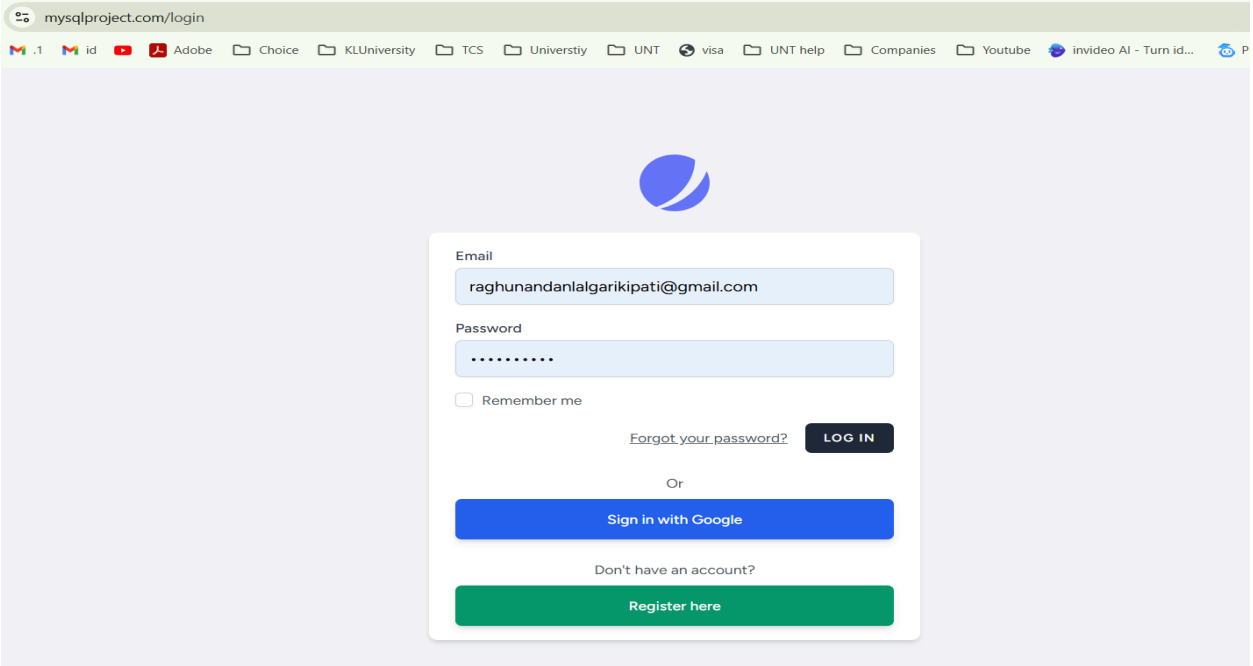
Assignment: Vulnerability Assessment of Your Secure E-commerce Project

MYSQL PROJECT APPLICATION REPORT

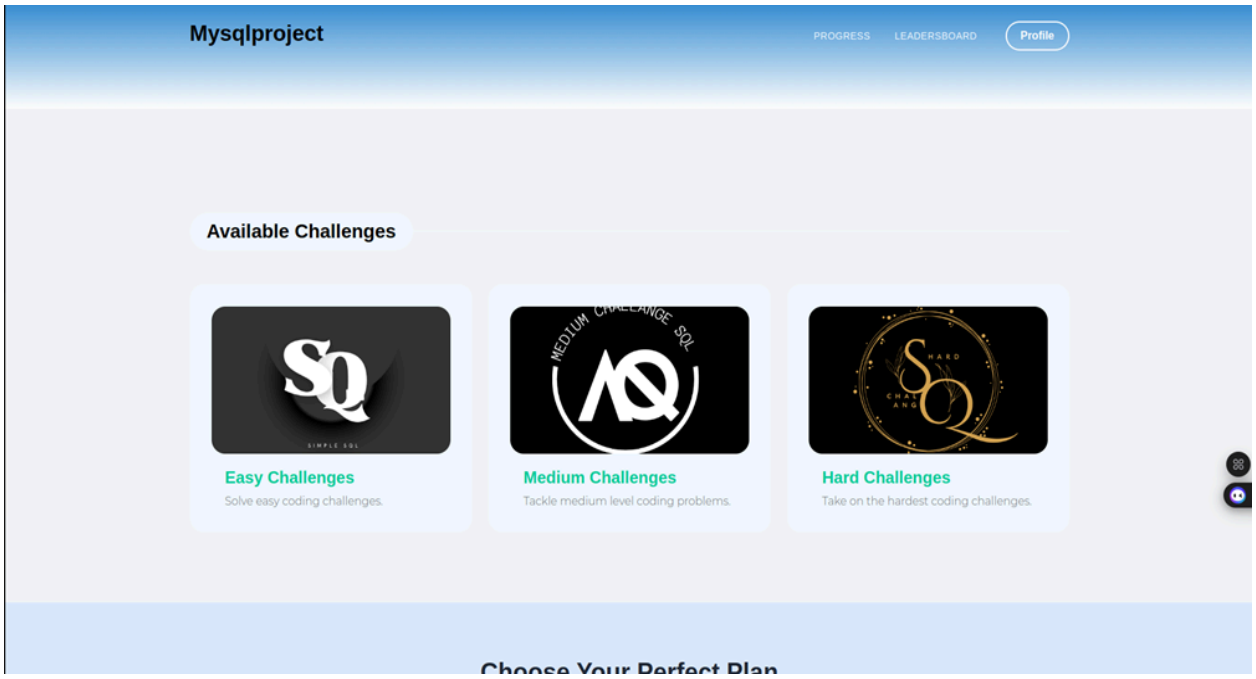
(https://mysqlproject.com/)

