Webアプリケーション脆弱性診断サービス

Webアプリケーション脆弱性診断サービスは、お客様が公開等を行っているWebサイトを構成するWebアプリケーションの脆弱性の検出を行うサービスです。
診断は、リモート／オンサイトのいずれかの診断方法で実施します。

■ 診断種別

リモート	オンサイト
・弊社の診断用ネットワークからインターネット越しに診断を行います。	・お客様のデーターセンターや事業場へ診断員が訪問し、お客様のネットワーク内部から診断を行います。

リモート／オンサイトいずれの場合も診断項目は変わりません。

■ 診断対象の環境について

Webアプリケーション脆弱性診断サービスでは、お客様のWebサイトに対し、通常の運用では想定されない値を含む様々なリクエストを送信します。
お客様の本番環境の停止や破壊を避けるために、診断作業用のテスト環境（開発環境など）を準備いただくことをおすすめします。

■ 診断項目

診断項目	診断内容
インジェクション	SQLインジェクション、コマンドインジェクション、CRLFインジェクションによる、コマンド挿入の脆弱性がないか調査します。
クロスサイトスクリプティング(XSS)	入力フォームから入力内容を表示する画面で、スクリプトを含む悪意のあるURLのリンクを仕掛けるクロスサイトスクリプティングの脆弱性がないか調査します。
パストラバーサル	パストラバーサルによる脆弱性がないか調査します。
XML外部エンティティ参照(XXE)	XML外部エンティティ参照 (XXE)による脆弱性がないか調査します。
オープンリダイレクト	オープンリダイレクトによる脆弱性がないか調査します。
シリアライズされたオブジェクト	シリアライズされたオブジェクトによる脆弱性がないか調査します。
インクルードにまつわる脆弱性	インクルードにまつわる脆弱性がないか調査します。
クリックジャッキング	クリックジャッキングによる脆弱性がないか調査します。
認証	認証回避、ログアウト機能の不備や未実装、過度な認証試行に対する対策不備など、認証に関するの脆弱性がないか調査します。
認可制御の不備	認可制御の不備による脆弱性がないか調査します。
クロスサイトリクエストフォージェリ(CSRF)	クロスサイトリクエストフォージェリ(CSRF)による脆弱性がないか調査します。
セッション管理の不備	セッションフィクセイション(セッション固定攻撃)、CookieのHttpOnly属性未設定、推測可能なセッションIDによる、セッション管理の不備がないか調査します。
情報漏洩	クエリストリング情報の漏洩、キャッシュからの情報漏洩やHTTPS利用時のCookieのSecure属性等の不備等による情報漏洩が発生しないか調査します。
サーバソフトウェアの設定の不備	ディレクトリリスティング、バージョン番号表示、不要なHTTPメソッドによる、サーバソフトウェアの設定の不備がないか調査します。
公開不要な機能・ファイル・ディレクトリの存在	公開不要な機能・ファイル・ディレクトリが存在しないか調査します。
JSON、JSONPにまつわる脆弱性	JSONエスケープの不備、JSON直接閲覧によるXSS、JSONPのコールバック関数名によるXSS、JSONハイジャック、JSONPの不適切な利用がないか調査します。[WebAPIのみ]
CORSの検証不備	CORSの検証不備がないか調査します。[WebAPIのみ]

■ 診断実施の流れ

1. 受付

- お客様からのお問い合わせを受け、診断実施内容および診断実施の希望時期を確認いたします。

2. 見積

- 受付後対象サイトのオブジェクト数確定から3営業日以内に診断実施の可否と見積を提示いたします。

※ 見積もりにはオブジェクト数（入力要素やパラメータの総数）が必要です（ご希望に応じお客様サイトをクロールして調査を行います）

※ 要員がアサインできない等により実施できない場合があります

3. 契約

- 正式なお申し込みを頂いた後、契約手続きをさせていただきます。

4. 事前準備

- 診断ツールの最新化や診断場所の手配などの事前準備に3～5営業日のお時間をいただきます。

5. 診断実施

- お客様と合意した日程・時間帯で診断作業を実施します。

※ 実施期間は、対象とするサイトの規模により変動します

6. 報告

- 診断結果を報告書にまとめてご報告します。

◆ 注意事項

Webアプリケーション脆弱性診断サービスは、Webアプリケーションの脆弱性を網羅的に調査するサービスですが、対象のWebアプリケーションの変更やWebサービスの設定変更により新しい脆弱性が生まれる可能性があります。診断結果で脆弱性が見つからなかった場合でも脆弱性が永続的に無いことを保証するものでは有りません。

製品・サービスについてのお問い合わせは

株式会社ＦＦＲＩセキュリティ
〒100-0005
東京都千代田区丸の内3-3-1　新東京ビル2階
TEL：03-6277-1811　E-mail：sales@ffri.jp

本製品に関する情報はインターネットでもご覧いただけます。
https://www.ffri.jp/

2021年12月現在　Ver 1.00.00