簡易 Web 脆弱性診断

本サービスはお客さまの Web サイトの脆弱性診断を実施できるサービスです。

※　診断対象はドメイン内のサイトのみです。

※　1 ドメインにつき、1 日 3 回までのご利用制限があります。

※　パッシブスキャン（攻撃を伴わない静的な診断）のみを実施いたします。

※　多くのお客さまにご利用いただいた場合、診断実施にお時間をいただく場合がございます。

※　診断結果（CSV）は英語でのご提供です。日本語は非対応となりますのでご了承ください。

※　本機能でご提供する脆弱性診断は、指定された URL を対象に、攻撃を伴わないパッシブスキャンのみを実施します。攻撃を伴わない簡易診断のため、特にリスクの高い脆弱性など、全ての脆弱性を発見できるものではありません。
また、検知された脆弱性の内容についての調査・修正はサポート対象範囲外となります。予めご了承ください。

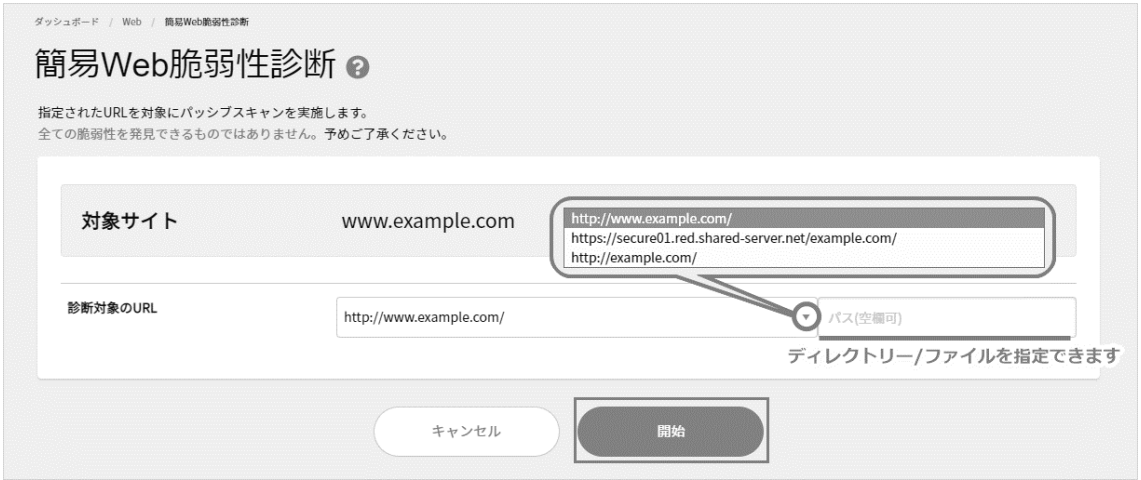
■簡易 Web 脆弱性診断を開始する

Control Panel の「Web」メニューから「Web 脆弱性診断」をクリック

診断 URL 一覧 の **新規追加** クリック

「診断対象の URL」に対象サイトを選択し **開始** をクリック

※ 「診断対象の URL」のプルダウンから、URL を選択する場合、「**www あり**」「**www なし**」「**https://**」から選択できます。



診断対象 URL	http://www.お客さまドメイン名/
	http://お客さまドメイン名/
	https://secure**.***.shared-server.net/www.お客さまドメイン名/ ※*の箇所はお客さまによって表記が異なります。

ご入力いただいた URL により、以下のエラーメッセージが表示される場合があります。
入力内容をご確認の上、あらためて入力をお試しください。

診断情報入力時のエラーメッセージ	
URL が存在しません。	対象 URL が確認できない場合に表示されます。
パスが長すぎます。	パス名の文字数が超過しています。
パスに使用できない文字が入力されています。	指定されたパスに使用できない文字が入力されています。
パスが存在しません。	指定されたパス（ディレクトリ・ファイル）が Web サーバー上で確認できない場合に表示されます。
診断 URL へのアクセスがタイムアウトしました。	タイムアウトエラーです。 数分程度、時間をおいてあらためてお試しください。
認証が必要なため、診断できません(CODE:401)。	対象のディレクトリやファイルに BASIC 認証などが設定されている場合に表示されます。
アクセスが拒否されました(CODE:403)。	対象のディレクトリやファイルへのアクセスが行えない場合に表示されます。パーミッションをご確認ください。
診断 URL へのアクセスに失敗しました(CODE:500)。	なんらかの理由でサイトへアクセスできない場合に表示されます。 アクセス可能かご確認の上、あらためてお試しください。
エラー：DNS が外部のホストを参照しています。	簡易 Web 脆弱性診断は、ご利用の Web サーバー内を診断対象とします。Web サイトの DNS レコードが外部サーバーへ接続されている場合は診断できません。

正常に開始された場合、「診断サイトを追加しました」のメッセージが表示され、診断サイト一覧の URL・診断状態が表示されます

「状態」の一覧	
順番待ち	「開始」して定期実行が行われる間、もしくは診断が込み合っていて順番待ち
診断中	診断処理中。中止で「停止中」に移行
停止中	停止指示を出して、実施処理が停止待ちの間
停止済	停止済み
完了	診断が成功
診断失敗	診断処理が失敗して終了

