LAB MANUAL
ON
SESSION HIJACKING

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION

SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Mr. Vipul Mandhar (Project Assistant)

Table of Contents

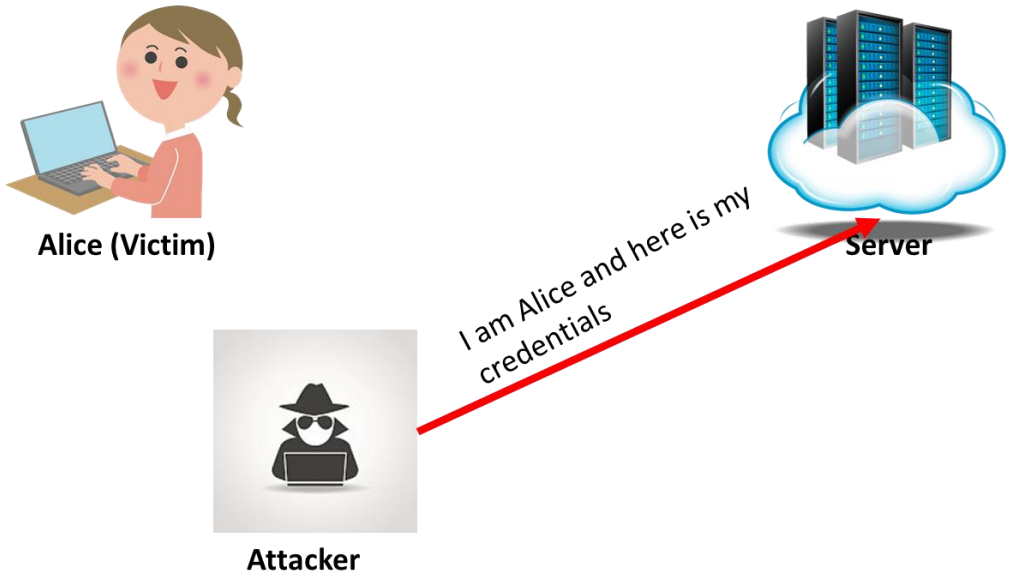
What Is Session Hijacking

Session Hijacking is when an attacker gets access to the session state of a particular user. The attacker steals a valid session ID which is used to get into the system and snoop the data. WhatsApp Sniffer is popular Session Hijacking attack. Session Hijacking first attack on Christmas day 1994 by Kevin Mitnick when http 0.9 was release.

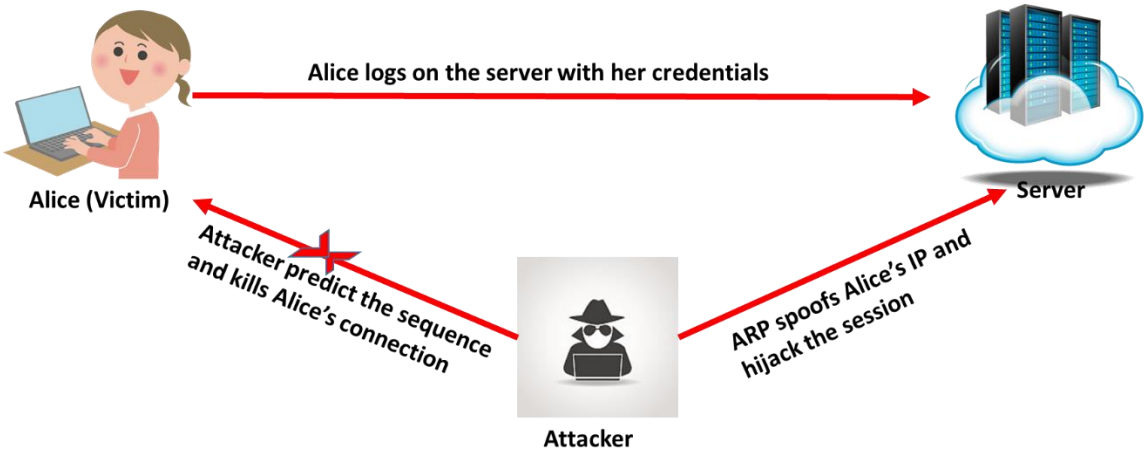
Spoofing vs. Hijacking

- **Spoofing**

  Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server



- Hijacking



Types of Session Hijacking

- There are 2 types of Session Hijacking

1) Active :

In an active attack, an attacker finds an active session and takes over.

2) Passive :

With passive attack, an attacker hijacks a session, but sits back, and watches and records all the traffic that is being sent forth

Session Hijacking Levels

- Session hijacking takes place at two levels:

1. Network Level:

Network level can be defined as the interception of the packets during the transmission between client and the server in a TCP and UDP session

2. Application Level:

Application level is about gaining control on HTTP user session by obtaining the session ID's

Network Level

- Network level session hijacking is particularly attractive to hackers because it provides some critical information to the attacker which is used to attack application level sessions
- Network level hijacking includes:

  TCP/IP Hijacking

IP Spoofing: Source Routed Packets

RST Hijacking

Blind Hijacking

Man in the Middle: Packet Sniffer

UDP Hijacking

Blind Hijacking

- In blind hijacking, an attacker injects data such as malicious commands into intercepted communications between two hosts.
- The hacker can send the data or comments but has no access to see the response.

Man in the Middle: Packet Sniffer (MITM) and UDP Hijacking

- In this attack, the packet sniffer is used to interface between the client and the server.

- The packets between the client and the server are routed through the hijacker's host by using two techniques:

1. Internet Control Message Protocol (ICMP)
2. ARP spoofing

- UDP Hijacking:
- Man in the Middle attack in the UDP hijacking can minimize the task of the attacker.

Application Level Session Hijacking

In this level, the hacker gains the session ID's to get control of the existing session or even create a new unauthorized session

- Application level session hijacking includes:

  Obtaining Session ID's

  Sniffing

  Brute Force

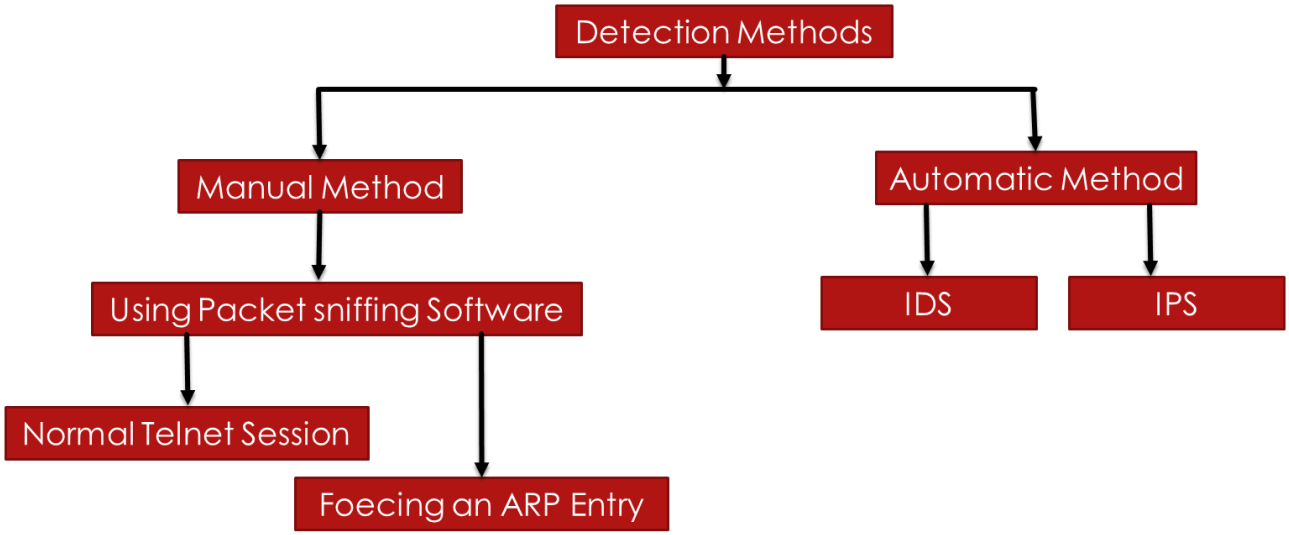
  Misdirected Trust

Session Hijacking Tools

- WireShark: sniffing packets
- Juggernaut: Linux base, Flow across the network
- Hunt: Unix base, sequence number prediction
- TTY Watcher: sun, monitor and control users system
- IP Watcher: commercial Software
- T-Sight : Windows , Commercial software

- Paros HTTP Hijacker: spidering, proxy-chaining, filtering, application vulnerability scanning.
- Hjksuite Tool:
- DnsHijacker Tool and many open source scripts like cookie injector.

Detection of Session Hijacking



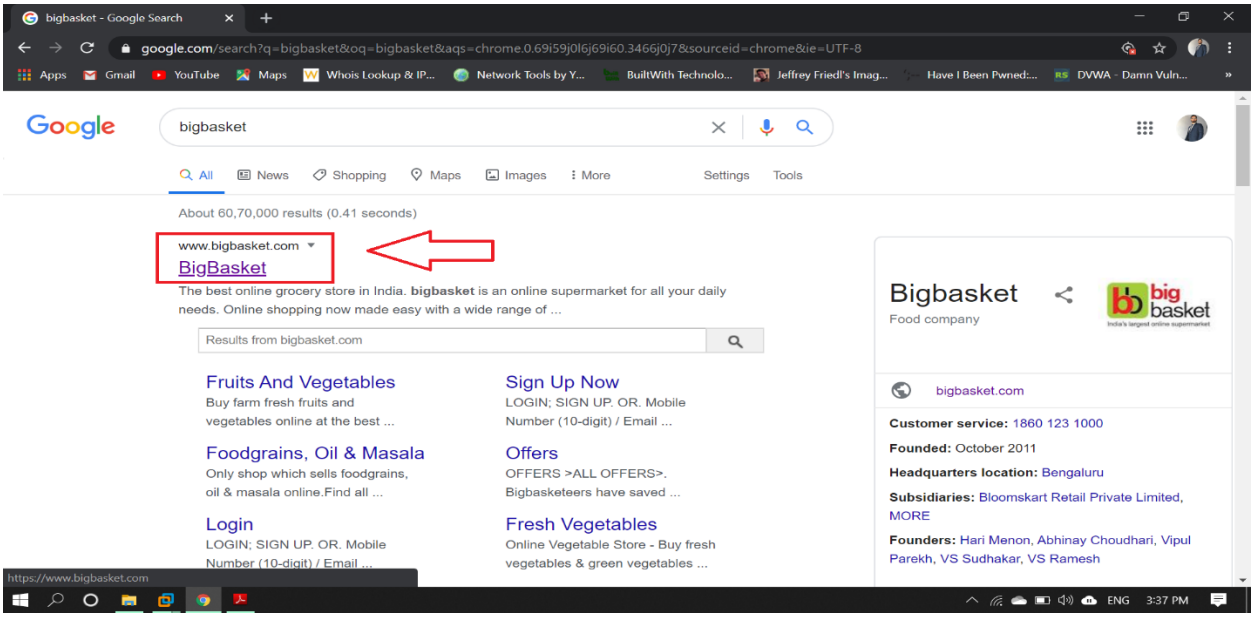
Prevention of Session Hijacking

- There are mainly four methods to prevent session hijacking:

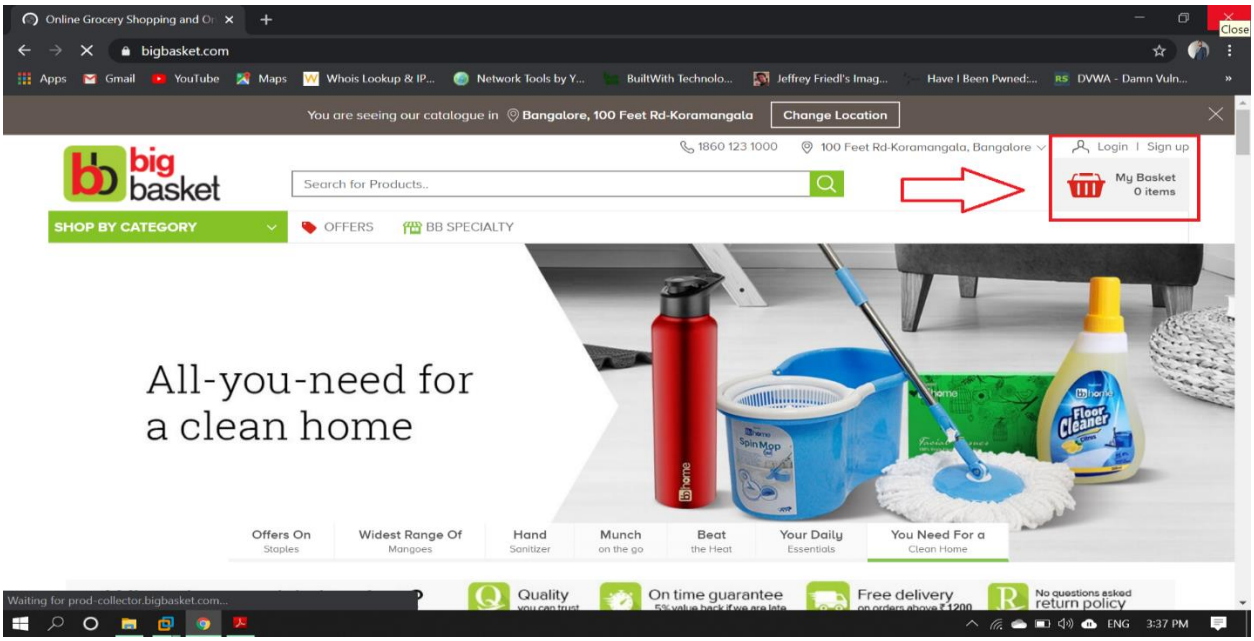
1. Encryption
2. Connections
3. Anti-virus Software
4. Employee education

