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

SECURITY SCORE: 45/100

OVERALL RISK LEVEL: HIGH

1. Network Scan Results (Nmap)

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

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: 2026-02-24 16:40:30 (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: 2026-02-24 16:41:09 (GMT0) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

- https://demo.owasp-juice.shop/assets/public/favicon_js.ico
- https://demo.owasp-juice.shop
- https://demo.owasp-juice.shop/styles.css

4. Vulnerability Intelligence (CVE Mapping)

Version-Associated CVEs (Unverified Exploit) in Apache httpd 2.4.66
- CVE-2025-55753: an integer overflow in the case of failed acme certificate renewal leads, after a number of failures (~30 days...
- CVE-2025-59775: server-side request forgery (ssrf) vulnerability in apache http server on windows with allowencodedslashe...
- [POTENTIAL] CVE-2025-65082: improper neutralization of escape, meta, or control sequences vulnerability in apache http server through envi...
- [POTENTIAL] CVE-2025-66200: mod_userdir+suexec bypass via allowoverride fileinfo vulnerability in apache http server. users with access to...
- [POTENTIAL] CVE-2025-58098: apache http server 2.4.65 and earlier with server side includes (ssi) enabled and mod_cgid (but not mod_cgi) p...

5. Attack Possibilities & Mitigation

[CRITICAL] Attack: Confirmed API Auth Bypass (SQLi to Token)
Evidence: Server parsed SQLi and generated a valid JSON session token at /rest/user/login
Mitigation: Implement strong input validation on JSON APIs and use parameterized queries.

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