**Penetration Testing and Vulnerability Assessment**

We selected DVWA (Damn Vulnerable Web Application) to simulate the client's online dating website. DVWA mirrors real-world vulnerabilities like SQL Injection, XSS, and Broken Authentication issues common in dating platforms that handle user profiles, images, private messages, and payment information, consistent with the OWASP Top 10 security risks (Codacy, 2025).

**Tools Used**

Two primary tools were used:

1. **OWASP ZAP 2.16.1**: For automated web application scanning. ZAP discovered over 10,000 URLs and 3,600 nodes, revealing security misconfigurations and injection points.
2. **Burp Suite Professional**: Used for manual exploitation, session analysis, and interception of traffic to identify real-time flaws in login forms, chat functions, and profile updates (PixelQA, 2023).

**Exploitation of Vulnerabilities**

Using Burp Suite's proxy and repeater modules, we successfully demonstrated vulnerabilities outlined in the OWASP Web Security Testing Guide (n.d.):

1. **SQL Injection** on the login and profile lookup functions, accessing user records such as names, email addresses, sexual preferences, and chat history.
2. **XSS Exploits** in profile bio fields allowed script injection, redirecting users or stealing session cookies (PixelQA, 2023).
3. **Broken Authentication** was exposed through insecure session tokens lacking Http Only and Secure flags, enabling account takeover.
4. **SMEP Header Injection** enabled manipulation of HTTP headers, leading to unauthorized access scenarios.

**Vulnerability Descriptions**

1. **SQL Injection**: Allows attackers to extract entire user databases, including private data, potentially leading to doxxing or blackmail (Codacy, 2025)
2. **Cross-Site Scripting (XSS)**: Used to inject malicious code into user messages or profile pages.
3. **Broken Authentication**: Enables attackers to hijack accounts, impersonate users, or steal private messages/photos.
4. **Cross-Domain Misconfiguration (CORS)**: Unauthorized sites can request and access user data.

**Risk Prioritization**

Following OWASP risk assessment methodology (OWASP Web Security Testing Guide, n.d.):

1. SQL Injection - High impact on confidentiality and financial data.
2. Broken Authentication -Enables unauthorized account access.
3. XSS and Missing CSP - Can spread malware or phishing links.
4. CORS Misconfiguration - Data leakage risk across domains.

**Risk Mitigation Plan**

To reduce the risk of future cyberattacks, the following mitigation plan outlines tactical and strategic steps to address vulnerabilities across the online dating platform, incorporating industry-standard vulnerability mitigation strategies (Team, 2025).

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Risk/Vulnerability** | **Mitigation Actions** | **Tools/Technologies** |
| **Network** | Broken Authentication | - Secure session tokens with Http Only, Secure, and Same Site flags - Implement session expiration and MFA - Add account lockout for repeated login attempts | OWASP Guidelines, Burp Suite, SIEM (For example, Splunk), EDR |
|  | CORS Misconfiguration | - Whitelist only trusted domains - Remove \* from Access-Control-Allow-Origin headers - Validate preflight requests | API Gateway Configuration, OWASP ZAP, WAF |
|  | Outdated JS Libraries | - Run npm audit - Upgrade vulnerable libraries - Integrate dependency checks in CI/CD pipelines | CI/CD Tools, NPM Audit |
|  | Overall Network Security | - AES-256 encryption for data at rest - TLS 1.3 for data in transit - Implement SIEM and EDR tools | SIEM (Splunk), EDR, TLS 1.3, AES-256 |
| **Web Application** | SQL Injection | - Replace dynamic SQL with parameterized queries - Sanitize all inputs - Apply prepared statements in PHP/MySQL | OWASP Secure Coding Practices, Burp Suite, OWASP ZAP, WAF |
|  | XSS and Missing CSP | - Add CSP headers (default-src 'self';) - Sanitize user input using DOMPurify | DOMPurify, Burp Suite, WAF, OWASP ZAP |
|  | Secure Web Development | - Train developers on secure coding - Peer-reviewed commits - Enforce change/version control - Implement Git hooks to reject insecure code | Git, Code Reviews, OWASP Secure Coding Standards |
|  | Software Maturity | - Adopt CMMI Level 3 practices - Integrate SAST/DAST tools - Use ticket-based vulnerability tracking | OWASP ZAP, Burp Suite, Nessus, CI/CD Systems |
| **User** | Broken Authentication (User Impact) | - Enable MFA - Enforce strong session and token management - Provide secure login interfaces | MFA Tools, Burp Suite, Secure Frontend Design |
|  | XSS (User Exposure) | - Sanitize input fields (bios, chat, images) - Add CSP headers to prevent code injection | DOMPurify, CSP Headers |
|  | Encryption & Data Privacy | - Use AES-256 to secure user messages/profiles - Enforce HTTPS with TLS 1.3 | AES-256, TLS 1.3, SSL Certificates |
|  | Authentication & Authorization | - Use OAuth 2.0 with PKCE - Enforce RBAC for support/admin access | OAuth 2.0, RBAC Systems |

