vex
Vulnerability Explorer

クイックスタート

VEX (Vulnerability Explorer)

UBsecure Inc. 2021-02-25

Version. 9.1.0.0

目次

1. はじめに

本書では、Vulnerability Explorer（以下Vex）でのWebアプリケーションを検査してレポートを出力するまでの簡単な検査の流れを紹介します。

説明は、弊社提供の検証用アプリケーションを検査するものとして記載しています。

アプリケーションに応じて適宜読み替えを行ってください。

(検出される検査総数などの数値や検出した脆弱性は、Vexのバージョンにより変更となる可能性があります。)

なお、本書内の表記ルールは以下の通りとなります。

✓Check!
□検査時における注意点、また確認していただきたい点などを記載します。

MEMO
・補足的な説明や、参考情報などを記載します。

1.1. 本書の位置付け

Vexに関連する基本的なマニュアルは以下の通りです。

No	マニュアル名	目的	提供形式
1	セットアップマニュアル	Vexを新規インストール、またはバージョンアップする方法	PDF
2	**クイックスタート**	**Vexのインストール後から、検査準備～検査実行までの基本的な操作方法**	**HTML**
3	ユーザガイド	各画面、および機能の詳細な説明 ※GUI上の本のアイコンをクリックする事でご利用可能です。	HTML
4	FAQ トラブルシュート Handlerガイド	よくある質問・トラブル・Handlerの設定方法に対する回答 ※GUI上の「？」アイコンをクリックする事でご利用可能です。 FAQサイト	ウィジェット 外部サイト
5	Vex-CLIガイド	Vexをコマンドライン上から操作する方法	PDF

※Vexのバージョンにより含まれるマニュアルが異なることがあります。

2. 検査を始める前に

Vex （Vulnerability Explorer）はWebアプリケーションのセキュリティ検査のツールです。
VexではWebアプリケーション検査、Server検査の実施機能を提供しています。

2.1. 検査項目

Vexでは、以下の検査を実現します。

検査カテゴリ	参考情報
SQLインジェクション	https://cwe.mitre.org/data/definitions/89.html
OSコマンドインジェクション	https://cwe.mitre.org/data/definitions/78.html
リモートコード実行	https://cwe.mitre.org/data/definitions/94.html
オープンリダイレクト	https://cwe.mitre.org/data/definitions/601.html
HTTPヘッダインジェクション	https://cwe.mitre.org/data/definitions/93.html
SSIインジェクション	https://cwe.mitre.org/data/definitions/97.html
XPathインジェクション	https://cwe.mitre.org/data/definitions/91.html
LDAPインジェクション	https://cwe.mitre.org/data/definitions/90.html
XML外部実体参照	https://cwe.mitre.org/data/definitions/611.html
安全でないデシリアライゼーション	https://cwe.mitre.org/data/definitions/502.html
ディレクトリトラバーサル	https://cwe.mitre.org/data/definitions/23.html
クロスサイトスクリプティング	https://cwe.mitre.org/data/definitions/79.html
クロスサイトリクエストフォージェリ	https://cwe.mitre.org/data/definitions/352.html
平文通信	https://cwe.mitre.org/data/definitions/319.html
セッションフィクセーション	https://cwe.mitre.org/data/definitions/384.html
セッション管理不備	https://cwe.mitre.org/data/definitions/1018.html
過度な情報漏えい	https://cwe.mitre.org/data/definitions/200.html
不適切なエラー処理	https://cwe.mitre.org/data/definitions/728.html
サービス運用妨害	https://cwe.mitre.org/data/definitions/400.html
セキュリティ設定の不備	https://cwe.mitre.org/data/definitions/731.html
ファイルおよびディレクトリの漏えい	https://cwe.mitre.org/data/definitions/538.html
脆弱性を含む製品の使用	https://cwe.mitre.org/data/definitions/1035.html
不適切なアクセス制御	https://cwe.mitre.org/data/definitions/284.html
NoSQLインジェクション	https://cwe.mitre.org/data/definitions/943.html

以下のような**複雑なWebアプリケーションの検査**も可能です。

・認証の通過を必要とする機能（ログイン後の会員専用メニューなど）
・重複チェックが存在するデータ登録機能（新規登録など）
・ データの削除機能
・パスワード変更機能
・画面遷移を管理しているサイト
・データ登録機能に対して、入力値が完了画面に表示されず、別画面で参照されるような作りのサイト

※画像認証であるCAPTCHAや、ソフトウェアキーボード、乱数表を利用した認証などの人の知覚を要する機能や、HTTPおよびHTTPS以外の通信手段を要する機能は検査を実施できません。

2.2. 検査における注意事項

Vexで検査を実施する上で、**注意事項**を以下に示します。

1. 検査対象の指定を誤ると、指定されたサイトへの攻撃とみなされる可能性があります。
2. 検査対象サーバやネットワークに負荷がかかります。
3. 擬似攻撃で検査対象システムが不安定となる可能性があります。
4. 検査対象によっては、データの書き込み、または削除が発生します。
   ※利用前にデータバックアップを取得してください。
5. Webサーバへの大量のアクセスが発生するため、大量のログが記録されます。
6. レポート、ログには、検査対象システムの重要情報が含まれます。
   ※取り扱いに注意してください。

2.3. Webアプリケーション検査におけるシステム構成

2.3.1. [1] Vexを利用するシステム構成イメージ

Vexで検査をする際の基本的なシステム構成は下記の通りです。

No	システム名	説明
1	クライアントPC	VexサーバにアクセスしてVexの操作を行うPC
2	Vexサーバ	Vexがインストールされたサーバ
3	検査対象サーバ	検査対象のWebアプリケーションが存在するWebサーバ
4	Vex操作用のブラウザ	クライアントPCでVexの操作を行うブラウザ
5	検査対象アプリケーション操作用のブラウザ	クライアントPCで検査対象サーバにアクセスして、Webアプリケーションの操作を行うブラウザ

MEMO

- クライアントPCから、Vexサーバ経由で検査対象サーバにアクセスすることで、VexにHTTPリクエスト/レスポンスを記録します。

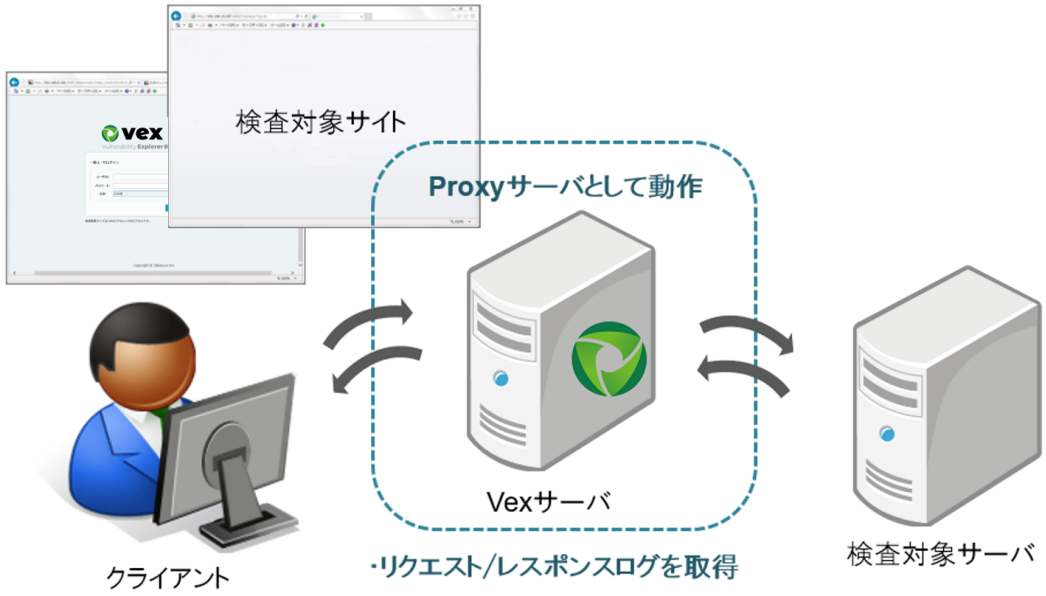
・上記の図ではクライアントPCとVexサーバを異なる端末としておりますが、同一端末にて構成することも可能です。
　なお、同一端末にて構成した場合においても、本マニュアル内の内容を読み替える必要はありません。

2.3.2. [2] Vexの動作

Vexは大きく分けて以下の4つの動作を行います。

- **① プロキシサーバとして動作（プロキシログ記録時）**

  検査対象となるWebアプリケーションの情報を記録する際にプロキシサーバとして動作します。利用者は、Vexがインストールされているサーバをブラウザのプロキシ設定に指定した上でWebアプリケーションにアクセスします。

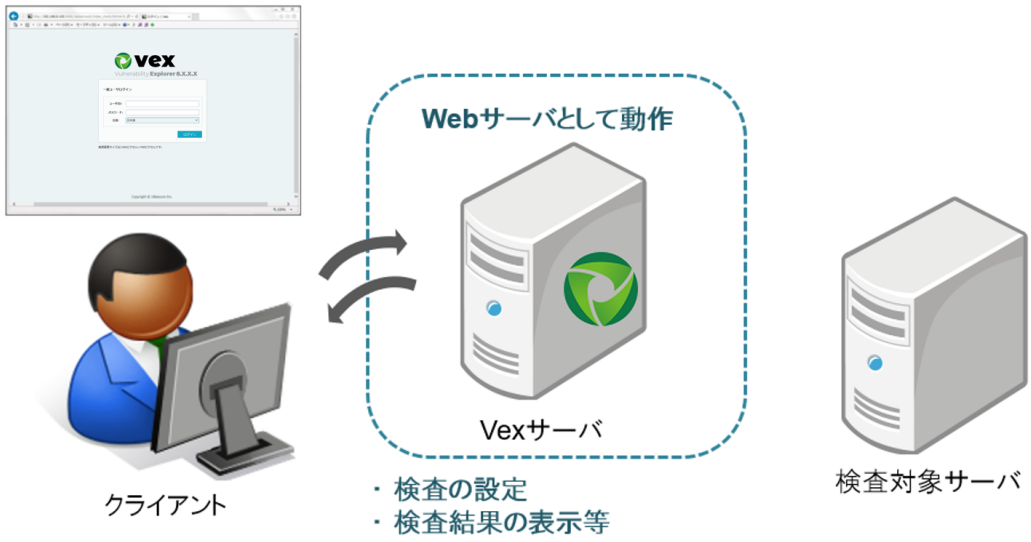


- **② 巡回サーバとして動作（巡回ログ記録時）**

  自動巡回を利用する際には、設定された情報に基づき、検査対象となるページを自動で抽出する巡回サーバとして動作します。

- **③ Webサーバとして動作（検査設定時、検査結果参照時）**

  記録された検査対象となるWebアプリケーションの情報を設定する際にWebサーバとして動作します。利用者は、本ツールがインストールされているサーバへブラウザからアクセスします。



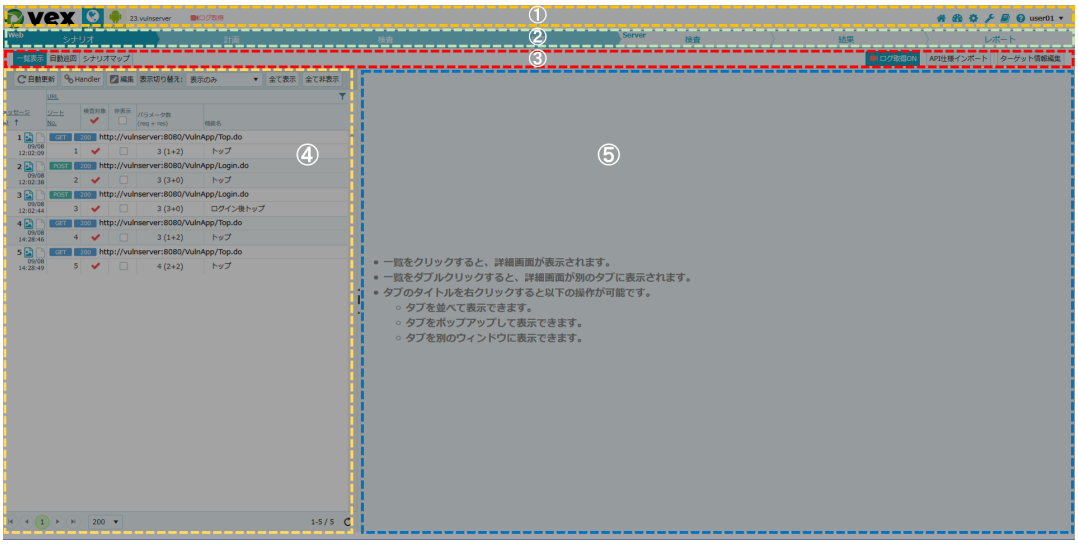
- **④ 検査サーバとして動作（検査実施時）**

  検査を実施する際には、設定された情報に基づき、自動的に検査リクエストを送信する検査サーバとして動作します。

2.4. Vexの画面構成

Vexの操作画面の構成要素を確認します。

以降の説明にあたり、画面の各部に関して、以下の名称を使用します。



No	システム名	説明	含まれる主な項目
1	ヘッダ	プロジェクト全体に 共通のメニュー	「プロジェクト一覧」「ダッシュボード」等
2	フローバー	検査フローに沿った ウィザードメニュー	Web「シナリオ」「計画」「検査」等
3	ツールバー	各検査フローに関連する機能を 表示	Web「シナリオ」選択時は、「自動巡回」 「画面遷移図」等
4	左ペイン	分割された画面の左側	ログ一覧や検査結果一覧等
5	右ペイン	分割された画面の右側	ログ詳細や脆弱性詳細等

MEMO
・上記の例では、2分割されている画面のため、「左ペイン」「右ペイン」としておりますが、 画面により、3分割される場合があります。

3. 検査準備設定

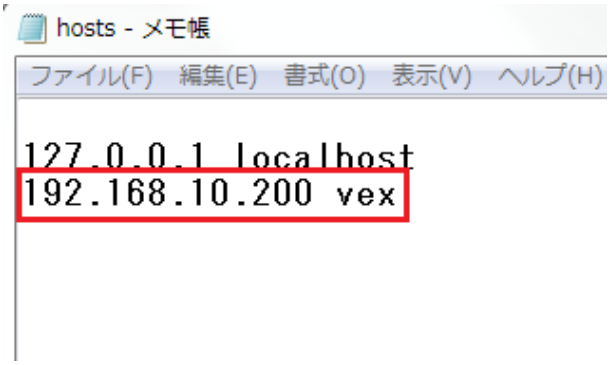
続けて、クライアント端末の設定について説明します。
本書では、VexサーバのIPアドレスを「**192.168.10.200**」と想定して記載しています。
※IPアドレスは、環境に伴って適宜読み替えを行ってください。

3.1. 動作環境

クライアントの動作環境は以下のとおりです。
・Internet Explorer 11
・Firefox 最新版

3.2. hostsファイルの編集

Vexを利用するクライアント端末のC:\WINDOWS\system32\drivers\etc\hostsファイルにVexサーバのIPアドレスとHost名を追加します。



IPアドレス	設定値
192.168.10.200 ※	vex

※Vexがインストールされたサーバの IPアドレスに置き換えて下さい。

MEMO
直接VexのIPアドレスへアクセスいただくことも可能ですが、本書では変更する場合の方法を記載いたします。

3.3. ブラウザの設定

検査対象画面を操作した際に発生するHTTPリクエスト/レスポンスをVexに記録するため、**検査対象アプリケーション操作用のブラウザ** に対し、プロキシ設定を行います。

3.3.1. [1] プロキシポート番号の確認

Vexユーザに紐づくプロキシポートを確認します。

1. クライアントのVex操作用ブラウザからログイン画面

   「http://vex:8080/Jabberwock/ 」へアクセスします。

2. 作成したユーザアカウントのIDとパスワードを入力してログインします。

3. ヘッダ右部のユーザ名のプルダウンメニューから「ユーザ情報編集」画面にアクセスします。

「プロキシポート」に表示されている番号を確認します。

本書では、Vexユーザのプロキシポートを「**9090**」※として説明いたします。

※実際にログインしたユーザに設定されたポート番号に置き換えて下さい。

MEMO

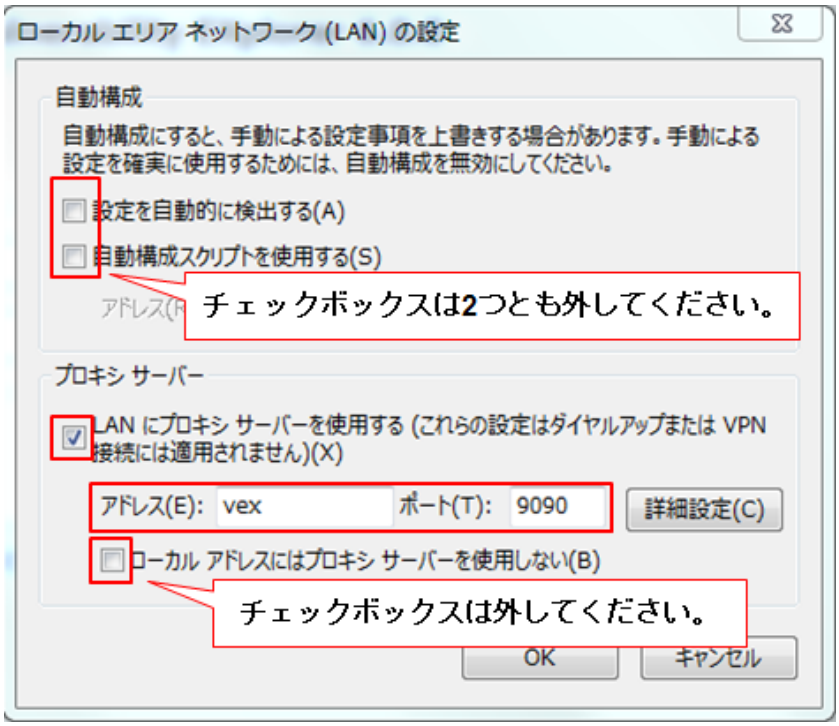
- ログインユーザにより、設定されているプロキシポート番号が異なります。
  Vexユーザを複数お持ちの場合は、それぞれの番号をご確認ください。
- ユーザアカウントの作成方法は、「セットアップマニュアル」の
  「ユーザライセンス（ユーザアカウント）の登録」を参照してください。

3.3.2. [2] プロキシ設定

ブラウザのプロキシ設定をVexに設定します。

IE11の場合、「ツール＞インターネットオプション＞接続＞LANの設定」からプロキシ設定を行います。
画面はVexのプロキシポートが「**9090**」※の場合です。

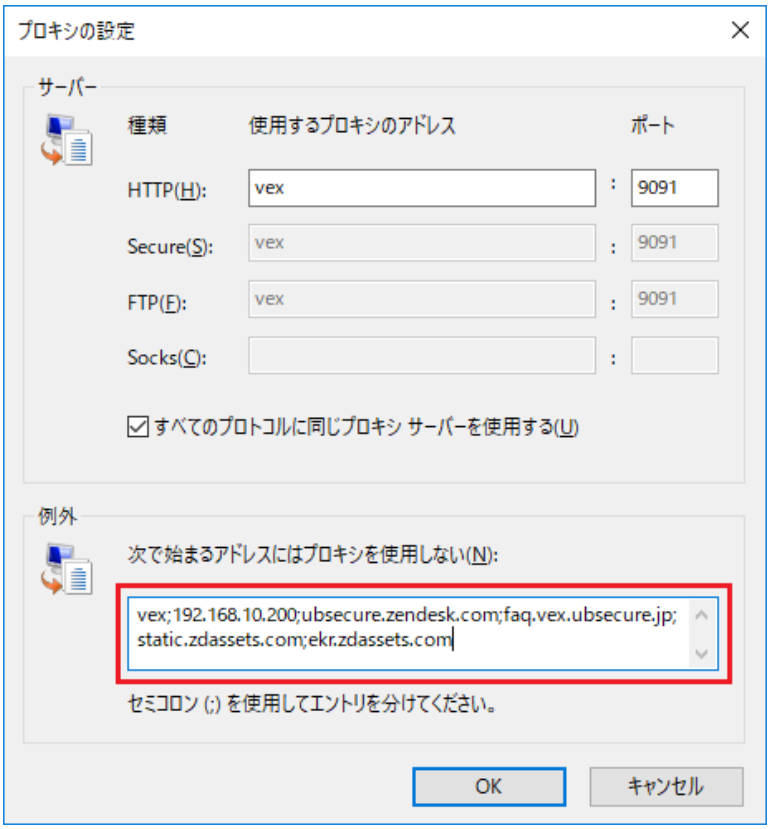
※実際にログインしたユーザに設定されたポート番号に置き換えて下さい。



3.3.3. [3] プロキシ除外設定

「詳細設定」ボタンをクリックし、プロキシの除外設定に以下を指定します。

「vex」：Vexサーバのhost名
「192.168.10.200」：VexサーバのIPアドレス※
「ubsecure.zendesk.com」：FAQ widget表示用
「faq.vex.ubsecure.jp」：FAQ widget表示用
「static.zdassets.com」：FAQ widget表示用
「ekr.zdassets.com」：FAQ widget表示用
※Vexがインストールされたサーバのipアドレスに置き換えて下さい。



3.4. CA証明書のインストール

検査対象サイトがHTTPSサイトの場合、操作ブラウザへVexが提供するCA証明書をインストールする必要があります。

3.4.1. [1] CA証明書のダウンロード

VexのCA証明書をダウンロードします。

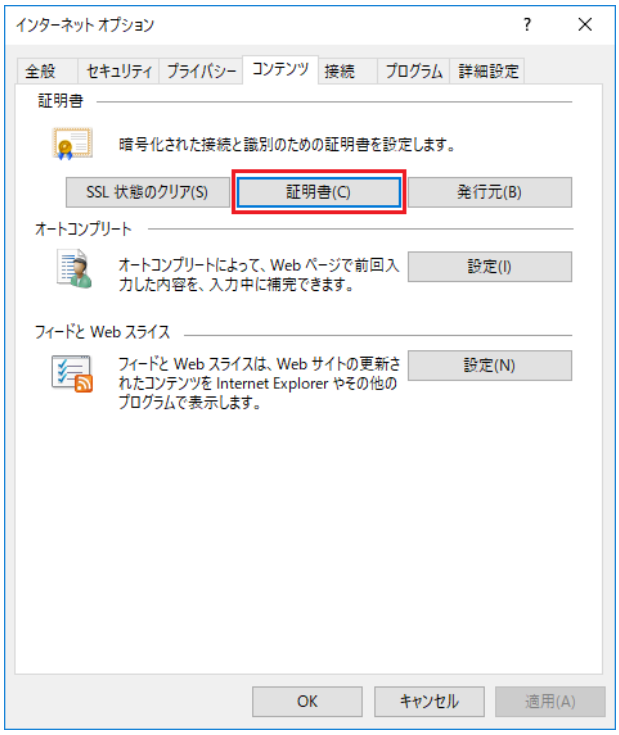
1. ヘッダ右部のユーザ名のプルダウンメニューから「Vex CA証明書」画面にアクセスします。

2. 「証明書ダウンロード」のリンクからCA証明書をダウンロードします。

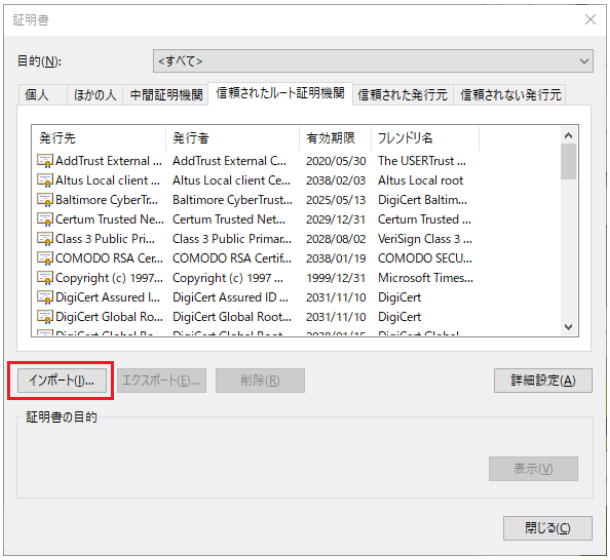
3.4.2. [2] CA証明書のインポート

VexのCA証明書を操作ブラウザへインポートします。

1. IE11の場合、「ツール＞インターネットオプション＞コンテンツ＞証明書」から証明書のインポートを行います。



2. 「信頼されたルート証明書機関」タブからインポートを選択し、VexのCA証明書をインポートします。



MEMO

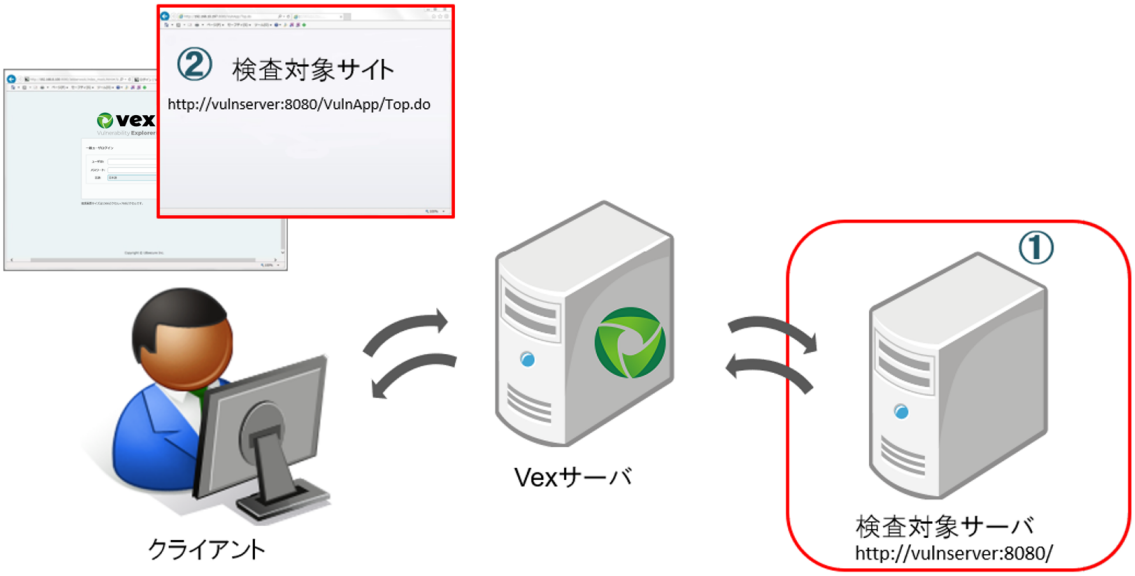
- Firefoxなど、他のブラウザを利用される場合は、同等の手順にてインストールを実施下さい。
- スマートフォン端末を使用する場合は、
  FAQサイトの記事「クライアント端末がスマートフォンの場合の設定」を参照して下さい。
- 検査対象サイトのHostがIPアドレスの場合、上記手順後も警告画面が表示される場合がございます。
  その際はセキュリティ例外の追加を行ってください。

