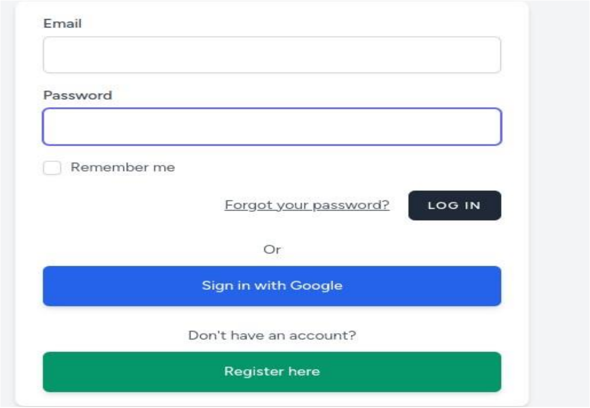
Name: Naveen Kumar Reddy Bhavanam

Student id :11823630

Vulnerability Assessment of Secure E-commerce Project

Preparation:

https://mysqlproject.com/



Email

Password

□ Remember me

Forgot your password? LOG IN

Or

Sign in with Google

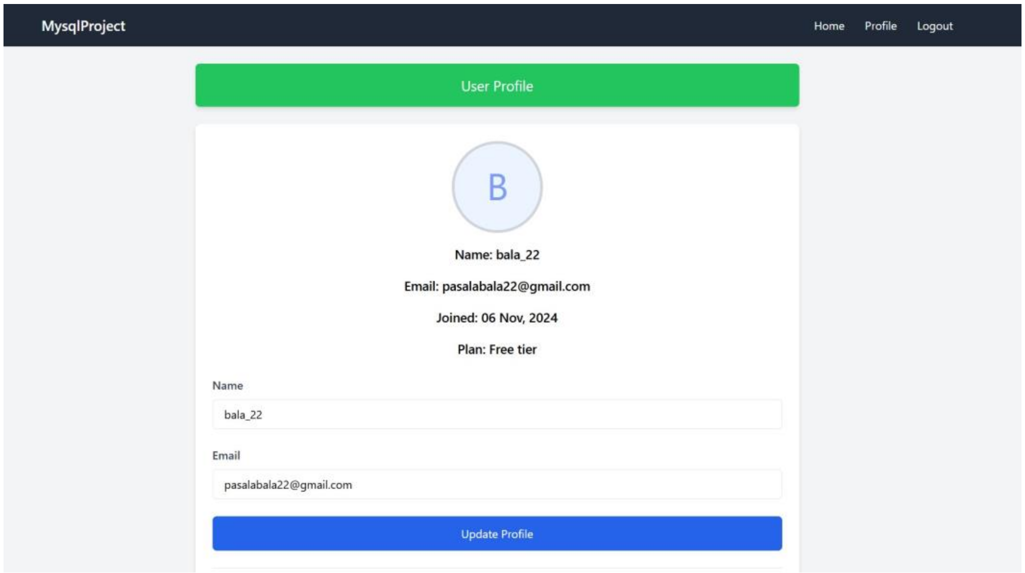
Don't have an account?

Register here

Subscription management:

Users with an interest in accessing these services can pay within the application using secure Stripe, or they can select one of two possible subscription types: monthly or annual.

User profile management:



Name: bala_22

Email: pasalabala22@gmail.com

Joined: 06 Nov, 2024

Plan: Free tier

Name

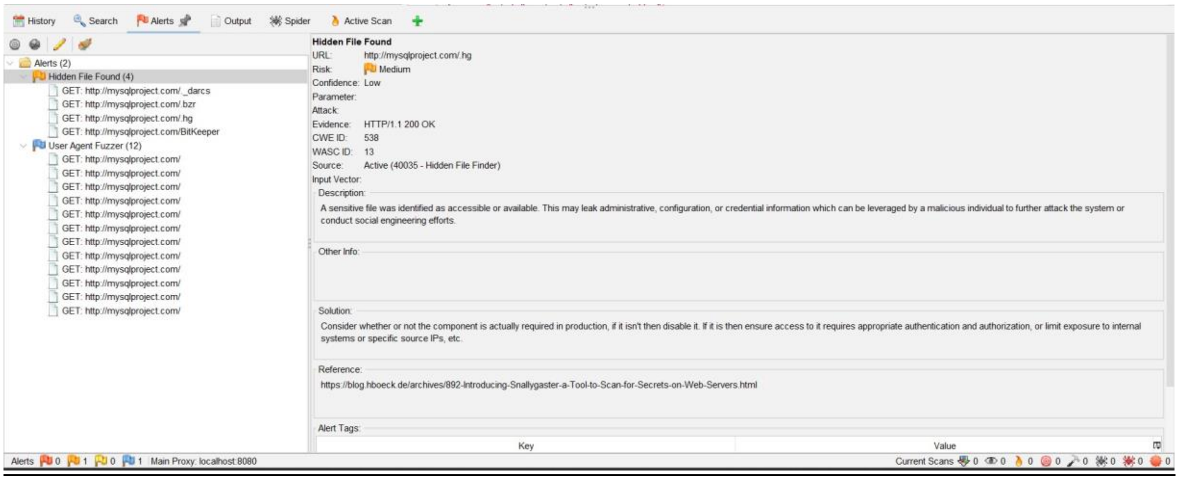
bala_22

Email

pasalabala22@gmail.com

Deliverables:

Owasp zap



```
Alerts (2)
  Hidden File Found (4)
    GET: http://mysqlproject.com/._darcs
    GET: http://mysqlproject.com/.bzr
    GET: http://mysqlproject.com/.hg
    GET: http://mysqlproject.com/BitKeeper
  User Agent Fuzzer (12)
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
    GET: http://mysqlproject.com/
```

Hidden File Found

URL: http://mysqlproject.com/.hg

Risk: Medium

Confidence: Low

Parameter:

Attack:

Evidence: HTTP/1.1 200 OK

CWE ID: 538

WASC ID: 13

Source: Active (40035 - Hidden File Finder)

Input Vector:

Description:

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other Info:

Solution:

Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.

Reference:

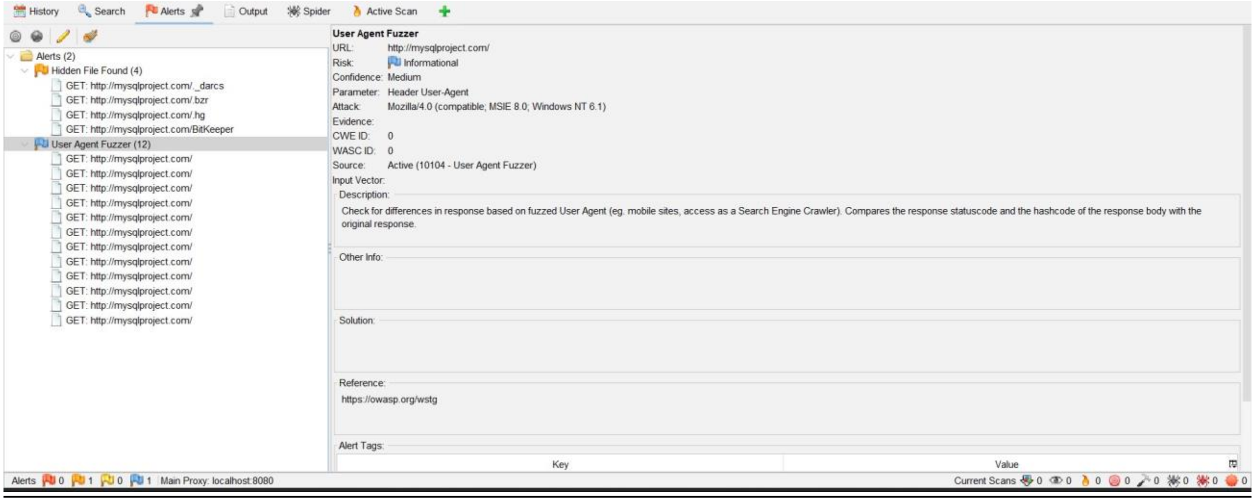
https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