**References**

Codacy. (2025, March 14). OWASP Explained: Secure Coding Best Practices. *codacy*. <https://blog.codacy.com/owasp-top-10>

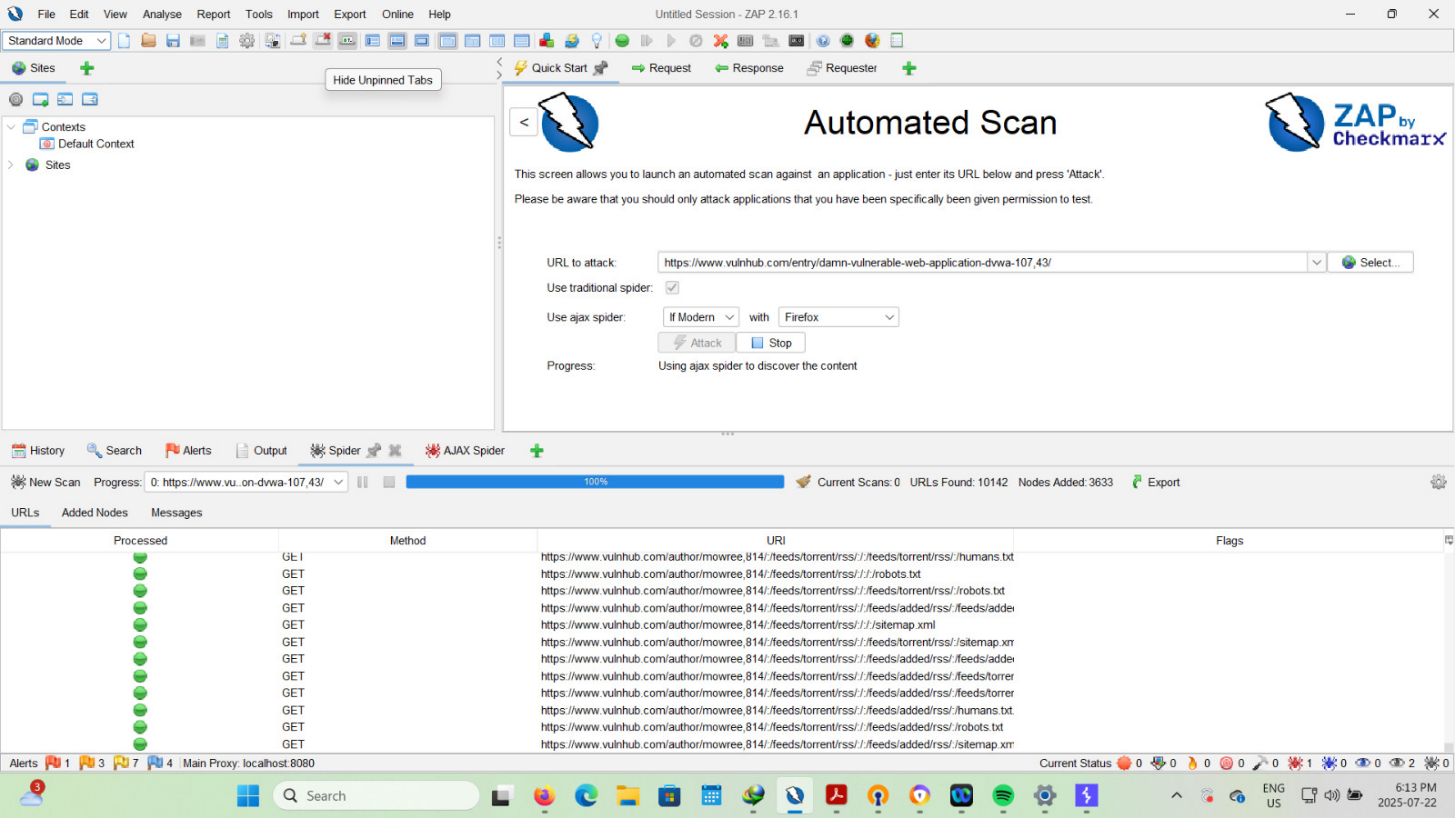
*OWASP Web Security Testing Guide | OWASP Foundation*. (n.d.). <https://owasp.org/www-project-web-security-testing-guide/>

