

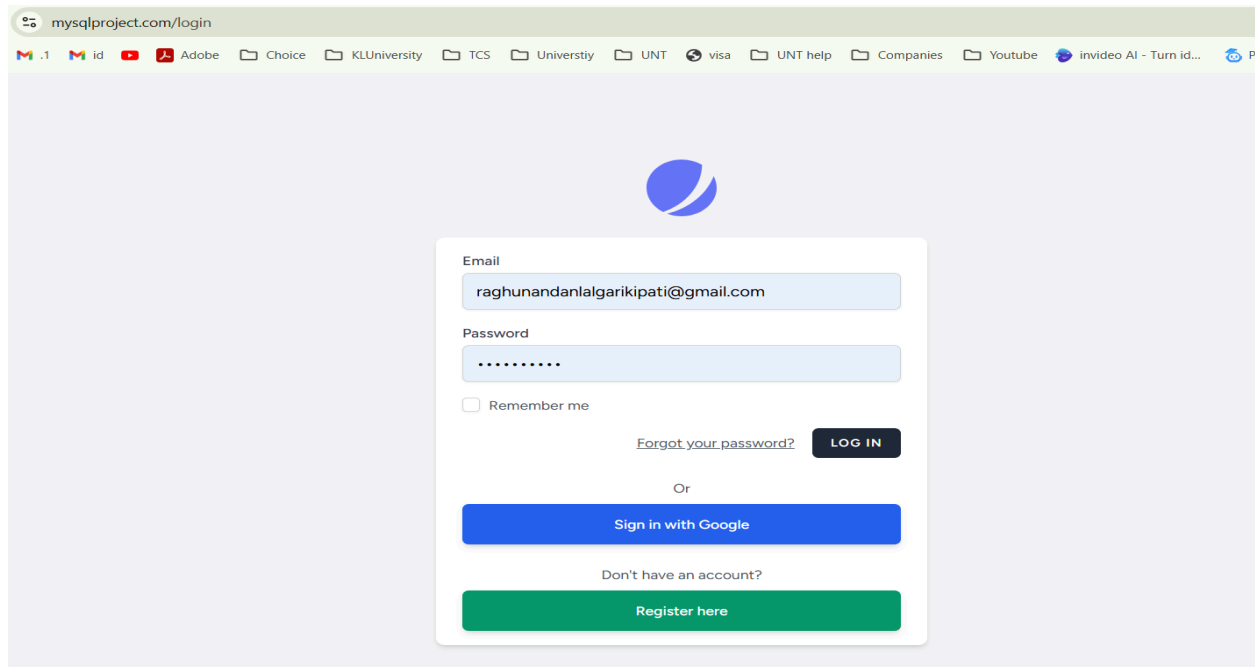
# Assignment: Vulnerability Assessment of Your Secure E-commerce Project

## MYSQL PROJECT APPLICATION REPORT

(<https://mysqlproject.com/>)

The website is live and hosted and also with SSL Certificate.