Alert Tags:

Key	Value

Alerts 🟥 0 🟧 1 🟨 0 🟦 1 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0



- Alerts (2)
  - Hidden File Found (4)
    - GET: http://mysqlproject.com/._darcs
    - GET: http://mysqlproject.com/.bzr
    - GET: http://mysqlproject.com/.hg
    - GET: http://mysqlproject.com/BitKeeper
  - User Agent Fuzzer (12)
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/
    - GET: http://mysqlproject.com/

User Agent Fuzzer

URL: http://mysqlproject.com/
Risk: Informational
Confidence: Medium
Parameter: Header User-Agent
Attack: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence:
CWE ID: 0
WASC ID: 0
Source: Active (10104 - User Agent Fuzzer)
Input Vector:

Description:

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Other Info:

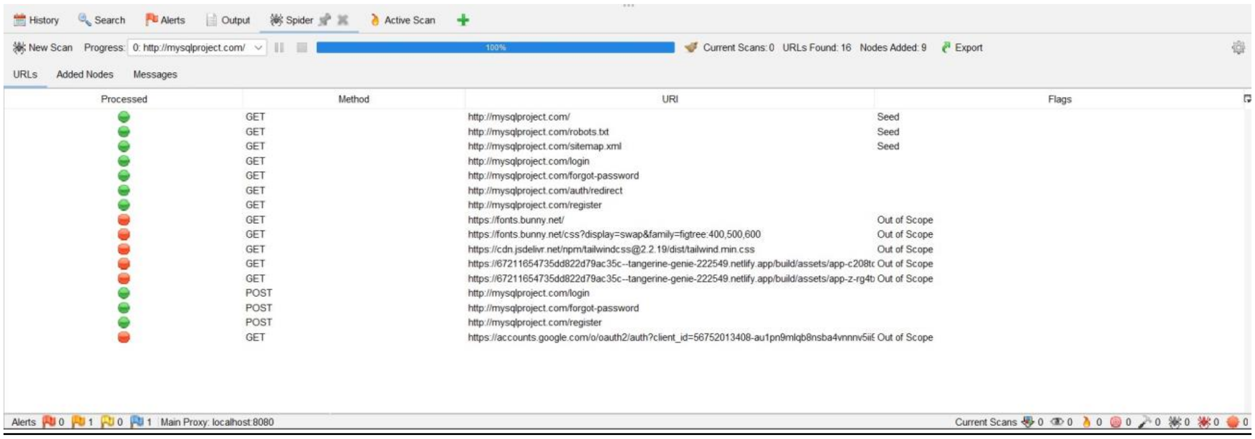
Solution:

Reference:

https://owasp.org/wstg

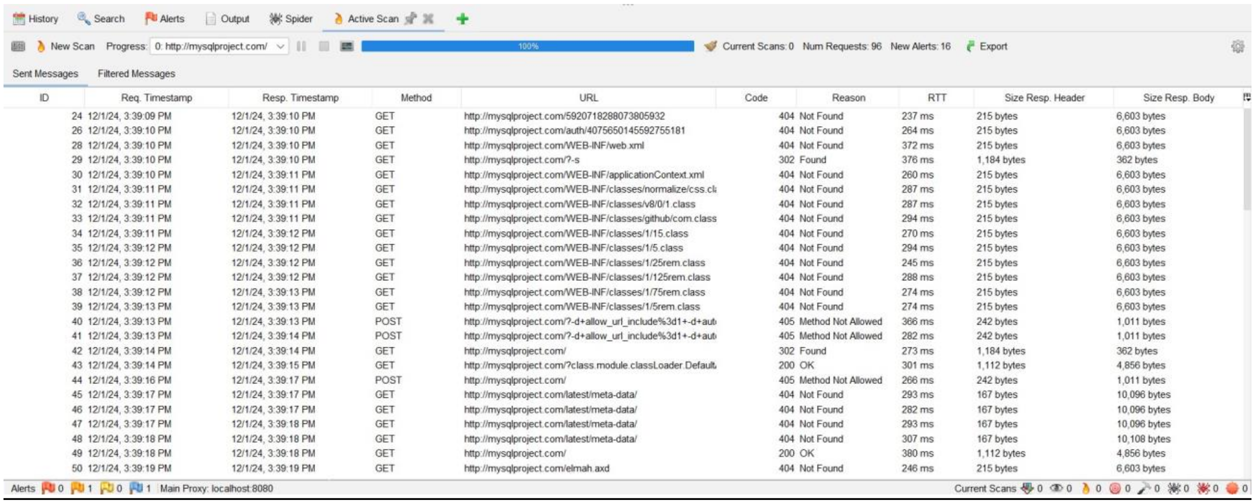
Alert Tags:

Key	Value



Current Scans: 0 URLs Found: 16 Nodes Added: 9

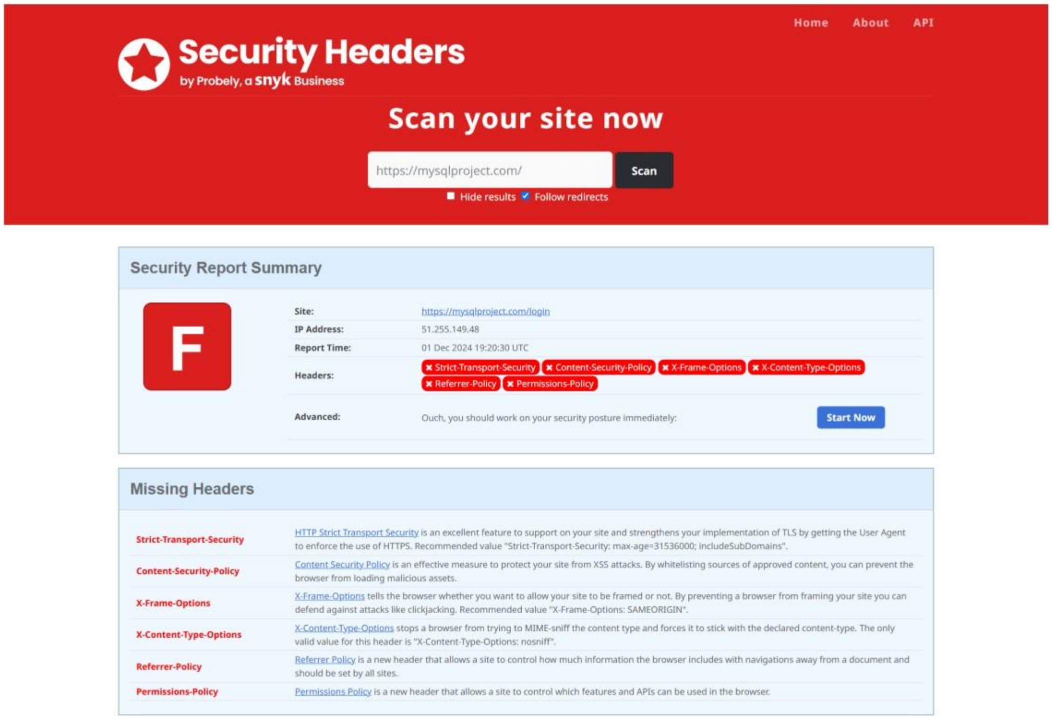
Processed	Method	URI	Flags
🟢	GET	http://mysqlproject.com/	Seed
🟢	GET	http://mysqlproject.com/robots.txt	Seed
🟢	GET	http://mysqlproject.com/sitemap.xml	Seed
🟢	GET	http://mysqlproject.com/login	
🟢	GET	http://mysqlproject.com/forgot-password	
🟢	GET	http://mysqlproject.com/auth/redirect	
🟢	GET	http://mysqlproject.com/register	
🔴	GET	https://fonts.bunny.net/	Out of Scope
🔴	GET	https://fonts.bunny.net/css?display=swap&family=figtree:400,500,600	Out of Scope
🔴	GET	https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css	Out of Scope
🔴	GET	https://67211654735dd822d79ac35c--tangerine-genie-222549.netlify.app/build/assets/app-c208tc	Out of Scope
🔴	GET	https://67211654735dd822d79ac35c--tangerine-genie-222549.netlify.app/build/assets/app-z-rg4b	Out of Scope
🟢	POST	http://mysqlproject.com/login	
🟢	POST	http://mysqlproject.com/forgot-password	
🟢	POST	http://mysqlproject.com/register	
🔴	GET	https://accounts.google.com/o/oauth2/auth?client_id=56752013408-au1pn9mlqb8nsba4vnnnv5ii	Out of Scope