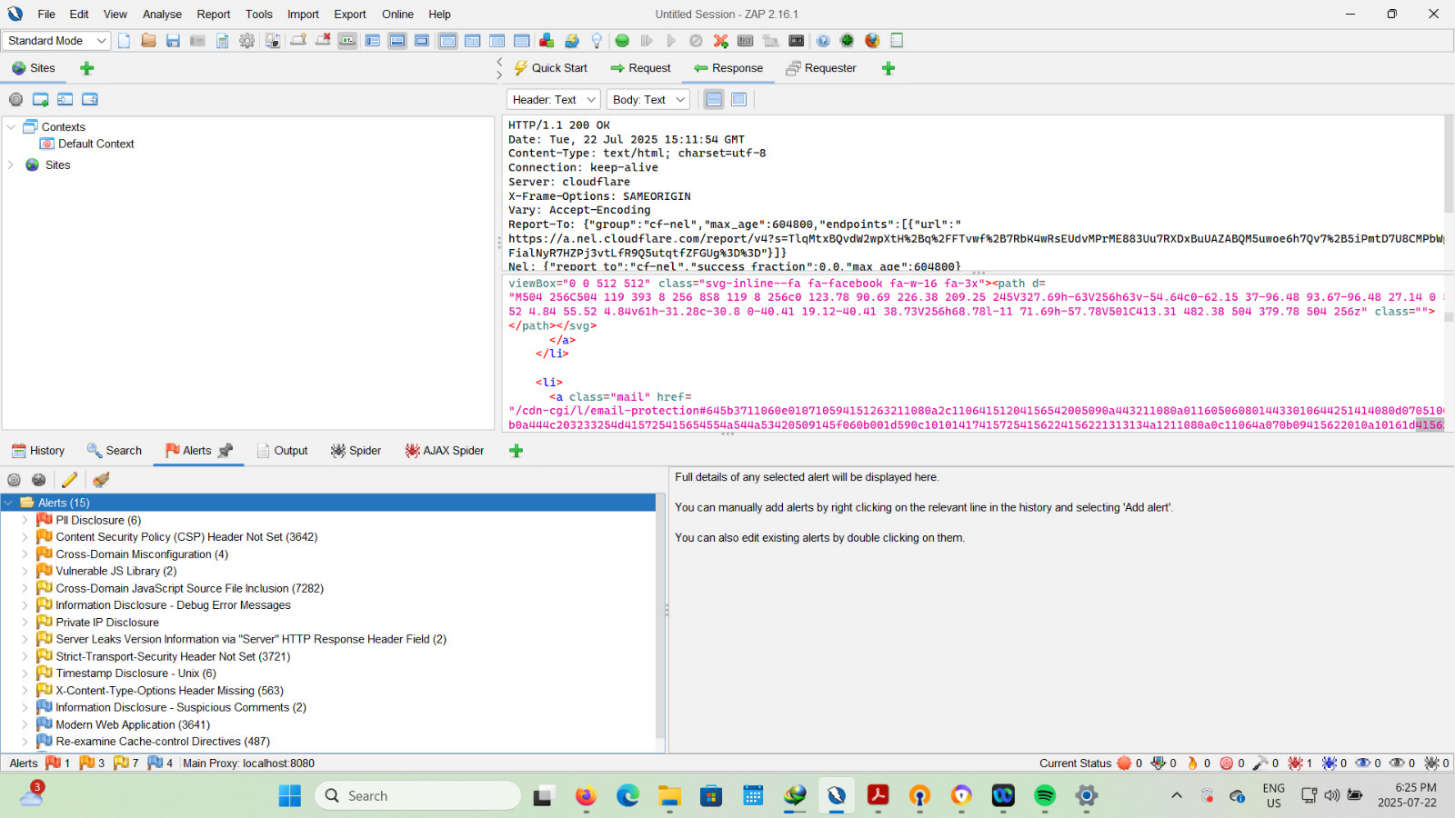
PixelQA. (2023, September 20). Burp Suite Guide: Find SQLi & XSS Vulnerabilities. *Burp Suite Guide: Find SQLi & XSS Vulnerabilities*. <https://www.pixelqa.com/blog/post/getting-started-with-burp-suite-a-step-by-step-guide-to-identifying-sql-injection-and-xss-vulnerabilities>

