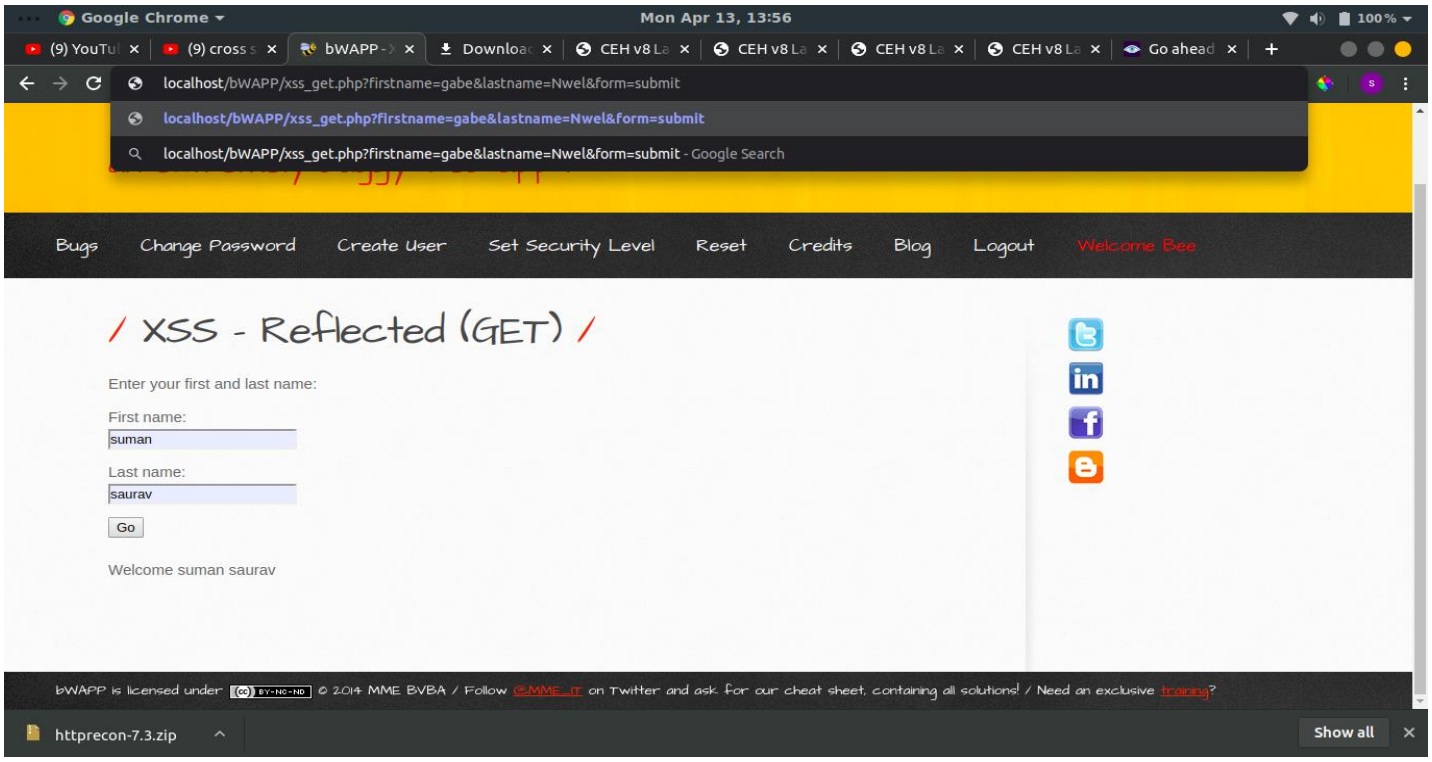


Fig: Changing the query string

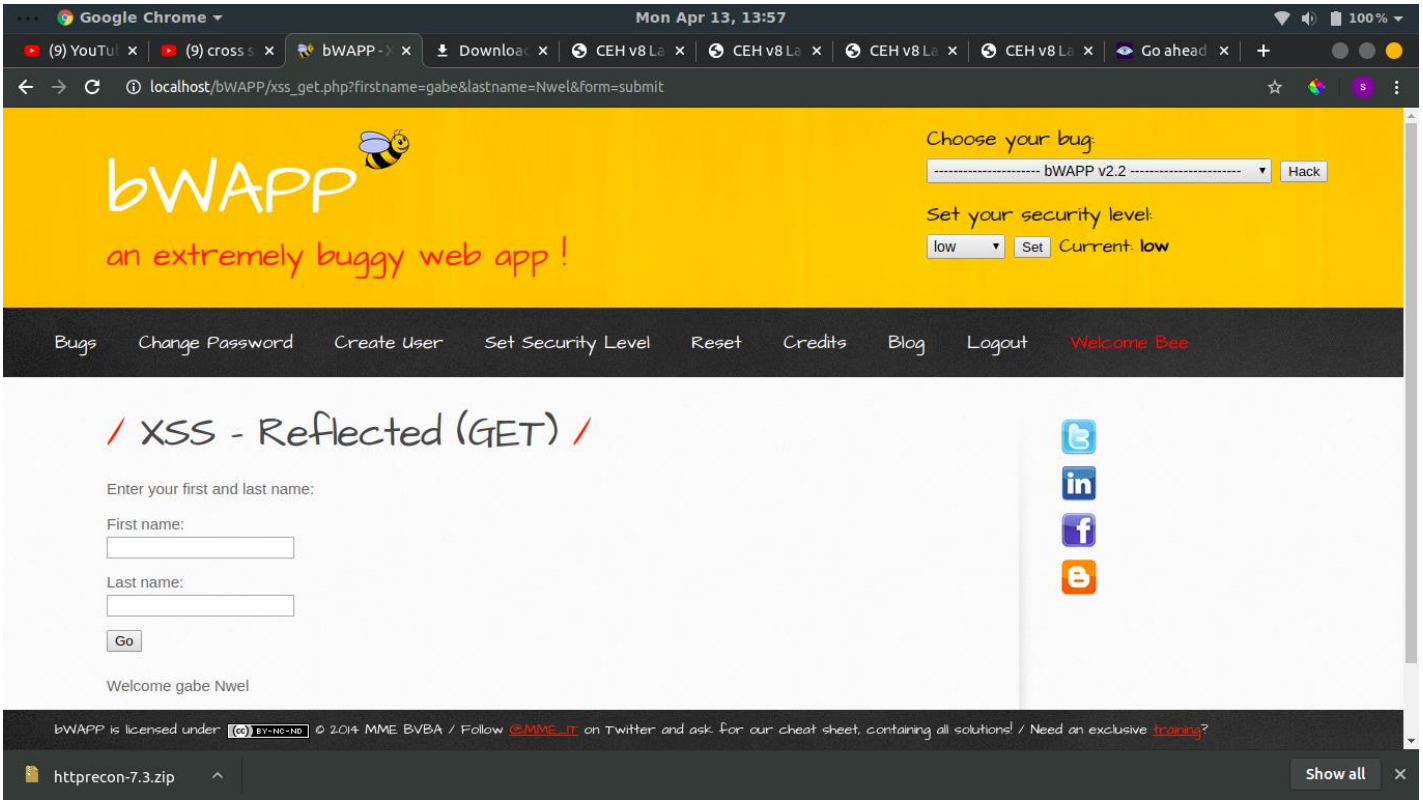


Fig: Changing the search results without even searching

(Experment-II)

Instead of giving simple string to the search, we have given a script tag. When we submitted that form website gave me an alert.