Current Scans: 0 Num Requests: 96 New Alerts: 16

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
24	12/1/24, 3:39:09 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/59207182880738O5932	404	Not Found	237 ms	215 bytes	6,603 bytes
26	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/auth/4075650145592755181	404	Not Found	264 ms	215 bytes	6,603 bytes
28	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/WEB-INF/web.xml	404	Not Found	372 ms	215 bytes	6,603 bytes
29	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/?-s	302	Found	376 ms	1,184 bytes	362 bytes
30	12/1/24, 3:39:10 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/applicationContext.xml	404	Not Found	260 ms	215 bytes	6,603 bytes
31	12/1/24, 3:39:11 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/classes/normalize/css.cl	404	Not Found	287 ms	215 bytes	6,603 bytes
32	12/1/24, 3:39:11 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/classes/v8/0/1.class	404	Not Found	287 ms	215 bytes	6,603 bytes
33	12/1/24, 3:39:11 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/classes/github/com.class	404	Not Found	294 ms	215 bytes	6,603 bytes
34	12/1/24, 3:39:11 PM	12/1/24, 3:39:12 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/15.class	404	Not Found	270 ms	215 bytes	6,603 bytes
35	12/1/24, 3:39:12 PM	12/1/24, 3:39:12 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/5.class	404	Not Found	294 ms	215 bytes	6,603 bytes
36	12/1/24, 3:39:12 PM	12/1/24, 3:39:12 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/25rem.class	404	Not Found	245 ms	215 bytes	6,603 bytes
37	12/1/24, 3:39:12 PM	12/1/24, 3:39:12 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/125rem.class	404	Not Found	288 ms	215 bytes	6,603 bytes
38	12/1/24, 3:39:12 PM	12/1/24, 3:39:13 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/75rem.class	404	Not Found	274 ms	215 bytes	6,603 bytes
39	12/1/24, 3:39:13 PM	12/1/24, 3:39:13 PM	GET	http://mysqlproject.com/WEB-INF/classes/1/5rem.class	404	Not Found	274 ms	215 bytes	6,603 bytes
40	12/1/24, 3:39:13 PM	12/1/24, 3:39:13 PM	POST	http://mysqlproject.com/?-d+allow_url_include%3d1+-d+aut	405	Method Not Allowed	366 ms	242 bytes	1,011 bytes
41	12/1/24, 3:39:13 PM	12/1/24, 3:39:14 PM	POST	http://mysqlproject.com/?-d+allow_url_include%3d1+-d+aut	405	Method Not Allowed	282 ms	242 bytes	1,011 bytes
42	12/1/24, 3:39:14 PM	12/1/24, 3:39:14 PM	GET	http://mysqlproject.com/	302	Found	273 ms	1,184 bytes	362 bytes
43	12/1/24, 3:39:14 PM	12/1/24, 3:39:15 PM	GET	http://mysqlproject.com/?class.module.classLoader.Default	200	OK	301 ms	1,112 bytes	4,856 bytes
44	12/1/24, 3:39:16 PM	12/1/24, 3:39:17 PM	POST	http://mysqlproject.com/	405	Method Not Allowed	266 ms	242 bytes	1,011 bytes
45	12/1/24, 3:39:17 PM	12/1/24, 3:39:17 PM	GET	http://mysqlproject.com/latest/meta-data/	404	Not Found	293 ms	167 bytes	10,096 bytes
46	12/1/24, 3:39:17 PM	12/1/24, 3:39:17 PM	GET	http://mysqlproject.com/latest/meta-data/	404	Not Found	282 ms	167 bytes	10,096 bytes
47	12/1/24, 3:39:17 PM	12/1/24, 3:39:18 PM	GET	http://mysqlproject.com/latest/meta-data/	404	Not Found	293 ms	167 bytes	10,096 bytes
48	12/1/24, 3:39:18 PM	12/1/24, 3:39:18 PM	GET	http://mysqlproject.com/latest/meta-data/	404	Not Found	307 ms	167 bytes	10,108 bytes
49	12/1/24, 3:39:18 PM	12/1/24, 3:39:18 PM	GET	http://mysqlproject.com/	200	OK	380 ms	1,112 bytes	4,856 bytes
50	12/1/24, 3:39:19 PM	12/1/24, 3:39:19 PM	GET	http://mysqlproject.com/elmah.axd	404	Not Found	246 ms	215 bytes	6,603 bytes

Security Headers:


Home
About
API
Security Headers
by Probely, a snyk Business
Scan your site now
https://mysqlproject.com/
Scan
□ Hide results ☑ Follow redirects