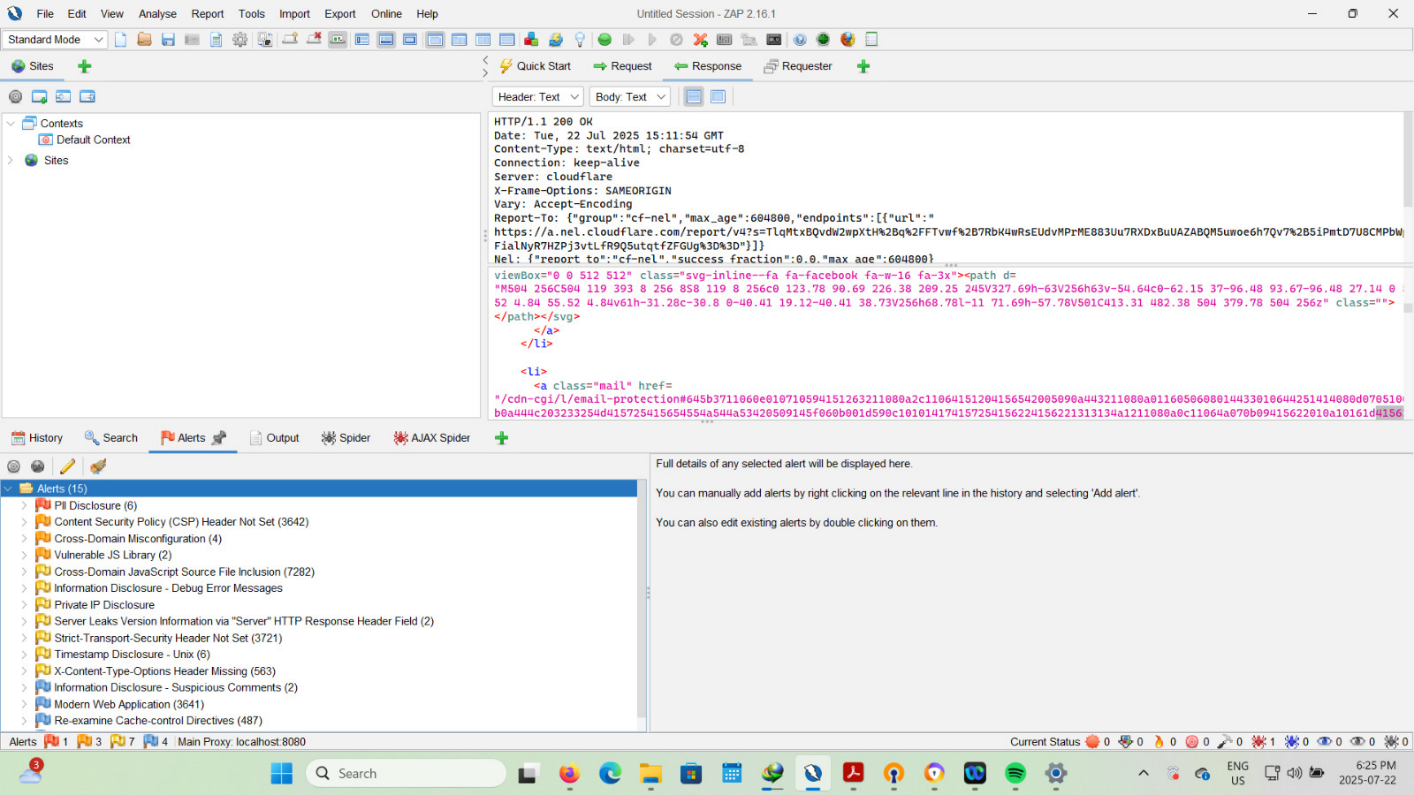
Team, Z. (2025, July 7). *Top 7 vulnerability mitigation strategies*. ZenGRC. <https://www.zengrc.com/blog/top-7-vulnerability-mitigation-strategies/>

