CyberShield Professional Security Analysis

Overall Risk Assessment:	Medium
Assessment Date:	2025-11-09 10:36:01

Technical Assessment Details

Scan ID:	5
URL Analyzed:	https://www.canva.com
HTTP Response Code:	403
Scan Completion Time:	2025-11-09 10:36:01

HTTP Response Headers Analysis

The following HTTP headers were detected in the server response. Security headers are highlighted.

Header Name	Value
Date	Sun, 09 Nov 2025 10:36:01 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	close
accept-ch	Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile
cf-mitigated	challenge
critical-ch	Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile
cross-origin-embedder-policy	require-corp
cross-origin-opener-policy	same-origin
cross-origin-resource-policy	same-origin
origin-agent-cluster	?1
permissions-policy	accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-wri...

referrer-policy	same-origin
server-timing	chlray;desc="99bcaaab1ebb9d99", cfOrigin;dur=0,cfEdge;dur=53
x-content-type-options	nosniff
x-frame-options	SAMEORIGIN
Cache-Control	private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-ch...
Expires	Thu, 01 Jan 1970 00:00:01 GMT
Set-Cookie	__cf_bm=JRpEr7vxmdz3Xy8gM11CaljKud1Vh1BzvILLpAk.eX0-1762684561-1.0.1.1
Report-To	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=fD5qve0J2j...
NEL	{"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
Vary	Accept-Encoding
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload
Server	cloudflare
CF-RAY	99bcaaab1ebb9d99-MRS
Content-Encoding	br

Security Headers Analysis

• ■ **Missing Content-Security-Policy:** Implement CSP to prevent XSS attacks.

• ✓ X-Frame-Options: SAMEORIGIN

• ✓ X-Content-Type-Options: nosniff

• ✓ Strict-Transport-Security header is present.

• ■■ **Missing X-XSS-Protection:** Consider adding this header for additional XSS protection.

• ■■ **Server Information Disclosure:** Server header reveals 'cloudflare'. Consider hiding server information.

Expert Remediation Recommendations

• Client errors detected. Ensure proper error handling and user input validation.

• Implement a Content Security Policy (CSP) to mitigate XSS attacks. Start with a restrictive policy and adjust as needed.

• Regularly update all software components, frameworks, and dependencies to patch known vulnerabilities.

• Implement a Web Application Firewall (WAF) to provide an additional layer of protection.

• Conduct regular security audits and penetration testing to identify and remediate vulnerabilities.

• Ensure all sensitive data is encrypted in transit (HTTPS) and at rest.

• Implement proper access controls and authentication mechanisms.

• Set up security monitoring and logging to detect and respond to security incidents.

HTTP Status Code Analysis

Status Code 403: Forbidden. Access is denied. Review access control policies.