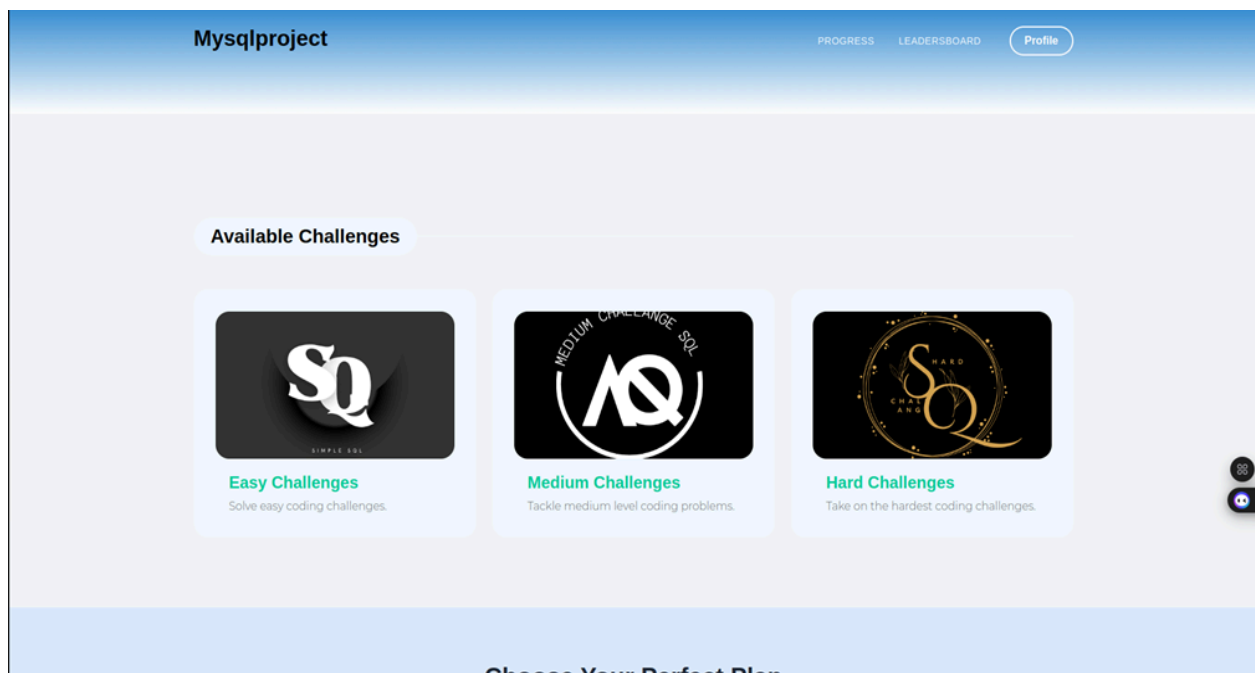
### Login Page



The screenshot shows the login page of the MySQL Project application. The browser address bar displays 'mysqlproject.com/login'. The page features a central login form with the following elements:

- Email:** A text input field containing 'raghunandanlalgarikipati@gmail.com'.
- Password:** A password input field with masked characters '.....'.
- Remember me:** An unchecked checkbox labeled 'Remember me'.
- Forgot your password?:** A link to the password recovery page.
- LOG IN:** A dark blue button to submit the login credentials.
- Or:** A separator text indicating alternative login methods.
- Sign in with Google:** A blue button for Google authentication.
- Don't have an account?:** A link to the registration page.
- Register here:** A green button for new user registration.

### Dashboard



The screenshot displays the user dashboard after a successful login. The interface includes a top navigation bar with the 'Mysqlproject' logo, links for 'PROGRESS' and 'LEADERBOARD', and a 'Profile' button. The main content area is titled 'Available Challenges' and presents three challenge levels:


- Easy Challenges:** Represented by a 'SQ' logo, with the description 'Solve easy coding challenges.'
- Medium Challenges:** Represented by an 'AQ' logo, with the description 'Tackle medium level coding problems.'
- Hard Challenges:** Represented by a 'SQ' logo with a crown, with the description 'Take on the hardest coding challenges.'

A footer section at the bottom of the dashboard is partially visible, titled 'Choose Your Perfect Plan'.

## Registration

mysqlproject.com/register

.1 id Adobe Choice KUNiversity TCS Universty UNT visa UNT help Companies Youtube invideo



Name

Email

Password

Confirm Password

[Already registered? Log in here](#) **REGISTER**

Or

**Sign in with Google**

## Multi-Factor Authentication

Assignment: Vulnerability Assessment Remediation plan: provide Vulnerability Assessment Request OTP Page Inbox (3) - raghunandanlalgarikipati

mysqlproject.com

Apps .1 id Adobe Choice KUNiversity TCS Universty UNT visa UNT help Companies Youtube invideo AI - Turn id... Phrasly AI - Login

### OTP Verification

Enter your email to request OTP:

**Request OTP**

Enter the OTP received in your email:

**Submit OTP**

# Problem Solving Environment

HomeAboutContact

SQL Practice Questions:

1. Create a Table

Create a table named **Students** with the following columns:

- **id** (INTEGER, Primary Key)
- **first\_name** (VARCHAR)
- **last\_name** (VARCHAR)
- **age** (INTEGER)
- **grade** (VARCHAR)

2. Insert Data

Insert the following records into the **Students** table:

- **id** = 1, **first\_name** = 'John', **last\_name** = 'Doe', **age** = 20, **grade** = 'A'
- **id** = 2, **first\_name** = 'Jane', **last\_name** = 'Smith', **age** = 22, **grade** = 'B'
- **id** = 3, **first\_name** = 'Sam', **last\_name** = 'Brown', **age** = 19, **grade** = 'C'

3. Update Data

Update the grade of the student with **id** = 2 to 'A'.

4. Delete Data

Delete the record of the student with **id** = 3.

5. Select Data

Write a query to select all students who are older than 20.

Write your SQL code here...

Run SQL Code

View Database

Show Solution

Output:

# Real Time Feedback

MySQL Project

SQL Execution Results

Execution ID: 6

Student ID: 8

SQL Code:

```
INSERT INTO Students (id, first_name, last_name,
VALUES
(1, 'John', 'Doe', 20, 'A'),
(2, 'Jane', 'Smith', 22, 'B'),
(3, 'Sam', 'Brown', 19, 'C');
```

Output:

SQL command executed successfully.

Created At:

26 Nov, 2024 07:05

Updated At:

26 Nov, 2024 07:05

Execution ID: 7

Student ID: 8

SQL Code:

```
CREATE TABLE Banks (
  bank_id INT PRIMARY KEY,
  name VARCHAR(100),
  location VARCHAR(100)
);
```

Output:

SQL command executed successfully.

Created At:

26 Nov, 2024 07:07

Updated At:

26 Nov, 2024 07:07

Execution ID: 8

Student ID: 8

SQL Code:

```
INSERT INTO Banks (bank_id, name, location) VALUES
(1, 'First National Bank', 'New York'),
(2, 'Global Bank', 'London');
```

Output:

SQL command executed successfully.

Created At:

26 Nov, 2024 07:08

Updated At:

26 Nov, 2024 07:08

© 2024 MySQL Project

## User Ranking

mysqlproject.com/rank

Mysqlproject

PROGRESS

LEADERSBOARD

Profile

### User Rankings

Rank	Username	Visualization
1	tonny blair	
2	bala_22	
3	pasala	
4	Rowdy	

## Payment Plan

Choose Your Perfect Plan

Select a subscription plan that suits your needs and enjoy premium features.

Free Trial

14-Day Free Trial

Get full access for 14 days—no credit card required!

Start Free Trial

Monthly Plan

\$10/month

Access all features with no commitment. Cancel anytime!

✓ Full access to all features

✓ No long-term commitment

✓ Cancel anytime

Subscribe Now

Yearly Plan

\$100/year

Best value! Save \$20 with our annual plan. Full access to all features.

✓ Full access to all features

✓ Save 20% with the annual plan

✓ Priority support

Get Started

# Profile

mysqlproject.com/profile

Home Profile Logout

## User Profile

**R**

Name: Raghu  
Email: raghunandanlalgarikipati@gmail.com  
Joined: 09 Nov, 2024  
Plan: 10 \$ monthly subscription active