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

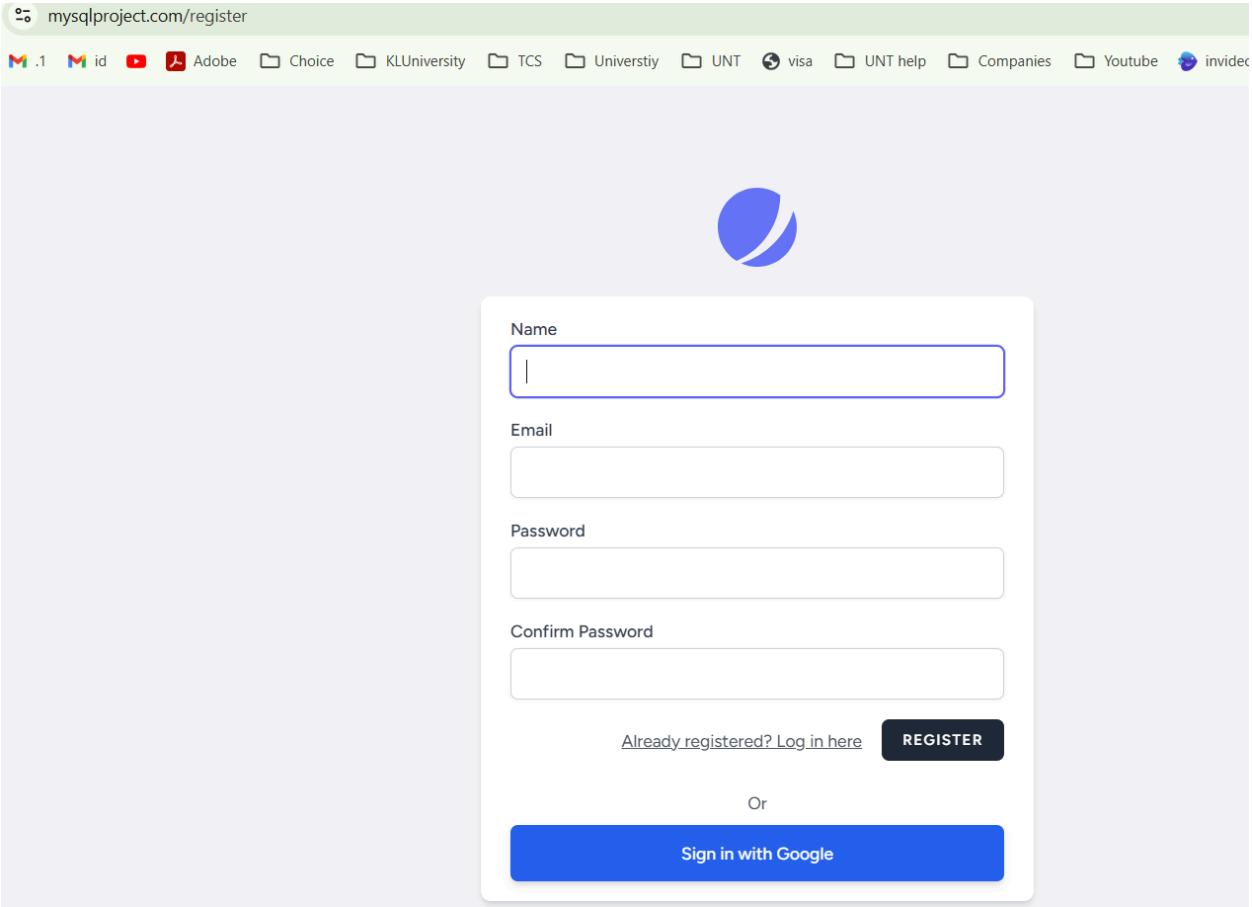
Login Page



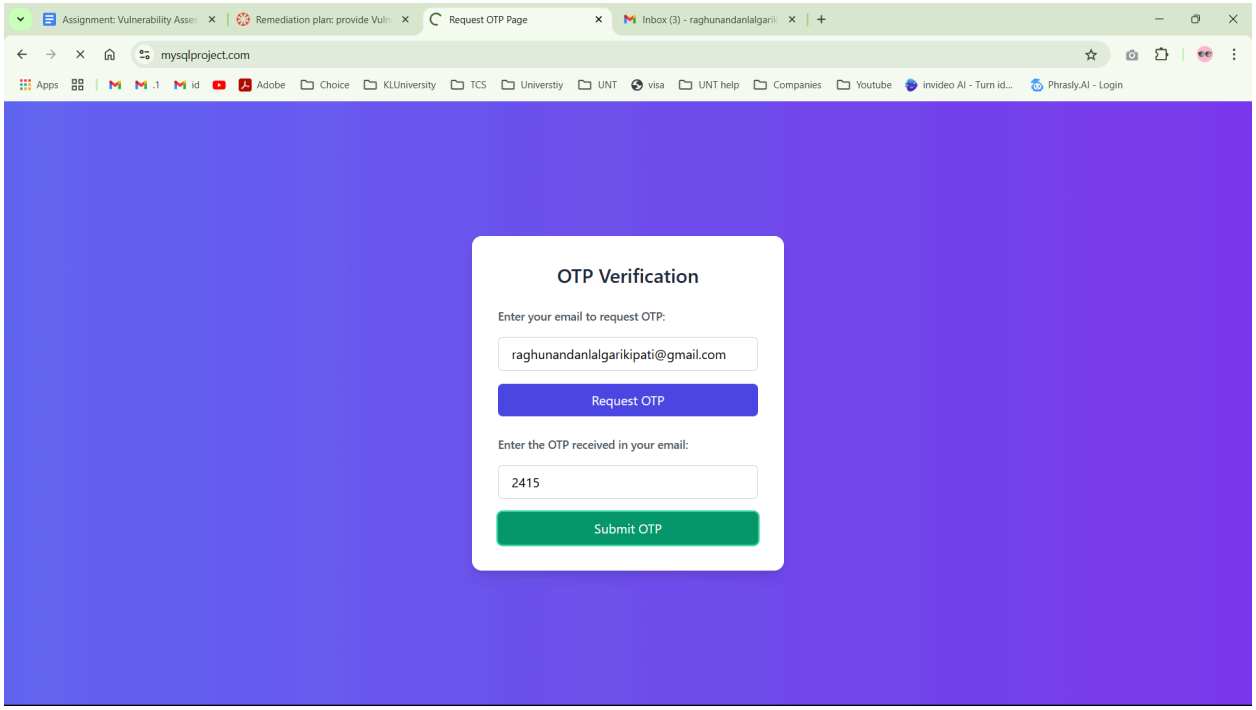
Dashboard



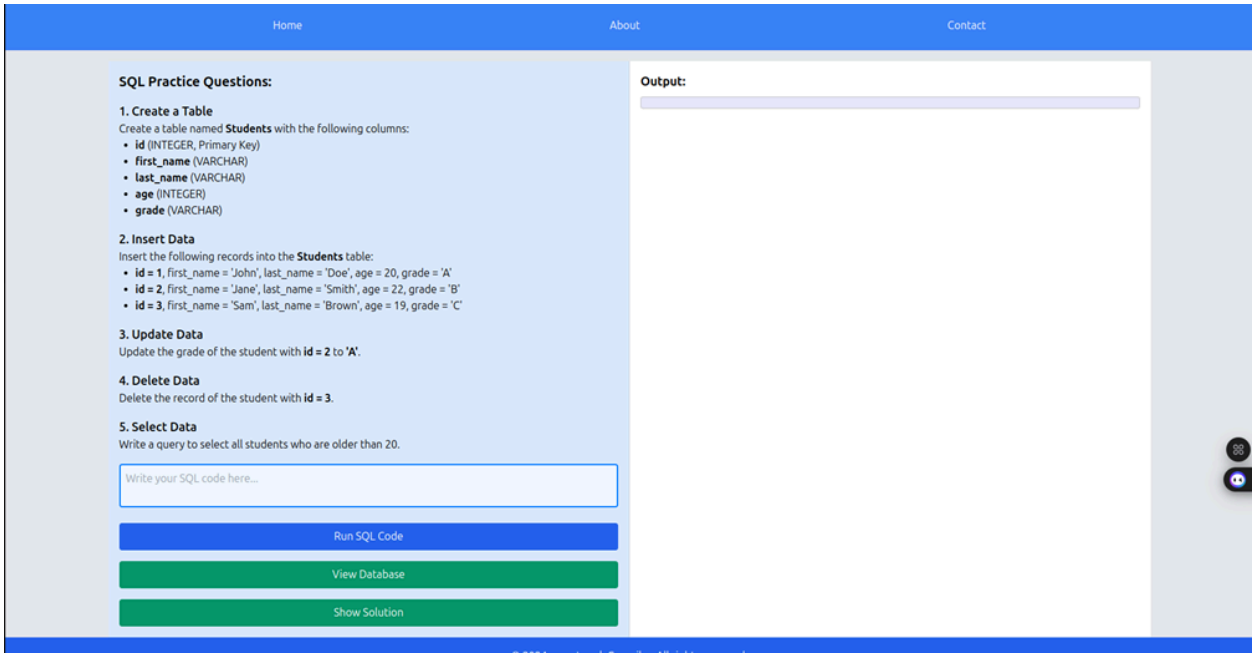
Registration