OUTPUT/SCREENSHOTS-

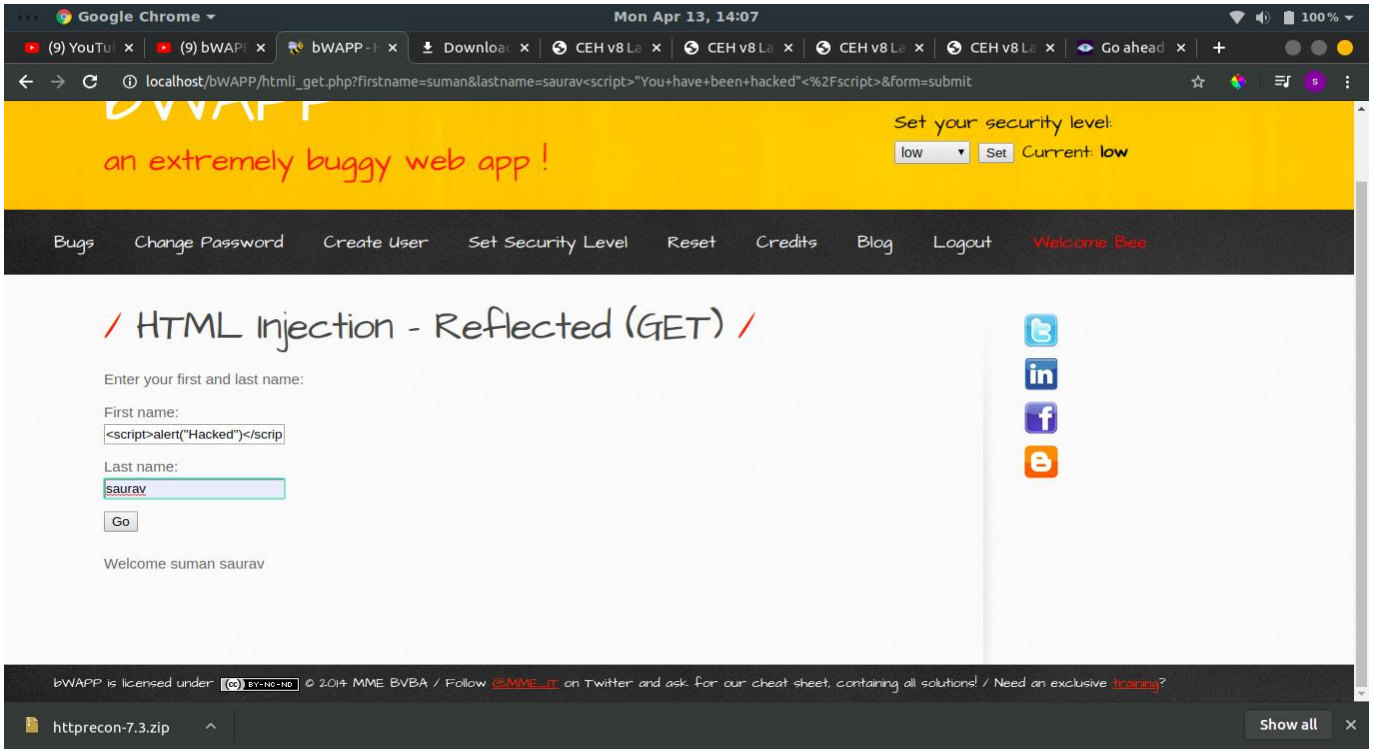


Fig: Giving simple string to search

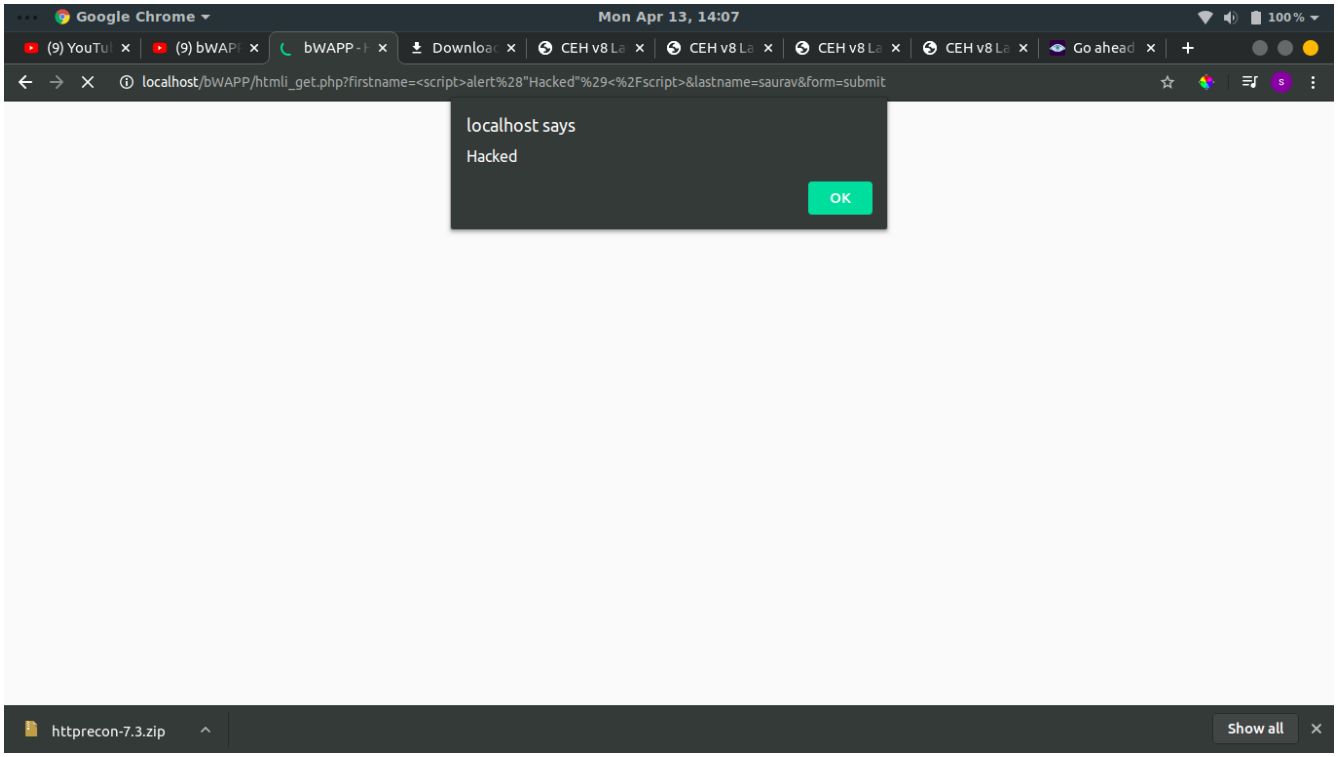


Fig: Website gave an alert

RESULT- We understood how cross-site scripting is very useful for web app hacking. We can change the search results without even searching. When we gave a simple string to the search, the website gave us an alert.

