Security Scan Report

Target: https://example.com

Generated: 16/1/2026

Scan ID: u-0f115db062b7c0dd030b16878c99dea5c354b49dc37b38eb8846179c7783e9d7-de6b681a

Executive Summary

Overall Risk Level: HIGH

VirusTotal Analysis

- **Total Engines:** 97
- **Malicious:** 1
- **Suspicious:** 0
- **Harmless:** 70
- **Undetected:** 26

PageSpeed Insights

- **Performance:** 100/100
- **Accessibility:** 0/100
- **Best Practices:** 0/100
- **SEO:** 0/100

Mozilla Observatory

- **Security Grade:** F
- **Score:** 10/100
- **Tests Passed:** 5
- **Tests Failed:** 5

OWASP ZAP Vulnerability Scan

- **Total Alerts:** 7
- **High Risk:** 0
- **Medium Risk:** 2
- **Low Risk:** 3
- **Informational:** 2

Top Vulnerabilities:

1. [Medium] Missing Anti-clickjacking Header
2. [Informational] Re-examine Cache-control Directives
3. [Medium] Content Security Policy (CSP) Header Not Set
4. [Informational] Retrieved from Cache
5. [Low] Strict-Transport-Security Header Not Set

urlscan.io Analysis

- **Verdict:** Clean
- **Threat Score:** 0/100
- **Domain:** example.com
- **Server IP:** 104.18.26.120
- **Country:** N/A
- **Server:** cloudflare

WebCheck Analysis

- **TLS Grade:** F
- **WAF Detected:** Yes
- **HSTS Enabled:** No
- **Technologies:** Cloudflare

AI-Generated Security Analysis

Executive Summary

The website `https://example.com` demonstrates excellent performance, achieving a perfect 100/100 score on PageSpeed Insights. However, its security posture is critically weak, highlighted by a malicious detection on VirusTotal and a failing 'F' grade from Mozilla Observatory due to significant configuration vulnerabilities, making it unsafe for sensitive interactions without immediate remediation.

Security Analysis

Risk level: High Risk due to a confirmed malicious detection and severe security configuration flaws.

VirusTotal Security Report:

- One malicious detection out of 97 engines scanned. This is a critical finding that demands immediate investigation, despite urlscan.io reporting the site as clean.

Full VT Stats: {"malicious":1,"undetected":26,"harmless":70,"suspicious":0,"timeout":0,"confirmed_timeout":0,"failure":0,"type_unsupported":0}

Mozilla Observatory Security Configuration Report:

Security Grade: F

Security Score: 10/100

- Tests Passed: 5, Tests Failed: 5 out of 10 total tests.
- This indicates significant failures in implementing fundamental security configurations.

OWASP ZAP Vulnerability Scan Report:

Total Alerts: 7

High Risk Vulnerabilities: 0

Medium Risk Vulnerabilities: 2

- Missing Anti-clickjacking Header: Exposes users to UI redressing attacks.
- Content Security Policy (CSP) Header Not Set: Allows various injection attacks (XSS, data injection).

Low Risk Vulnerabilities: 3

Informational: 2

urlscan.io Website Analysis Report:

Malicious Verdict: No - Clean

Threat Score: 0/100

Server: cloudflare (indicating a WAF/CDN is in place)

TLS Issuer: Cloudflare TLS Issuing ECC CA 3

• It's important to note the contradiction between urlscan.io's 'Clean' verdict and VirusTotal's 'Malicious' detection; the latter should be prioritized for investigation.

WebCheck Comprehensive Scan Report:

Security Headers: Content-Type, Transfer-Encoding, Connection, Last-Modified, Allow, Age, CF-Cache-Status, Vary, Server, CF-Ray are present.

• Critical Missing Headers: Content-Security-Policy, X-Frame-Options (or equivalent CSP directive), Strict-Transport-Security (HSTS), X-Content-Type-Options, Referrer-Policy. These align with ZAP and Observatory findings.

TLS/SSL Configuration: N/A (specific grade not provided, but Cloudflare handles TLS issuance).

Firewall/WAF Detection: Detected: Cloudflare (positive, as it adds a layer of protection).

HSTS Status: Not enabled. This leaves the site vulnerable to SSL stripping attacks.

Key security findings and threats detected:

• A single but critical malicious detection by VirusTotal.
• Extremely poor security configuration reflected by an 'F' grade from Mozilla Observatory.
• Confirmed missing anti-clickjacking and Content Security Policy (CSP) headers, which are medium-risk vulnerabilities.
• Lack of HSTS (Strict-Transport-Security) implementation.
• General absence of several recommended security headers.

Specific concerns or red flags: The primary red flag is the VirusTotal malicious detection. Coupled with the 'F' security grade and identified missing critical security headers, the site presents a significant security risk. The discrepancy between VirusTotal and urlscan.io needs resolution.