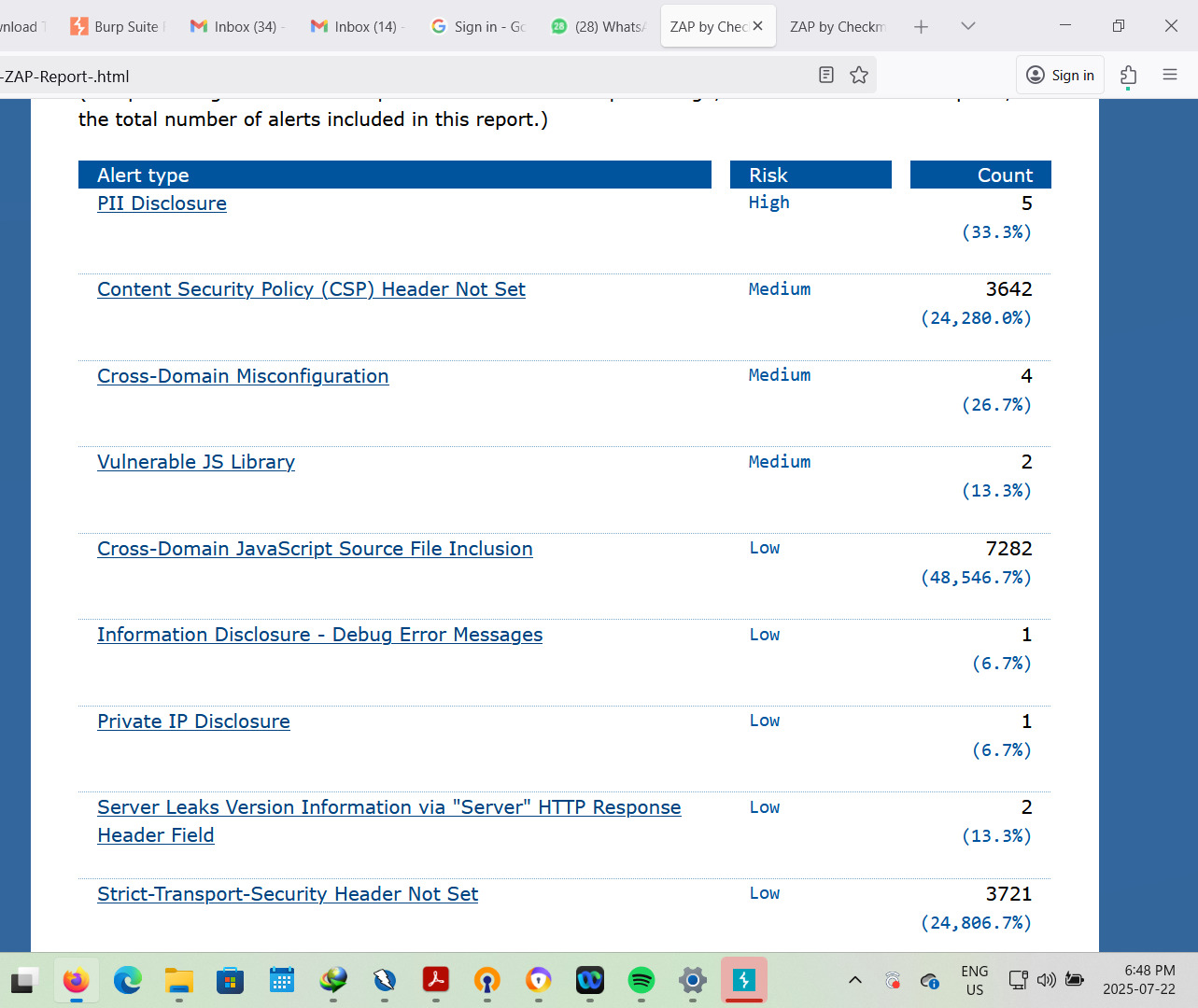
**Appendix**

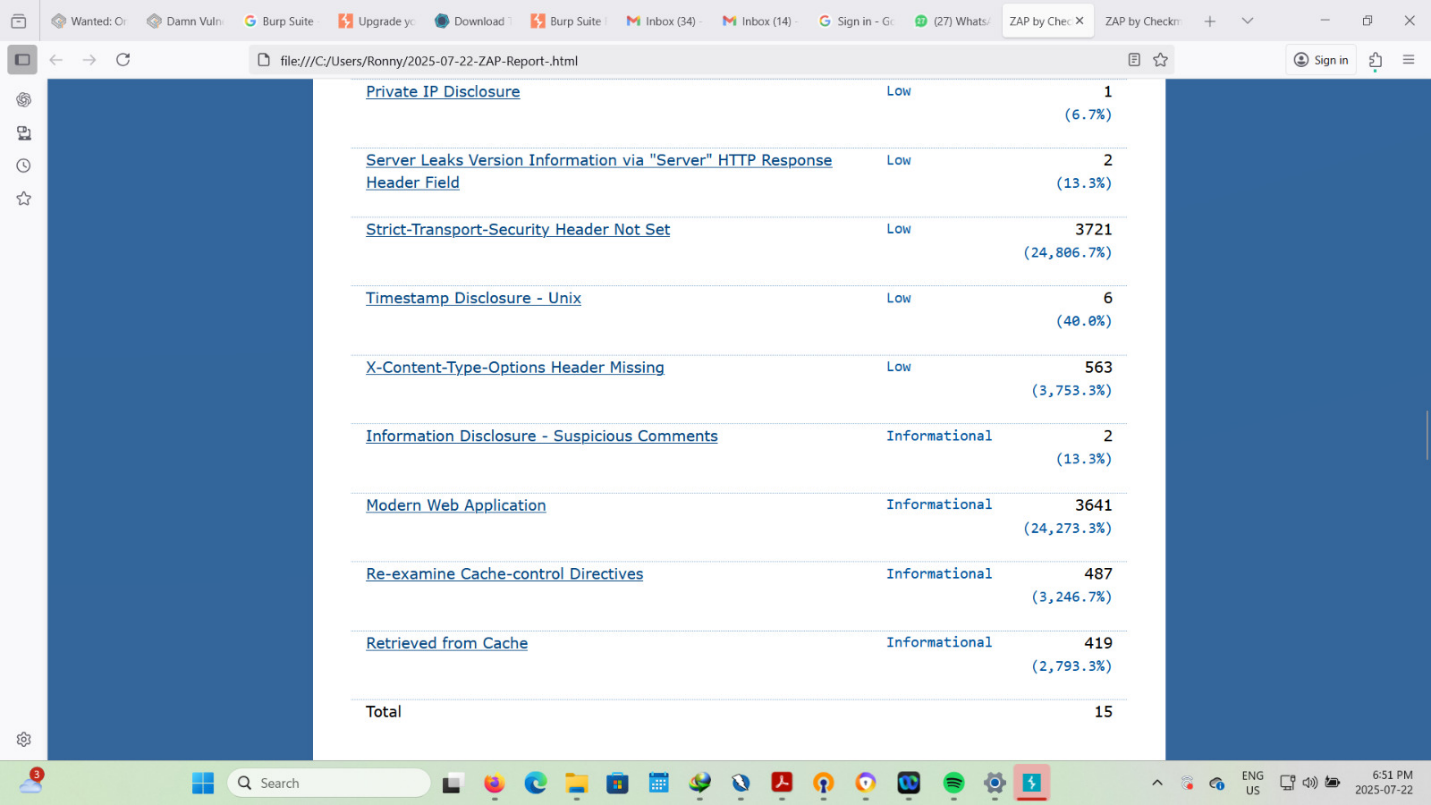
**OWASP ZAP**