SQL INJECTION

AIM - (1) Log on without valid credentials

(2) Create a user account using a SQL injection query.

OS USED – Ubuntu (Linux)

THEORY-

SQL INJECTION-

SQL injection is a code injection technique that might destroy your database . It is one of the most common web hacking techniques.

It is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application's web server by malicious users.SQL injection is the placement of malicious code in SQL statements, via web page input.

Exploitation of SQL Injection in Web Applications

Web servers communicate with database servers anytime they need to retrieve or store user data. SQL statements by the attacker are designed so that they can be executed while the web-server is fetching content from the application server. It compromises the security of a web application.

SOFTWARES / WEB APPLICATIONS USED –

1.Buggy Web App (bWAPP)-

Buggy web application (bWAPP) is a free and open source deliberately insecure web application. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with WAMP / XAMPP or download the *bee-box*, a custom Linux VM pre-installed with bWAPP.

It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. It has over 100 web vulnerabilities that make it so unique.It covers all major known web bugs, including all risks from the OWASP Top 10 project.

2.phpMyAdmin-

phpMyAdmin is a free software tool written in PHP, intended to handle the administration of MySQL over the Web. phpMyAdmin supports a wide range of operations on MySQL and MariaDB. Frequently used operations (managing databases, tables, columns, relations, indexes, users, permissions, etc) can be performed via the user interface, while you still have the ability to directly execute any SQL statement.

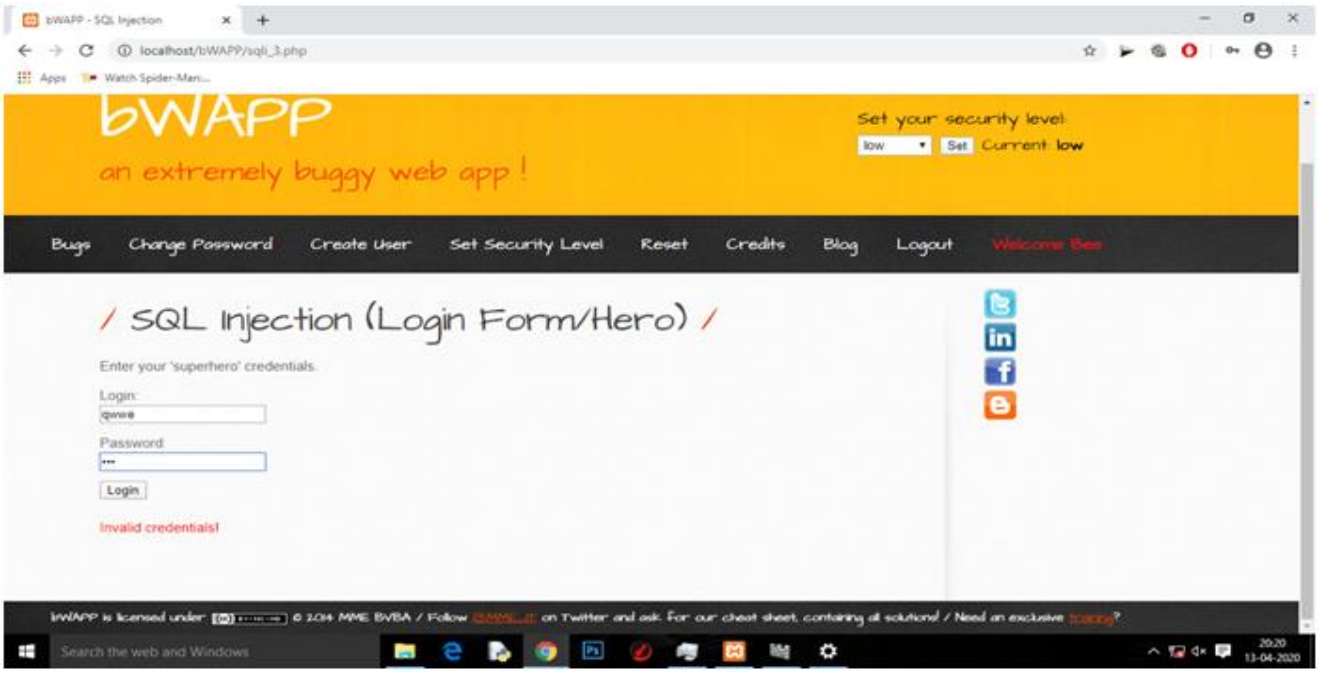
Major features of phpMyAdmin are that it has a very Intuitive web interface and it . Support for most MySQL features like browse and drop databases, tables, views, fields and indexes and create, copy, drop, rename and alter databases, tables, fields and indexes , maintenance server, databases and tables, with proposals on server configuration. Other features like you can create graphics of your database layout in various formats and Importing data from CSV and SQL and Exporting the data to various formats such as CSV, SQL, XML, PDF, etc is easily possible .You can also create complex queries using Query-by-example (QBE).