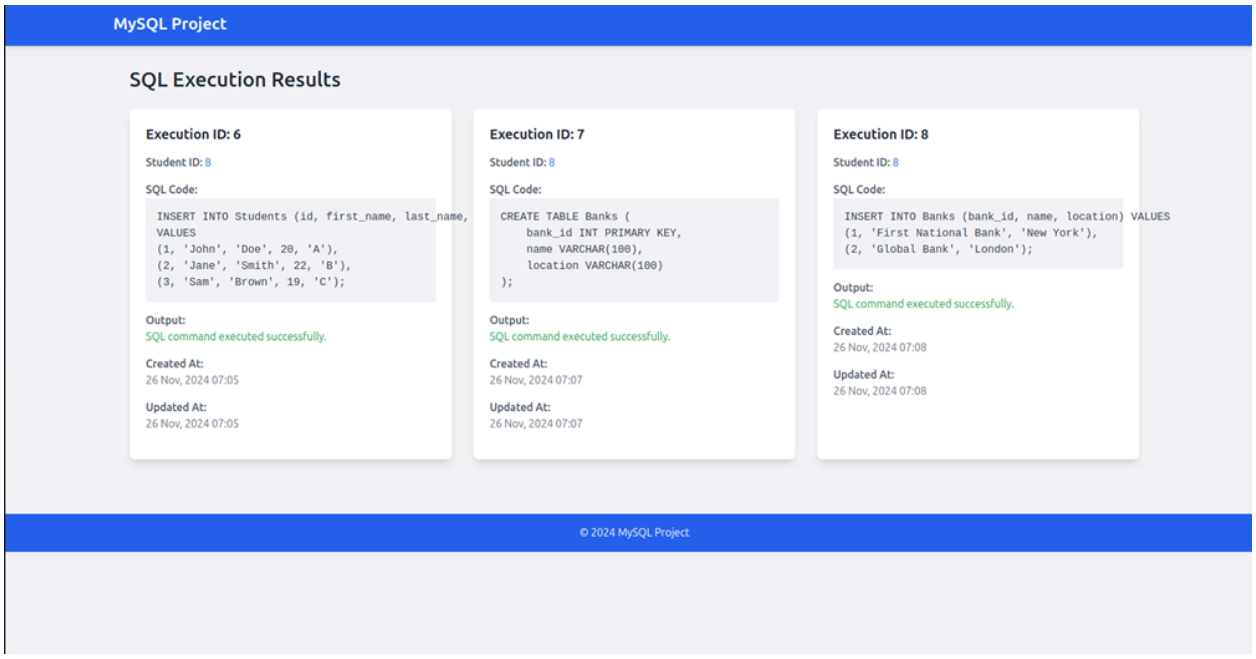
Multi-Factor Authentication



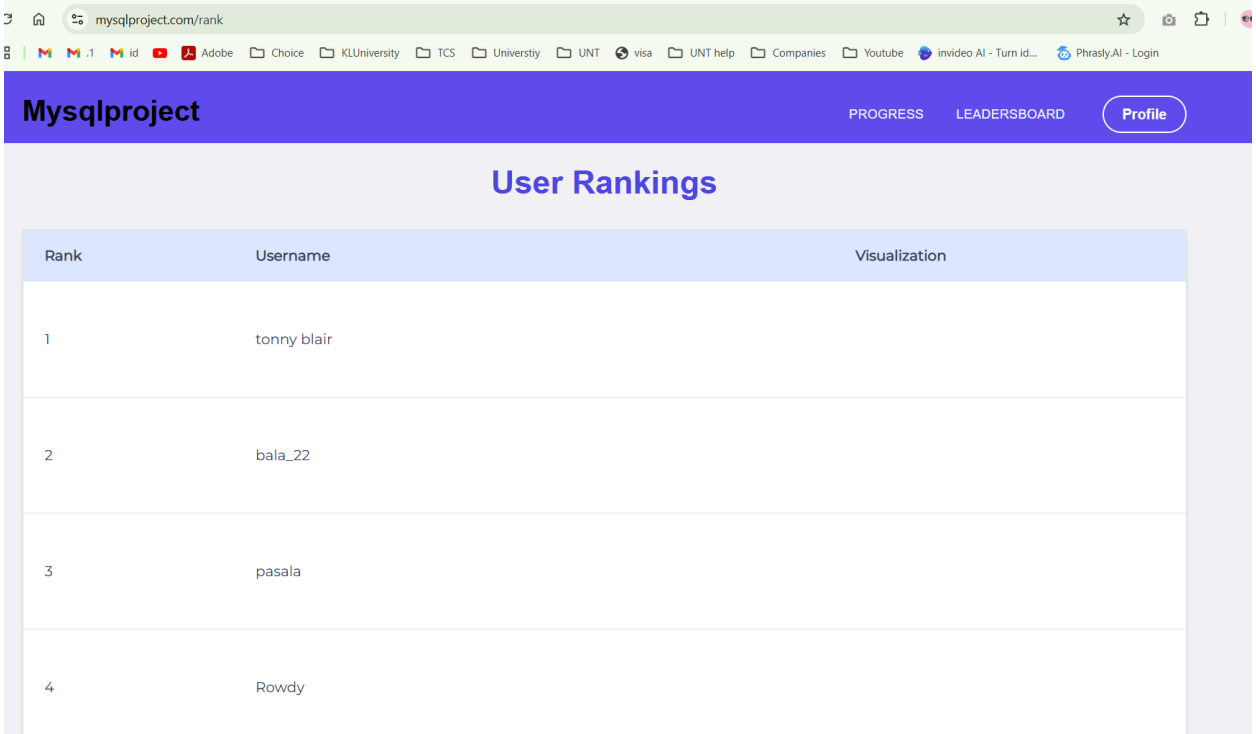
Problem Solving Environment



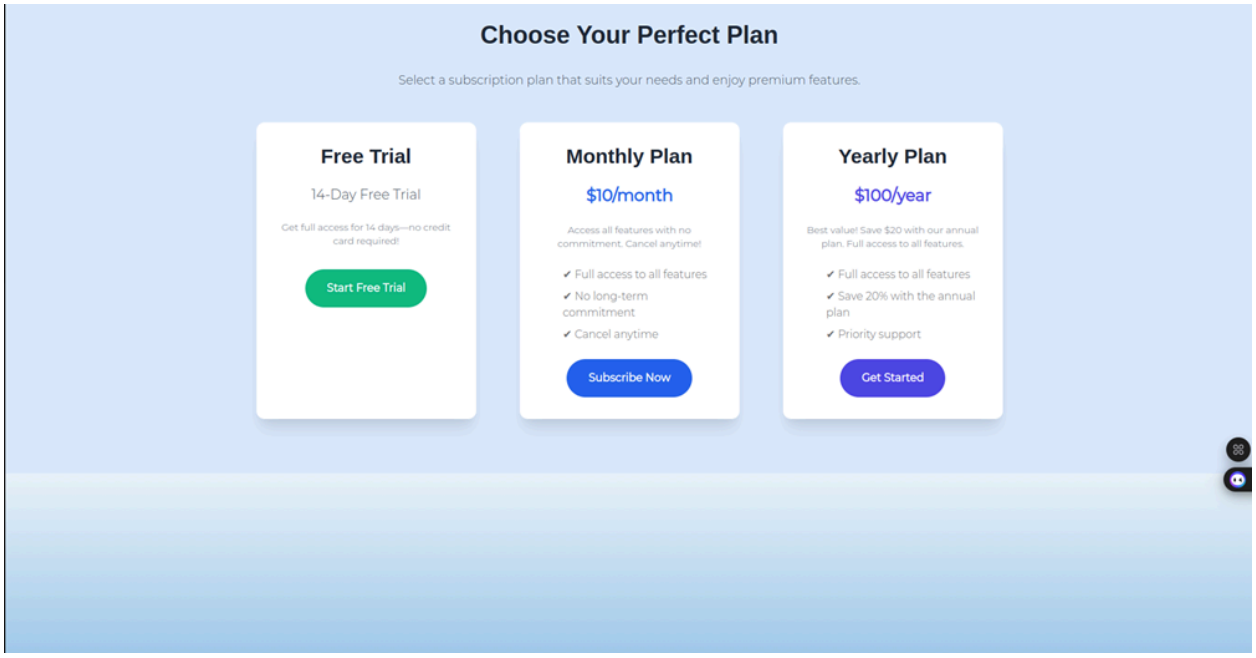
Real Time Feedback



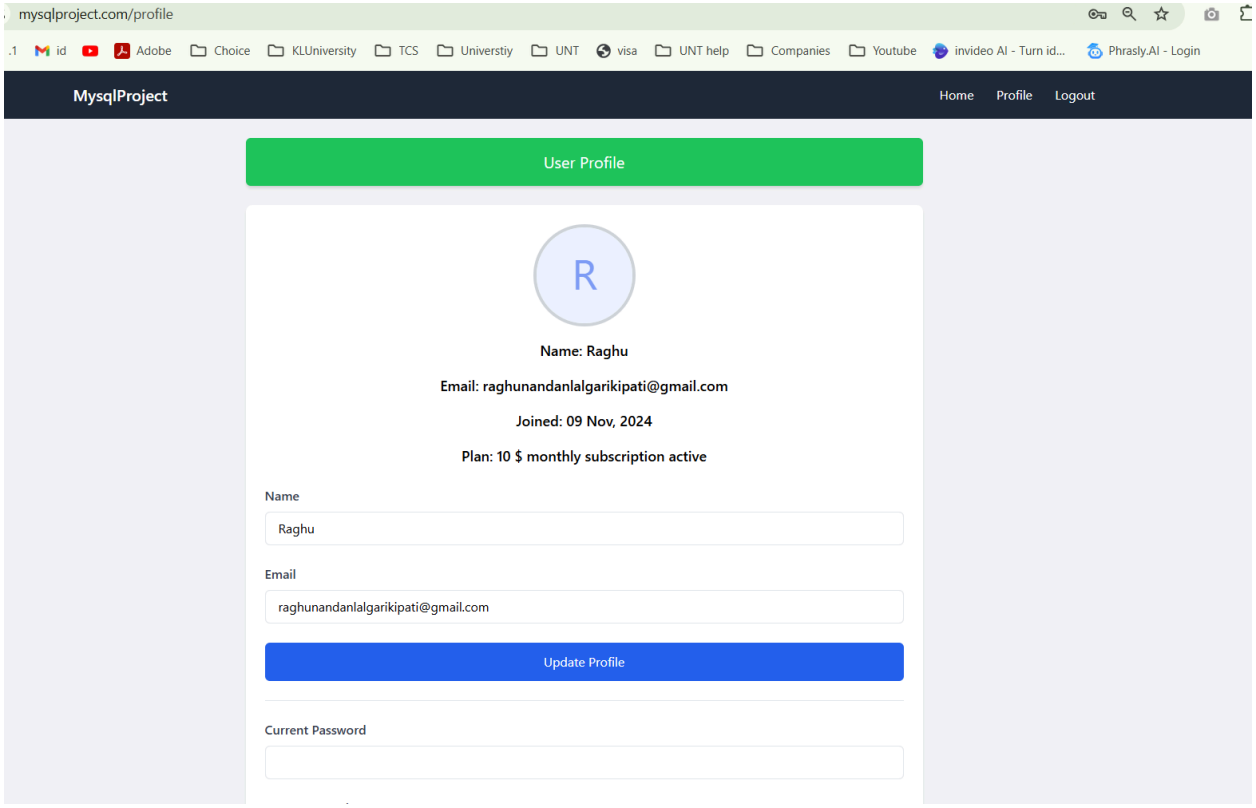
