# Web Application Penetration Test Report (WAPT)

COMPLETED WITH FINDINGS

**Company:** Example Inc.

Audit-ready output focused on findings, evidence, and test coverage.

**Job ID:** 2ecbdff8
**Company:** Example Inc.
**Test type:** Black Box (Unauthenticated)
**Generated (UTC):** 2026-03-30 12:02

**Package:** ISO 27001/2022 Evidence Pack
**Recipient:** john@example.com
**Target:** https://example.com

## Executive Summary

Passive-first assessment aligned to OWASP testing categories (WSTG structure). OWASP Baseline provides passive DAST signals; controlled active probes include HTTP behavior, DNS posture, SQL injection heuristics, curated directory brute-force, and subdomain enumeration. Any stage execution error is reported as failed coverage (no fallback substitution).

| Total Findings | Checks Executed | Coverage Completed | Coverage Degraded/Failed |
|---|---|---|---|
| 11 | 34 | 12 | 0 |

Tests run: OWASP Quick Checks, Active HTTP Probes, Domain DNS Checks, HTTP Behavior Checks, Extended Exposure Checks, Session/Auth Checks, SQLi Probes, Directory Brute-Force, Subdomain Enumeration, TLS Posture Scan, OWASP Baseline

**DevOps metric interpretation**

| Metric | How DevOps should read it |
|---|---|
| Total Findings | Prioritized remediation queue. Focus first on higher severity and internet-facing controls. |
| Checks Executed | Coverage breadth. Higher count means wider control validation across transport, headers, behavior, and exposure. |
| Coverage Completed | Pipeline stages that executed successfully; treat degraded/failed stages as assessment blind spots. |
| Severity Distribution | Capacity planning signal. Use to split fixes into immediate, sprint, and hardening backlog work. |
| Check Status Breakdown | `fail/warn` indicate action required; `info/pass` are context and validation baselines. |

### SEVERITY DISTRIBUTION

| Severity | Count |
|---|---|
| HIGH | 1 |
| MEDIUM | 4 |
| LOW | 6 |

### CHECK STATUS BREAKDOWN

| Status | Count |
|---|---|
| FAIL | 1 |
| WARN | 10 |
| INFO | 8 |
| PASS | 15 |

## Coverage and Scope

| Metric | Value |
|---|---|
| Scope origin | https://example.com |
| URLs discovered | 1 |
| URLs tested active | 1 |
| Completed stages | Discovery, OWASP Quick Checks, Active HTTP Probes, Domain DNS Checks, HTTP Behavior Checks, Extended Exposure Checks, Session/Auth Checks, SQLi Probes, Directory Brute-Force, Subdomain Enumeration, TLS Posture Scan, OWASP Baseline |
| Degraded stages | None |
| Failed stages | None |

## Scope Constraints and Assumptions

| Constraint | Value |
|---|---|
| Assessment mode | Unauthenticated |
| Scope mode | Domain scope |
| Target origin | https://example.com |
| Discovery depth | URLs discovered=1 |
| Active probe breadth | URLs tested=1 |

No skipped/degraded/failed stage constraints were recorded for this run.

## Executed Stages vs Outcome

| Stage | Status | Checks |
|---|---|---|
| Discovery | COMPLETED | 1 |
| OWASP Quick Checks | COMPLETED | 1 |
| Active HTTP Probes | COMPLETED | 1 |
| Domain DNS Checks | COMPLETED | 6 |
| HTTP Behavior Checks | COMPLETED | 6 |
| Extended Exposure Checks | COMPLETED | 2 |
| Session/Auth Checks | COMPLETED | 3 |
| SQLi Probes | COMPLETED | 1 |
| Directory Brute-Force | COMPLETED | 1 |
| Subdomain Enumeration | COMPLETED | 1 |
| TLS Posture Scan | COMPLETED | 1 |
| OWASP Baseline | COMPLETED WITH FINDINGS | 8 |

## Findings

### Target reachable over HTTP(S)

HIGH

OWASP: OWASP WSTG-INFO | Source: Baseline | Confidence: medium | Owner: Platform/App

OWASP reference: https://owasp.org/www-project-web-security-testing-guide/stable/

**What this means**

Target reachable over HTTP(S) returned status High.

