Vulnerability Assessment Report: demo.owasp-juice.shop

SECURITY SCORE: 35/100

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: 80
+ Start Time: 2026-02-24 15:54:32 (GMT0)
---------------------------------------------------------------------------
+ Server: Heroku
+ Retrieved via header: 1.1 heroku-router
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'report-to' found, with contents: {"group":"heroku-nel","endpoints":[
{"url":"https://nel.heroku.com/reports?s=tJDwA1eqpL4eHbxNlHXWlpUl%2B%2FwxS40v5cubJAN5Xg
s%3D\u0026sid=812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1771948478"}],"max_age":3600
}
+ Uncommon header 'nel' found, with contents: {"report_to":"heroku-nel","response_heade
rs":["Via"],"max_age":3600,"success_fraction":0.01,"failure_fraction":0.1}
+ Uncommon header 'reporting-endpoints' found, with contents: heroku-nel="https://nel.h
eroku.com/reports?s=tJDwA1eqpL4eHbxNlHXWlpUl%2B%2FwxS40v5cubJAN5Xgs%3D&sid;=812dcc77-0b
d0-43b1-a5f1-b25750382959&ts;=1771948478"
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ lines
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains
or wildcards.
+ Server leaks inodes via ETags, header found with file /index.do, fields: 0xW/1252f
0x19c905fb95c
+ Uncommon header 'x-recruiting' found, with contents: /#/jobs
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'feature-policy' found, with contents: payment 'self'
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Server banner has changed from 'Heroku' to 'Apache/2.4.66 (Unix)' which may suggest a
WAF, load balancer or proxy is in place
+ Uncommon header 'access-control-allow-methods' found, with contents:
GET,HEAD,PUT,PATCH,POST,DELETE
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php,
forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote
administrative access, harvesting user info and more. Default login to admin interface
is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security
problems as described by www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL
trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be
viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-3092: /.svn/entries: Subversion Entries file may contain directory listing
information.
+ OSVDB-3092: /.svn/wc.db: Subversion SQLite DB file may contain directory listing
information.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ OSVDB-3092: /.hg/dirstate: Mercurial DirState file may contain directory listing
information.
+ 26 items checked: 1 error(s) and 27 item(s) reported on remote host
+ End Time: 2026-02-24 15:59:01 (GMT0) (269 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

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

4. Vulnerability Intelligence (CVE Mapping)

Validated Vulnerabilities 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: Broken Authentication (API Auth Bypass) at /rest/user/login
Evidence: Bypassed login via POST /rest/user/login
Mitigation: Implement strong input validation on JSON APIs.

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