User Ranking



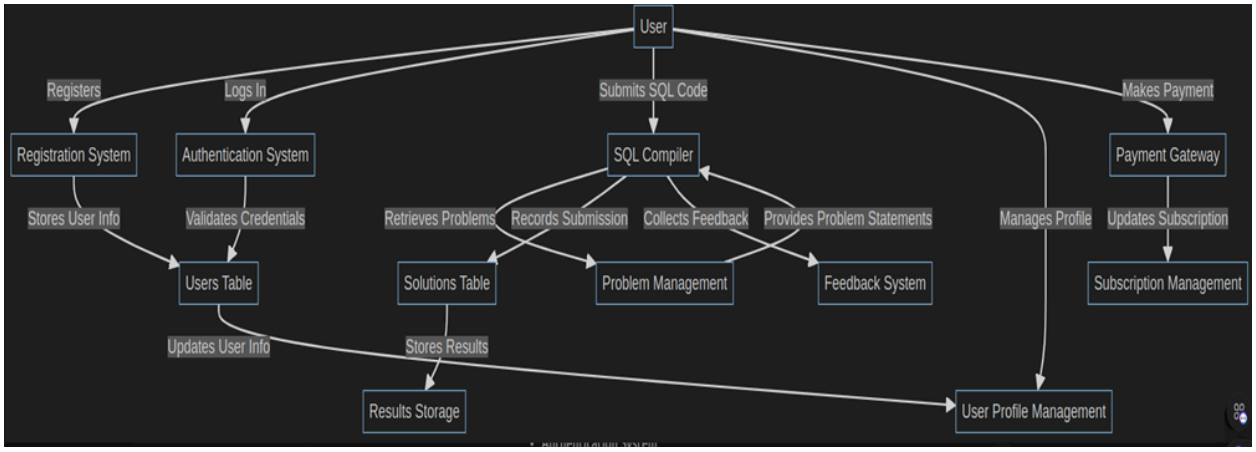
Payment Plan



Profile



Data Flow Diagram

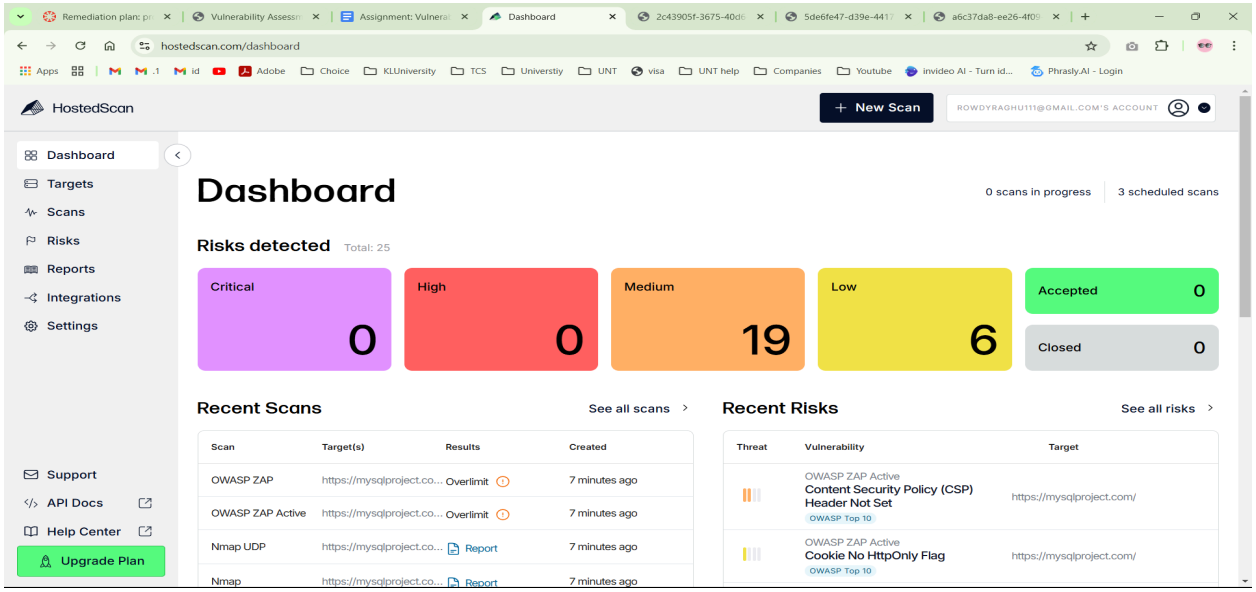


Tool Selection: Industrial and Professional Tools for Vulnerability Assessment

