Group 19: Web Based Project Management Tool for Small Business

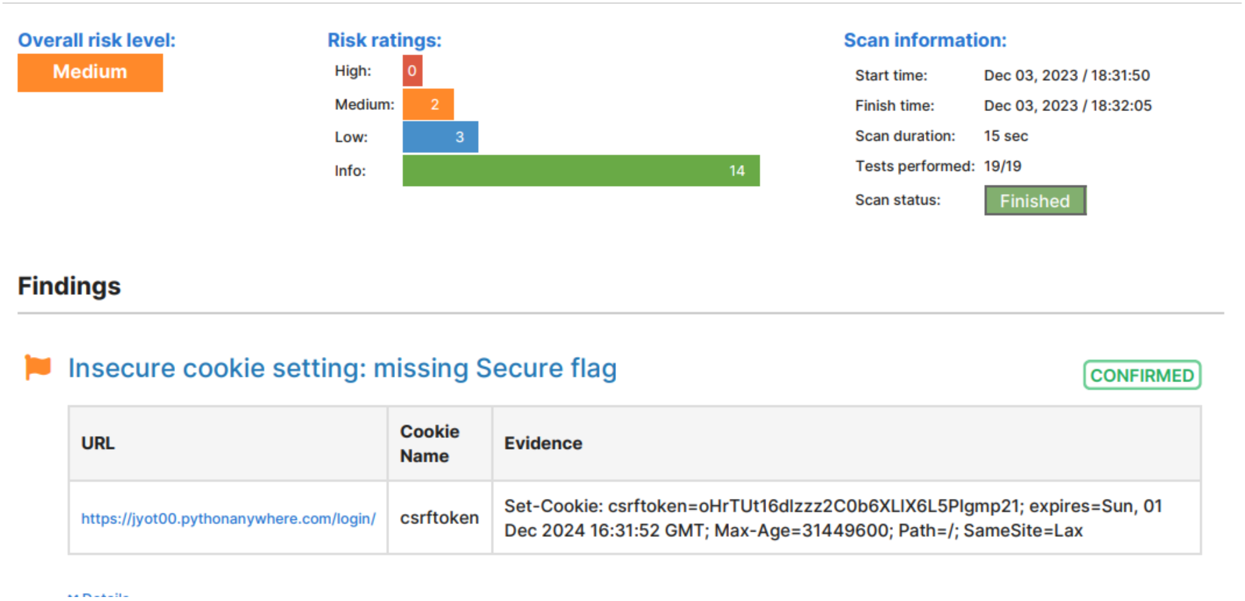
Non Functional Testing

1. Security testing

⟶Security testing in non-functional testing of a website involves evaluating the system's defences against unauthorized access, vulnerabilities, and potential threats. It includes identifying weaknesses, testing authentication mechanisms, ensuring data encryption, verifying compliance with security standards, patch management, and assessing resilience against attacks like DDoS. The goal is to uncover and address security flaws before they're exploited, ensuring the website and its users' data remain safe.

→For security testing we used the Pentest tool.

Report Of Overall Risk Level Of Website:



Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	2
Low:	3
Info:	14

Scan information:

Start time:	Dec 03, 2023 / 18:31:50
Finish time:	Dec 03, 2023 / 18:32:05
Scan duration:	15 sec
Tests performed:	19/19
Scan status:	Finished

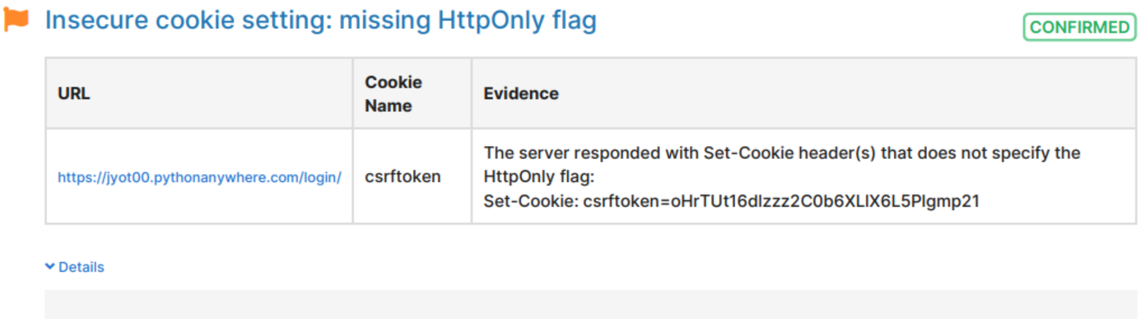
Findings

Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence
https://jyot00.pythonanywhere.com/login/	csrftoken	Set-Cookie: csrftoken=oHrTUt16dlzzz2C0b6XLIX6L5Plgmp21; expires=Sun, 01 Dec 2024 16:31:52 GMT; Max-Age=31449600; Path=/; SameSite=Lax

