



Threat Level 0

No vulnerabilities have been discovered by the scanner.

Scan Detail

Target	https://www.cardanocube.io/
Scan Type	DCOne Crypto Scan
Scan Duration	3 minutes
Requests	1737
Average Response Time	67ms
Maximum Response Time	1092ms

0

Critical

0

High

0






Medium

0

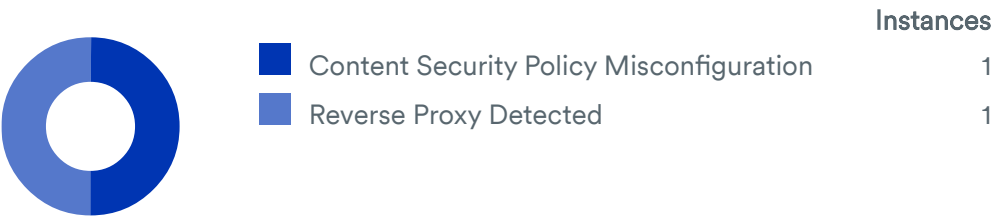
Low

2

Informational

Severity	Vulnerabilities	Instances
 Critical	0	0
 High	0	0
 Medium	0	0
 Low	0	0
 Informational	2	2
Total	2	2

Informational



Impacts

SEVERITY		IMPACT	
	Informational	1	Content Security Policy Misconfiguration
	Informational	1	Reverse Proxy Detected

Content Security Policy Misconfiguration

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

<https://www.cardanocube.io/>

Verified

- **Missing object-src in CSP Declaration**
 - **First observed on:** <https://www.cardanocube.io/>
 - **CSP Value:** frame-ancestors 'self'
 - **CSP Source:** header
 - **Summary:** Acunetix detected that object-src is missed in CSP declaration. It allows the injection of plugins which can execute JavaScript.
 - **Impact:** N/A
 - **Remediation:** Set object-src to 'none' in CSP declaration: Content-Security-Policy: object-src 'none';
 - **References:**
 - N/A

Request

```
GET / HTTP/1.1
Referer: https://www.cardanocube.io/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: www.cardanocube.io
Connection: Keep-alive
```

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy \(CSP\) to Secure Web Applications](https://www.invicti.com/blog/web-security/content-security-policy/)

<https://www.invicti.com/blog/web-security/content-security-policy/>

[The dangers of incorrect CSP implementations](https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)

<https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/>

[Leverage Browser Security Features to Secure Your Website](https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

<https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/>

Reverse Proxy Detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

<https://www.cardanocube.io/>

Detected reverse proxy: Fastly

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: www.cardanocube.io
Connection: Keep-alive
```

Recommendation

None

Coverage

 <https://www.cardanocube.io>