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

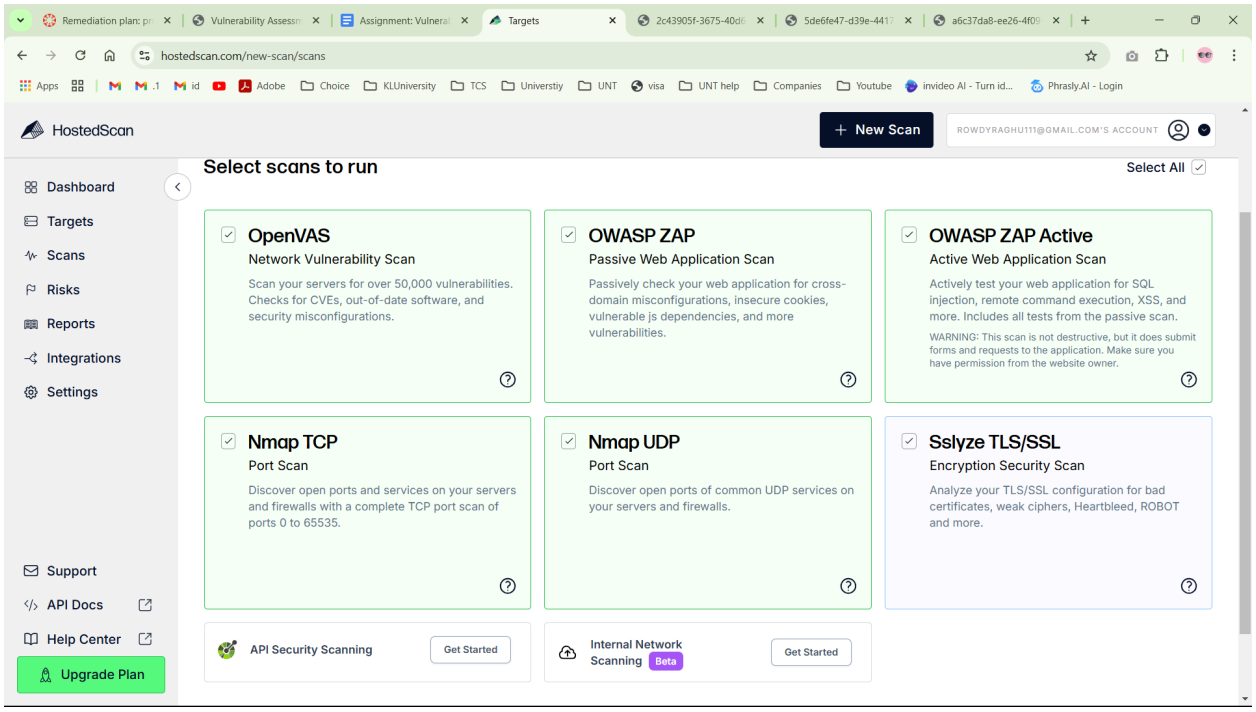
HostedScan

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

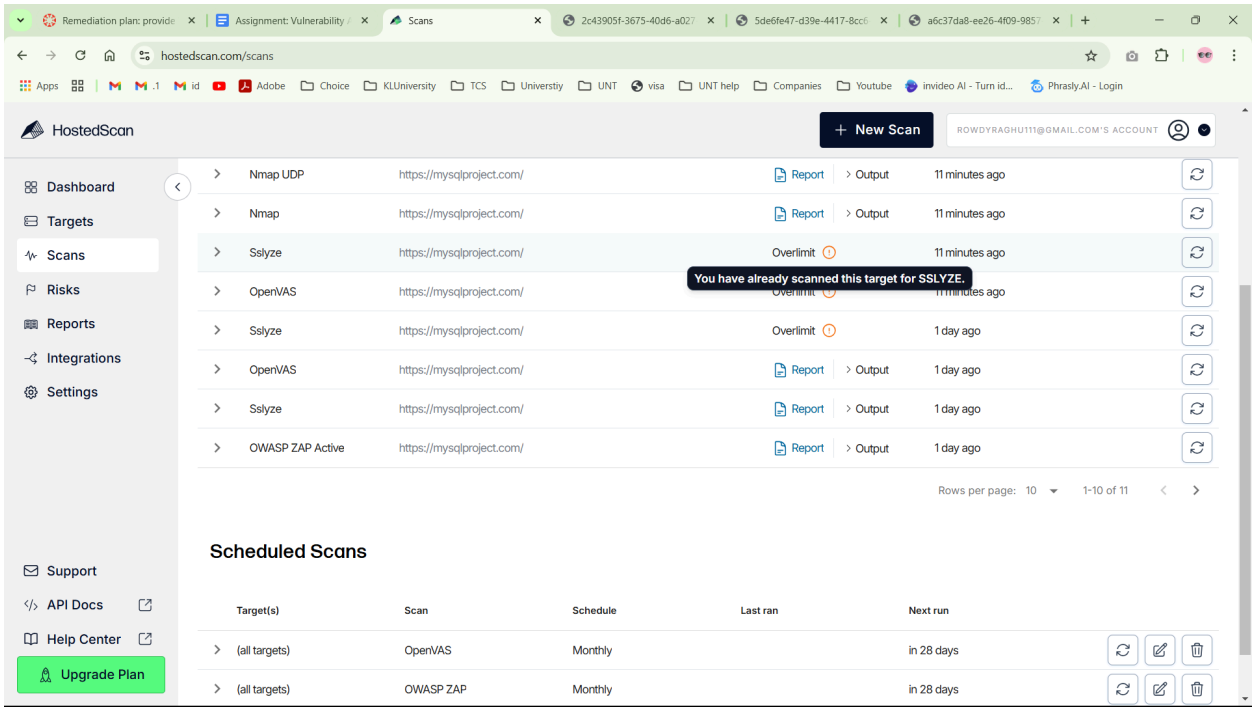


Step 2- In the dashboard, click on Targets and add Targets. Enter the URL of your website.

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



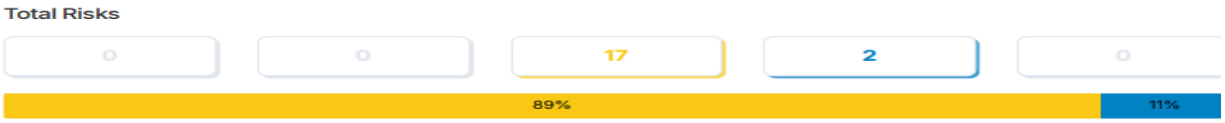
Step 4- Next Configure the scan and click on start scan.