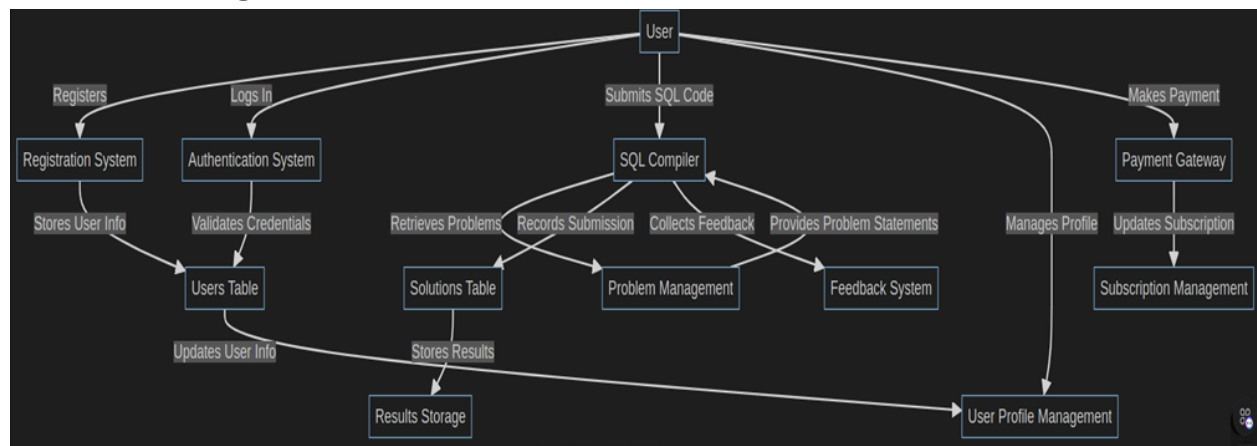
Name  
Raghu

Email  
raghunandanlalgarikipati@gmail.com

Update Profile

Current Password

## Data Flow Diagram



## Tool Selection: Industrial and Professional Tools for Vulnerability Assessment

1. HostedScan
2. Security Headers
3. OWASP ZAP (Zed Attack Proxy)

## HostedScan

Step 1- Open the website link on your browser <https://hostedscan.com/login>.

The screenshot shows the HostedScan dashboard. On the left is a sidebar with navigation links: Dashboard, Targets, Scans, Risks, Reports, Integrations, and Settings. The main area is titled 'Dashboard' and shows '0 scans in progress' and '3 scheduled scans'. Below this, a 'Risks detected' section shows a total of 25 risks, categorized by severity: Critical (0), High (0), Medium (19), Low (6), Accepted (0), and Closed (0). Below the risk categories are two tables: 'Recent Scans' and 'Recent Risks'. The 'Recent Scans' table lists scans for OWASP ZAP, OWASP ZAP Active, Nmap UDP, and Nmap, all with 'Overlimit' results. The 'Recent Risks' table lists vulnerabilities like 'OWASP ZAP Active Content Security Policy (CSP) Header Not Set' and 'OWASP ZAP Active Cookie No HttpOnly Flag'.

Step 2- In the dashboard, click on Targets and add Targets. Enter the URL of your website.

Step 3- In the dashboard, click on new Scan and select the required scans you want to run.

The screenshot shows the 'Select scans to run' page in HostedScan. The page has a sidebar with navigation links: Dashboard, Targets, Scans, Risks, Reports, Integrations, and Settings. The main area is titled 'Select scans to run' and has a 'Select All' checkbox. Below this, there are six scan options, each with a checkbox and a description: OpenVAS (Network Vulnerability Scan), OWASP ZAP (Passive Web Application Scan), OWASP ZAP Active (Active Web Application Scan), Nmap TCP (Port Scan), Nmap UDP (Port Scan), and Sslyze TLS/SSL (Encryption Security Scan). At the bottom, there are two buttons: 'API Security Scanning' and 'Internal Network Scanning (Beta)', both with 'Get Started' links.

Step 4- Next Configure the scan and click on start scan.

The screenshot shows the HostedScan interface with a sidebar on the left containing links to Dashboard, Targets, Scans, Risks, Reports, Integrations, and Settings. The main area displays a list of scans for the target `https://mysqlproject.com/`. The scans are as follows:


Scan Type	Target	Status	Report	Output	Time
Nmap UDP	<code>https://mysqlproject.com/</code>	Completed	Report	Output	11 minutes ago
Nmap	<code>https://mysqlproject.com/</code>	Completed	Report	Output	11 minutes ago
Sslyze	<code>https://mysqlproject.com/</code>	Overlimit			11 minutes ago
OpenVAS	<code>https://mysqlproject.com/</code>	Overlimit			11 minutes ago
Sslyze	<code>https://mysqlproject.com/</code>	Overlimit			1 day ago
OpenVAS	<code>https://mysqlproject.com/</code>	Completed	Report	Output	1 day ago
Sslyze	<code>https://mysqlproject.com/</code>	Completed	Report	Output	1 day ago
OWASP ZAP Active	<code>https://mysqlproject.com/</code>	Completed	Report	Output	1 day ago

