CheckmarxによるZAPスキャンレポート

2026 年 5 月 16 日、20:35:13 に ZAP で生成

コンテンツ

このレポートについて

レポートパラメータ

コンテキスト

コンテキストが選択されていなかったため、デフォルトですべてのコンテキストが含まれています。

サイト

以下のサイトが対象となりました。

- http://www.teruyasu.jp
- https://www.teruyasu.jp

（サイトが選択されていない場合は、デフォルトで全てのサイトが含まれます。）

レポートにデータを含めるためには、対象となるサイトが、対象となるコンテキストのいずれかに属している必要があります。

リスクレベル

含まれるもの： 高、中、低、情報

除外対象： なし

信頼度

含まれる: ユーザー確認済み、高、中、低

除外対象： ユーザー確認済、高、中、低、誤検知（誤った警告）

要約

リスクと信頼度別の警告件数

この表は、レポートに含まれるリスクレベルと信頼度レベルごとのアラート数を示しています。

（括弧内のパーセンテージは、レポートに含まれるアラートの総数に対する割合（小数点以下第1位まで四捨五入）を表しています。）

		自信				
		ユーザー確認済み	高い	中	低い	合計
リスク	高い	0 (0.0%)	1 (3.8%)	3 (11.5%)	0 (0.0%)	4 (15.4%)
	中	0 (0.0%)	1 (3.8%)	3 (11.5%)	1 (3.8%)	5 (19.2%)
	低い	0 (0.0%)	2 (7.7%)	8 (30.8%)	1 (3.8%)	11 (42.3%)
	情報	0 (0.0%)	1 (3.8%)	2 (7.7%)	3 (11.5%)	6 (23.1%)
	合計	0 (0.0%)	5 (19.2%)	16人 (61.5%)	5 (19.2%)	26 (100%)

サイト別およびリスク別の警告件数

この表は、1つ以上の警告が発せられた各サイトについて、リスクレベルごとに発せられた警告の数を示しています。

信頼度レベルが「誤検知」のアラートは、これらの集計から除外されています。

（括弧内の数字は、そのリスクレベル以上で当該サイトに対して発令された警告の件数です。）

		リスク			
		高い (=高い)	中 (>= 中)	低い (>= 低い)	情報 (>= 情報)
サイト	https://www.teruyasu.jp	4 (4)	5 (9)	11 (20)	6 (26)

アラートの種類別のアラート件数

この表は、各アラートタイプの発生件数と、そのアラートタイプのリスクレベルを示しています。

（括弧内のパーセンテージは、本レポートに含まれるアラートの総数に対する各件数の割合（小数点以下第1位まで四捨五入）を表しています。）

アラートの種類	リスク	カウント
クロスサイトスクリプティング（リフレクテッド）	高い	1 (3.8%)
外部リダイレクト	高い	4 (15.4%)
個人情報開示	高い	18人 (69.2%)
SQLインジェクション - SQLite	高い	16人 (61.5%)
アプリケーションエラー開示	中	1 (3.8%)
コンテンツセキュリティポリシー（CSP）ヘッダーが設定されていません	中	1989年 (7,650.0%)
クリックジャッキング対策ヘッダーがありません	中	1570 (6,038.5%)
セキュアページには、スクリプトを含む混合コンテンツが含まれます。	中	2 (7.7%)
アンチCSRFが使用されていない	中	7050 (27,115.4%)
Cookie No HttpOnlyフラグ	低い	1 (3.8%)

