CyberShield Professional Security Analysis

Overall Risk Assessment:	Low
Assessment Date:	2025-11-11 18:10:09

Technical Assessment Details

Scan ID:	8
URL Analyzed:	https://pos.assetcoding.sa/
HTTP Response Code:	200
Scan Completion Time:	2025-11-11 18:10:09

HTTP Response Headers Analysis

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

Header Name	Value
Date	Tue, 11 Nov 2025 18:10:09 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
<b>X-Powered-By</b>	PHP/8.2.27
Cache-Control	no-cache, private
set-cookie	XSRF-TOKEN=eyJpdiI6IjVYZndlbjkrd2l6NkpGM1E3bGhES3c9PSIsInZhbHVlIjoidmp
Content-Encoding	br
platform	hostinger
panel	hpanel
<b>Content-Security-Policy</b>	upgrade-insecure-requests
<b>Server</b>	hcdn

alt-svc	h3=":443"; ma=86400
x-hcdn-request-id	9195c84197096657ecd3dd062f79186f-fra-edge2
x-hcdn-cache-status	DYNAMIC
x-hcdn-upstream-rt	0.175

Security Headers Analysis

- ✓ Content-Security-Policy header is present.
- ■ **Missing X-Frame-Options:** Add this header to prevent clickjacking attacks.
- ■ **Missing X-Content-Type-Options:** Add 'nosniff' to prevent MIME type sniffing.
- ■■ **Missing Strict-Transport-Security:** Recommended for HTTPS sites to enforce secure connections.
- ■■ **Missing X-XSS-Protection:** Consider adding this header for additional XSS protection.
- ■■ **Server Information Disclosure:** Server header reveals 'hcdn'. Consider hiding server information.
- ■■ **Technology Disclosure:** X-Powered-By header reveals technology stack. Remove this header.

Expert Remediation Recommendations

- Add Strict-Transport-Security header to enforce HTTPS connections and prevent protocol downgrade attacks.
- 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 200: Success. The request was successful. This is the expected response for normal operations.

CONFIDENTIAL - Generated by CyberShield Professional Security Platform

Report generated on 2025-11-11 21:10:49 UTC