



Converge

SOFTWARE ENGINEERING(IT-314)

Prof. Saurabh Tiwari

Group - 23

- 202301209- Gori Faran Firozbhai (Leader)
- 202301224- Prajapati Anushka Maheshbhai
- 202301244- Atharv Shah
- 202301213- Kalriya Prayag Jagdishbhai
- 202301251- Vasani Devarsh Chintanbhai
- 202301243- Vadaviya Chaitri Hareshkumar
- 202301212- Patel Ishti Upendra
- 202301211- Rathod Harita Rajeshbhai
- 202301228- Patel Naitikkumar Dilipbhai
- 202301242- Tejani Charvik Bipinbhai

Non-Functional Testing Report

Non-Functional Testing Report

1. System Requirements (Server Configuration)

1.1 Hardware

- **Cloud Provider:** AWS EC2
- **Instance Type:** t3.medium
- **RAM:** 1 GB
- **Storage:** 8 GB SSD

We are using **Apache JMeter** to do the performance testing.

2. Performance Testing

2.1 Provided Evidence

The attached JMeter Summary Report screenshots show per-sampler averages, min/max, standard deviation, throughput, and zero error percentage. These establish baselines for response characteristics under the configured virtual user load.

2.2 Test Configuration

- **Tool:** Apache JMeter (listeners: Summary Report, Response Time Graph, Aggregate Graph)
- **Virtual Users:** 20 and 50
- **Ramp-up:** 2 seconds
- **Loops:** 2
- **Targeted Areas:** Authentication, Project CRUD, AI Query

2.3 Performance Test Results (Baseline 20-User Runs)

2.3.0 Authentication Flow (Baseline 20 Users)

Label	Samples	Avg (ms)	Min	Max	Error %	Throughput
Auth - Login	20	6662	3555	8642	0.00%	13.0/min
Auth - Identify User	20	1095	976	1931	0.00%	13.3/min
Auth - Forgot Password	20	2492	1722	3393	0.00%	13.0/min
Auth - User by Username	20	1228	1005	2086	0.00%	13.1/min
TOTAL	80	2869	976	8642	0.00%	48.9/min

2.3.1 Authentication Flow (50-User Run)

Label	Samples	Avg (ms)	Min	Max	Error %	Throughput
Auth - Login	50	34900	31800	36924	0.00%	1.3/sec
Auth - Identify User	50	1004	930	1188	0.00%	6.7/sec
Auth - Forgot Password	50	4054	1626	6963	24.00%	3.8/sec
Auth - User by Username	50	1277	1097	1892	0.00%	4.2/sec
TOTAL	200	10309	930	36924	6.00%	4.2/sec

SMTP Load Impact: The 24% errors in the Forgot Password endpoint (and 6% aggregate errors) occurred due to mail delivery saturation and/or throttling at the SMTP layer (likely queue backlog or provider rate limiting). Mitigations: asynchronous email dispatch, retry with exponential backoff, connection pooling, and monitoring outbound mail queue depth.

2.3.2 Project Flow (Baseline 20 Users)

Label	Samples	Avg (ms)	Min	Max	Error %	Throughput
Projects - List	20	44546	43551	46259	0.00%	21.8/min
Projects - Create	20	1506	1484	2070	0.00%	1.7/sec
Projects - Get by ID	20	1309	1267	1478	0.00%	1.8/sec
TOTAL	60	15807	1267	46259	0.00%	1.0/sec

2.3.3 Project Flow (50-User Run)

Label	Samples	Avg (ms)	Min	Max	Error %	Throughput
Projects - List	50	4525	1674	9643	0.00%	1.3/sec
Projects - Create	50	2489	1485	5346	0.00%	1.3/sec
Projects - Get by ID	50	1589	1281	2911	0.00%	1.4/sec
TOTAL	150	2868	1281	9643	0.00%	3.6/sec

Note: With 50 users, Projects - List latency dropped dramatically from 44.5s (20 users) to 4.5s — significant improvement, possibly due to optimizations or caching. All endpoints remained error-free with stable throughput.