Risk description: Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

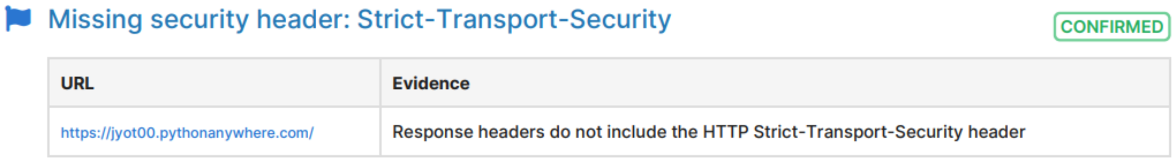


Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://jyot00.pythonanywhere.com/login/	csrftoken	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: csrftoken=oHrTUt16dlzzz2C0b6XLIX6L5Plgmp21

Risk Description: A cookie has been set without the HttpOnly flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

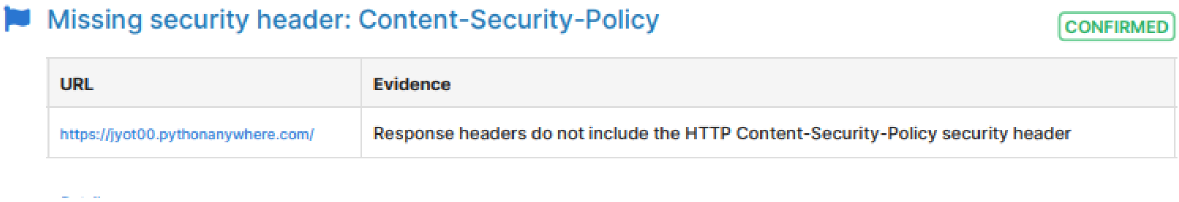


Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://jyot00.pythonanywhere.com/	Response headers do not include the HTTP Strict-Transport-Security header

Risk Description: The HTTP Strict-Transport-Security header instructs the browser to initiate only secure (HTTPS) connections to the web server and deny any unencrypted HTTP connection attempts. Lack of this header permits an attacker to force a victim user to initiate a cleartext HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).



Missing security header: Content-Security-Policy

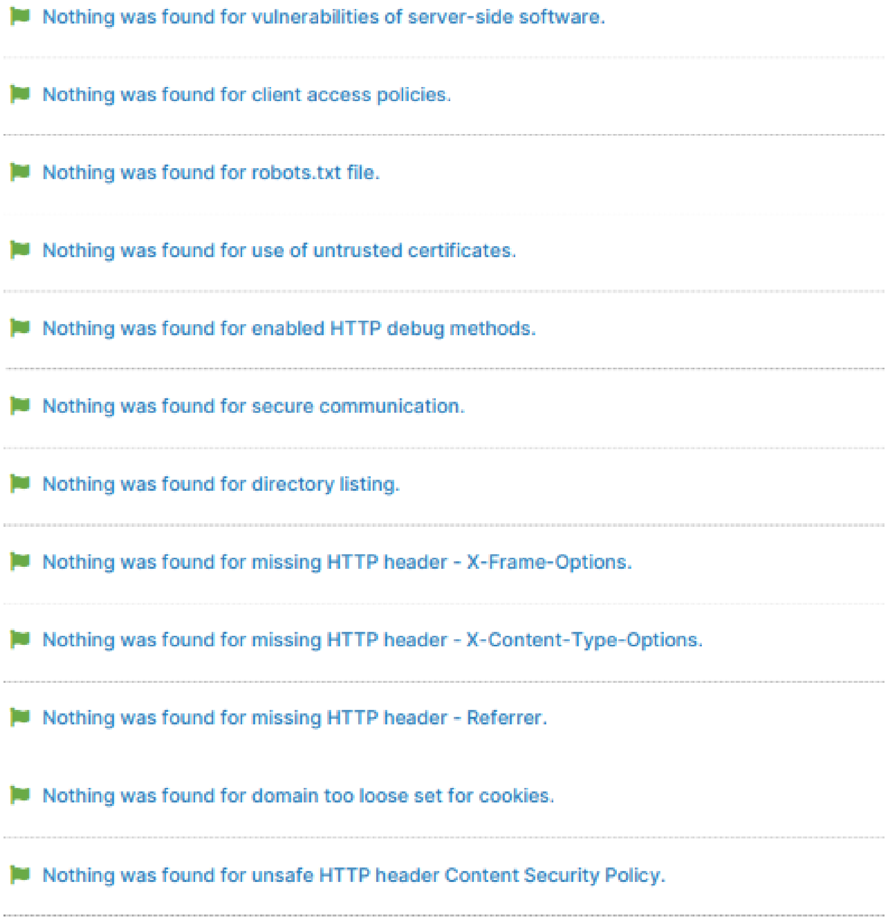
CONFIRMED

URL	Evidence
https://jyot00.pythonanywhere.com/	Response headers do not include the HTTP Content-Security-Policy security header