(1) Log in without valid credentials

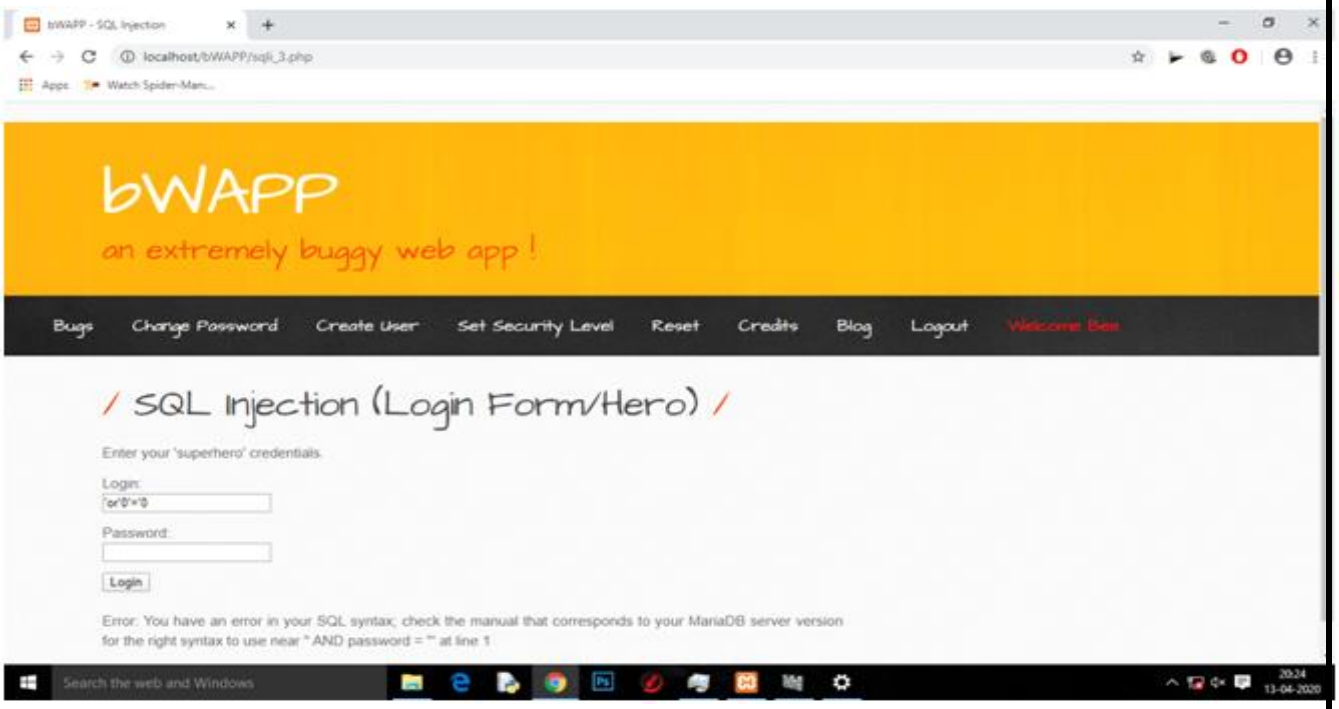
PROCEDURE/EXPLANATION-

Firstly we tried to login using wrong credentials and as you can see that website didn't allow us to do so. So, in the next attempt we entered A SQL QUERY (whose value is always true) in the form instead of a normal string and the website interpreted it as true and we were able to login to someone's account (which you can see in output picture three).