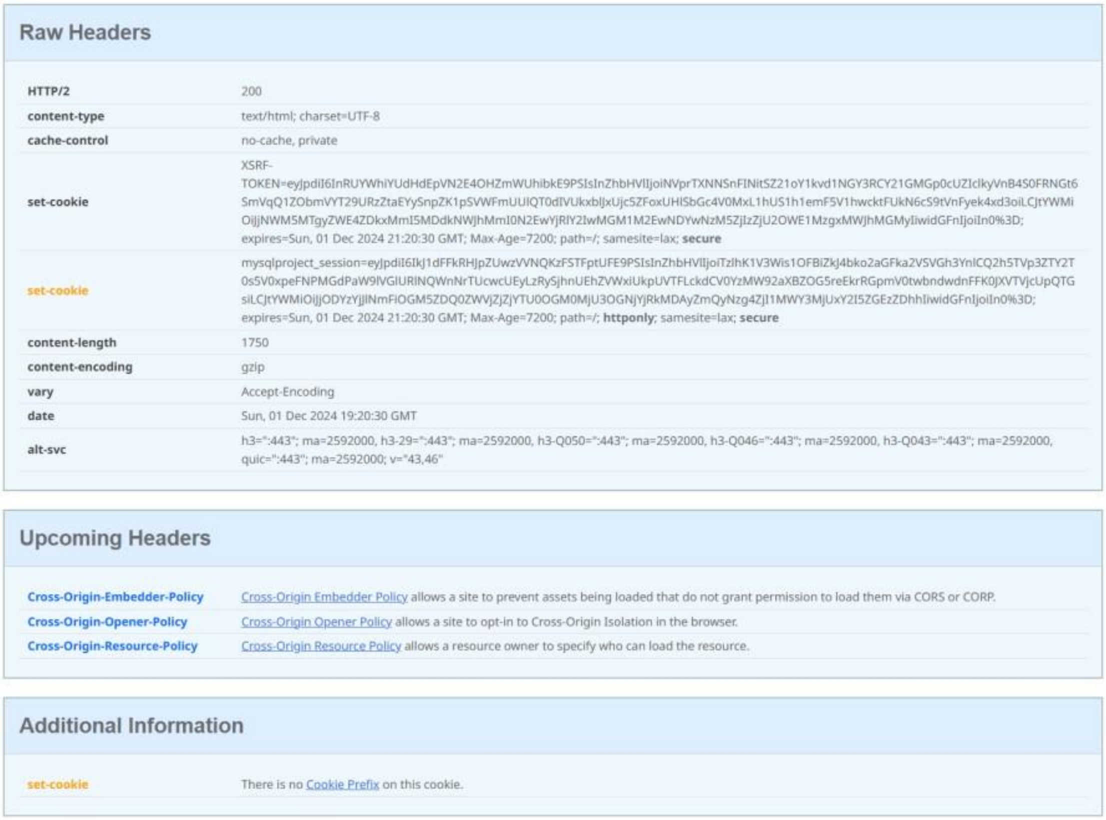
Security Report Summary

F

Site:	https://mysqlproject.com/login
IP Address:	51.255.149.48
Report Time:	01 Dec 2024 19:20:30 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Advanced:	Ouch, you should work on your security posture immediately: Start Now

Missing Headers

Strict-Transport-Security	HTTP Strict Transport Security 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".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.



Raw Headers

HTTP/2	200
content-type	text/html; charset=UTF-8
cache-control	no-cache, private
set-cookie	XSRF-TOKEN=eyJpdiI6InRUYWhiYUdHdEpVN2E4OHZmWUhibkE9PSIsInZhbHVlIjoiNVprTXNNSnFINitSZ21oY1kvd1NGY3RCY21GMGp0cUZIclkyVnB4S0FRNGt6SmVqQ1ZObmVYT29URzZtaEYySnpZK1pSVWFmUUlQT0dIVUkxbljxUjc5ZFoxUHlSbGc4V0MxL1hUS1h1emF5V1hwcktFUkN6cS9tVnFyek4xd3oiLCJtYWMiOiJjNWM5MTgyZWE4ZDkxMmI5MDdkNWJhMmI0N2EwYjRlY2IwMGM1M2EwNDYwNzM5ZjIzZjU2OWE1MzgxMWJhMGMyIiwidGFnIjoiIn0%3D; expires=Sun, 01 Dec 2024 21:20:30 GMT; Max-Age=7200; path=/; samesite=lax; **secure**
set-cookie	mysqlproject_session=eyJpdiI6IkJ1dFFkRHJpZUwzVVNQKzFSTFptUFE9PSIsInZhbHVlIjoiTzlhK1V3Wis1OFBiZkJ4bko2aGFka2VSVGh3YnlCQ2h5TVp3ZTY2T0s5V0xpeFNPMGdPaW9lVGlURlNQWnNrTUcwcUEyLzRySjhnUEhZVWxiUkpUVTFLckdCV0YzMW92aXBZOG5reEkrRGpmV0twbndwdnFFK0JXVTVjcUpQTGsiLCJtYWMiOiJjODYzYjJlNmFiOGM5ZDQ0ZWVjZjZjYTU0OGM0MjU3OGNjYjRkMDAyZmQyNzg4ZjI1MWY3MjUxY2I5ZGEzZDhhIiwidGFnIjoiIn0%3D; expires=Sun, 01 Dec 2024 21:20:30 GMT; Max-Age=7200; path=/; **httponly**; samesite=lax; **secure**
content-length	1750
content-encoding	gzip
vary	Accept-Encoding
date	Sun, 01 Dec 2024 19:20:30 GMT
alt-svc	h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

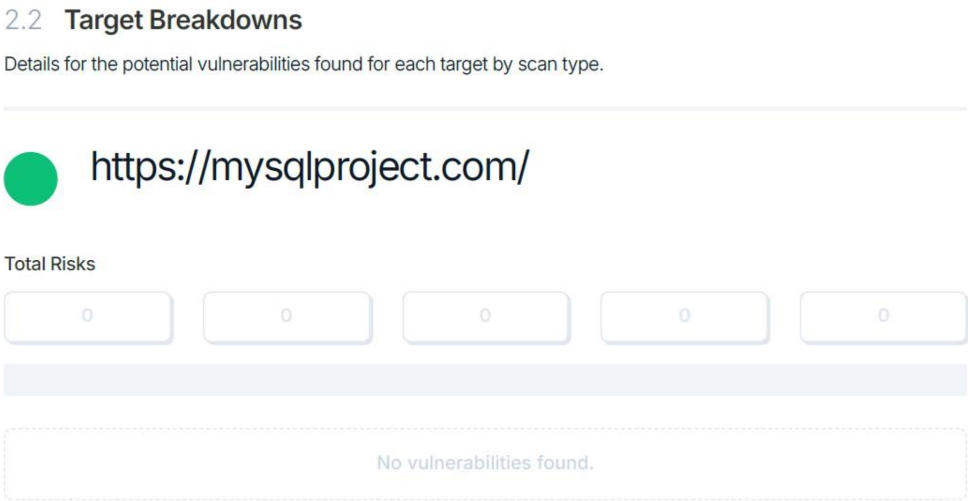
Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

set-cookie	There is no Cookie Prefix on this cookie.

HostedScan:



2.2 Target Breakdowns

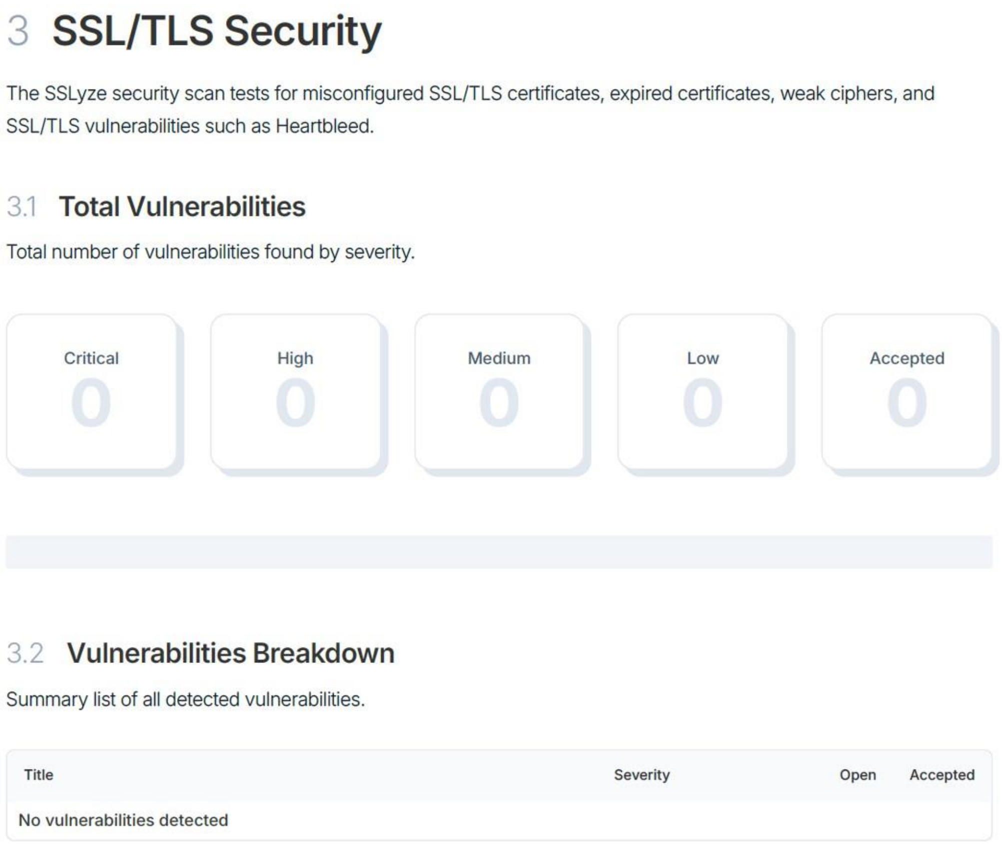
Details for the potential vulnerabilities found for each target by scan type.

● https://mysqlproject.com/

Total Risks

0	0	0	0	0

No vulnerabilities found.



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

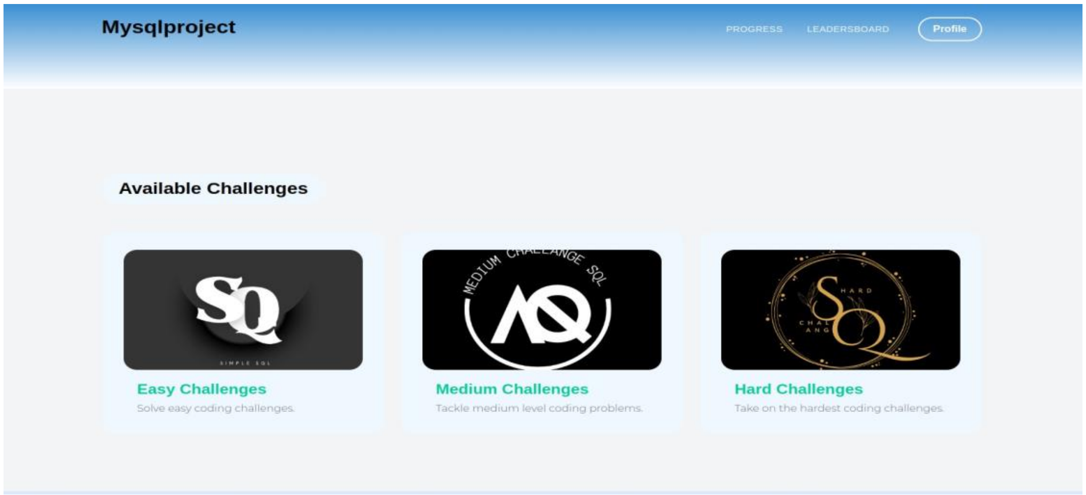
3.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

Summary report:

MySQL Project Application is an effective, well-structured web application that has been developed with main purpose of solving problems in various activities. It comes with an interactive view, users can access the system on any device.



Available Challenges

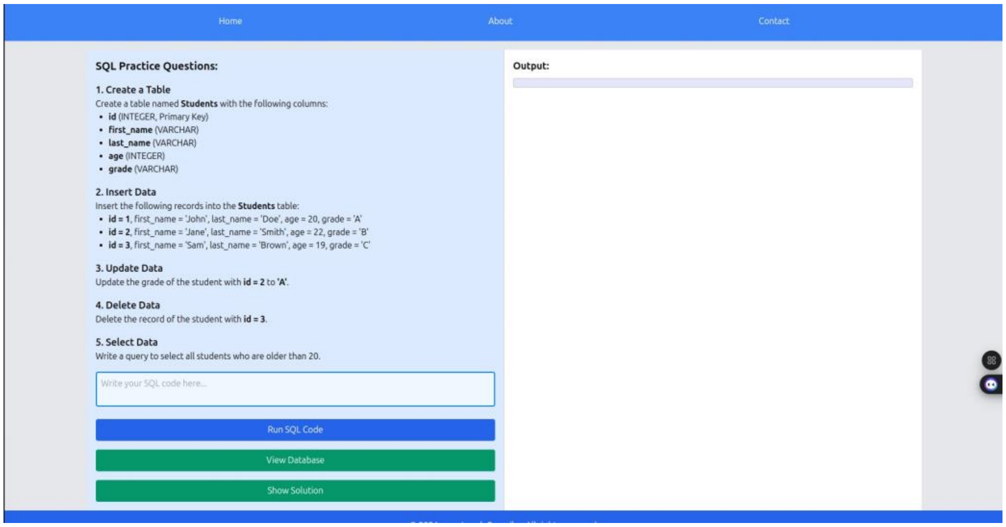
Easy Challenges
Solve easy coding challenges.

Medium Challenges
Tackle medium level coding problems.

Hard Challenges
Take on the hardest coding challenges.

Problem solving environment:

The specificities of the application include a split pane interface on which a user can choose between easy, medium, or hard problems, as well as on which SQL queries are compiled.



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

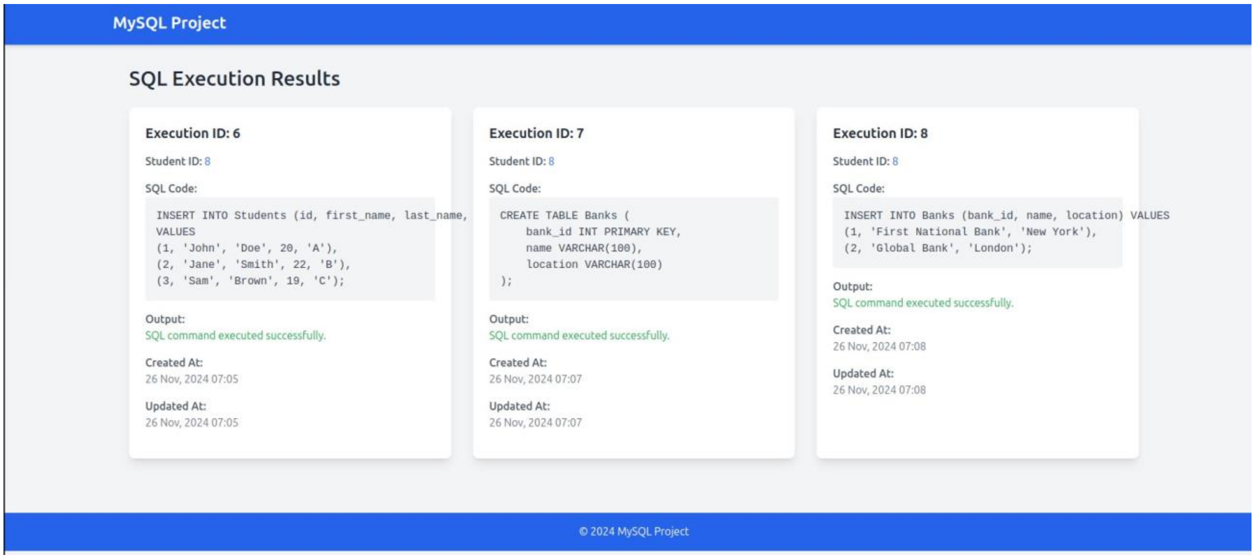
Delete the record of the student with **id = 3**.

