


Risk Management Report – OWASP Juice Shop Vulnerability Scan

 **Date of Scan:** June 17, 2025

 **Target:** `demo.owasp-juice.shop` (81.169.145.156)

 **Tool & Command:** `nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop`

1. CVE-2011-3192 – Apache ByteRange DoS

This vulnerability exploits the way Apache handles HTTP ByteRange headers, which are used to request specific parts of a file. An attacker can send multiple overlapping or malformed range requests in a single packet, forcing the server to allocate excessive resources in response. This could cause the server to consume memory until it crashes or becomes unresponsive.

Risk Impact: High

Likelihood: Medium

Severity (CVSS): 7.8 (High)

Mitigation: It is strongly recommended to update Apache to the latest stable version, where this issue is patched. Additionally, implementing a Web Application Firewall (WAF) or a reverse proxy like Nginx can help filter out malformed requests before they reach Apache.

2. CVE-2007-6750 – Slowloris Denial of Service

The Slowloris attack targets threaded web servers (like Apache) by opening multiple connections and keeping them alive indefinitely by sending partial HTTP requests. This exhausts the server's pool of available threads, causing legitimate user requests to be delayed or denied entirely.

Risk Impact: Medium

Likelihood: High

Severity (CVSS): 5.0 (Medium)

Mitigation: Administrators should enable timeout settings for client requests and limit the number of concurrent connections allowed per IP. Deploying a reverse proxy (e.g., HAProxy, Nginx) or a specialized tool like `mod_reqtimeout` can also help defend against Slowloris-style attacks.

3. CVE-2005-3299 – phpMyAdmin Local File Inclusion (LFI)

This legacy vulnerability in phpMyAdmin allows an attacker to exploit the `subform` parameter in `grab_globals.lib.php` to perform Local File Inclusion. By crafting a malicious request, attackers may include arbitrary files from the server's file system, such as `/etc/passwd`, gaining access to sensitive system configuration or user information.

Risk Impact: High

Likelihood: Medium

Severity (CVSS): 6.4 (Medium)

Mitigation: Although Juice Shop simulates vulnerable conditions, in real-world environments, phpMyAdmin should always be kept up to date. File inclusion protections should be in place via input sanitization, and sensitive tools like phpMyAdmin should be firewalled and accessible only from trusted networks.

4. Script Execution Failures (e.g., http-vuln-cve2017-1001000)

During the scan, several Nmap NSE vulnerability scripts failed to execute, possibly due to configuration limitations, timeout issues, or network filtering. These failures limit the visibility of potentially present vulnerabilities and represent a form of operational risk — blind spots in the assessment.

Risk Impact: Low

Likelihood: Medium

Severity (CVSS): N/A

Mitigation: Re-run the scan using elevated permissions (e.g., `sudo`), extend timeout thresholds, or use an alternate vulnerability scanner such as OpenVAS or Nessus. Ensuring consistent and complete scans is essential for identifying all relevant risks.



Conclusion

The scan results from `demo.owasp-juice.shop`, a purposely insecure application, revealed realistic vulnerabilities that mirror those found in outdated or poorly configured production systems. The most pressing concerns are related to Denial of Service (DoS) and Local File Inclusion, both of which can cause significant service disruption or data exposure. While Juice Shop is used for training and simulation, these risks highlight the importance of regular patching, service hardening, and proactive network defense. It is recommended that these findings be used to strengthen the understanding of vulnerability management and inform future penetration tests or audits.