Infrastructure Analysis

Technology Stack: The site utilizes Cloudflare for content delivery, security (WAF), and TLS/SSL management. The server is identified as `cloudflare`.

DNS Configuration: Not available in the provided report.

Cookie Security Analysis: Not available in the provided report.

Security.txt and Robots.txt presence: Both `security.txt` and `robots.txt` files were not found.

Performance Analysis

Overall performance rating: Excellent, with a Performance Score of 100/100.

Key performance metrics: A perfect score indicates exceptional loading speed, responsiveness, and visual stability, likely benefiting from Cloudflare's CDN capabilities.

Accessibility and SEO considerations: Scores are N/A/100 for both Accessibility and SEO, meaning these aspects were not evaluated in the provided report.

Environmental impact (carbon footprint): Not available in the provided report.

Actionable Recommendations

Security Improvements

Immediate Malware Investigation: Urgently investigate the single malicious detection reported by VirusTotal. This should involve comprehensive server and code scans, log analysis, and review of recent changes.

Implement Critical Security Headers:

• Content Security Policy (CSP): Implement a strict CSP to mitigate XSS and data injection attacks. Start with a reporting-only mode to fine-tune it.

• X-Frame-Options / CSP `frame-ancestors`: Implement `X-Frame-Options: DENY` or `Content-Security-Policy: frame-ancestors 'none'` to prevent clickjacking.
• Strict-Transport-Security (HSTS): Enable the `Strict-Transport-Security` header to enforce HTTPS-only connections and prevent SSL stripping attacks. Use `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.
• X-Content-Type-Options: Implement `X-Content-Type-Options: nosniff` to prevent MIME-type sniffing vulnerabilities.
• Referrer-Policy: Implement a `Referrer-Policy` header (e.g., `Referrer-Policy: strict-origin-when-cross-origin`) to control how referrer information is sent.

Address OWASP ZAP Vulnerabilities:

• Specifically address the Medium-risk issues related to Anti-clickjacking and CSP.
• Review and mitigate the Low-risk vulnerabilities identified by ZAP.

TLS Improvements: While Cloudflare generally provides good TLS, ensure the latest TLS versions (1.2/1.3) are enforced and deprecated cipher suites are disabled.

Mozilla Observatory Grade Improvement: By implementing the recommended security headers, the Mozilla Observatory grade should significantly improve from 'F' towards 'A'.

Security.txt and Robots.txt:

• Create a `security.txt` file at `/.well-known/security.txt` to provide security researchers with a point of contact.
• Create a `robots.txt` file at `/robots.txt` to guide search engine crawlers, even if it's empty, to prevent unnecessary 404s.

Performance Optimizations

• No specific performance optimizations are needed at this time, given the perfect 100/100 score. The current setup, likely leveraging Cloudflare, is performing optimally.
• Focus on maintaining current performance levels with any future changes or updates.

Best Practices to Implement

• Regular Security Audits: Conduct frequent vulnerability scans and penetration tests to identify and remediate new security flaws.
• Security Monitoring: Implement continuous security monitoring, including file integrity monitoring, intrusion detection, and log analysis.
• Accessibility and SEO Audits: Although not covered in the report, performing dedicated audits for Accessibility and SEO is crucial for user experience and search engine visibility.

Conclusion

The URL `https://example.com` demonstrates outstanding performance, ensuring a fast and responsive user experience. However, its security posture is critically flawed. The presence of a malicious detection by VirusTotal, combined with an 'F' security grade from Mozilla Observatory and identified critical missing security headers, indicates a severe risk. While Cloudflare provides some protective layers, the fundamental configurations of the website itself are highly vulnerable. Therefore, the URL **is not currently safe to use for any sensitive operations or data exchange** without immediate and significant security remediation efforts.

Japanese Version

セキュリティスキャンレポート

Target: https://example.com
生成日: 16/1/2026
Scan ID: u-0f115db062b7c0dd030b16878c99dea5c354b49dc37b38eb8846179c7783e9d7-de6b681a

エグゼクティブサマリー

全体的なリスクレベル: 高

VirusTotal分析

- **総エンジン数:** 97
- **悪意のある検出:** 1
- **不審:** 0
- **無害:** 70
- **未検出:** 26

PageSpeed Insights

- **パフォーマンス:** 100/100
- **アクセシビリティ:** 0/100
- **ベストプラクティス:** 0/100
- **SEO:** 0/100

Mozilla Observatory

- **セキュリティ評価:** F
- **スコア:** 10/100
- **合格テスト:** 5
- **不合格テスト:** 5

OWASP ZAP 脆弱性スキャン

- **総アラート数:** 7
- **高リスク:** 0
- **中リスク:** 2
- **低リスク:** 3
- **情報提供:** 2

検出された脆弱性:

1. [Medium] Missing Anti-clickjacking Header
2. [Informational] Re-examine Cache-control Directives
3. [Medium] Content Security Policy (CSP) Header Not Set
4. [Informational] Retrieved from Cache
5. [Low] Strict-Transport-Security Header Not Set

urlscan.io 分析

- **判定:** クリーン
- **脅威スコア:** 0/100
- **ドメイン:** example.com
- **サーバーIP:** 104.18.26.120
- **国:** N/A
- **サーバー:** cloudflare

WebCheck 分析

- **TLS評価:** F
- **WAF検出:** はい
- **HSTS有効:** いいえ
- **テクノロジー:** Cloudflare

AIによるセキュリティ分析

エグゼクティブサマリー

`https://example.com` は、PageSpeed Insightsで完璧な100/100スコアを達成し、優れたパフォーマンスを示しています。しかし、そのセキュリティ体制は致命的に脆弱であり、VirusTotalでの悪意のある検出と、重大な設定の脆弱性によるMozilla Observatoryの「F」評価によって浮き彫りになっています。そのため、直ちに対策を講じなければ、機密性の高いやり取りには安全ではありません。

セキュリティ分析

リスクレベル: 悪意のある検出が確認され、深刻なセキュリティ設定の欠陥があるため、高リスクです。

VirusTotal セキュリティレポート:

- スキャンされた97エンジンのうち1つが悪意のある検出。urlscan.ioはサイトがクリーンであると報告しているものの、これは直ちに調査を必要とする重要な発見です。

完全なVT統計: {"malicious":1,"undetected":26,"harmless":70,"suspicious":0,"timeout":0,"confirmed_timeout":0,"failure":0,"type_unsupported":0}

Mozilla Observatory セキュリティ設定レポート:

セキュリティ評価: F

セキュリティスコア: 10/100

- テスト合格: 5、テスト不合格: 5（全10テスト中）。
- これは、基本的なセキュリティ設定の実装における重大な失敗を示しています。

OWASP ZAP 脆弱性スキャンレポート:

総アラート数: 7

高リスク脆弱性: 0

中リスク脆弱性: 2

- アンチクリックジャッキングヘッダーの欠落: ユーザーをUI再構成攻撃に晒します。
- コンテンツセキュリティポリシー (CSP) ヘッダーが未設定: さまざまなインジェクション攻撃 (XSS、データインジェクション) を許可します。

低リスク脆弱性: 3

情報: 2

urlscan.io ウェブサイト分析レポート:

悪意の評価: なし - クリーン

脅威スコア: 0/100

サーバー: cloudflare (WAF/CDNが導入されていることを示す)

TLS発行者: Cloudflare TLS Issuing ECC CA 3

• urlscan.ioの「クリーン」評価とVirusTotalの「悪意のある」検出の矛盾に注意することが重要です。後者を調査の優先事項とするべきです。

WebCheck 総合スキャンレポート:

セキュリティヘッダー: Content-Type, Transfer-Encoding, Connection, Last-Modified, Allow, Age, CF-Cache-Status, Vary, Server, CF-Ray が存在します。

• 重大な欠落ヘッダー: Content-Security-Policy, X-Frame-Options (または同等のCSPディレクティブ), Strict-Transport-Security (HSTS), X-Content-Type-Options, Referrer-Policy。これらはZAPおよびObservatoryの調査結果と一致しています。

TLS/SSL設定: N/A (具体的な評価は提供されていませんが、CloudflareがTLS発行を処理しています)。

ファイアウォール/WAF検出: 検出: Cloudflare (保護層を追加するため、肯定的です)。

HSTSステータス: 有効化されていません。これにより、サイトはSSLストリッピング攻撃に対して脆弱になります。

主要なセキュリティの発見と検出された脅威:

• VirusTotalによる単一だが重要な悪意のある検出。
• Mozilla Observatoryの「F」評価に反映された極めて貧弱なセキュリティ設定。
• アンチクリックジャッキングおよびコンテンツセキュリティポリシー (CSP) ヘッダーの欠落が確認されており、これらは中リスクの脆弱性です。
• HSTS (Strict-Transport-Security) の実装不足。
• 推奨される複数のセキュリティヘッダーが一般的に欠落しています。

特定の懸念事項または危険信号: 主要な危険信号はVirusTotalの悪意のある検出です。「F」のセキュリティ評価と、欠落している重要なセキュリティヘッダーが特定されたことに加え、このサイトは重大なセキュリティリスクを抱えています。VirusTotalとurlscan.ioの間の矛盾は解決される必要があります。