5. Select Data

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

Real time feedback:

The application has a split pane design to select easy, medium or hard questions and has the system to compile SQL queries.



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.

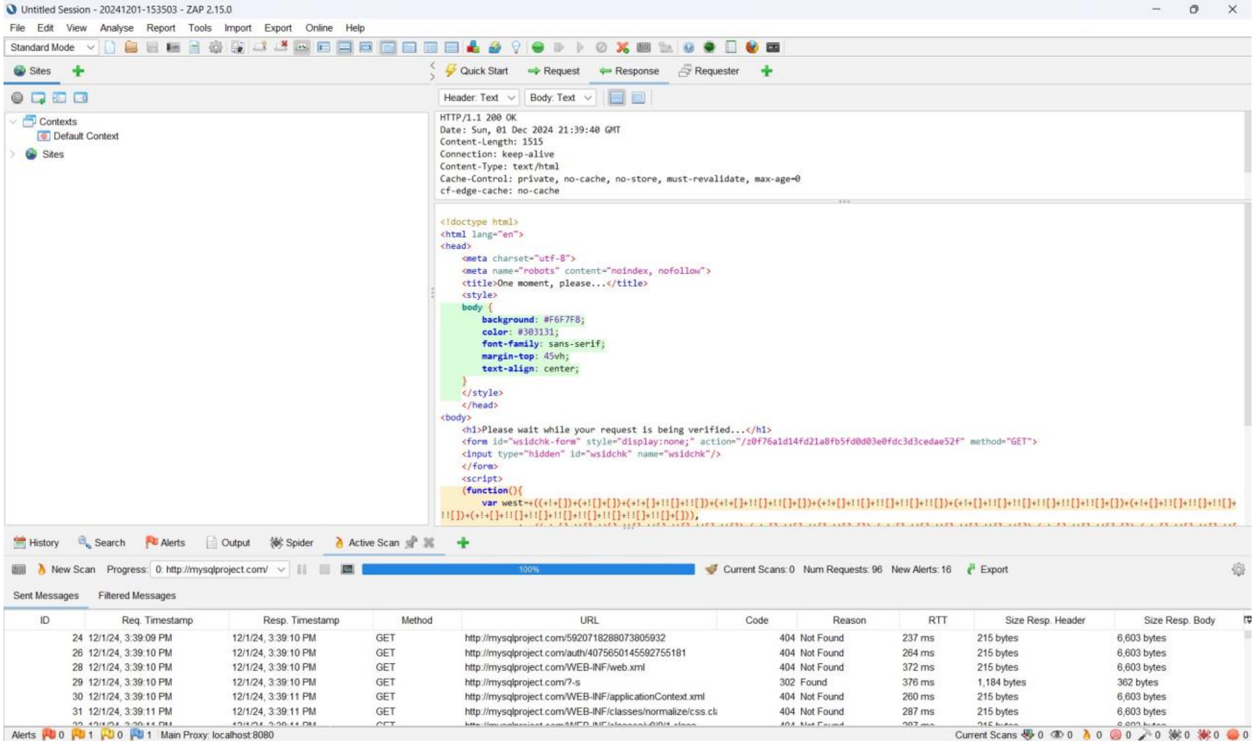
Created At:
26 Nov, 2024 07:08

Updated At:
26 Nov, 2024 07:08

Tool stages:

Owasp zap

After entering the URL of our website

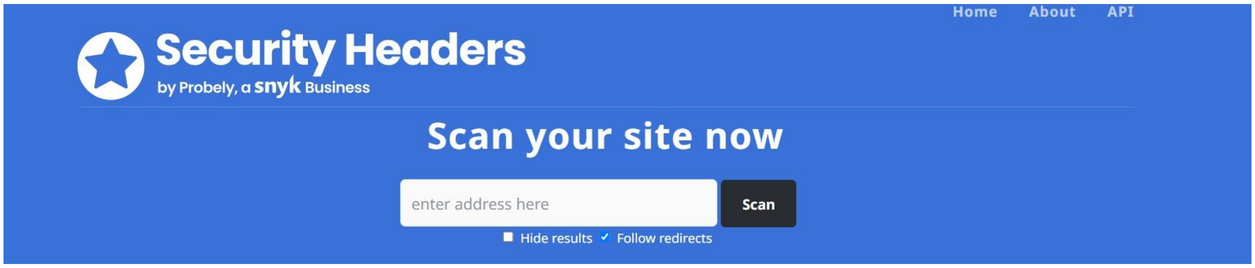

Untitled Session - 20241201-153503 - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
History Search Alerts Output Spider Active Scan
New Scan
Progress: 0: http://mysqlproject.com/
100%
Current Scans: 0 Num Requests: 96 New Alerts: 16
Export
Sent Messages Filtered Messages
Alerts 0 1 0 1 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

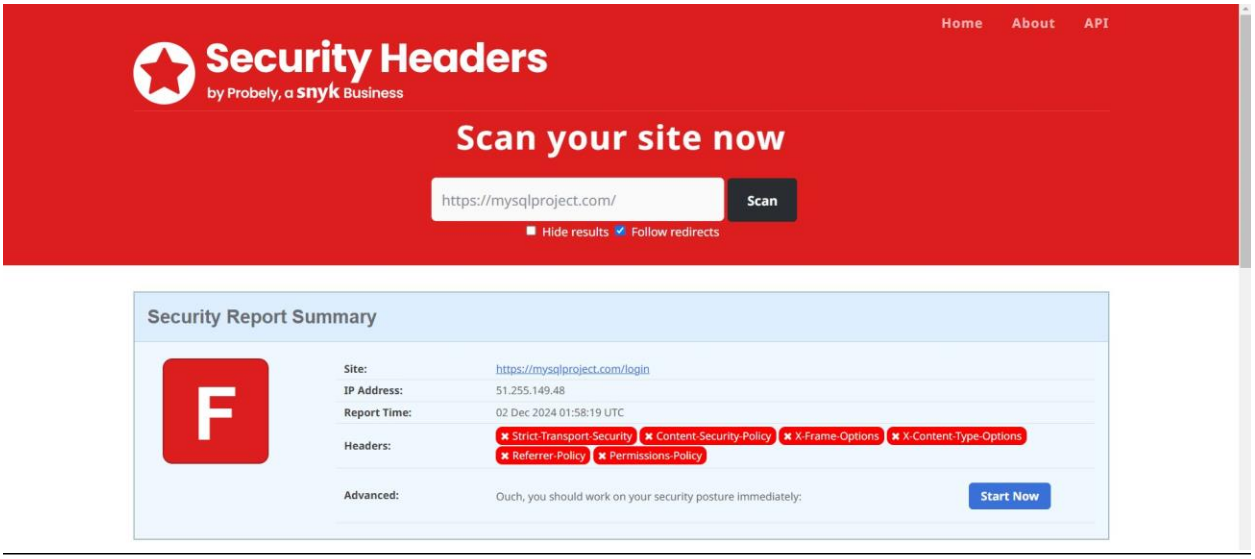
```
HTTP/1.1 200 OK
Date: Sun, 01 Dec 2024 21:39:40 GMT
Content-Length: 1515
Connection: keep-alive
Content-Type: text/html
Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
cf-edge-cache: no-cache
```

```
<!doctype html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="robots" content="noindex, nofollow">
    <title>One moment, please...</title>
    <style>
    body {
        background: #F6F7F8;
        color: #303131;
        font-family: sans-serif;
        margin-top: 45vh;
        text-align: center;
    }
    </style>
    </head>
<body>
    <h1>Please wait while your request is being verified...</h1>
    <form id="wsidchk-form" style="display:none;" action="/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f" method="GET">
    <input type="hidden" id="wsidchk" name="wsidchk"/>
    </form>
    <script>
    (function(){
        var west=+((+!+[])+(+![]+[])+(+!+[]+!![]+!![])+(+!+[]+!![]+!![]+[])+(+!+[]+!![]+!![]+!![]+!![])+(+!+[]+!![]+!![]+!![]+!![]+!![]+[])+(+!+[]+!![]+!![]+!![]+
!![])+(+!+[]+!![]+!![]+!![]+!![]+!![]+!![]+[])),
```