**Why this matters**

This issue is rated High and may increase security risk if left unresolved.

**What to change**

Review the affected control (`Target reachable over HTTP(S)`), apply least-privilege/default-secure configuration, and deploy via infrastructure-as-code.

**How to verify**

Re-run the same scan check and confirm this finding is no longer reported. Reference: HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate ve.

**Technical reference**

HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1016)')))

### CAA policy present

MEDIUM

OWASP: OWASP WSTG-INFO | Source: DNS Checks | Confidence: medium | Owner: Platform/SRE

OWASP reference: https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

**What this means**

Domain DNS posture indicates a configuration gap or weak control signal.

**Why this matters**

Misconfigured DNS can increase spoofing, issuance, and operational risk.

**What to change**

Harden DNS records (CAA, SPF, DMARC, DNSSEC where feasible) and remove unintended wildcard behavior.

**How to verify**

Query DNS records and confirm expected policy records and host resolution behavior.

**Technical reference**

No CAA record detected.

### HTTP to HTTPS redirect behavior

MEDIUM

OWASP: OWASP A05 Security Misconfiguration | Source: HTTP Behavior | Confidence: medium | Owner: Platform/App

OWASP reference: https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/06-Test_HTTP_Methods

**What this means**

HTTP to HTTPS redirect behavior returned status Medium.

**Why this matters**

This issue is rated Medium and may increase security risk if left unresolved.

**What to change**

Review the affected control (`HTTP to HTTPS redirect behavior`), apply least-privilege/default-secure configuration, and deploy via infrastructure-as-code.

**How to verify**

Re-run the same scan check and confirm this finding is no longer reported. Reference: status=200 location=none.

**Technical reference**

status=200 location=none

### OWASP - Content Security Policy (CSP) Header Not Set

MEDIUM

OWASP: OWASP Baseline | Source: DAST | Confidence: 3 | Owner: App + Edge

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

**What this means**

No Content Security Policy is enforced for script/resource loading.

**Why this matters**

XSS and third-party script abuse have a larger blast radius.

**What to change**

Define a restrictive `Content-Security-Policy` (`default-src 'self'`) and explicitly allow required sources.

**How to verify**

Run `curl -I <url>` and confirm `Content-Security-Policy` exists and matches approved domains.

**Description**

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection a

**Technical reference**

riskcode=2; confidence=3; cwe=693; wasc=15; instances=3

### OWASP - Missing Anti-clickjacking Header

MEDIUM

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Platform/App

OWASP reference: https://owasp.org/www-project-web-security-testing-guide/stable/

**What this means**

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

**Why this matters**

This issue is rated Medium and may increase security risk if left unresolved.

**What to change**

Review the affected control (`OWASP - Missing Anti-clickjacking Header`), apply least-privilege/default-secure configuration, and deploy via infrastructure-as-code.

**How to verify**

Re-run the same scan check and confirm this finding is no longer reported. Reference: riskcode=2; confidence=2; cwe=1021; wasc=15; instances=1.

**Description**

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

**Technical reference**

riskcode=2; confidence=2; cwe=1021; wasc=15; instances=1

### OWASP - Cross-Origin-Embedder-Policy Header Missing or Invalid

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

COEP header is missing or not strict.

**Why this matters**

Cross-origin resource isolation is weaker, increasing browser-level attack surface in modern contexts.

**What to change**

Set `Cross-Origin-Embedder-Policy: require-corp` where application compatibility allows.

**How to verify**

Run `curl -I <url>` and verify `Cross-Origin-Embedder-Policy: require-corp` on HTML responses.