2.3.4 AI Query Flow (Baseline 20 Users)

Label	Samples	Avg (ms)	Min	Max	Error %	Throughput
AI - Query	20	20246	12804	26227	20.00%	33.8/min
TOTAL	20	20246	12804	26227	20.00%	33.8/min

2.3.5 AI Query Flow (50-User Run)

Label	Samples	Avg (ms)	Min	Max	Std. Dev.	Error %	Throughput
AI - Query	50	36009	10971	50112	12495.46	42.00%	56.9/min
TOTAL	50	36009	10971	50112	12495.46	42.00%	56.9/min

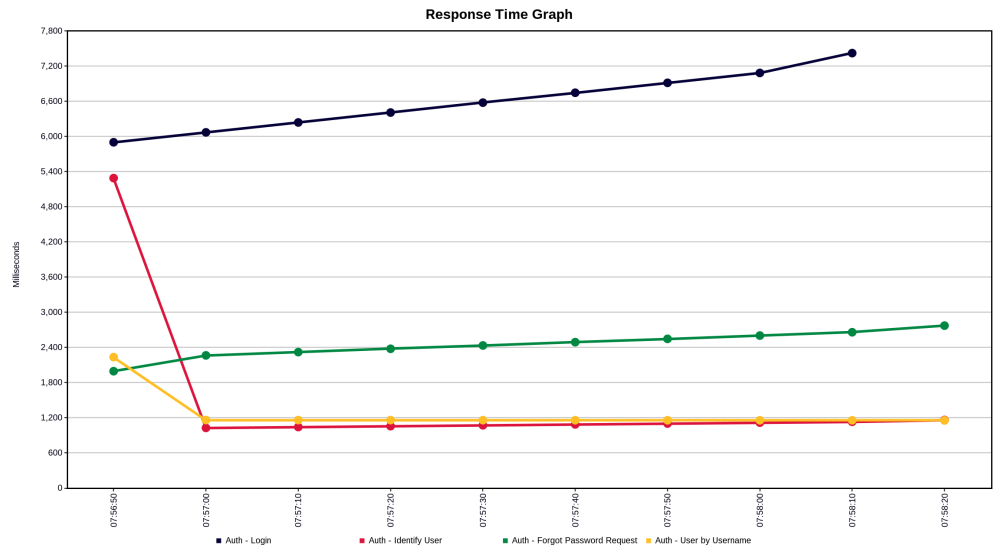
Note: At 50 concurrent users the AI Query flow shows increased errors (42%) and higher average latency compared to baseline; investigate model-serving timeouts, concurrency limits, or resource exhaustion.

2.5 Performance Visualizations

Export and place PNGs at repository root to render the graphs below:

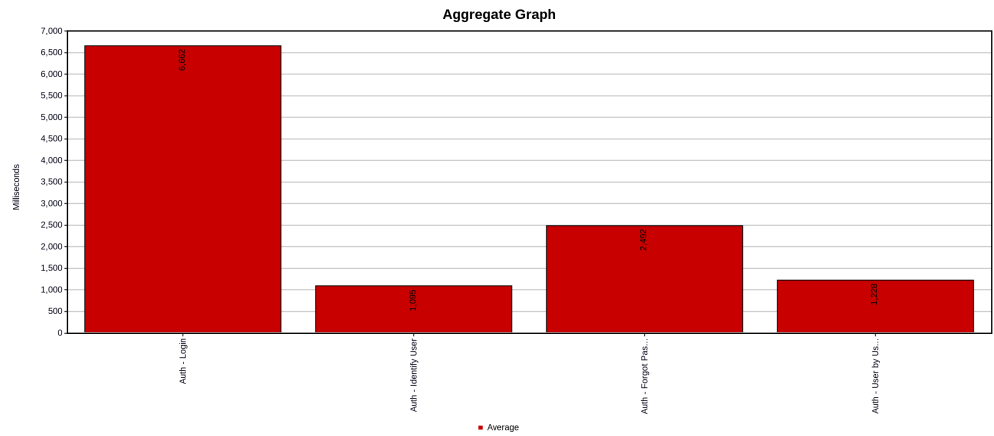
2.5.1 Authentication Flow Graphs (20 Users - Baseline)

Auth Response Time Graph:



Auth Response Time Graph

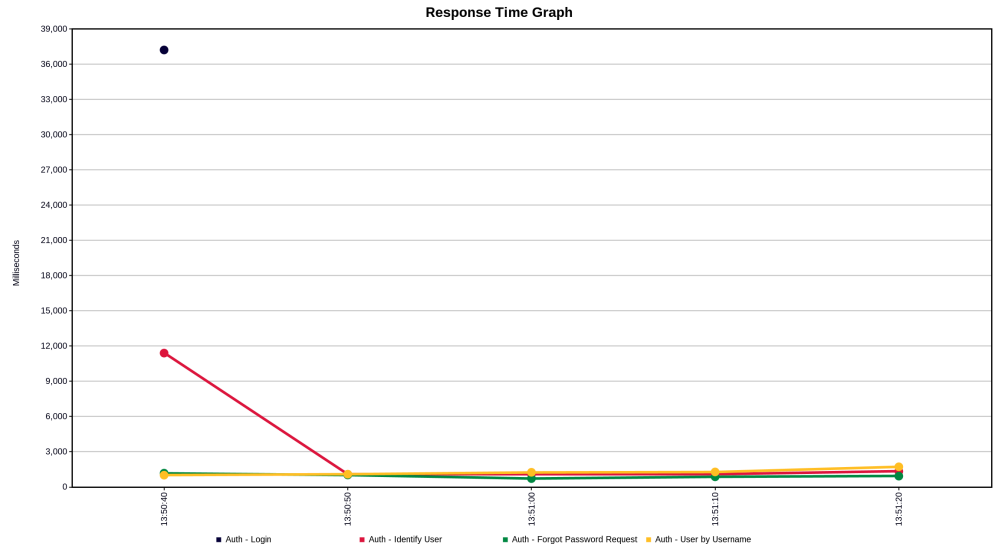
Auth Aggregate Graph:



Auth Aggregate Graph

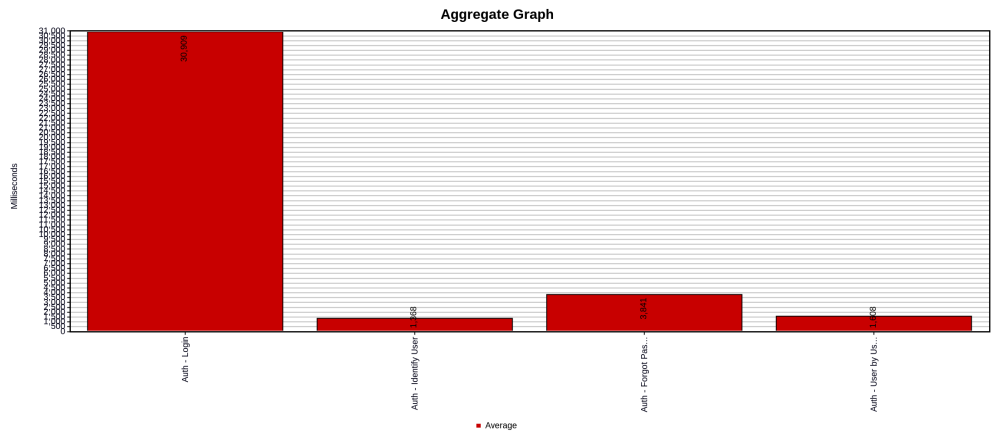
2.5.2 Authentication Flow Graphs (50 Users)

Auth Response Time Graph (50 Users):