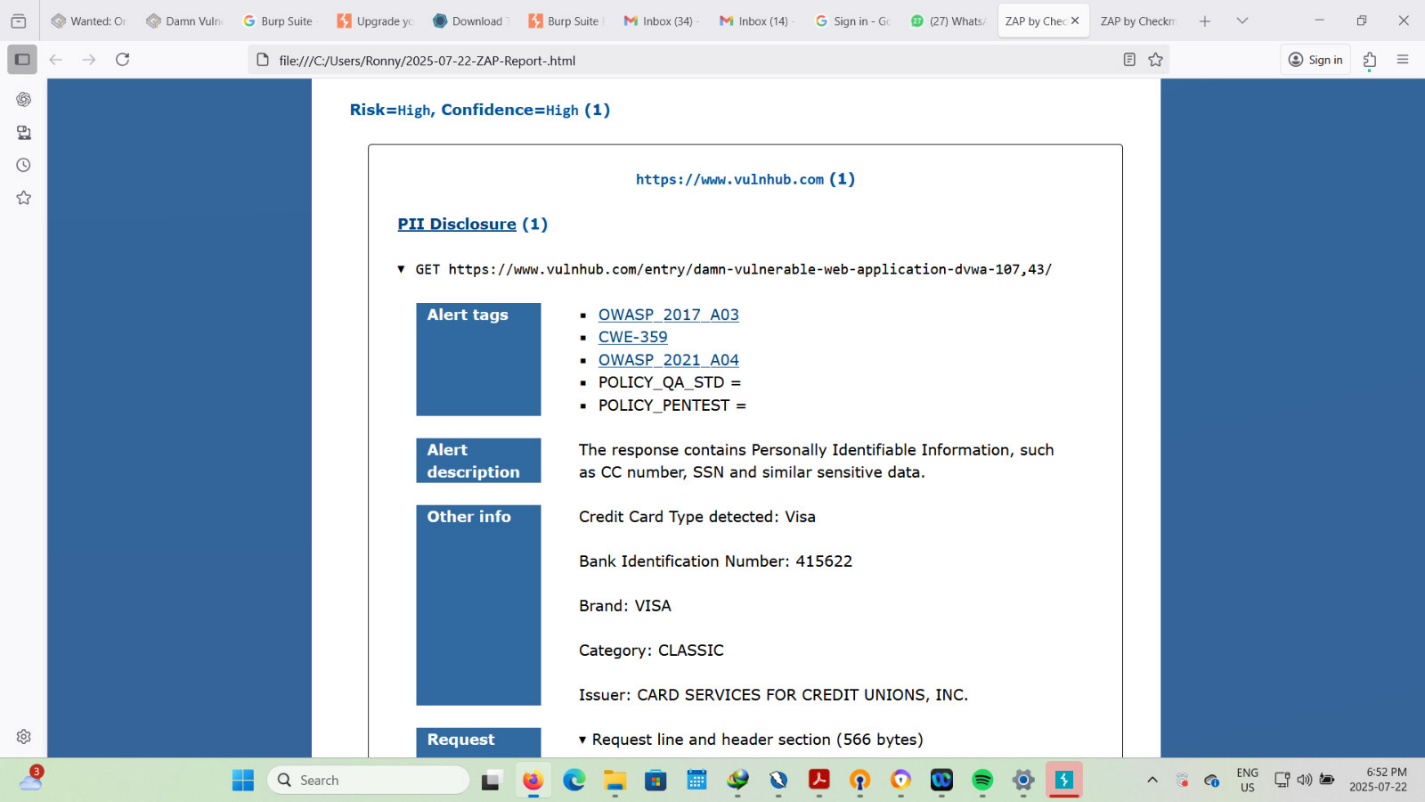


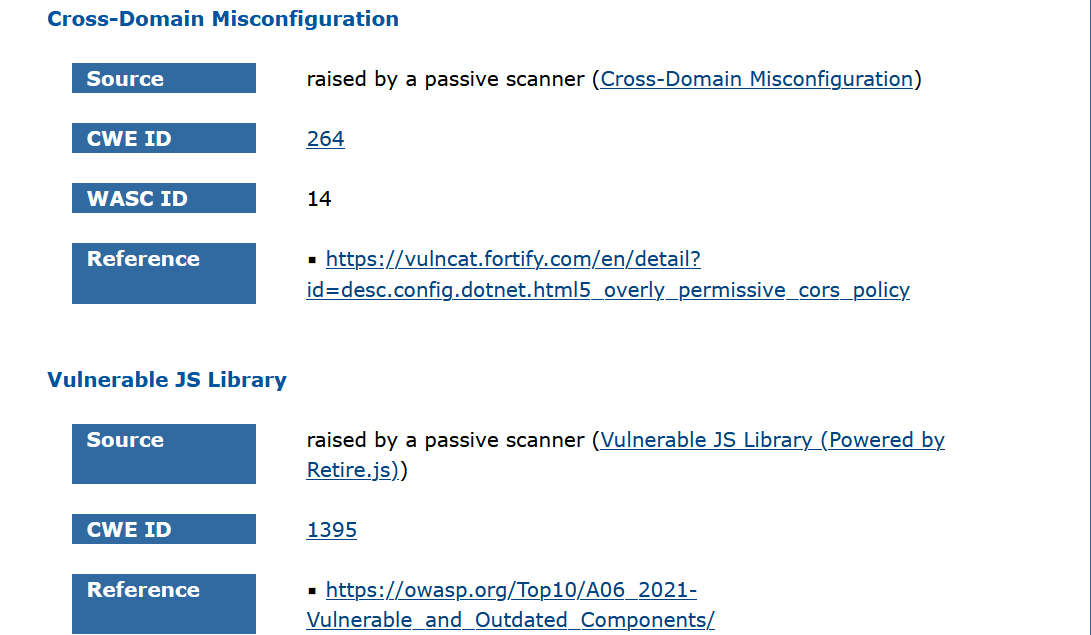












A