**Description**

Cross-Origin-Embedder-Policy header is a response header that prevents a document from loading any cross-origin resources that don't explicitly grant the document permission (us

**Technical reference**

riskcode=1; confidence=2; cwe=693; wasc=14; instances=1

### OWASP - Cross-Origin-Opener-Policy Header Missing or Invalid

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

COOP header is missing or not strict.

**Why this matters**

Browser context isolation is reduced, increasing risks around cross-window interactions.

**What to change**

Set `Cross-Origin-Opener-Policy: same-origin` on application pages unless a specific exception is required.

**How to verify**

Run `curl -I <url>` and verify `Cross-Origin-Opener-Policy: same-origin`.

**Description**

Cross-Origin-Opener-Policy header is a response header that allows a site to control if others included documents share the same browsing context. Sharing the same browsing cont

**Technical reference**

riskcode=1; confidence=2; cwe=693; wasc=14; instances=1

### OWASP - Cross-Origin-Resource-Policy Header Missing or Invalid

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

CORP header is missing or too permissive.

**Why this matters**

Cross-origin resource sharing boundaries are less explicit, which can increase exposure.

**What to change**

Set `Cross-Origin-Resource-Policy` appropriately (often `same-origin` for sensitive resources).

**How to verify**

Run `curl -I <asset_url>` and confirm `Cross-Origin-Resource-Policy` is present with expected value.

**Description**

Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst differen

**Technical reference**

riskcode=1; confidence=2; cwe=693; wasc=14; instances=1

### OWASP - Permissions Policy Header Not Set

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

Browser feature permissions are not explicitly restricted.

**Why this matters**

Unneeded browser capabilities may be available to application contexts.

**What to change**

Define `Permissions-Policy` to deny unused features (camera, microphone, geolocation, etc.).

**How to verify**

Run `curl -I <url>` and confirm a restrictive `Permissions-Policy` header is present.

**Description**

Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures

**Technical reference**

riskcode=1; confidence=2; cwe=693; wasc=15; instances=3

### OWASP - Strict-Transport-Security Header Not Set

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 3 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

Strict HTTPS enforcement is not configured on one or more responses.

**Why this matters**

Browsers may allow insecure downgrade paths and weaken transport protection.

**What to change**

Set `Strict-Transport-Security` on HTTPS responses with a long max-age and include subdomains when ready.

**How to verify**

Run `curl -I <url>` and confirm `Strict-Transport-Security` is present on HTTPS responses.

**Description**

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it

**Technical reference**

riskcode=1; confidence=3; cwe=319; wasc=15; instances=3

### OWASP - X-Content-Type-Options Header Missing

LOW

OWASP: OWASP Baseline | Source: DAST | Confidence: 2 | Owner: Edge/Ingress

OWASP reference: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

**What this means**

MIME sniffing protection header is missing.

**Why this matters**

Browsers may interpret files as executable content when they should not.

**What to change**

Set `X-Content-Type-Options: nosniff` for all responses.

**How to verify**

Run `curl -I <url>` and verify `X-Content-Type-Options: nosniff`.

**Description**

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the respons

**Technical reference**

riskcode=1; confidence=2; cwe=693; wasc=15; instances=1

## OWASP CATEGORY COUNTS

| Category | Count |
|---|---|
| OWASP A05 Security Misconfiguration | 1 |
| OWASP Baseline | 8 |
| OWASP WSTG-INFO | 2 |

