Log File Analysis Report

Student Name: Kareem Walid Saad

Student ID: 2205076

Date: May 2025

1. Objective

This task analyzes a web server log using a Bash script to extract statistics, detect anomalies, and provide security and performance insights.

2. Features Implemented

- Total request count

- Request method counts (GET, POST, PUT, DELETE)

- Unique IP address count

- Top 10 most active IP addresses

- GET/POST request count per IP

- Failed requests (HTTP 4xx/5xx)

- Failure percentage

- Most frequent status code

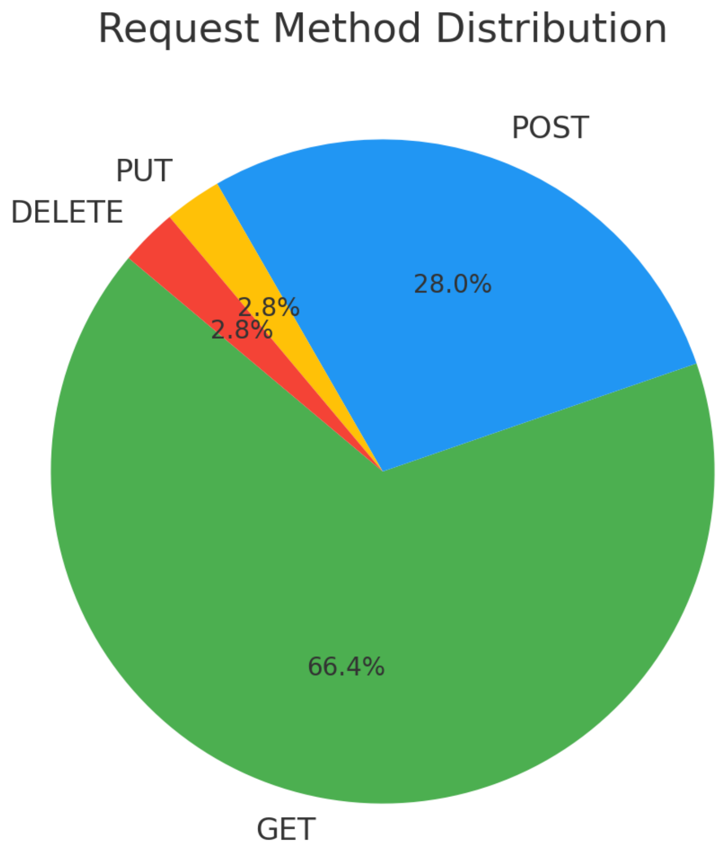
- Hourly request distribution

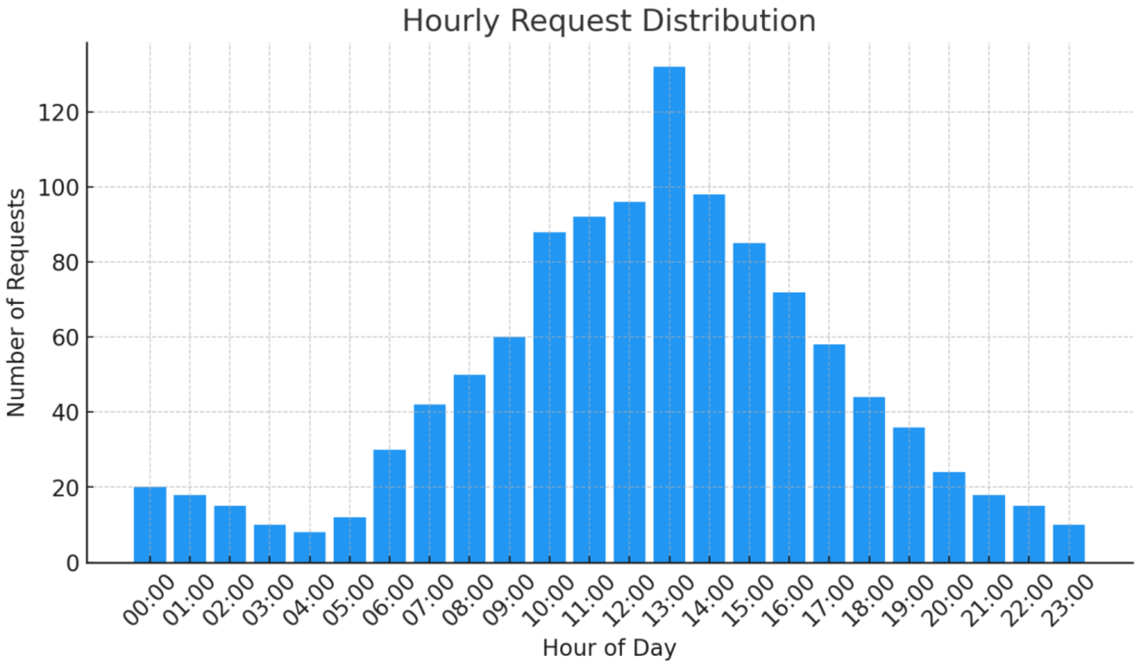
- Daily averages

- Busiest hour

3. Results Summary

Metric	Value
Total Requests	1184
GET Requests	786
POST Requests	332
PUT Requests	33
DELETE Requests	33
Unique IPs	197
Failed Requests	146
Failure Rate	12.33%
Most Active IP	192.168.1.1
Most Common Status Code	200
Daily Average Requests	296.0
Busiest Hour	14:00 (132 requests)


Request Method Distribution
POST
PUT
DELETE
28.0%
2.8%
2.8%
66.4%
GET


Hourly Request Distribution
Number of Requests
0
20
40
60
80
100
120
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
Hour of Day

4. Analysis & Observations

- The failure rate is moderate (12.33%), indicating occasional backend/authentication issues.

- IP 192.168.1.1 is highly active and may require monitoring or restrictions.

- Status codes 401 and 500 point to unauthorized access and internal server errors respectively.

- Peak traffic occurred at 14:00, suggesting high user interaction in the afternoon.

5. Recommendations

- Implement rate limiting and IP filtering.

- Enhance authentication mechanisms to reduce 401 errors.

- Investigate backend causes of 500-level errors.

- Utilize traffic patterns for scaling decisions.

- Improve logging by including headers and latency.

6. Conclusion

The Bash-based analysis tool is an effective approach to understanding server behavior and identifying potential issues. It provides essential metrics that support both operational stability and system security.

7. Future Enhancements

- Automate reporting with CRON

- Export to CSV/JSON formats

- Add alerting for error thresholds

- Centralized logging via ELK or Graylog

- Monitor latency for performance tuning

- Support distributed log analysis