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

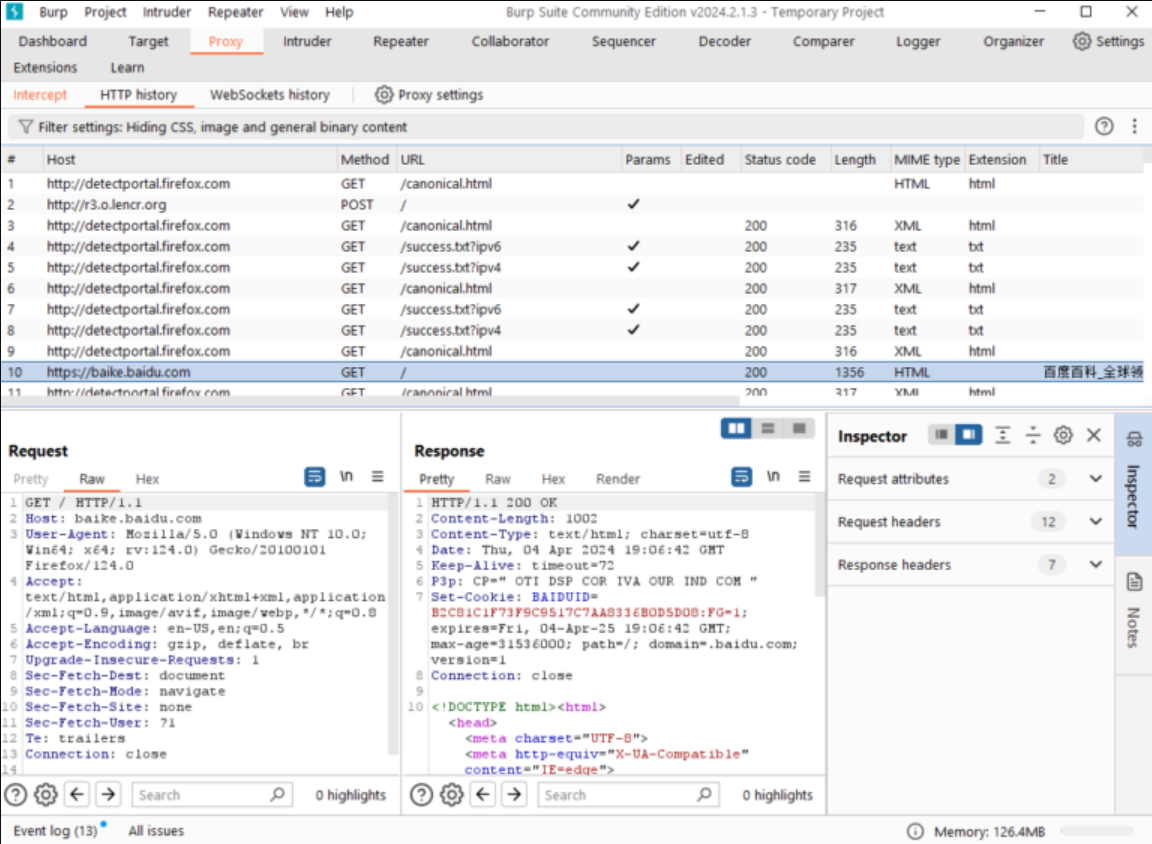
AI-generated content may be incorrect.