※　診断にかかる時間は、対象のサイトのディレクトリー・ファイル数により異なります。

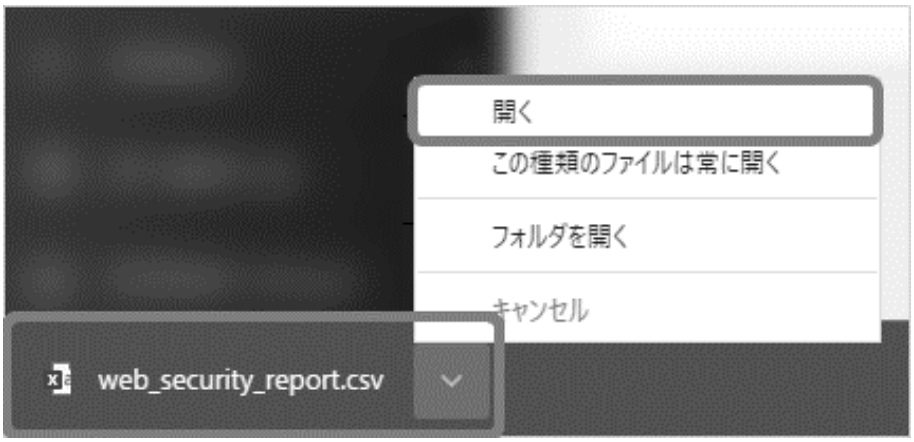
■「状態」が「診断失敗」となった場合

脆弱性診断の登録が成功した場合も、診断開始から診断終了までになんらかの事由で診断が失敗する場合があります。

「診断失敗」の一覧	
診断の最大時間を超えました	制限時間内(60 分)に診断が終わらない場合に表示されます。 サブディレクトリを指定するなど、対象を絞って実行してください。
結果ファイルの保存に失敗しました	Web ディレクトリへの結果の保存に失敗した場合に表示されます。 Web のディスク使用量をご確認ください。
検出上限を超えました	脆弱性の検出数が多すぎる場合に表示されます。 サブディレクトリを指定するなど、対象を絞って実行してください。

画面右上の **更新** をクリック後、診断サイト一覧の URL 右に表示される **結果取得** をクリック

「web_security_report.csv」のファイル名で CSV ファイルがダウンロードされますので、内容をご確認ください。



■診断結果について

診断結果は、CSV ファイルでの取得のほか、JSON 形式のファイルがお客さまの Web ディレクトリ内に自動的に保存されます。
※契約者・ドメイン管理者の権限でのみ確認が可能です。

1. ［Web］メニューをクリック
2. ［ファイルマネージャー］をクリック
3. ディレクトリ「web_security_report」をクリック

診断結果 JSON ファイル パス	/ドメイン名/web_security_report/www.ドメイン名_**yyyyMMddhhmmss_XXXXX**.json ➢ **yyyyMMddhhmmss**：診断日時 ➢ **XXXXX**：一意の数字が割り当てられます

■Web サイト脆弱性診断の結果確認

※　診断結果（CSV 形式）の内容はすべて英語で出力されます。（日本語非対応）
お手数ですが、翻訳ツールなどをご利用いただき、内容をご確認ください。

	A	B	C	D	E	F	G	H
1	Risk	URL	Method	Name	Description	Evidence	Solution	Link
2	Low	http://www.example.com/	GET	Information Disclosure - Debug Error Messages	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS	under construction	Disable debugging messages before pushing to production.	https://jvndb.jvn.jp/ja/cwe/CWE-200.html https://www.zaproxy.org/docs/alerts/10023/
3	Low	http://www.example.com/	GET	X-Content-Type-Options Header Missing	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 response body, potentially causing the response body to be interpreted and displayed as a content type other than the		Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing	https://jvndb.jvn.jp/ja/cwe/CWE-693.html https://www.zaproxy.org/docs/alerts/10021/
4	Medium	http://www.example.com/	GET	X-Frame-Options Header Not Set	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.		Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN.	https://jvndb.jvn.jp/ja/cwe/CWE-1021.html https://www.zaproxy.org/docs/alerts/10020/
5								
6	3 alerts found.							

Risk：危険度	**Informational　情報**	報告された脆弱性の危険度が表示されます。 Information, Low, Medium, High の順で危険度が上がり、 **High** は急ぎ対応が必要になります。
	Low　低	
	Medium　中	
	High　高	
URL：対象 URL		脆弱性が発見された URL です。
Method：HTTP メソッド		URL の HTTP リクエストのメソッドです。 GET, POST, DELETE, PUT などがあります。
Name：アラート名		脆弱性の名称です。 対象 URL（対象ファイル）にどのような脆弱性が発見されたかの概要です。
Description：詳細		脆弱性の概略です。 対象 URL（対象ファイル）にどのような脆弱性が発見されたかが表示されます。
Evidence：再現方法		脆弱性の再現方法です。
Solution：解決策		脆弱性の解決方法です。
Link：参照リンク		対象の脆弱性が該当する共通脆弱性タイプ（CWE）のリンクを記載しています。 「JVN iPedia - 脆弱性対策情報データベース」 「ZAP アラート詳細」 の参照リンクが表示されます。