Task 4 Findings

Name: Abdullah Akram

Roll No: DHC-3606

Week: 4

Title: Advanced Threat Detection & Web Security Enhancements

July 13, 2025

1 Introduction

During Week 4 of the Cyber Security Internship, key security enhancements were implemented to fortify a PHP-based login system. This document presents the findings from the implementation of advanced threat detection and web security measures, focusing on the effectiveness of API security hardening, rate limiting, and security header configurations. The findings validate the system's improved resilience against common web threats and its alignment with internship objectives.

2 API Security Findings

The API security measures implemented in `login.php` were tested to ensure robust protection:

- **API Key Authentication**: The system successfully validates requests using the `X-API-KEY` header against the `API_SECRET_KEY` defined in `config.php`. Unauthorized requests without a valid key consistently return an HTTP 401 Unauthorized response, confirming that only trusted clients can access the API endpoints.
- **Rate Limiting Effectiveness**: Rate limiting restricts each IP to 5 login attempts per minute, with data stored in JSON files within a secure `rates/` folder. Testing showed that exceeding this limit triggers an HTTP 429 Too Many Requests response, effectively mitigating brute-force attack risks. The use of a dedicated folder with `.htaccess` (Deny from all) ensures that rate-limiting files are inaccessible via the browser.
- **CORS Restrictions**: Cross-Origin Resource Sharing (CORS) headers were configured to allow only POST and OPTIONS methods, with headers like `Content-Type` and `X-API-KEY` permitted. For development, `Access-Control-Allow-Origin: *` was used Fragile-X syndrome, but it will be restricted to the production domain in deployment, ensuring controlled access.

3 Security Headers Findings

The implementation of security headers significantly strengthened the application:

- **Content Security Policy (CSP)**: The CSP restricts resources to `self`, preventing unauthorized script or style injections. Testing confirmed that external scripts are blocked, and only inline styles (with `unsafe-inline`) are permitted to maintain compatibility with the existing UI.
- **HSTS Enforcement**: The `Strict-Transport-Security` header enforces HTTPS with a 2-year `max-age`, ensuring encrypted connections across all subdomains. This enhances user trust by preventing man-in-the-middle attacks.
- **Additional Protections**: Headers like `X-Content-Type-Options: nosniff`, `X-Frame-Options: DENY`, and `X-XSS-Protection: 1; mode=block` were validated to prevent MIME-type sniffing, clickjacking, and enable browser-level XSS protection, respectively, with no negative impact on functionality.

4 System Behavior and User Experience

Testing revealed the following user-facing outcomes:

- **Successful Logins**: Valid credentials correctly authenticate users, set session variables (_SESSION['id'], username, etc.), and redirect to dashboard.php, ensuring a seamless login experience.
- **Error Handling**: Invalid credentials or excessive login attempts display clear error messages (e.g., ”User not found” or ”Too many requests”) in a styled alert box, maintaining user-friendliness while enforcing security.
- **Production Readiness**: The system is fully functional on a local XAMPP environment (http://127.0.0.1/home-rental/) and ready for production with minor adjustments (e.g., updating CORS origins and enabling JWT for token-based authentication).

5 Conclusion

The findings confirm that the Week 4 security enhancements have effectively hardened the PHP-based login system. API key authentication and rate limiting provide strong defenses against unauthorized access and brute-force attacks, while CORS and security headers (CSP, HSTS, etc.) ensure protection against script injections and insecure connections. The system is robust, user-friendly, and compliant with internship requirements, with potential for future enhancements like JWT integration or Linux-based intrusion detection.