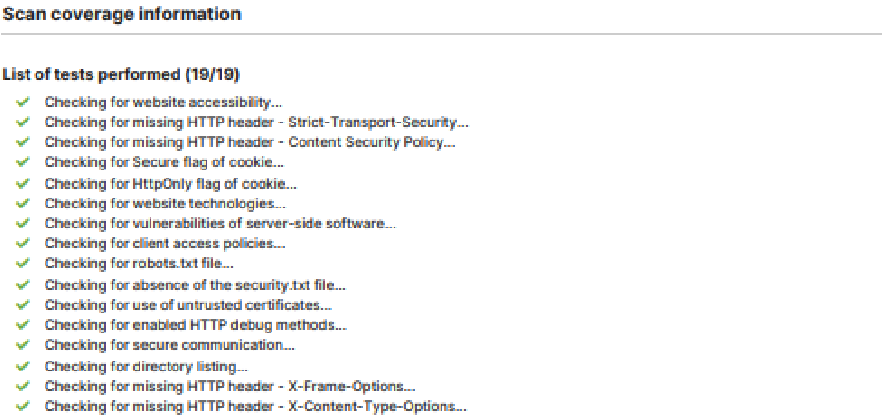
Risk description: The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site

Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Security Tests Passed By website:



- Nothing was found for vulnerabilities of server-side software.
- Nothing was found for client access policies.
- Nothing was found for robots.txt file.
- Nothing was found for use of untrusted certificates.
- Nothing was found for enabled HTTP debug methods.
- Nothing was found for secure communication.
- Nothing was found for directory listing.
- Nothing was found for missing HTTP header - X-Frame-Options.
- Nothing was found for missing HTTP header - X-Content-Type-Options.
- Nothing was found for missing HTTP header - Referrer.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for unsafe HTTP header Content Security Policy.



Scan coverage information

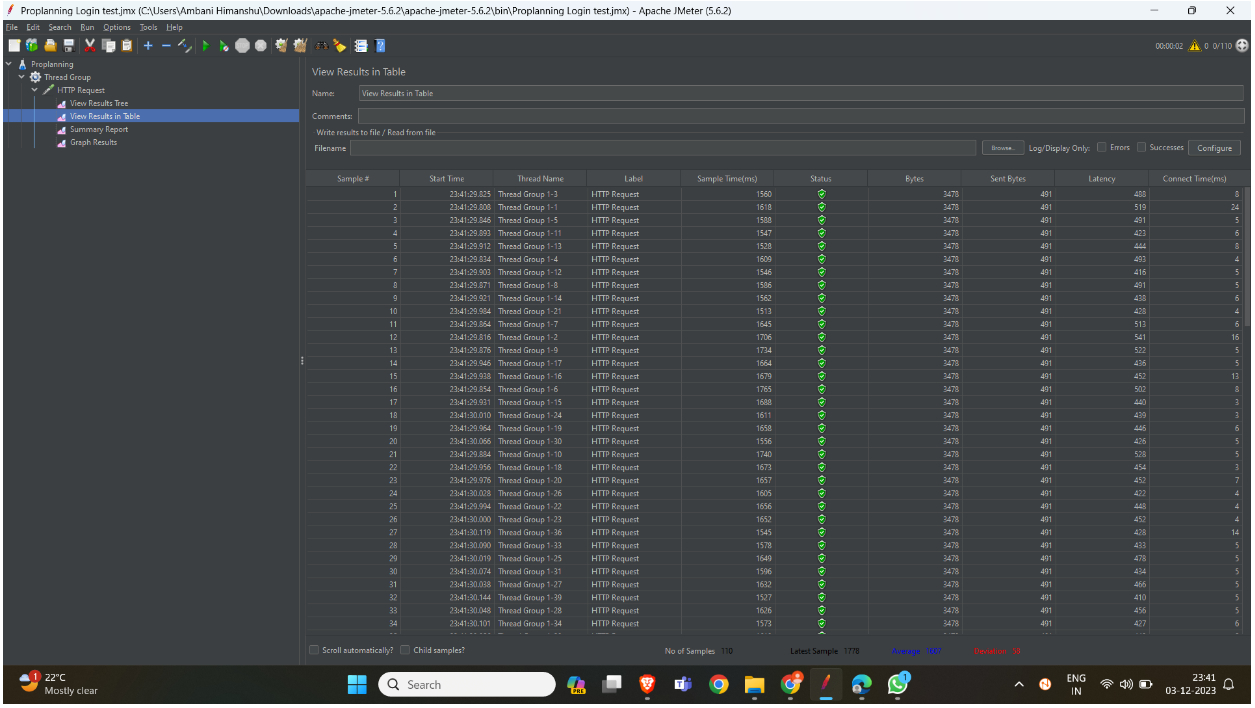
List of tests performed (19/19)

- ✓ Checking for website accessibility...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...

2. Load Testing

→In this Testing I used the jmeter to perform load testing.

→ Load testing Involves simulating user traffic to measure the load of the system can go through various loads. I first set up JMeter and added the link of the system in the URL added the different users for different test cases ran the test cases and checked the working of the system and the system can load 100+ users at the same time.