4. 検査の流れ

4.1. 検査対象の確認

検査を実施する対象Webアプリケーションの情報を確認します。

本書では、検査対象ホスト「vulnserver」上のWebアプリケーションを検査するものとして説明します。



No	項目	内容 ※
1	検査対象ホスト名	vulnserver
2	検査対象サイトURL	\http//vulnserver:8080/VulnApp/Top.do

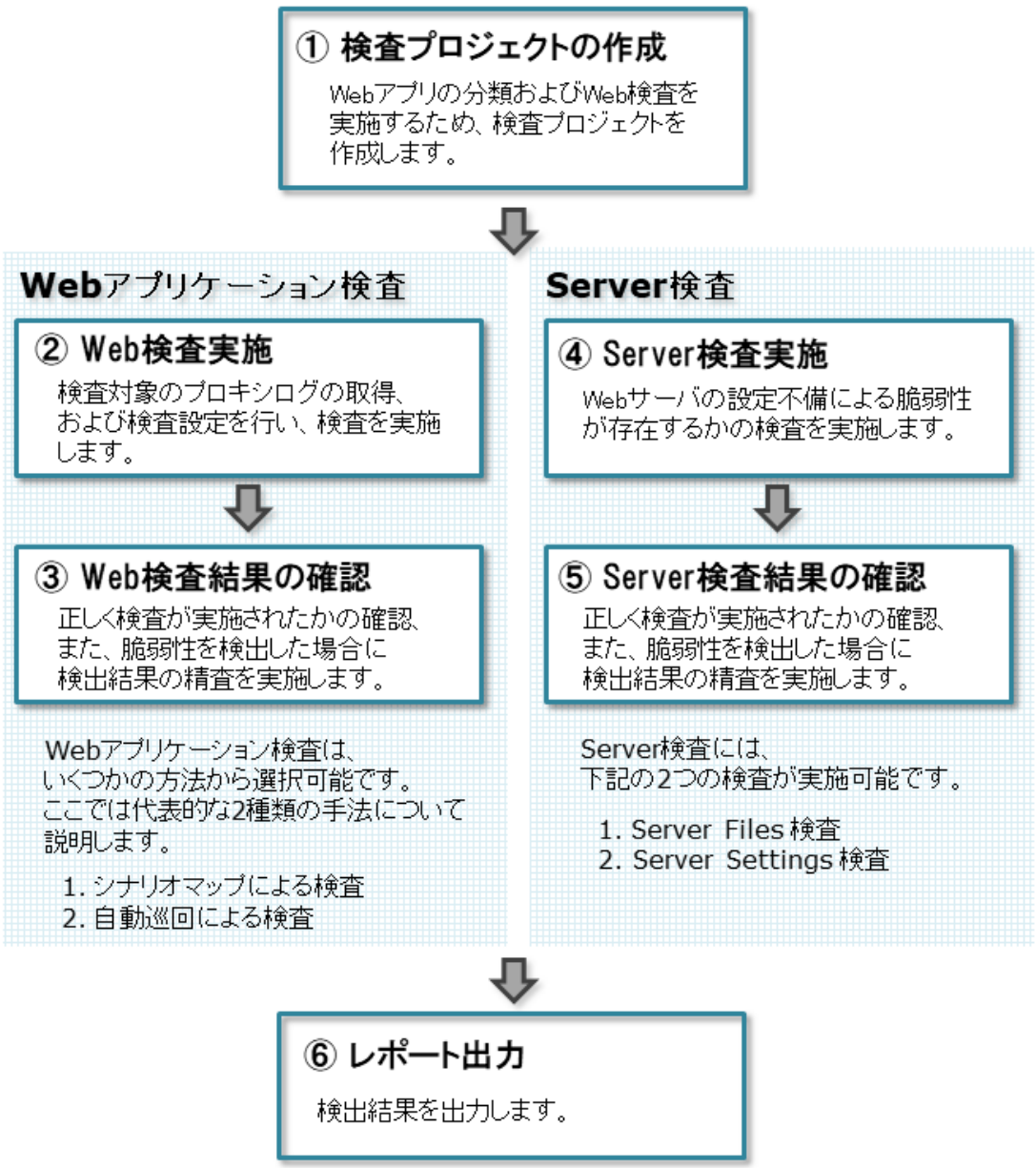
※環境に伴って適宜読み替えを行ってください。

✓Check!
□禁止項目（アクセス禁止の機能等）の有無を事前に確認をしてください。 □Basic認証やログイン認証等が存在する場合は、有効なアカウント情報をご準備ください。 □検査を開始すると大量のアクセスが発生するため、関係者様への連絡を行ってください。 □検査により、意図しないデータの登録、変更、削除が発生する可能性があります。 重要なデータは必ずバックアップを残してください。

4.2. Vex検査の進め方

基本的なWebアプリケーションの検査手順に関して説明します。

Vexは、Webアプリケーション、およびWebサーバの検査が可能です。



それでは、検査の流れに沿って、実際にVexを操作していきましょう。

4.2.1. 手順①検査プロジェクトの作成

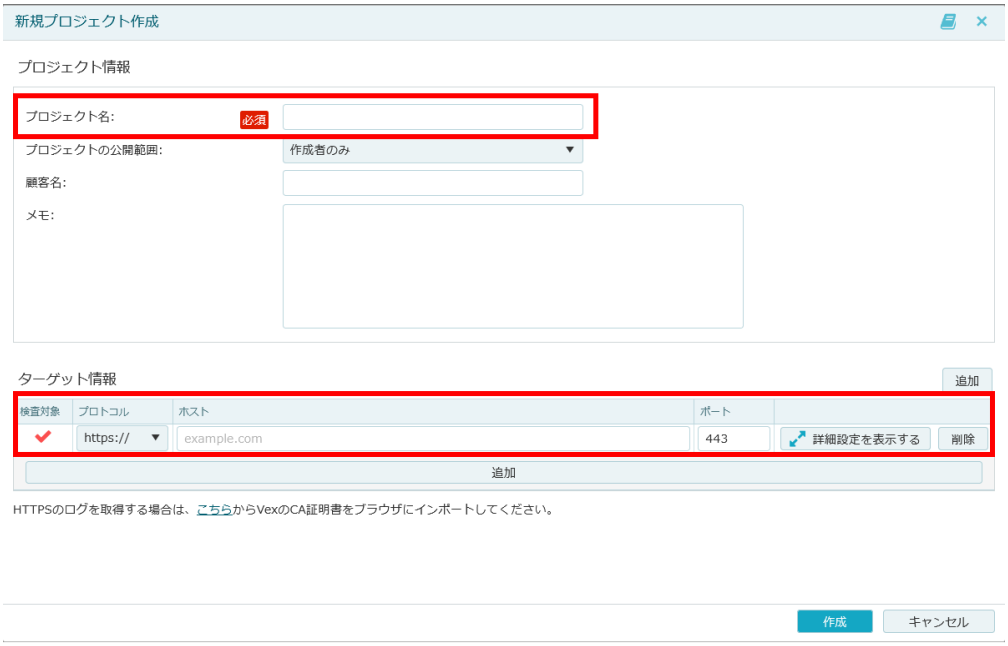
検査を始めるにあたり、まずは新しく検査プロジェクトを作成します。

1. クライアントのVex操作用ブラウザから、下記ログイン画面へアクセスします。

   「http://vex:8080/Jabberwock/」

2. 作成したユーザアカウントのIDとパスワードを入力してログインします。
3. 画面左上の「新規プロジェクト作成」ボタンからプロジェクト新規作成を行います。

4. 新規プロジェクトの作成画面で、任意の「プロジェクト名」、「ターゲット情報」を入力し実行ボタンをクリックします。



項目	説明
プロジェクト名	検証用サイトの名前を入力します。
ターゲット情報	検査を行う対象ホスト、または、検査を行う対象を巡回する際にアクセスする必要があるホストのプロトコル、ホスト名、ポート番号を入力します。 対象URLをホスト部分に入力することで、プロトコル、ホスト名、ポート番号を判別し自動入力します。 例）対象のURLがhttp://vulnserver:80/test/login.doの場合 プロトコル：http:// ホスト ：vulnserver ポート ：8080 ※上記は記載例です。実際の環境に合わせて変更してください。 ここで指定した対象の条件に一致するもののみ、プロキシログに記録、および検査を実行することが可能です。 検査対象ホストにはホスト名のみを指定してください。
追加ボタン	ターゲットの追加をします。 以下の場合、ターゲット情報の追加が必要です。 ・ アクセスする必要があるホストが複数存在する場合 ・ 検査対象にホスト http、https 両方が含まれる場合 ※画面の一番下の「作成」ボタンを押下するまで反映されません。

MEMO

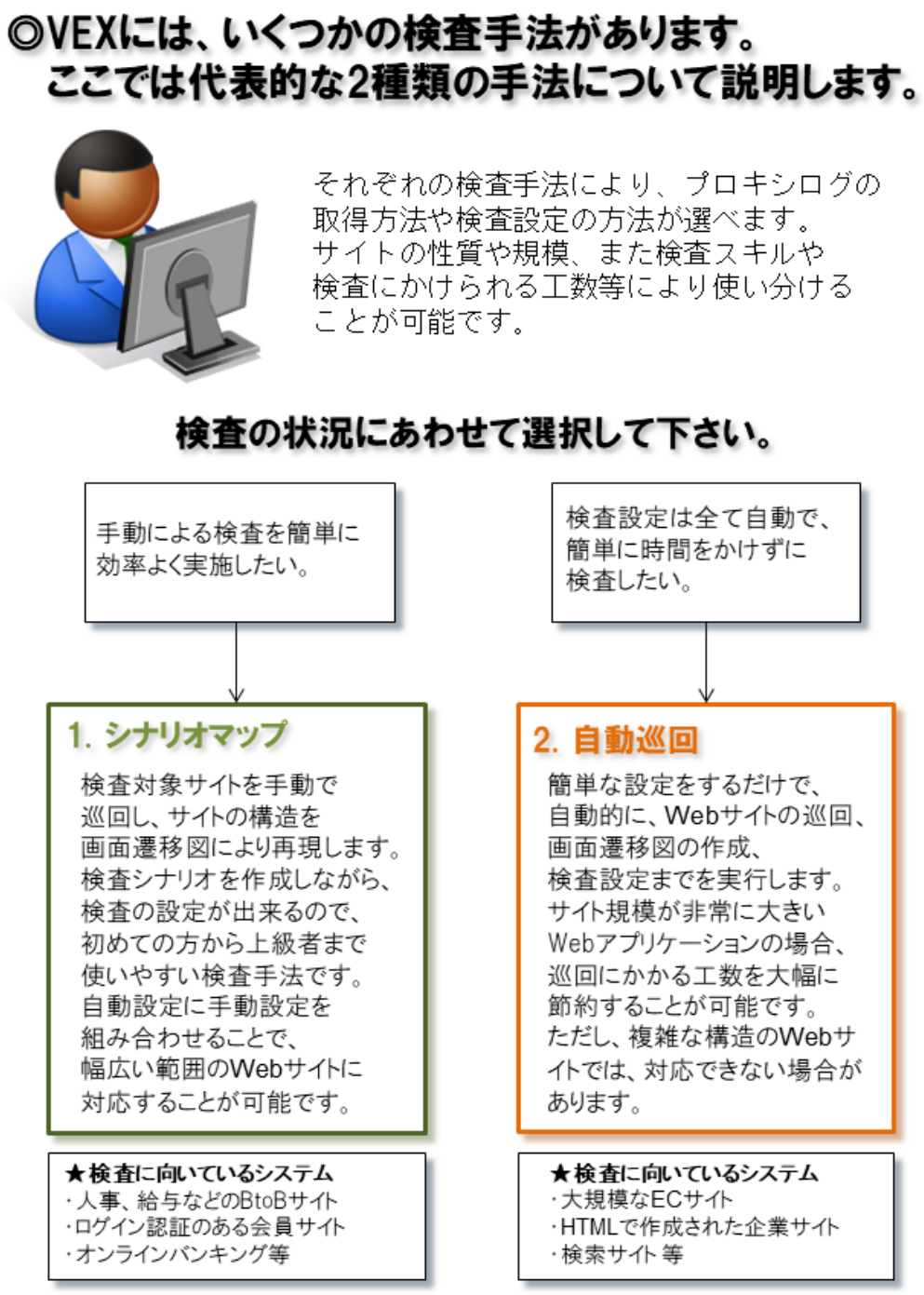
・Basic認証等が設定されている場合は、ターゲット情報の該当項目（「詳細設定」内）に入力してください。
※自動巡回を利用する場合に必要です。

・外部プロキシの設定や、DNSの設定も可能です。
ターゲット情報の各項目の内容については、「ユーザガイド」の「一般ユーザ画面」＞「プロジェクト一覧」＞「新規プロジェクト作成」＞「ターゲット情報」を参照してください。

5. プロジェクトが作成されます。

4.2.2. 手順② Web検査実施

Webアプリケーションの脆弱性検査を実施します。



詳細はシナリオマップによる検査へ 詳細は自動巡回による検査へ

ご利用される各検査手法の実施手順に進んでください。

4.2.2.1. シナリオマップによる検査

シナリオマップを使うと、ブラウザで検査対象へアクセスするだけで自動的に検査の設定（以下、検査シナリオ）を作成することができます。 自動的に作成された検査シナリオが不十分な場合でも、簡単にシナリオを修正することができます。

ここでは、VulnAppという架空のWebサイト対して検査をする例を用いて操作方法を説明します。

4.2.2.1.1. シナリオマップによる検査実施手順

シナリオマップによる検査は、以下の4ステップで実施します。

<STEP 1> シナリオマップ作成
<STEP 2> テスト送信
<STEP 3> 検査プラン作成
<STEP 4> 検査実施

4.2.2.1.2. <STEP 1> シナリオマップ作成

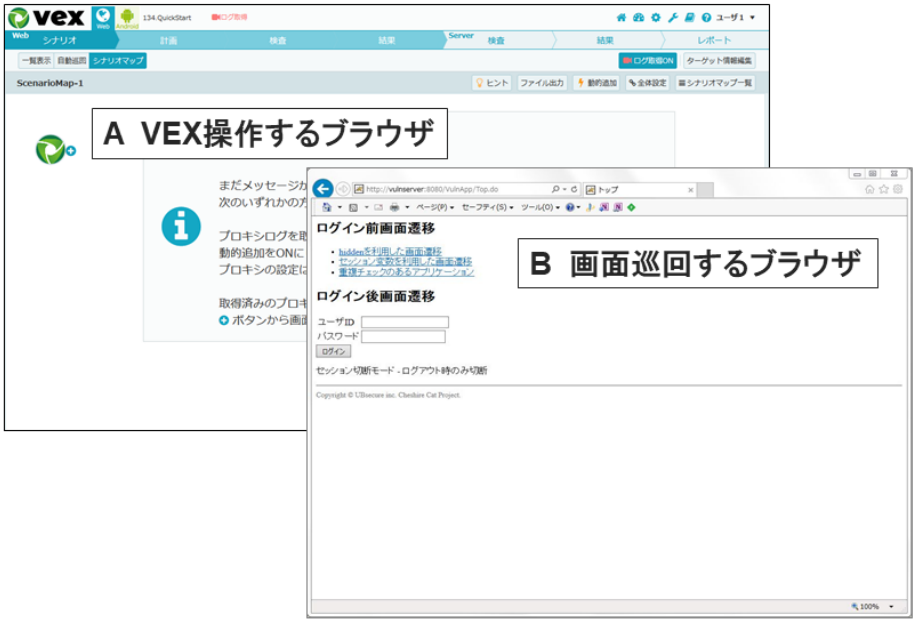
1．フローバーの「Webシナリオ」＞「シナリオマップ」をクリックします。

以下の画面が表示されます。

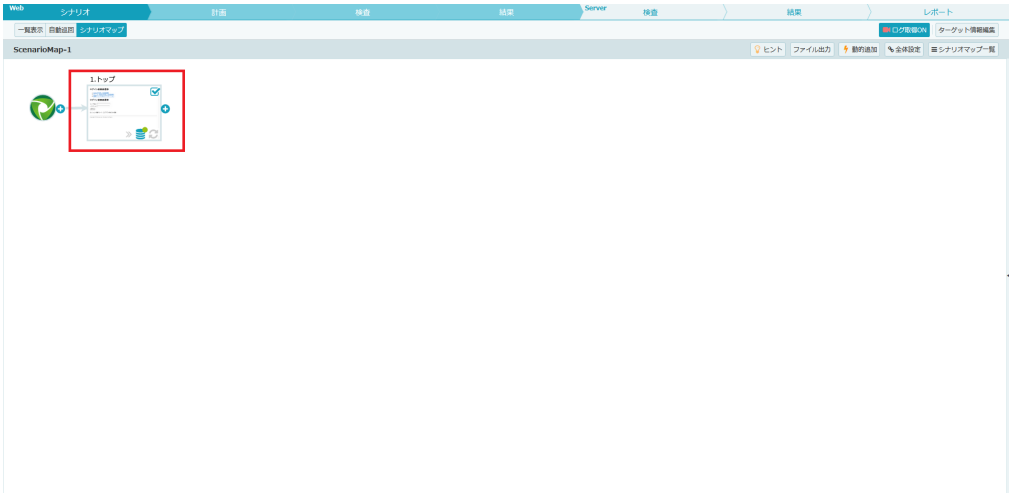
最初に、ツールバー右側に表示されているボタンが「ログ取得ON」の状態になっていることを確認してください。

次に、画面右側に表示されている下図のエリアより、「動的追加」ボタンがONになっていることを確認します。

2．Vex操作用のブラウザ（下記図Aのブラウザ）を立ち上げたまま、それとは別にもう1つブラウザ（下記図Bのブラウザ）を立ち上げます。 Bのブラウザにのみプロキシの設定を行い、VulnAppのトップページである「http://vulnserver:8080/VulnApp/Top.do」にアクセスします。



数秒待つと、シナリオマップにメッセージが下図のように追加されます。



3．Bのブラウザで引き続きVulnAppを操作し、メッセージを取得します。
例として「ログイン・問い合わせ入力・確認・完了」までの操作を行います。

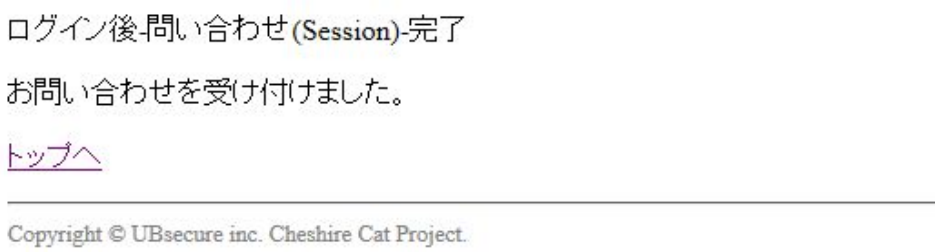
① **検査対象サイトの操作**：トップページよりログイン処理を実行する

② **検査対象サイトの操作**：「セッション変数を利用した画面遷移」にアクセスする

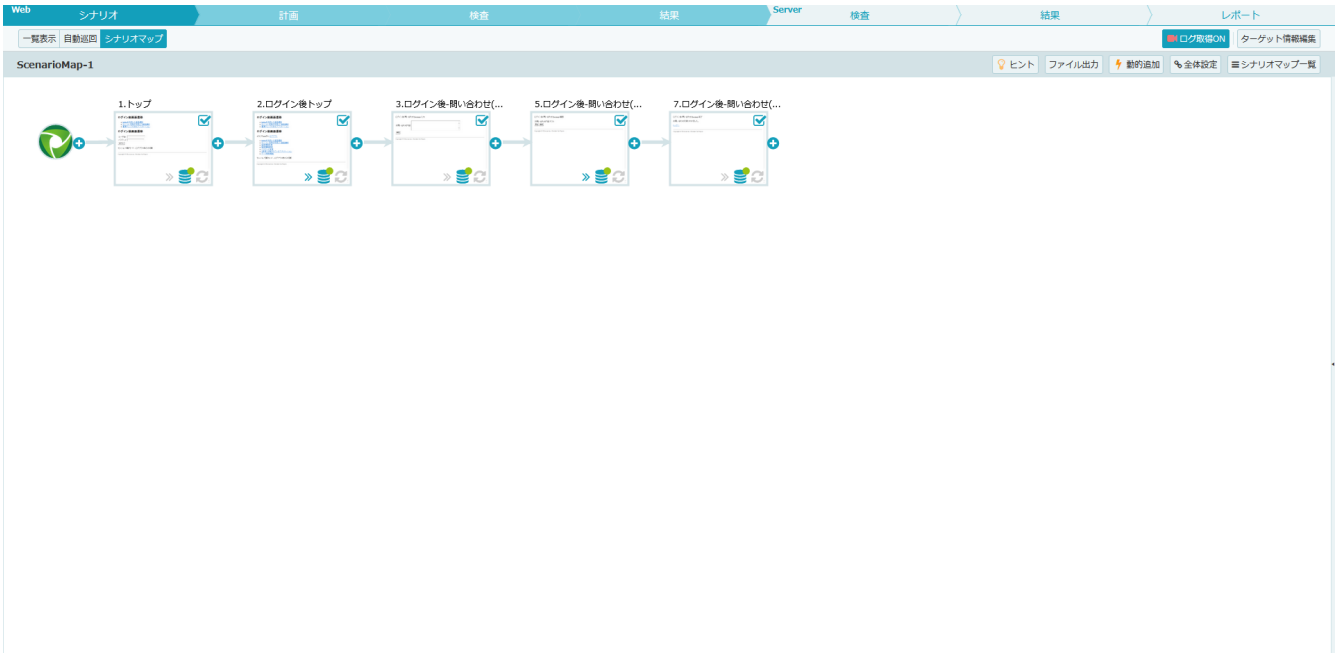
③ **検査対象サイトの操作**：必要項目を入力し、「確認」ボタンをクリックする

④ **検査対象サイトでの操作**：「登録」ボタンをクリックする

⑤ 検査対象サイトの完了画面が表示される



Aのブラウザにてシナリオマップ上にメッセージが追加されていることを確認してください。



✓Check!

□引き続きメッセージを追加する場合は、こまめにシナリオマップを確認し、メッセージが追加されていることを確認しながら行うことを推奨します。

□メッセージの追加が終わったら、「ログ取得ON」を「ログ取得OFF」に変更し、「動的追加」をOFFにしてください。
「ログ取得ON」と「動的追加」がONのままになっていると、意図しないメッセージが追加されてしまうことがあります。

MEMO

シナリオマップは1つのプロジェクトの中に複数作成することができます。
シナリオマップ一覧の「新規作成」ボタンから作成可能です。

4.2.2.1.3. <STEP 2> テスト送信

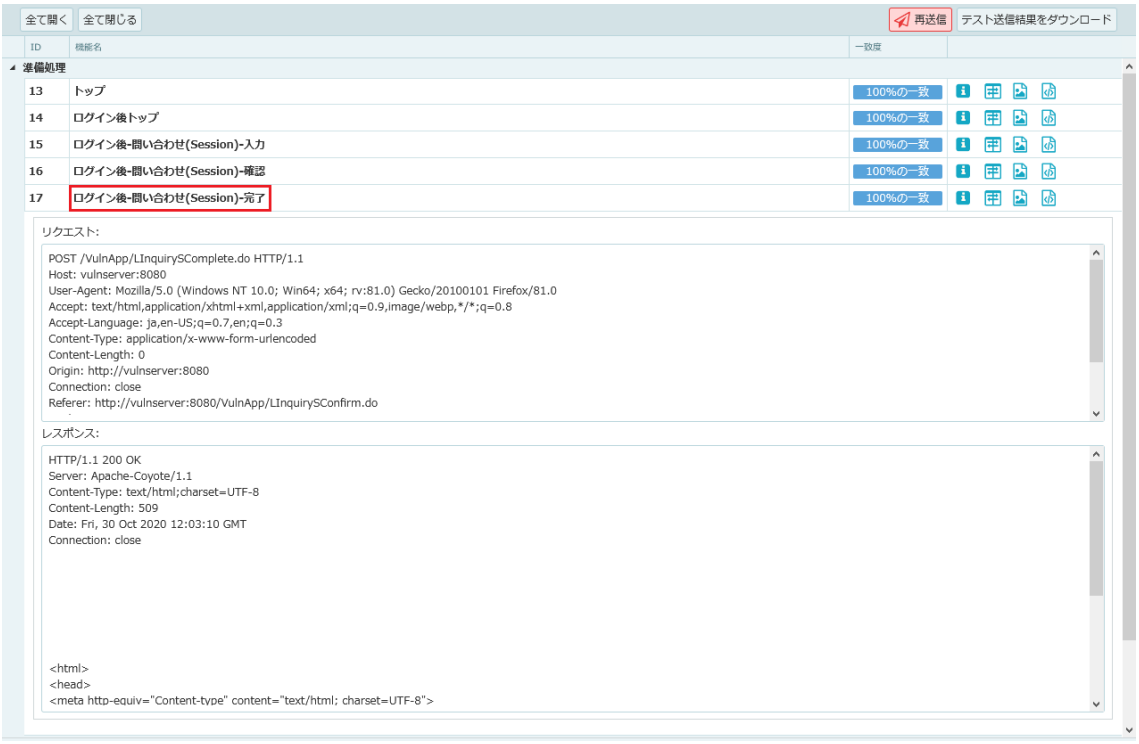
「テスト送信」を行うことによって、作成した検査シナリオが正しく作成されているかを確認することができます。 「テスト送信」では作成した検査シナリオに基づいて実際にリクエストを送信します。 送信結果を確認し、目的のメッセージまで到達できているかを確認してください。 手順は以下のとおりです。

