Authentication Traffic Analysis – OWASP Juice Shop

By: ShayVon Ballard

This project documents the observation and analysis of authentication related network traffic within **OWASP Juice Shop**, a deliberately vulnerable web application designed for security training and testing. The objective was to gain hands on experience reviewing client server interactions during authentication attempts using standard web application analysis tools.

The scope of this analysis was limited to passive traffic inspection and request/response review during normal application use. No intrusive testing, credential attacks, or authorization bypass techniques were performed.

METHODOLOGY

The analysis began with observation of network activity using browser developer tools during normal interaction with the OWASP Juice Shop application. Network requests were reviewed to identify authentication related traffic, with attention given to request type, endpoint, and response status codes generated during login attempts.

After identifying relevant authentication requests, Burp Suite Community Edition was used as an intercepting proxy to capture and review HTTP request and response data. Traffic observed through the proxy was compared with browser-based observations to validate request behavior and confirm consistent server responses. All activity was limited to non-intrusive inspection and review of application traffic.

OBSERVATION AND ANALYSIS

During initial application load, multiple HTTP GET requests were observed for static resources and configuration data, including JavaScript files, fonts, and application configuration endpoints. These requests returned successful 200 responses and appeared consistent with normal application startup behavior. No authentication-related data was observed during this phase.

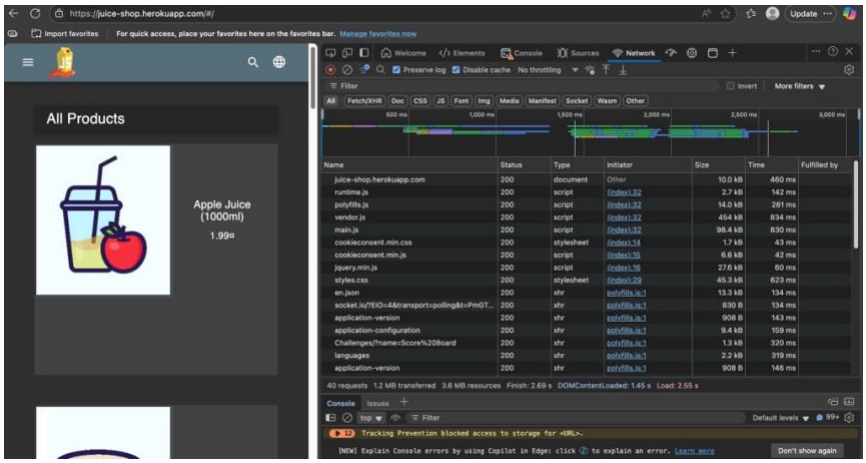

Figure 1: Initial HTTP traffic observed in Burp Suite Community Edition during normal interaction with the OWASP Juice Shop application, showing multiple GET and POST requests generated by client side activity.

AUTHENTICATION ATTEMPT OBSERVATION

During a login attempt, an authentication-related XHR request was observed targeting the application's login endpoint. The request was sent using the POST method and resulted in a 401 Unauthorized response. This behavior indicates that the application properly rejected invalid credentials during authentication processing.

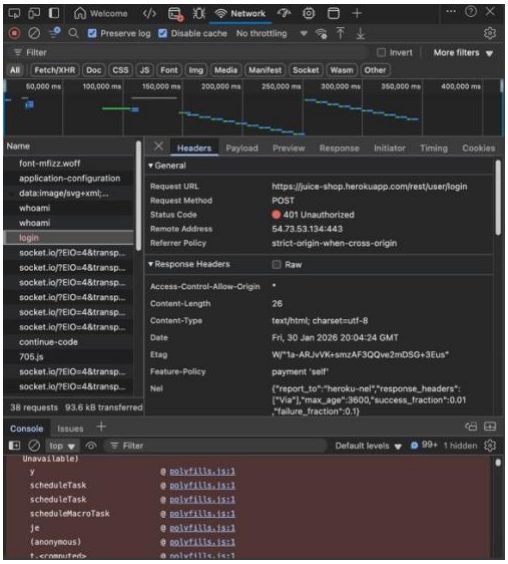

Figure 2: Authentication-related network requests identified within Burp Suite HTTP history, highlighting the login POST request selected for further inspection.

REQUEST AND RESPONSE HEADER REVIEW

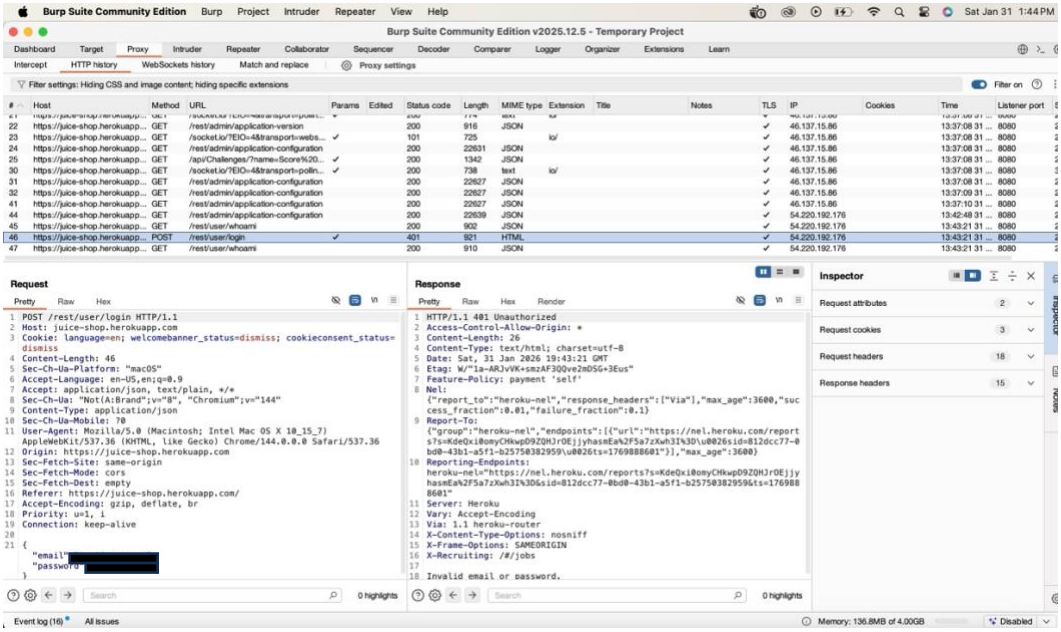

Figure 3: Authentication POST request showing request and response headers and payload structure. Credential values redacted.

The authentication request was observed returning a 401 Unauthorized response when invalid credentials were submitted. Review of response headers did not indicate exposure of sensitive information. Standard security headers were present, and the server response behavior aligned with expected authentication failure handling.

KEY OBSERVATION

Review of authentication-related network traffic showed that the application correctly rejected invalid login attempts by returning a 401 Unauthorized response. No authentication tokens, session identifiers, or sensitive internal error messages were observed in server responses during failed authentication attempts.

Response headers included standard security related configurations and did not expose unnecessary implementation details. The observed behavior aligns with expected authentication failure handling and indicates appropriate server side validation of user credentials. No evidence of improper authentication handling or information leakage was identified during inspection of network traffic.