Session Hijacking practical

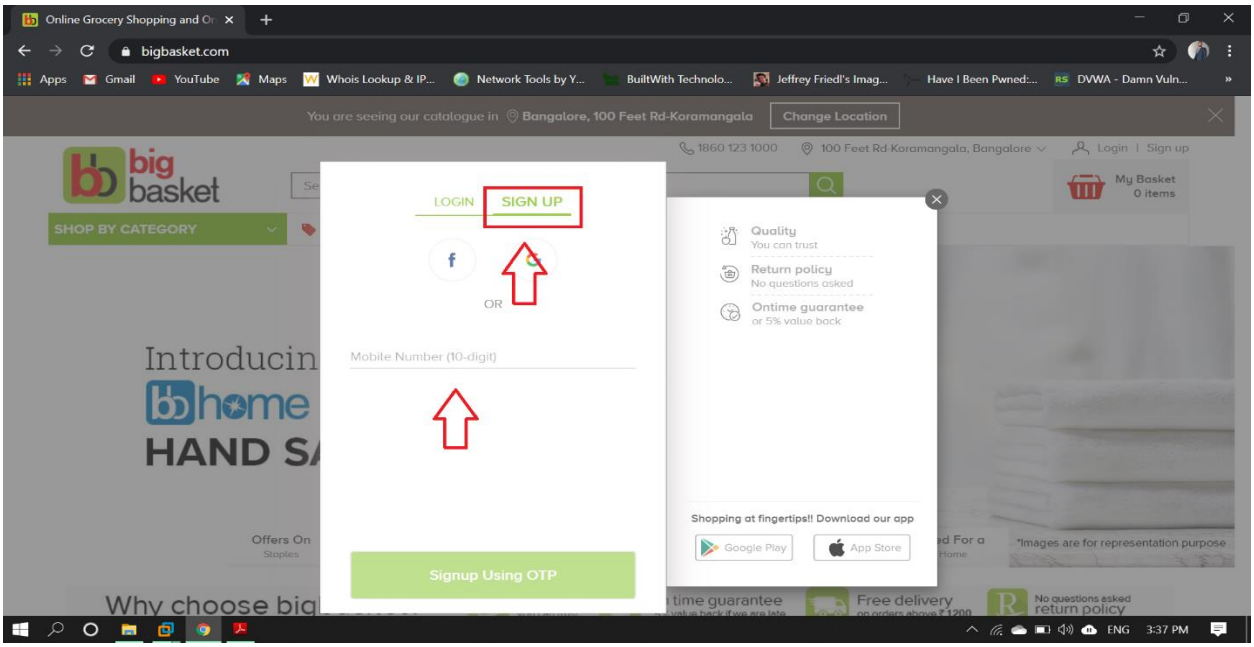
Step 1: Search for any online shopping site in this case we are using BigBasket as an example (In Victims Browser).



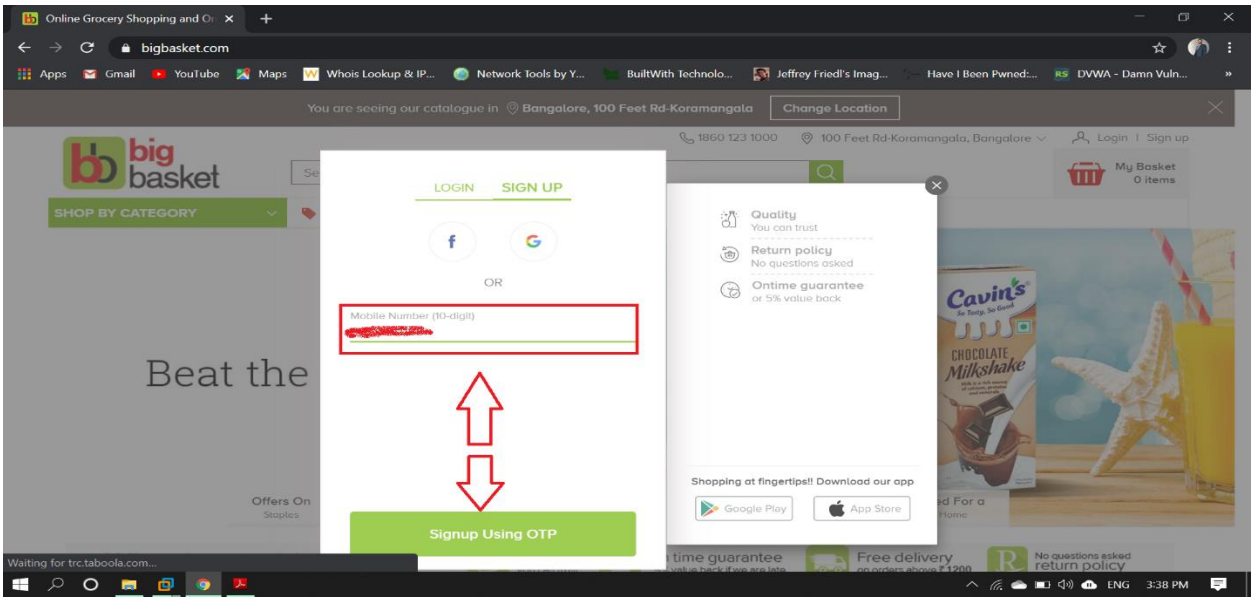
Step 2: Open the website and on the right side there is login and signup option choose one from them.



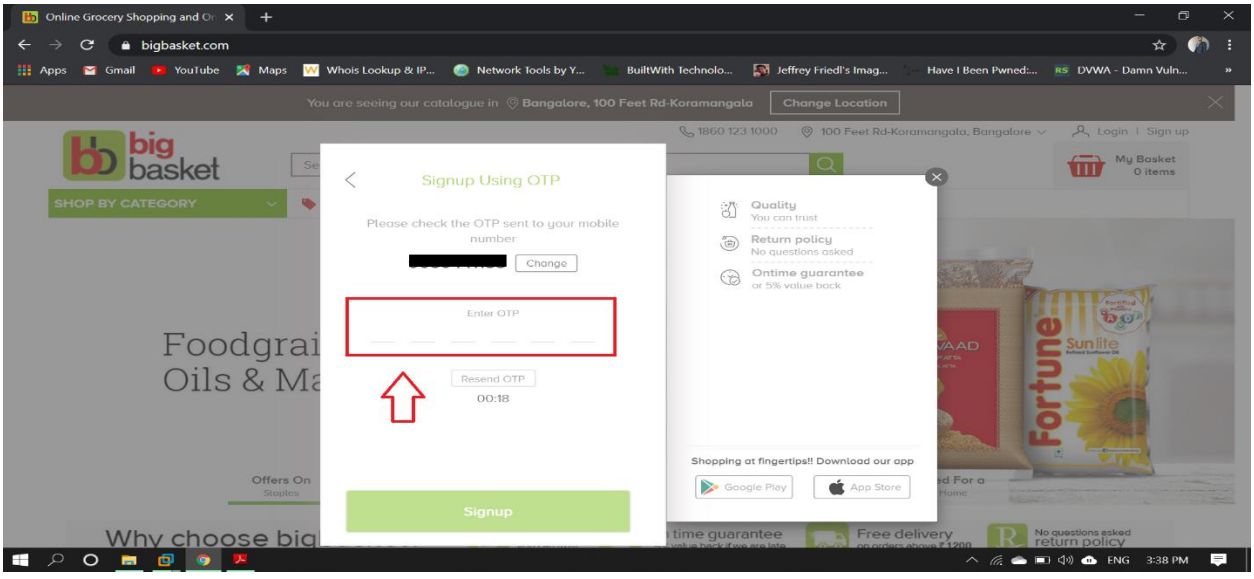
Step 3: Enter Credentials to Sign up or Login.



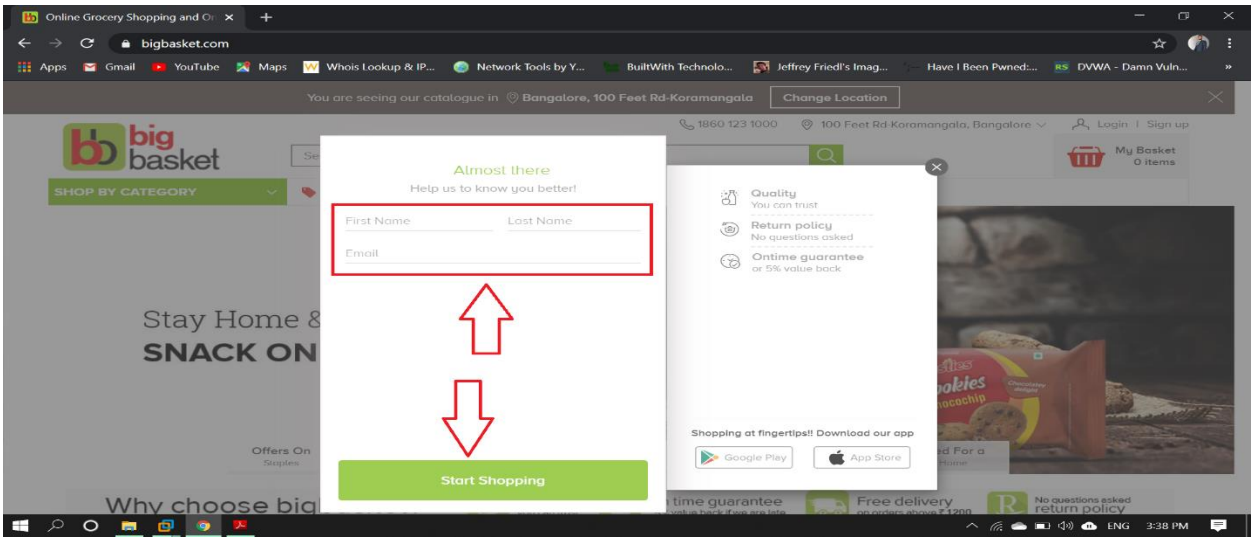
Step 4: In this case we are using contact no for the sign up process.



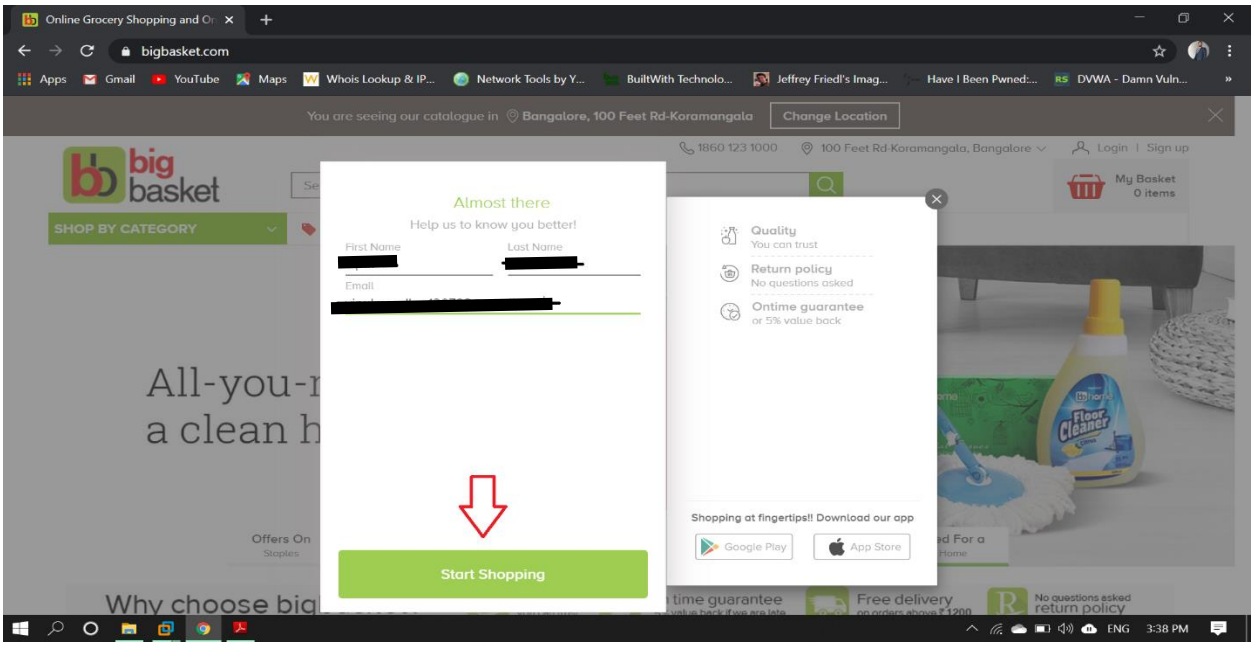
Step 5: Enter the One time password that is received on your phone to sign up.