1．テスト送信を実行したいメッセージの「テスト送信」アイコンをクリックします。

MEMO

・画面遷移の一番末尾に位置するメッセージのテスト送信を行うと、その遷移の先頭から末尾までの送信結果を確認できます。

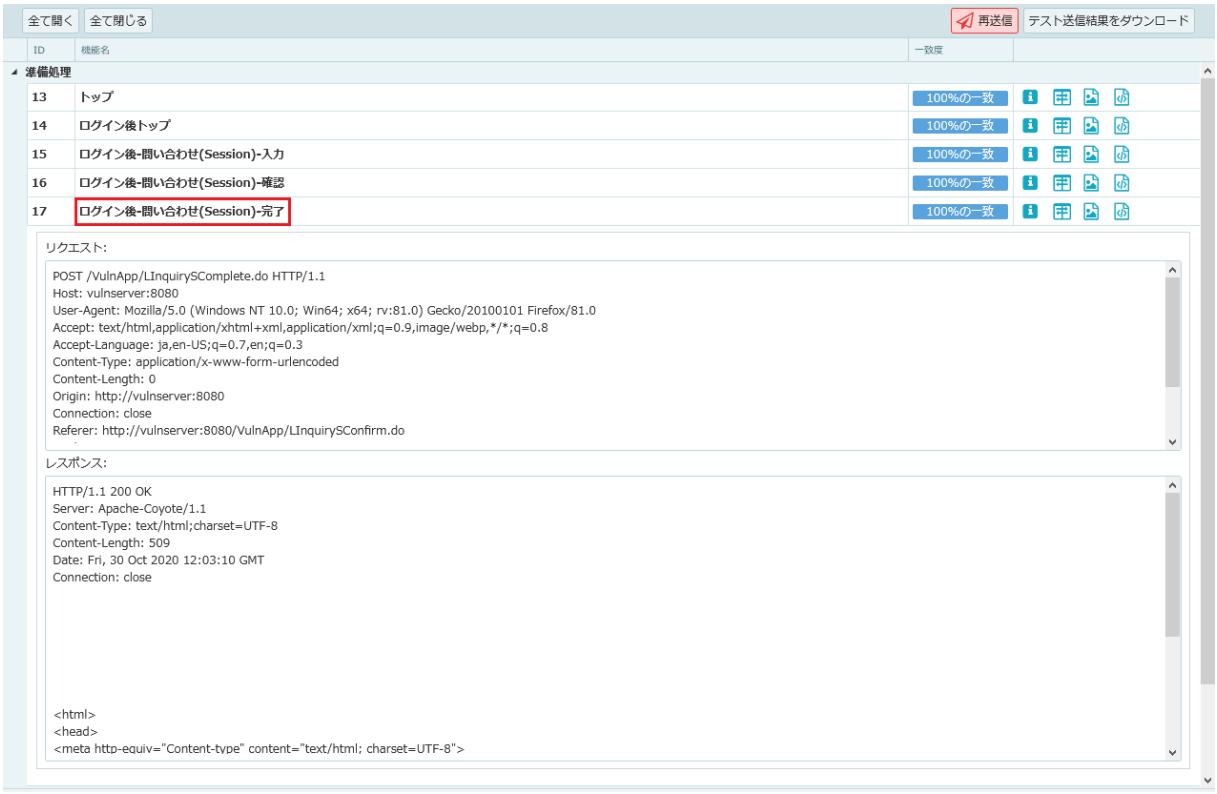
テスト送信の結果が右側に表示されます。



2．テスト送信結果を確認し、検査シナリオが正しく作成されていることを確認します。

テスト送信時に得られた画面がメッセージを記録した時の画面と同じ画面であれば正しく作成されていると判断します。 画面が同じ画面であることを判定するために、テスト送信結果画面では画面の「一致度」を使用します。 「一致度」は、記録されたメッセージのレスポンスと、テスト送信時のレスポンスがどれくらい一致しているかを表しています。

一致度が大きく減少している場合、元のメッセージと異なる動作をしている可能性があります。「機能名」をクリックすると表示されるメッセージ本文から目的の画面のHTMLが出力されていることを確認してください。

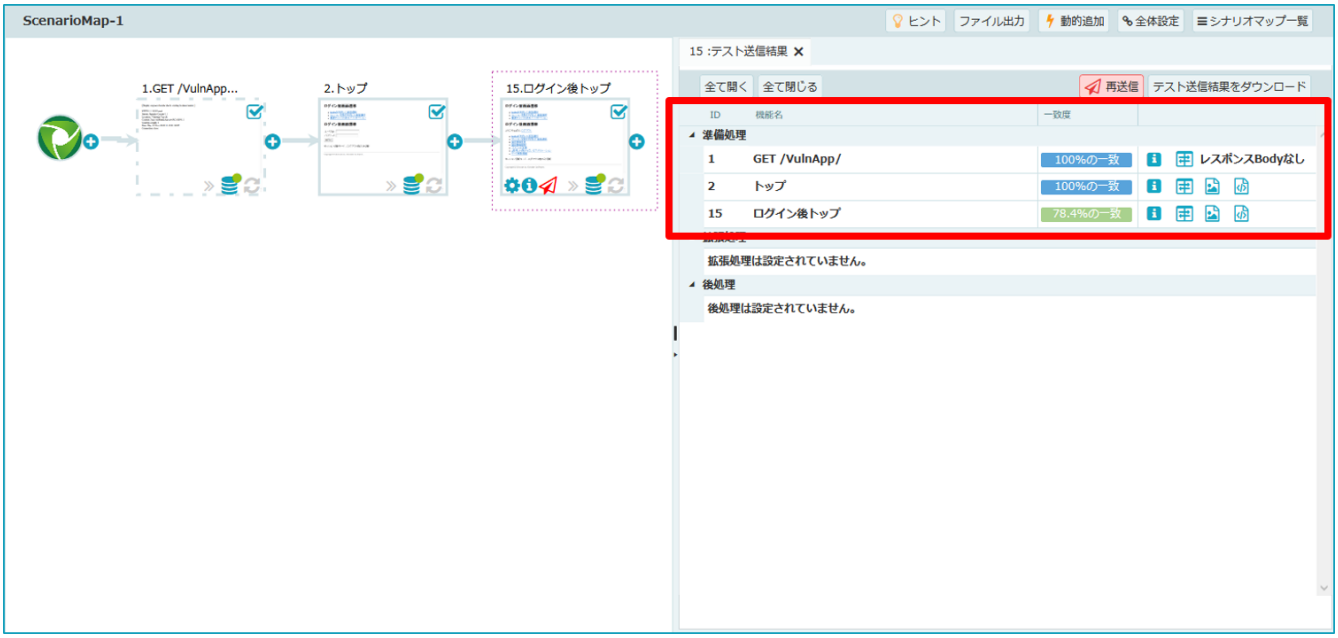


✓Check!
□一致度が高い場合でも異なる画面を示していていたり、一致度が低くても同一画面を示している場合があるので注意が必要です。 例1) 一致度が高い場合で異なる画面を示している。 ・ヘッダやフッタがある画面のように各画面に共通して表示している部分が画面の大半を占める場合 例2) 一致度が低い場合で同一画面を示している。 ・もともとのメッセージの行数が少ない場合 ・一覧画面のように、操作によってコンテンツの表示量が変わる画面の場合

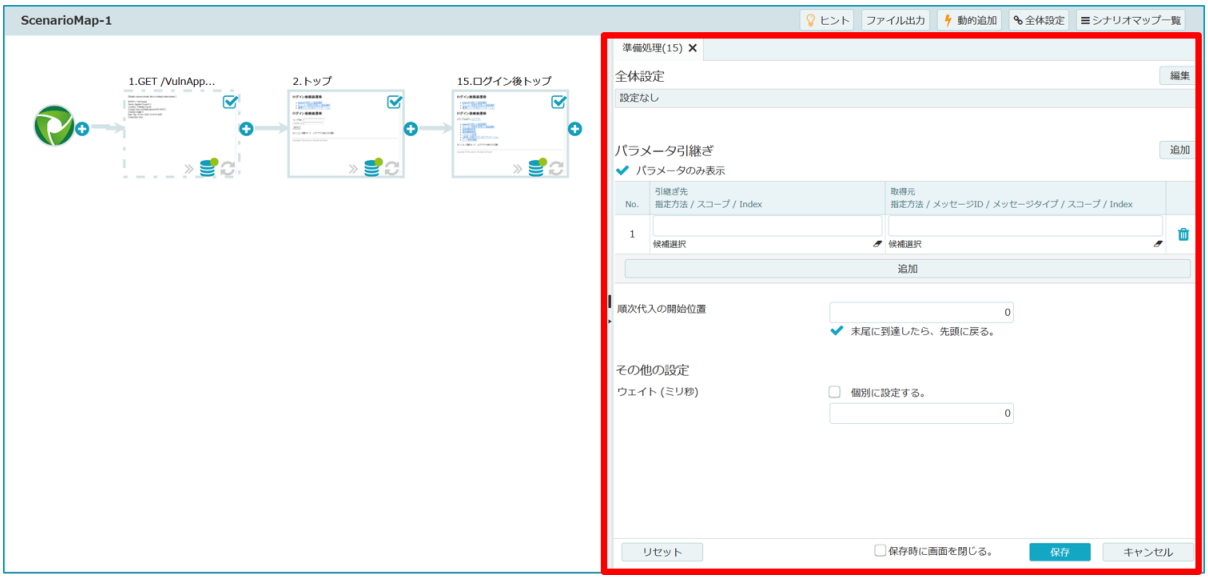
「一致度」の他にも画面の同一性を確認するための機能があります。
下記表を参照し目的に応じて活用してください。

No.	アイコン	機能	内容
1		詳細表示	テスト送信時のリクエスト、レスポンスの詳細情報を確認します。
2		レスポンスの差分	記録されたメッセージのレスポンスとテスト送信時のレスポンスの差分を表示します。
3		HTMLを表示	テスト送信時のレスポンスをブラウザで描画します。
4		ソースを表示	テスト送信時のHTMLソースを表示します。

3．テスト送信の一致度が低い場合はメッセージの「準備処理」アイコンをクリックし、準備処理の設定を編集します。



4.「準備処理」アイコンをクリックすると、画面右側に準備処理の設定画面が表示されます。



準備処理のパラメータ引継ぎを編集します。

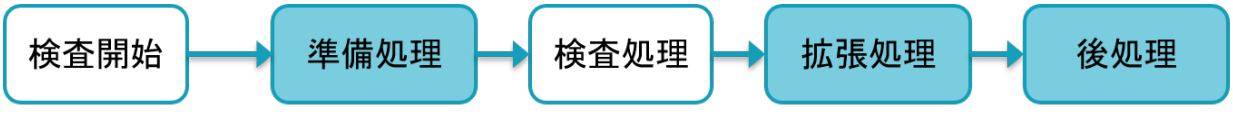
トークンなどの画面遷移の度に変化するパラメータをどのように引継ぐか設定し、正しい画面遷移を行うようにします。

設定項目	解説
引継ぎ先	リクエストとして、送信するパラメータを指定します。 2種類の方法で指定できます。 • ドロップダウンリストからパラメータの名前を選択する。 一覧に表示された中から引継ぎを行いたいパラメータを選択します。 • 正規表現を指定する。 正規表現を用いて、値の引継ぎ先を指定します。
取得元	引継ぎ先に設定する値をどのように取得するかを指定します。 5種類の方法で指定できます。 • ドロップダウンリストからパラメータの名前を選択する。 一覧に表示された中から値を取得したいパラメータを選択します。 • 正規表現を指定する。 正規表現を用いて、値の取得方法を指定します。 • 静的置換を指定する。 引継ぎ先の値に対して、常に同じ値を設定します。 • 順次代入を指定する。 あらかじめ用意した値の一覧を用いて、順に値を指定します。 • 自動的に設定する。 直前の画面のaタグやLocationヘッダなどを参照し、自動的に値を引き継ぎます。

MEMO

シナリオマップ上のメッセージに一律設定したい準備処理がある場合は、全体設定を活用することをお勧めします。
メッセージ一つ一つに同じ引継ぎを設定する必要がなくなり効率的です。画面右上の「全体設定」ボタンから設定可能です。

正確な検査を行うための機能として、準備処理の他に拡張処理・後処理という機能が提供されています。これらをまとめて「Handler」と呼びます。 検査中のHandlerの実行タイミングは、以下の図のようになります。



※準備処理・拡張処理・後処理は省略可能

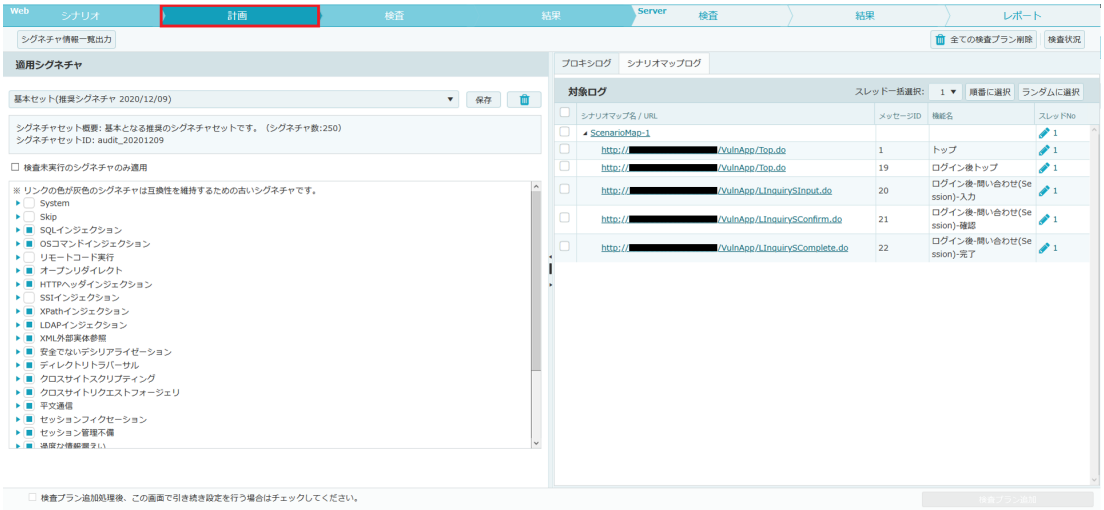
それぞれの処理の目的や設定が必要になる場面は下記表のとおりです。

No	Handler種類	解説
1	準備処理	検査対象のリクエストを再現するための処理です。 二重登録対策、CSRF対策が実装されているサイトではシナリオ作成時に取得したメッセージをそのまま送信するだけでは検査対象のリクエストを正しく再現できません。 以下のような機能を検査する場合に準備処理を行ってください。 • 画面遷移間にワンタイムトークン等の検査対象サイトが毎回新しく発行する値を持つパラメータを含んでいる
2	拡張処理	検査実行時に脆弱性の検出範囲を拡張する処理です。 検査の反応が出る画面は検査対象メッセージのレスポンスのみとは限りません。 検査対象メッセージの他に確認すべきメッセージを設定することで、下記のような検査を行うことができます。 • データ更新機能における更新結果が更新後画面に表示されず別の一覧画面に表示されるなど、情報入力機能と情報表示機能が別々に存在する
3	後処理	検査によって変更された内部データを元に戻す処理です。 例えばログイン機能のように、未ログインの状態から処理を行う必要がある場合、後処理にはログイン状態を戻す機能であるログアウトのメッセージを登録しておきます。 以下のような機能を検査する場合に後処理を行ってください。 • 二重ログイン禁止のサイト • パスワード変更機能の検査におけるパスワード復帰処理

4.2.2.1.4. <STEP 3> 検査プランの作成

検査設定が完了したら、検査プランを作成します。

1. フローバーの「Web計画」ボタンをクリックします。



MEMO
Web「計画」画面は、左右2つに分かれています。 左ペイン：「検査シグネチャ選択」 右ペイン：「検査対象選択」

1. 検査シグネチャを選択します。

※検査シグネチャは、Vexが検査に使用する検査パターンです。

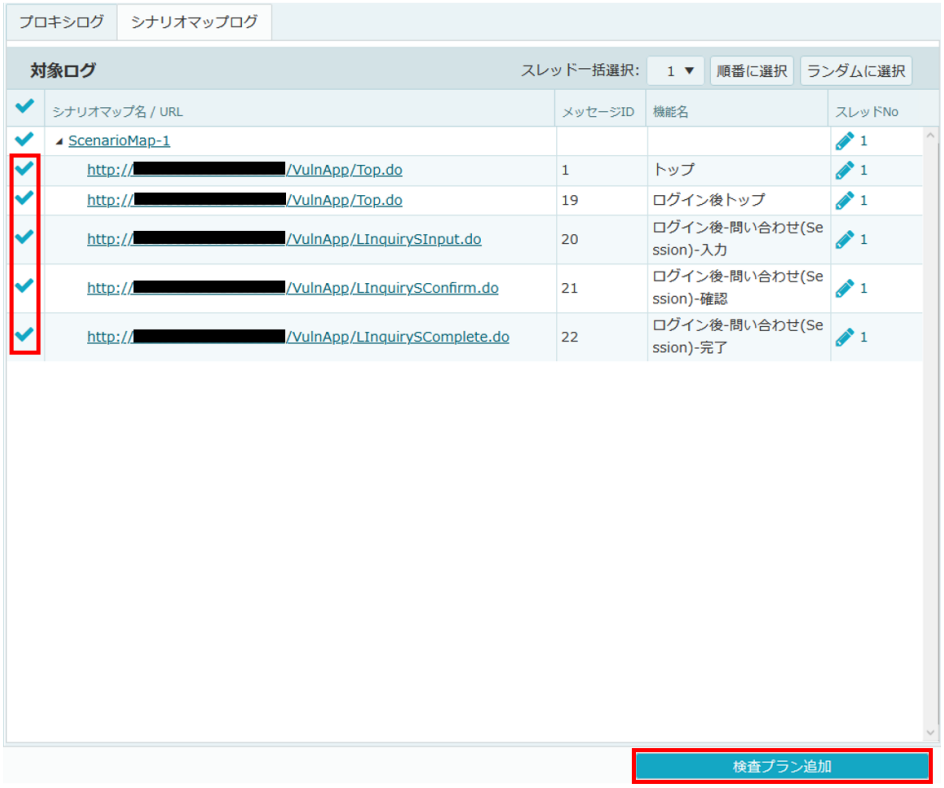
検査シグネチャには以下の3種類があります。

種類	説明
基本セット	推奨のシグネチャセットです。主要な脆弱性を検出するためのシグネチャが選択されています。
網羅用	比較的検出率の低い問題や、基本セットで検査している類似の問題に関しても検査を実施するシグネチャセットです。その為、同じ問題を重複して検出する可能性や、検査総時間が非常に膨大になる可能性があります。
速度重視	利用されていない可能性のあるパラメータを自動判別し、自動的に検査対象から外すことで、検査総時間を短縮するシグネチャセットです。

本書では、基本セット（推奨シグネチャ）を選択します。

1. 検査プランを作成します。

検査プランへ追加するメッセージを選択し、「検査プラン追加」ボタンをクリックします。



検査プランが登録されます。

MEMO

マルチスレッドの利用により検査スピードの向上が見込めますが、検査対象となるWebサイトによっては正しい検査が実施できなくなる可能性があります。

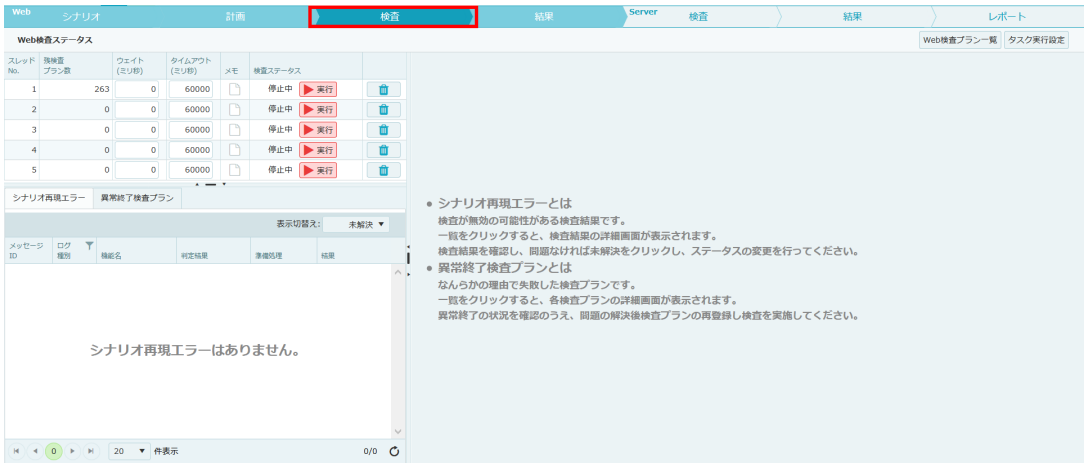
例えば、二重ログインの禁止制御がかかっているアプリケーションは、マルチスレッドを使用した検査に適しません。

また、会員情報の登録と変更など機能同士が干渉し合う部分を、スレッドにそれぞれ分けて検査を実施すると片方のスレッドが送信した検査内容が別のスレッドに影響を与えてしまうため、機能が干渉し合う処理への同時検査は行わないことを推奨します。

詳細は、ユーザガイドの「スレッド使用時の注意点（検査）」を参照してください。

4.2.2.1.5. <STEP 4> 検査実施

1. フローバーの「Web検査」ボタンをクリックします。



MEMO

Web「検査」画面は、大きく分けて3つに分かれています。
　左上ペイン：「検査ステータス」
　左下ペイン：「シナリオ再現エラー」および「異常終了検査プラン」
　右ペイン ：「Web検査進捗表示」

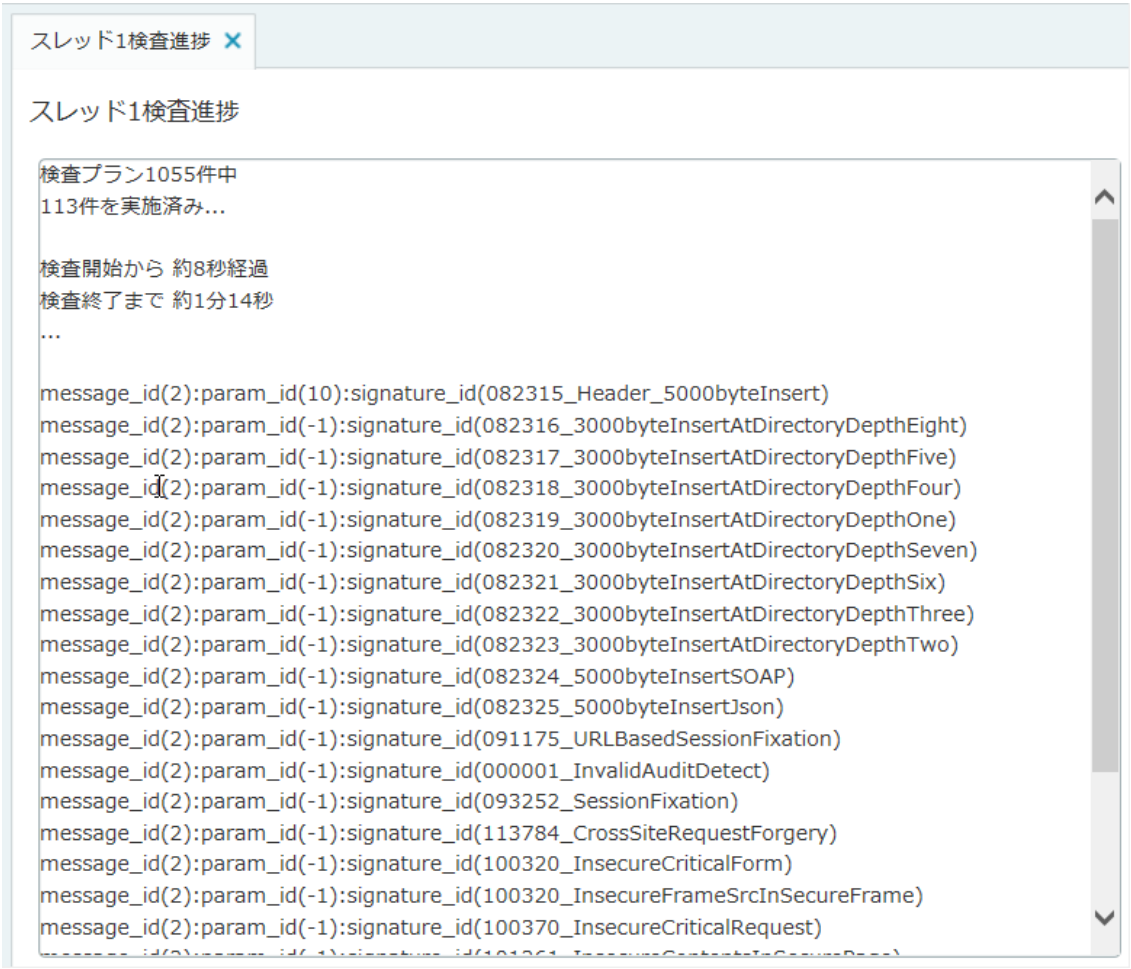
1. 検査プランが登録されているスレッドの「実行」ボタンより検査を開始します。

✓Check!