Proplanning Login test.jmx (C:\Users\Ambani Himanshu\Downloads\apache-jmeter-5.6.2\apache-jmeter-5.6.2\bin\Proplanning Login test.jmx) - Apache JMeter (5.6.2)
File Edit Search Run Options Tools Help
00:00:02 0 0/110
Proplanning
Thread Group
HTTP Request
View Results Tree
View Results in Table
Summary Report
Graph Results
22°C
Mostly clear
Search
ENG
IN
23:41
03-12-2023

View Results in Table

Name: View Results in Table

Comments:

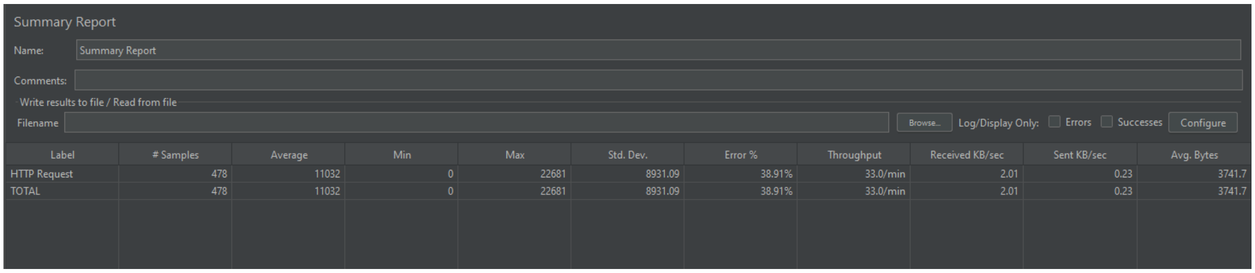
Write results to file / Read from file

Filename

Browse... Log/Display Only: □ Errors □ Successes Configure

Sample #	Start Time	Thread Name	Label	Sample Time(ms)	Status	Bytes	Sent Bytes	Latency	Connect Time(ms)
1	23:41:29.825	Thread Group 1-3	HTTP Request	1560	✓	3478	491	488	8
2	23:41:29.808	Thread Group 1-1	HTTP Request	1618	✓	3478	491	519	24
3	23:41:29.846	Thread Group 1-5	HTTP Request	1588	✓	3478	491	491	5
4	23:41:29.893	Thread Group 1-11	HTTP Request	1547	✓	3478	491	423	6
5	23:41:29.912	Thread Group 1-13	HTTP Request	1528	✓	3478	491	444	8
6	23:41:29.834	Thread Group 1-4	HTTP Request	1609	✓	3478	491	493	4
7	23:41:29.903	Thread Group 1-12	HTTP Request	1546	✓	3478	491	416	5
8	23:41:29.871	Thread Group 1-8	HTTP Request	1586	✓	3478	491	491	5
9	23:41:29.921	Thread Group 1-14	HTTP Request	1562	✓	3478	491	438	6
10	23:41:29.984	Thread Group 1-21	HTTP Request	1513	✓	3478	491	428	4
11	23:41:29.864	Thread Group 1-7	HTTP Request	1645	✓	3478	491	513	6
12	23:41:29.816	Thread Group 1-2	HTTP Request	1706	✓	3478	491	541	16
13	23:41:29.876	Thread Group 1-9	HTTP Request	1734	✓	3478	491	522	5
14	23:41:29.946	Thread Group 1-17	HTTP Request	1664	✓	3478	491	436	5
15	23:41:29.938	Thread Group 1-16	HTTP Request	1679	✓	3478	491	452	13
16	23:41:29.854	Thread Group 1-6	HTTP Request	1765	✓	3478	491	502	8
17	23:41:29.931	Thread Group 1-15	HTTP Request	1688	✓	3478	491	440	3
18	23:41:30.010	Thread Group 1-24	HTTP Request	1611	✓	3478	491	439	3
19	23:41:29.964	Thread Group 1-19	HTTP Request	1658	✓	3478	491	446	6
20	23:41:30.066	Thread Group 1-30	HTTP Request	1556	✓	3478	491	426	5
21	23:41:29.884	Thread Group 1-10	HTTP Request	1740	✓	3478	491	528	5
22	23:41:29.956	Thread Group 1-18	HTTP Request	1673	✓	3478	491	454	3
23	23:41:29.976	Thread Group 1-20	HTTP Request	1657	✓	3478	491	452	7
24	23:41:30.028	Thread Group 1-26	HTTP Request	1605	✓	3478	491	422	4
25	23:41:29.994	Thread Group 1-22	HTTP Request	1656	✓	3478	491	448	4
26	23:41:30.000	Thread Group 1-23	HTTP Request	1652	✓	3478	491	452	4
27	23:41:30.119	Thread Group 1-36	HTTP Request	1545	✓	3478	491	428	14
28	23:41:30.090	Thread Group 1-33	HTTP Request	1578	✓	3478	491	433	5
29	23:41:30.019	Thread Group 1-25	HTTP Request	1649	✓	3478	491	478	5
30	23:41:30.074	Thread Group 1-31	HTTP Request	1596	✓	3478	491	434	5
31	23:41:30.038	Thread Group 1-27	HTTP Request	1632	✓	3478	491	466	5
32	23:41:30.144	Thread Group 1-39	HTTP Request	1527	✓	3478	491	410	5
33	23:41:30.048	Thread Group 1-28	HTTP Request	1626	✓	3478	491	456	5
34	23:41:30.101	Thread Group 1-34	HTTP Request	1573	✓	3478	491	427	6

