

# Vulnerability Assessment Report: bakewithzoha.com

## SECURITY SCORE: 96/100

OVERALL RISK LEVEL: LOW

*Note: Target is protected by a WAF/CDN. Score adjusted for mitigated risks.*

### 1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http		<b>http-title:</b> Did not follow redirect to https://bakewithzoha.co...
443	http		<b>http-title:</b> Bake With Zoha   Simple And Indulgent Bakes... <b>ssl-cert:</b> Subject: commonName=bakewithzoha.com Subject Alter...
8080	http		<b>http-title:</b> Site doesn't have a title (text/plain; charset=UTF...)
8443	http		<b>ssl-cert:</b> Subject: commonName=bakewithzoha.com Subject Alter... <b>http-title:</b> 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 17:32:01 (GMT0)
-----
+ Server: cloudflare
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'cf-ray' found, with contents: 9d2875df18b7f3eb-MAA
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Cookie __cf_bm created without the httponly flag
+ IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ Cookie __cfuvvid 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 17:32:04 (GMT0) (3 seconds)
-----
+ 1 host(s) tested
```

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

### 3. Crawled Website Endpoints

- https://bakewithzoha.com/
- https://bakewithzoha.com/less-sweet-german-chocolate-cake/
- https://bakewithzoha.com/recipes/
- https://bakewithzoha.com/light-and-chocolatey-black-forest-cake/
- https://bakewithzoha.com/#feastmobilemenu
- https://bakewithzoha.com/tandoori-chicken-star-bread/
- https://bakewithzoha.com/sticky-toffee-bread-pudding/
- https://bakewithzoha.com/contact/
- https://bakewithzoha.com
- https://bakewithzoha.com/lifechanging-brooklyn-blackout-cake/
- https://bakewithzoha.com/gingerbread-dulce-de-leche-layered-cake/
- https://bakewithzoha.com/shop/
- https://bakewithzoha.com/about/
- [FORM] https://bakewithzoha.com/
- https://bakewithzoha.com/the-texas-sheet-cake-that-converted-me/
- https://bakewithzoha.com/perfect-cream-puffs/

### 4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

### 5. Attack Possibilities & Mitigation

**[LOW] Attack:** Cross-Site Request Forgery (CSRF) / Data Theft

**Mitigation:** Replace full wildcard '\*' entries in crossdomain.xml with specific, trusted domain origins.

**[LOW] Attack:** Clickjacking / Cross-Site Scripting (XSS)

**Mitigation:** Implement X-Frame-Options and Content-Security-Policy headers.