Investigation Report: IEUK Engineering Sector Skills

Marcus Aviles

Wednesday 16th July, 2025

1 Introduction

The website experienced repeated service disruptions. A log of HTTP requests made to the server was provided to determine the source of the issue. This report outlines the methodology used to analyse the data and highlights key findings that point to the root cause of the shutdowns.

2 Assumptions

The assumptions I made: request logs contain IP addresses, country code, timestamps, http request, status code, response size, device information, response time; No rate limiting per IP address;

3 Analysis

The data had to be cleaned:

- Removed white space an unnecessary symbols from each log
- Separated each key data in each log
- Converted each log into an log data object

Grouped logs into windows of time

- Grouped logs into the time frames, 1 minute apart
- Calculated the time frame with the highest average number of failures

Initial inspection of logs from the highest average failure window showed IP addresses with suspicious activity, such as high number of http requests within 1 minute, and repetitive requests.
Inspected IP addresses

- Inspection of the time frame with highest average number of failures
- Get the top 5 IP addresses that had the highest number of requests
- output their logs

Key observations:

- Certain IPs send 12 requests to the server within the time frame
- All requests by these IP addresses are related to signing in and logging in
- All requests to sign up and login have the username "chris" or "lisa", and have simple passwords like "welcome123" and "Test123"

```
185.220.100.77
URL: POST /api/auth/login?username=chris&password=temp HTTP/1.1 | STATUS CODE: 401
URL: POST /api/admin/login?username=chris&password=summer2024 HTTP/1.1 | STATUS CODE: 401
URL: POST /login?username=chris&password=company123 HTTP/1.1 | STATUS CODE: 401
URL: POST /api/auth/signin?username=chris&password=password321 HTTP/1.1 | STATUS CODE: 423
URL: POST /admin/login?username=lisa&password=qwerty HTTP/1.1 | STATUS CODE: 429
URL: POST /api/v1/auth/login?username=lisa&password=password1 HTTP/1.1 | STATUS CODE: 401
URL: POST /auth/signin?username=lisa&password=admin123 HTTP/1.1 | STATUS CODE: 401
URL: POST /api/login?username=lisa&password=guest HTTP/1.1 | STATUS CODE: 401
URL: POST /api/auth/login?username=lisa&password=temp HTTP/1.1 | STATUS CODE: 401
URL: POST /api/admin/login?username=lisa&password=summer2024 HTTP/1.1 | STATUS CODE: 401
URL: POST /login?username=lisa&password=company123 HTTP/1.1 | STATUS CODE: 401
URL: POST /api/auth/signin?username=lisa&password=password321 HTTP/1.1 | STATUS CODE: 423
```

Figure 1: Example of suspicious IP address's request

4 Root Cause

Based on the evidence, the root cause appears to be a denial-of-service attack. The server failed to handle the excessive load, leading to downtime.

5 Conclusion and Recommendations

The website shutdowns were caused by high-frequency requests from specific IP addresses. To mitigate this:

- Implement rate limiting per IP address (free)
- Enable bot detection and challenge mechanisms like CAPTCHA (cheap)
- Monitor traffic patterns and alert on anomalies (requires time and money)