Security Vulnerability Report: Open HTTP Redirect in DVWA

Vulnerability Name: Open HTTP Redirect

Application: Damn Vulnerable Web Application (DVWA)
Module: open_redirect
Tested URL: http://localhost/dvwa/vulnerabilities/open_redirect/?url=https://evil.com

Overview: An open redirect vulnerability exists in the DVWA application that allows an attacker to redirect users to arbitrary external URLs by manipulating the url query parameter. This can be exploited for phishing, credential theft, or redirecting users to malicious domains.

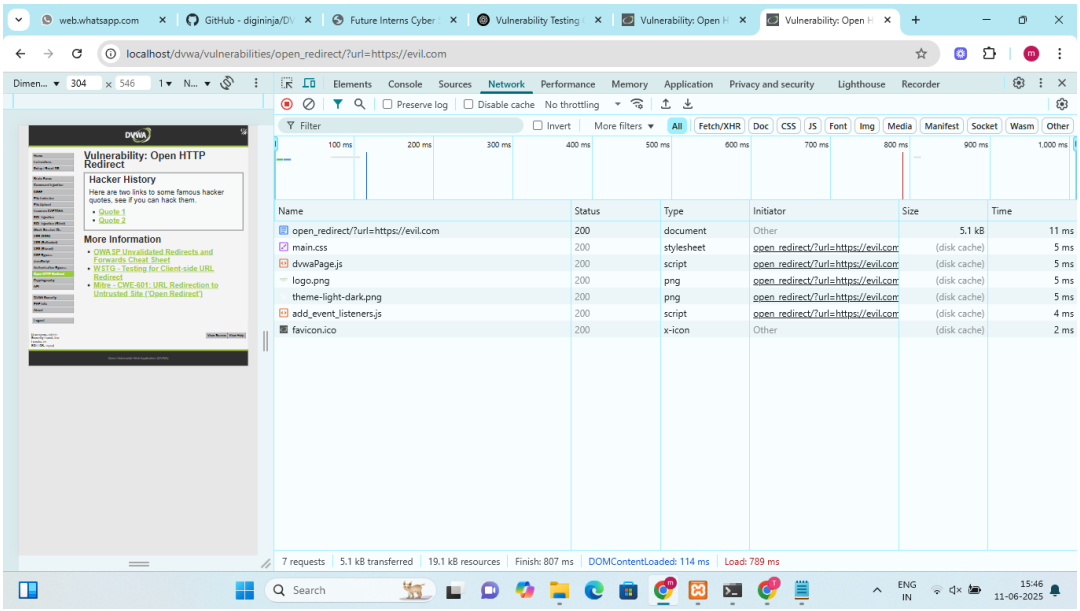
Steps to Reproduce:

1. Open the DVWA application and navigate to the Open Redirect module.
2. Modify the URL in the browser to:

   http://localhost/dvwa/vulnerabilities/open_redirect/?url=https://evil.com
3. Press Enter. The browser redirects to https://evil.com.
4. Use browser DevTools (Network tab) to confirm that the redirection occurred and assets were loaded from the evil.com domain.

Evidence:

- Screenshot showing successful redirection to https://evil.com with a 200 status code for the document.
- All page resources including scripts and images load from the malicious domain.



Security Impact:

- **Phishing:** Attackers can trick users into visiting fake login pages hosted on external sites.
- **Loss of Trust:** Users may associate the redirection with the original trusted domain.
- **Malware Propagation:** Redirection can lead to drive-by downloads or malicious code.

Recommendations:

- **Input Validation:** Only allow redirection to predefined internal paths or use a whitelist for external URLs.
- **User Confirmation:** Display a confirmation screen before redirecting to external URLs.
- **Remove Unused Functionality:** If external redirects are not necessary, disable or remove the functionality.

References:

- OWASP Cheat Sheet: Unvalidated Redirects and Forwards
- OWASP Testing Guide: Client-side URL Redirect
- CWE-601: URL Redirection to Untrusted Site

Date of Test: 11 June 2025

Tester: [Redacted for Privacy]