セキュリティスキャンレポート

https://sample-site.example/

スキャン日時: 2026-10-23T13:30:46 — vcheck 0.1.0 (authorized scan)

F	1	6	14	5	1
総合判定	致命的	高危険	中危険	低危険	情報

致命的 1件を含む計27件を検出 — 即時対応を強く推奨します。

検出ソフトウェア

種別	slug	バージョン	最新	状態
core	wordpress	7.1.3	7.1.3	最新
plugin	woocommerce	10.2.4	11.2.1	古い!!!
plugin	js_composer	8.6.1	repo外	repo外(商用等)
plugin	revslider	6.7.37	repo外	repo外(商用等)
plugin	lbg_famous_gallery_addon_visual_composer	?	repo外	repo外
plugin	prague-plugins	?	repo外	repo外
plugin	the-grid	2.8.0	repo外	repo外(商用等)
plugin	quikblock	?	repo外	repo外
plugin	real3d-flipbook	4.11.2	repo外	repo外(商用等)
plugin	wvt	1.2.1	repo外	repo外(商用等)
plugin	formidable	6.24.1	7.0	古い!!!
theme	prague	2.5.12	repo外	評価データなし

脆弱性・設定問題 (重大度順)

致命的 The Grid — 無認証コマンド注入 (RCE) — the-grid 2.8.0 は影響範囲内!!! (W-CVE-2026-94169)

検出: the-grid 2.8.0 / 影響: <= 2.8.1 (修正: 2.8.2+) / CVSS 10.0 / 公開 2026-10-14 / CVSS 10.0。Patchstack が mass-exploit キャンペーン化を予告

対策: the-grid を 2.8.2+ へ更新、または使用終了 (削除)

参考: https://patchstack.com/database/wordpress/plugin/the-grid/vulnerability/wordpress-the-grid-plugin-2-8-1-remote-code-execution-rce-vulnerability

高危険 strict-transport-security なし — HTTP強制 + TLSDowngrade攻撃防止。無いと初回接続時のSSL Stripが可能 (H-strict-trans)

レスポンスヘッダに存在しない

対策: 推奨値: max-age=31536000; includeSubDomains

高危険 **緊急CVE CVE-2026-109618 (PHP RCE (php2shell) — メモリ枯渇(OOM)処理中の未初期化内部データ悪用) — PHPバージョン不明 → 対象か要確認!!!** (P-W-CVE-2026-109618)

CVSS 9.2 / 公開 2026-10-21 (2日前) / 認証不要・遠隔任意コード実行 (PHP 5.4以降全バージョン/全SAPI)。野生悪用観測済み (Patchstack/Cloudflare/Amazon)

対策: PHP を修正版へ切替: 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35。8.1以下は修正版なし=8.2+移行必須 (WordPress.org公式も警告)

参考: https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security
参考: https://patchstack.com/articles/php-major-vulnerability-alert-10-2026

高危険 **緊急CVE CVE-2026-109619 (PHP RCE (php2shell) — 解放済みメモリの stale global state 再利用) — PHPバージョン不明 → 対象か要確認!!!** (P-W-CVE-2026-109619)

CVSS 9.2 / 公開 2026-10-21 (2日前) / 認証不要・遠隔任意コード実行。RCE未満でもワーカーメモリ (パスワード・APIキー) 漏えい可能

対策: PHP を修正版へ切替: 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35

参考: https://patchstack.com/articles/php-major-vulnerability-alert-10-2026

高危険 **Formidable Forms — PayPalサブスクリプション支払い検証バイパス (未認証で支払い完了扱い) — formidable 6.24.1 は影響範囲内!!!** (W-CVE-2026-11361)

検出: formidable 6.24.1 / 影響: <= 6.32.0 (修正: 6.32.1+) / CVSS 7.5 / 公開 2026-08-06 / 未認証で支払い完了を偽装可能

対策: formidable を 6.32.1+ へ更新

参考: https://github.com/advisories/ghsa-ww4h-86qv-rmr8

高危険 **Formidable Forms — 未認証保存XSS (frm-user-id パラメータ) — formidable 6.24.1 は影響範囲内!!!** (W-WF-frm-6331)

検出: formidable 6.24.1 / 影響: <= 6.33.1 / CVSS 7.2 / 公開 2026-01-01 / Wordfence Intelligence 登録 (未認証保存XSS)

対策: formidable を最新 (6.33.2+) へ更新

参考: https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/formidable/formidable-forms-6331-unauthenticated-stored-cross-site-scripting-via-frm-user-id-parameter

高危険 **REST API でユーザー列挙が可能 [/wp-json/wp/v2/users] (ログインID=メールアドレスが公開!!!)** (W5)

id=1 name=f.ozaki.1204@gmail.com ★管理者

対策: REST users エンドポイント無効化 (functions.php filter) + ログインIDを推測困難なものに変更。攻撃者はこれでブルートフォースのIDリストを作る。

中危険 DMARC レコードなし — SPF通過の偽メールを止める仕組みがない (D2)

```
dig TXT _dmarc.sample-site.example -> なし
```

対策: TXT "v=DMARC1; p=quarantine; rua=mailto:..." から開始 (ruaでレポート収集→p=rejectへ段階上げ)

中危険 content-security-policy なし — XSSが発生してもスクリプト実行を抑制する最強の盾。無いと注入されたJSが自由に動く (H-content-secu)

レスポンスヘッダに存在しない

対策: 推奨値: まず Report-Only で始めて徐々に厳格化 (script-src 'self')

中危険 x-frame-options なし — クリックジャッキング防止。無いとサイトを透明iframeに重ねて操作させられる (H-x-frame-opti)

レスポンスヘッダに存在しない

対策: 推奨値: SAMEORIGIN (CSP frame-ancestors でも可)