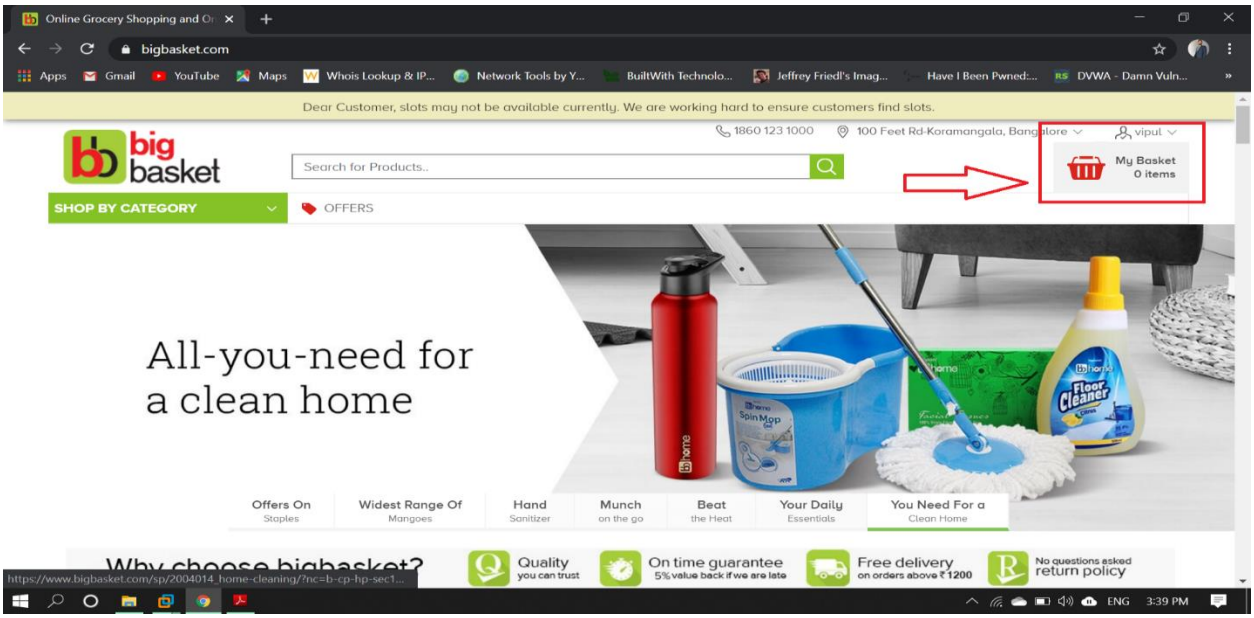
Step 6: Fill the required information to complete the sign up process.



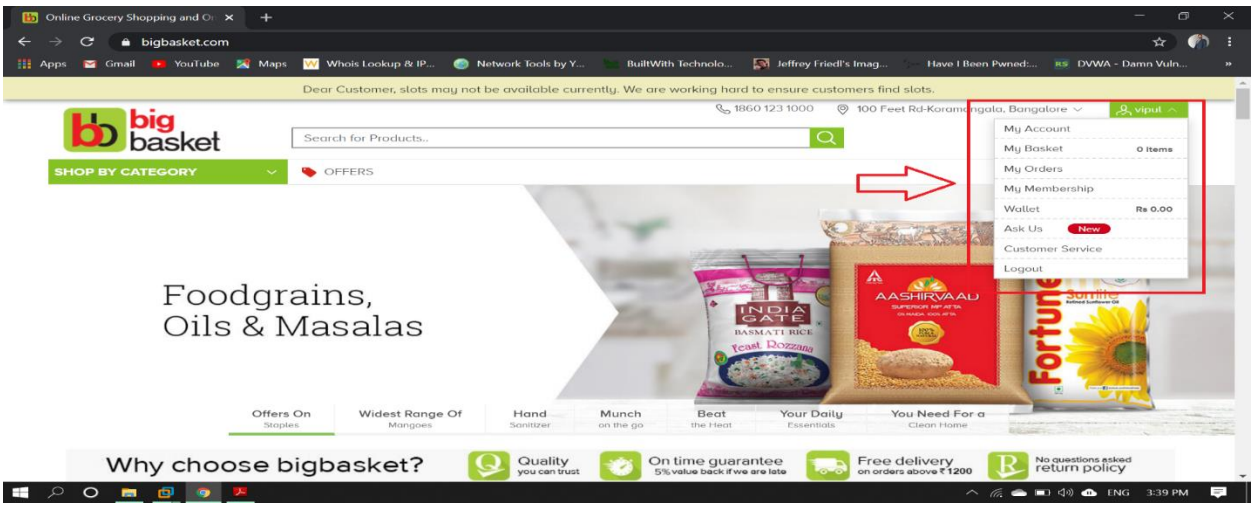
Step 7: After that click on Start Shopping.



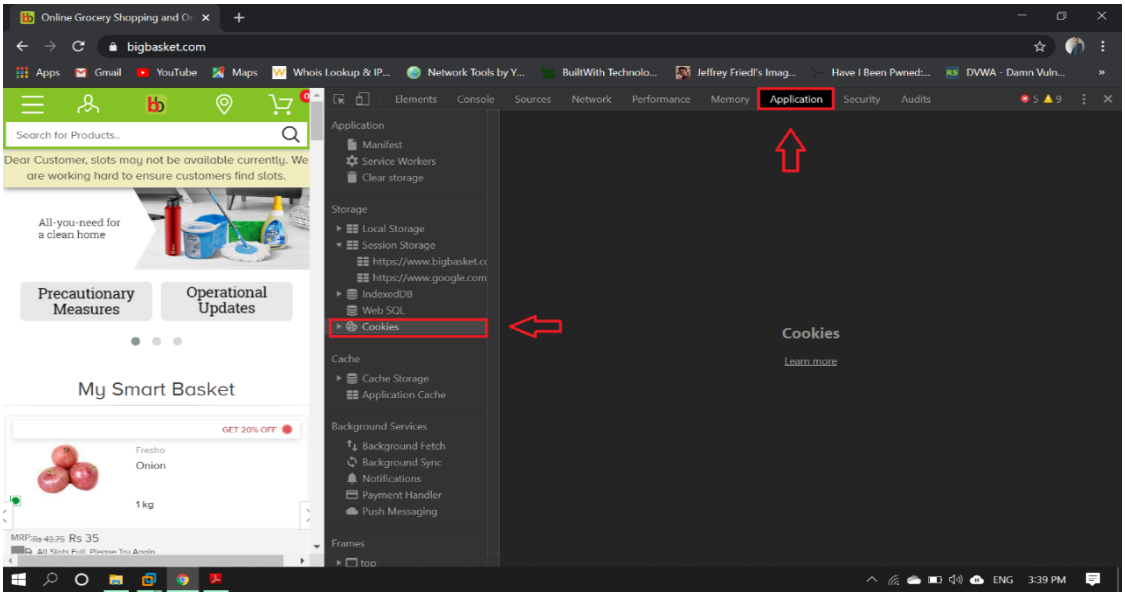
Step 8: In right side corner it is visible that signed up with user name vipul (In Victims browser).



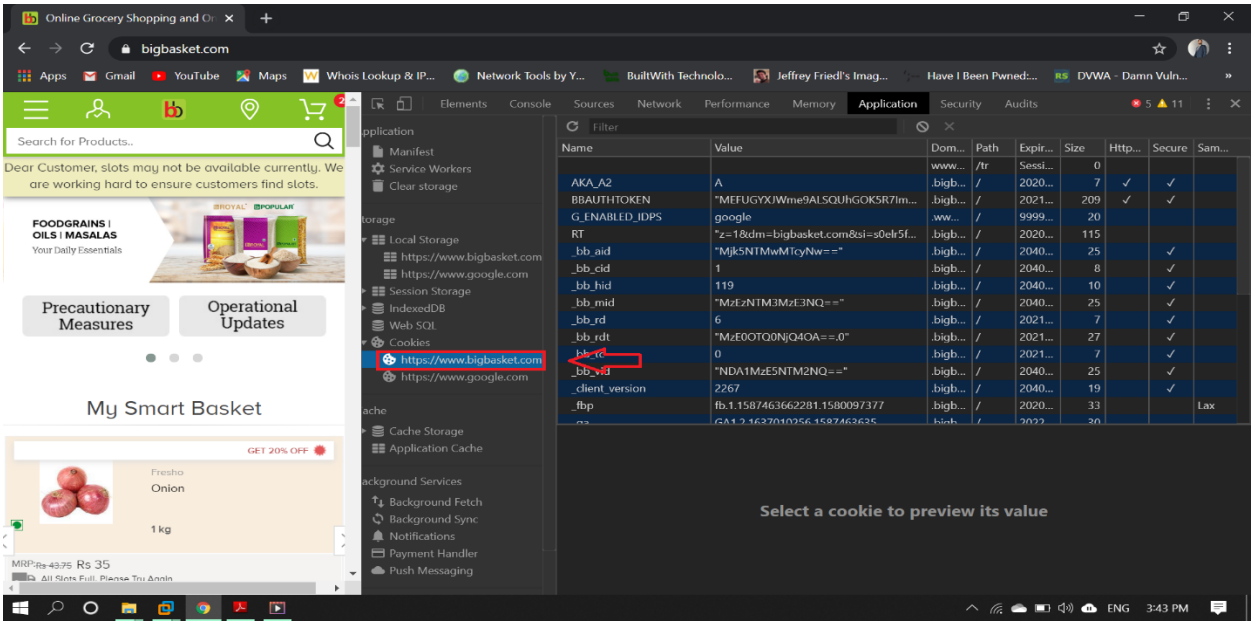
Step 9: Here its shows the other information related to account of the victims.



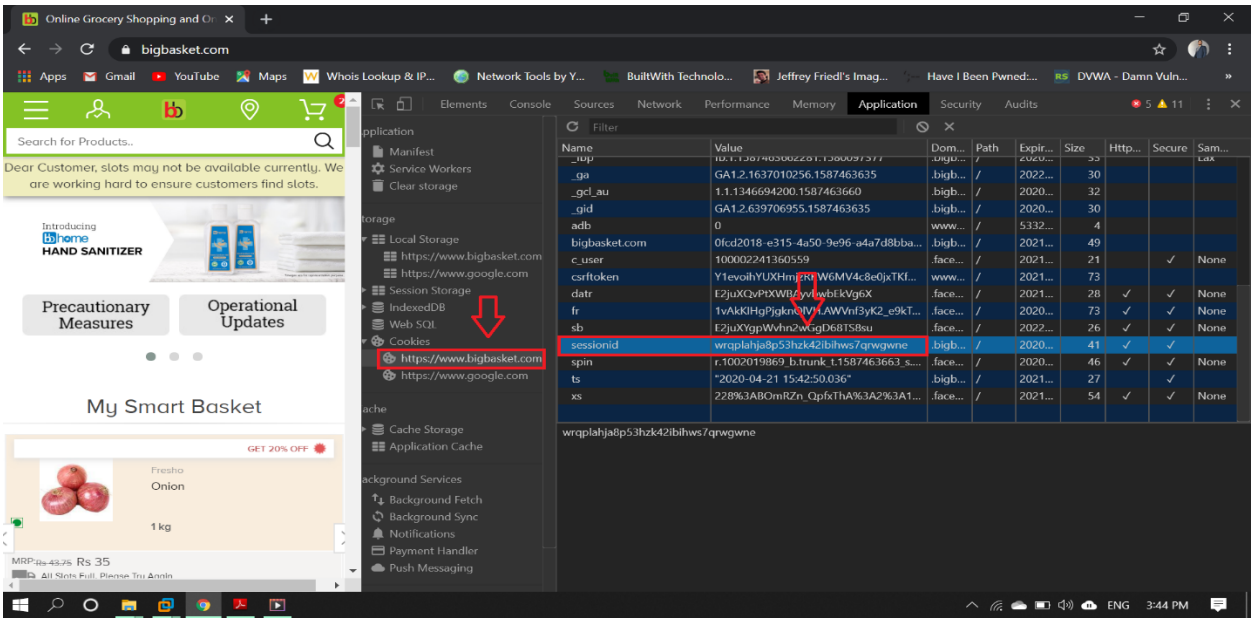
Step 10: Press **Function key+F12** to get the cookies detail as shown in the figure given below.



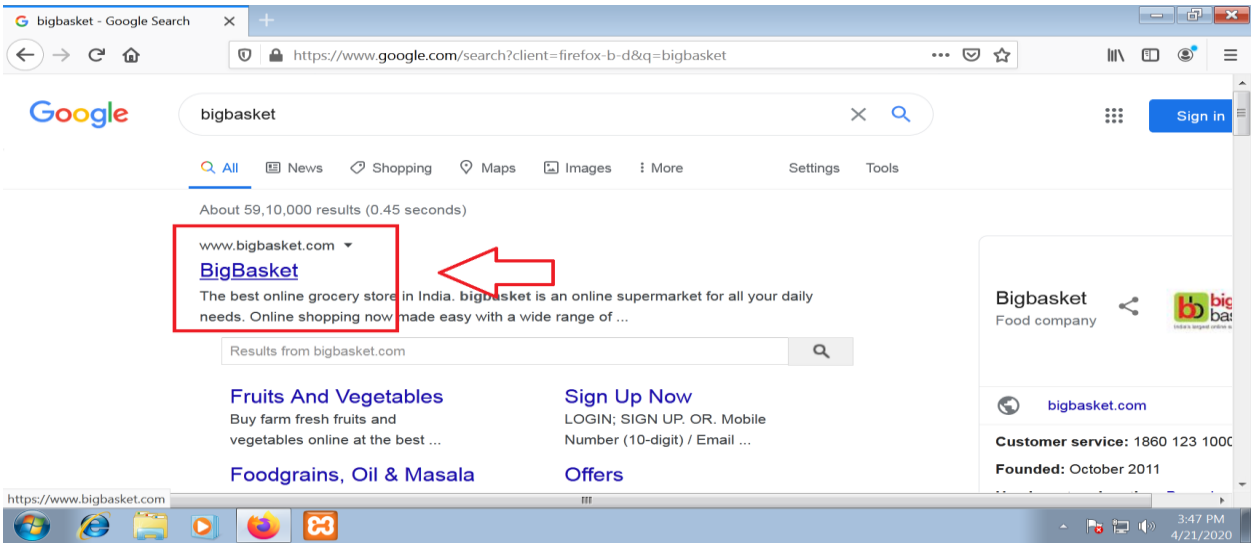
Step 11: Click on application then on cookies option that is in left of the screen to collect the session ID of the victim current session of BigBasket website .