Below the scans is a 'Scheduled Scans' section with the following table:

Target(s)	Scan	Schedule	Last ran	Next run
(all targets)	OpenVAS	Monthly		in 28 days
(all targets)	OWASP ZAP	Monthly		in 28 days

## Summary Report

- When we ran the nmap report on the website i found a total of **17 Medium** and **2 Low** Vulnerabilities in the TCP ports

 <https://mysqlproject.com/>

### Total Risks



Open TCP Ports	Severity	First Detected	Last Detected
Open TCP Port: 21	Medium	0 days ago	0 days ago
Open TCP Port: 110	Medium	0 days ago	0 days ago
Open TCP Port: 143	Medium	0 days ago	0 days ago
Open TCP Port: 995	Medium	0 days ago	0 days ago
Open TCP Port: 993	Medium	0 days ago	0 days ago
Open TCP Port: 2078	Medium	0 days ago	0 days ago
Open TCP Port: 2083	Medium	0 days ago	0 days ago
Open TCP Port: 2095	Medium	0 days ago	0 days ago
Open TCP Port: 2082	Medium	0 days ago	0 days ago
Open TCP Port: 2077	Medium	0 days ago	0 days ago
Open TCP Port: 2087	Medium	0 days ago	0 days ago
Open TCP Port: 2096	Medium	0 days ago	0 days ago
Open TCP Port: 2086	Medium	0 days ago	0 days ago
Open TCP Port: 1624	Medium	0 days ago	0 days ago
Open TCP Port: 25	Medium	0 days ago	0 days ago
Open TCP Port: 465	Medium	0 days ago	0 days ago
Open TCP Port: 587	Medium	0 days ago	0 days ago
Open TCP Port: 443	Low	0 days ago	0 days ago

- 2) When we ran the Active Web Application Vulnerabilities which is generally SQL injection, remote command execution, XSS, and more. I have found **2 Medium** and **4 Low** vulnerabilities in the Active web application.

3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
Missing Anti-clickjacking Header	Medium	1	0
Content Security Policy (CSP) Header Not Set	Medium	1	0
Cookie No HttpOnly Flag	Low	1	0
X-Content-Type-Options Header Missing	Low	1	0
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1	0
Strict-Transport-Security Header Not Set	Low	1	0

- 3) For both Network Vulnerability and SSL/TLS Security, we haven't found any sort of vulnerabilities.

3 SSL/TLS Security

The SSLyze security scan tests for misconfigured SSL/TLS certificates, expired certificates, weak ciphers, and SSL/TLS vulnerabilities such as Heartbleed.

3.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



3 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

3.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.





## Security Headers

Step 1- Open the website link on your browser <https://securityheaders.com>.

Step 2- Enter your Website URL in the input box.

Remediation plan: provide Vuln... x Vulnerability Assessment of You... x Analyse your HTTP response he... x +

securityheaders.com

Home About API

# Security Headers

by Probely, a snyk Business

## Scan your site now

Scan

☐ Hide results ☒ Follow redirects

### Grand Totals

A+	6,972,278
A	35,360,889
B	7,581,572
C	14,375,352
D	35,075,313
E	9,342,559
F	136,830,258
R	47,323,417
<b>Total</b>	<b>292,861,638</b>

### Recent Scans

www.bxlm100.com	F
www.iliilli.com	D
zh-cn.queenmobile....	F
mp4gain.com	F
mindfulacademy.fr	F
bookmarkinform.inf...	D
belair19theater.co...	D
preprod-api.secuna...	A
adocday.com	A

### Hall of Fame

preprod-api.secuna...	A
adocday.com	A
areon-ua.com	A
wolfram-ua.com	A
cursoos.so.enf.br	A
petnet.com.ph	A
www.eptarefrigerat...	A
ava.souenfermagem...	A
www.souenfermagem...	A

### Hall of Shame

www.bxlm100.com	F
zh-cn.queenmobile....	F
mp4gain.com	F
mindfulacademy.fr	F
www.airsoftmarkt.n...	F
v2v.in	F
pasarinko.zeroweb...	F
internetjo.iwinv.n...	F
la.queenmobile.org	F

Step 3- Now click the Scan button to begin.