セキュアフラグのないクッキー	低い	1 (3.8%)
SameSite属性のないCookie	低い	1 (3.8%)
クロスドメインJavaScriptソースファイルのインクルージョン	低い	7108 (27,338.5%)
情報漏洩 - デバッグエラーメッセージ	低い	1 (3.8%)
セキュアページには混合コンテンツが含まれています	低い	103 (396.2%)
サーバーが「X-Powered-By」HTTPレスポンスヘッダーフィールドを介して情報を漏洩する	低い	831 (3,196.2%)
サーバーがHTTPレスポンスヘッダーの「Server」フィールドを介してバージョン情報を漏洩	低い	4291 (16,503.8%)
Strict-Transport-Security ヘッダーが設定されていません	低い	4058 (15,607.7%)
X-Content-Type-Options ヘッダーがありません	低い	3638 (13,992.3%)
タイムスタンプの露見 - Unix	低い	1 (3.8%)
投稿を取得する	情報	6 (23.1%)
情報開示 - 不審なコメント	情報	996 (3,830.8%)
最新のWebアプリケーション	情報	1945年 (7,480.8%)
キャッシュ制御ディレクティブを再検討する	情報	2 (7.7%)
ユーザーエージェントファザー	情報	1812 (6,969.2%)
ユーザーが制御可能なHTML要素属性（潜在的なXSS脆弱性）	情報	943 (3,626.9%)
合計		26

アラート

リスク=高、信頼度=高 (1)

https://www.teruyasu.jp (1)

個人情報開示 （1）

▼GET https://www.teruyasu.jp/products/handle_collection.html

アラートタグ

- OWASP_2021_A04
- OWASP_2017_A03

アラートの説明

応答には、クレジットカード番号、社会保障番号、その他同様の機密データなどの個人識別情報が含まれています。

その他の情報

検出されたクレジットカードの種類：ダイナースクラブ

銀行識別番号：300000

ブランド：DISCOVER

カテゴリー：名刺

発行者：ダイナースクラブ・インターナショナル

リクエスト

▼リクエスト行とヘッダー部分（342バイト）

```
GET https://www.teruyasu.jp/products/handle_collection.html
HTTP/1.1
Host: www.teruyasu.jp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
Pragma: no-cache
Cache-Control: no-cache
Referer: https://www.teruyasu.jp
Cookie: ECSESSID=a13n2g53hl6p5kmdm8ok3sr2i0
```

▼リクエスト本文（0バイト）

応答

▼ステータス行とヘッダーセクション（369バイト）

```
HTTP/1.1 200 OK
Date: Sat, 16 May 2026 08:21:31 GMT
Server: Apache/2.2.31 (Amazon)
X-Powered-By: PHP/5.3.29
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Expires: 0
Vary: Accept-Encoding,User-Agent
Access-Control-Allow-Credentials: true
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Content-Length: 216665
```

▶ レスポンスボディ（216665バイト）

証拠

30000000410732

リスク=高、信頼度=中 (3)

https://www.teruyasu.jp (3)

クロスサイトスクリプティング（リフレクテッド） （1）

▶ 投稿 https://www.teruyasu.jp/dbsys/words.php

外部リダイレクト （1）

▶ GET https://www.teruyasu.jp/index.html?
banner_472_64=8175774919077704545.owasp.org

SQLインジェクション - SQLite (1)

▶ 投稿 https://www.teruyasu.jp/frontparts/login_check.php

リスク=中、信頼度=高 (1)

https://www.teruyasu.jp (1)

コンテンツセキュリティポリシー（CSP）ヘッダーが設定されていません （1）

▶ GET https://www.teruyasu.jp/

リスク=中、信頼度=中 (3)

https://www.teruyasu.jp (3)

アプリケーションエラーの開示 （1）

▶ GET https://www.teruyasu.jp/contact/

クリックジャッキング対策ヘッダーがありません (1)

▶ GET https://www.teruyasu.jp/

セキュアページには混合コンテンツ（スクリプトを含む）が含まれます （1）

▶ GET https://www.teruyasu.jp/contact/unsub.html

リスク=中、信頼度=低 (1)

https://www.teruyasu.jp (1)

アンチCSRFが使用されていない (1)

▶ GET https://www.teruyasu.jp/

リスク=低、信頼度=高 (2)

https://www.teruyasu.jp (2)

サーバーが「Server」HTTPレスポンスヘッダーフィールドを介してバージョン情報を漏洩する （1）

▶ GET https://www.teruyasu.jp/robots.txt

Strict-Transport-Security ヘッダーが設定されていません (1)