インフラストラクチャ分析

テクノロジースタック: このサイトは、コンテンツ配信、セキュリティ (WAF)、TLS/SSL管理にCloudflareを利用しています。サーバーは `cloudflare` として識別されます。

DNS設定: 提供されたレポートには含まれていません。

Cookieセキュリティ分析: 提供されたレポートには含まれていません。

Security.txt および Robots.txt の存在: `security.txt` および `robots.txt` ファイルは両方とも見つかりませんでした。

パフォーマンス分析

全体的なパフォーマンス評価: 優れています。パフォーマンススコアは100/100です。

主要なパフォーマンス指標: 完璧なスコアは、卓越した読み込み速度、応答性、視覚的安定性を示しており、CloudflareのCDN機能の恩恵を受けている可能性が高いです。

アクセシビリティとSEOの考慮事項: アクセシビリティとSEOの両方でスコアはN/A/100であり、これらの側面は提供されたレポートでは評価されていません。

環境への影響 (二酸化炭素排出量): 提供されたレポートには含まれていません。

実行可能な推奨事項

セキュリティ改善

即時マルウェア調査: VirusTotalによって報告された単一の悪意のある検出を緊急に調査してください。これには、包括的なサーバーおよびコードスキャン、ログ分析、最近の変更のレビューが含まれるべきです。

重要なセキュリティヘッダーの実装:
• コンテンツセキュリティポリシー (CSP): XSSおよびデータインジェクション攻撃を軽減するために厳格なCSPを実装してください。チューニングのためにレポート専用モードから開始してください。
• X-Frame-Options / CSP `frame-ancestors`: クリックジャッキングを防ぐために `X-Frame-Options: DENY` または `Content-Security-Policy: frame-ancestors 'none'` を実装してください。
• Strict-Transport-Security (HSTS): HTTPSのみの接続を強制し、SSLストリッピング攻撃を防ぐために `Strict-Transport-Security` ヘッダーを有効にしてください。`Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` を使用してください。
• X-Content-Type-Options: MIMEタイプスニッフィングの脆弱性を防ぐために `X-Content-Type-Options: nosniff` を実装してください。
• Referrer-Policy: リファラー情報の送信方法を制御するために `Referrer-Policy` ヘッダー (例: `Referrer-Policy: strict-origin-when-cross-origin`) を実装してください。

OWASP ZAPの脆弱性への対応:
• 特に、クリックジャッキングおよびCSP関連の中リスクの問題に対処してください。
• ZAPによって特定された低リスクの脆弱性をレビューし、軽減してください。

TLS改善: Cloudflareは一般的に良好なTLSを提供していますが、最新のTLSバージョン (1.2/1.3) が強制され、非推奨の暗号スイートが無効になっていることを確認してください。

Mozilla Observatoryの評価改善: 推奨されるセキュリティヘッダーを実装することにより、Mozilla Observatoryの評価は「F」から「A」へと大幅に改善されるはずです。

Security.txt および Robots.txt:
• セキュリティ研究者に連絡先を提供するために、`/.well-known/security.txt` に `security.txt` ファイルを作成してください。
• 検索エンジンのクローラーを誘導するために、空であっても `/robots.txt` に `robots.txt` ファイルを作成し、不要な404を防いでください。

パフォーマンス最適化

• 完璧な100/100のスコアを考慮すると、現時点では特定のパフォーマンス最適化は必要ありません。現在の設定は、Cloudflareを活用している可能性が高く、最適に動作しています。
• 今後の変更や更新があっても、現在のパフォーマンスレベルを維持することに焦点を当ててください。

実装すべきベストプラクティス

• 定期的なセキュリティ監査: 新しいセキュリティの欠陥を特定し、修正するために、頻繁な脆弱性スキャンと侵入テストを実施してください。
• セキュリティ監視: ファイル整合性監視、侵入検知、ログ分析を含む継続的なセキュリティ監視を実装してください。
• アクセシビリティとSEO監査: レポートには含まれていませんが、アクセシビリティとSEOのための専用監査の実施は、ユーザーエクスペリエンスと検索エンジンの可視性にとって不可欠です。

結論

URL `https://example.com` は優れたパフォーマンスを示し、高速で応答性の高いユーザーエクスペリエンスを保証します。しかし、そのセキュリティ体制には致命的な欠陥があります。VirusTotalによる悪意のある検出、Mozilla Observatoryの「F」のセキュリティ評価、および特定された重要な欠落セキュリティヘッダーの存在は、深刻なリスクを示しています。Cloudflareはいくつかの保護層を提供していますが、ウェブサイト自体の基本的な設定は非常に脆弱です。したがって、直ちにかつ大幅なセキュリティ対策を講じなければ、このURLは**現在、機密性の高い操作やデータ交換に安全に使用することはできません**。