

Security Assessment Report - dable.org

Server Information

ip_address: 162.19.253.138
server: nginx/1.22.1
powered_by: Unknown
content_type: text/html

headers:

Server: nginx/1.22.1
Date: Wed, 25 Dec 2024 03:14:12 GMT
Content-Type: text/html
Last-Modified: Fri, 29 Nov 2024 13:27:10 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Etag: W/"6749c12e-5a65"
Content-Encoding: gzip
response_time: 0

DNS Records

Type: A

- 162.19.253.138

Type: MX

- 10 mx1.improvmx.com.
- 20 mx2.improvmx.com.

Type: NS

- fortaleza.ns.porkbun.com.
- salvador.ns.porkbun.com.
- maceio.ns.porkbun.com.
- curitiba.ns.porkbun.com.

Type: TXT

- "v=spf1 include:spf.improvmx.com ~all"
- "hosting-site=dable"

Type: SOA

- curitiba.ns.porkbun.com. dns.cloudflare.com. 2358378837 10000 2400 604800 1800

WHOIS Information

registrar: Porkbun LLC
creation_date: 2024-02-11 08:43:59
expiration_date: 2025-02-11 08:43:59
last_updated: 2024-08-09 12:18:41

name_servers:

- maceio.ns.porkbun.com
- curitiba.ns.porkbun.com
- salvador.ns.porkbun.com
- fortaleza.ns.porkbun.com

status:

- clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>
- clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
emails: abuse@porkbun.com
org: Private by Design, LLC

Open Ports

Port	State	Service	Version
22	open	ssh	9.2p1 Debian 2+deb12u3
53	open	domain	
80	open	http	1.22.1
443	open	http	1.22.1

Vulnerabilities

Type: Security Headers

Severity: Medium
Description: Missing HSTS header
Remediation: Add Strict-Transport-Security header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing X-Frame-Options header
Remediation: Add X-Frame-Options header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing X-Content-Type-Options header
Remediation: Add X-Content-Type-Options header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing Content Security Policy
Remediation: Add Content-Security-Policy header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing XSS Protection header
Remediation: Add X-XSS-Protection header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing Referrer Policy
Remediation: Add Referrer-Policy header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing Permissions Policy
Remediation: Add Permissions-Policy header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing COEP header
Remediation: Add Cross-Origin-Embedder-Policy header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing COOP header
Remediation: Add Cross-Origin-Opener-Policy header with appropriate values

Type: Security Headers

Severity: Medium
Description: Missing CORP header
Remediation: Add Cross-Origin-Resource-Policy header with appropriate values

Type: CSRF

Severity: Medium

Description: No CSRF token found in form: <https://dablie.org/>

Remediation: Implement CSRF tokens for all forms

Type: Sensitive File Exposure

Severity: High

Description: Sensitive file detected: `/.git/config`

Remediation: Remove or protect access to `/.git/config`

Type: Unsafe JavaScript

Severity: Medium

Description: Potentially dangerous inline JavaScript detected

Remediation: Avoid using `eval()` or `document.write()`. Use safer alternatives.