▶ GET https://www.teruyasu.jp/robots.txt

リスク=低、信頼度=中 (8)

https://www.teruyasu.jp (8)

Cookie 非 HttpOnly フラグ (1)

▶ GET https://www.teruyasu.jp/cart/

セキュアフラグのないクッキー （1）

▶ GET https://www.teruyasu.jp/cart/

SameSite属性のないCookie （1）

▶ GET https://www.teruyasu.jp/cart/

クロスドメインJavaScriptソースファイルのインクルージョン （1）

▶ GET https://www.teruyasu.jp/

情報漏洩 - デバッグエラーメッセージ (1)

▶ GET https://www.teruyasu.jp/contact/

セキュアページには混合コンテンツが含まれます （1）

▶ GET https://www.teruyasu.jp/email/20161102_fuchu.html

サーバーが「X-Powered-By」HTTPレスポンスヘッダーフィールドを介して情報を漏洩する （1）

▶ GET https://www.teruyasu.jp/cart/

X-Content-Type-Options ヘッダーがありません (1)

▶ GET https://www.teruyasu.jp/robots.txt

リスク=低、信頼度=低 (1)

https://www.teruyasu.jp (1)

タイムスタンプの露見 - Unix (1)

▶ GET https://www.teruyasu.jp/mov/mov3.mp4

リスク=情報、信頼度=高 (1)

https://www.teruyasu.jp (1)

POST用のGET (1)

▶ GET https://www.teruyasu.jp/dbsys/entry.php

リスク＝情報、確信度＝中 (2)

https://www.teruyasu.jp (2)

最新のWebアプリケーション (1)

▶ GET https://www.teruyasu.jp/

ユーザーエージェントファザー (1)

▶ 投稿 https://www.teruyasu.jp/entry/

リスク＝情報、信頼度＝低い (3)

https://www.teruyasu.jp (3)

情報開示 - 不審なコメント (1)

▶ GET https://www.teruyasu.jp/contact/

キャッシュ制御ディレクティブを再検討する (1)

▶ GET https://www.teruyasu.jp/robots.txt

ユーザーが制御可能なHTML要素属性（潜在的なXSS脆弱性） (1)

▶ 投稿 https://www.teruyasu.jp/forgot/

付録

アラートの種類

このセクションには、レポートに含まれるアラートの種類に関する追加情報が記載されています。

クロスサイトスクリプティング（リフレクテッド）

ソース	アクティブスキャナによって発生した （クロスサイトスクリプティング（リフレクテッド））
CWE ID	79
WASC ID	8
参照	▪ http://projects.webappsec.org/Cross-Site-Scripting

	▪ http://cwe.mitre.org/data/definitions/79.html

外部リダイレクト

ソース	アクティブスキャナによって発生しました （外部リダイレクト）
CWE ID	601
WASC ID	38
参照	▪ http://projects.webappsec.org/URL-Redirector-Abuse ▪ http://cwe.mitre.org/data/definitions/601.html

個人情報開示

ソース	パッシブスキャナーによって発生した （個人情報開示）
CWE ID	359
WASC ID	13

SQLインジェクション - SQLite

ソース	アクティブスキャナによって発生した脆弱性 （SQLインジェクション - SQLite）
CWE ID	89
WASC ID	19
参照	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

アプリケーションエラー開示

ソース	パッシブスキャナによって発生したエラー （アプリケーションエラー開示）
CWE ID	200
WASC ID	13

コンテンツセキュリティポリシー（CSP）ヘッダーが設定されていません

ソース	パッシブスキャナによって発生しました （コンテンツセキュリティポリシー（CSP）ヘッダーが設定されていません）
CWE ID	693
WASC ID	15
参照	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

	US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://content-security-policy.com/

クリックジャッキング対策ヘッダーがありません

ソース	パッシブスキャナによって発生しました （アンチクリックジャッキングヘッダー）
CWE ID	1021
WASC ID	15
参照	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