□ Scroll automatically? □ Child samples? No of Samples 110 Latest Sample 1778 Average 1607 Deviation 58



Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename

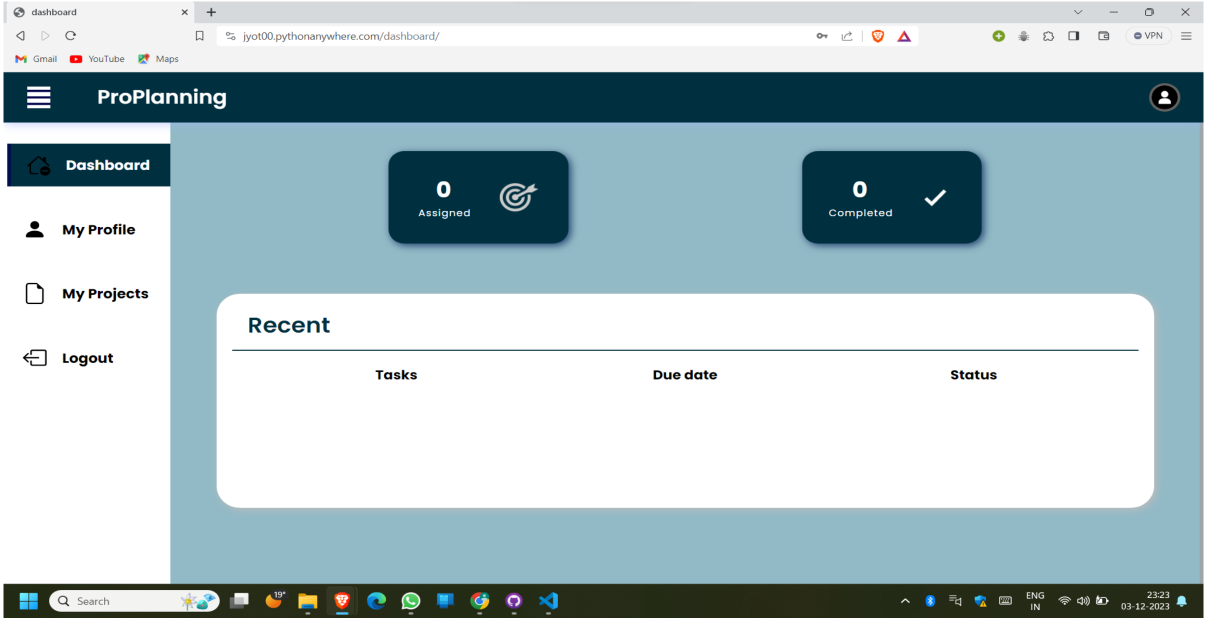
Browse... Log/Display Only: □ Errors □ Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
HTTP Request	478	11032	0	22681	8931.09	38.91%	33.0/min	2.01	0.23	3741.7
TOTAL	478	11032	0	22681	8931.09	38.91%	33.0/min	2.01	0.23	3741.7

3. Compatibility testing

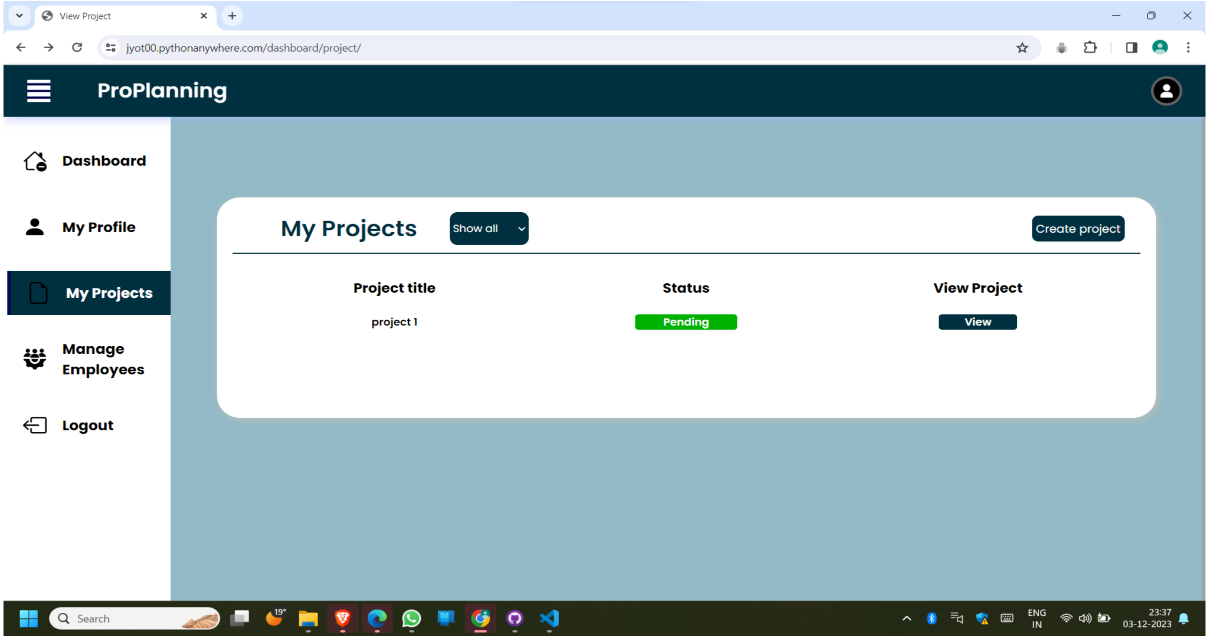
We have ensured that the portal runs on the all latest web browsers including Edge, Chrome, brave etc.