## OWASP BASELINE RISKCODE COUNTS

| Riskcode | Count |
|---|---|
| 2 | 2 |
| 1 | 6 |
| 0 | 3 |

## Top OWASP Baseline Alerts

| Title | Severity | Confidence |
|---|---|---|
| OWASP - Content Security Policy (CSP) Header Not Set | MEDIUM | 3 |
| OWASP - Missing Anti-clickjacking Header | MEDIUM | 2 |
| OWASP - Cross-Origin-Embedder-Policy Header Missing or Invalid | LOW | 2 |
| OWASP - Cross-Origin-Opener-Policy Header Missing or Invalid | LOW | 2 |
| OWASP - Cross-Origin-Resource-Policy Header Missing or Invalid | LOW | 2 |
| OWASP - Permissions Policy Header Not Set | LOW | 2 |
| OWASP - Strict-Transport-Security Header Not Set | LOW | 3 |
| OWASP - X-Content-Type-Options Header Missing | LOW | 2 |

## No Findings by Test Area

| Test Area | Checks With No Findings | Example Checks |
|---|---|---|
| Active Probes | 2 | Reflected input probe, Method exposure probe |
| Exposure Checks | 3 | Extended sensitive path exposure check, JavaScript endpoint hint extraction, Directory and file brute-force probe |
| Injection Checks | 1 | SQL injection error-based probe |
| Session/Auth Checks | 3 | Session cookie attribute posture, Session fixation indicator check, Logout invalidation signal |

## Detailed Tests

| Title | Source | Status | Rating | OWASP | Summary | Owner |
|---|---|---|---|---|---|---|
| Target reachable over HTTP(S) | Baseline | FAIL | HIGH | OWASP WSTG-INFO | HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate ve | Platform/App |
| Reflected input probe | Active Probes | INFO | LOW | OWASP A03 Injection | url=https://example.com error=HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: /?auditproof_probe=a3dbffe028fc9f29 (Caused by SSLError(SSLCertVerif | Platform/App |
| Method exposure probe | Active Probes | INFO | LOW | OWASP A05 Security Misconfiguration | url=https://example.com error=HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE | App/API + Edge |
| DNS record posture | DNS Checks | PASS | LOW | OWASP WSTG-INFO | A=2, AAAA=2, CNAME=0, MX=1, NS=2, TXT=2 | Platform/SRE |
| CAA policy present | DNS Checks | WARN | MEDIUM | OWASP WSTG-INFO | No CAA record detected. | Platform/SRE |
| DNSSEC signal check | DNS Checks | PASS | LOW | OWASP WSTG-INFO | DNSKEY records detected: 4 | Platform/SRE |
| SPF policy signal | DNS Checks | PASS | LOW | OWASP WSTG-INFO | SPF detected. | Platform/SRE |
| DMARC policy signal | DNS Checks | PASS | LOW | OWASP WSTG-INFO | DMARC detected. | Platform/SRE |
| Wildcard DNS behavior | DNS Checks | PASS | LOW | OWASP WSTG-INFO | whlmxvhfmwgxkm.example.com did not resolve | Platform/SRE |
| HTTP to HTTPS redirect behavior | HTTP Behavior | WARN | MEDIUM | OWASP A05 Security Misconfiguration | status=200 location=none | Platform/App |
| Canonical host consistency | HTTP Behavior | INFO | LOW | OWASP A05 Security Misconfiguration | HTTPSConnectionPool(host='www.example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificat | Platform/App |
| Host header reflection probe | HTTP Behavior | INFO | LOW | OWASP A01 Broken Access Control | HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate ve | App/API + Edge |
| Open redirect probe on common parameters | HTTP Behavior | PASS | LOW | OWASP A01 Broken Access Control | No obvious redirect to external control domain observed. | App/API + Edge |
| | | PASS | LOW | | | |