Step 4- This tool scans for the HTTP response headers which are sent by web servers to improve the security of web applications.

## Summary Report


Scan your site now

https://mysqlproject.com/

Scan

☐ Hide results

☒ Follow redirects



Security Report Summary

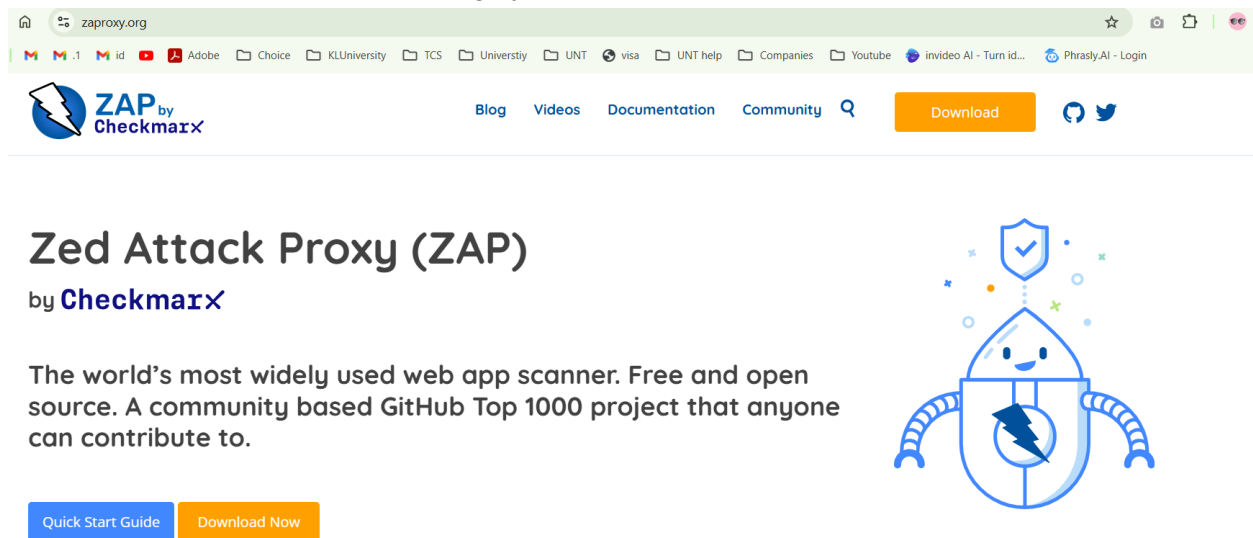
Site:	<a href="https://mysqlproject.com/login">https://mysqlproject.com/login</a>
IP Address:	51.255.149.48
Report Time:	01 Dec 2024 23:17:13 UTC
Headers:	<div><div>✖ Strict-Transport-Security</div><div>✖ Content-Security-Policy</div><div>✖ X-Frame-Options</div><div>✖ X-Content-Type-Options</div><div>✖ Referrer-Policy</div><div>✖ Permissions-Policy</div></div>
Advanced:	<div>Ouch, you should work on your security posture immediately:</div> <div>Start Now</div>

Missing Headers	
<b>Strict-Transport-Security</b>	<a href="#">HTTP Strict Transport Security</a> is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".