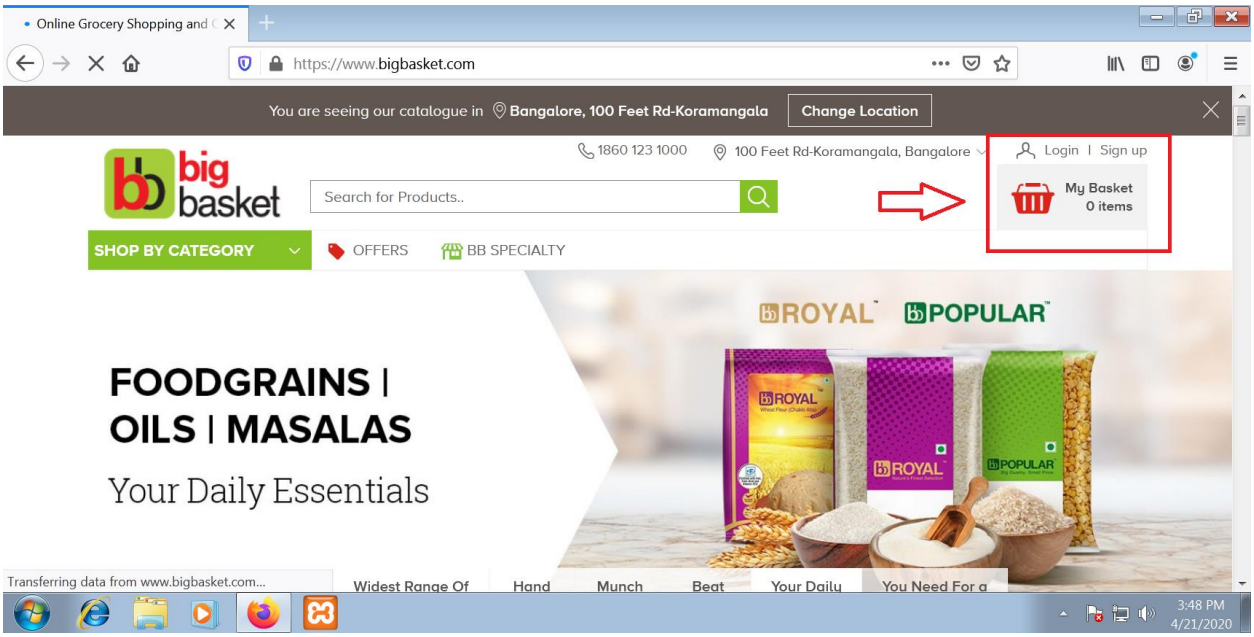
Step 12: In cookies we get the following details like Name, value, domain and many more from that find for Session Id and copy the value given to that.



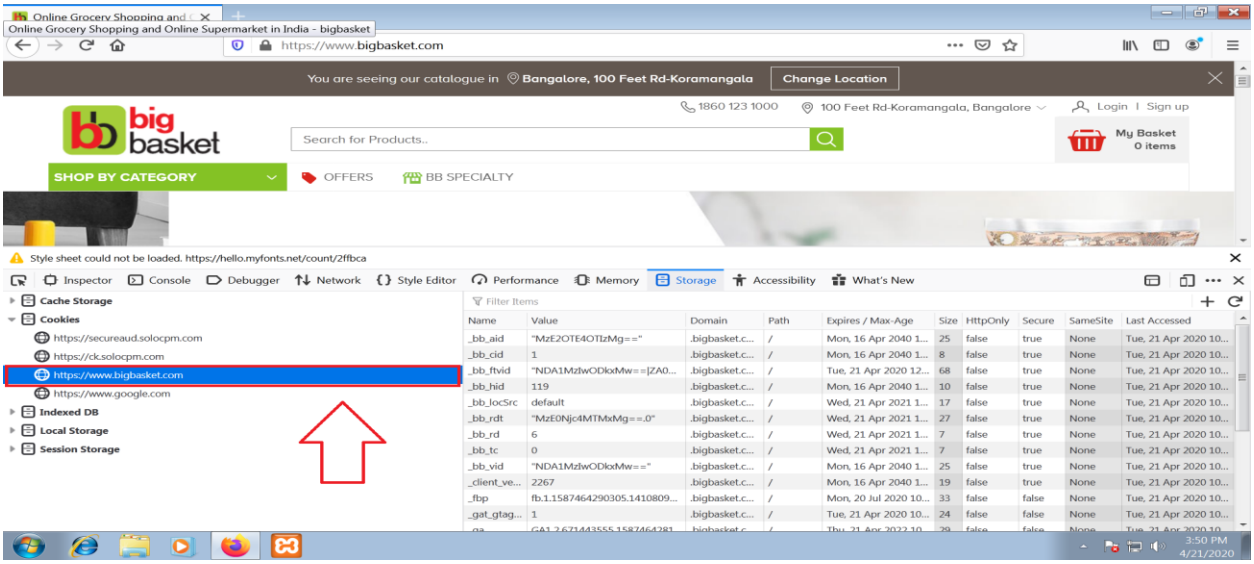
Step 13: Now in other browser (Attackers) open the BigBasket website to login directly without filling the login credentials.



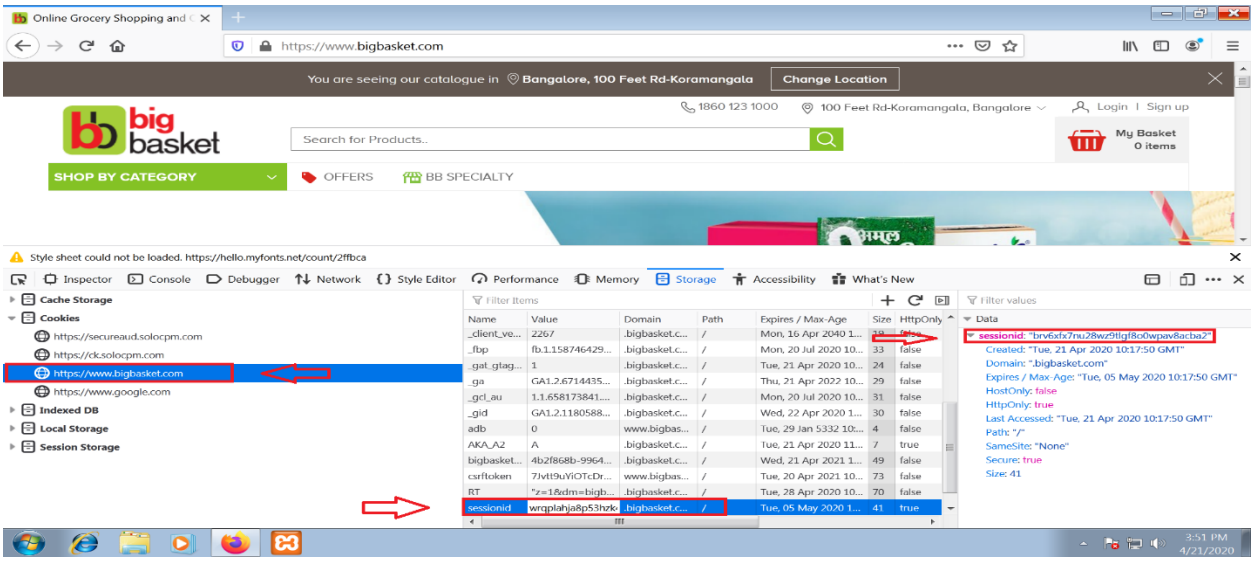
Step 14: Here it is clearly visible that no one is logged In.



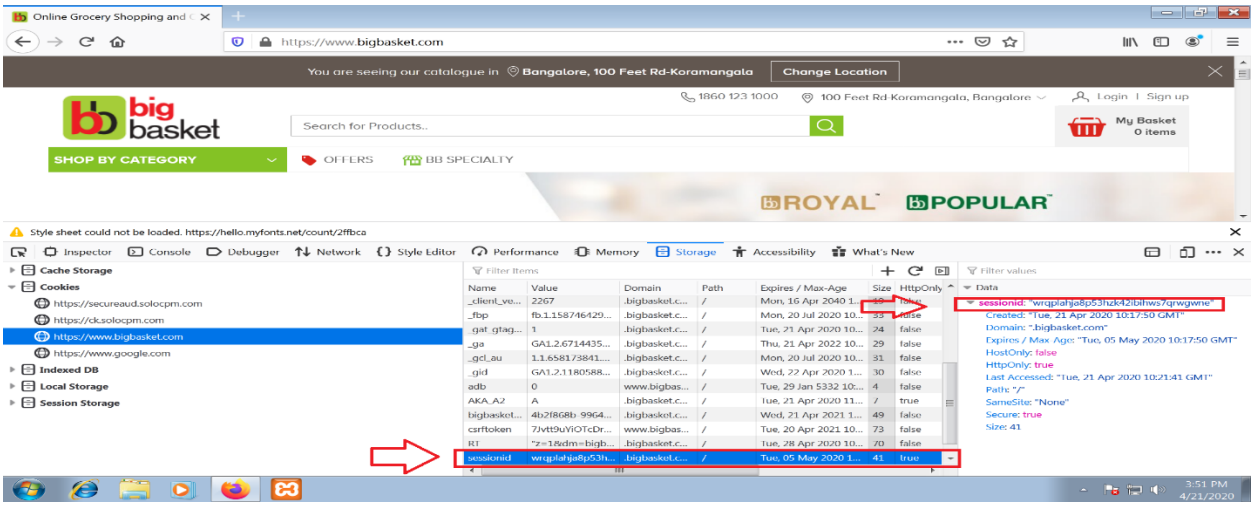
Step 15: Again press the **Function key+F12** to view the cookies detail.



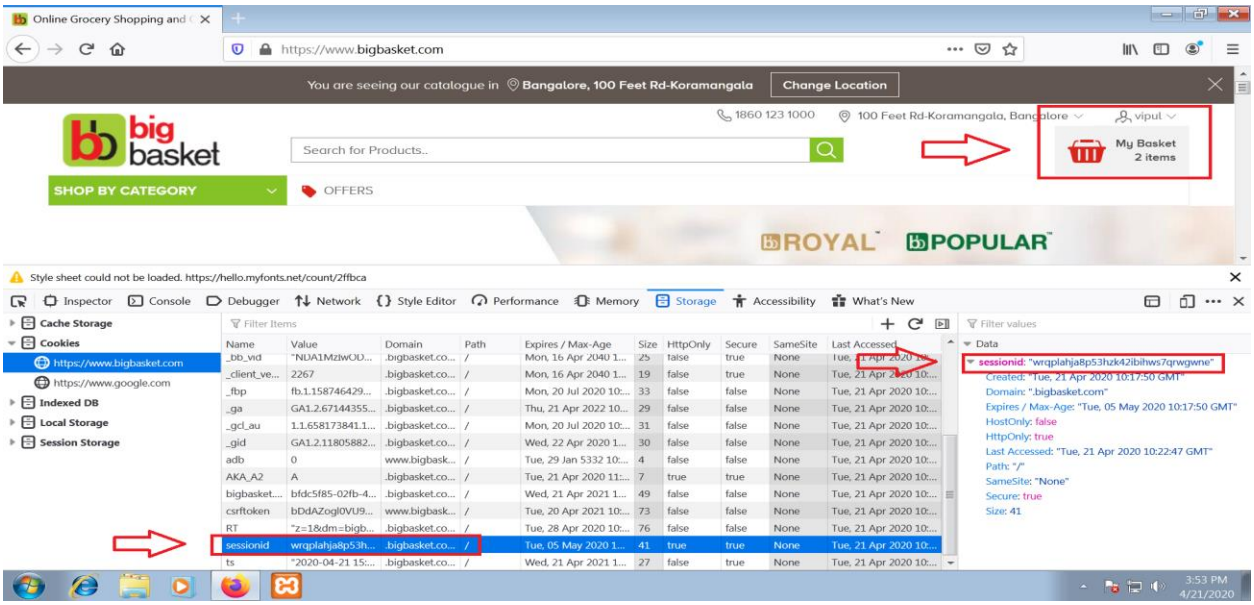
Step 16: Click on storage and then on cookies that is the leftside of the screen, and check for Session Id and its value.



Step 17: Replace the Session Id value of Attacker with the previous one that is copied from the other browser i.e. of victims.



Step 18: After replacing the value press Enter and refresh the page and you will login with Victims Login Details as shown in right side of the image .



INTRODUCTION TO XAMPP

XAMPP is a freely available and open source cross-platform web server solution stack package, consist of the Apache HTTP Server, MySQL database, and interpreters for scripts written in the PHP and Perl programming languages.

X----------Cross-platform
A----------Apache
M----------MariaDB (Mysql)
P----------PHP
P----------Perl

AVAILABILITY

XAMPP is available for:

- Microsoft Windows
- Linux
- Solaris
- Mac OS

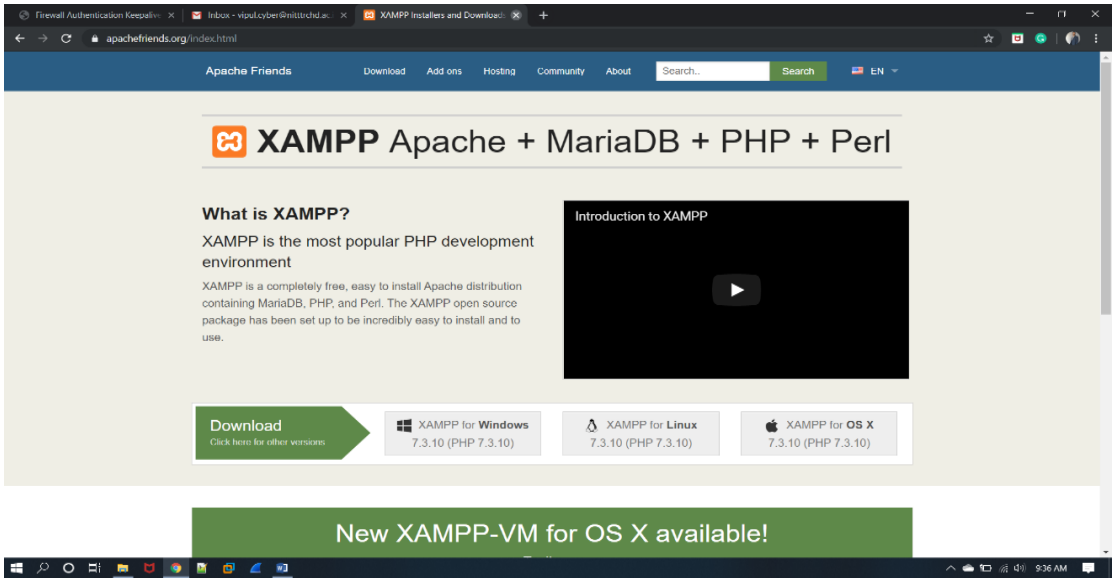
And it is mainly used for web development projects.