Brave



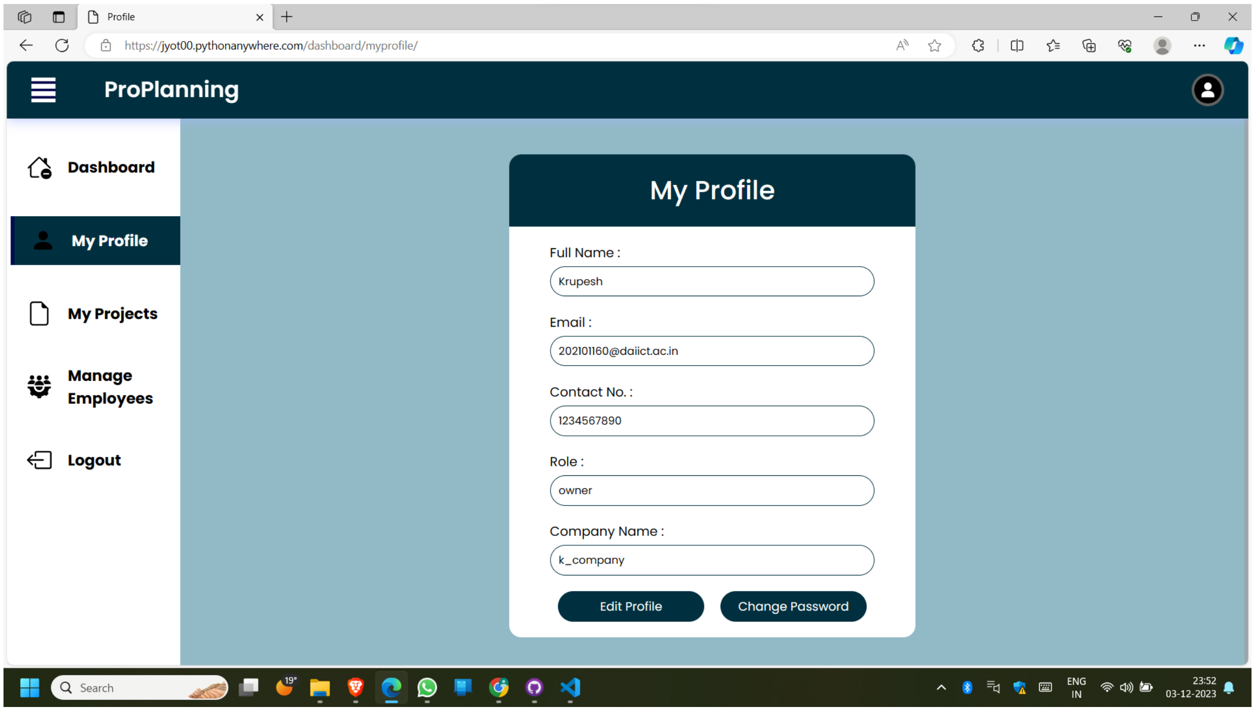
Tasks	Due date	Status

Chrome



Project title	Status	View Project
project 1	Pending	View

Microsoft Edge



My Profile

Full Name : Krupesh

Email : 202101160@daiict.ac.in

Contact No. : 1234567890

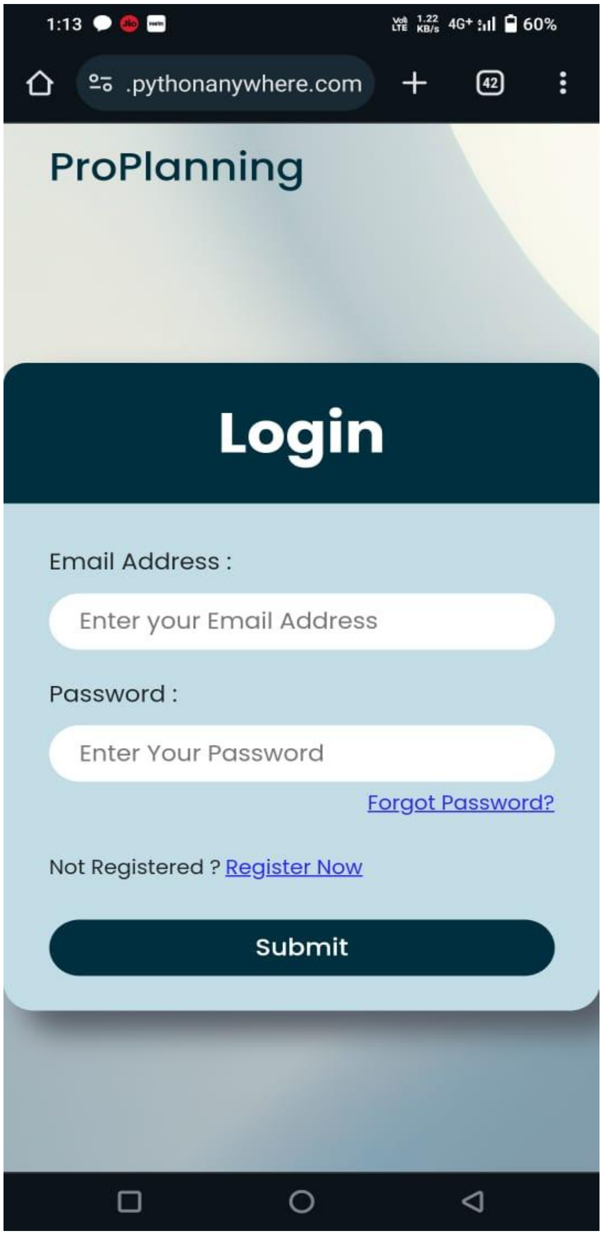
Role : owner

Company Name : k_company

4. Cross-device testing

In this testing process, we focuses on ensuring a seamless online