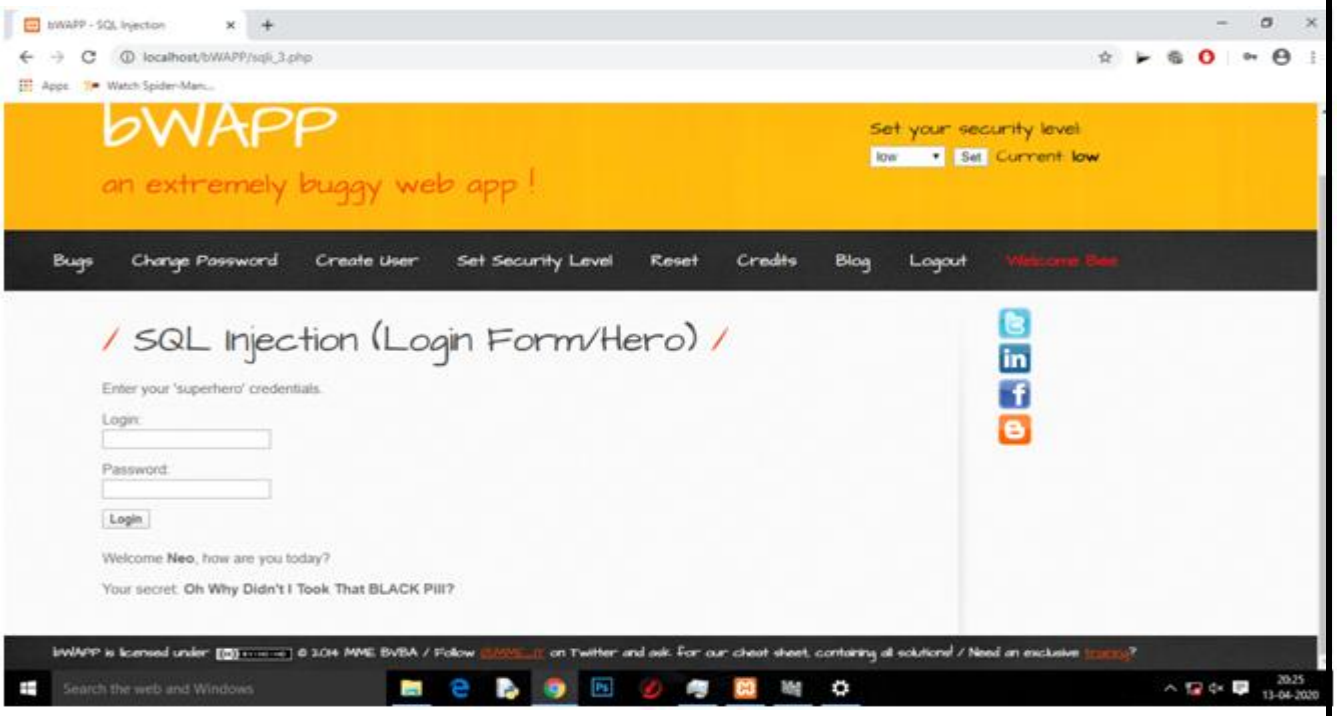
OUTPUT/SCREENSHOTS-



First Attempt - As you can see,Website didn't allowed us to login because we tried to login using wrong credentials .



Second Attempt- We Entered a SQL query whose value is always true in the form instead of normal string and website interpreted it as true.



Logged In- As we used a SQL query in the previous case so we were able to log in ,as you can see the “Welcome Bee” in nav-bar .