中危険 ポート 21 (ftp) が開いている (I-21)

```
TCP connect sample-site.example:21 -> open
```

対策: FTP — 平文プロトコル。使用終了なら閉鎖

中危険 nuclei検出: WordPress REST API ユーザー列挙 (?search=@ 経由) (N-CVE-2023-5561)

```
https://sample-site.example/?rest_route=/wp/v2/users&search=@ [route="?rest_route=/wp/v2/users&"] — nuclei template
```

対策: W5対策と同一脆弱性 (検出経路違い): REST users エンドポイント無効化 + ログインID変更

参考: https://nvd.nist.gov/vuln/detail/CVE-2023-5561

中危険 プラグイン formidable が古い (6.24.1 < 7.0) (R-formidable)

```
readme.txt stable tag: 6.24.1 / repo最新: 7.0
```

対策: formidable を 7.0 に更新

中危険 プラグイン woocommerce が古い (10.2.4 < 11.2.1) (R-woocommerce)

```
readme.txt stable tag: 10.2.4 / repo最新: 11.2.1
```

対策: woocommerce を 11.2.1 に更新

中危険 Slider Revolution — パストラバーサル (任意ファイル読み取り) — revslider 6.7.37 は影響範囲内!!! (W-CVE-2025-9217)

検出: revslider 6.7.37 / 影響: <= 7.0.9 / CVSS 6.5 / 公開 2025-08-29 / 約400万サイトが露出との報道。wp-config.php 等の読み取りに直結

対策: revslider を 7.0.10+ (最新) へ更新。6.x 系は全て影響

参考: https://www.infosecurity-magazine.com/news/flaw-slider-revolution-plugin

中危険 WPBakery Page Builder — 保存XSS (dataパラメータ、Subscriber+の低権限で可能) — js_composer 8.6.1 は影響範囲内!!! (W-CVE-2026-15101)

検出: js_composer 8.6.1 / 影響: <= 8.7.4 / CVSS 5.4 / 公開 2026-09-03 / 購読者権限でも実行可能な保存XSS

対策: WPBakery を 8.7.5+ へ更新

参考: https://www.sentinelone.com/vulnerability-database/cve-2026-15101

中危険 Real3D FlipBook — 認可欠如 (capability check欠如) — real3d-flipbook 4.11.2 は影響範囲内!!! (W-CVE-2026-86842)

検出: real3d-flipbook 4.11.2 / 影響: <= 5.3 (修正: 5.4+) / CVSS 6.5 / 公開 2026-09-24 / Author+ 権限で他人のフリップブック削除・設定変更。公開PoCも2016年から存在する由来的ターゲット

対策: real3d-flipbook を 5.4+ へ更新、未使用なら削除

参考: https://github.com/advisories/GHSA-c2cv-7vq9-6xf7

中危険 WPBakery Page Builder — Broken Access Control — js_composer 8.6.1 は影響範囲内!!! (W-PS-jscomposer-873)

検出: js_composer 8.6.1 / 影響: <= 8.7.2 (修正: 8.7.3+) / CVSS 6.5 / 公開 2026-05-13 / capability check 欠如 (Patchstack)

対策: WPBakery を 8.7.3+ へ更新

参考: https://patchstack.com/database/wordpress/plugin/js_composer/vulnerability/wordpress-wpbakery-page-builder-plugin-8-7-2-broken-access-control-vulnerability

中危険 RSSフィードから投稿者ユーザー名が漏えい (f.ozaki.1204@gmail.com) (W10)

GET /feed/ -> dc:creator でユーザー名が取得できる

対策: functions.php でフィードの dc:creator を除去。表示名はニックネームに。

中危険 XML-RPC が完全有効 (W7)

POST xmlrpc.php system.listMethods -> 200, 78メソッド (multicall有効 = 総当たり高速化)

対策: xmlrpc.php をブロック (使用プラグイン確認の上)。Jetpack等は pingback のみ無効化で可。

中危険 **ログイン画面が全世界に公開 (WAF/レート制限なし)** (W8)

```
GET wp-login.php -> 200 (WAF/CDNなし!!! 直暴露)
```

対策: Cloudflare 等のWAFを前段に置き、wp-login に Turnstile + レート制限を適用。IP制限も可。

低危険 **permissions-policy なし — カメラ/位置情報等のAPI濫用防止** (H-permissions-)

レスポンスヘッダに存在しない

対策: 推奨値: camera=(), microphone=(), geolocation=()

低危険 **referrer-policy なし — URL経由での情報漏えい防止** (H-referrer-pol)

レスポンスヘッダに存在しない

対策: 推奨値: strict-origin-when-cross-origin

低危険 **x-content-type-options なし — MIME Sniffing経由の攻撃防止** (H-x-content-ty)

レスポンスヘッダに存在しない

対策: 推奨値: nosniff

低危険 **readme.html が公開 (WPバージョン情報漏えい: 7.1.3)** (W1)

```
GET https://sample-site.example/readme.html -> 200, WordPress 7.1.3 [別経路指紋 (generator/asset ?ver=)]
```

対策: nginx で readme.html をブロック (location = /readme.html { return 404; })。削除でも可。

低危険 **wp-cron.php が外部から起動可能** (W12)

```
GET wp-cron.php -> 200 (アクセスのたびにWP内部ジョブが走る)
```

対策: DISABLE_WP_CRON + サーバー側cron (systemd/crontab 5分毎) への移行が定石。トラフィック増時にDB負荷になる。

情報 **MX あり (1件)** (D3)

```
0 sample-site.example.
```

本レポートは承認済みスキャンに基づく。外部サイトへの実施には事前にオーナーの書面同意を得ること。