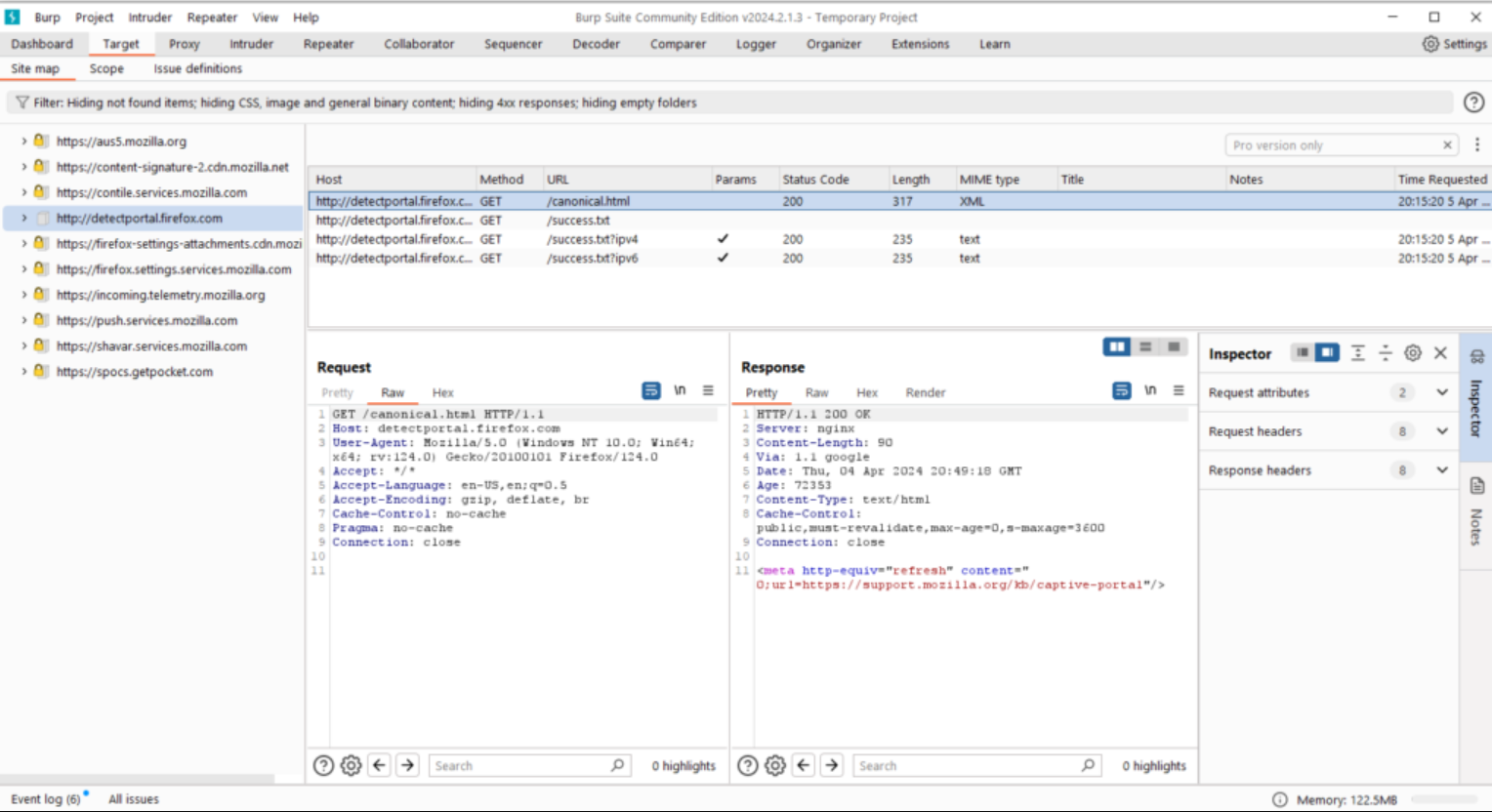
A screenshot of a computer

AI-generated content may be incorrect.



**Burp Suite Professional**



****