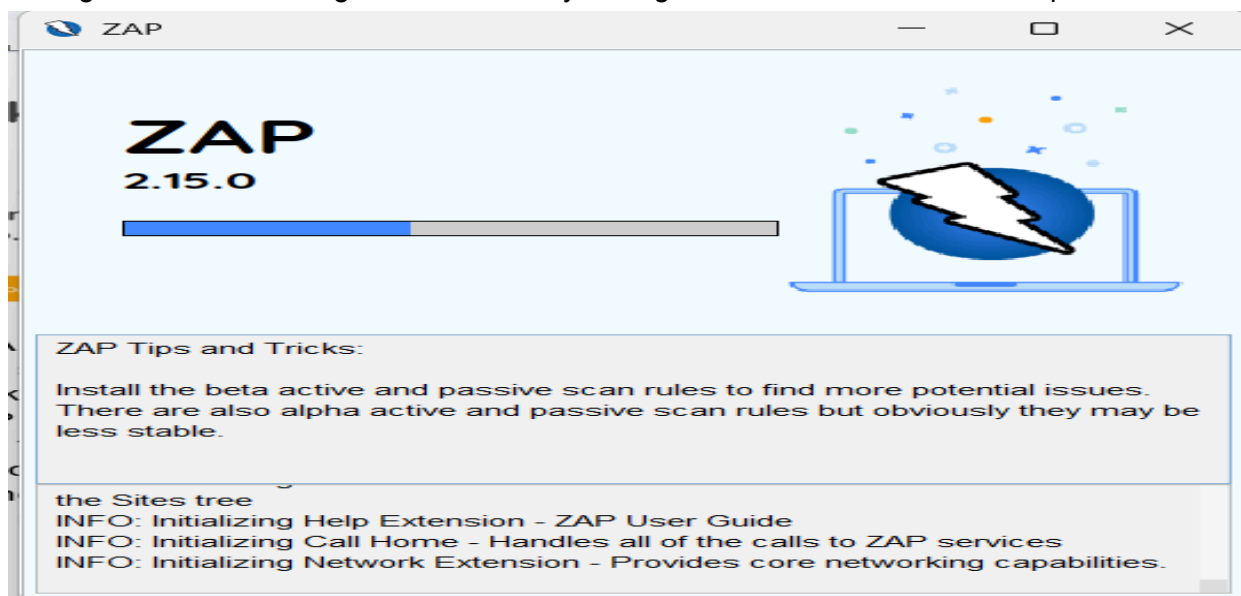
- 1) The report says that there is no cookie prefix on the cookies. This could lead to security risks. To overcome this we need to implement cookie prefixes.
- 2) The report says there are missing Security Headers and this leads to various attacks on the website. To overcome this we need to implement a Strict Transport Security Header to strengthen the TLS of the website.

## OWASP ZAP (Zed Attack Proxy)

Step 1– Go to the website at <https://www.zaproxy.org>.  
and then select the specific operating system and download and install it,



Step 2- Launch ZAP. By default, it uses the IP address 127.0.0.1 and port 8080. Open your browser's network settings and configure it to route traffic through ZAP. For Firefox, go to Settings > Network Settings > Manual Proxy Configuration, and enter the IP and port.



Step 3- In OWASP ZAP, navigate to the Automated Scan section. Enter the URL of the website you want to test in the "URL to Attack" field. Depending on your needs, you can select a Passive Scan, which observes traffic as you browse or an Active Scan which probes the application for vulnerabilities.

The screenshot shows the OWASP ZAP Automated Scan configuration window. The 'URL to attack' field is populated with 'https://mysqlproject.com/'. The 'Use traditional spider' checkbox is checked. The 'Use ajax spider' dropdown is set to 'Always' with 'Firefox Headless' selected. The 'Attack' button is highlighted. The 'Progress' bar shows 'Not started'. Below the interface, a table displays scan results for two requests to the login page, both returning 200 OK status codes.

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Proxy	30/11/24, 1:47:28 PM	GET	https://mysqlproject.com/login	200	OK	952 ms	4,859 bytes	Medium		AntiCSRF, Comment, For...
44	Proxy	30/11/24, 1:49:23 PM	GET	https://mysqlproject.com/login/	200	OK	1.59 s	1,556 bytes	Medium		Form, Hidden, Script

## Summary Report

- 1) Through the ZAP Active scan I have found that there are a variety of HTTP status codes and also there are few resources which could not be found on the server.
- 2) I have found a few vulnerabilities where few posts return 419 proxy authentication required which actually tells that the requests are being blocked through a proxy server.
- 3) I also found there are few improper URL formatting or routing.
- 4) Through ZAP Ajax Scan I have found that the scan has successfully received a 200 OK response and is functioning correctly.