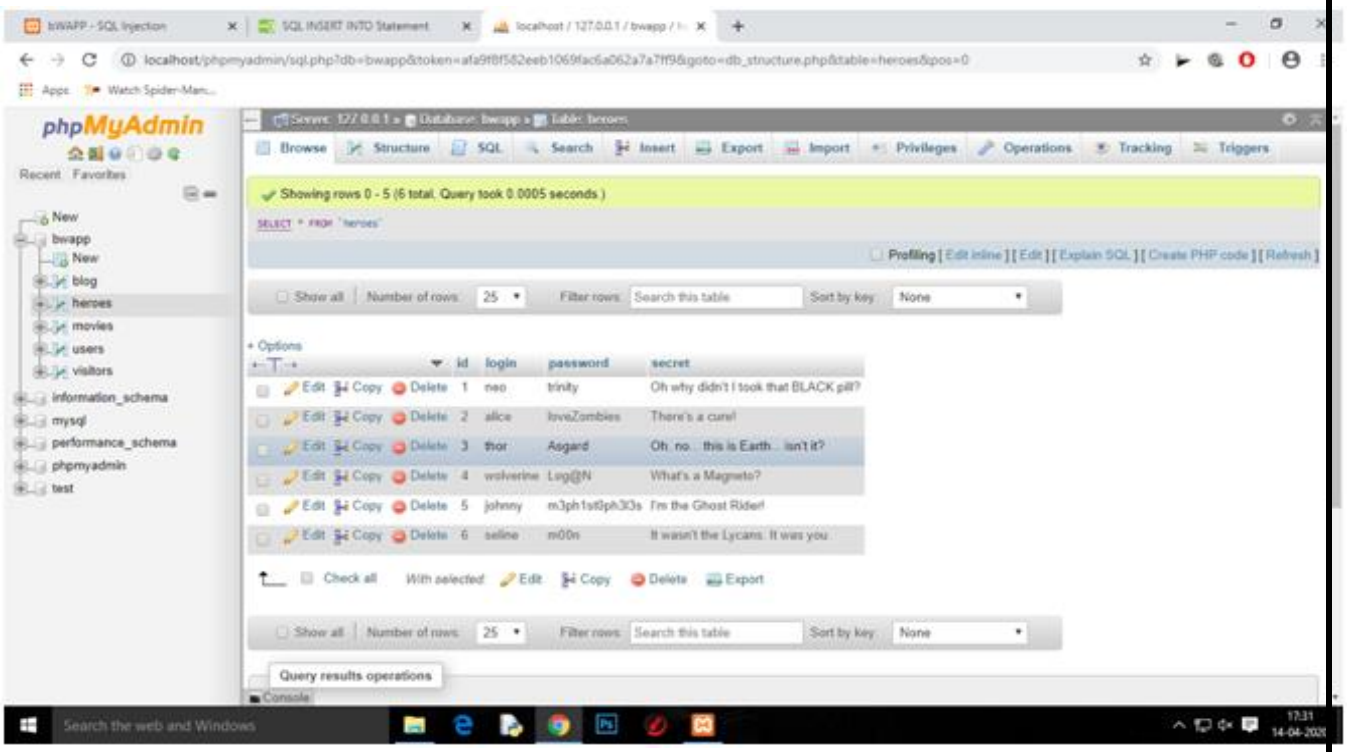
(2) Creating a user account using a SQL injection query.

PROCEDURE/EXPLANATION:-

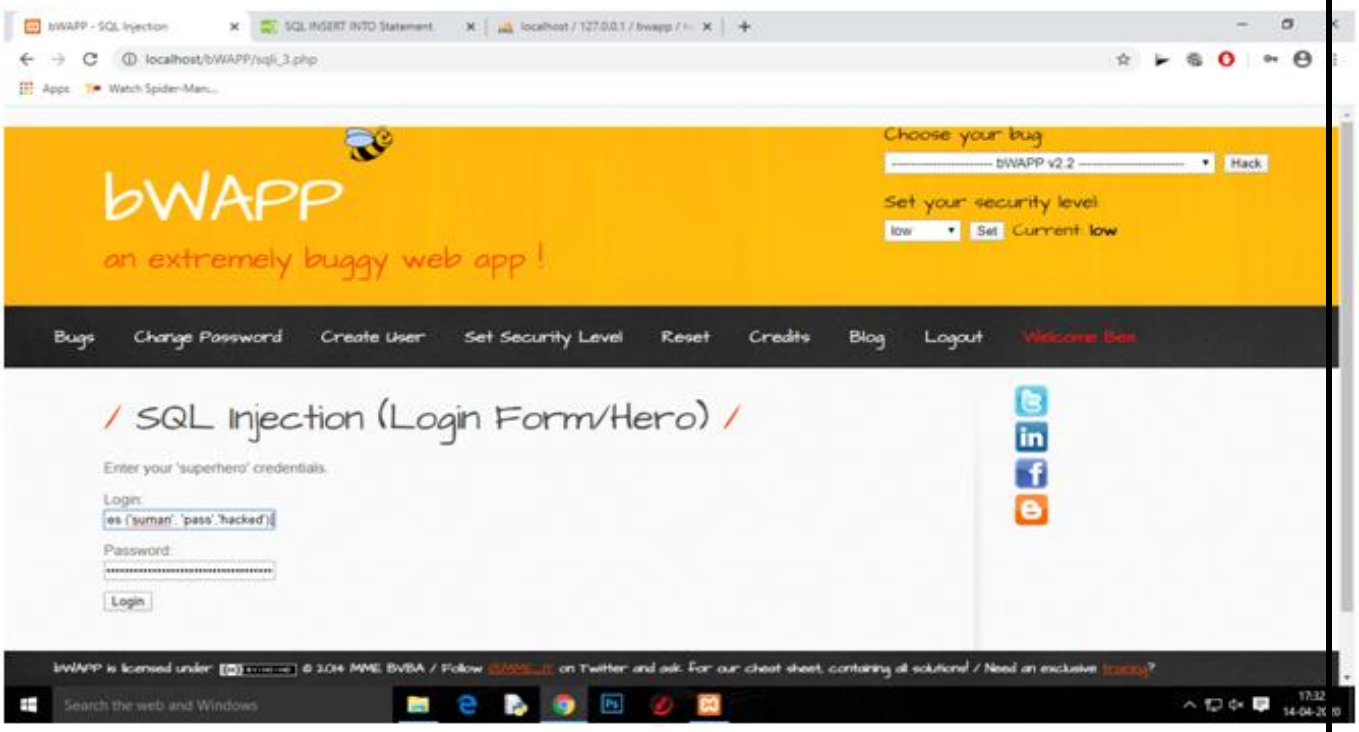
Here in the first picture you can see the heroes database in which each user have an id, name, password and secret column. In second picture you can see the form which is connected to the above mentioned database, here I have added another query

