Security Scan Report

secure-js.democuda.org

2025-12-25 18:11:50

Executive Summary | **Scan Details**

257	1	0	0
High	Medium	Low	Info

Executive Summary

Scan Findings

Find The Admin Panel

View Details →

- Found 255 admin panels.

Subfinder

View Details →

- No subdomains detected.

Katana

View Details →

- Detected 8 URLs.

Related Sites Discovery

View Details →

- Discovered 10 related subdomain(s), 5 responding to HTTP requests (50.0% response rate)
- 4 successful HTTP response(s) (200 OK) across all hosts
- Most common technologies: Cloudflare (1), Onsen UI (1), Osano:3.1.0 (1)

Test SSL

View Details →

- SSL/TLS configuration appears secure. No vulnerabilities or weak ciphers detected in TLS 1.2+.

Mozilla Observatory

View Details →

- -= Observatory grade and score summary =-
- Grade: D-, Score: 25, Tests Passed: 7, Tests Failed: 3

External Script Detection

View Details →

- Script detection could not complete: Session.request() got an unexpected keyword argument 'max_redirects'. Did you mean 'allow_redirects'?

Wafw00f

View Details →

- Detected WAF: Barracuda.

Identified Issues

- 258 potential issues were identified.
- Categories involved: Information Disclosure, Content Security, Access Control.
- Severity breakdown: High=257, Medium=1, Low=0.

View All Issues by Severity →

Issues Found

High Severity Issues

Exposed Admin Panel `Access Control`

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel `Access Control`

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Exposed Admin Panel Access Control

Reported by: Find The Admin Panel View tool details →

Remediation: Restrict access to admin panels using IP whitelisting, VPN requirements, or move to non-standard URLs. Implement multi-factor authentication and monitor for brute-force attempts. A WAF can help by rate-limiting login attempts, blocking common attack patterns, providing geographical access restrictions to administrative interfaces, and implementing virtual patching against known admin panel vulnerabilities.

Content Security Policy with unsafe-inline Content Security

Reported by: Mozilla Observatory View tool details →

Remediation: Refactor inline scripts and styles to use external resources with integrity checks. A WAF can help mitigate XSS risks by inspecting and filtering malicious payloads in HTTP requests.

SRI Not Implemented and External Scripts Not Loaded Securely

Content Security

Reported by: Mozilla Observatory View tool details →

Remediation: Load all external scripts over HTTPS and add SRI attributes to ensure resource integrity. A WAF can monitor external script requests and block suspicious or tampered resources.

↑ Home

Medium Severity Issues

Unsafe Referrer Policy **Information Disclosure**

Reported by: Mozilla Observatory View tool details →

Remediation: Set a strict Referrer-Policy header such as 'no-referrer' or 'strict-origin-when-cross-origin'. A WAF can inject or override the Referrer-Policy header to prevent information leakage.

↑ Home

Detailed Results by Tool

This section provides detailed results from each security tool that was executed during the scan. Click on any tool name below to navigate directly to its results.

Find The Admin Panel

Scans target for exposed admin login pages

Subfinder

Subdomain finder.

WhatWeb

Identifies technologies used by a website.

Katana

Site crawler and URL finder.

Related Sites Discovery

Discovers related subdomains and probes for live web services

Test SSL

Tests SSL and TLS posture

Mozilla Observatory

Runs Mozilla Observatory to analyze web application security.

External Script Detection

Detects and analyzes external JavaScript files loaded by the target.

Wafw00f

Detects and identifies Web Application Firewalls (WAFs) on the target.

Find The Admin Panel

Purpose: Scans target for exposed admin login pages

Website: https://github.com/DV64/Find-The-Admin-Panel

Timestamp: 2025-12-25T18:11:49.030

Summary:

Found 255 exposed admin panels.