Summary Report

1) 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/



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.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

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

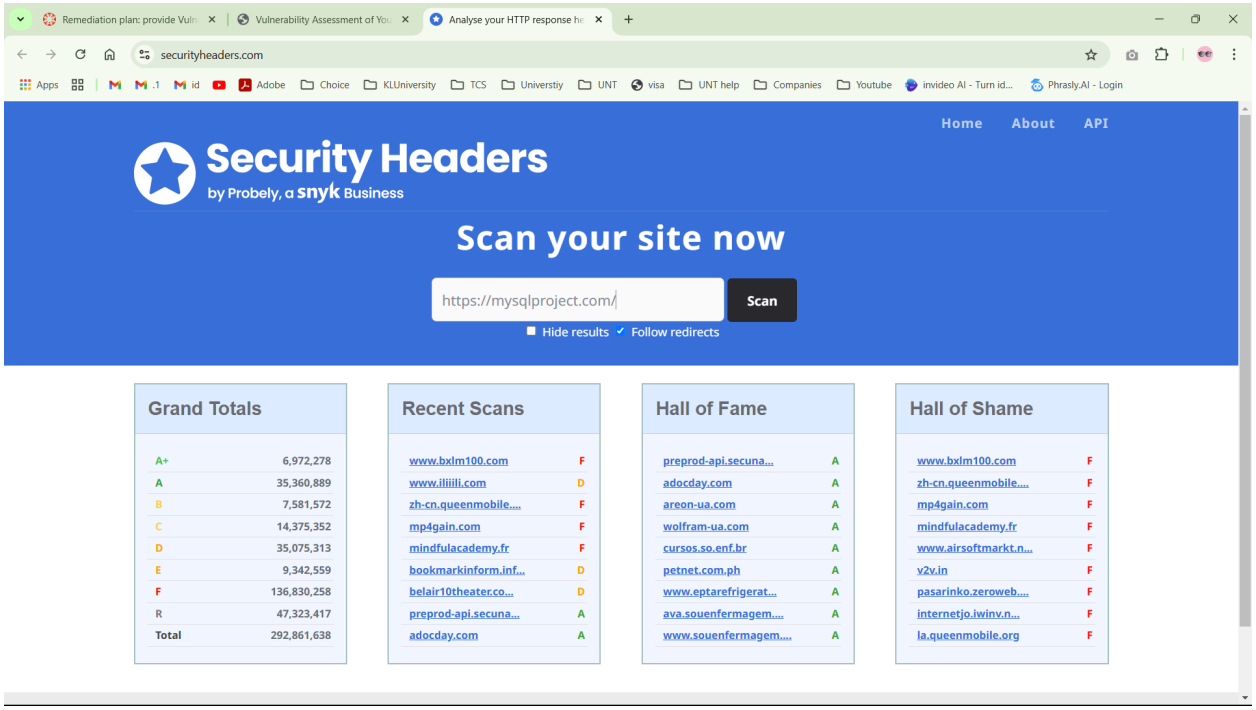
Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	0	0

Security Headers

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

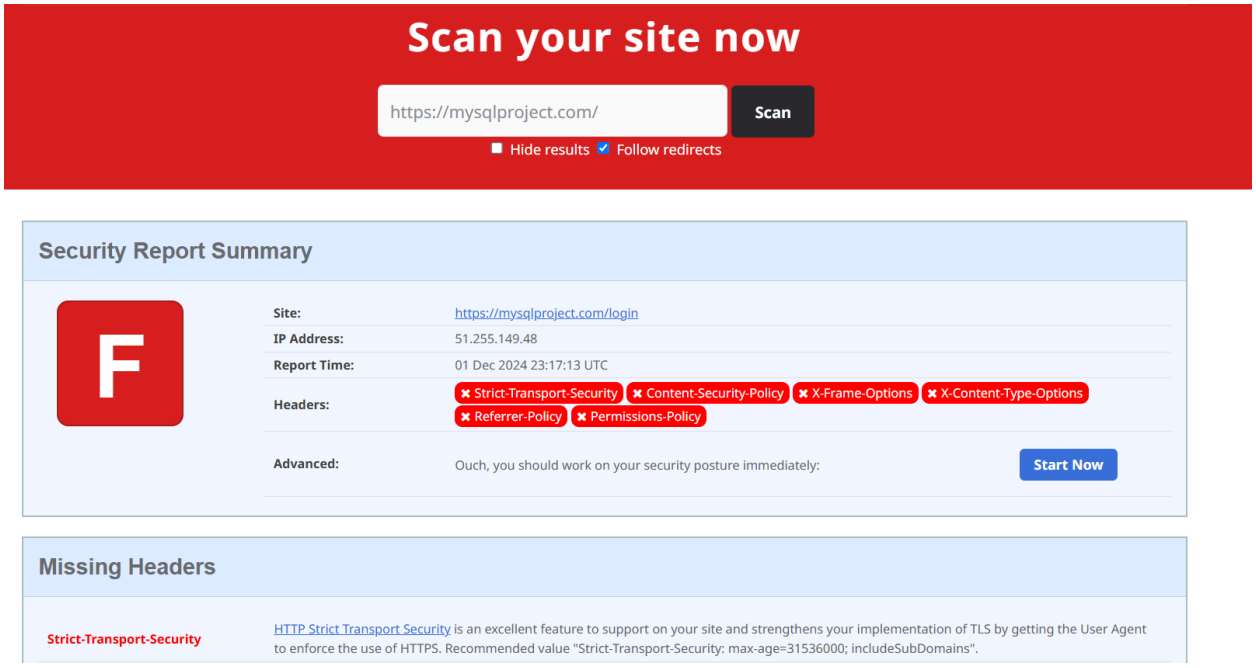
Step 2- Enter your Website URL in the input box.



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.

