Vulnerability Assessment Report: bakewithzoha.com

SECURITY SCORE: 85/100

OVERALL RISK LEVEL: LOW

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http		**http-title:** Did not follow redirect to https://bakewithzoha.co...
443	http		**http-title:** Bake With Zoha | Simple And Indulgent Bakes... **ssl-cert:** Subject: commonName=bakewithzoha.com Subject Alter...
8080	http		**http-title:** Site doesn't have a title (text/plain; charset=UTF...
8443	http		**ssl-cert:** Subject: commonName=bakewithzoha.com Subject Alter... **http-title:** Site doesn't have a title (text/plain; charset=utf...

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 172.64.150.187
+ Target Hostname: bakewithzoha.com
+ Target Port: 80
+ Start Time: 2026-02-23 16:39:31 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'cf-ray' found, with contents: 9d2828f1eaf77eb6-MAA
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Cookie __cf_bm created without the httponly flag
+ IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ Cookie _cfuvid created without the httponly flag
+ 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.
+ Uncommon header 'proxy-status' found, with contents:
Cloudflare-Proxy;error=http_request_error
+ 26 items checked: 0 error(s) and 12 item(s) reported on remote host
+ End Time: 2026-02-23 16:39:34 (GMT0) (3 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

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

3. Crawled Website Endpoints

- No endpoints found

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Session Hijacking / Cookie Theft
Mitigation: Set HttpOnly and Secure flags on all sensitive cookies.

[LOW] Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.

[LOW] Attack: Cross-Site Request Forgery (CSRF) / Data Theft
Mitigation: Replace full wildcard '*' entries in crossdomain.xml with specific, trusted domain origins.