Exposed Admin Panels (showing 50 of 255)

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/academy/admin/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/adm/admloginuser.asp`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/account/admin/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/access-admin/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/acct_login/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/admcontrol/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/adm1n/login.php`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/admin#/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/admin-05/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/accounting-admin/`

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/account/login

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/activecampaign/admin/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin&/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-04/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/acces-administrateur/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/access/admin

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin*/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/access-panel/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-03/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/adm/admloginuser.php

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/acquisition/admin/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/access-dashboard/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/aadmin/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/access-login/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/adm/login/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-08/

Validation request - Confidence: 86.0%

http://secure-js.democuda.org/acp/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/account/login/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/_login/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-07/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/access-control/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/adm1nistrator/login.php

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/accounting/admin/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/academic-admin/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-01/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin$/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/account/admin

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/_control/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin!strator/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin+/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/adm/login.do

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-02/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/_administrator_/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/admin-06/

Validation request - Confidence: 86.0%
http://secure-js.democuda.org/_panel/

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/acces-admin/`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/adm/login.php`

Validation request - Confidence: 86.0%
`http://secure-js.democuda.org/admin-abac/`

Note: 205 additional panel(s) not shown in PDF. View the full interactive HTML report for complete details.

Details:

Exposed Admin Panels:

Panel #1:

URL: http://secure-js.democuda.org/academy/admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #2:

URL: http://secure-js.democuda.org/adm/admloginuser.asp

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #3:

URL: http://secure-js.democuda.org/account/admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #4:

URL: http://secure-js.democuda.org/access-admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #5:

URL: http://secure-js.democuda.org/acct_login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #6:

URL: http://secure-js.democuda.org/admcontrol/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #7:

URL: http://secure-js.democuda.org/adm1n/login.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #8:

URL: http://secure-js.democuda.org/admin#/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #9:

URL: http://secure-js.democuda.org/admin-05/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #10:

URL: http://secure-js.democuda.org/accounting-admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #11:

URL: http://secure-js.democuda.org/account/login

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #12:

URL: http://secure-js.democuda.org/activecampaign/admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #13:

URL: http://secure-js.democuda.org/admin&/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #14:

URL: http://secure-js.democuda.org/admin-04/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #15:

URL: http://secure-js.democuda.org/acces-administrateur/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #16:

URL: http://secure-js.democuda.org/access/admin

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #17:

URL: http://secure-js.democuda.org/admin-/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #18:

URL: http://secure-js.democuda.org/admin*/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #19:

URL: http://secure-js.democuda.org/access-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #20:

URL: http://secure-js.democuda.org/admin-03/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #21:

URL: http://secure-js.democuda.org/admin

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #22:

URL: http://secure-js.democuda.org/adm/admloginuser.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #23:

URL: http://secure-js.democuda.org/acquisition/admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #24:

URL: http://secure-js.democuda.org/access-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #25:

URL: http://secure-js.democuda.org/aadmin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #26:

URL: http://secure-js.democuda.org/access-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #27:

URL: http://secure-js.democuda.org/adm/login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #28:

URL: http://secure-js.democuda.org/admin-08/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #29:

URL: http://secure-js.democuda.org/acp/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #30:

URL: http://secure-js.democuda.org/account/login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #31:

URL: http://secure-js.democuda.org/_login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #32:

URL: http://secure-js.democuda.org/admin-07/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #33:

URL: http://secure-js.democuda.org/access-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #34:

URL: http://secure-js.democuda.org/adm1nistrator/login.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #35:

URL: http://secure-js.democuda.org/accounting/admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #36:

URL: http://secure-js.democuda.org/academic-admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #37:

URL: http://secure-js.democuda.org/admin-01/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #38:

URL: http://secure-js.democuda.org/admin$/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #39:

URL: http://secure-js.democuda.org/account/admin

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #40:

URL: http://secure-js.democuda.org/_control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #41:

URL: http://secure-js.democuda.org/admin!strator/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #42:

URL: http://secure-js.democuda.org/admin+/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #43:

URL: http://secure-js.democuda.org/adm/login.do

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #44:

URL: http://secure-js.democuda.org/admin-02/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #45:

URL: http://secure-js.democuda.org/_administrator_/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #46:

URL: http://secure-js.democuda.org/admin-06/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #47:

URL: http://secure-js.democuda.org/_panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #48:

URL: http://secure-js.democuda.org/acces-admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #49:

URL: http://secure-js.democuda.org/adm/login.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #50:

URL: http://secure-js.democuda.org/admin-abac/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #51:

URL: http://secure-js.democuda.org/admin-51/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #52:

URL: http://secure-js.democuda.org/admin-11/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #53:

URL: http://secure-js.democuda.org/admin-3arabi-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #54:

URL: http://secure-js.democuda.org/admin-2022/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #55:

URL: http://secure-js.democuda.org/admin-aapanel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #56:

URL: http://secure-js.democuda.org/admin-3rbi/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #57:

URL: http://secure-js.democuda.org/admin-ae/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #58:

URL: http://secure-js.democuda.org/admin-2027/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #59:

URL: http://secure-js.democuda.org/admin-2026/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #60:

URL: http://secure-js.democuda.org/admin-active-directory/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #61:

URL: http://secure-js.democuda.org/admin-access-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #62:

URL: http://secure-js.democuda.org/admin-3arabi-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #63:

URL: http://secure-js.democuda.org/admin-2fa/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #64:

URL: http://secure-js.democuda.org/admin-access-management/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #65:

URL: http://secure-js.democuda.org/admin-accounting/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #66:

URL: http://secure-js.democuda.org/admin-2028/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #67:

URL: http://secure-js.democuda.org/admin-2023/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #68:

URL: http://secure-js.democuda.org/admin-access-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #69:

URL: http://secure-js.democuda.org/admin-15/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #70:

URL: http://secure-js.democuda.org/admin-13/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #71:

URL: http://secure-js.democuda.org/admin-2021/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #72:

URL: http://secure-js.democuda.org/admin-2030/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #73:

URL: http://secure-js.democuda.org/admin-7afz/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #74:

URL: http://secure-js.democuda.org/admin-accept/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #75:

URL: http://secure-js.democuda.org/admin-academic/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #76:

URL: http://secure-js.democuda.org/admin-3rb/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #77:

URL: http://secure-js.democuda.org/admin-10/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #78:

URL: http://secure-js.democuda.org/admin-admin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #79:

URL: http://secure-js.democuda.org/admin-3d/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #80:

URL: http://secure-js.democuda.org/admin-accesspoint/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #81:

URL: http://secure-js.democuda.org/admin-3arabi-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #82:

URL: http://secure-js.democuda.org/admin-7isab/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #83:

URL: http://secure-js.democuda.org/admin-af-ZA/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #84:

URL: http://secure-js.democuda.org/admin-2029/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #85:

URL: http://secure-js.democuda.org/admin-addon-manager/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #86:

URL: http://secure-js.democuda.org/admin-access-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #87:

URL: http://secure-js.democuda.org/admin-2024/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #88:

URL: http://secure-js.democuda.org/admin-access/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #89:

URL: http://secure-js.democuda.org/admin-2025/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #90:

URL: http://secure-js.democuda.org/admin-administrator/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #91:

URL: http://secure-js.democuda.org/admin-3arabi-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #92:

URL: http://secure-js.democuda.org/admin-3arabi/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #93:

URL: http://secure-js.democuda.org/admin-2aman/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #94:

URL: http://secure-js.democuda.org/admin-5g-management/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #95:

URL: http://secure-js.democuda.org/admin-account/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #96:

URL: http://secure-js.democuda.org/admin-09/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #97:

URL: http://secure-js.democuda.org/admin-access-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #98:

URL: http://secure-js.democuda.org/admin-12/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #99:

URL: http://secure-js.democuda.org/admin-14/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #100:

URL: http://secure-js.democuda.org/admin-area-51/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #101:

URL: http://secure-js.democuda.org/admin-ai-insights/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #102:

URL: http://secure-js.democuda.org/admin-ai/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #103:

URL: http://secure-js.democuda.org/admin-amsterdam/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #104:

URL: http://secure-js.democuda.org/admin-api-documentation/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #105:

URL: http://secure-js.democuda.org/admin-agree/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #106:

URL: http://secure-js.democuda.org/admin-arb-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #107:

URL: http://secure-js.democuda.org/admin-akamai/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #108:

URL: http://secure-js.democuda.org/admin-ai-training/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #109:

URL: http://secure-js.democuda.org/admin-alpha/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #110:

URL: http://secure-js.democuda.org/admin-arb-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #111:

URL: http://secure-js.democuda.org/admin-aman/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #112:

URL: http://secure-js.democuda.org/admin-ai-platform/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #113:

URL: http://secure-js.democuda.org/admin-arabic-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #114:

URL: http://secure-js.democuda.org/admin-aiops/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #115:

URL: http://secure-js.democuda.org/admin-algeria/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #116:

URL: http://secure-js.democuda.org/admin-arb/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #117:

URL: http://secure-js.democuda.org/admin-archive/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #118:

URL: http://secure-js.democuda.org/admin-arb-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #119:

URL: http://secure-js.democuda.org/admin-api-monetization/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #120:

URL: http://secure-js.democuda.org/admin-api-keys/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #121:

URL: http://secure-js.democuda.org/admin-arabic-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #122:

URL: http://secure-js.democuda.org/admin-arb-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #123:

URL: http://secure-js.democuda.org/admin-arabi/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #124:

URL: http://secure-js.democuda.org/admin-api-gateway/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #125:

URL: http://secure-js.democuda.org/admin-ai-inference/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #126:

URL: http://secure-js.democuda.org/admin-ai-analytics/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #127:

URL: http://secure-js.democuda.org/admin-ajenti/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #128:

URL: http://secure-js.democuda.org/admin-ai-models/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #129:

URL: http://secure-js.democuda.org/admin-angular/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #130:

URL: http://secure-js.democuda.org/admin-approve/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #131:

URL: http://secure-js.democuda.org/admin-ansible/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #132:

URL: http://secure-js.democuda.org/admin-app/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #133:

URL: http://secure-js.democuda.org/admin-api/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #134:

URL: http://secure-js.democuda.org/admin-amsterdam.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #135:

URL: http://secure-js.democuda.org/admin-arabic-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #136:

URL: http://secure-js.democuda.org/admin-alert/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #137:

URL: http://secure-js.democuda.org/admin-araby/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #138:

URL: http://secure-js.democuda.org/admin-api-security/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #139:

URL: http://secure-js.democuda.org/admin-api-testing/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #140:

URL: http://secure-js.democuda.org/admin-analytics/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #141:

URL: http://secure-js.democuda.org/admin-app-store/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #142:

URL: http://secure-js.democuda.org/admin-approval/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #143:

URL: http://secure-js.democuda.org/admin-ajustes-es/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #144:

URL: http://secure-js.democuda.org/admin-api-management/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #145:

URL: http://secure-js.democuda.org/admin-apply/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #146:

URL: http://secure-js.democuda.org/admin-ar/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #147:

URL: http://secure-js.democuda.org/admin-am-ET/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #148:

URL: http://secure-js.democuda.org/admin-arabic-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #149:

URL: http://secure-js.democuda.org/admin-ar-AR/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #150:

URL: http://secure-js.democuda.org/admin-bahrain/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, PHP

Panel #151:

URL: http://secure-js.democuda.org/admin-australia.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #152:

URL: http://secure-js.democuda.org/admin-bahth/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #153:

URL: http://secure-js.democuda.org/admin-ba7th/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #154:

URL: http://secure-js.democuda.org/admin-au.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #155:

URL: http://secure-js.democuda.org/admin-at/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #156:

URL: http://secure-js.democuda.org/admin-audio/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #157:

URL: http://secure-js.democuda.org/admin-auth/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #158:

URL: http://secure-js.democuda.org/admin-auth0/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #159:

URL: http://secure-js.democuda.org/admin-begin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #160:

URL: http://secure-js.democuda.org/admin-au/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #161:

URL: http://secure-js.democuda.org/admin-benelux/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #162:

URL: http://secure-js.democuda.org/admin-beta/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #163:

URL: http://secure-js.democuda.org/admin-be/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #164:

URL: http://secure-js.democuda.org/admin-automation/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #165:

URL: http://secure-js.democuda.org/admin-authorization/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #166:

URL: http://secure-js.democuda.org/admin-berlin.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #167:

URL: http://secure-js.democuda.org/admin-barrier/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #168:

URL: http://secure-js.democuda.org/admin-beta/v4/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #169:

URL: http://secure-js.democuda.org/admin-bg-BG/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #170:

URL: http://secure-js.democuda.org/admin-autonomous-systems/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #171:

URL: http://secure-js.democuda.org/admin-backup/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #172:

URL: http://secure-js.democuda.org/admin-azure/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #173:

URL: http://secure-js.democuda.org/admin-bh/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #174:

URL: http://secure-js.democuda.org/admin-beta/v2/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #175:

URL: http://secure-js.democuda.org/admin-bereich/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #176:

URL: http://secure-js.democuda.org/admin-backend/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #177:

URL: http://secure-js.democuda.org/admin-auditing/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #178:

URL: http://secure-js.democuda.org/admin-basic/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #179:

URL: http://secure-js.democuda.org/admin-automate/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #180:

URL: http://secure-js.democuda.org/admin-beta/v1/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #181:

URL: http://secure-js.democuda.org/admin-authenticate/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #182:

URL: http://secure-js.democuda.org/admin-automation-anywhere/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #183:

URL: http://secure-js.democuda.org/admin-area/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #184:

URL: http://secure-js.democuda.org/admin-barcelona/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #185:

URL: http://secure-js.democuda.org/admin-audit/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #186:

URL: http://secure-js.democuda.org/admin-barcelona.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #187:

URL: http://secure-js.democuda.org/admin-banking/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #188:

URL: http://secure-js.democuda.org/admin-belgie/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #189:

URL: http://secure-js.democuda.org/admin-australia/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #190:

URL: http://secure-js.democuda.org/admin-bereich/login

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #191:

URL: http://secure-js.democuda.org/admin-argentina/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #192:

URL: http://secure-js.democuda.org/admin-berlin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #193:

URL: http://secure-js.democuda.org/admin-azure-ad/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #194:

URL: http://secure-js.democuda.org/admin-authentication/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #195:

URL: http://secure-js.democuda.org/admin-bert/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #196:

URL: http://secure-js.democuda.org/admin-aws/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #197:

URL: http://secure-js.democuda.org/admin-beveiligd/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #198:

URL: http://secure-js.democuda.org/admin-beheer/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #199:

URL: http://secure-js.democuda.org/admin-beta/v3/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #200:

URL: http://secure-js.democuda.org/admin-bitcoin/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #201:

URL: http://secure-js.democuda.org/admin-chef/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #202:

URL: http://secure-js.democuda.org/admin-boss/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #203:

URL: http://secure-js.democuda.org/admin-breda/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #204:

URL: http://secure-js.democuda.org/admin-brain/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #205:

URL: http://secure-js.democuda.org/admin-business/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #206:

URL: http://secure-js.democuda.org/admin-bluetooth-devices/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #207:

URL: http://secure-js.democuda.org/admin-chief/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #208:

URL: http://secure-js.democuda.org/admin-captain/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #209:

URL: http://secure-js.democuda.org/admin-cicd/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #210:

URL: http://secure-js.democuda.org/admin-check

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #211:

URL: http://secure-js.democuda.org/admin-centraal/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #212:

URL: http://secure-js.democuda.org/admin-blueprism/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #213:

URL: http://secure-js.democuda.org/admin-blockchain-explorer/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #214:

URL: http://secure-js.democuda.org/admin-certificates/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #215:

URL: http://secure-js.democuda.org/admin-biometric/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #216:

URL: http://secure-js.democuda.org/admin-business-process/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #217:

URL: http://secure-js.democuda.org/admin-circleci/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #218:

URL: http://secure-js.democuda.org/admin-broadcast/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #219:

URL: http://secure-js.democuda.org/admin-blog-control/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #220:

URL: http://secure-js.democuda.org/admin-canada.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #221:

URL: http://secure-js.democuda.org/admin-bordeaux/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #222:

URL: http://secure-js.democuda.org/admin-bi/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #223:

URL: http://secure-js.democuda.org/admin-big-data/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #224:

URL: http://secure-js.democuda.org/admin-bordeaux.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #225:

URL: http://secure-js.democuda.org/admin-blackboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #226:

URL: http://secure-js.democuda.org/admin-check/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #227:

URL: http://secure-js.democuda.org/admin-blue-team/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #228:

URL: http://secure-js.democuda.org/admin-carbon/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #229:

URL: http://secure-js.democuda.org/admin-ca/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #230:

URL: http://secure-js.democuda.org/admin-blog-panel/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #231:

URL: http://secure-js.democuda.org/admin-change/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #232:

URL: http://secure-js.democuda.org/admin-canvas/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #233:

URL: http://secure-js.democuda.org/admin-bronze/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #234:

URL: http://secure-js.democuda.org/admin-ca-ES/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #235:

URL: http://secure-js.democuda.org/admin-blog-dashboard/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #236:

URL: http://secure-js.democuda.org/admin-chicago/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #237:

URL: http://secure-js.democuda.org/admin-chicago.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3, HTTP/2

Panel #238:

URL: http://secure-js.democuda.org/admin-canada/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #239:

URL: http://secure-js.democuda.org/admin-ceo/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #240:

URL: http://secure-js.democuda.org/admin-blog-management/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #241:

URL: http://secure-js.democuda.org/admin-bitbucket/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #242:

URL: http://secure-js.democuda.org/admin-bigquery/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #243:

URL: http://secure-js.democuda.org/admin-blog-login/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #244:

URL: http://secure-js.democuda.org/admin-bots/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #245:

URL: http://secure-js.democuda.org/admin-caas/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #246:

URL: http://secure-js.democuda.org/admin-chile/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #247:

URL: http://secure-js.democuda.org/admin-bn-BD/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #248:

URL: http://secure-js.democuda.org/admin-ca.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #249:

URL: http://secure-js.democuda.org/admin-blockchain/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #250:

URL: http://secure-js.democuda.org/adm!n!strator/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #251:

URL: http://secure-js.democuda.org/adm1nistrador/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #252:

URL: http://secure-js.democuda.org/adm.php

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #253:

URL: http://secure-js.democuda.org/sysadm/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #254:

URL: http://secure-js.democuda.org/adm.cfm

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Panel #255:

URL: http://secure-js.democuda.org/adm-zone/

Title: Validation request

Confidence: 86.0%

Status Code: 200

Login Form Detected: Yes

Technologies: HTTP/3

Results:

View panel details below

Report Notes:

```
ftap --url secure-js.democuda.org --detection-mode stealth -d /opt/kast-web/kast_results/secure-js.democuda.org-20251225-180823 -e json -f ftap.json --concurrency 10
```

Subfinder

Purpose: Subdomain finder.

Website: https://github.com/projectdiscovery/subfinder

Timestamp: 2025-12-25T18:08:51.211

Disposition: success

Summary:
No subdomains were found.

No subdomains found.

Details:
Detected 0 unique subdomain(s).

Results:

View subdomain details below

Report Notes:

```
subfinder -v -d secure-js.democuda.org -rl 150 -o /opt/kast-web/kast_results
/secure-js.democuda.org-20251225-180823/subfinder_tmp.json -cs -oJ
```

WhatWeb

Purpose: Identifies technologies used by a website.

Website: https://github.com/urbanadventurer/whatweb

Timestamp: 2025-12-25T18:08:37.872

Disposition: success

Summary:

{'http://secure-js.democuda.org - HTTP 302': 'Country [UNITED STATES]; IP [135.18.212.153]; RedirectLocation [https://secure-js.democuda.org/]'}

{'https://secure-js.democuda.org (#1) - HTTP 200': 'Country [UNITED STATES]; IP [135.18.212.153]; JQuery (v2.2.4); Script [module, text/javascript]; Strict-Transport-Security [max-age=31536000; includeSubDomains; preload]; Title [OWASP Juice Shop]; UncommonHeaders [access-control-allow-origin,feature-policy,x-recruiting,referrer-policy, content-security-policy,x-content-type-options]; X-Frame-Options [SAMEORIGIN, SAMEORIGIN]'}

{'https://secure-js.democuda.org (#2) - HTTP 200': 'Country [UNITED STATES]; IP [135.18.212.153]; JQuery (v2.2.4); Script [module, text/javascript]; Strict-Transport-Security [max-age=31536000; includeSubDomains; preload]; Title [OWASP Juice Shop]; UncommonHeaders [access-control-allow-origin,feature-policy,x-recruiting,referrer-policy, content-security-policy,x-content-type-options]; X-Frame-Options [SAMEORIGIN, SAMEORIGIN]'}

Results:


```
{
"name": "whatweb"
"timestamp": "2025-12-25T18:08:23.993"
"disposition": "success"
"results":
  [
    {
    "target": [... truncated ...]
    "http_status": [... truncated ...]
```

```
      "request_config": [... truncated ...]
      "plugins": [... truncated ...]
      }
      {
      "target": [... truncated ...]
      "http_status": [... truncated ...]
      "request_config": [... truncated ...]
      "plugins": [... truncated ...]
      }
      {
      "target": [... truncated ...]
      "http_status": [... truncated ...]
      "request_config": [... truncated ...]
      "plugins": [... truncated ...]
      }
    ]
  }
```


Report Notes:

`whatweb -a 3 --read-timeout 30 --max-redirects 2 --log-json /opt/kast-web/kast_results/secure-js.democuda.org-20251225-180823/whatweb.json secure-js.democuda.org`

Katana

Purpose: Site crawler and URL finder.

