Vexトレーニングテキスト

基本マスターコース

目次

Version 0

1. Vexについて

まずはVexについて覚えておきましょう。

1-1. Webアプリケーション検査

Webアプリケーション検査には、様々な方法があります。

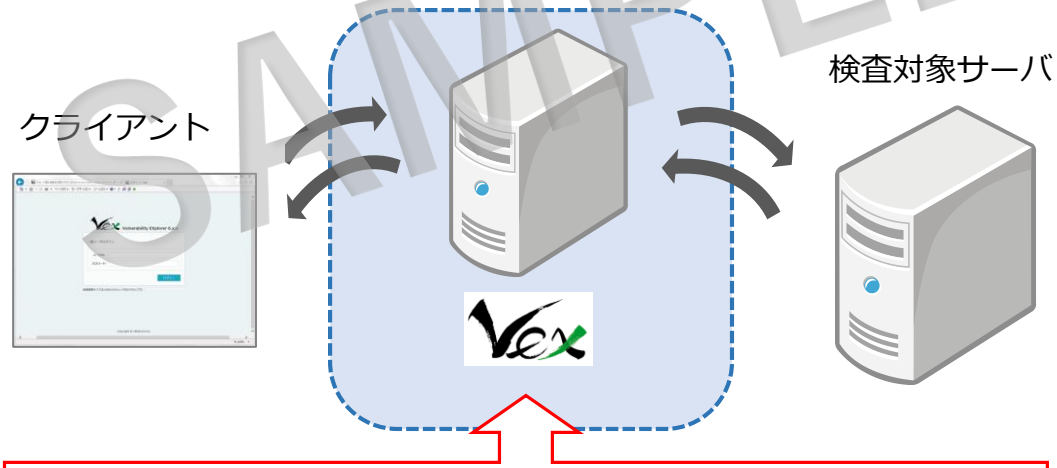
SAST
Static Application Security Testing

DAST
Dynamic Application Security Testing

IAST
Interactive Application Security Testing

VexはDASTツールに入ります

Vex検査のイメージ



Vexがクライアントと検査対象サーバの中間にプロキシサーバとして位置し、
通信をプロキシログとして記録します。
また、記録されたHTTPリクエストに疑似的な攻撃パターンを含めて検査対象アプリに送信し、
その際のHTTPレスポンスを解析し、脆弱性の有無を確認します。

Check

DASTは検査パターンを送信した際のWebサーバの挙動から
脆弱性を判断するため、アプリケーションの開発言語や
Webサーバの種類や構成に影響されないで検査が可能です。

2. 検査前の準備

Vexを利用する前に、クライアント側の設定を確認しましょう。

2-1. 利用可能なブラウザ

Vexを操作する際のブラウザとして、以下をサポートしています。

- Internet Explorer 11
- Firefox 最新版

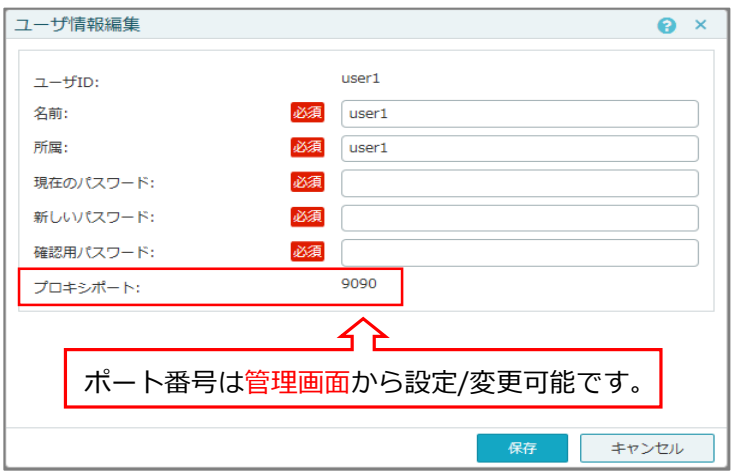
Check 検査対象サイトを操作するクライアントブラウザに関しては、プロキシ設定が可能であれば、特に制限はありません。

2-2. ブラウザのプロキシ設定

Vexにプロキシログを記録するために必要な設定をします。

手順

(1) Vexにログイン後、画面右上の「ユーザ名」のプルダウンメニュー「ユーザ情報編集」画面から、ログインしたユーザに紐づいたプロキシポート番号を確認します。



3. 基本的な検査の進め方

Vexを利用した基本的な検査の進め方を確認します。

手順① 検査プロジェクトの作成

プロジェクトには、検査対象のプロキシログ情報、
検査設定、検査結果ログ、レポート情報などが
保管されます。

Webアプリケーション検査

手順② Web検査実施

手順③ Web検査結果の確認

正しく検査が実施されたかの確認、また、脆弱性を検出した場合に
検出結果の精査を実施します。

Server検査

手順④ Server検査実施

Webサーバの設定不備による脆弱性の検査を実施します。
Server検査には、下記の２つが提供されています。

1. Server File検査
2. Server Settings検査

手順⑤ Server検査結果の確認

正しく検査が実施されたかの確認、また、脆弱性を検出した場合に
検出結果の精査を実施します。

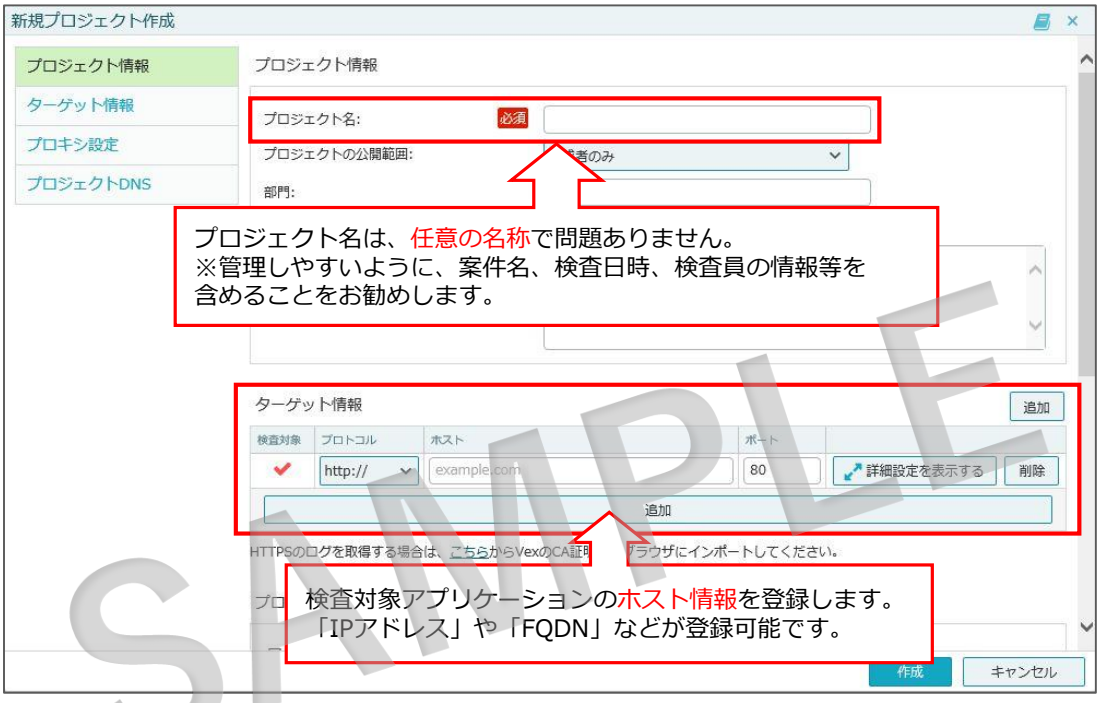
手順⑥ レポート出力

報告対象者やポリシーに沿って、検出結果のレポートを出力します。

4. 検査プロジェクトの作成

プロジェクト作成画面上にて、検査対象サイトの情報や通信時の詳細設定が可能です。

4-1. プロジェクト作成画面



Check

検査対象サイトがHTTP(ポート:80)とHTTPS (ポート:443)が混在する場合や
画像ファイルやCSSファイル等を外部サイトから読み込んでいる場合は、
ターゲットを「追加」して、全てのホスト情報を登録してください。

注目

「ターゲット情報」に登録されているホストのみ、
Vexがアクセスを許可します。
登録されていないホストへの通信は、Vexが遮断しますので、
必要な情報は全て登録してください。
ただし、登録する必要があっても、検査対象ではない場合は「検査対象」のチェックを外してください。

5. 3つの検査手法

Vexには、3種類の検査手法があります。

それぞれの検査手法により、プロキシログの取得方法や検査設定の方法が選べます。

サイトの性質や規模、また検査スキルや検査にかけられる工数等により使い分けることが可能です。

Case1
サイト巡回（ログの取得）も検査設定も全て自動で、簡易的に検査したい。

Case2
サイト巡回は手動で行うが、検査設定はある程度、自動的に済ませたい。

Case3
サイト巡回も、検査設定も全て手動で行いたい。

1. 自動巡回 本コース

簡単な設定をするだけで、自動的に、Webサイトの巡回、画面遷移図の作成、および検査設定までを実行します。

サイト規模が非常に大きいWebアプリケーションの場合、巡回にかかる工数を大幅に節約することが可能です。
ただし、複雑な構造のWebサイトでは、対応できない場合があります。

★検査に向いているシステム
・大規模なECサイト
・HTMLで作成された企業サイト
・検索サイト 等

2. 画面遷移図 本コース

検査対象サイトを手動で巡回し、サイトの構造を画面遷移図により再現します。

検査シナリオを作成しながら、検査の設定が出来るので、初めての方から上級者まで使いやすい検査手法です。
自動設定に手動設定を組み合わせることで、幅広い範囲のWebサイトに対応することが可能です。

★検査に向いているシステム
・小～中規模なECサイト
・ログイン認証のある会員サイト
・検索サイト 等

3. Handler

1つ1つの検査対象全てに対して、詳細な検査設定をすることが可能なため、多様なWebサイトに対応可能な検査手法です。

慣れないうちは、設定に手間が多少かかりますが、一度使いこなせば、幅広いWebサイトの検査にも対応でき、検査時間を短縮することも可能です。

★検査に向いているシステム
・オンラインバンキング
・人事、給与などのBtoBサイト
・Ajax、json、API 等