experience for users across various devices. The primary objective is to achieve optimal functionality and user satisfaction through cross-device testing. Our testing phase included popular mobile devices such as the Vivo Y73, Oppo Reno6, Onepluse node CE etc.

Vivo Y73



ProPlanning

Login

Email Address :

Enter your Email Address

Password :

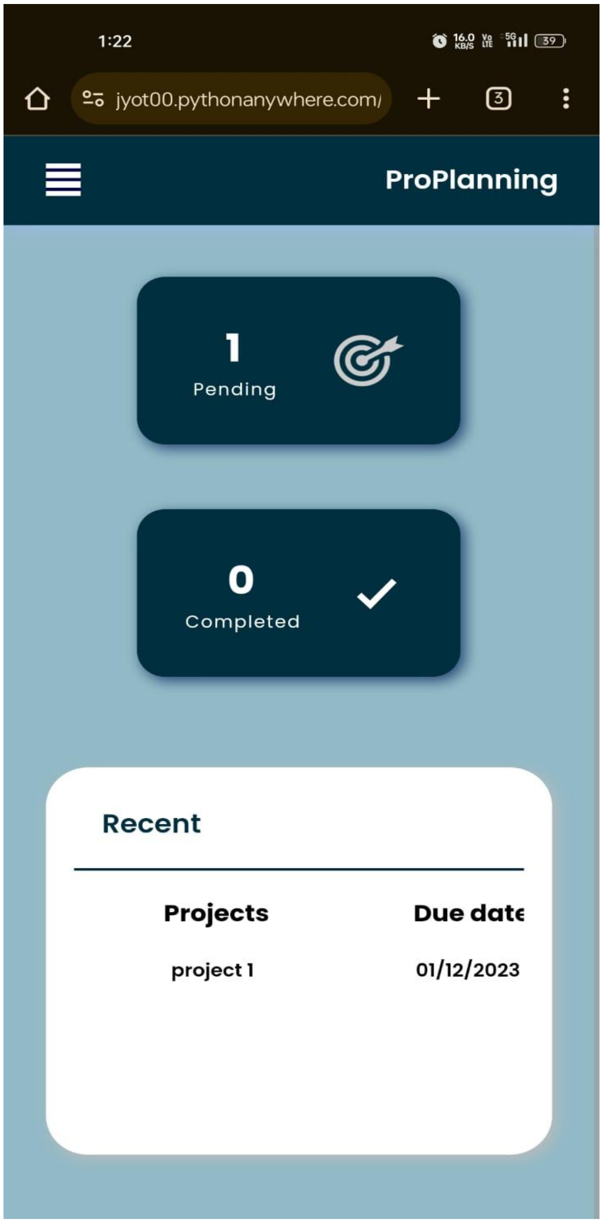
Enter Your Password

Forgot Password?