セキュアページには、スクリプトを含む混合コンテンツが含まれます。

ソース	パッシブスキャナによって検出された （セキュアページには混合コンテンツが含まれる）
CWE ID	311
WASC ID	4
参照	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

アンチCSRFが使用されていない

ソース	パッシブ スキャナーによって発生しました (アンチCSRF自らが使用されていない)
CWE ID	352
WASC ID	9
参照	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Cookie No HttpOnlyフラグ

ソース	パッシブスキャナによって発生 （Cookie No HttpOnlyフラグ）
CWE ID	1004
WASC ID	13
参照	▪ https://owasp.org/www-community/HttpOnly

セキュアフラグのないクッキー

ソース	パッシブスキャナによって発生した事象 （セキュアフラグのないCookie）
CWE ID	614
WASC ID	13
参照	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

SameSite属性のないCookie

ソース	パッシブスキャナーによって発生した （SameSite属性のないCookie）
CWE ID	1275
WASC ID	13
参照	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

クロスドメインJavaScriptソースファイルのインクルージョン

ソース	パッシブスキャナによって発生した問題 （クロスドメインJavaScriptソースファイルのインクルージョン）
CWE ID	829
WASC ID	15

情報漏洩 - デバッグエラーメッセージ

ソース	パッシブスキャナによって発生したエラー （情報漏洩 - デバッグエラーメッセージ）
CWE ID	200
WASC ID	13

セキュアページには混合コンテンツが含まれています

ソース	パッシブスキャナによって検出された （セキュアページには混合コンテンツが含まれる）
CWE ID	311

WASC ID	4
参照	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

サーバーが「X-Powered-By」HTTPレスポンスヘッダーフィールドを介して情報を漏洩する

ソース	パッシブスキャナーによって報告された問題 （「X-Powered-By」HTTPレスポンスヘッダーフィールドを介してサーバーが情報を漏洩）
CWE ID	200
WASC ID	13
参照	▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

サーバーがHTTPレスポンスヘッダーの「Server」フィールドを介してバージョン情報を漏洩

ソース	パッシブスキャナによって発生した （HTTPサーバー応答ヘッダー）
CWE ID	200
WASC ID	13
参照	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Strict-Transport-Security ヘッダーが設定されていません

ソース	パッシブスキャナによって発生したエラー （Strict-Transport-Securityヘッダー）
CWE ID	319
WASC ID	15
参照	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers

	▪ http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ http://caniuse.com/stricttransportsecurity ▪ http://tools.ietf.org/html/rfc6797

X-Content-Type-Options ヘッダーがありません

ソース	パッシブスキャナによって発生したエラー （X-Content-Type-Optionsヘッダーが見つかりません）
CWE ID	693
WASC ID	15
参照	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

タイムスタンプの露見 - Unix

ソース	パッシブスキャナーによって生成されました (タイムスタンプの露見)
CWE ID	200
WASC ID	13
参照	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

投稿を取得する

ソース	アクティブスキャナによって発生したリクエスト （POSTの場合はGET）
CWE ID	16
WASC ID	20

情報開示 - 不審なコメント

ソース	パッシブスキャナーによって検出されました （情報漏洩 - 不審なコメント）
CWE ID	200
WASC ID	13

最新のWebアプリケーション

ソース	パッシブスキャナによって発生した問題 （最新のWebアプリケーション）

キャッシュ制御ディレクティブを再検討する

ソース	パッシブスキャナによって発生したエラー （キャッシュ制御ディレクティブの再検査）
CWE ID	525
WASC ID	13
参照	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

ユーザーエージェントファザー

ソース	アクティブスキャナ （ユーザーエージェントファザー） によって発生
参照	▪ https://owasp.org/wstg

ユーザーが制御可能なHTML要素属性（潜在的なXSS脆弱性）

ソース	パッシブスキャナによって発生した脆弱性 （ユーザーが制御可能なHTML要素属性（潜在的なXSS））
CWE ID	20
WASC ID	20
参照	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute