脆弱性診断サービスの特徴

- 詳細なヒアリングを通じて、対象システムの特性や期間・コストを明瞭化し、お客様課題の解決に向けた最適なプランをご提案致します。
- OWASP TOP10に対応したツールを使用し、Webアプリケーションの一般的な脆弱性から最新のセキュリティトレンドや脆弱性動向、ユーザからのフィードバックを取り入れながら定期的にシグネチャを追加・更新しています。
- 危険度の高い脆弱性を検出した場合は、診断期間中であっても診断期間の終了を待たずに即日の速報レポートを提供します。
- 報告書を提出した後も30日間無償でお客様のご質問にお応えし致します。経験と知識が必要なセキュリティ対策について、技術的な不安を解消しながらセキュリティレベルの向上を図るためのご支援をさせていただきます。

診断項目

診断項目	概要	予想される被害
SQLインジェクション	送信されたクエリにSQL文を挿入することで、データベースへ問い合わせの処理を利用する	・データベースの改ざん ・個人情報などの情報漏洩
OSコマンドインジェクション	OSの操作に使用されるOSコマンドを挿入する事で、任意のOSコマンドを実行する	・サーバー内の情報の改ざんや漏洩 ・不正なプログラムのダウンロード ・他のシステムページへの攻撃の踏み台
リモートコード実行	パラメータ値にURL（またはURLの一部）を送信する事で、攻撃者が指定したアクセス先へ実行できる	・端末の乗っ取り
オープンリダイレクト	スクリプトの一部を別ファイルから読み込む際に、攻撃者が指定した外部サーバのURLをファイルとして読み込ませることで、任意のスクリプトを動作させる	・意図しないサイトへのアクセス ・パスワードの抜き取り
HTTPヘッダインジェクション	HTTPヘッダの不備を利用し、ヘッダ行に挿入することで不正な動作を起こす	・XSS、セッションハイジャックのもとになる可能性
SSIインジェクション	SSIコマンドを攻撃者に勝手に実行されてしまう	・サイトの情報漏洩、改ざん
XPathインジェクション	XPathクエリーを利用し、パラメーターを通じて不正な値を入力させる	・サイトの情報漏洩、改ざん
LDAPインジェクションン	検索フィルタ文字列に、LDAPクエリとして混ぜ込み送信し、LDAP認証を突破される	・なりすまし ・LDAPデータベースの情報抜き取り
XML外部実体参照	アプリケーションがXMLを解析したときに、XMLの特殊構文を悪用する	・ディレクトリトラバーサル、ポートスキャン等に繋がる恐れ
安全でないデシリアライゼーション	cookieやセッション変数などからシリアライズ関数を用いて復元する際に、攻撃者が任意のコードを実行できる	・クレジットカードの情報抜取
ディレクトリトラバーサル	ファイルを選択できるフォームに相対パスや絶対パスを挿入して送信する事で、サーバ内のファイル閲覧できる	・公開されてないファイルの閲覧 ・情報漏洩
クロスサイトスクリプティング	動的なWebサイトに悪意のあるコードを挿入することによりアクセス時に不正な操作を実行させる	・偽のWebページへ誘導し情報をだまし取る ・偽の情報を拡散させる ・cookieの漏洩
クロスサイトリクエストフォージェリ	偽装したURLを開かせることにより、利用者に意図せず特定のサイト上で何らかの操作を行わせる	・意図しない攻撃への加担 ・意図しない商品が購入される
平文通信	httpなどの暗号化されてない平文で通信を行っている	・盗聴、改ざん、認証情報の漏洩
セッションフィクセーション	利用者のセッションIDを強制的に指定し、ログインをしたときに攻撃者がログイン済みのセッションIDを入手する(セッションハイジャック)	・なりすまし
セッション管理不備	セッションIDの漏洩や予測可能なセッションIDを使っている場合、攻撃者が簡単にセッションを乗っ取れる	・なりすまし
過度な情報漏えい	人為的な要因などにより、必要以上の情報が表示されている	・他の攻撃手法のヒント、または情報漏洩
不適切なエラー処理	予期しないステータスコードや詳細なエラーメッセージなどにより、必要以上の情報が表示されている	・他の攻撃手法のヒント、または情報漏洩
サービス運用妨害	意図的にサーバーに負荷をかけるDos攻撃など、サービスを妨げる行為	・サービスの遅延、一時停止
セキュリティ設定の不備	セキュリティが未設定や初期設定のままの状態	・不正アクセス、マルウェア
ファイルおよびディレクトリの漏えい	アクセスを許可されていない権限のアカウントでもファイルやディレクトリにアクセスできる	・情報漏洩
脆弱性を含む製品の使用	これまでに脆弱性が発見された製品、バージョンを使用している	・情報漏洩、踏み台