□検査を開始すると大量のアクセスが発生するため、関係者様への連絡を行ってください。
□検査により、意図しないデータの登録、変更、削除が発生する可能性があります。
重要なデータは必ずバックアップを残してください。

検査が開始されると、検査ステータスが「実行中」に変化します。

検査中のスレッドの行の上でクリックすると、右ペインに「Web検査進捗表示」が表示されます。



MEMO

・検査中にも、ログの取得やHandlerの作成などの他の機能を使用することが可能です。
・マルチスレッドの利用により、最大5つの検査を同時に実行出来ます。
・検査終了までの見込み時間は、サーバの稼働状況や準備処理の設定状況等により大きく変動する可能性があります。目安として参照してください。

画面中の各項目に関しては、下記の表をご確認ください。

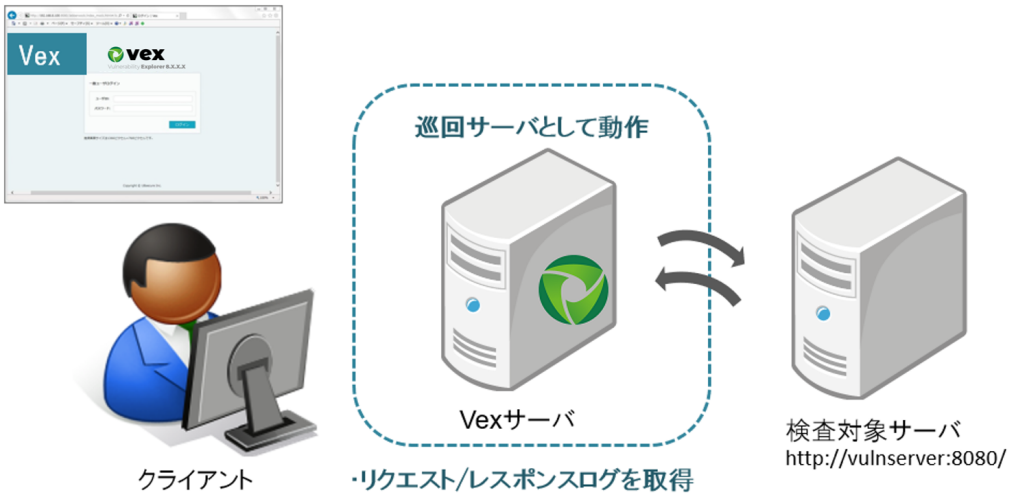
No.	項目	内容
1	スレッドNo	検査を実行する単位です。
2	残検査プラン数	登録されている検査プラン数が表示されます。
3	ウェイト	検査間隔をミリ秒単位で指定することが可能です。 Webサーバへの負荷を軽減したい場合などに使用します。 デフォルトは0ミリ秒が設定されています。
4	タイムアウト	検査時に検査サーバからのレスポンスを待つ最大時間です。 デフォルトは60000ミリ秒（1分）が設定されています。

「シナリオマップによる検査」は以上です。手順③「Web検査結果の確認」へ進んで下さい。

4.2.2.2. 自動巡回による検査

対象サイトに対し自動で巡回を行った結果から遷移図を作成し、作成された遷移図から検査対象確認や検査前設定を実施することが可能です。

本書では、下記の検査環境を例として、操作説明をいたします。



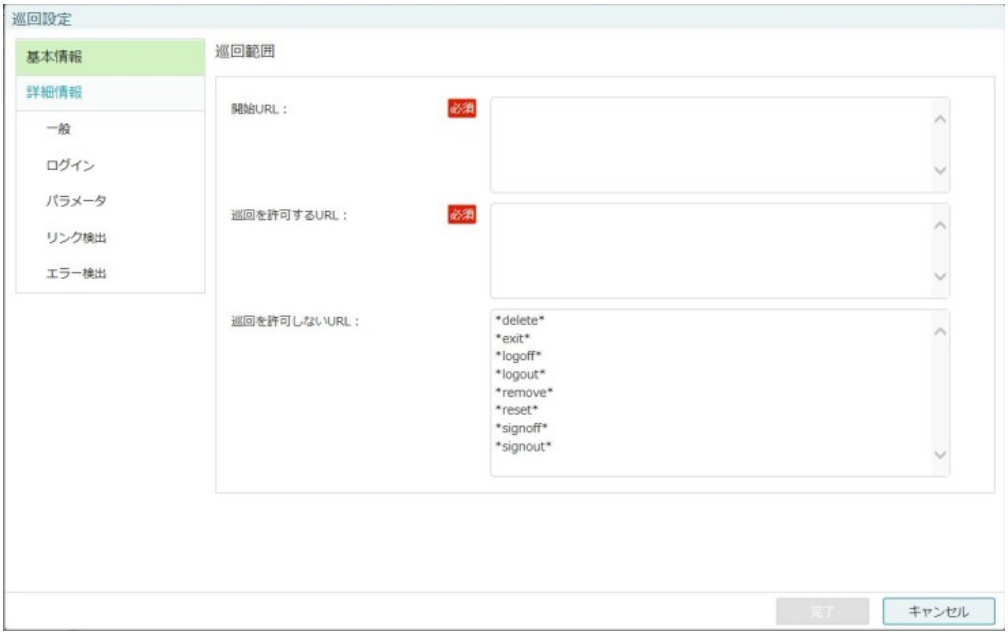
項目	内容 ※
検査対象ホスト名	vulnserver
巡回を開始するURL	http://vulnserver:8080/VulnApp/Top.do
巡回を実施する範囲	/VulnApp/ディレクトリの配下（サブディレクトリ含む）

※環境に伴って適宜読み替えを行ってください。

4.2.2.2.1. <STEP1> 巡回設定

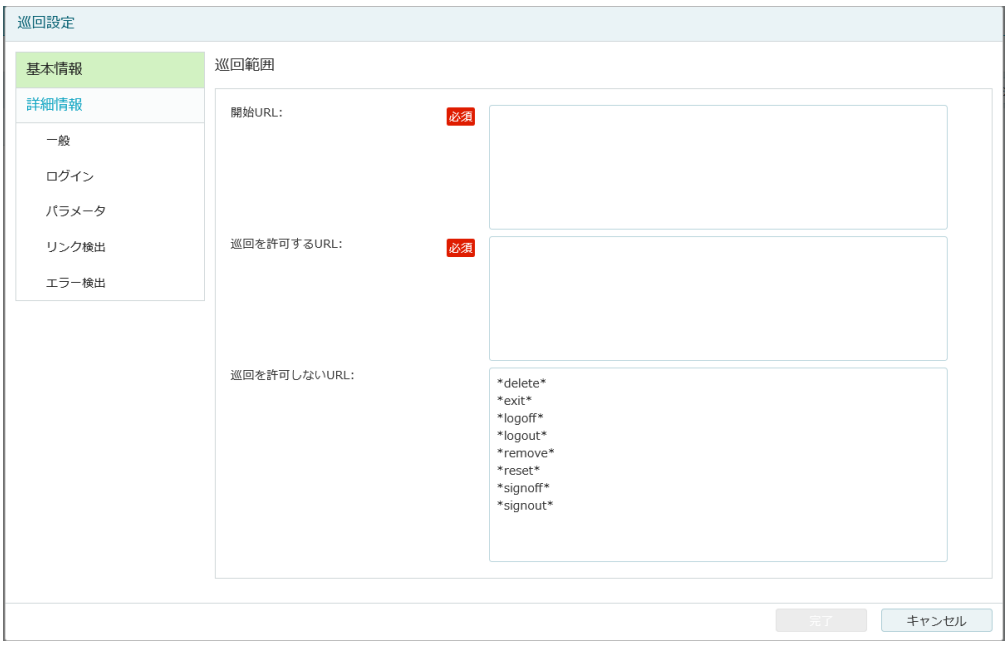
自動巡回を開始するには、まず巡回するための基本的な設定を行います。

1. フローバーのWeb「シナリオ」の「自動巡回」ボタンをクリックします。



2. 初めて自動巡回画面を開くと、「巡回設定」画面が表示されます。

   本画面で、自動巡回の基本設定を行います。

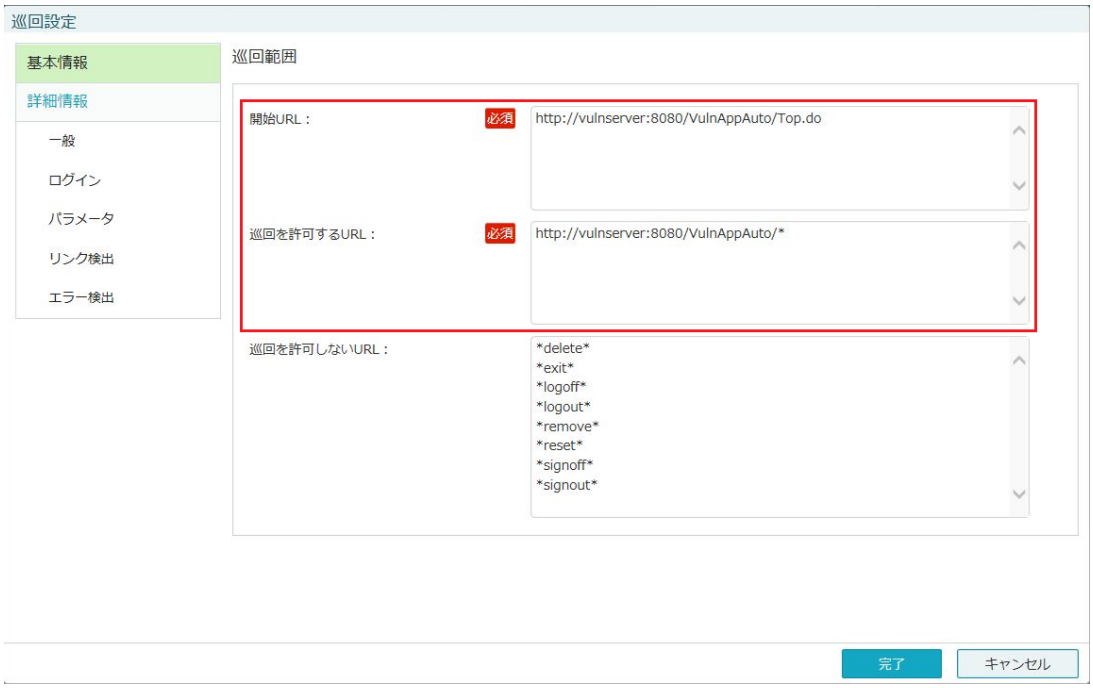


3. 巡回の開始点と巡回範囲を設定します。

「開始URL」には巡回の開始URLを入力し、「巡回を許可するURL」には巡回範囲を入力します。巡回範囲には、ワイルドカード（*）を用いて指定します。

MEMO

・複数のURLを巡回する場合は、それぞれのURLを改行で区切り指定してください。



各項目には、下記の入力値を入力します。

No	項目	入力値 ※
1	開始URL	http://vulnserver:8080/VulnAppAuto/Top.do
2	巡回を許可するURL	http://vulnserver:8080/VulnAppAuto/*

※環境に伴って適宜読み替えを行ってください。

✓Check!

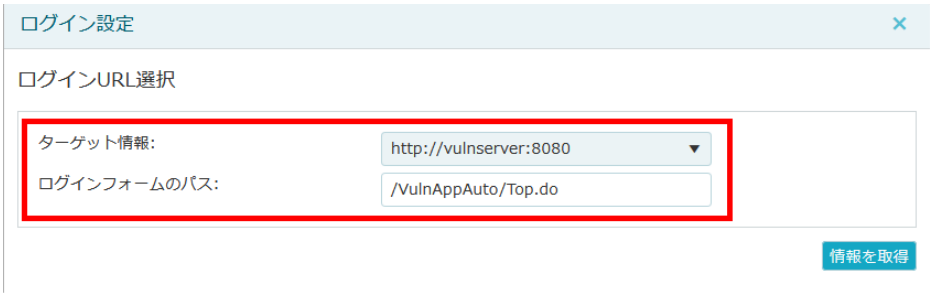
□[重要] 自動巡回は、本番環境では利用しないでください。
※設定内容に従い、Vexが自動でWebアクセスを行いますため、意図しないデータの登録や削除などが発生する可能性があります。

□「開始URL」はプロジェクトのターゲット情報に含まれている必要があります。
□「開始URL」は「巡回を許可するURL」に含まれている必要があります。
□アクセス禁止のURLが事前にわかる場合は、「巡回を許可しないURL」に設定してください。
□Basic認証等が設定されている場合は、事前にプロジェクト情報編集画面に登録してください。
□設定情報を変更する場合は、画面右上の「巡回設定」ボタンから再度編集出来ます。

4. 対象アプリケーションにログイン機能が存在する場合は、ログイン設定を行います。

「巡回設定 > 詳細情報 > ログイン」からログインの設定を開きます。

5. 「新規作成」ボタンをクリックし、「ログイン設定」画面を開きます。



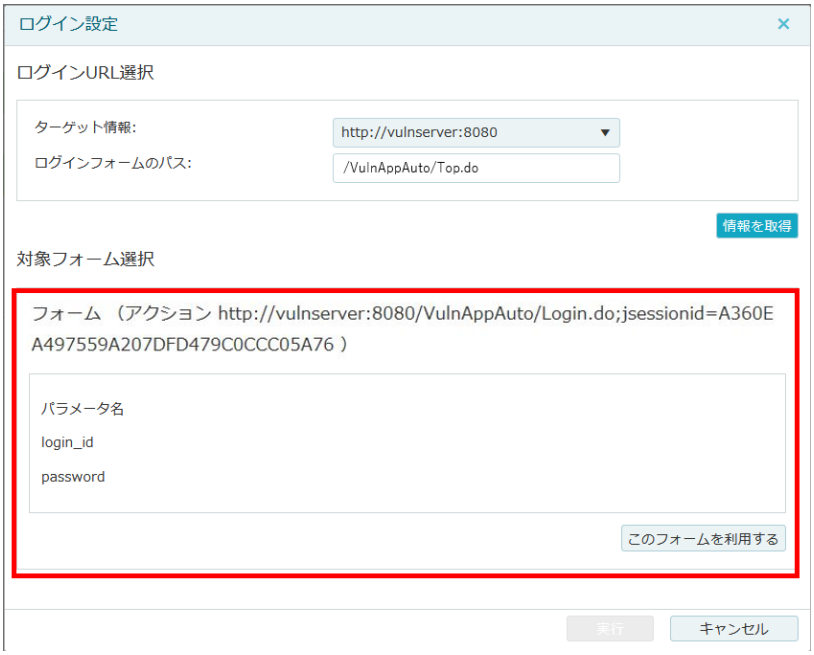
ターゲット情報を選択した後、「ログインフォームのパス」に「ログインID、パスワードを入力するフォームの存在するパス」を入力し、「情報を取得」ボタンを押します。

各項目には、下記の入力値を入力します。

No	項目	設定値 ※
1	ターゲット情報	http://vulnserver:8080
2	ログインフォームのパス	/VulnAppAuto/Top.do

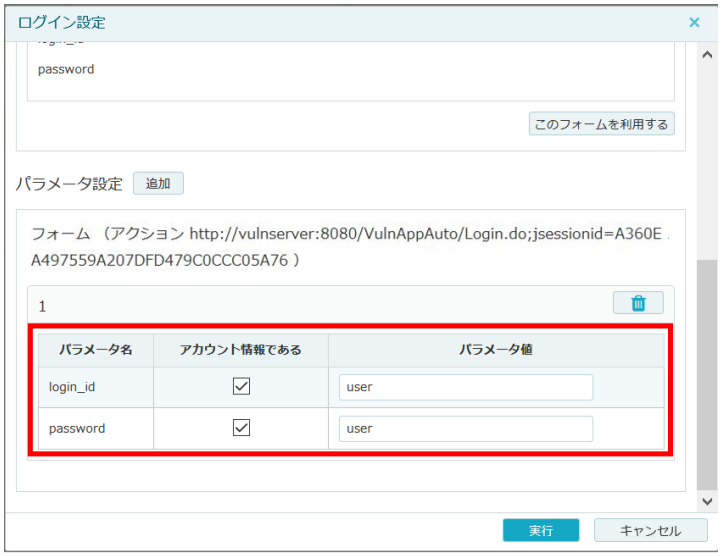
※環境に伴って適宜読み替えを行ってください。

6. 「情報を取得」ボタンを押すとVexから「ログインフォームのパス」にアクセスが発生し、指定パスに含まれるフォーム情報が取得されます。



使用するフォームの「このフォームを利用する」ボタンをクリックします。

7. 選択されたフォームに含まれるパラメータが表示されるので、パラメータ値にログインに必要な値を入力します。



各項目には、下記の入力値を入力します。

No	パラメータ名	パラメータ値 ※	備考
1	login_id	user	ログインIDを送信するパラメータ
2	password	user	パスワードを送信するパラメータ

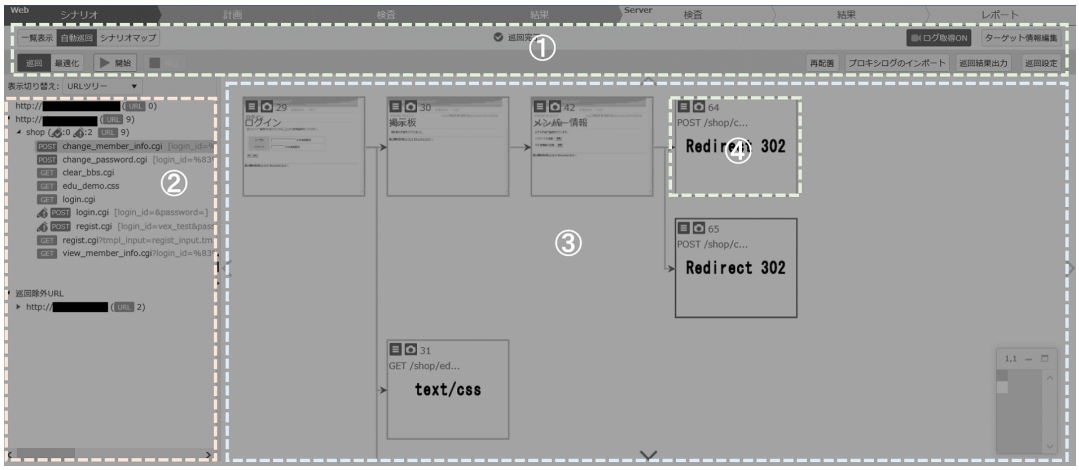
※環境に伴って適宜読み替えを行ってください。

8. ログイン情報が登録されたことを確認し、「完了」ボタンをクリックします。

MEMO

- 作成済みのログイン設定は、再度編集することや削除する事が可能です。
- ログイン失敗時に別のアカウントを利用する場合は、別のログイン情報を登録して下さい。
- ログイン設定を行った場合、同一URLでもログイン前後で別ページと判断され、
- 同一URLのページが検出されることがあります。
    - その他の詳細な設定を行う場合は、「ユーザガイド」の「一般ユーザ画面」＞「Webシナリオ」＞「巡回設定」＞「詳細情報」＞「ログイン設定」を参照してください。

自動巡回の基本的な画面構成、および名称を確認してください。



No	名称	説明
1	メニュー	巡回の開始／停止等の操作メニュー、ステータス等を表示します。
2	ツリー	巡回により取得したURLを表示します。
3	ビュー	画面遷移図の生成／組み替え等を行います。
4	ノード	画面遷移図を構成する要素（各リクエスト情報）です。

本書では、上記の用語を使用して説明を行います。

4.2.2.2.2. <STEP2> 巡回実施

1. メニューの「開始」ボタンをクリックし、巡回を開始します。

自動巡回画面を開始すると、メニューのステータスが「巡回未実施」から「巡回中」に変化します。巡回は、「中断」「再開」「停止」が可能です。

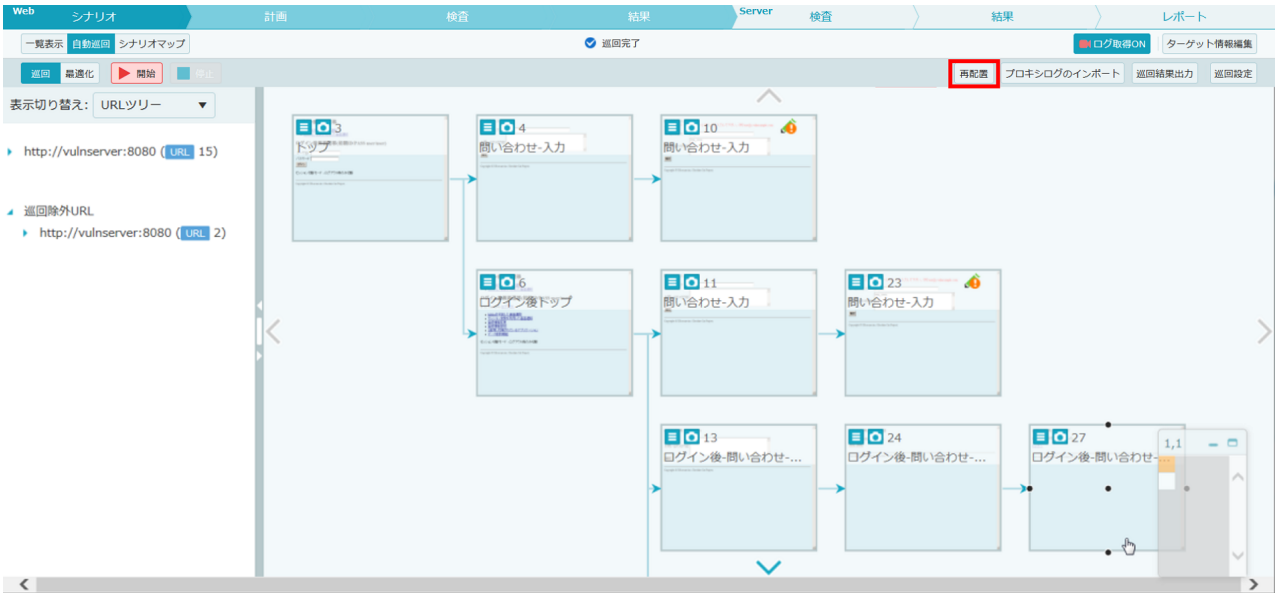
メニューのステータスが「巡回完了」と表示されるまで、しばらくお待ちください。

MEMO

- 巡回中もツリーを操作することでビューを表示することが可能です。
- 自動巡回の検査結果、検査プラン、最適化の実施結果が存在する状態で巡回を実施した場合、既存の情報が削除されます。また、自動巡回の検査が実行中の場合は検査を停止します。
- 自動巡回に要する時間は、サイトの規模、検出リンクの数、検査サーバのレスポンスの速さ、Vexインストール端末のスペック等に依存します。

2. 自動巡回が完了したら、巡回結果の確認をします。

メニューの「再配置」ボタンをクリックすると、ビュー内に画面遷移図が表示されます。



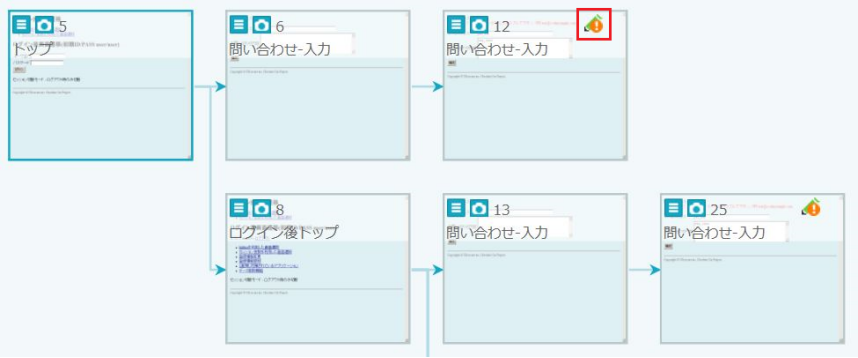
アイコンをクリックすると、取得された画面キャプチャを表示します。

MEMO

- 巡回時に検出したリンクが、過去に検出したリンクと同一の場合、そのリンクに対応してリクエストは送信されません。また、巡回結果に表示されません。
- 巡回時に受信したレスポンスが、過去に受信したレスポンスと重複する場合、同一のページに対するアクセスであると判断し、巡回結果に表示されません。

3. ビューの中に マークが付いたノードが存在する場合があります。

   マークが表示されているノードでは、入力値チェックによるエラーなどの理由で、画面遷移に失敗している可能性があります。



   入力値チェックによるエラーの場合、対象ノードのパラメータ値を変更することで、対象ノード以降の画面遷移を取得出来る可能性があります。

   エラーの発生原因は、対象ノードの画面キャプチャや詳細情報から調査します。

   エラーが発生しているノードの アイコンをクリックし、画面キャプチャを確認します。

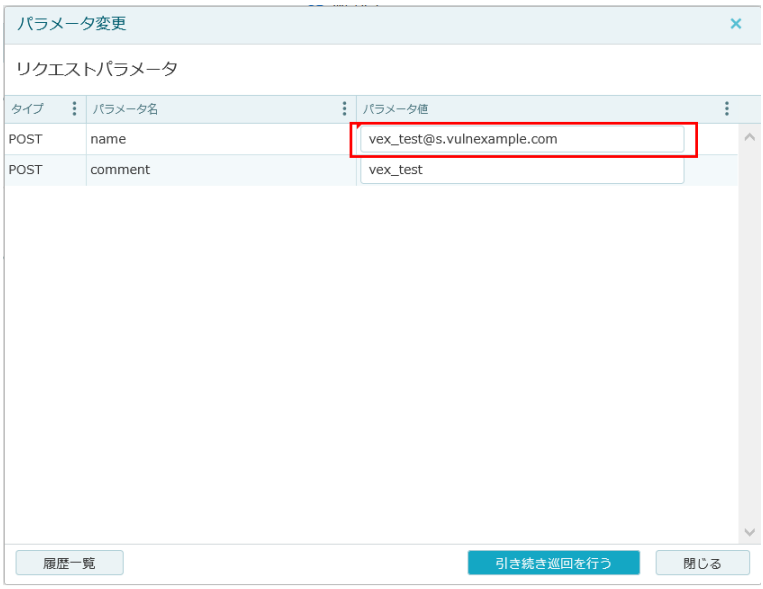
   画面キャプチャ内に表示されたエラーメッセージより、パラメータ値がメールアドレス形式でないために画面遷移に失敗していることが推測できます。

上記のような場合、Vexの自動巡回では問題が発生した箇所のパラメータ値を個別に変更して、自動巡回を再開する事が可能です。

4. 対象ノードの ボタンを押して、ノード操作画面を開きます。

ノード操作画面の「パラメータを変更」ボタンをクリックして、「パラメータ変更」画面を開きます。

5. リクエストパラメータに適切な値を設定し、「引き続き巡回を行う」をクリックします。

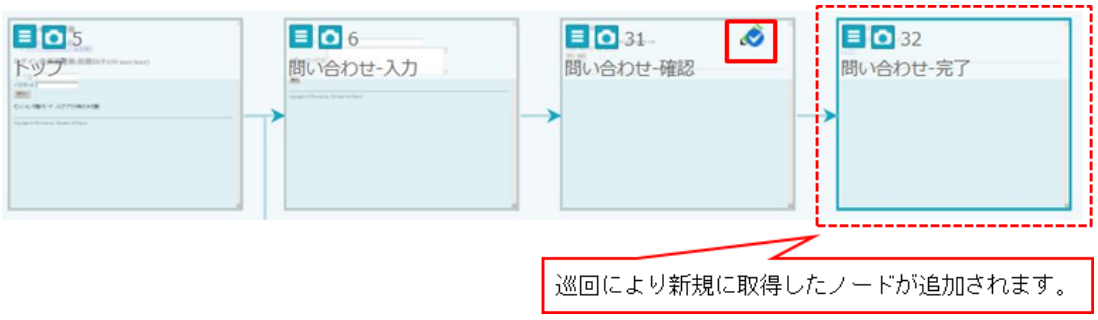


各項目には、下記の入力値を入力します。

タイプ	パラメータ名	元の設定値	変更後の設定値 ※
POST	name	vex_test	vex_test@s.vulnexample.com
POST	comment	vex_test	vex_test（変更なし）

※環境に伴って適宜読み替えを行ってください。

6. パラメータ値を変更後、正常に巡回出来た場合は、対象ノードのアイコンが マークに変更され、以降の画面遷移図が追加されます。



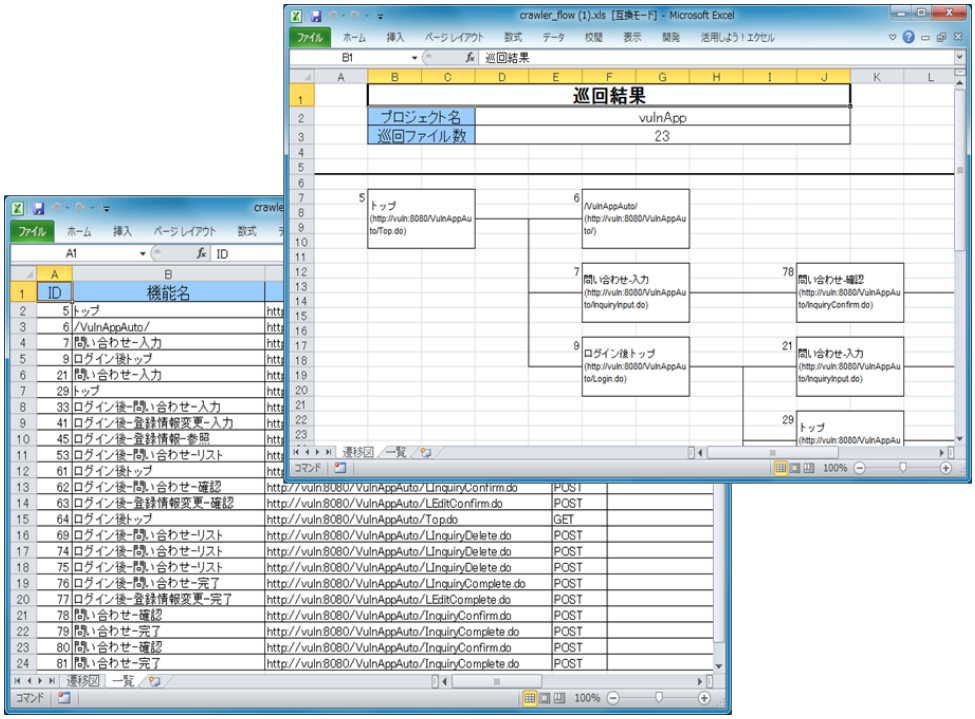
アイコンが変更されたノード、および追加されたノードの画面キャプチャを確認し、正しく画面遷移した際の画面が取得されていることを確認します。

画面遷移図内に⛵マークが付いたノードが他にも存在する場合は、同様にノードの詳細を確認し、問題を解決して下さい。

✓Check!

□パラメータの変更箇所が大量に発生した場合は、「巡回設定>パラメータ」で送信するパラメータ値の初期設定値を変更することが可能です。

メニューの「巡回結果出力」をクリックすると、作成された画面遷移図、および取得した画面一覧をエクセル形式で出力することが可能です。

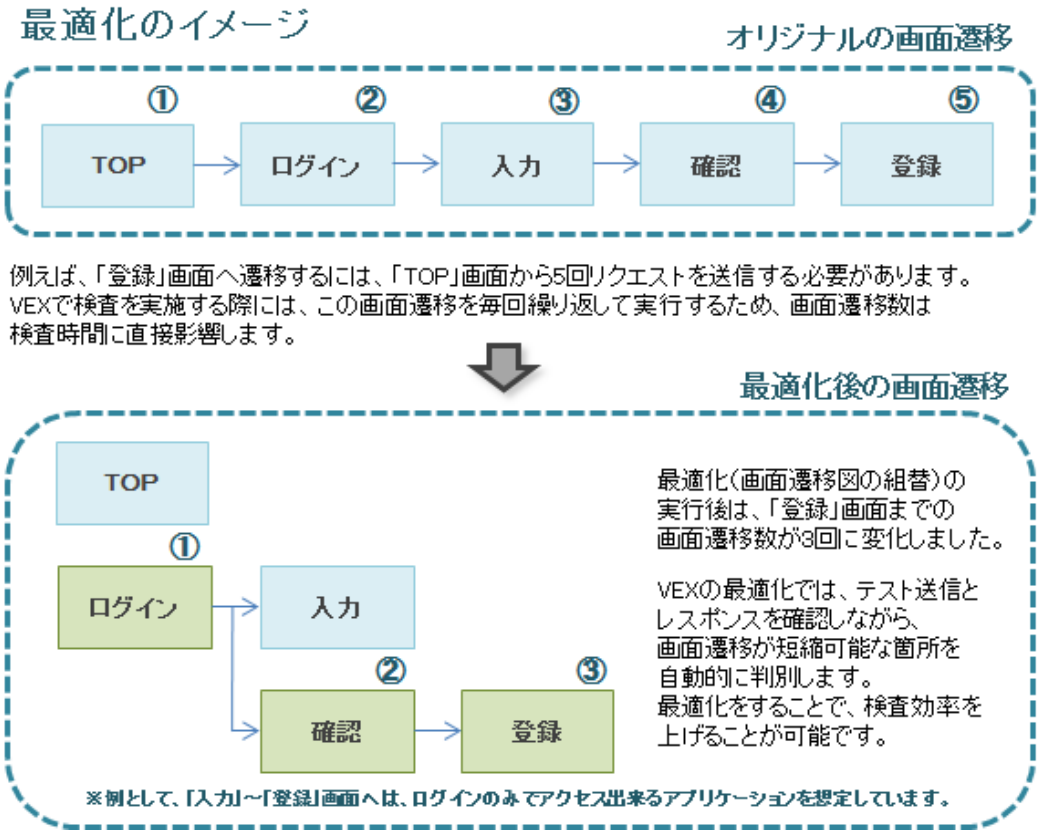


4.2.2.2.3. <STEP3> 最適化実施

続けて検査設定を行います。Vexでは、検査設定を自動的に実施し、さらに最適化機能を提供しています。

4.2.2.2.4. [1] 最適化について

最適化とは、検査を効率よく実施するために、画面遷移図を組み替えて、目的の画面までの遷移数を短縮する機能です。



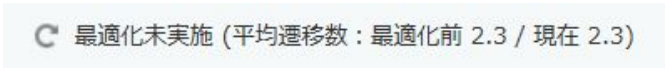
4.2.2.2.5. [2] 最適化の実施

1. メニューの「最適化」ボタンをクリックし、最適化の準備を実行します。

   最適化の準備が終わると最適化画面が表示されます。

2. メニューの「開始」ボタンをクリックし、最適化を開始します。

   最適化実行前のステータス

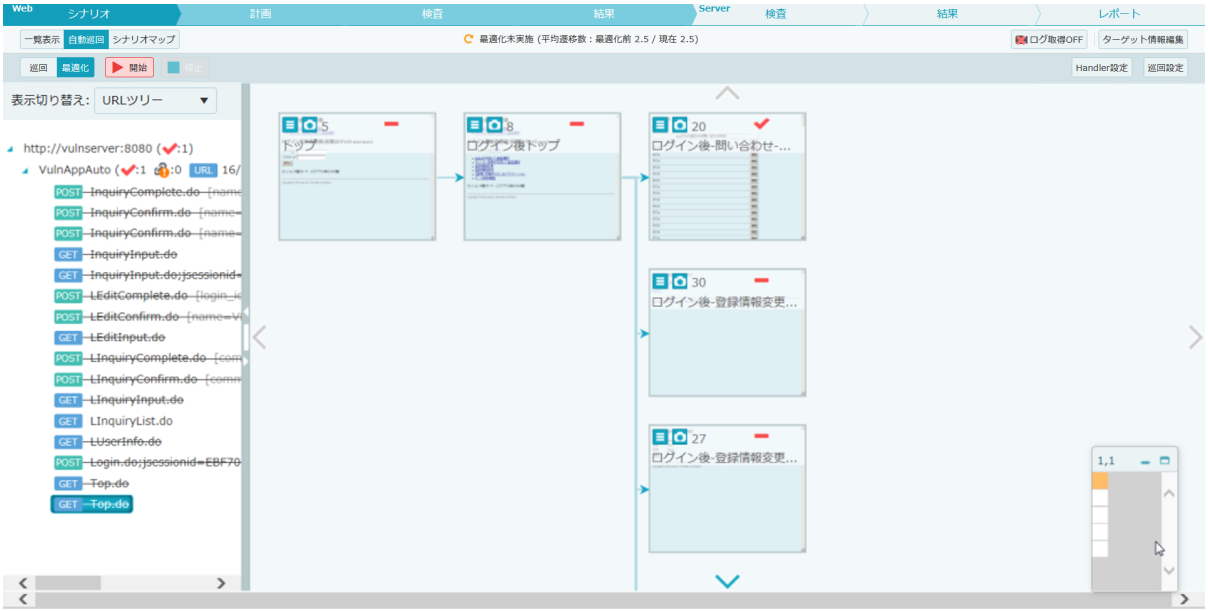


   最適化が完了するまで、しばらくお待ちください。

   平均遷移数が、最適化により減少していることを確認出来ます。

MEMO
・自動巡回の検査結果、検査プラン、最適化の実施結果が存在する状態で最適化を実施した場合、既存の情報が削除されます。 また、自動巡回の検査が実行中の場合は検査を停止します。

3. メニューのステータスに「最適化完了」と表示されたら、ツリー内のGET（またはPOST）のメッセージを選択して、ビューを表示します。



最適化後の画面遷移図が、最適化前から変化していることが確認出来ます。

MEMO

最適化完了後のビューで マークが付いたノードが存在する場合があります。
最適化後の画面遷移図における マークは、「最適化中に取得したHTTPレスポンス」と、「巡回時に取得したHTTPレスポンス」の差分が大きい場合に表示されます。
画面キャプチャ等を確認し、画面遷移に失敗している場合は、自動検査設定ではなく、Handlerの設定（手動での検査設定）をする必要があります。

また、検査対象を選定する場合は、最適化後の画面遷移図の各ノード操作画面上で、検査対象の設定・解除を行うことが可能です。

検査対象から外したい場合は、ノード上のチェックマークをクリックします。

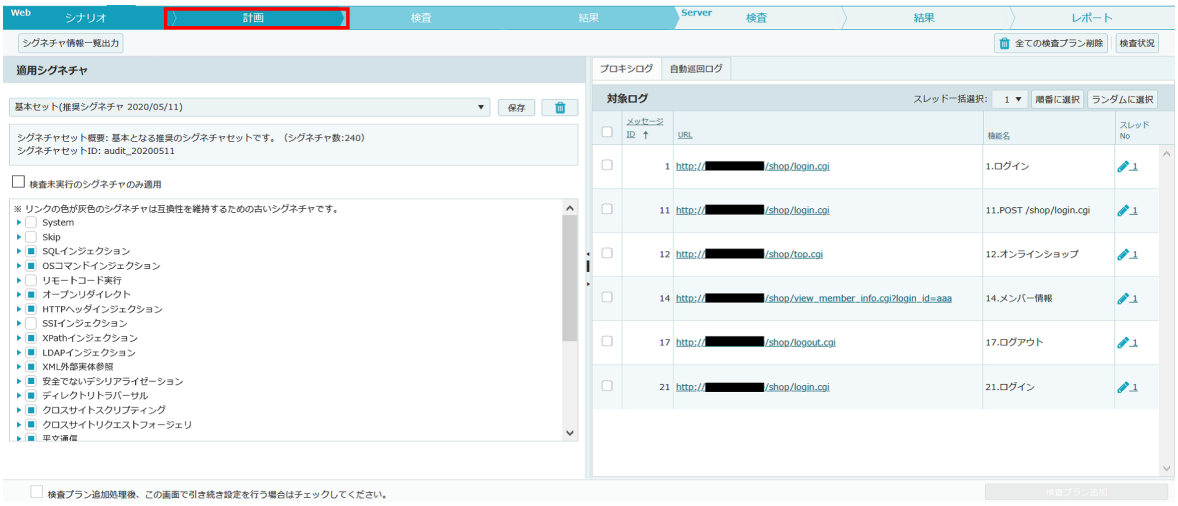
また、 ボタンをクリックすると、ノード操作画面が開きます。

「ノード及びノード配下を全て検査対象から除外」ボタンをクリックすると、対象ノードとその配下の全てのノードを除外とすることが出来ます。

✓Check!
□[重要] 検査禁止の対象がある場合は必ず除外してください。

4.2.2.2.6. <STEP4> 検査プランの作成

1. フローバーのWeb「計画」ボタンをクリックします。



MEMO
Web「計画」画面は、左右2つに分かれています。 　左ペイン：「検査シグネチャ選択」 　右ペイン：「検査対象選択」

2. Web「計画」＞適用シグネチャ選択で、検査シグネチャを選択します。
   ※検査シグネチャは、Vexが検査に使用する検査パターンです。

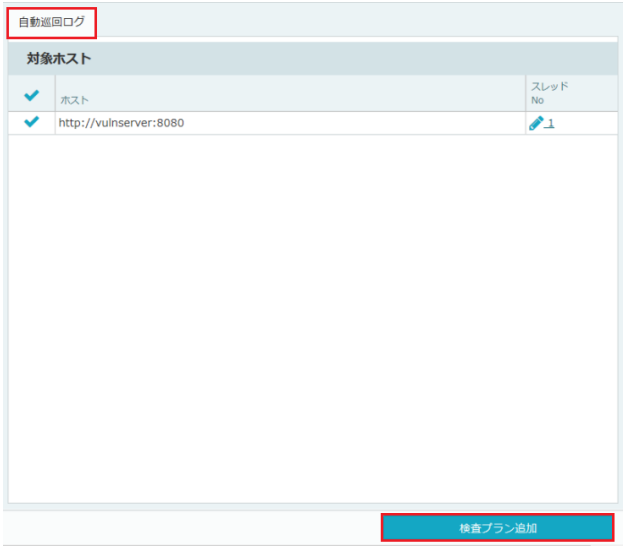
   検査シグネチャには以下の3種類があります。

種類	説明
基本セット	推奨のシグネチャセットです。 主要な脆弱性を検出するためのシグネチャが選択されています。
網羅用	比較的検出率の低い問題や、基本セットで検査している類似の問題に関しても検査を実施するシグネチャセットです。その為、同じ問題を重複して検出する可能性や、検査総時間が非常に膨大になる可能性があります。
速度重視	利用されていない可能性のあるパラメータを自動判別し、自動的に検査対象から外すことで、検査総時間を短縮するシグネチャセットです。

   本書では、基本セット（推奨シグネチャ）を選択します。

3. 検査プランを作成します。

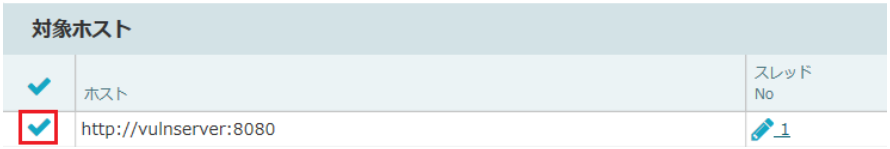
「検査対象選択」の「自動巡回ログ」のタブを選択します。



MEMO

手動で取得したログが存在する場合は、「プロキシログ」タブが選択されている場合があります。

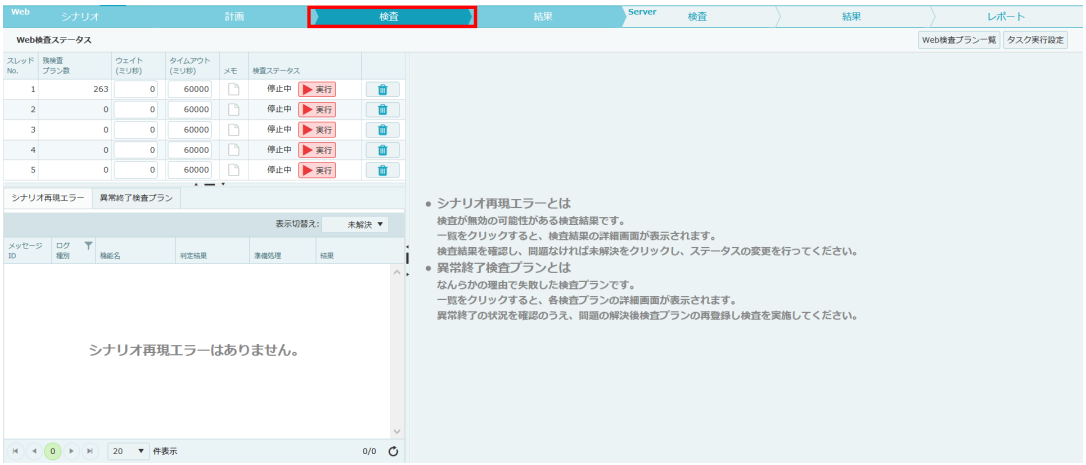
検査対象とするホストを選択し、「検査プラン追加」ボタンをクリックします。



検査プランが登録され、Web「検査」に遷移します。

4.2.2.2.7. <STEP5> 検査実施

1. フローバーのWeb「検査」ボタンをクリックします。



MEMO

Web「検査」画面は、大きく分けて3つに分かれています。
　左上ペイン：「検査ステータス」
　左下ペイン：「シナリオ再現エラー」および「異常終了検査プラン」
　右ペイン ：「Web検査進捗表示」

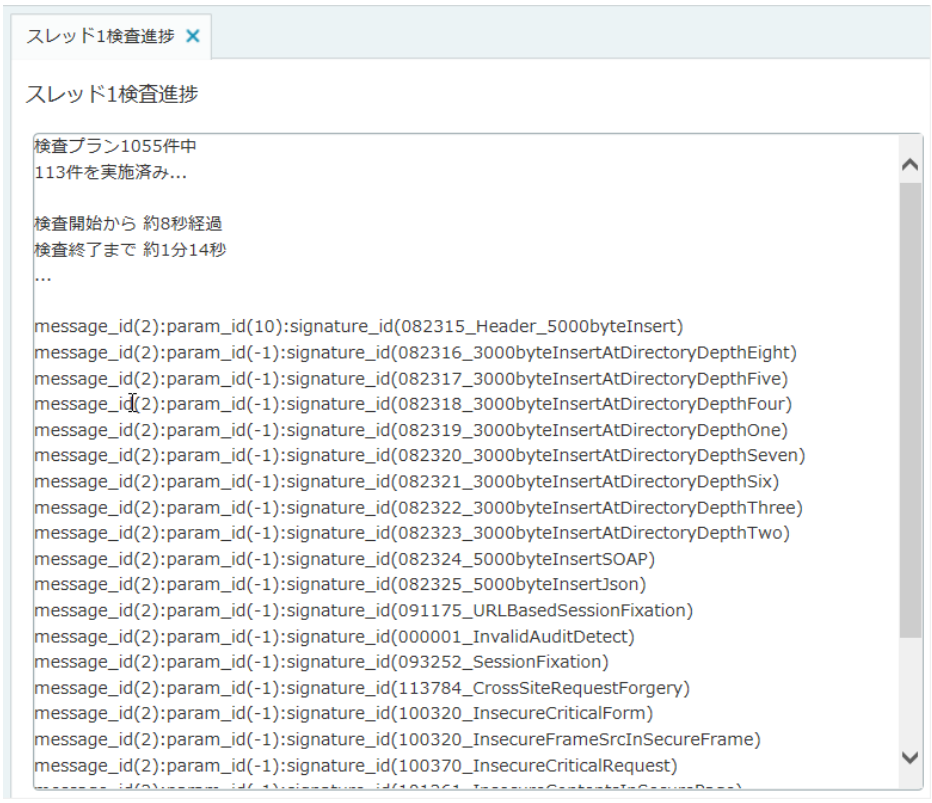
2. 検査プランが登録されているスレッドの「実行」ボタンより 検査を開始します。

✓Check!

□検査を開始すると大量のアクセスが発生するため、関係者様への連絡を行ってください。
□検査により、意図しないデータの登録、変更、削除が発生する可能性があります。
重要なデータは必ずバックアップを残してください。

検査が開始されると、検査ステータスが「実行中」に変化します。

検査中のスレッドをクリックすると、右ペインに「Web検査進捗表示」が表示されます。



MEMO

- 検査中にも、ログの取得やHandlerの作成などの他の機能を使用することが可能です。
  - マルチスレッドの利用により、最大5つの検査を同時に実行出来ます。
  - 検査終了までの見込み時間は、サーバの稼働状況や準備処理の設定状況等により大きく変動する可能性があります。目安として参照してください。

画面中の各項目に関しては、下記の表をご確認ください。

No	項目	内容
1	スレッドNo	検査を実行する単位です。 マルチスレッドの利用により検査スピードの向上が見込めますが、マルチスレッドを利用する場合には注意が必要です。 詳細は「ユーザガイド」の「スレッド使用時の注意点（自動巡回）」を参照してください。
2	残検査プラン数	登録されている検査プラン数が表示されます。
3	ウェイト	検査リクエストを送信する間隔をミリ秒単位で指定することが可能です。 Webサーバへの負荷を軽減したい場合などに使用します。
4	タイムアウト	検査時に検査サーバからのレスポンスを待つ最大時間です。 デフォルトは60000ミリ秒（1分）が設定されています。

「自動巡回による検査」は以上です。
手順③「Web検査結果の確認」へ進んで下さい。

4.2.3. 手順③Web検査結果の確認

Webアプリケーション検査結果を確認します。

✓Check!
□検査の途中でも検査結果の確認が可能です。 □画面上部に**「検査エラー」**と表示されている場合、検査に失敗している可能性があります。 検査中に表示された場合は、一旦検査を中断し、アラートの原因を確認してください。 詳しくは「検査エラー」をご参照ください。

4.2.3.1. 検査結果の確認

1. フローバーのWeb「結果」ボタンをクリックします。

画面内の各項目に関しては、下記の表をご確認ください。

No	項目	内容
1	リクエスト編集	手動で検査パターンを編集して送信する機能です。
2	検査総数	検査総数（内、未閲覧数）です。
3	検出数	脆弱性検出数（内、未閲覧数）です。
4	判定数	検査結果を確認した結果、脆弱性と判断した数です。

MEMO
・検査結果の確認には、「Web検査結果(リクエスト毎)」と「Web検査結果(シグネチャ毎)」の2種類が用意されています。

2. Vexが検出した検査項目を確認します。

脆弱性を検出しているリクエストが存在する場合は、「検出数」リンクをクリックします。

機能名	検査総数	検出数	判定数
1.トップ	1617(1613)	30(27)	30
2.ログイン後トップ	2088(2088)	47(47)	47
3.ログイン後-問い合わせ(Session)-入力	942(942)	13(13)	13
4.ログイン後-問い合わせ(Session)-確認	801(798)	18(16)	18
5.ログイン後-問い合わせ(Session)-完了	712(712)	14(14)	14

各検査対象にて検出した脆弱性の一覧を表示します。

MEMO

- Web「結果」画面は、左右2つに分かれています。
  左ペイン：「Web検査結果一覧」
  右ペイン：「Web検査結果詳細」

一覧画面に表示される内容は以下の通りです。

No	アイコン	項目	内容
1	ー	検査結果ID	実行された各検査の情報を管理するIDです。

No	アイコン	項目	内容
2		HTML表示	検査時のレスポンスをブラウザ画面で表示します。 Web検査結果詳細を未確認の状態の場合が表示され、確認後は が表示されます。 確認がされていない検出項目を容易に認識するための機能です。
3		メモ	判定結果を変更した理由などを残しておくと便利です。
4	ー	カテゴリ	脆弱性種別です。
5	ー	概要	検出したシグネチャの概要です。
6		判定	検出の場合 が表示されます。 クリックすると （過検知）に変更され、検出対象から外れます。
7		危険度	検出した各脆弱性の危険度です。 「緊急」「高」「中」「低」「情報」の5種類に分けられており、クリックすると、任意の危険度への変更が可能です。
8		再送	該当の検査パターンの再テストを行います。
9	ー	ターゲット	該当の検査パターンを適用したパラメータ名が表示されます。 対象がリクエスト全体の場合は「request」の文字が表示されます。
10	ー	元値	プロキシログに記録されているオリジナルの値です。
11	ー	変更値	プロキシログに記録されているオリジナルの値です。
12	ー	検出トリガ	脆弱性を検出した際に、脆弱性が存在すると判定した文字列です。
13		詳細	右ペインに「Web検査結果詳細」を表示します。

詳細を確認したい検出項目の「詳細」リンクをクリックすると、右ペインに「Web検査結果詳細」が表示されます。

右ペインの「Web検査結果詳細」を確認します。

「Web検査結果詳細」では、脆弱性を検出した時の、検査パターンを含んだリクエスト、およびレスポンス情報が確認出来ます。

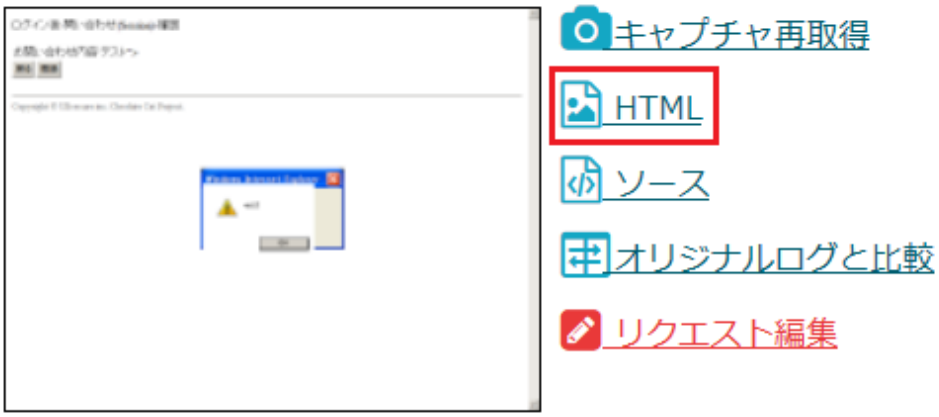
タブ構成で「検査情報」「リクエスト」「レスポンス」の表示の切替えが可能です。

それでは、本画面上で、検出内容の確認をします。

Vexは、検査時のレスポンス情報の画面キャプチャを自動で取得します。

「Web検査結果詳細」の画面キャプチャをクリックすると、大きな画像で表示します。

今回の例では、検査パターンで挿入したJavaScriptが動作していることを、画面キャプチャからも確認出来ます。



また、「HTML」アイコンをクリックすると、ブラウザで表示することが出来るため、JavaScriptが実際に動作し、問題のある挙動であることが確認可能です。

MEMO

- 判断に迷う場合は、再送アイコンをクリックし、事象に再現性があるかを確認してください。
  再送により検出が再現しない場合は、誤検知の可能性がございます。
- 誤検知と判断した場合は、判定のアイコンを から に変更して下さい。
- 本画面からも、危険度の変更が可能です。

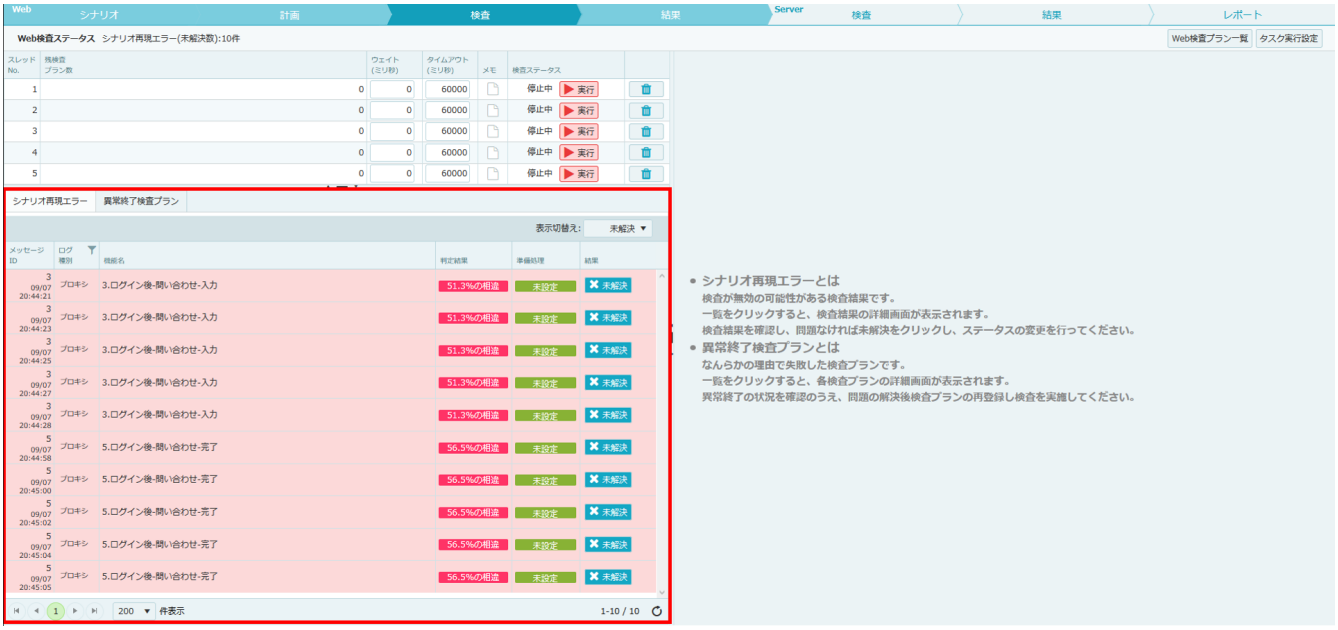
4.2.3.2. 検査エラー

検査が終了していても、メニュー内に「検査エラー」のアラートが表示されている場合、検査に失敗している可能性があります。

✓Check!
☐ 検査中に表示された場合は、一旦検査を中断し、アラートの原因を確認してください。

「検査エラー」をクリックすると、「エラー一覧」を表示します。

※フローバーのWeb「検査」画面へ遷移します。



検査エラーには、下記の2種類があります。

項目	説明
シナリオ再現エラー	ログ記録時とテスト送信時のHTTPレスポンスの一致率が低い場合に表示されます。
異常終了検査プラン	検査対象ホストから応答がないなど、検査実行ができなかった場合に表示されます。

4.2.3.2.1. [1] シナリオ再現エラー

検査の有効性判断において無効の可能性があると判定された場合、「シナリオ再現エラー」が表示されま

す。

Vexは検査設定の有効性を確認するため、検査中にもテスト送信（検査パターンを含まない正常リクエスト）を定期的に送信します。

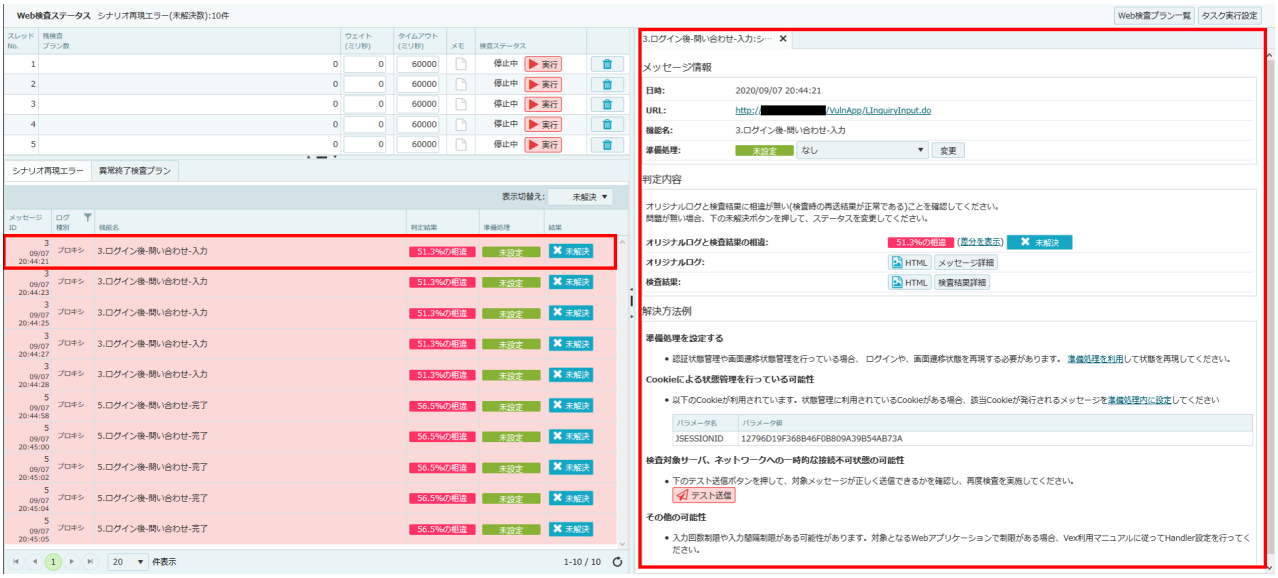
なんらかの理由により、検査の途中で検査設定が無効な状態になってしまった場合、エラー画面に画面遷移するなど「ログ記録時のレスポンス」と「テスト送信時のレスポンス」の相違度が高くなることが想定されます。

相違度が一定の閾値を超えた場合、Vexは「シナリオ再現エラー」を検出します。

「シナリオ再現エラー」を検出した場合、正しく検査出来ているか、失敗しているかを確認する必要があります。

＜確認方法＞

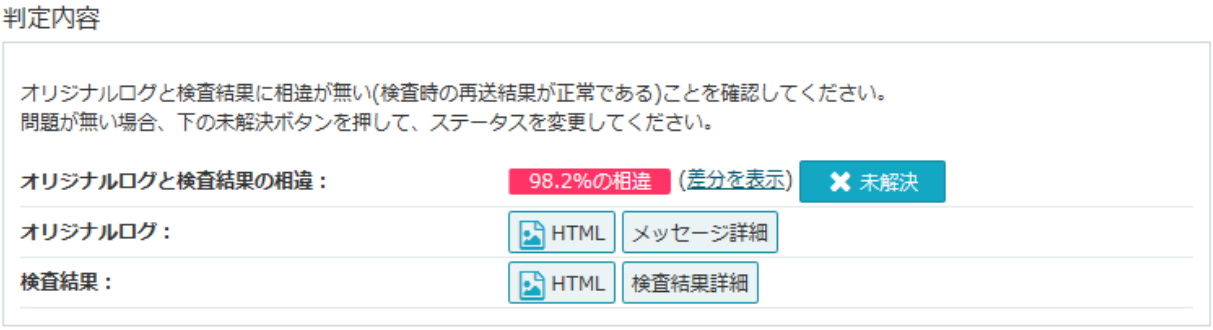
1. 「シナリオ再現エラー」一覧の「機能名」をクリックします。

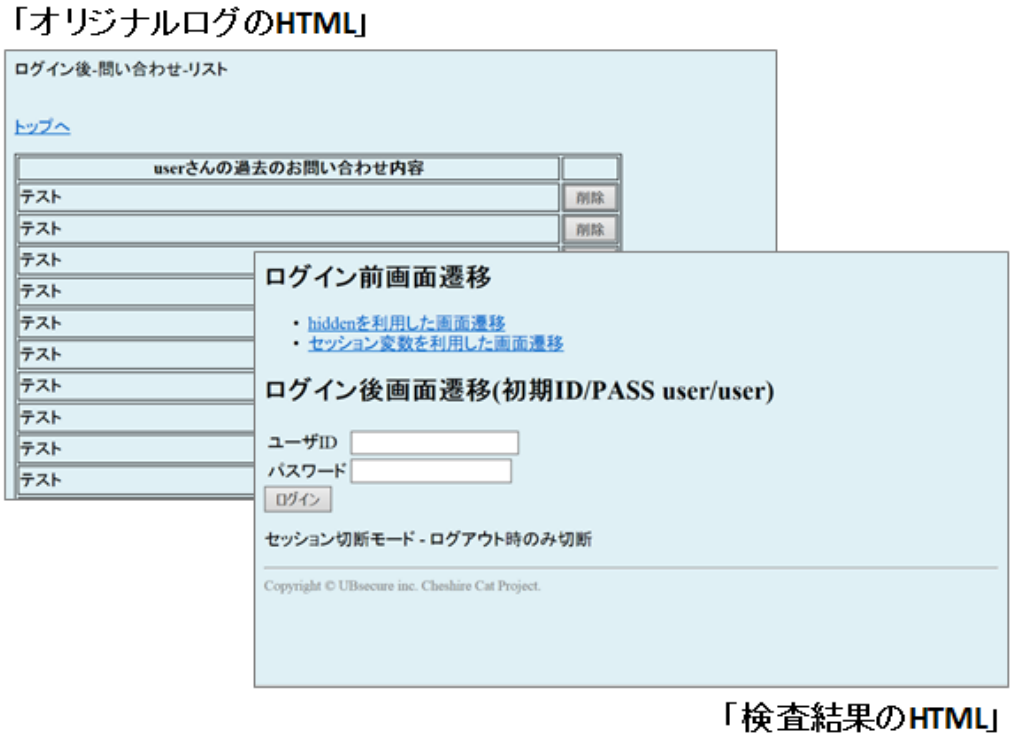


右ペインに「エラー詳細」が表示されます。

2. 「オリジナルログ」と「検査結果」の「HTML」ボタンをクリックします。

ケース1.「オリジナルログ」と「検査結果」の「HTML」が大きく異なる場合





「オリジナルログ」と「検査結果」の「HTML」を比較すると、「オリジナルログ」は、ログイン後の機能の「お問い合わせリスト」が表示されているのに対し、「検査結果」はログイン前の画面を表示しています。

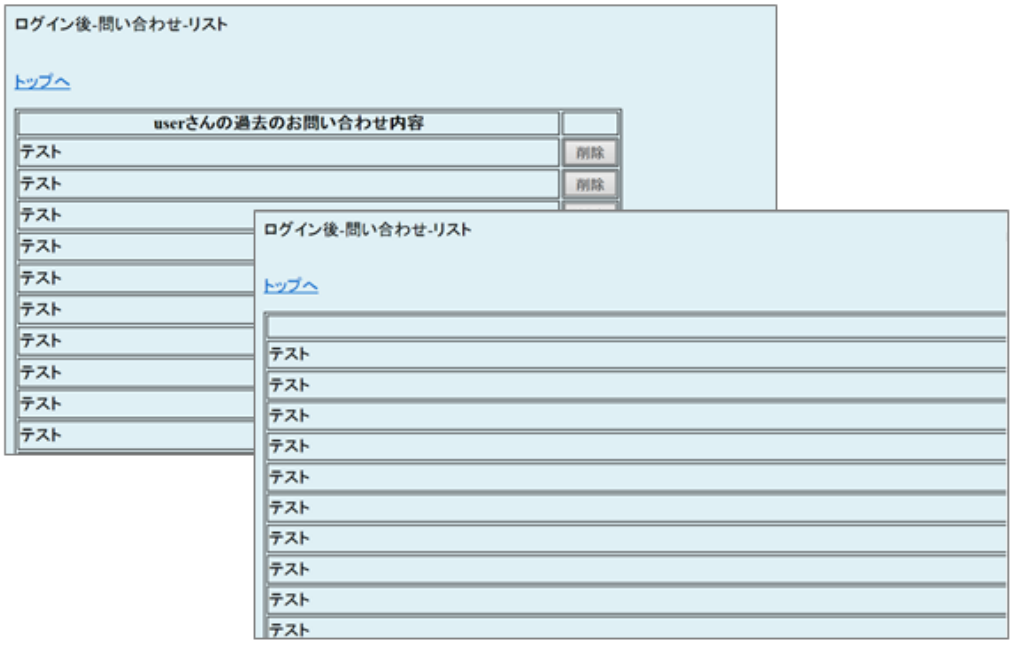
このようなケースの場合、**正しくログイン手順の準備処理がされていない**と考えられます。

準備処理が設定されていない場合や、準備処理が設定されていても必要なパラメータの引継ぎが出来ていない場合があります。

検査設定を見直し、再度テスト送信を行って設定に不備がないことを確認してください。

ケース2.「オリジナルログ」と「検査結果」の「HTML」が比較的類似している場合

「オリジナルログのHTML」



「検査結果のHTML」

「オリジナルログ」と「検査結果」の「HTML」を比較すると、「オリジナルログ」も「検査結果」も同じログイン後の機能の「お問い合わせリスト」画面を表示しています。

画面遷移自体は正しく出来ている事から、**準備処理は正しく出来ている**と考えてられるため、相違が発生している原因を調査して下さい。

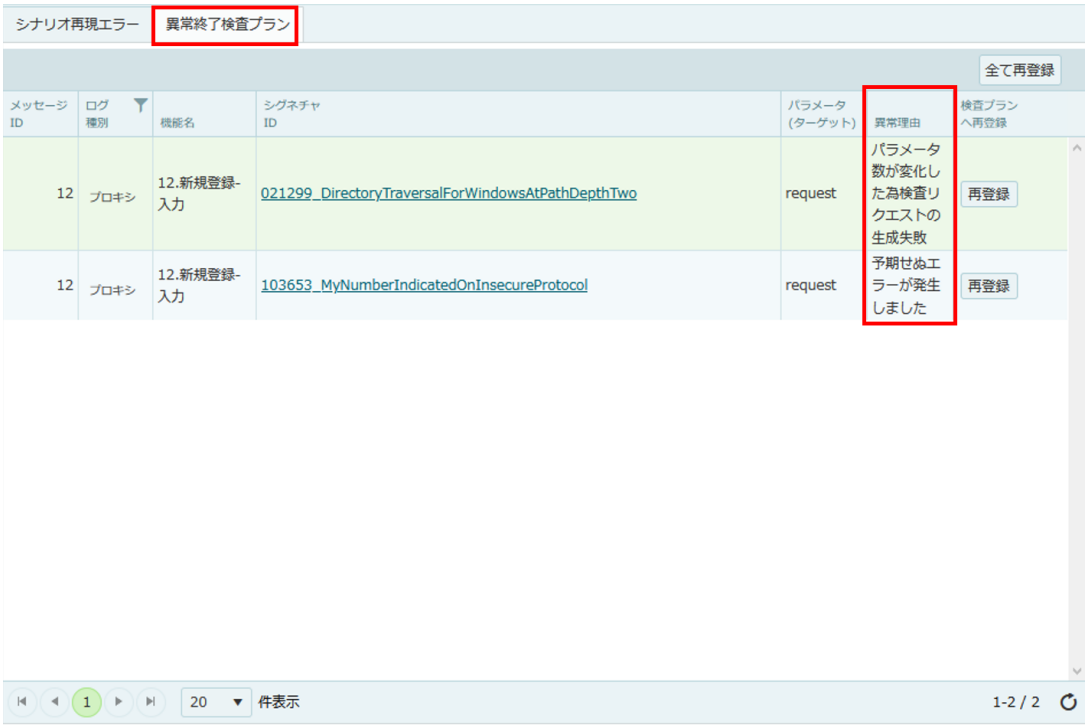
このようなケースの場合、HTML画面を詳しく確認すると、リストに表示されているレコードの数が異なる場合が考えられます。

検査の過程で、表示される情報に変化が発生する可能性がある画面の検査においては、Vexが「シナリオ再現エラー」を検出することがありますが、検査設定に不備がないと判断した場合は、解決済の状態にすることで「検査エラー」が表示されなくなります。

✓Check!（よくありがちな原因）
□画面遷移が正しく再現されていないことにより、パラメータ引継ぎのエラーが発生している □機械的なパラメータ引継ぎが困難なパラメータが存在する □二重ログインが禁止されているアプリケーションで、ログインエラーが発生している □会員退会処理など一度しか実行出来ない機能を検査している場合 □検査の過程においてデータが追加、もしくは削除される等、レスポンスが大きく変化する機能を検査した場合（対応不要） 原因の違いにより対応方法が異なります。 詳しくはFAQ サイトのカテゴリ「Handler ガイド」から「ケース毎の設定方法」をご参照ください。

4.2.3.2.2. [2] 異常終了検査プラン

検査の実行がなんらかの理由で失敗した場合には、「異常終了検査プラン」が表示されます。



異常理由が、「検査対象ホストから応答がない」である場合、検査対象サーバがレスポンスを返さなかったことを意味します。検査時の負荷等により、一時的にサーバからの応答に影響が発生した可能性があります。

「再登録」ボタンをクリックすると、検査プランに再登録されますので、再度検査を実施してください。

No	項目	内容
1	メッセージID	HTTPメッセージを識別するメッセージIDです。
2	ログ種別	表示する対象を全て、プロキシログ、自動巡回ログの中から選択できます。

No	項目	内容
3	機能名	HTTPメッセージに該当する機能名です。
4	シグネチャID	検査シグネチャIDです。 押下するとシグネチャ情報が表示されます。
5	パラメータ (ターゲット)	検査対象となったパラメータ（ターゲット）です。
6	異常理由	検査の失敗理由が表示されます。
7	検査プランへ 再登録	失敗した検査プランを、再実行するようにプランへ再登録します。再登録されるプランは、登録済み検査プランの先頭に追加されます。

MEMO

- 再度検査を実施しても同様の事象が発生する場合は、該当検査パターンを送信した際の検査対象サーバの挙動であると考えられます。

4.2.4. 手順④ Server検査実施

4.2.4.1. Server検査の種類と基本設定

1. フローバーのServer「検査」ボタンをクリックします。

MEMO
・Server「検査」画面は、左右2つに分かれています。 　左ペイン：「Server検査対象一覧」 　右ペイン：「Server検査進捗確認」

検査対象サーバは、新規プロジェクトの作成時にターゲット情報として検査対象ホストに　指定したサーバです。

Server検査には「Server Files検査」、「Server Settings検査」の2種類があります。

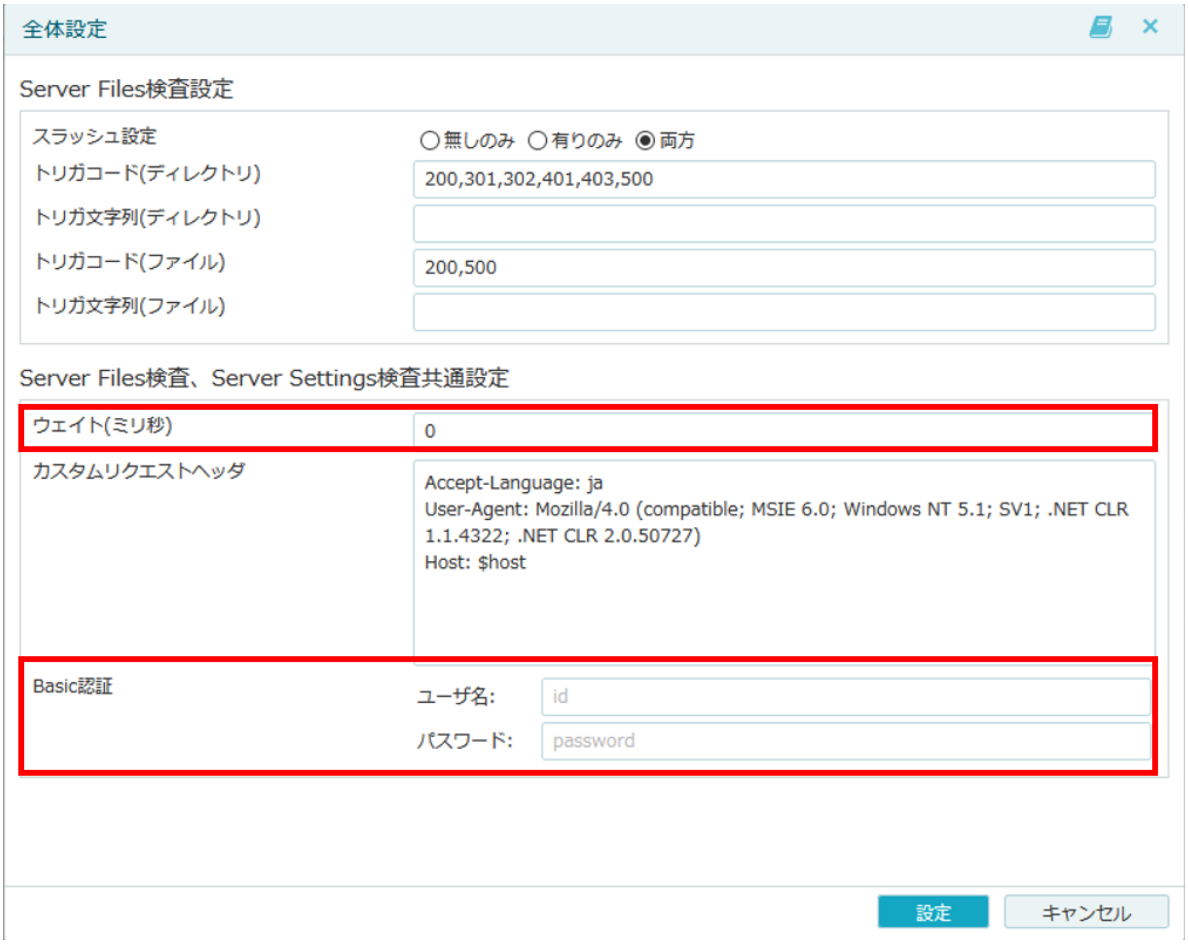
各検査の内容は下記をご確認ください。

項目	内容
Server Files検査	テスト用ファイルやバックアップファイルなど、Webアプリケーションの動作に不要と考えられるファイルの検出を行います。
Server Settings検査	サーバの設定ミスに由来する既知の脆弱性を検出します。

2. 検査の全体設定を行います

「Server検査対象一覧」内の設定アイコンをクリックします。

「Server検査 全体設定」画面が表示されます。



検査対象サーバへの負荷を軽減したい場合は、ウェイト設定をご利用ください。

また、検査対象サーバにBasic認証がかけられている場合は「Basic認証」欄に、ユーザ名とパスワードを入力してください。

MEMO

・その他の項目ついては、「ユーザガイド」の「一般ユーザ画面」＞「Server検査」を参照してください。

4.2.4.2. Server Files検査の実施

Server Files検査では、公開するべきでないファイルの有無を検査します。

例えばバックアップファイルや、アプリケーションインストール時にデフォルトで配置されるサンプルファイルなど、公開ディレクトリに配置すべできではないファイルが該当します。

1. Server Files検査の「検査プラン作成」をクリックします。

「Server Files検査実行内容確認」画面が表示されます。

MEMO

Server Files検査は、「ディレクトリ名」「ファイル名」などのリストを 順番に組み合せてURLを作成し、Webサーバ上でアクセス可能がどうかを確認します。

2. すでにWebアプリケーション検査の巡回により、プロキシログが記録されている場合は、検査対象アプリケーションに特有の「ディレクトリ名」「ファイル名」等の情報を、「プロキシログからインポート」ボタンをクリックすることで取り込むことができます。

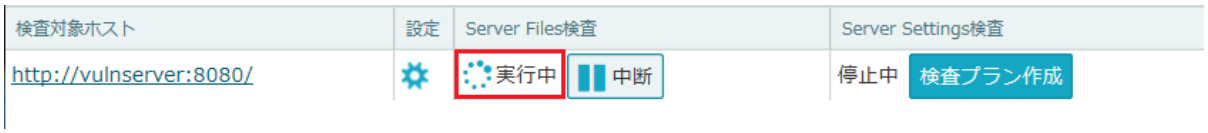
「プロキシログからインポート」ボタンをクリックすると、シグネチャセットに「インポート済み」の文字列が表示されます。

MEMO

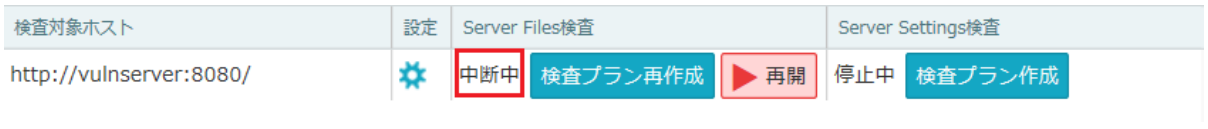
・プロキシログに存在する「ディレクトリ名」「ファイル名」を取り込むことにより、より精度の高い検査が可能です。
そのため、Server検査は、Web検査の巡回後に実施することを推奨します。

3. 検査の準備が整いましたら「実行」ボタンをクリックし、Server Files検査を開始します。

Server Files検査のステータスが「実行中」に変化します。



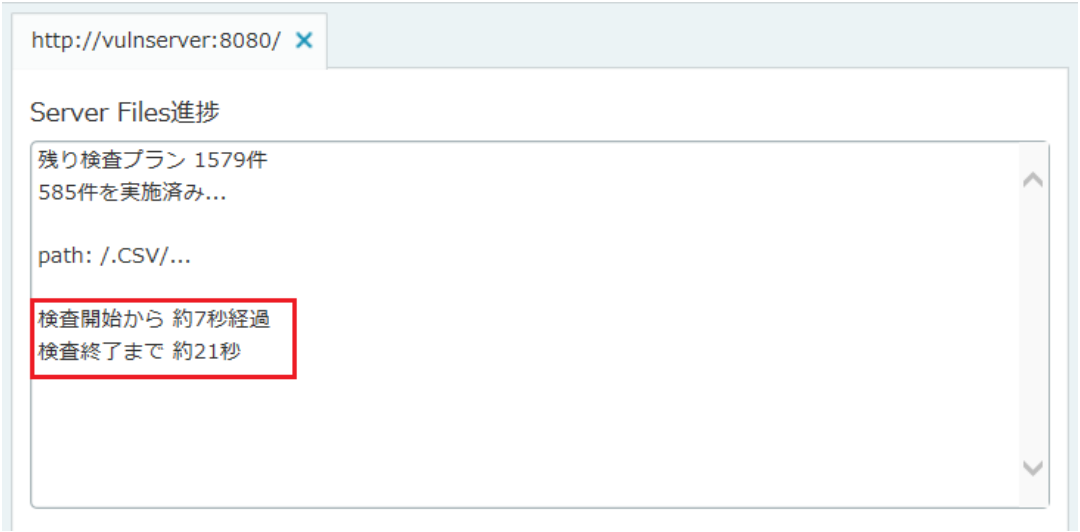
中断ボタンをクリックするとステータスが「中断中」に変化します。



MEMO

・検査を再開する場合は、「再開」ボタンをクリックしてください。
・「検査プラン再作成」をクリックすると、「Server Files検査実行内容確認」画面を開き検査が最初から再実行されます。

