Vulnerability Assessment Report: bakewithzoha.com

SECURITY SCORE: 60/100

OVERALL RISK LEVEL: HIGH

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	http		open
8080	http		open
8443	http		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 104.18.37.69
+ Target Hostname: bakewithzoha.com
+ Target Port: 80
+ Start Time: 2026-02-13 17:17:27 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare
+ Uncommon header 'alt-svc' found, with contents: h3=":443"; ma=86400
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'referrer-policy' found, with contents: same-origin
+ Uncommon header 'cf-ray' found, with contents: 9cd5fab78a7985ae-BOM
+ 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: 2026-02-13 17:17:32 (GMT0) (5 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- https://bakewithzoha.com/perfect-cream-puffs/
- https://bakewithzoha.com/
- https://bakewithzoha.com/the-texas-sheet-cake-that-converted-me/
- https://bakewithzoha.com/gingerbread-dulce-de-leche-layered-cake/

- [FORM] https://bakewithzoha.com/
- https://bakewithzoha.com/#feastmobilemenu
- https://bakewithzoha.com/less-sweet-german-chocolate-cake/
- https://bakewithzoha.com/light-and-chocolatey-black-forest-cake/
- https://bakewithzoha.com
- https://bakewithzoha.com/recipes/
- https://bakewithzoha.com/contact/
- https://bakewithzoha.com/tandoori-chicken-star-bread/
- https://bakewithzoha.com/lifechanging-brooklyn-blackout-cake/
- https://bakewithzoha.com/about/
- https://bakewithzoha.com/sticky-toffee-bread-pudding/
- https://bakewithzoha.com/shop/

4. Vulnerabilities Detected

- Insecure Cross-Domain Policy
- Insecure Cookies
- Missing Security Headers

5. Vulnerability Intelligence (CVE Mapping)

Modern Vulnerabilities in Cloudflare http proxy
- [CRITICAL 9.1] CVE-2025-6087: A Server-Side Request Forgery (SSRF) vulnerability was identified in the @opennextjs/cloudflare package. The vulnerability stems from an unimplemented...

6. Attack Possibilities & Mitigation

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

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

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