Vulnerability Assessment Report: https://demo.owasp-juice.shop

SECURITY SCORE: 25/100

OVERALL RISK LEVEL: CRITICAL

1. Network Scan Results (Nmap)

Port	State	Service	Version	Evidence
21	OPEN	ftp	3.4.0r16	None
25	FILTERED	smtp		None
80	OPEN	http-proxy		**http-title:** Application Error...
135	FILTERED	msrpc		None
139	FILTERED	netbios-ssn		None
179	FILTERED	bgp		None
443	OPEN	http	2.4.66	**http-title:** Application Error... **ssl-cert:** Subject: commonName=*.owasp-juice.shop Subject Alt...
445	FILTERED	microsoft-ds		None
8080	OPEN	http-proxy		**http-title:** Application Error...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 81.169.145.156
+ Target Hostname: demo.owasp-juice.shop
+ Target Port: 443
+ Start Time: 2026-02-25 06:24:58 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.66 (Unix)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 26 items checked: 8 error(s) and 1 item(s) reported on remote host
+ End Time: 2026-02-25 06:25:39 (GMT0) (41 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled & Fuzzed Endpoints

- https://demo.owasp-juice.shop

4. Vulnerability Intelligence (CVE Mapping)

Intelligence-Mapped CVEs for Apache httpd 2.4.66
- CVE-2025-55753 [CVSS: 7.5] (Confidence: LOW): An integer overflow in the case of failed ACME certificate renewal leads, after a number of failures...
- CVE-2025-59775 [CVSS: 7.5] (Confidence: LOW): Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server on Windows with AllowEnc...
- [POTENTIAL] CVE-2025-65082 [CVSS: 6.5] (Confidence: LOW): Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache HTTP Server th...
- [POTENTIAL] CVE-2025-66200 [CVSS: 5.4] (Confidence: LOW): mod_userdir+suexec bypass via AllowOverride FileInfo vulnerability in Apache HTTP Server. Users with...
- [POTENTIAL] CVE-2025-58098 [CVSS: 8.3] (Confidence: LOW): Apache HTTP Server 2.4.65 and earlier with Server Side Includes (SSI) enabled and mod_cgid (but not ...

5. Attack Possibilities & Mitigation

[NOTE] Attack: Missing Content-Security-Policy (CSP)
Mitigation: Implement a strict CSP header.

[LOW] Attack: Missing Anti-Clickjacking Protection
Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.