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
24	12/1/24, 3:39:09 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/5920718288073805932	404	Not Found	237 ms	215 bytes	6,603 bytes
26	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/auth/4075650145592755181	404	Not Found	264 ms	215 bytes	6,603 bytes
28	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/WEB-INF/web.xml	404	Not Found	372 ms	215 bytes	6,603 bytes
29	12/1/24, 3:39:10 PM	12/1/24, 3:39:10 PM	GET	http://mysqlproject.com/?-s	302	Found	376 ms	1,184 bytes	362 bytes
30	12/1/24, 3:39:10 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/applicationContext.xml	404	Not Found	260 ms	215 bytes	6,603 bytes
31	12/1/24, 3:39:11 PM	12/1/24, 3:39:11 PM	GET	http://mysqlproject.com/WEB-INF/classes/normalize/css.cl	404	Not Found	287 ms	215 bytes	6,603 bytes

Security Headers:




Home
About
API
Security Headers
by Probely, a snyk Business
Scan your site now
https://mysqlproject.com/
Scan
□ Hide results ☑ Follow redirects
Start Now

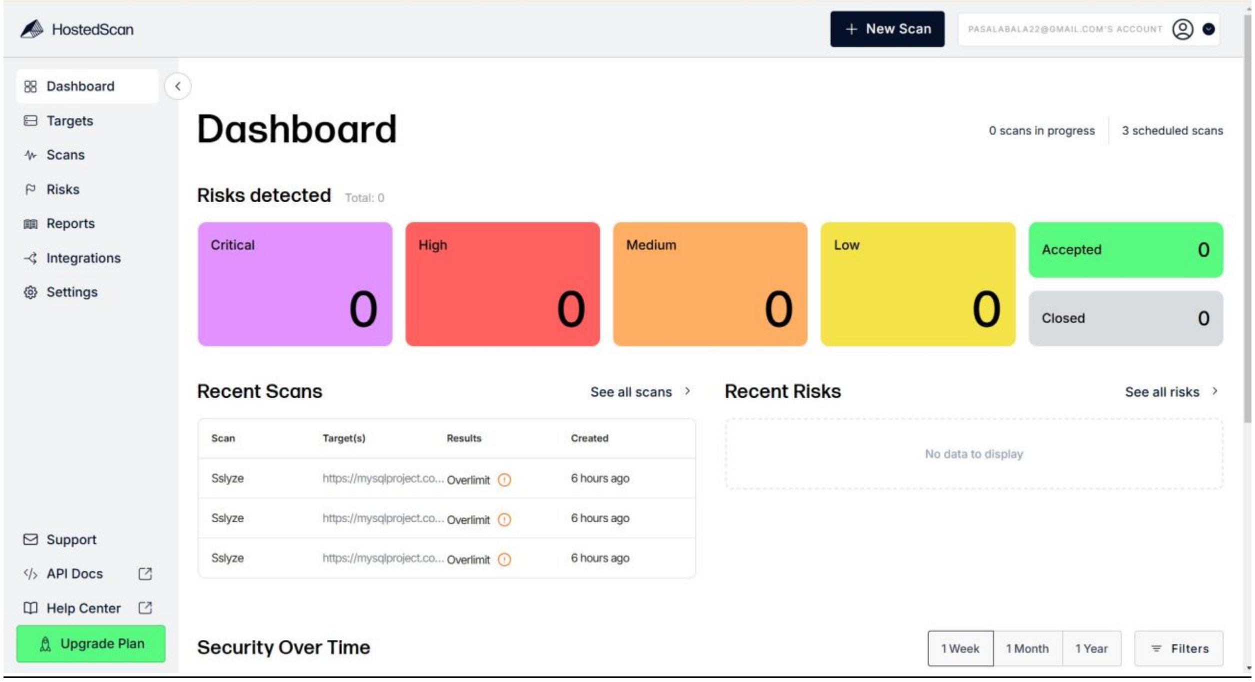
Security Report Summary

F

Site:	https://mysqlproject.com/login
IP Address:	51.255.149.48
Report Time:	02 Dec 2024 01:58:19 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Advanced:	Ouch, you should work on your security posture immediately:

HostedScan:

Initially the hostedscan page



Dashboard

0 scans in progress | 3 scheduled scans

Risks detected Total: 0

Critical 0 | High 0 | Medium 0 | Low 0 | Accepted 0 | Closed 0

Recent Scans

Scan	Target(s)	Results	Created
Sslyze	https://mysqlproject.co...	Overlimit	6 hours ago
Sslyze	https://mysqlproject.co...	Overlimit	6 hours ago
Sslyze	https://mysqlproject.co...	Overlimit	6 hours ago

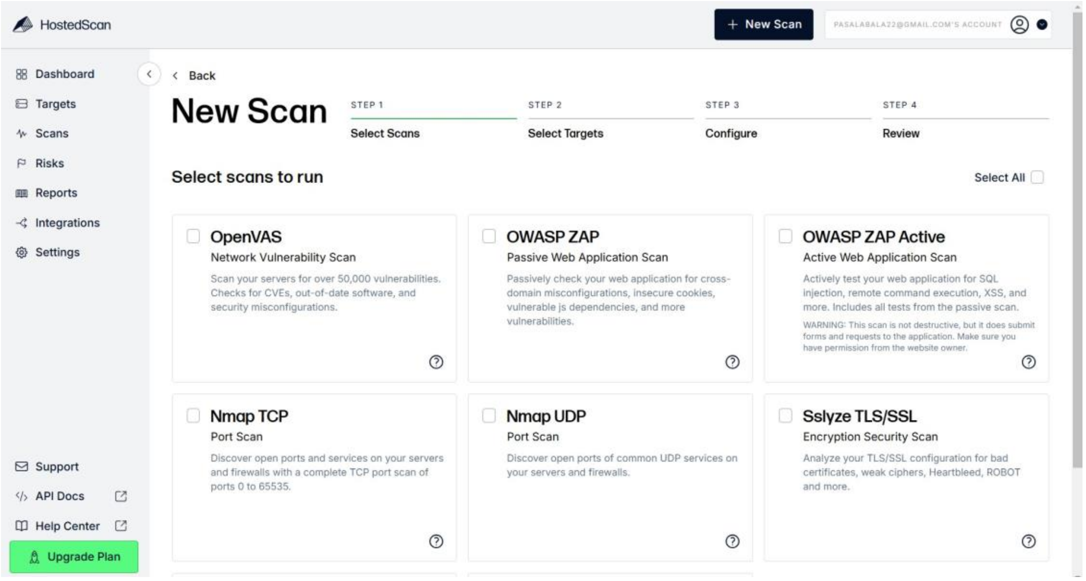
Recent Risks

No data to display

Security Over Time

Then click on new scan

You will get page like this



New Scan

Select scans to run

□ **OpenVAS**
Network Vulnerability Scan
Scan your servers for over 50,000 vulnerabilities. Checks for CVEs, out-of-date software, and security misconfigurations.