Not Registered ? Register Now

Submit

Oppo reno 6



ProPlanning

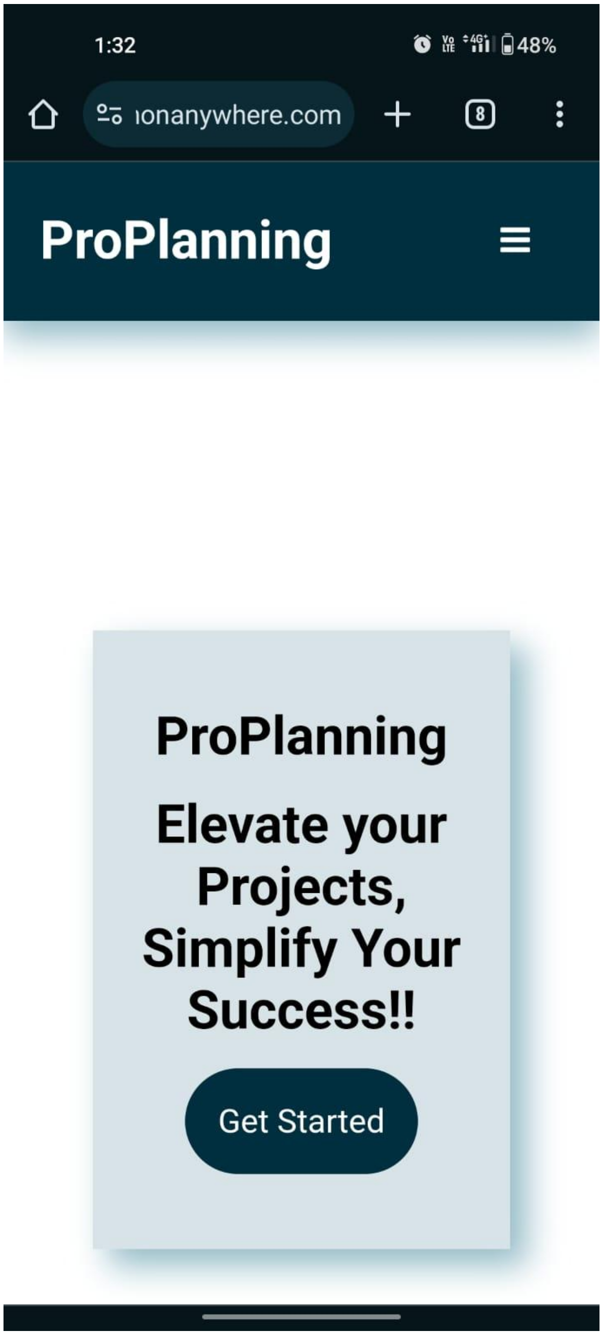
1
Pending

0
Completed

Recent

Projects	Due date
project 1	01/12/2023

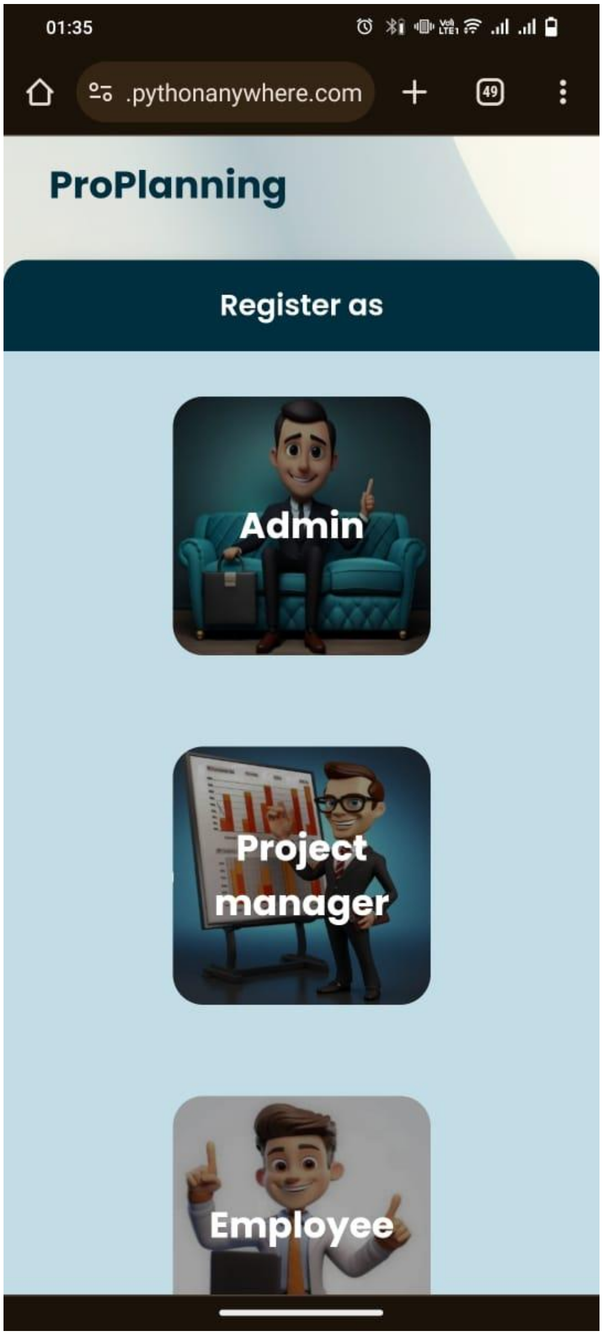
1+ node CE



ProPlanning

Elevate your Projects, Simplify Your Success!!

Iqoo Neo 6



Register as