Vulnerability Assessment Report: zero.webappsecurity.com

SECURITY SCORE: 81/100

OVERALL RISK LEVEL: MEDIUM

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http	1.1	**http-title:** Zero - Personal Banking - Loans - Credit Cards...
443	https		**ssl-cert:** Subject: commonName=zero.webappsecurity.com/organi...
8080	http	1.1	**http-title:** Zero - Personal Banking - Loans - Credit Cards...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 54.82.22.214
+ Target Hostname: zero.webappsecurity.com
+ Target Port: 80
+ Start Time: 2026-02-24 15:04:40 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ Server banner has changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32)
mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40' which may suggest a WAF, load balancer or
proxy is in place
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server.
+ 26 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2026-02-24 15:05:13 (GMT0) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

3. Crawled & Fuzzed Endpoints

- http://zero.webappsecurity.com/resources/css/font-awesome.css
- http://zero.webappsecurity.com/resources/css/bootstrap.min.css

- http://zero.webappsecurity.com/index.html
- http://zero.webappsecurity.com/resources/css/main.css
- http://zero.webappsecurity.com/
- http://zero.webappsecurity.com

4. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Filtered 5 legacy vulnerabilities.

5. Attack Possibilities & Mitigation

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

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