| Title | Source | Status | Rating | OWASP | Summary | Owner |
|---|---|---|---|---|---|---|
| HTTP verb matrix probe | HTTP Behavior | | | OWASP A05 Security Misconfiguration | No unexpected verb acceptance observed. | App/API + Edge |
| Error handling leakage probe | HTTP Behavior | INFO | LOW | OWASP A05 Security Misconfiguration | HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: /auditproof-does-not-exist-nke87ee3kw (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTI | Platform/App |
| Extended sensitive path exposure check | Exposure Checks | PASS | LOW | OWASP A05 Security Misconfiguration | No strong exposure signature from extended path list. | Platform + Edge |
| JavaScript endpoint hint extraction | Exposure Checks | PASS | LOW | OWASP WSTG-INFO | No endpoint hints found across 0 JS files. | App/API |
| Session cookie attribute posture | Session/ Auth Checks | INFO | LOW | OWASP A07 Identification and Authentication Failures | No Set-Cookie observed on landing flow. | App/API |
| Session fixation indicator check | Session/ Auth Checks | INFO | LOW | OWASP A07 Identification and Authentication Failures | Auth login URL not configured; fixation probe skipped. | App/API |
| Logout invalidation signal | Session/ Auth Checks | INFO | LOW | OWASP A07 Identification and Authentication Failures | No authenticated cookie artifact available; logout invalidation probe skipped. | App/API |
| SQL injection error-based probe | Injection Checks | PASS | LOW | OWASP A03 Injection | probes_run=5; no SQL error signatures observed. | App/API |
| Directory and file brute-force probe | Exposure Checks | PASS | LOW | OWASP A05 Security Misconfiguration | No high-signal path hits from curated wordlist. | Platform + App |
| Subdomain enumeration check | DNS Checks | PASS | LOW | OWASP WSTG-INFO | base_domain=example.com; no candidate subdomains resolved. | Platform/SRE |
| OWASP - Content Security Policy (CSP) Header Not Set | DAST | WARN | MEDIUM | OWASP Baseline | riskcode=2; confidence=3; cwe=693; wasc=15; instances=3;desc=Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, | App + Edge |
| OWASP - Missing Anti-clickjacking Header | DAST | WARN | MEDIUM | OWASP Baseline | riskcode=2; confidence=2; cwe=1021; wasc=15; instances=1;desc=The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'f | Platform/App |
| OWASP - Cross-Origin-Embedder-Policy Header Missing or Invalid | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=2; cwe=693; wasc=14; instances=1;desc=Cross-Origin-Embedder-Policy header is a response header that prevents a document from loading any cross-origin resourc | Edge/Ingress |
| OWASP - Cross-Origin-Opener- | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=2; cwe=693; wasc=14; instances=1;desc=Cross- | Edge/Ingress |

| Title | Source | Status | Rating | OWASP | Summary | Owner |
|---|---|---|---|---|---|---|
| Policy Header Missing or Invalid | | | | | Origin-Opener-Policy header is a response header that allows a site to control if others included documents share | |
| OWASP - Cross-Origin-Resource-Policy Header Missing or Invalid | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=2; cwe=693; wasc=14; instances=1;desc=Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resourc | Edge/Ingress |
| OWASP - Permissions Policy Header Not Set | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=2; cwe=693; wasc=15; instances=3;desc=Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of bro | Edge/Ingress |
| OWASP - Strict-Transport-Security Header Not Set | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=3; cwe=319; wasc=15; instances=3;desc=HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying u | Edge/Ingress |
| OWASP - X-Content-Type-Options Header Missing | DAST | WARN | LOW | OWASP Baseline | riskcode=1; confidence=2; cwe=693; wasc=15; instances=1;desc=The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet E | Edge/Ingress |
| OWASP - Re-examine Cache-control Directives | DAST | PASS | LOW | OWASP Baseline | riskcode=0; confidence=1; cwe=525; wasc=13; instances=1;desc=The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. Fo | App/API + Edge |
| OWASP - Retrieved from Cache | DAST | PASS | LOW | OWASP Baseline | riskcode=0; confidence=2; cwe=525; wasc=-1; instances=3;desc=The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may r | Platform/App |
| OWASP - Storable and Cacheable Content | DAST | PASS | LOW | OWASP Baseline | riskcode=0; confidence=2; cwe=524; wasc=13; instances=3;desc=The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the | App/API + Edge |