

Vulnerability Scan Report: OWASP Juice Shop

1. Scan Details

- Date & Time of Scan: Wednesday, June 18, 2025, at 16:30:47
- Target Scanned: demo.owasp-juice.shop (81.169.145.156)

Nmap Command Used:


```
bash
CopyEdit
nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
```

-

2. Open Ports and Services

Port	State	Service	Version
21	open	ftp	ftpd.bin round-robin file server 3.4.0r16
25	filtered	smtp	Filtered (likely behind a firewall)
80	open	http-proxy	F5 BIG-IP load balancer http proxy

3. Vulnerabilities Found

CVE ID	Description	Status
CVE-2005-3299	phpMyAdmin 2.6.4 grab_globals.lib.php file inclusion vulnerability via subform parameter. Allows local file inclusion.	 Potential

-

Additional Notes:

- The scan attempted DOM-based XSS, stored XSS, and CSRF tests — no XSS or CSRF vulnerabilities were confirmed.
- The `http-majordomo2-dir-traversal` script failed to execute.
- The phpMyAdmin traversal was marked "VULNERABLE" but with **State: UNKNOWN**.

4. Critical Assets Identified

These were inferred from service behavior and HTML content:

- Login Page – Detected via standard application structure in HTML.
- Admin/Configuration Panel – Possible due to phpMyAdmin directory traversal attempts.
- Cookie Consent Scripts & Analytics – Use of tracking libraries like CookieConsent and jQuery.
- FTP Service on Port 21 – Could expose sensitive configuration or credential files if misconfigured.

5. Threat Hunting Commentary

The OWASP Juice Shop is an intentionally vulnerable web app, and this scan reflects several signs of that. Notably, the exposed FTP service on port 21 is uncommon for production systems and should be monitored closely. The presence of a vulnerable phpMyAdmin component, especially with a possible Local File Inclusion (LFI) via **CVE-2005-3299**, poses a significant threat if the vulnerability is exploitable. The filtered SMTP port may suggest firewall activity or segmentation, but further investigation is needed. While no XSS or CSRF vulnerabilities were confirmed, the application architecture suggests high potential for user data manipulation and privilege escalation in a real-world scenario.