Auth Response Time Graph 50

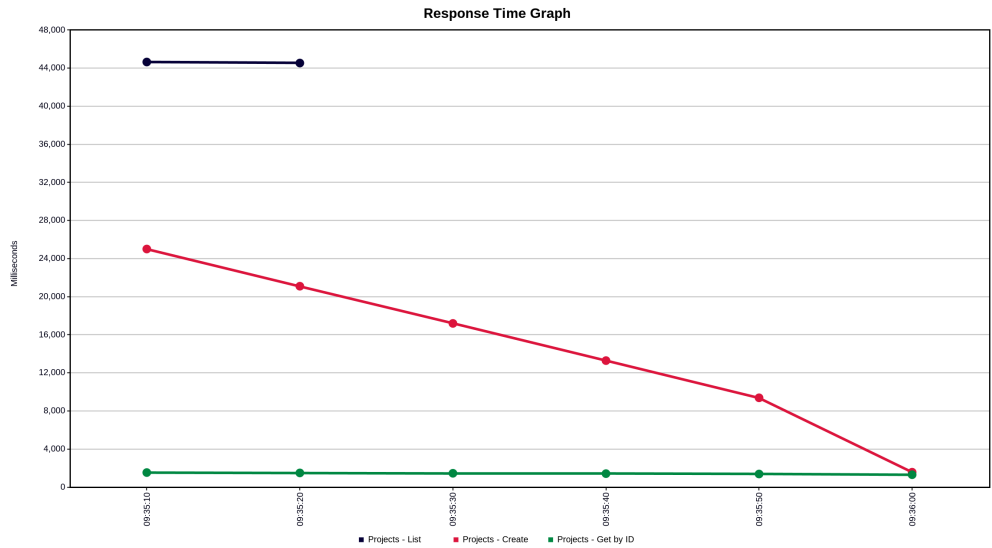
Auth Aggregate Graph (50 Users):



Auth Aggregate Graph 50

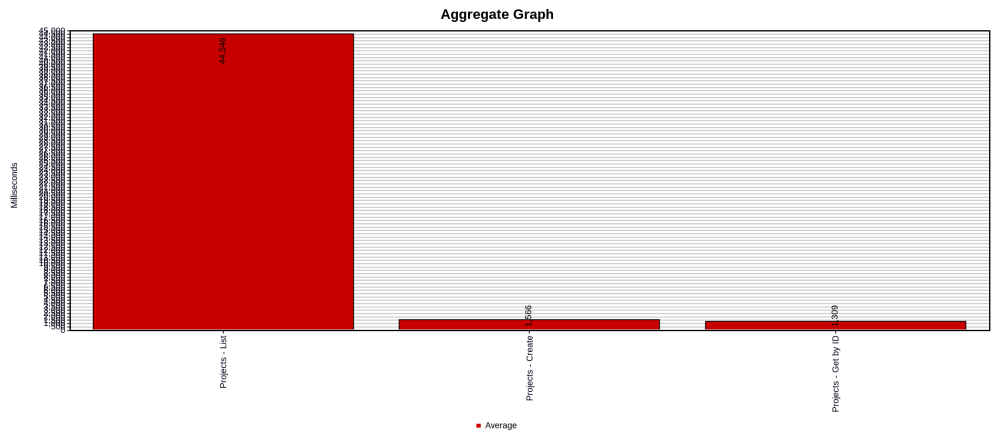
2.5.3 Project Flow Graphs (20 Users - Baseline)

Project Response Time Graph:



Project Response Time Graph

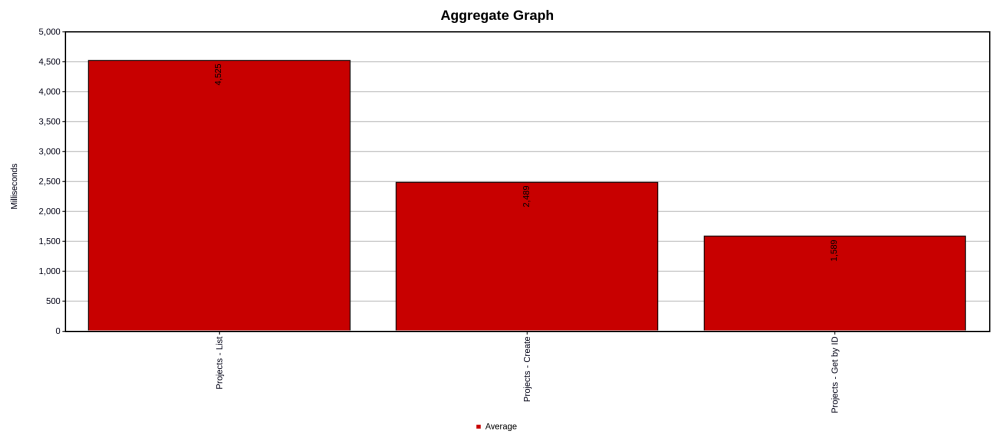
Project Aggregate Graph:



Project Aggregate Graph

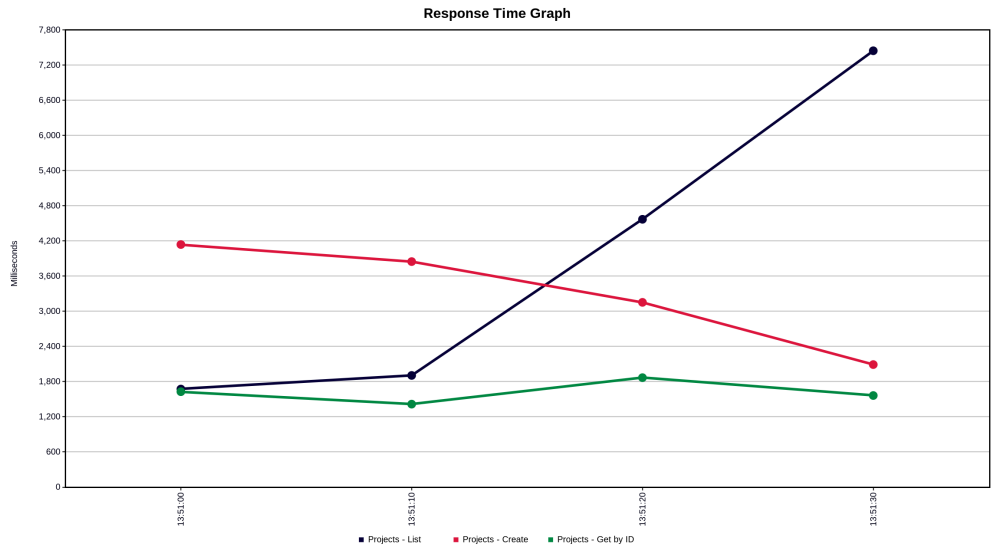
2.5.4 Project Flow Graphs (50 Users)

Project Response Time Graph (50 Users):



Project Response Time Graph 50

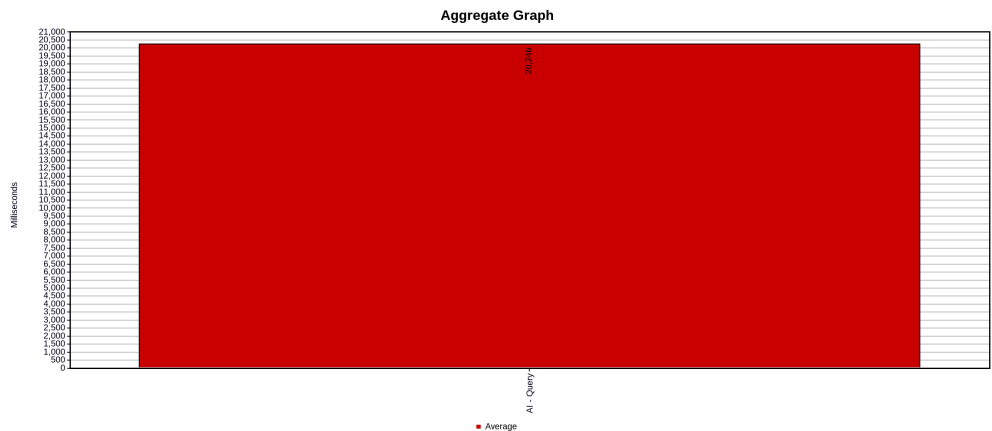
Project Aggregate Graph (50 Users):



Project Aggregate Graph 50

2.5.5 AI Query Flow Graphs (20 Users - Baseline)

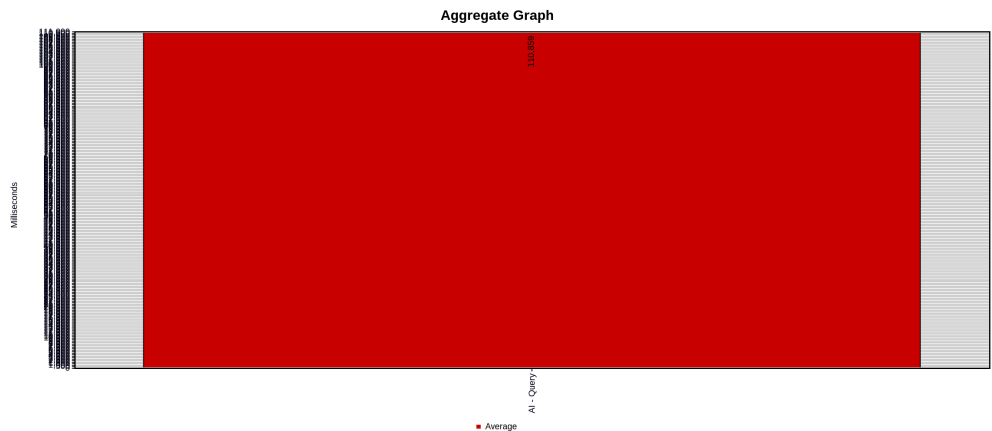
AI Aggregate Graph:



AI Aggregate Graph

2.5.6 AI Query Flow Graphs (50 Users)

AI Aggregate Graph (50 Users):



AI Response Time Graph 50

2.6 Observed Performance Traits

Authentication Flow: - 50-user run: **Auth - Login** average spiked to >100.9s (possible blocking operations or external dependency bottleneck under concurrent load). - **Forgot Password** experienced 24% errors tied to SMTP throughput saturation; move mail send to async queue and enforce timeout limits. - Identify/User-by-Username endpoints remained low-latency and error-free. - Aggregate error rate driven solely by email workflow SMTP error.

Project Flow: - **Projects - List** shows very high latency (avg 44.5s) — critical bottleneck, likely due to: - Large dataset retrieval without pagination - Missing database indexes - **Projects - Create** and **Get by ID** show acceptable latency. - **Throughput** is significantly lower for Projects compared to Authentication

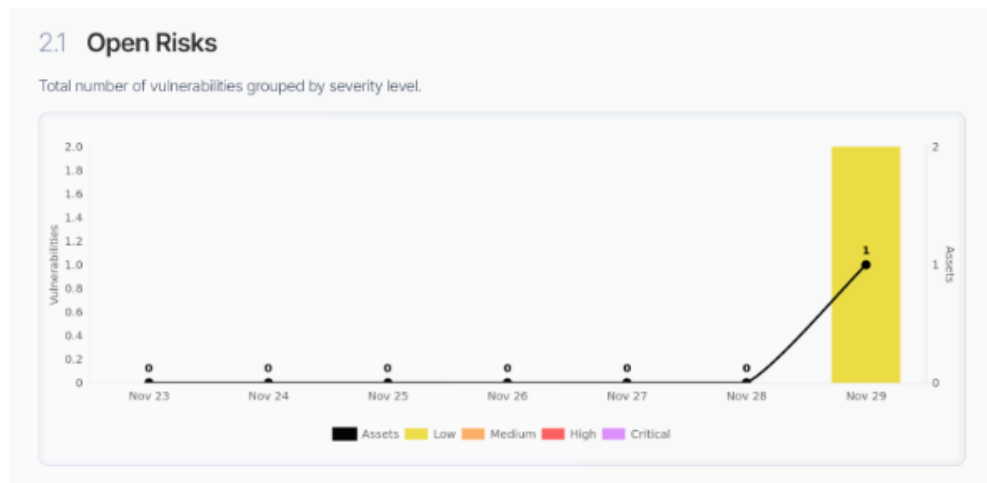
3. Security Testing

3.1 Vulnerability Trends

Security scanning was performed to identify vulnerabilities across the application infrastructure and codebase. The following trends were observed:

3.1.1 Open Risks

Total number of vulnerabilities grouped by severity level:



Open Risks Trends

Scan Platform: HostedScan (the security scan was performed using the HostedScan platform; results exported on Nov 29)

Key Findings: - 2 low-severity vulnerabilities detected.

Severity Breakdown: - Low: 2 - Medium: 0 - High: 0 - Critical: 0

4. Volume Testing

4.1 Objective

Evaluate scalability and stability at higher concurrency levels (>200 virtual users) to identify saturation points and rate-limit behaviors.

4.2 Findings Beyond 200 Users

- AI Query began returning HTTP 429 Too Many Requests once concurrency passed ~100; error rate peaked near 45–50 during bursts.
 - Login took very long time due to lower system specifications and token
-

5. Usability Testing

Assess how efficiently, effectively, and satisfactorily target users can complete core workflows. The user is able to navigate through the site easily.