Website: https://github.com/projectdiscovery/katana

Timestamp: 2025-12-25T18:08:50.351

Summary:
Detected 8 unique URL(s).

Discovered URLs (showing 8 of 8)

```
[GET] https://secure-js.democuda.org
[a] [GET] https://secure-js.democuda.org/uNi_x4hSphMjoRlsKz-0Ui6hCyWvd3_g5DLNX591Ko0=.html
[link] [GET] https://secure-js.democuda.org/styles.css
[script] [GET] https://secure-js.democuda.org/bnith__Z796apkzn4Uh64oSly_Yh4MeStjO2JYigPs5r2B2hEUep-DiRRrJRGB56PJAdKh0
[script] [GET] https://secure-js.democuda.org/main.js
[script] [GET] https://secure-js.democuda.org/polyfills.js
[script] [GET] https://secure-js.democuda.org/runtime.js
[script] [GET] https://secure-js.democuda.org/vendor.js
```

Details:
Detected 8 unique URL(s).

Results:

View URL details below

Report Notes:

```
katana -v -silent -u secure-js.democuda.org -o /opt/kast-web/kast_results/secure-js.democuda.org-20251225-180823/katana.txt -ob
```

Related Sites Discovery

Purpose: Discovers related subdomains and probes for live web services

Website: https://github.com/mercutioviz/kast

Timestamp: 2025-12-25T18:10:08.356

Summary:
Discovered 10 subdomain(s), 5 responding to HTTP requests (50.0% response rate)

Total Subdomains: 10

Live Hosts: 5 (50.0% response rate)

Dead Hosts: 5

Live Hosts (Top 25)

Host	Ports	Technologies
insecure.democuda.org	80, 443	Port 80 (503): None Port 443 (503): None
insecure-js.democuda.org	80, 443	Port 443 (200): Cloudflare, Onsen UI, Osano:3.1.0, cdnjs, jQuery:2.2.4 Port 80 (200): Cloudflare, Onsen UI, Osano:3.1.0, cdnjs, jQuery:2.2.4
secure-js.democuda.org	80, 443	Port 443 (200): None Port 80 (200): None
dvwa-insecure.democuda.org	80, 443	Port 443 (503): None Port 80 (503): None
dvwa-secure.democuda.org	80, 443	Port 80 (503): None Port 443 (503): None

Dead Hosts (5)

```
crapi.democuda.org, dvwa.democuda.org, test01.democuda.org, lab.democuda.org,
secure.democuda.org
```

Details:

Target: secure-js.democuda.org

Apex Domain: democuda.org

Scanned Domain: democuda.org

Total Subdomains Discovered: 10

Live Hosts: 5

Dead Hosts: 5

Response Rate: 50.0%

Unique Technologies: 5

Results:

See live and dead host information below

Test SSL

Purpose: Tests SSL and TLS posture

Website: https://testssl.sh/

Timestamp: 2025-12-25T18:08:58.394

Summary:
No vulnerabilities or cipher issues detected.

Details:
No SSL/TLS vulnerabilities or cipher issues detected.

Results:

Scan completed successfully. No vulnerabilities or cipher issues detected.

Report Notes:

```
testssl -U -E --connect-timeout 10 --warnings=batch -oJ /opt/kast-web/kast_results/secure-js.democuda.org-20251225-180823/testssl.json secure-js.democuda.org
```

Mozilla Observatory

Purpose: Runs Mozilla Observatory to analyze web application security.