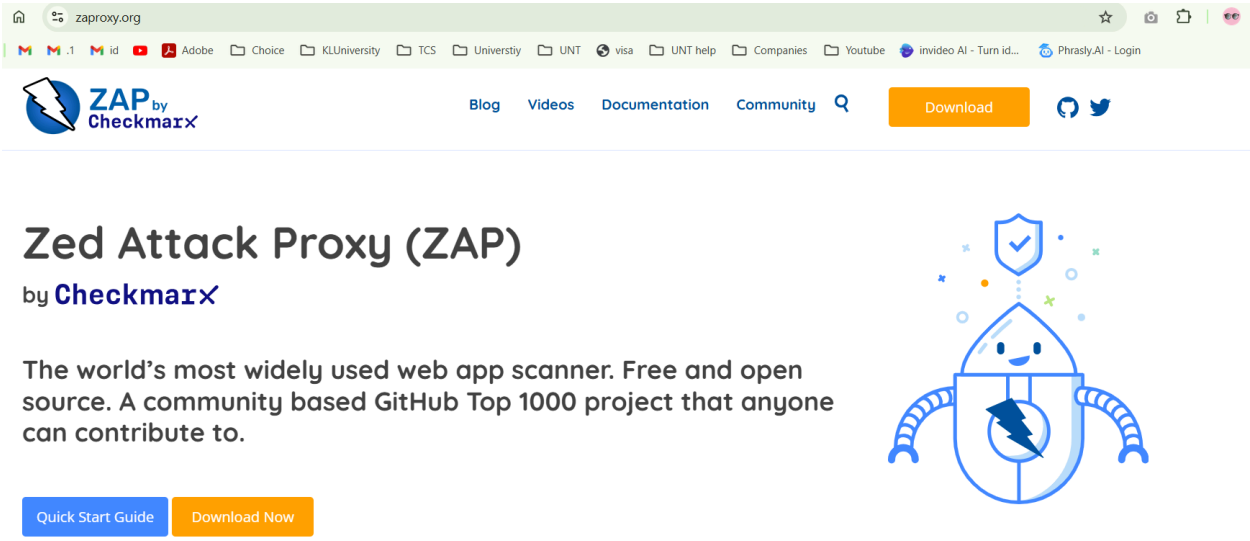
Summary Report



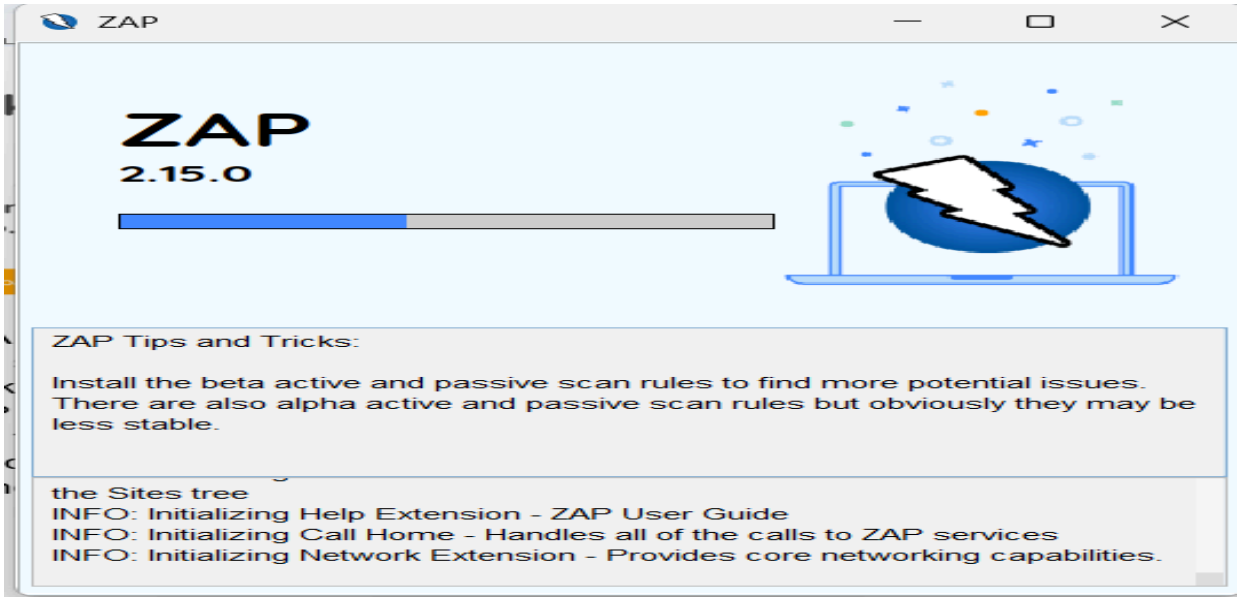
1) The report says that there is no cookie prefix on the cookies. This could lead to security risks. To overcome this we need to implement cookie prefixes.
2) The report says there are missing Security Headers and this leads to various attacks on the website. To overcome this we need to implement a Strict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

OWASP ZAP (Zed Attack Proxy)

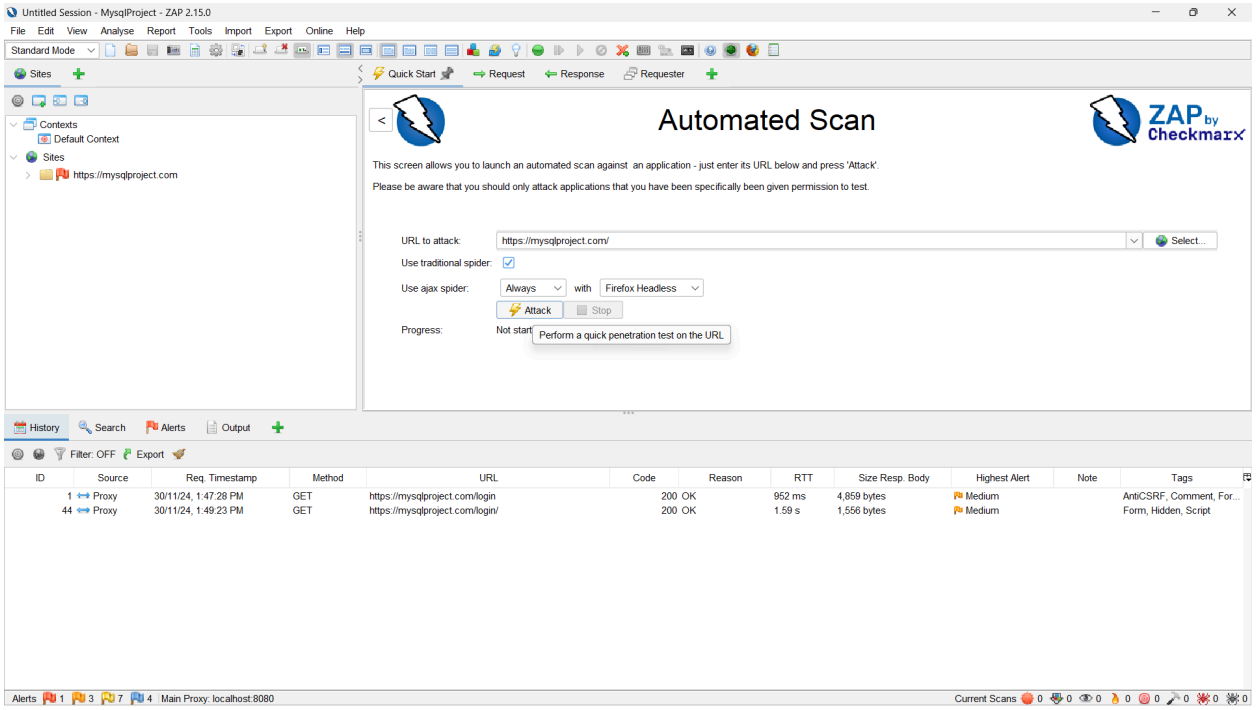
Step 1– Go to the website at https://www.zaproxy.org.
and then select the specific operating system and download and install it,



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.



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 Azax Scan I have found that the scan has successfully received a 200 OK response and is functioning correctly.