□ **OWASP ZAP**
Passive Web Application Scan
Passively check your web application for cross-domain misconfigurations, insecure cookies, vulnerable js dependencies, and more vulnerabilities.

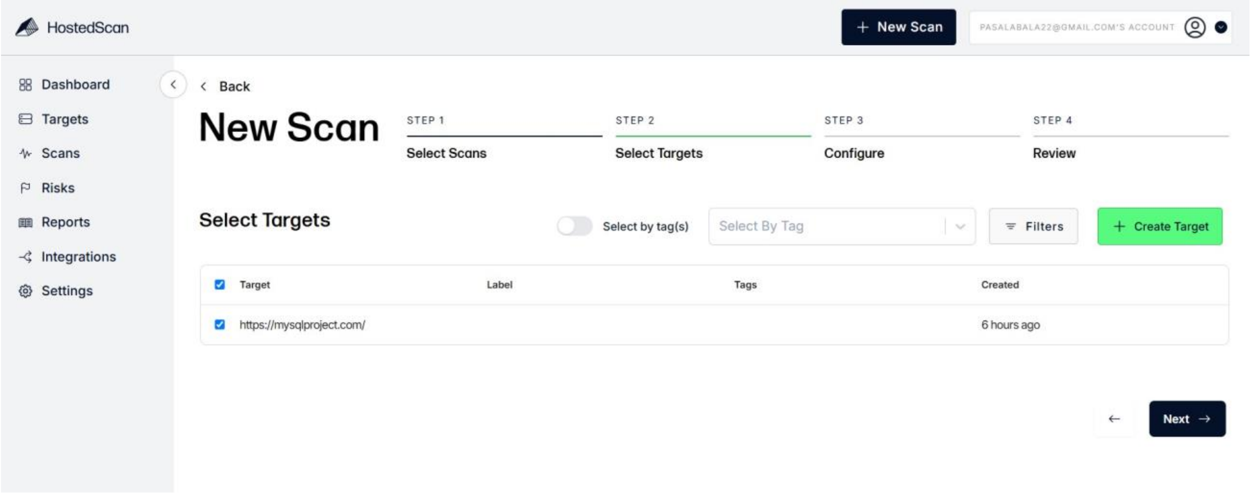
□ **OWASP ZAP Active**
Active Web Application Scan
Actively test your web application for SQL injection, remote command execution, XSS, and more. Includes all tests from the passive scan.
WARNING: This scan is not destructive, but it does submit forms and requests to the application. Make sure you have permission from the website owner.

□ **Nmap TCP**
Port Scan
Discover open ports and services on your servers and firewalls with a complete TCP port scan of ports 0 to 65535.

□ **Nmap UDP**
Port Scan
Discover open ports of common UDP services on your servers and firewalls.

□ **Sslyze TLS/SSL**
Encryption Security Scan
Analyze your TLS/SSL configuration for bad certificates, weak ciphers, Heartbleed, ROBOT and more.

Then select Sslyze TLS/SSL Then
it shows like this.

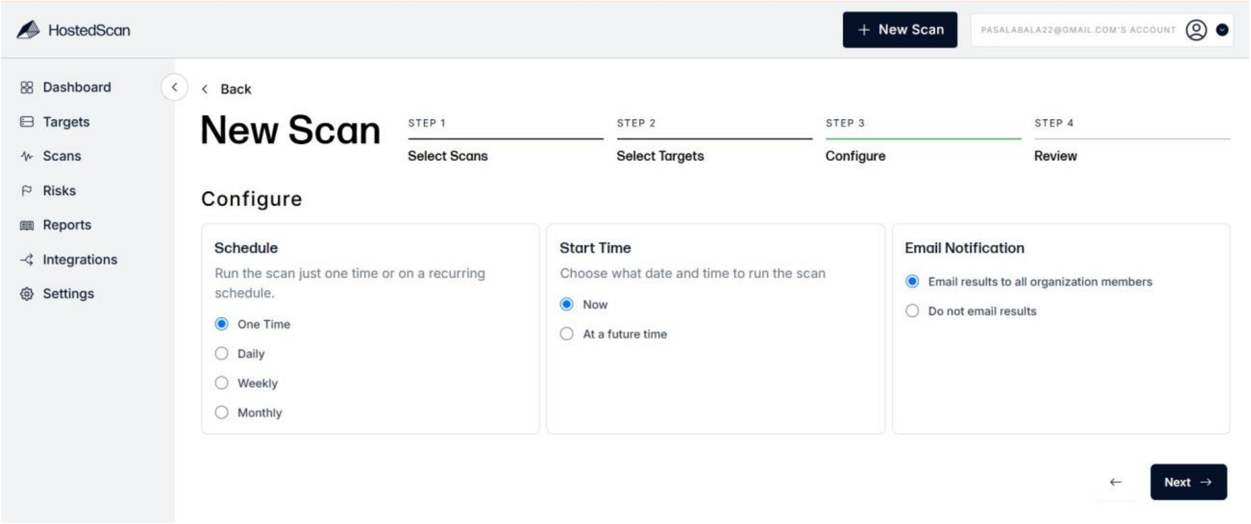


New Scan

Select Targets

☑	Target	Label	Tags	Created
☑	https://mysqlproject.com/			6 hours ago

Here select I selected the website and clicked next.



New Scan

STEP 1 Select Scans | STEP 2 Select Targets | STEP 3 Configure | STEP 4 Review

Configure

Schedule
Run the scan just one time or on a recurring schedule.
● One Time
○ Daily
○ Weekly
○ Monthly

Start Time
Choose what date and time to run the scan
● Now
○ At a future time

Email Notification
● Email results to all organization members
○ Do not email results

Again, click next
After that, click start scan then I got the result for my website.

Findings:

Owasp zap

- User agent fuzer
- Hidden File Found

SSH keys

- server.key
- privatekey.key
- myserver.key
- key.pem
- id_rsa
- id_dsa

Configuration files

- composer.json
- composer.lock
- wpeprivate/config.json
- config/databases.yml and some other risks**.**

Security Headers:

Missing security headers, exposure of sensitive information and insecure cookie configuration has also been highlighted in Image 2 of the text. These are un-set X frame options, X content type options and content security policy which help to limit such vulnerabilities as cross-site scripting.

HostedScan:

From the result no vulnerabilities found in the mysql website.

Recommendations:

Owasp zap

Disable exposed files and directories, control access to crucial directories and folders, review Philips' OAuth settings, test server responses to 'User-Agent' headers, check necessary folders and files, apply proper authorization and authentication, delete leaks, avoid directory listings, apply access controls, and eliminate critical directories as well as sanitize and validate inputs.

Security Headers

It has also suggested that the missing security headers should be implemented in the web applications, the configuration of session cookies.

This should be done to enable the HTTPOnly, Secure, SameSite flags, and to properly set up the CORS- related policies to avoid cross origin threats. One of the things that organisations should consider is to monitor security headers for any threats and possibilities.