XAMPP INSTALLATION

Steps to install Xampp Server

Open the XAMPP website.

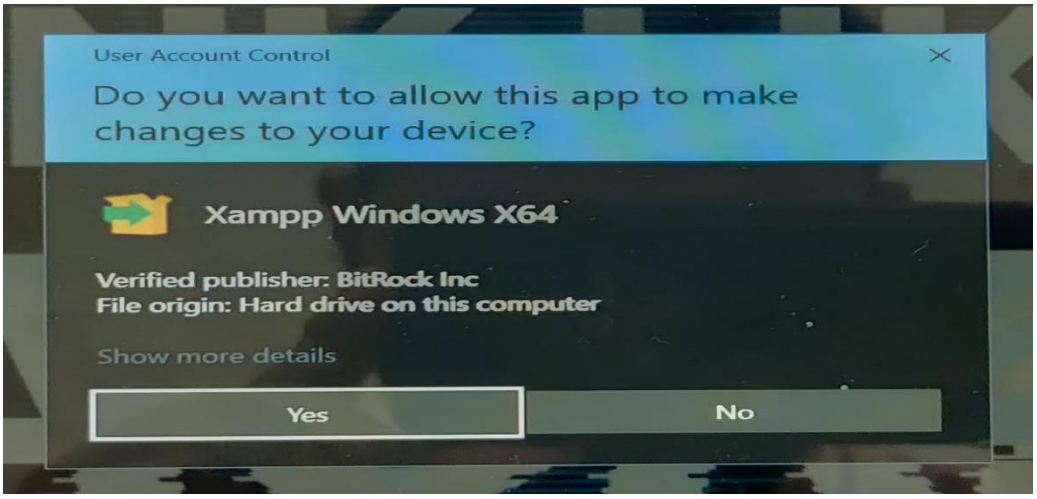
Go to https://www.apachefriends.org/index.html in your computer's web browser.



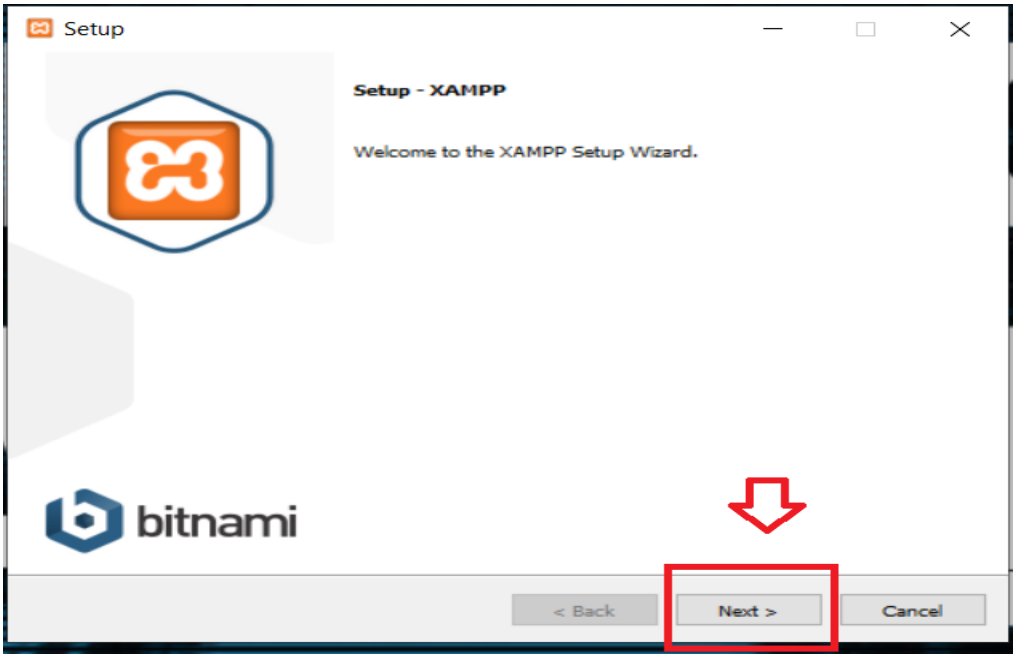
Step 1 Click XAMPP for Windows. It's a grey button near the bottom of the page. Depending on your browser, you may first have to select a save location or verify the download.

Step 2 Double-click the downloaded file. This file should be named something like xampp-win64-7.2.4-0-VC15-installer, and you'll find it in the default downloads location (e.g., the "Downloads" folder or the desktop).

Step 3 Click *Yes* when prompted. This will open the XAMPP setup window. You may have to click OK on a warning if you have User Account Control (UAC) activated on your computer.

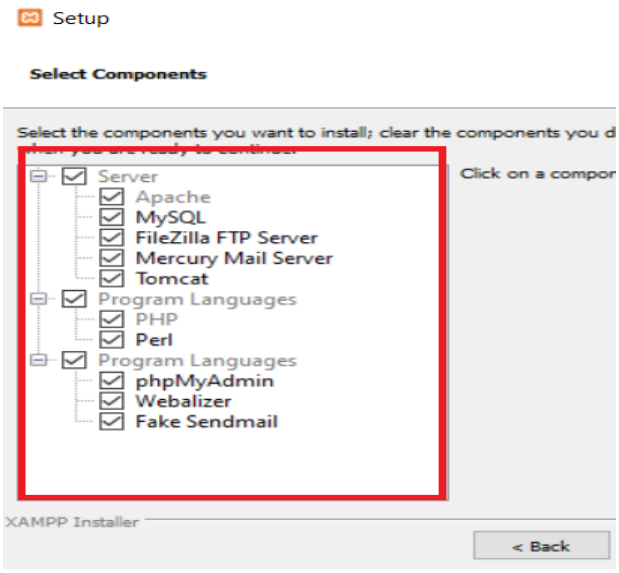


Step 4 Click Next. It's at the bottom of the setup window.

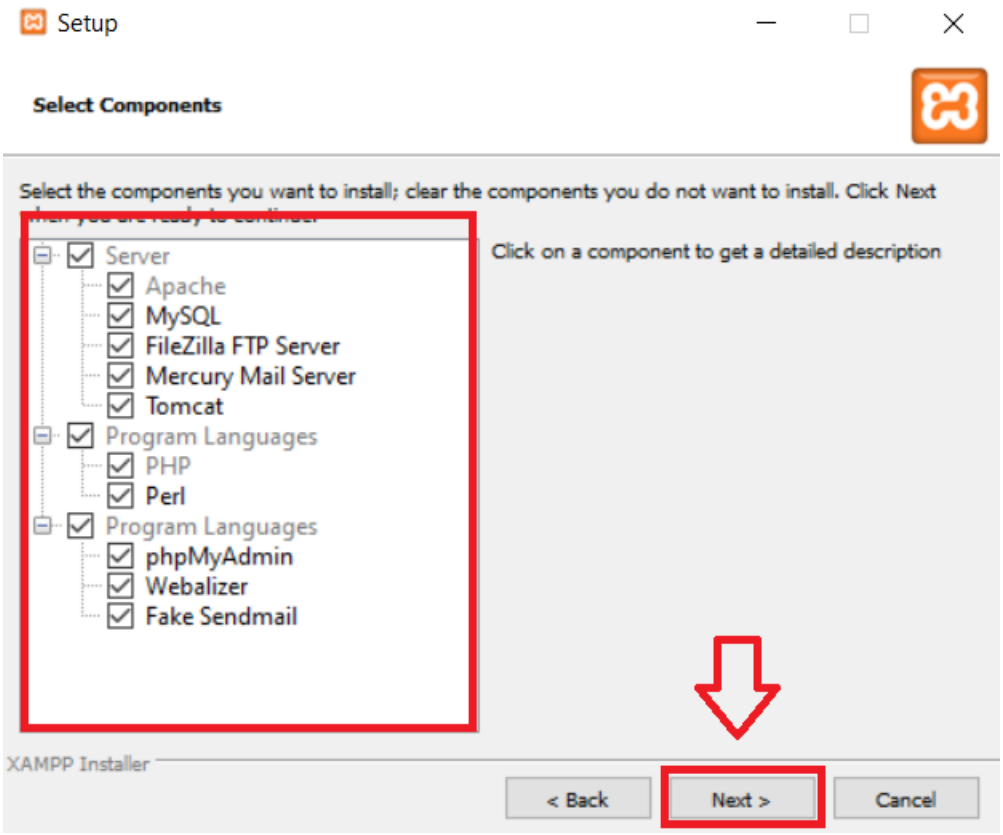


Step 5 Select aspects of XAMPP to install. Review the list of XAMPP attributes on the left side of the window; if you see an attribute that you don't want to install as part of XAMPP, uncheck its box.

- By default, all attributes are included in your XAMPP installation.

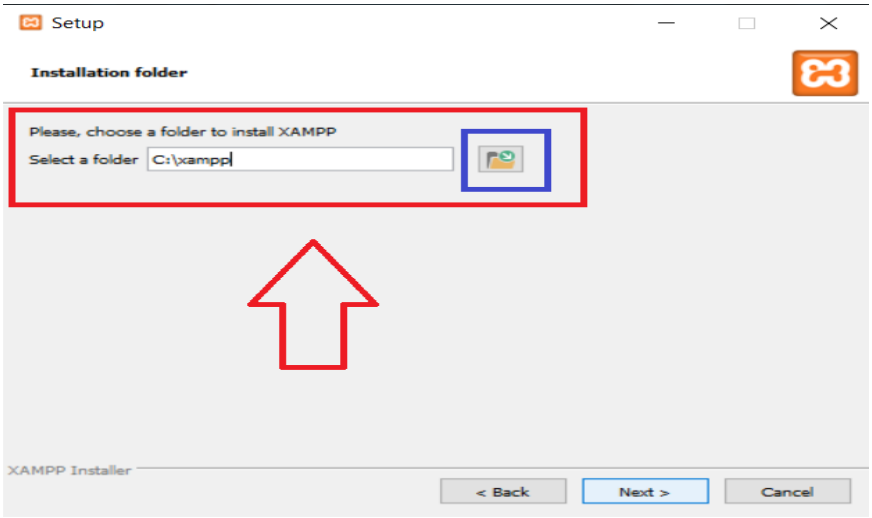


Step 6 Click Next. It's at the bottom of the window.



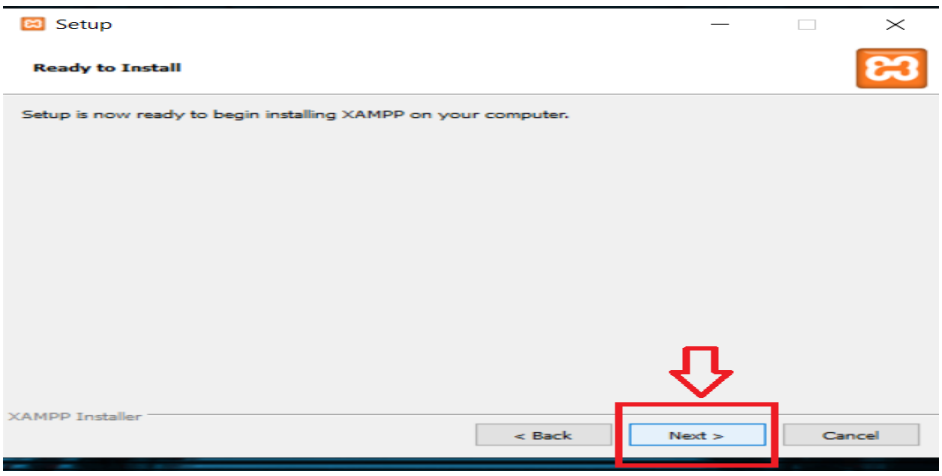
Step 7 Select an installation location. Click the folder-shaped icon to the right of the current installation destination, then click a folder on your computer.

- You can select a folder (e.g., Desktop) and then click Make New Folder to create a new folder and select it as the installation destination.



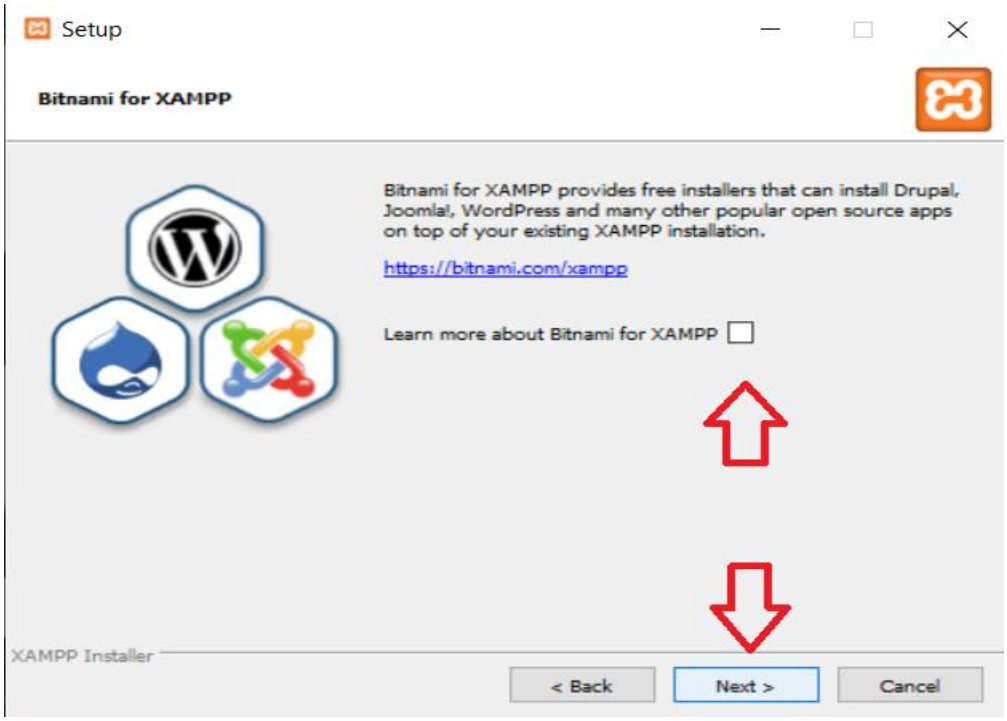
Step 8 Click OK. Doing so confirms your selected folder as your XAMPP installation location.

Step 9 Click Next. You'll find it at the bottom of the page.



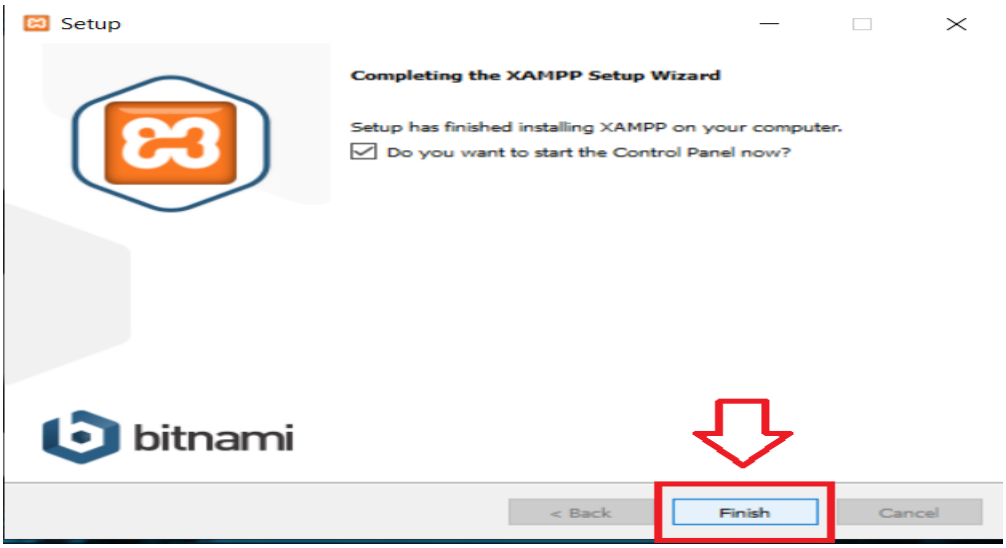
Step 10 Uncheck the "Learn more about Bitnami" box, then click Next. The "Learn more about Bitnami" box is in the middle of the page.

Step 11 Begin installing XAMPP. Click Next at the bottom of the window to do so. XAMPP will begin installing its files into the folder that you selected.



Step 12 Click Finish when prompted. It's at the bottom of the XAMPP window. Doing so will close the

- Window and open the XAMPP Control Panel, which is where you'll access your servers.



Step 13 Xampp server will run like this and start Apache and MYSQL.

Step 14 Click on finish.

INTRODUCTION TO DVWA

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. The main goal of DVWA is to be an aid for security professionals/experts to check their skills and tools in a proper legal environment.

This will helps web developers to better sense the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

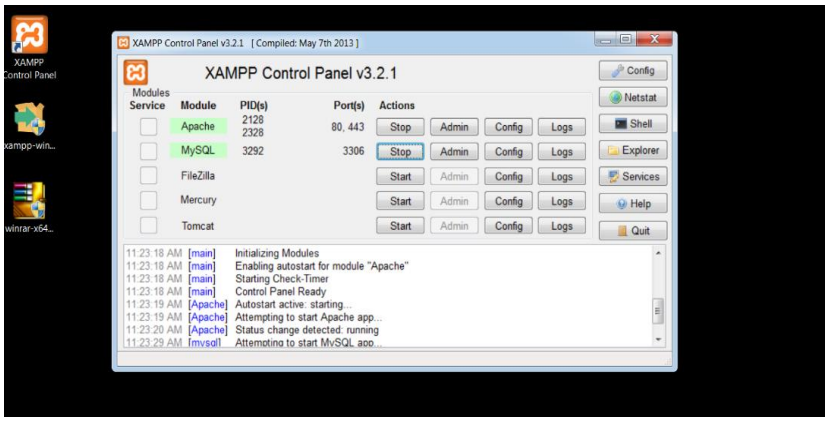
DVWA INSTALLATION

Steps to setup DVWA on your windows PC:

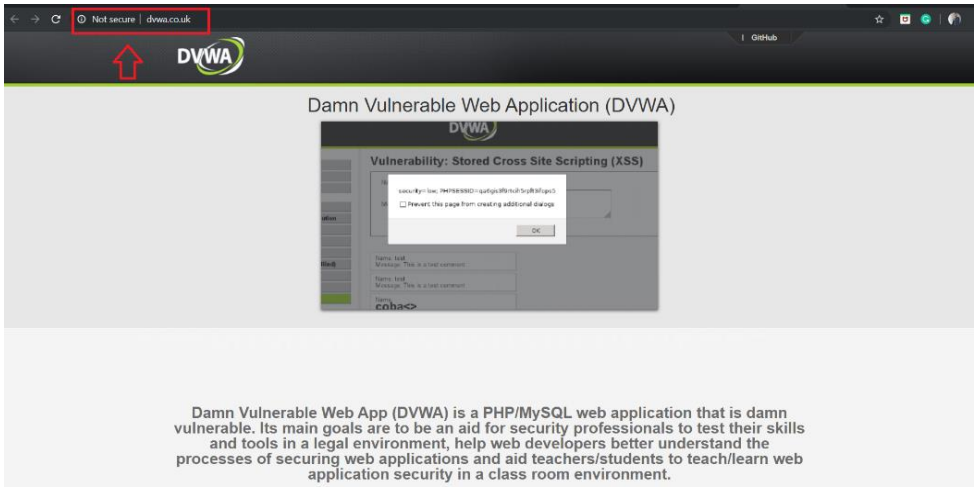
Step 1 Download and install XAMPP on your computer.

Step 2 Open XAMPP:

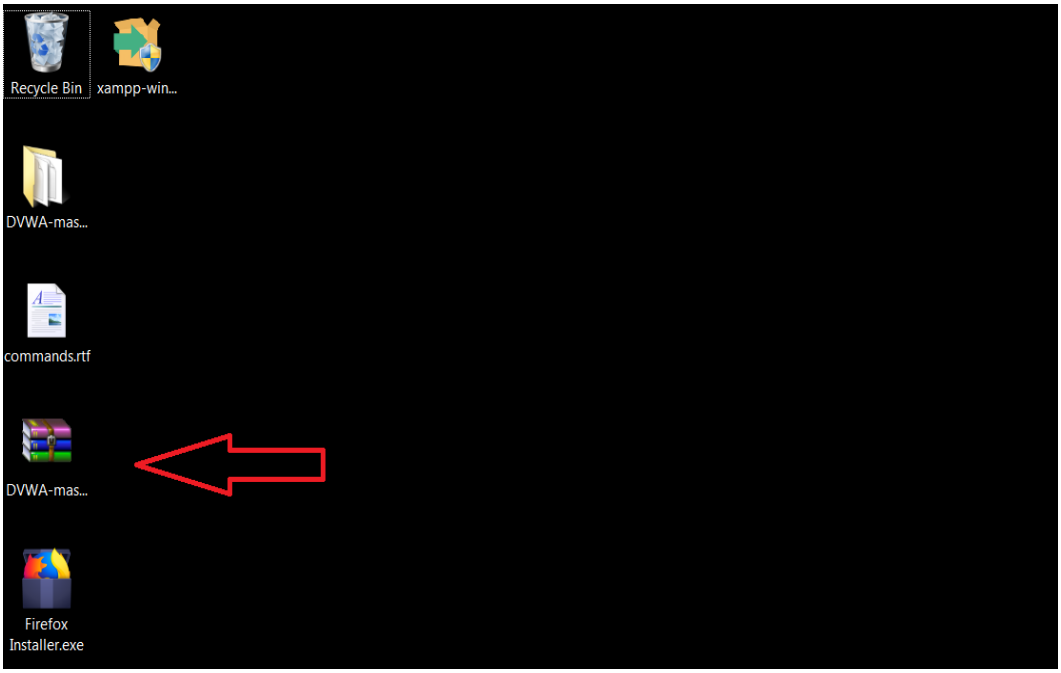
Then open the XAMPP control panel and start “Apache” and “MySQL” service.



Step 3 Download Damn Vulnerable Web App (DVWA)

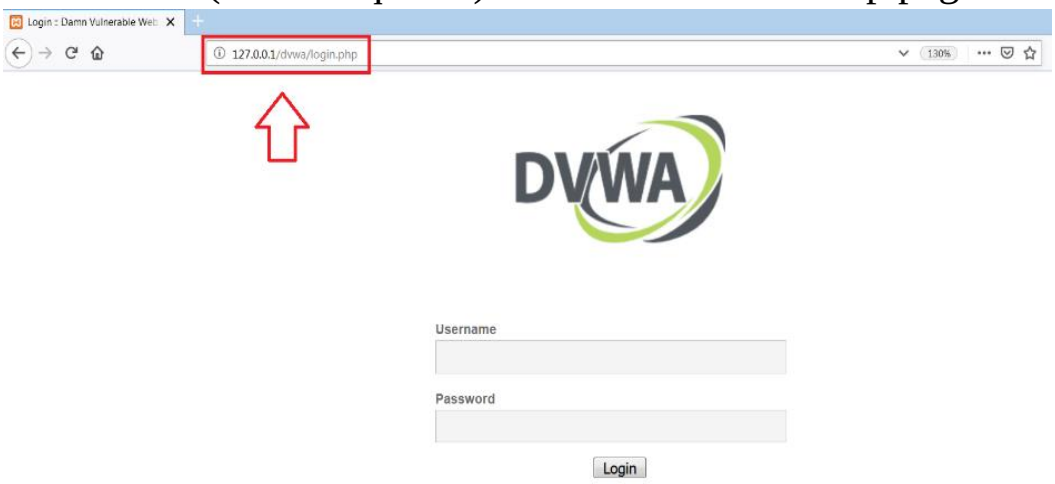


Step 4 Extract the Zip to htdocs :

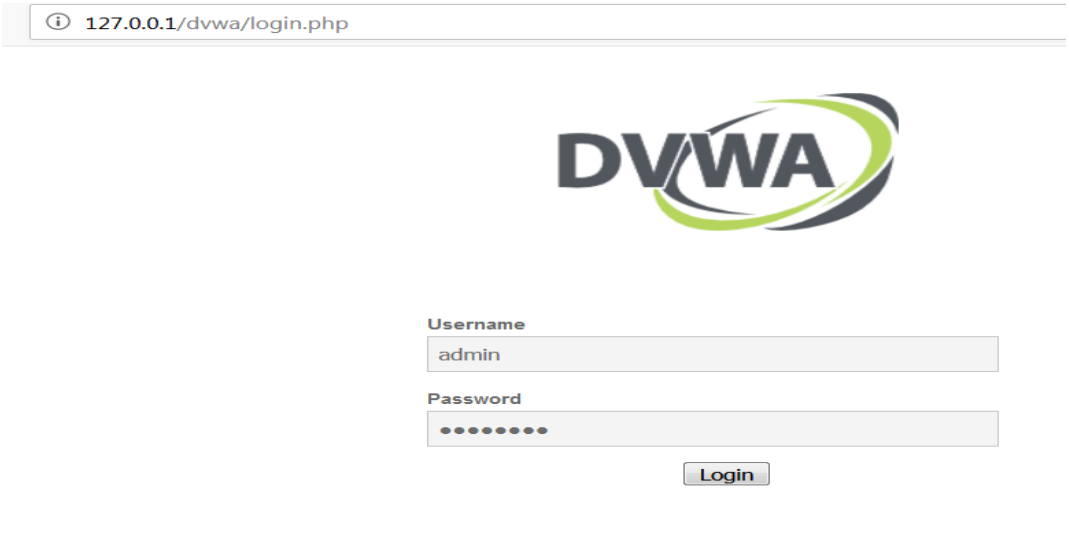


Step 5 Open the web browser:

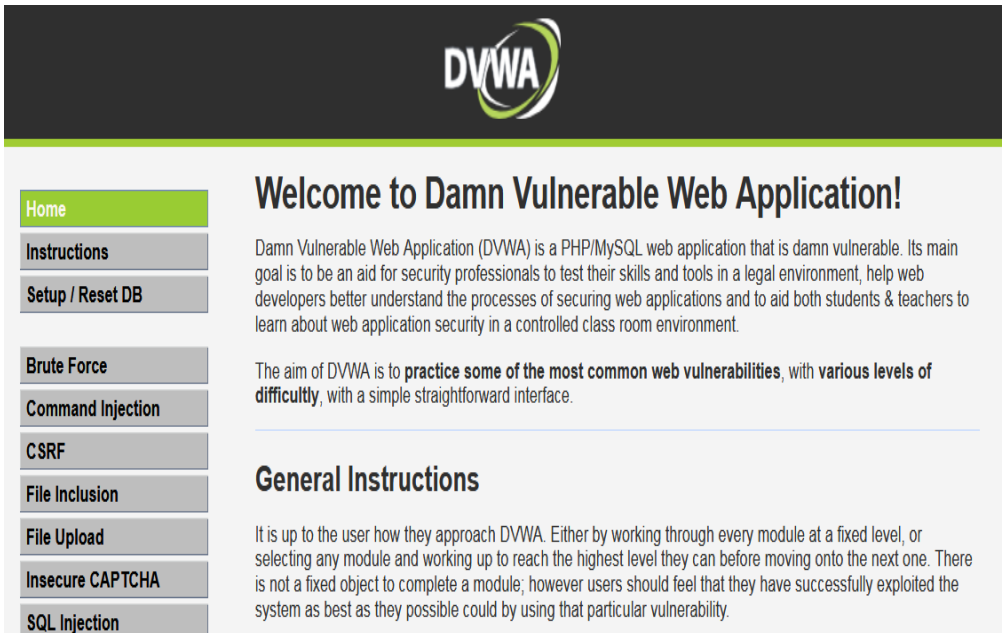
Step 6 Open the browser and then type "127.0.0.1/DVWA" in the address bar (without quotes). You will see the setup page



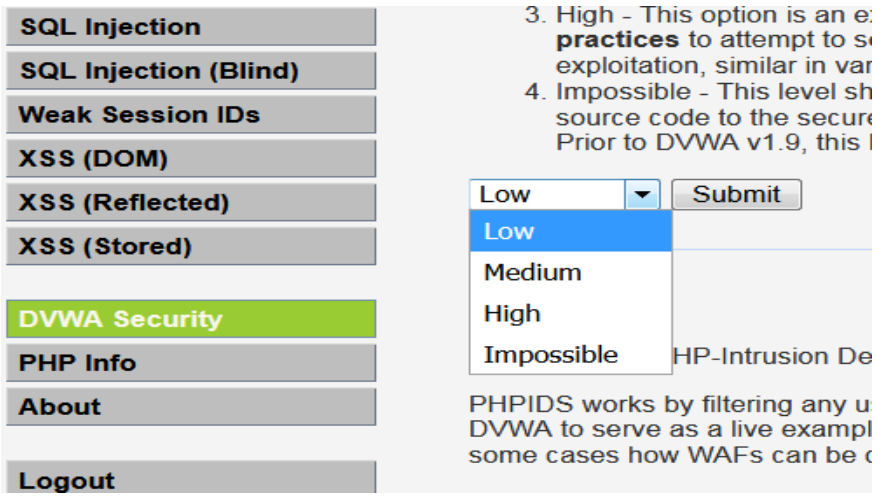
Step 7 To Login in DVWA just type User Name= Admin and Password=Password i.e. by default user name and password.



Step 8 After Login this screen will be available on the browser.



Step 9 Set the security levels of DVWA according to your requirement.

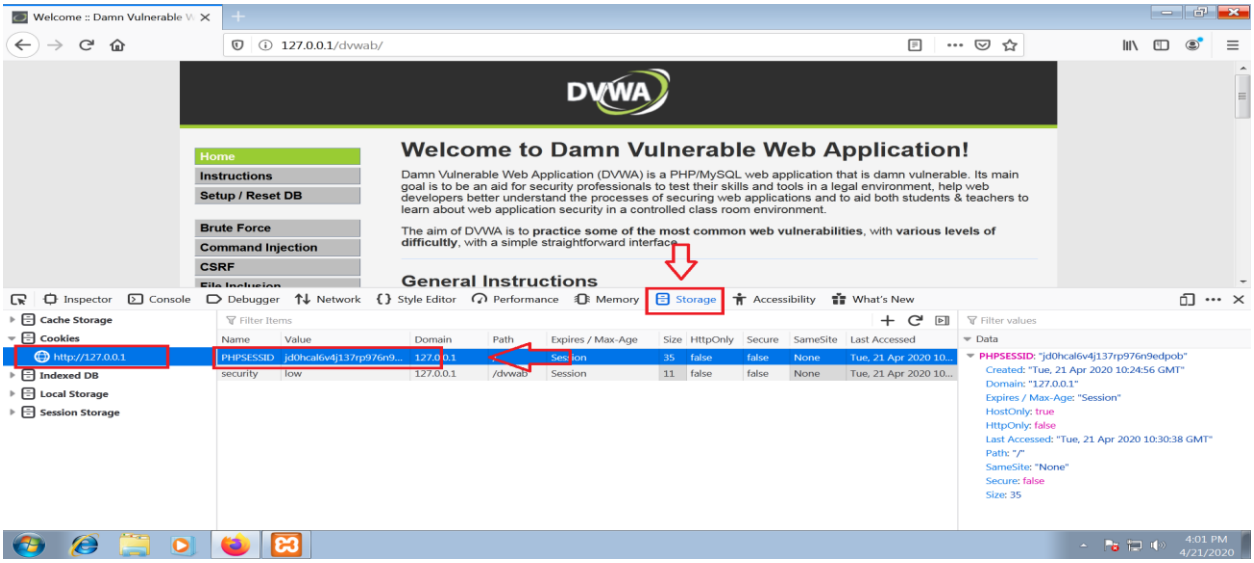


on DVWA

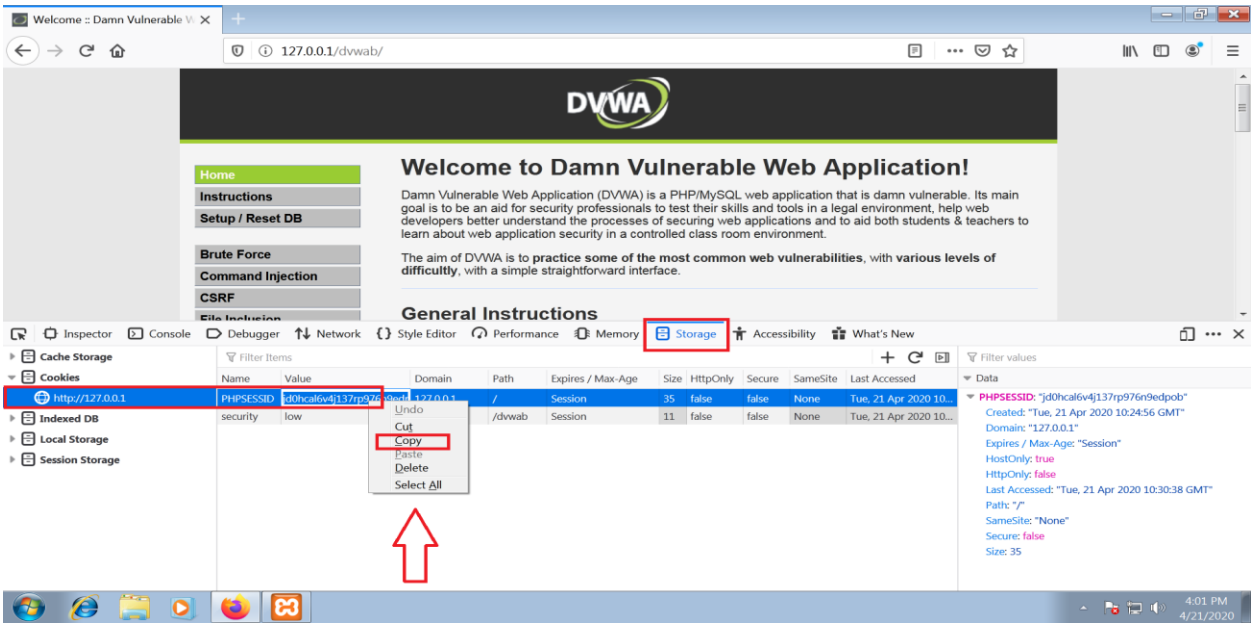
Steps to perform

Step 1: Fill the credentials to login in victims browser.

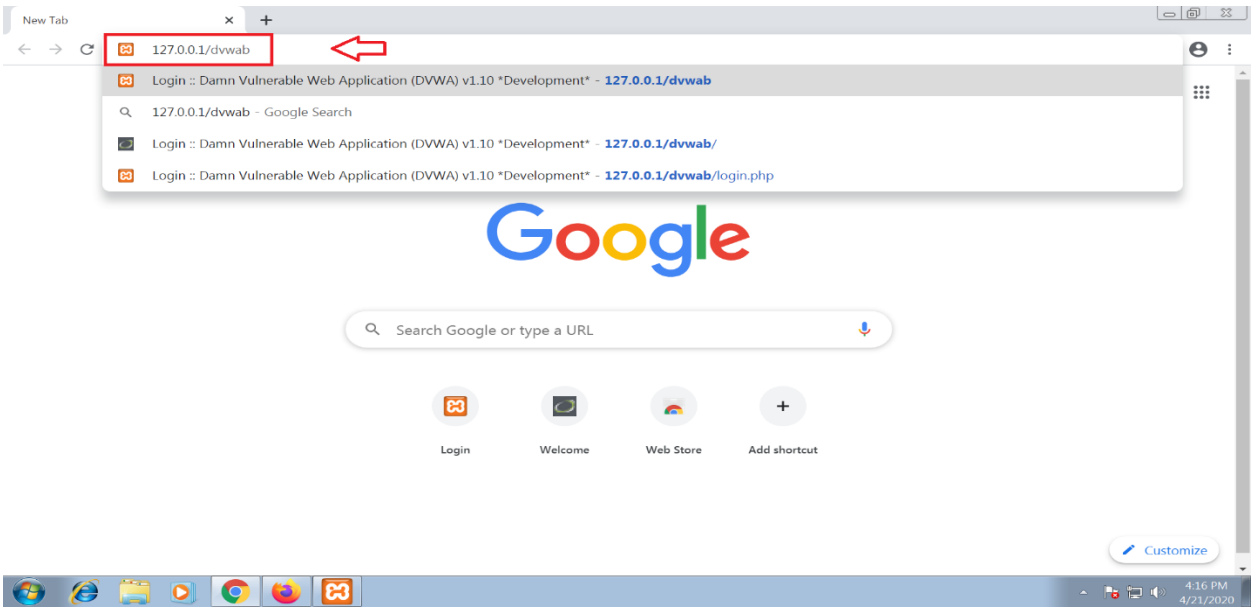
Step 2: Press the **Function Key+F12** to get the cookies details.



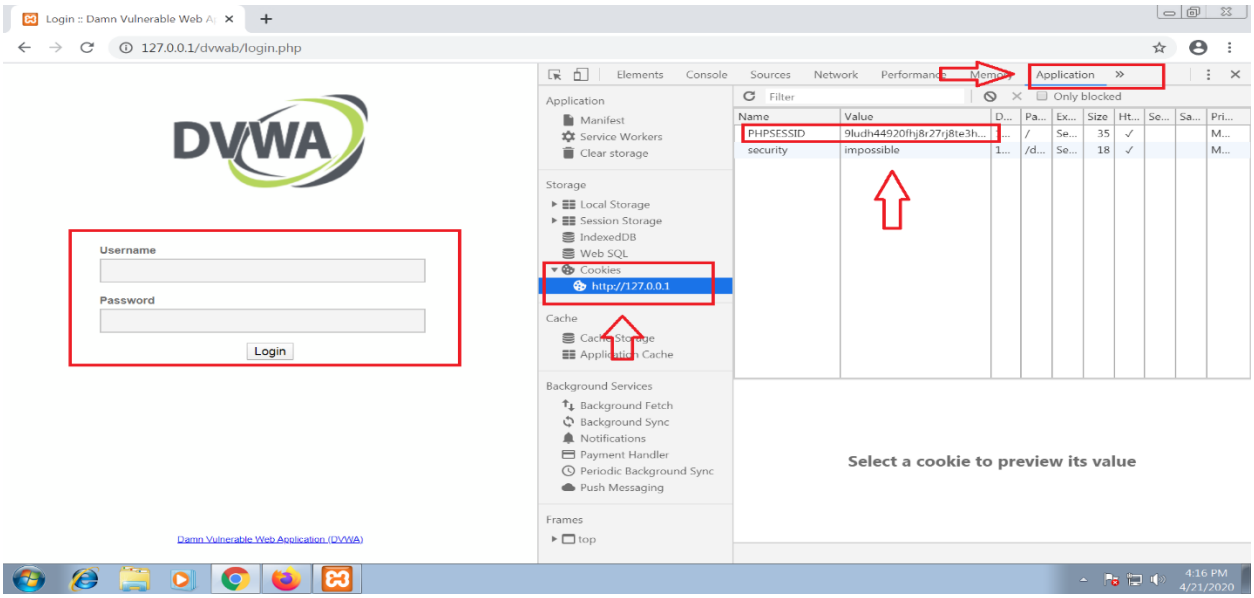
Step 3: Click on storage then cookies to get the value given to SESSID and copy that value from victims browser.