実行中に一覧の「検査対象ホスト」をクリックすると、右ペインに「Server検査進捗確認」が表示されます。「Server検査進捗確認」には、おおよその検査の残り時間が表示されます。



検査が終了すると、ステータスは「終了」に変化し、「Server検査進捗確認」には「停止中」が表示されます。

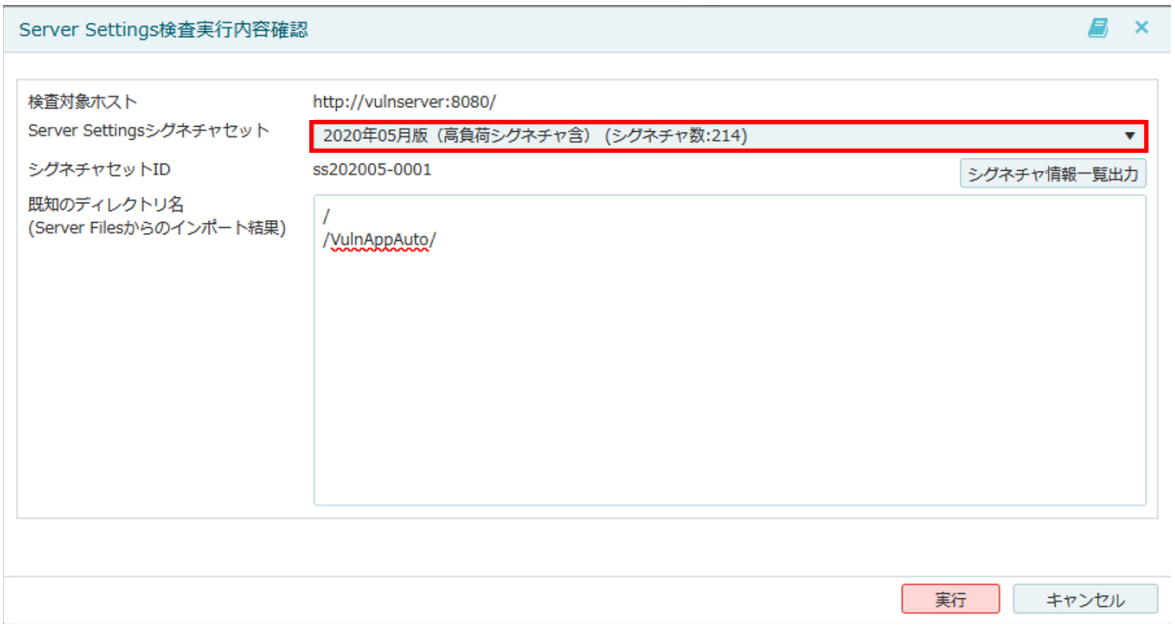
4.2.4.3. Server Settings検査の実施

Server Settings検査では、サーバの設定に起因する脆弱性や、使用しているプロダクトに存在する公開済の脆弱性の有無を検査します。

1. Server Settings検査の「検査プラン作成」をクリックします。

「Server Settings検査実行内容確認」画面が表示されます。

本画面では、Server Settingsシグネチャセットの選択をします。



MEMO

「既知のディレクトリ名」には、Server Files検査で存在が確認されたディレクトリ情報がインポートされます。
そのため、Server Files検査の後に実施することを推奨します。

Server Settings検査のシグネチャセットは下記をご確認ください。

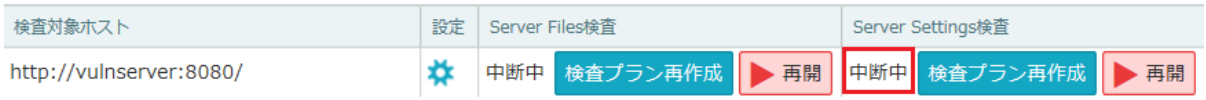
シグネチャセット名	説明
20XX年XX月版 ※	負荷のかかるシグネチャを除外したServer検査用のシグネチャセットです。
20XX年XX月版 （高負荷シグネチャ含）※	上記、シグネチャセットに、Buffer Over FlowやDoSなど、サーバに負荷のかかる検査を含みます。 ※サーバダウンが懸念される場合は使用を控えてください。

※環境に伴って適宜読み替えを行ってください。

2. 検査の準備が整いましたら「実行」ボタンをクリックし、Server Settings検査を開始します。

Server Settings検査のステータスが「実行中」に変化します。

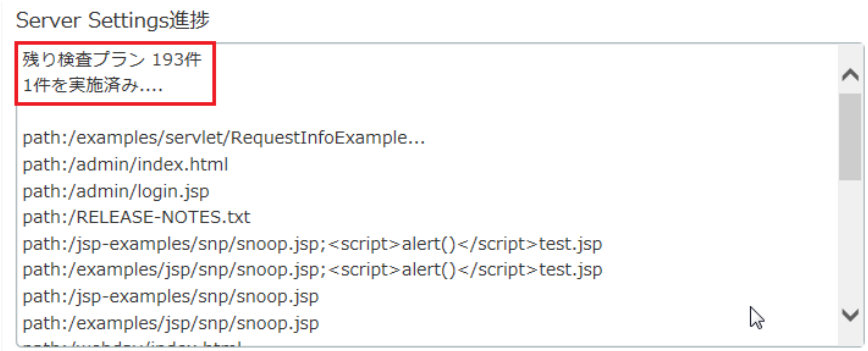
中断ボタンをクリックするとステータスが「中断中」に変化します。



MEMO

・検査を再開する場合は、「再開」ボタンをクリックしてください。
・「プラン再作成」をクリックすると、
「Server Settings検査設定」画面を開き検査が最初から再実行されます。

実行中に一覧の「検査対象ホスト」の上をクリックすると、右ペインに「Server検査進捗確認」が表示されます。「Server検査進捗確認」には、残り検査プラン数が表示されます。



検査が終了すると、ステータスは「終了」に変化し、「Server検査進捗確認」には「検査が終了しました。」が表示されます。

4.2.5. 手順⑤ Server検査結果の確認

4.2.5.1. Server Files検査結果の確認

1. フローバーのServer「結果」ボタンをクリックします。

画面内の各項目に関しては、下記の表をご確認ください。

No	項目	内容
1	検査総数	検査総数（内、未閲覧数）です。
2	ループ数	その配下のいかなるディレクトリ、ファイルも、全体設定で設定したトリガにマッチするため、再帰的にディレクトリを検出してしまうと判断されたディレクトリの総数です。
3	検出数	脆弱性検出数（内、未閲覧数）です。
4	判定数	検査結果を確認した結果、脆弱性と判断した数です。 レポート出力対象件数です。

2. Vexが検出した検査項目を確認します。

   脆弱性を検出している場合は「検出数」のリンクをクリックし、Server Files検査で検出した脆弱性の一覧を表示します。

MEMO

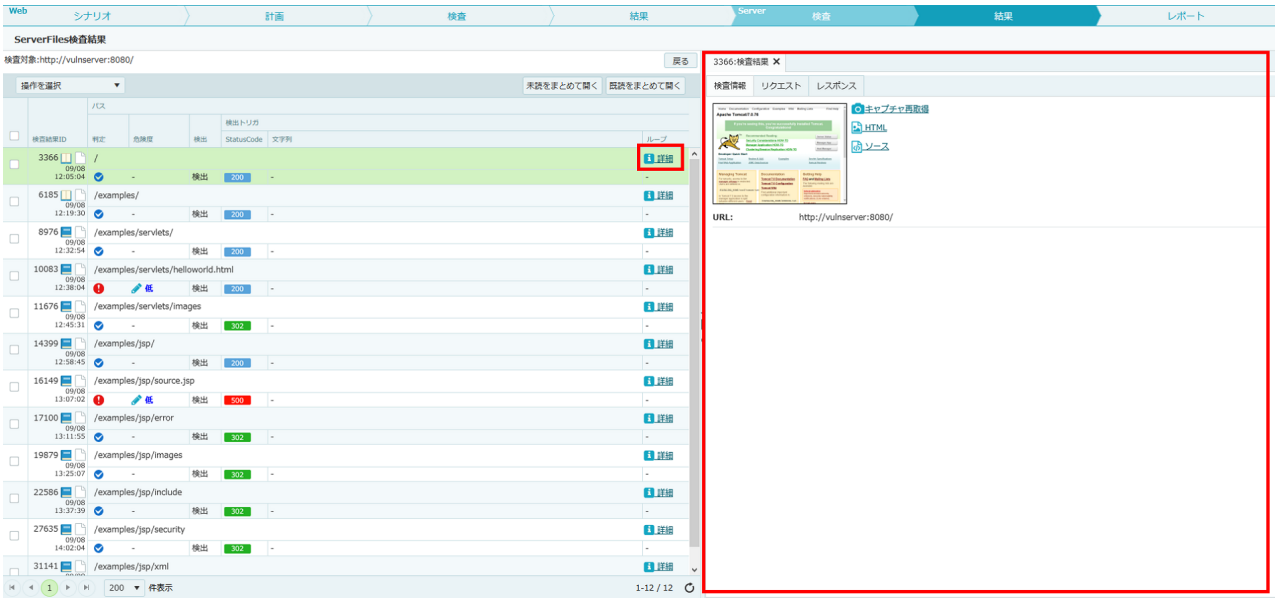
Server Files検査結果画面は、左右2つに分かれています。
　左ペイン：「Server Files検査結果一覧」
　右ペイン：「Server Files検査結果詳細」

「Server Files検査結果一覧」の表示内容を確認します。

No	アイコン	項目	内容
1	ー	検査結果ID	実行された各検査の情報を管理するIDです。
2		HTML表示	検査時のレスポンスをブラウザ画面で表示します。 Server Files検査結果詳細を未確認の状態の場合 が表示され、確認後は が表示されます。 確認がされていない検出項目を容易に認識するための機能です。
3		メモ	判定結果を変更した理由などを残しておくと便利です。
4	ー	パス	脆弱性を検出したパスです。
5		判定	検出の場合 が表示されます。 クリックすると に変更され、検出対象から外れます。

No	アイコン	項目	内容
6		危険度	検出した各脆弱性の危険度です。 「緊急」「高」「中」「低」「情報」の5種類に分けられており、クリックすると、任意の危険度への変更が可能です。
7	200 など	Status Code	レスポンスに含まれるステータスコードです。
8	ー	文字列	検出した際に一致したトリガ文字列が表示されます。
9	ー	ループ	該当ディレクトリ配下で、存在しないファイルに対してトリガコード、もしくはトリガ文字列が一致した場合に、一致したトリガが表示されます。
10		詳細	右ペインに「Server Files検査結果詳細」を表示します。

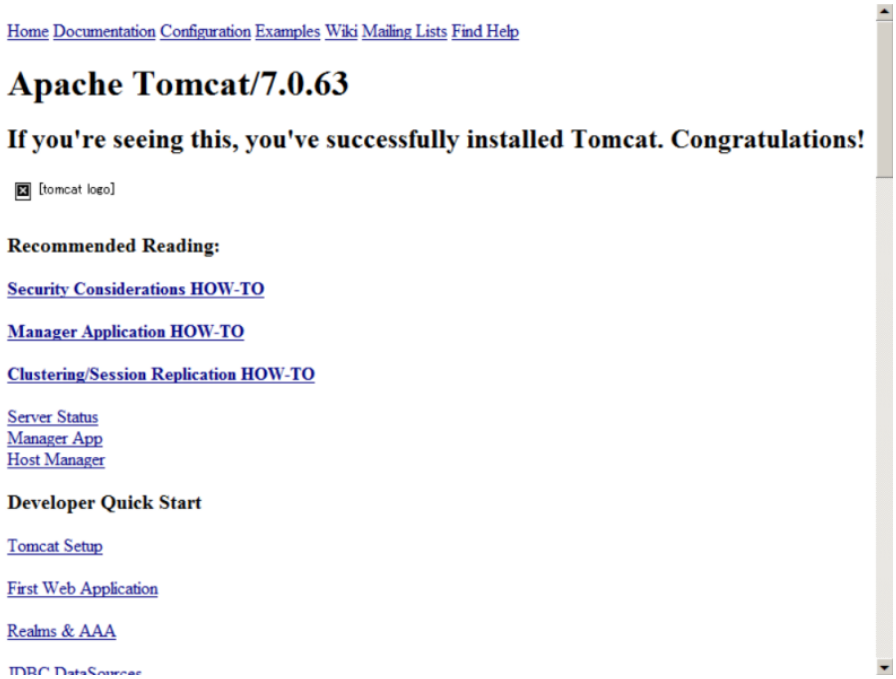
検出項目の「詳細」アイコンをクリックすると、右ペインに「Server Files検査結果詳細」が表示されます。



実際に検査実施時のリクエスト、およびレスポンス情報を閲覧することが出来ます。

タブ構成で「検査情報」「リクエスト」「レスポンス」の表示の切替えが可能です。

画面キャプチャをクリックすると、大きな画像を表示します。



検出したファイルが公開するべきではないかどうかを確認してください。

4.2.5.2. Server Settings検査結果の確認

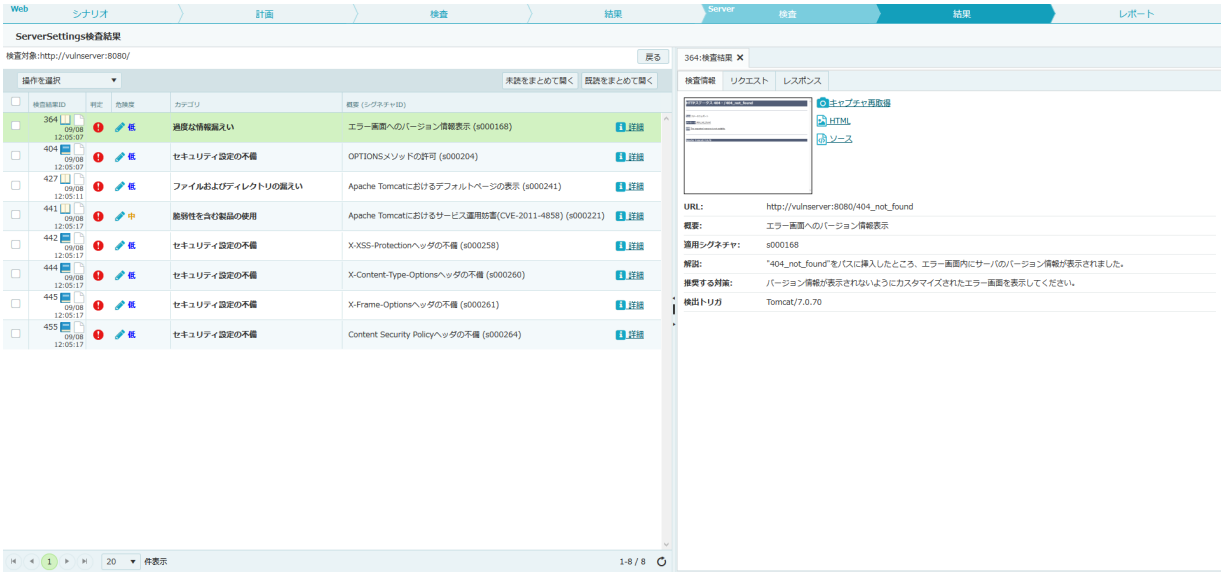
1. フローバーのServer「結果」ボタンをクリックします。

画面内の各項目に関しては、下記の表をご確認ください。

No	項目	内容
1	検査総数	検査総数（内、未閲覧数）です。
2	検出数	脆弱性検出数（内、未閲覧数）です。
3	判定数	検査結果を確認した結果、脆弱性と判断した数です。 レポート出力対象件数です。

2. Vexが検出した検査項目を確認します。

脆弱性を検出している場合は「検出数」のリンクをクリックし、Server Settings検査で検出した脆弱性の一覧を表示します。



MEMO

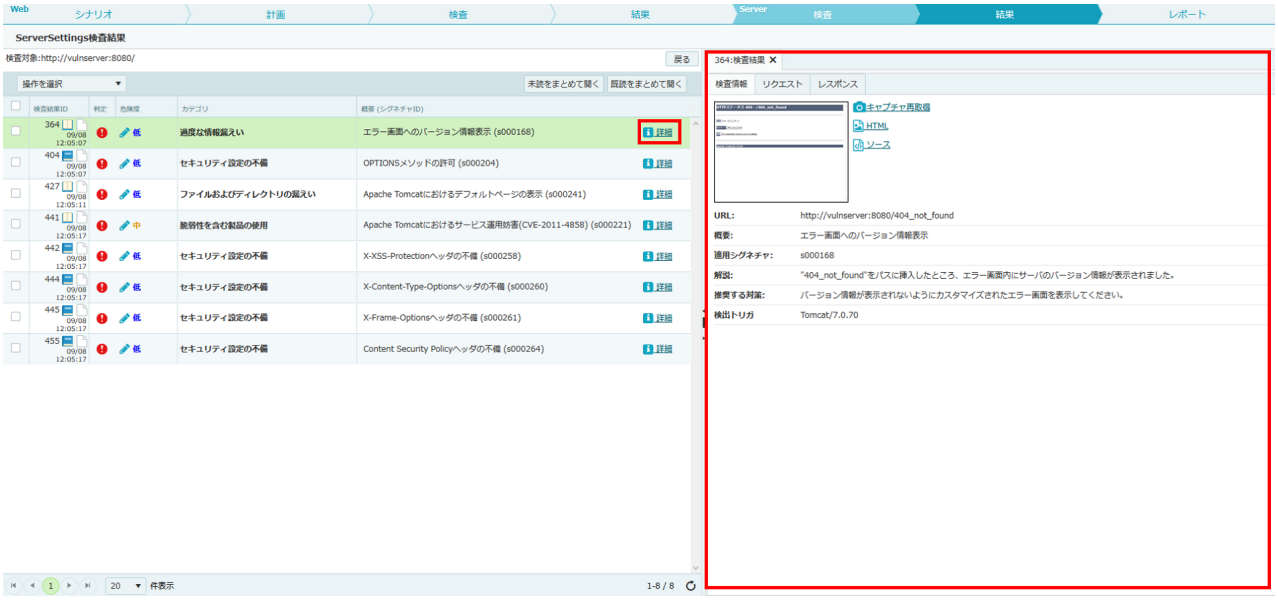
・Server Settings検査結果画面は、左右2つに分かれています。
　左ペイン：「Server Settings検査結果一覧」
　右ペイン：「Server Settings検査結果詳細」

「Server Settings検査結果一覧」の表示内容を確認します。

No	アイコン	項目	内容
1	ー	検査結果ID	実行された各検査の情報を管理するIDです。
2		HTML表示	検査時のレスポンスをブラウザ画面で表示します。 Server Settings検査結果詳細を未確認の状態の場合 が表示され、確認後はが表示されます。 確認がされていない検出項目を容易に認識するための機能です。
3		メモ	判定結果を変更した理由などを残しておくと便利です。
4	ー	カテゴリ	脆弱性種別です。
5	ー	パス	脆弱性を検出したパスです。
6		判定	検出の場合が表示されます。 クリックするとに変更され、検出対象から外れます。

No	アイコン	項目	内容
7		危険度	検出した各脆弱性の危険度です。 「緊急」「高」「中」「低」「情報」の5種類に分けられており、クリックすると、任意の危険度への変更が可能です。
8	ー	検出トリガ	脆弱性を検出した際に、脆弱性が存在すると判定した文字列です。
9		詳細	右ペインに「Server Settings検査結果詳細」を表示します。

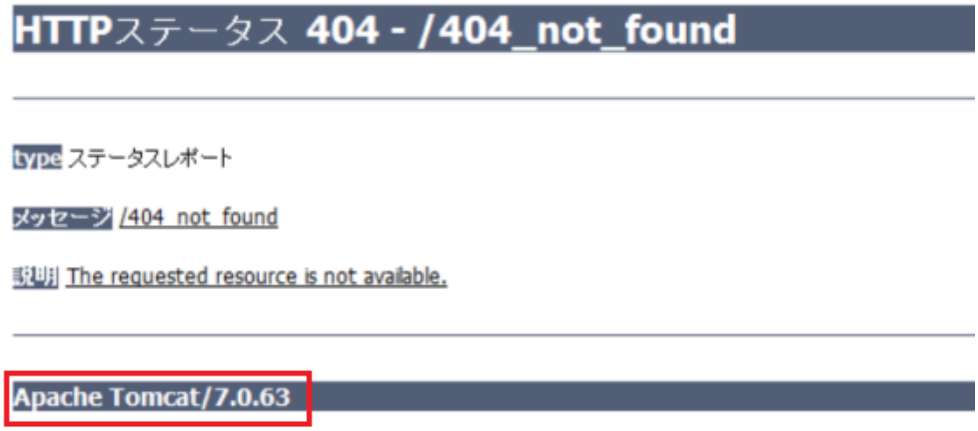
詳細を確認したい検出項目の「詳細」アイコンをクリックし、「Server Settings検査結果詳細」を右ペインに表示します。



実際に検査実施時のリクエスト、およびレスポンス情報を閲覧することが出来ます。

タブ構成で「検査情報」「リクエスト」「レスポンス」の表示の切替えが可能です。

画面キャプチャをクリックすると、大きな画像を表示します。



上記の例では、レスポンス画面内にサーバの製品情報が確認出来ます。

MEMO

Server Settingsで検出する内容には以下のような項目があります。
・ バナー情報の公開やサーバの設定によるシステム情報の漏えいの危険性
・ 使用しているプロダクトに存在する公開済の脆弱性

4.2.6. 手順⑥ レポート出力

4.2.6.1. レポート出力設定

1. フローバーの「レポート」ボタンをクリックします。

   初めてアクセスすると、「レポート出力設定」画面がポップアップで開きます。

   本画面では、レポートに記載する可変情報を登録します。

MEMO

- 「レポート定義情報」の入力項目は、ご利用のライセンスのエディションにより異なります。

2. レポート出力情報を設定します。

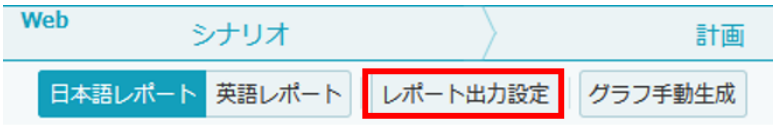
「レポート定義情報」の必須入力項目を入力し、レポートに掲載する項目を、「出力内容のカスタマイズ」から選択します。

「出力内容のカスタマイズ」にて選択可能な項目は以下の通りです。

No	項目	内容
1	画面キャプチャ	レポートに画面キャプチャを出力するか否かを設定します。
2	脆弱性毎の検出結果	検査対象メッセージ及び、ホストで検出された脆弱性を検出シグネチャ毎に出力するか否かを設定します。
3	リクエスト毎の脆弱性検出結果	検査対象メッセージで検出された脆弱性を検査対象リクエスト毎に出力するか否かを設定します。
4	ホスト別の脆弱性検出結果	検査対象ホストに対するServer検査で検出された脆弱性をホスト毎に出力するか否かを設定します。
5	検査対象リクエスト詳細情報	全ての検査対象メッセージの詳細情報（画面キャプチャ、送信パラメーター一覧）を出力するか否かを設定します。
6	脆弱性詳細解説ページ	検出された脆弱性の一般的な解説のページを出力するか否かを設定します。
7	付録	Web検査、Server Files検査、Server Settings検査それぞれの検査実行時間、検査総数の情報が出力されます。 検査実行時間は、30分以内の連続した検査時間を計測します。 Web検査実行時に選択したシグネチャIDの一覧が出力されます。
8	テスト結果チェックリスト	チェックリスト(xls)を分割して出力します。 検査対象のリクエストが大量にある場合に使用します。

3. 「実行」ボタンをクリックし、設定を完了します。

設定内容を変更したい場合は、ツールバー「レポート設定出力」ボタンから変更可能です。



なお、「レポート出力設定」画面の「オプション」タブをクリックすると、その他カスタマイズが可能です。

「レポートのマージ」機能を使用すると、複数プロジェクトに分割した内容を一つのレポートに結合して出力することが可能です。

4.2.6.2. レポートの出力

1. レポートを出力します。

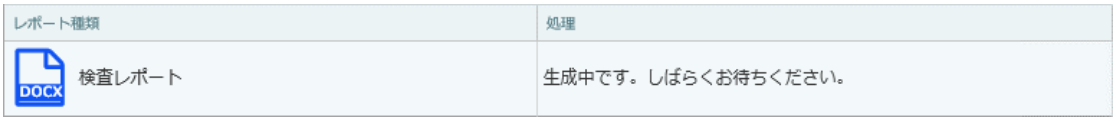
   「レポート出力設定」を完了すると、レポート出力が可能です。

   Vexには、様々なフォーマットでのレポートが用意されています。

No	レポート種別	説明
1	検査レポート（DOCX）	検査結果のレポートをDOCX形式で出力します。

No	レポート種別	説明
2	検査対象情報（CSV）	検査対象としてチェックされたメッセージ情報をURL、機能名、パラメータ数を保持したCSV ファイルとして出力します。
3	テスト結果 チェックリスト（XLS）	XLS チェックリスト形式でのレポートを出力します。
4	テスト結果 チェックリスト（CSV）	CSV チェックリスト形式でのレポートを出力します。
5	検査結果サマリシート（ZIP）	検査結果サマリ形式でのレポートを出力します。
6	「安全なウェブサイトの作り方」チェックリスト（ZIP）	IPAの「安全なウェブサイトの作り方」チェックリストに準拠したレポートを出力します。
7	OWASP TOP10 2017 レポート（DOCX）	OWASP TOP10 2017に準拠したレポートを出力します。
8	PCI DSS v3.2 レポート（DOCX）	PCI DSS v3.2に準拠したレポートを出力します。
9	Code Dx形式レポート（XML）	Code Dxにインポート可能なレポートを出力します。
10	ThreadFix形式レポート（JSON）	threaFixにインポート可能なレポートを出力します。

