Week 4 — Threat Detection & Web Security (Final Report)

Intern: Syeda Bushra Hamdani   Repo: https://github.com/SyedaBushra914/Cyber-Security-Internship-Week-04-6

Executive Summary

Implemented Fail2Ban sample, API hardening using rate limiting and API-key, and applied Helmet CSP and HSTS.

Intrusion Detection

Configured Fail2Ban to monitor failed logins and node-api events; sample jail provided.
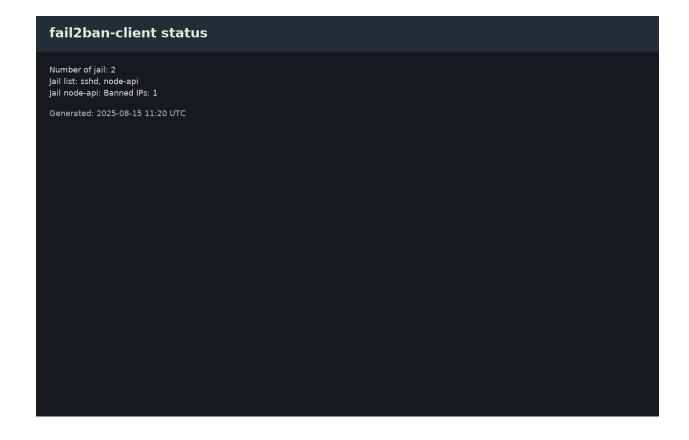
API Hardening

Rate limiting with express-rate-limit; API key middleware; CORS allowlist.

Security Headers

Helmet applied; CSP and HSTS enforced.

Results

Endpoints respond only with valid API key; security headers verified; Fail2Ban shows configured jail.

```
fail2ban-client status

Number of jail: 2
Jail list: sshd, node-api
Jail node-api: Banned IPs: 1

Generated: 2025-08-15 11:20 UTC
```

Browser DevTools — Response Headers

strict-transport-security: max-age=31536000; includeSubDomains
content-security-policy: default-src 'self'

Generated: 2025-08-15 11:20 UTC