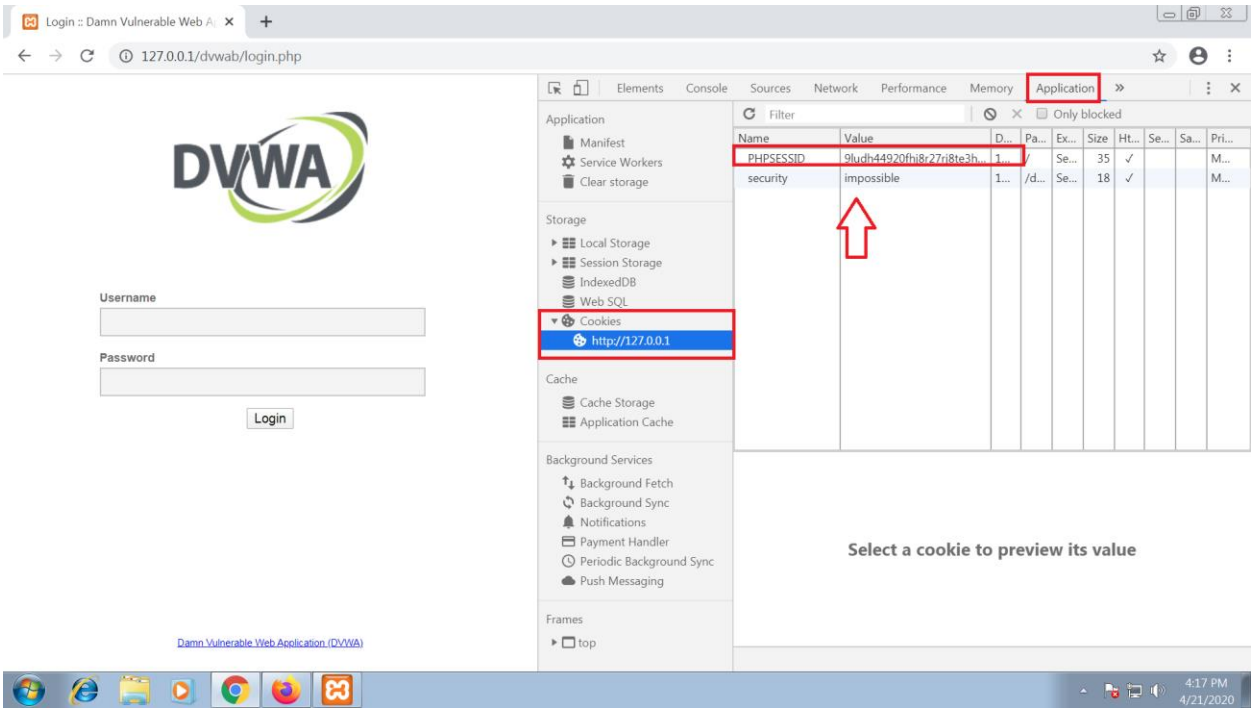
Step 4: Now open DVWA website on other browser i.e. of Attackers.



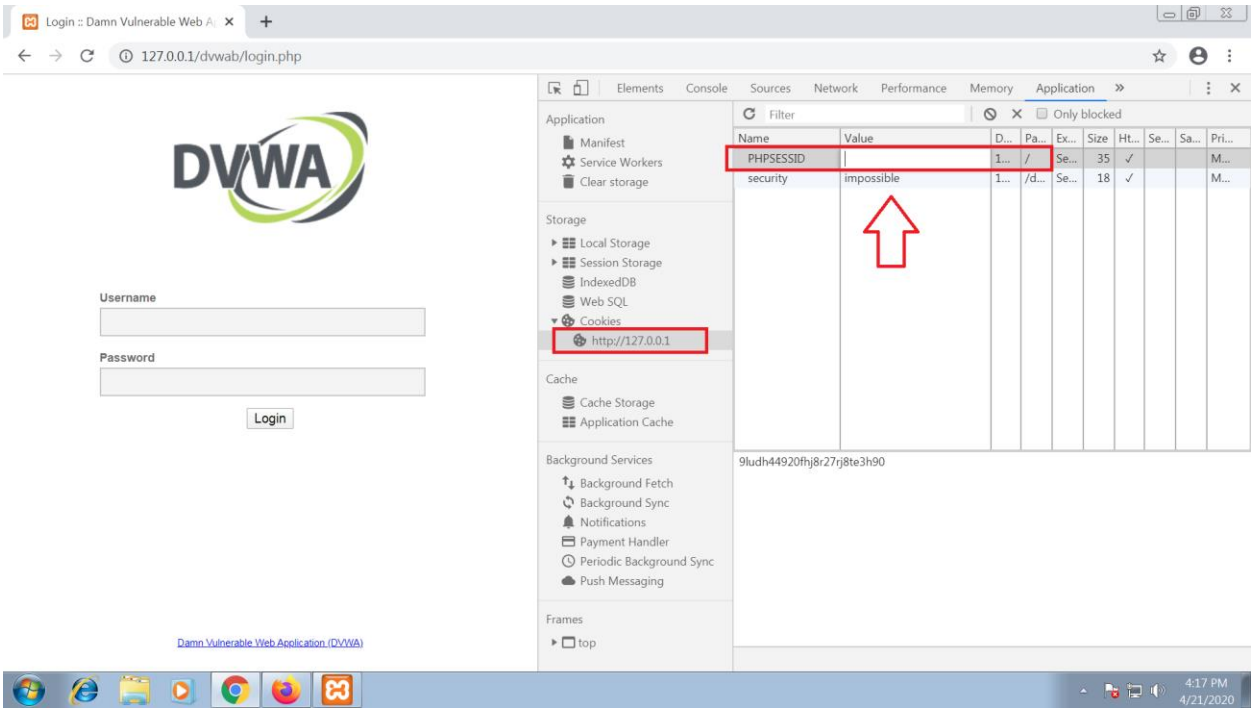
Step 5: Before login press Function Key+F12 to get the cookies detail of current session of DVWAB in attackers browser.



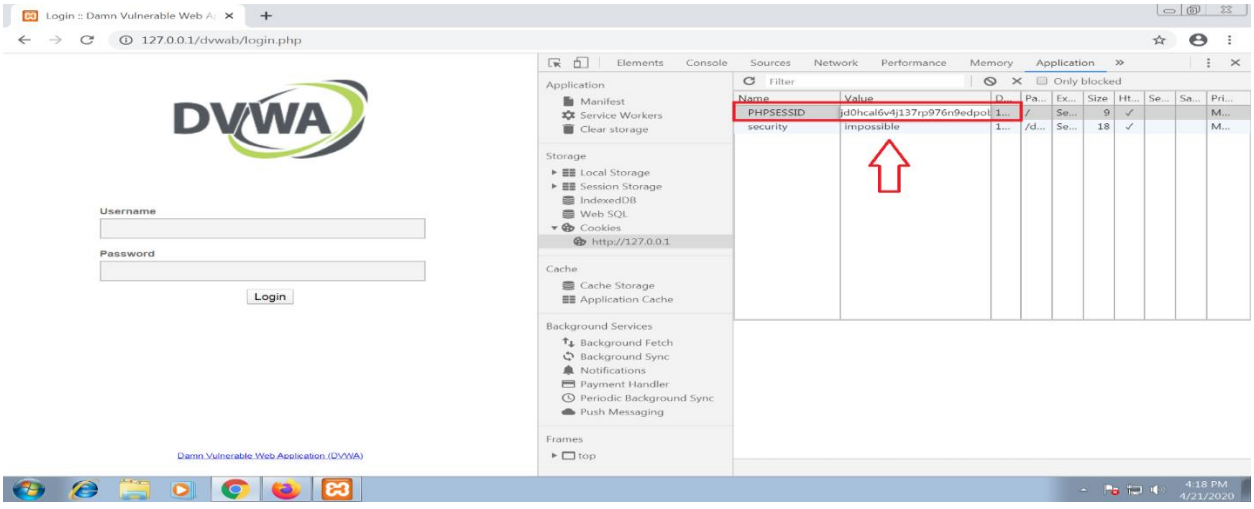
Step 6: Click on application and then on cookies to get the value of PHPSESSID.



Step 7: Remove the value given to PHPSESSID in attackers system.

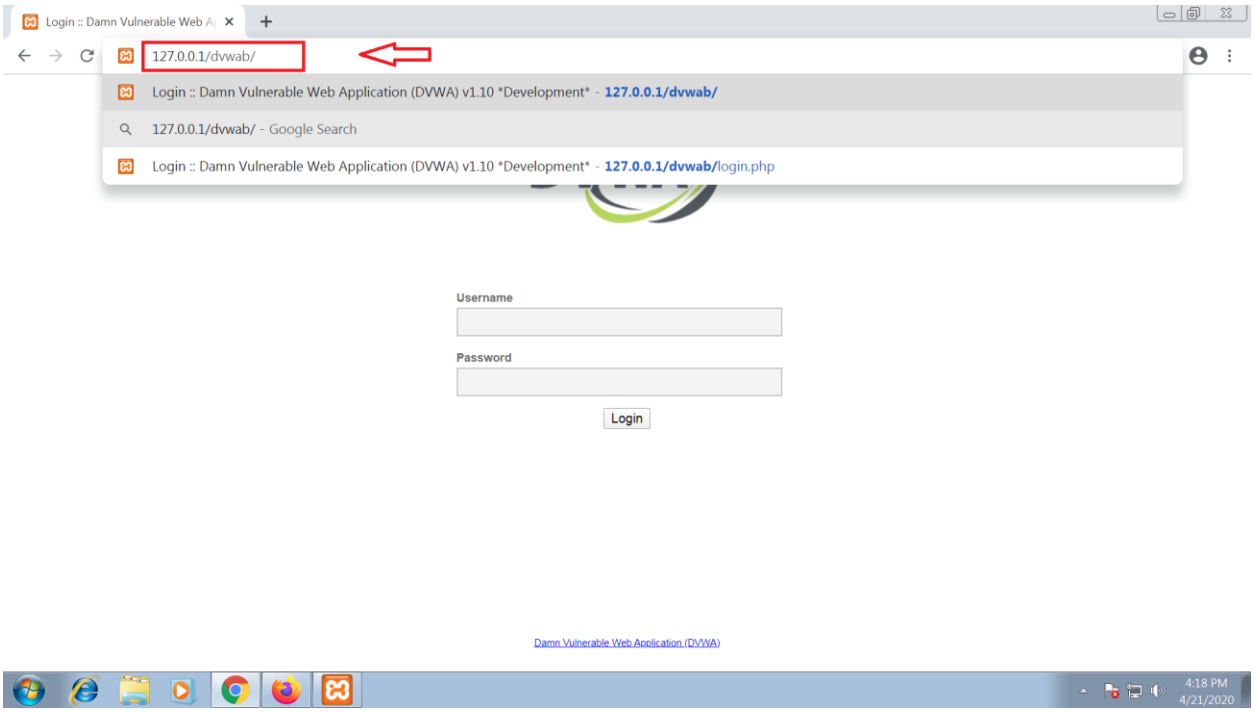


Step 8: Replace the PHPSESSID of attackers browser with victims value that is copied earlier.

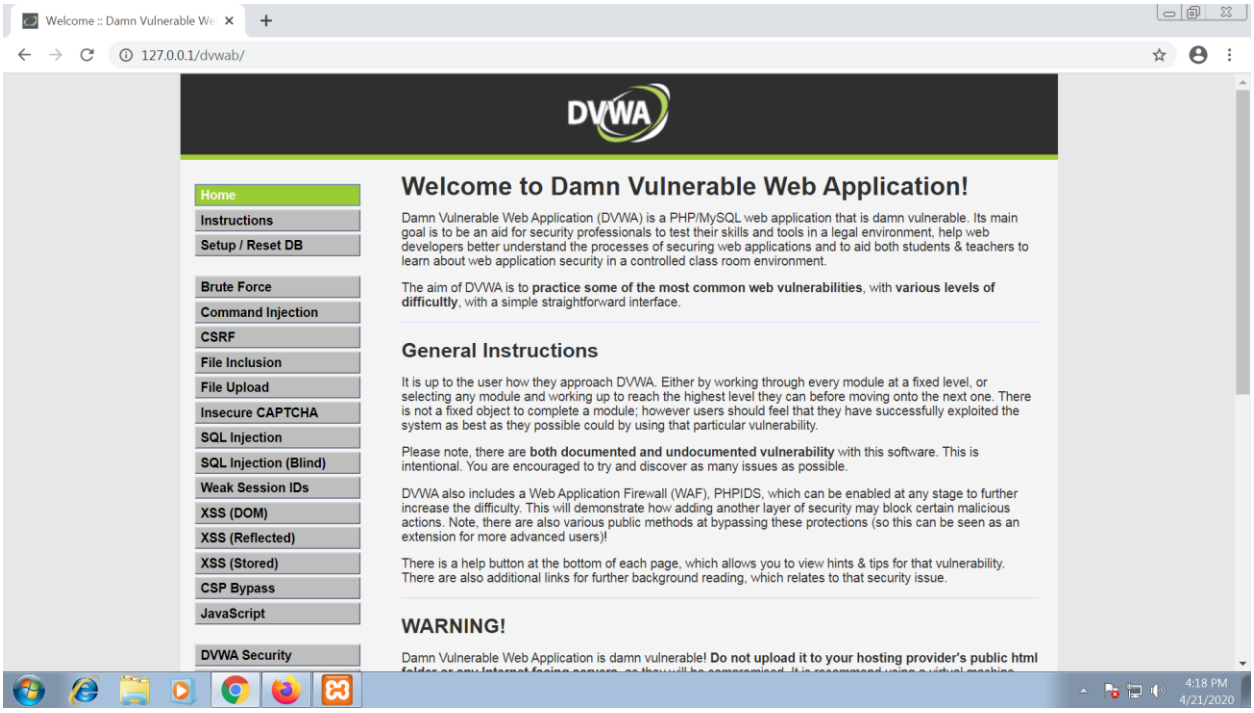


Step 9: In Attackers browser remove the login.php.

Step 10: As shown in the browser i.e. 127.0.0.1/dvwab/ press Enter.



Step 11: In Attackers browser we are loggin with Victims credentials by just replacing the PHPSESSID value.


Welcome :: Damn Vulnerable We
127.0.0.1/dvwab/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficultly, with a simple straightforward interface.
General Instructions
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.
Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.
WARNING!
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html
4:18 PM
4/21/2020