Security Scan Report

insecure-js.democuda.org

2025-12-25 18:05:54

Executive Summary | **Scan Details**

4	1	0	0
High	Medium	Low	Info

Executive Summary

Scan Findings

Find The Admin Panel

View Details →

- No admin panels found.

Subfinder

View Details →

- No subdomains detected.

Katana

View Details →

- Detected 7 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 (2), Onsen UI (2), Osano:3.1.0 (2)

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: F, Score: 0, Tests Passed: 6, Tests Failed: 4

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 →

- No WAFs were detected.

Identified Issues

- 5 potential issues were identified.
- Categories involved: Transport Security, Clickjacking Protection, WAF Detection, Content Security.
- Severity breakdown: High=4, Medium=1, Low=0.

View All Issues by Severity →

Issues Found

High Severity Issues

Content Security Policy Not Implemented

Content Security

Reported by: Mozilla Observatory

View tool details →

Remediation: Implement a strong Content Security Policy header to restrict the sources of scripts, styles, and other resources. A WAF can inject a default Content Security Policy header to provide immediate protection against XSS attacks.

HSTS Not Implemented

Transport Security

Reported by: Mozilla Observatory

View tool details →

Remediation: Implement the HSTS header to enforce HTTPS connections and protect against protocol downgrade attacks. A WAF can inject the HSTS header to enforce HTTPS connections and protect against protocol downgrade attacks.

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.

No WAF Detected WAF Detection

Reported by: Wafw00f View tool details →

Remediation: Deploy a WAF in front of the application to provide an additional layer of security against common web attacks.

↑ Home

Medium Severity Issues

Invalid X-Frame-Options header Clickjacking Protection

Reported by: Mozilla Observatory View tool details →

Remediation: Correct the X-Frame-Options header to 'DENY' or 'SAMEORIGIN'. A WAF can enforce proper header policies and block framing attempts from unauthorized sources.

↑ 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: 2025-12-25T18:05:26.982

Summary:
No exposed admin panels were found.

No admin panels found.

Details:
No admin panels detected.

Results:

View panel details below

Report Notes:

```
ftap --url insecure-js.democuda.org --detection-mode stealth -d /opt/kast-web/kast_results/insecure-js.democuda.org-20251225-180418 -e json -f ftap.json --concurrency 10
```

Subfinder

Purpose: Subdomain finder.

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

Timestamp: 2025-12-25T18:04:44.542

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 insecure-js.democuda.org -rl 150 -o /opt/kast-web/kast_results/insecure-js.democuda.org-20251225-180418/subfinder_tmp.json -cs -oJ
```

WhatWeb

Purpose: Identifies technologies used by a website.

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

Timestamp: 2025-12-25T18:04:32.059

Disposition: success

Summary:

{'http://insecure-js.democuda.org - HTTP 302': 'Country [UNITED STATES]; IP [4.152.87.222]; RedirectLocation [https://insecure-js.democuda.org/]'}

{'https://insecure-js.democuda.org (#1) - HTTP 200': 'Country [UNITED STATES]; IP [4.152.87.222]; JQuery (v2.2.4); Script [module, text/javascript]; Title [OWASP Juice Shop]; UncommonHeaders [access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting]; X-Frame-Options [SAMEORIGIN, SAMEORIGIN]'}

{'https://insecure-js.democuda.org (#2) - HTTP 200': 'Country [UNITED STATES]; IP [4.152.87.222]; JQuery (v2.2.4); Script [module, text/javascript]; Title [OWASP Juice Shop]; UncommonHeaders [access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting]; X-Frame-Options [SAMEORIGIN, SAMEORIGIN]'}

Results:


```
{
"name": "whatweb"
"timestamp": "2025-12-25T18:04:18.800"
"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/insecure-js.democuda.org-20251225-180418/whatweb.json insecure-js.democuda.org`

Katana

Purpose: Site crawler and URL finder.

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

Timestamp: 2025-12-25T18:04:43.550

Summary:
Detected 7 unique URL(s).

Discovered URLs (showing 7 of 7)

```
[GET] https://insecure-js.democuda.org
[link] [GET] https://insecure-js.democuda.org/styles.css
[script] [GET] https://insecure-js.democuda.org/bnith__moG8utBJ8IJS_zNpMC5aufOzBlg5EYrLkoIC4b3D73ltcr4r7f3OBp4_9Cf4VlLe
[script] [GET] https://insecure-js.democuda.org/main.js
[script] [GET] https://insecure-js.democuda.org/polyfills.js
[script] [GET] https://insecure-js.democuda.org/runtime.js
[script] [GET] https://insecure-js.democuda.org/vendor.js
```

Details:
Detected 7 unique URL(s).

Results:

View URL details below

Report Notes:

```
katana -v -silent -u insecure-js.democuda.org -o /opt/kast-web/kast_results/
insecure-js.democuda.org-20251225-180418/katana.txt -ob
```

Related Sites Discovery

Purpose: Discovers related subdomains and probes for live web services

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

Timestamp: 2025-12-25T18:05:53.799

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

	Port 80 (200): Cloudflare, HSTS, Onsen UI, Osano:3.1.0, cdnjs, jQuery:2.2.4

Dead Hosts (5)

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

Details:

Target: insecure-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: 6

Results:

See live and dead host information below

Test SSL

Purpose: Tests SSL and TLS posture

Website: https://testssl.sh/

Timestamp: 2025-12-25T18:05:42.827

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/insecure-js.democuda.org-20251225-180418/testssl.json insecure-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: 2025-12-25T18:04:28.765

Disposition: success

Summary:

Grade: F, Score: 0, Tests Passed: 6, Tests Failed: 4

Results:


```
{
"scan":
  {
  "algorithmVersion": 4
  "grade": "F"
  "error": null
  "score": 0
  "statusCode": 200
  "testsFailed": 4
  "testsPassed": 6
  "testsQuantity": 10
  "responseHeaders":
    {
    "access-control-allow-origin": [... truncated ...]
    "x-content-type-options": [... 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 ...]
    "connection": [... truncated ...]
    }
  }
```

```
"tests":
  {
  "content-security-policy":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": null
    "http": [... truncated ...]
    "meta": [... truncated ...]
    "policy": null
    "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": [... truncated ...]
    }
  "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": null
    "http": [... truncated ...]
```

```
    "meta": [... truncated ...]
    }
  "strict-transport-security":
    {
    "expectation": [... truncated ...]
    "pass": [... truncated ...]
    "result": [... truncated ...]
    "scoreModifier": [... truncated ...]
    "data": null
    "includeSubDomains": [... truncated ...]
    "maxAge": null
    "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 insecure-js.democuda.org`

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: 2025-12-25T18:04:43.587

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: 2025-12-25T18:04:24.060

Disposition: success

Summary:
No WAF detected

Details:
No WAF detected.

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

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

Test URL: /?vcxtjljo=UNION+SELECT+ALL+FROM+information_schema+AND+%22+or+SLEEP%285%29+or+%22

Results:


```
[
  {
  "detected": false
  "firewall": "None"
  "manufacturer": "None"
  "trigger_url": null
  "url": "https://insecure-js.democuda.org"
  }
]
```


Report Notes:

```
wafw00f insecure-js.democuda.org -a -vvv -T 30 -f json -o /opt/kast-web/kast_results/insecure-js.democuda.org-20251225-180418/wafw00f.json
```