insert into heroes value (‘suman’, ‘pass’,‘hacked’);

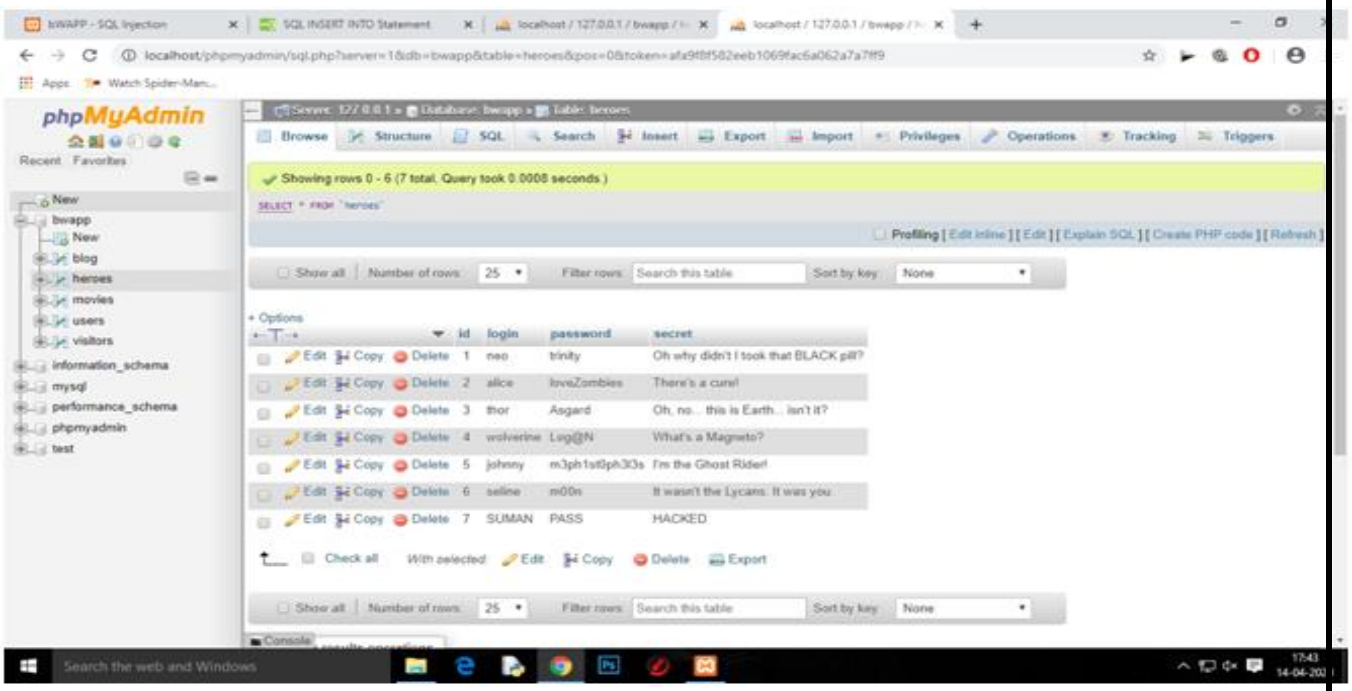
Instead of required values which on submitting have created a new row of the above mentioned values which you can see .In the last picture now we will be able to login (using login: suman password: pass).



DATABASE - "heroes" in which each user have an 'id', 'name', 'password' and 'secret' columns.



It is the form through which our database is connected .Here we added a query **insert into heroes value ('suman', 'pass','hacked');** So,Row is inserted.



As the row was inserted using a query. So,We were able to login (using login: suman and password: pass).

RESULT-

We understood how SQL injection is very useful for web hacking .We were able to Log in without valid credentials and we also created a user account using a SQL injection query.