Website: https://developer.mozilla.org/en-US/blog/mdn-http-observatory-launch/

Timestamp: 2025-12-25T18:08:34.028

Disposition: success

Summary:

Grade: D-, Score: 25, Tests Passed: 7, Tests Failed: 3

Results:


```
{
"scan":
  {
  "algorithmVersion": 4
  "grade": "D-"
  "error": null
  "score": 25
  "statusCode": 200
  "testsFailed": 3
  "testsPassed": 7
  "testsQuantity": 10
  "responseHeaders":
    {
    "access-control-allow-origin": [... truncated ...]
    "x-frame-options": [... truncated ...]
    "feature-policy": [... truncated ...]
    "x-recruiting": [... truncated ...]
    "accept-ranges": [... truncated ...]
    "cache-control": [... truncated ...]
    "last-modified": [... truncated ...]
    "etag": [... truncated ...]
    "content-type": [... truncated ...]
    "vary": [... truncated ...]
    "date": [... truncated ...]
    "referrer-policy": [... truncated ...]
    "content-security-policy": [... truncated ...]
    "strict-transport-security": [... truncated ...]
    "x-content-type-options": [... truncated ...]
```

```
    "connection": [... truncated ...]
    }
  }
"tests":
  {
  "content-security-policy":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    "http": [... truncated ...]
    "meta": [... truncated ...]
    "policy": [... truncated ...]
    "numPolicies": [... truncated ...]
    }
  "cookies":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": null
    "sameSite": [... truncated ...]
    }
  "cross-origin-resource-sharing":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": null
    }
  "redirection":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "destination": [... truncated ...]
    "redirects": [... truncated ...]
    "route": [... truncated ...]
    "statusCode": [... truncated ...]
    }
  "referrer-policy":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
```

```
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    "http": [... truncated ...]
    "meta": [... truncated ...]
    }
  "strict-transport-security":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    "includeSubDomains": [... truncated ...]
    "maxAge": [... truncated ...]
    "preload": [... truncated ...]
    "preloaded": [... truncated ...]
    }
  "subresource-integrity":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    }
  "x-content-type-options":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    }
  "x-frame-options":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": [... truncated ...]
    }
  "cross-origin-resource-policy":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": null
    "http": [... truncated ...]
    "meta": [... truncated ...]
```

```
    }
  }
}
```


Report Notes:

`mdn-http-observatory-scan secure-js.democuda.org`

← Back to Tool Index | ↑ Home | ← Previous | Next →

External Script Detection

Purpose: Detects and analyzes external JavaScript files loaded by the target.

Website: https://developer.mozilla.org/en-US/docs/Web/HTML/Element/script

Timestamp: 2025-12-25T18:08:50.389

Disposition: fail

Summary:

Script detection failed: Session.request() got an unexpected keyword argument 'max_redirects'. Did you mean 'allow_redirects'?

Results:


```
"Session.request() got an unexpected keyword argument 'max_redirects'. Did you mean 'allow_redirects'?"
```


Report Notes:

Script detection failed to complete

Wafw00f

Purpose: Detects and identifies Web Application Firewalls (WAFs) on the target.

Website: https://github.com/EnableSecurity/wafw00f

Timestamp: 2025-12-25T18:08:28.577

Disposition: success

Summary:
Detected 1 WAF(s): Barracuda

Details:
WAF Detected: Barracuda

Manufacturer: Barracuda Networks

Test URL: /?lyvdwyde=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E&xwzdmyqz=UNION+SELECT+ALL+FROM+information_schema+AND+%22+or+SLEEP%285%29+or+%22&sdcekwil=..%2F..%2Fetc%2Fpasswd

Test URL: /?jxjyjvuz=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E

Trigger URL: https://secure-js.democuda.org/?lyvdwyde=%3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E&xwzdmyqz=UNION+SELECT+ALL+FROM+information_schema+AND+%22+or+SLEEP%285%29+or+%22&sdcekwil=..%2F..%2Fetc%2Fpasswd

Results:


```
[
  {
  "detected": true
  "firewall": "Barracuda"
  "manufacturer": "Barracuda Networks"
```

```
    "trigger_url":
    "https://secure-js.democuda.org/?lyvdwyde=
    %3Cscript%3Ealert%28%22XSS%22%29%3B%3C%2Fscript%3E&amp;xwzdmyqz=
    UNION+SELECT+ALL+FROM+information_schema+AND+%22+or+SLEEP%285%29+or+%22&amp;sdcekwil=.
    .%2F..%2Fetc%2Fpasswd"
    "url": "https://secure-js.democuda.org"
    }
  ]
```


Report Notes:

`wafw00f secure-js.democuda.org -a -vvv -T 30 -f json -o /opt/kast-web/kast_results/secure-js.democuda.org-20251225-180823/wafw00f.json`