出力したいレポートの「レポート生成・ダウンロード」ボタンをクリックします。

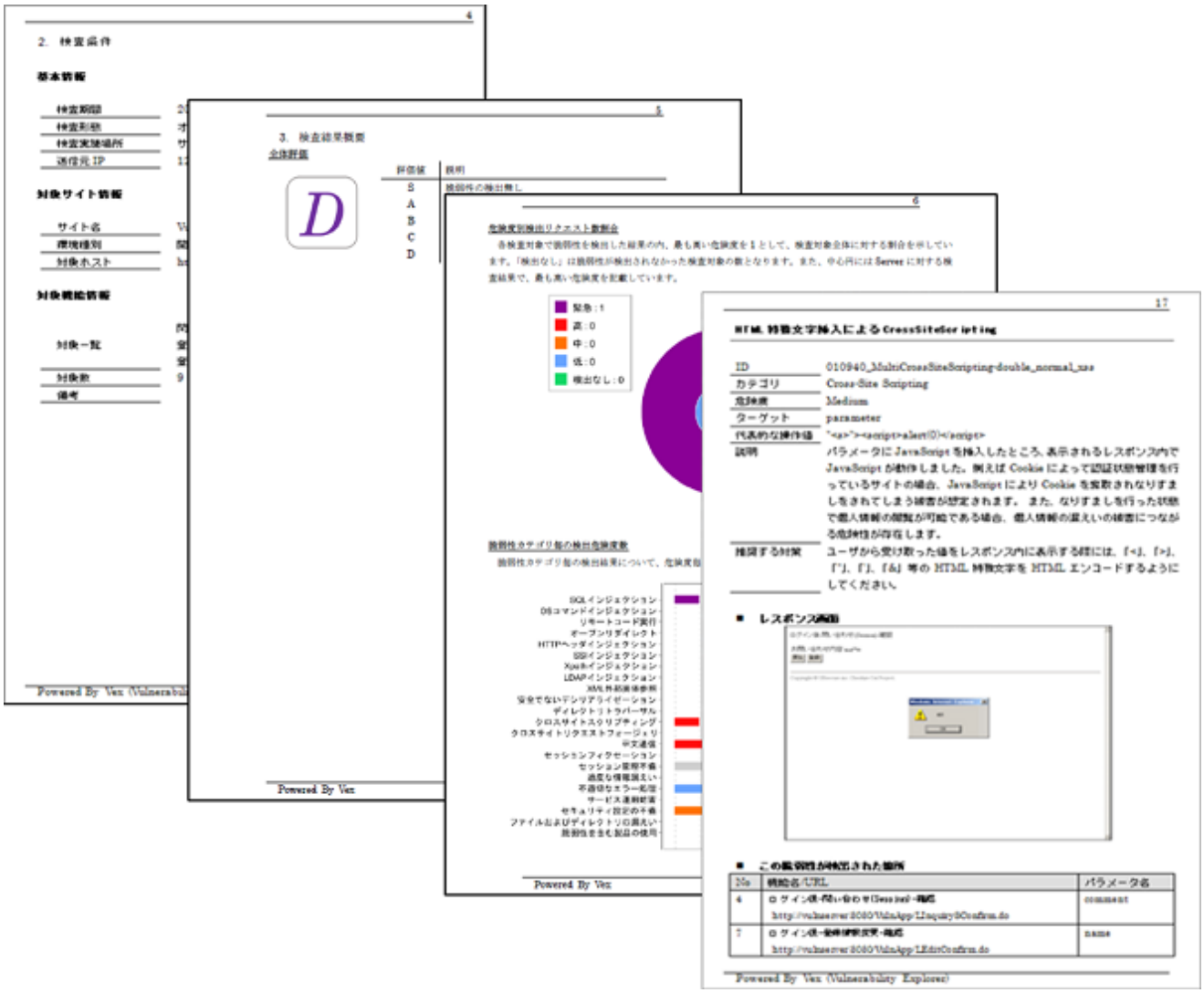


レポートが生成されると、「生成済レポートのダウンロード」ボタンが表示されましたら、レポートをダウンロードします。

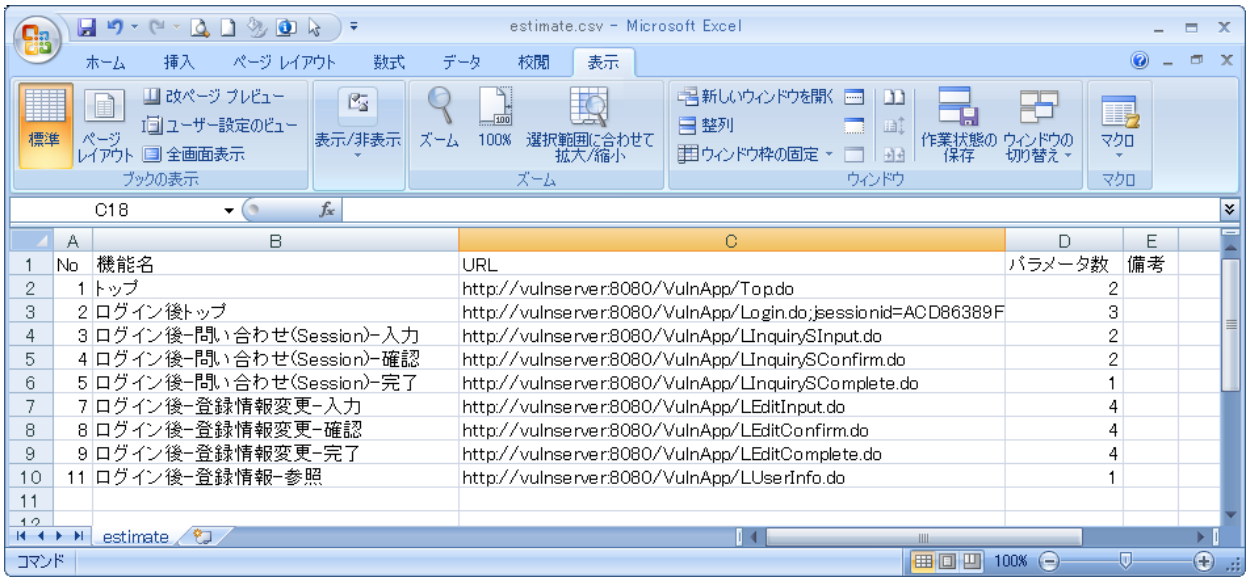
MEMO

- 検査対象数や検出数により、検査レポートの出力に数分かかる場合があります。
- レポート生成中は、別の画面の閲覧が可能です。
- 各レポートは、日本語と英語で出力可能です。

検査レポート（DOCX）



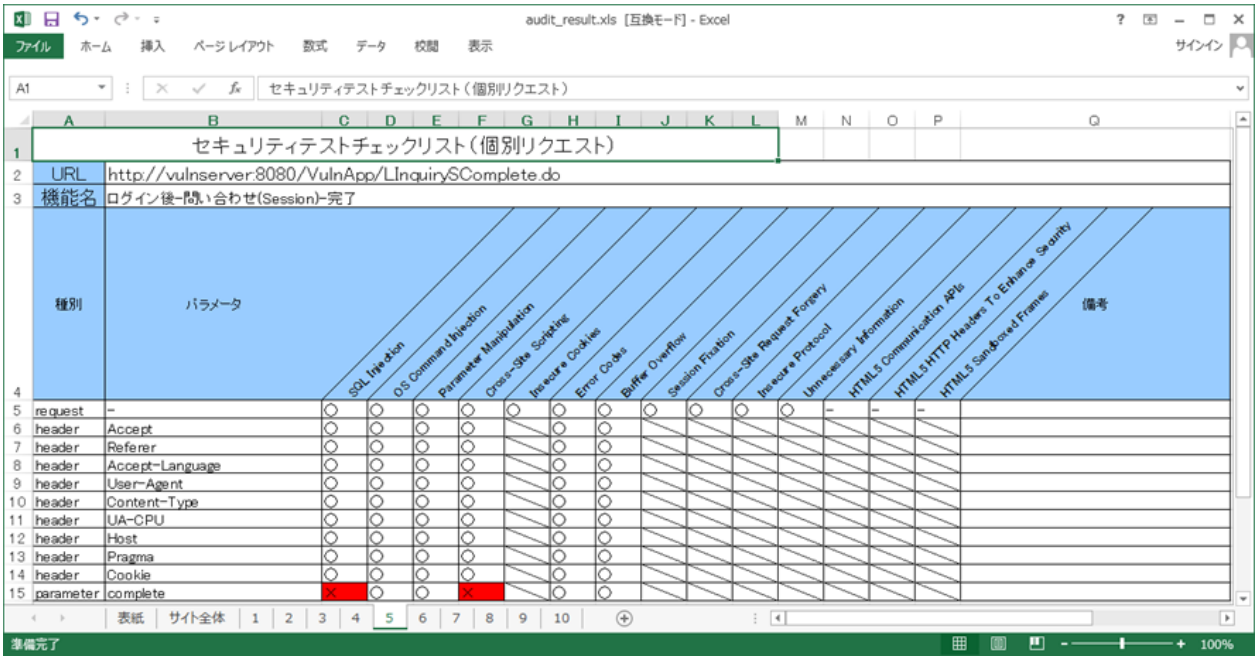
検査対象情報（CSV）



estimate.csv - Microsoft Excel

No	機能名	URL	パラメータ数	備考
1	トップ	http://vulnserver:8080/VulnApp/Top.do	2	
2	ログイン後トップ	http://vulnserver:8080/VulnApp/Login.do;jsessionid=ACD86389F	3	
3	ログイン後-問い合わせ(Session)-入力	http://vulnserver:8080/VulnApp/LInquirySInput.do	2	
4	ログイン後-問い合わせ(Session)-確認	http://vulnserver:8080/VulnApp/LInquirySConfirm.do	2	
5	ログイン後-問い合わせ(Session)-完了	http://vulnserver:8080/VulnApp/LInquirySComplete.do	1	
7	ログイン後-登録情報変更-入力	http://vulnserver:8080/VulnApp/LEditInput.do	4	
8	ログイン後-登録情報変更-確認	http://vulnserver:8080/VulnApp/LEditConfirm.do	4	
9	ログイン後-登録情報変更-完了	http://vulnserver:8080/VulnApp/LEditComplete.do	4	
11	ログイン後-登録情報-参照	http://vulnserver:8080/VulnApp/LUserInfo.do	1	

テスト結果チェックリスト（XLS）



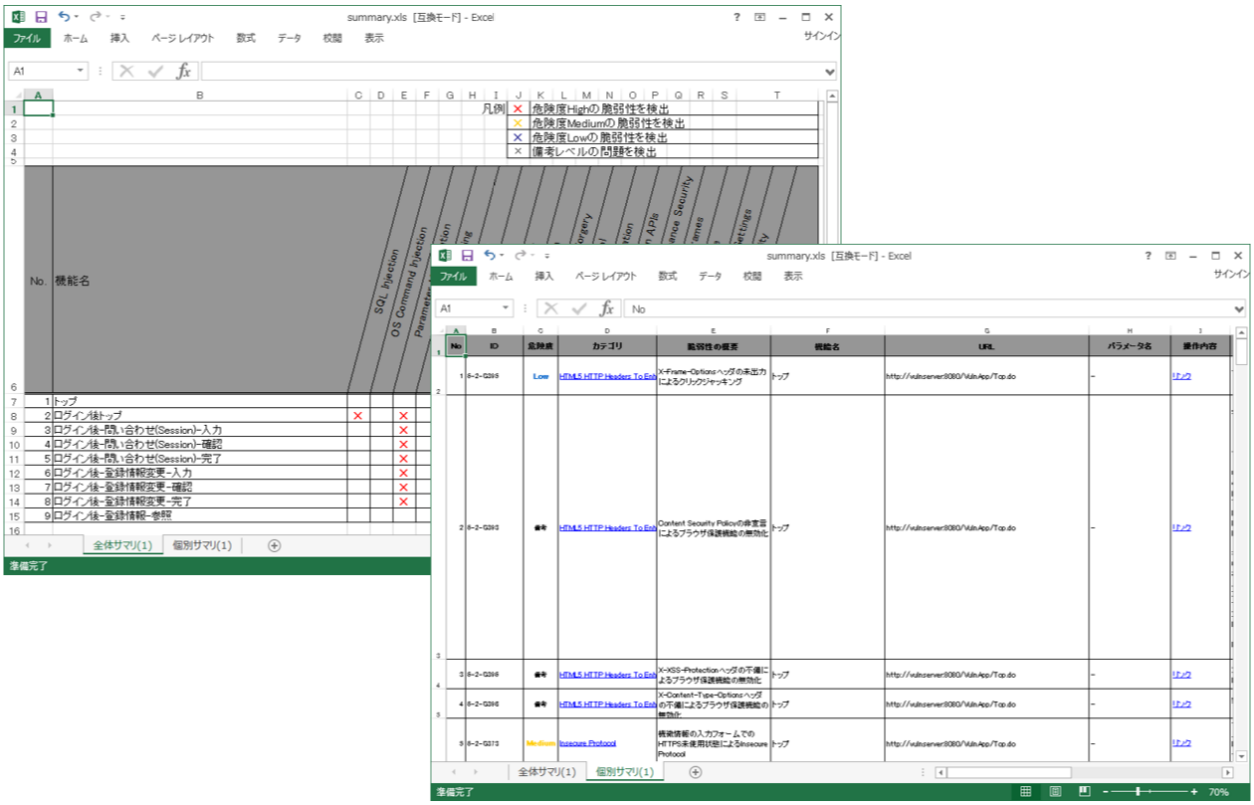
audit_result.xls [互換モード] - Excel

セキュリティテストチェックリスト（個別リクエスト）

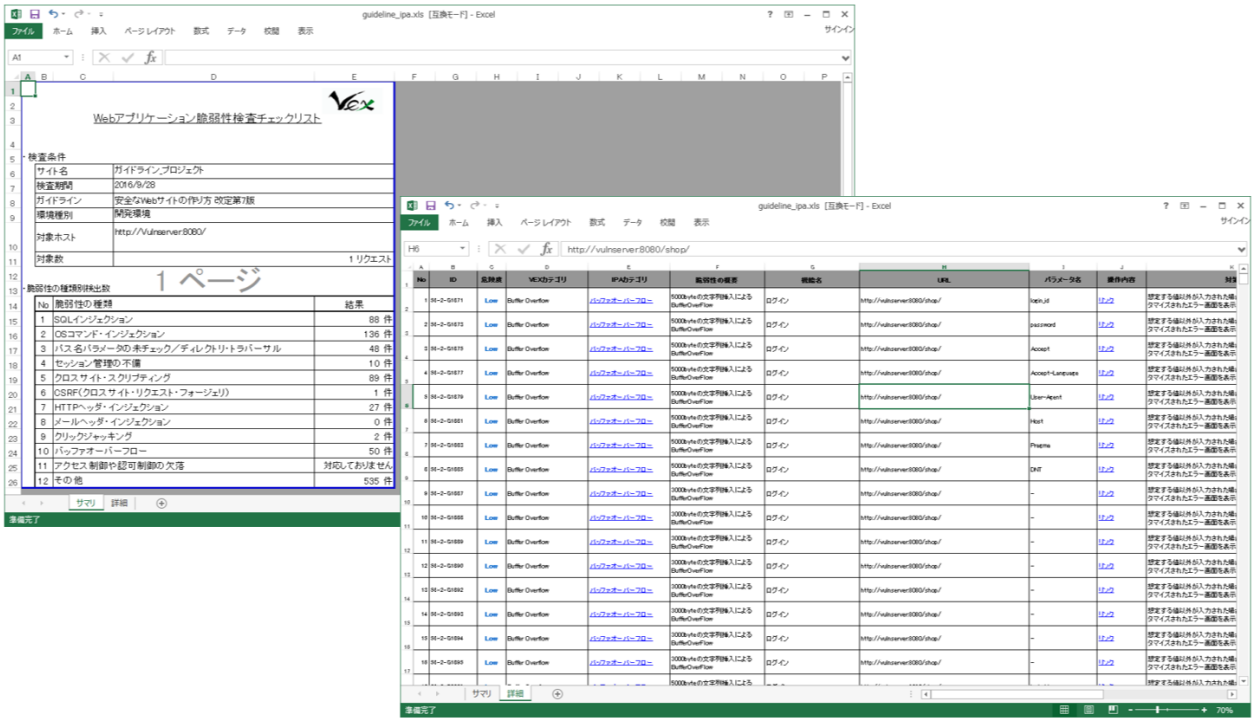
URL	http://vulnserver:8080/VulnApp/LInquirySComplete.do
機能名	ログイン後-問い合わせ(Session)-完了

種別	パラメータ	SQL Injection	OS Command Injection	Parameter Manipulation	Cross-Site Scripting	Insecure Cookies	Error Codes	Buffer Overflow	Session Fixation	Cross-Site Request Forgery	Insecure Protocol	Unnecessary Information	HTML5 Communication APIs	HTML5 HTTP Headers To Enhance Security	HTML5 Sandboxed Frames	備考
request	-	○	○	○	○	○	○	○	○	○	○	-	-	-		
header	Accept	○	○	○	○		○	○								
header	Referer	○	○	○	○		○	○								
header	Accept-Language	○	○	○	○		○	○								
header	User-Agent	○	○	○	○		○	○								
header	Content-Type	○	○	○	○		○	○								
header	UA-CPU	○	○	○	○		○	○								
header	Host	○	○	○	○		○	○								
header	Pragma	○	○	○	○		○	○								
header	Cookie	○	○	○	○		○	○								
parameter	complete	×	○	○	×		○	○								

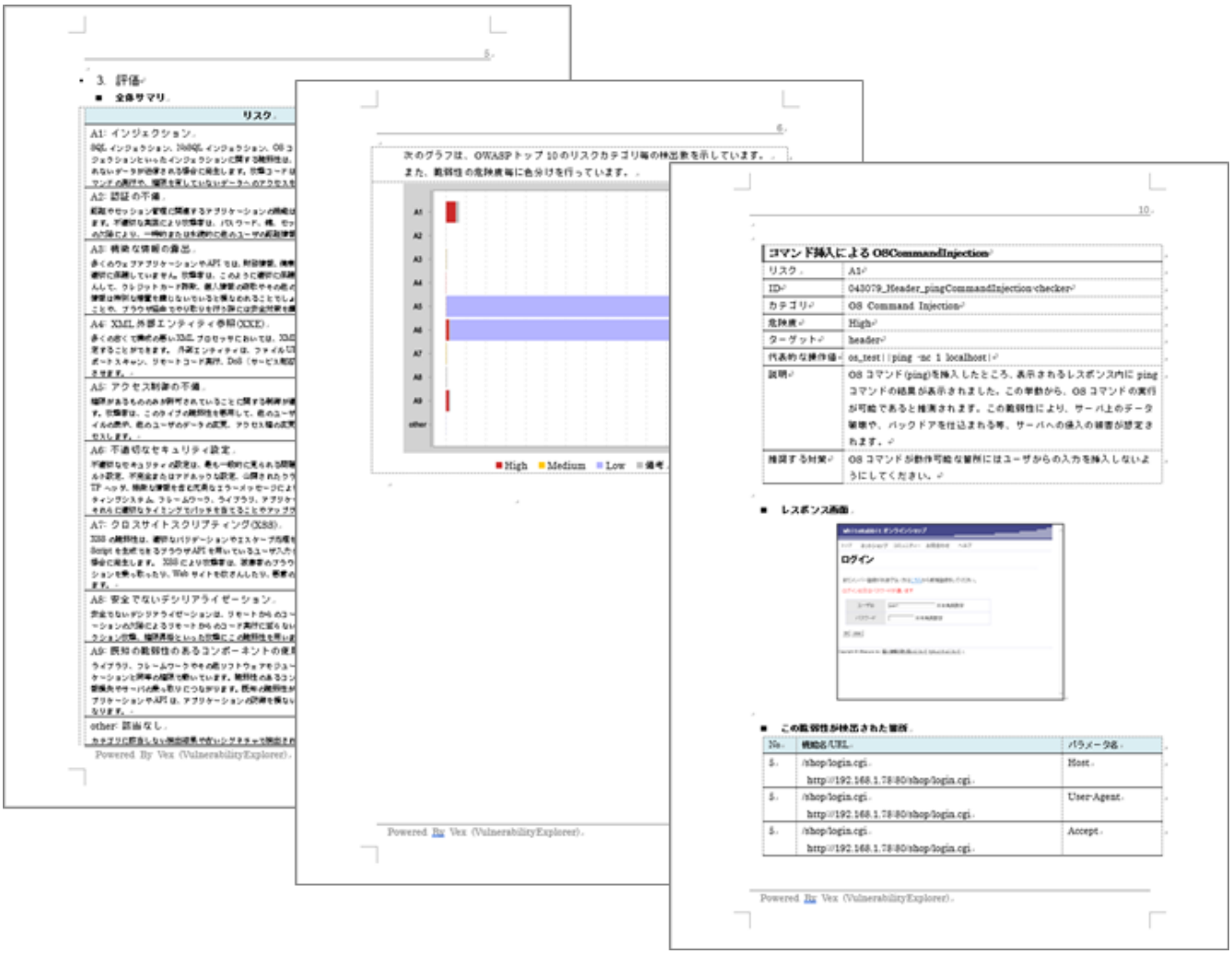
検査結果サマリシート（ZIP）



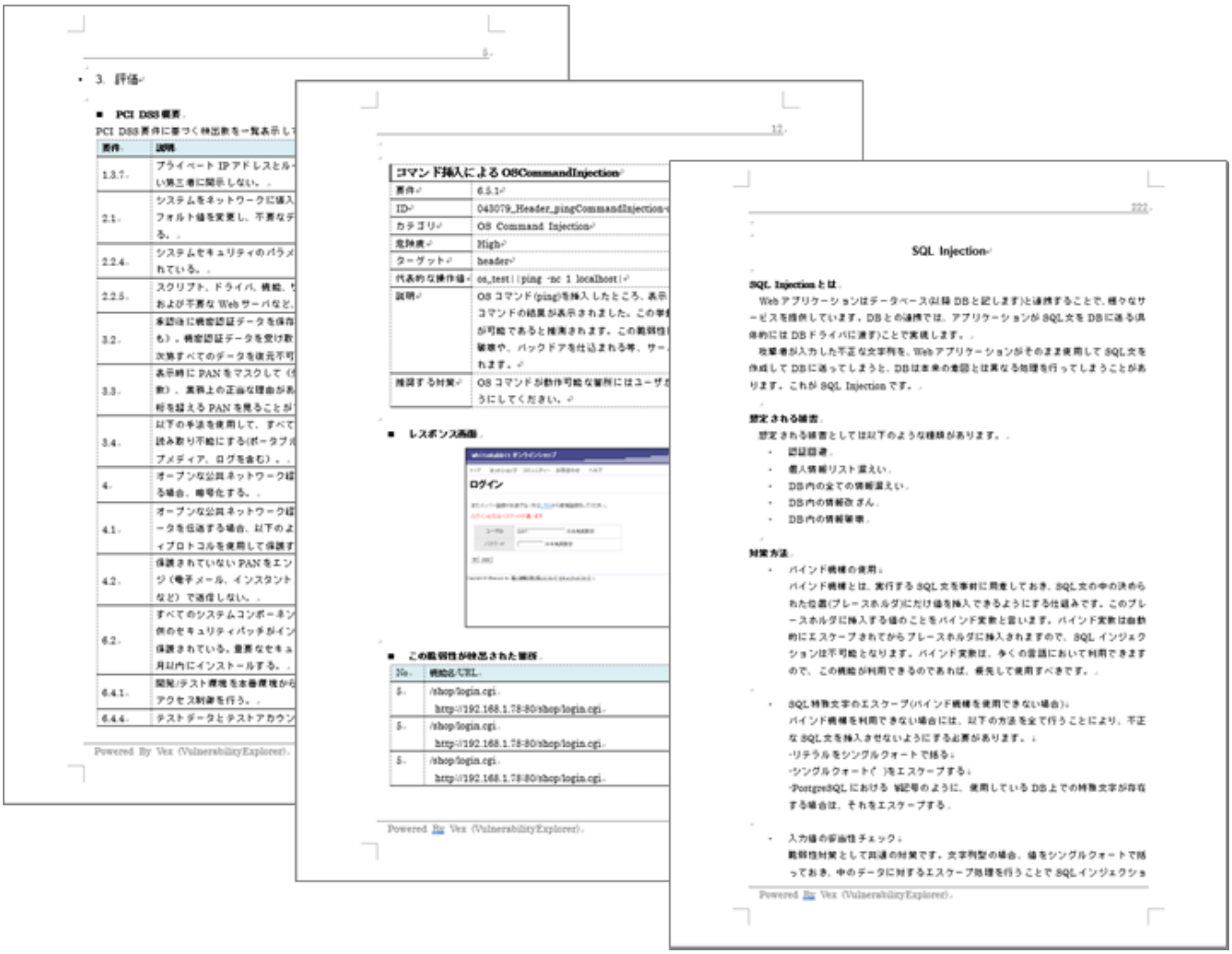
「安全なウェブサイトの作り方」チェックリスト（ZIP）



OWASP TOP10 2017 レポート（DOCX）



PCI DSS v3.2 レポート（DOCX）



4.2.6.3. レポート言語

各レポートは、日本語と英語で出力可能です。

4.2.6.3.1. [1] 英語レポートについて

・ Vex5.0.0以降の以下Web検査シグネチャ（互換性を維持するためのもの以外）は、英語で出力されます。

「網羅用(全てのシグネチャを適用します。 2014/01/31)」

・ Vex5.0.0以降の以下Server検査のシグネチャは、英語で出力されます。

「2014年01月版（高負荷シグネチャ含）通常版に負荷のかかる検査項目を含みます。」

・ Vex5.0.0以降で作成したプロジェクトのみ出力可能です。

※Vex5.0.0未満で作成したプロジェクトは未対応です。

・ Android 静的解析オプションは未対応です。

マイナーバージョンアップ時の英語化ポリシー

・ シグネチャが新規に追加された場合は、英語化されます。

・ 互換性を維持するためのシグネチャ（既に英語化されている）は、そのまま維持されます。

4.2.6.3.2. [2] 入力項目

以下の項目は、フォームから入力した文章がそのままレポートに出力されます。入力する際は、出力するレポートに合わせた言語で入力してください。

・「脆弱性基本情報変更」画面で脆弱性情報をカスタマイズする場合の、解説、対策

・レポート用設定

・カスタムシグネチャ

5. 他社商標について

下記の他社登録商標・商標をはじめ、マニュアル等に記載されている会社名、システム名、製品名は一般に各社の登録商標または商標です。なお、本文および図表中では、「™」、「®」は明記しておりません。

Java 及びすべてのJava関連の商標及びロゴは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標または商標です。

JDKは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標または商標です。

iPad、iOSは、米国および他の国々で登録されたApple Inc.の商標です。

Macは、米国および他の国々で登録されたApple Inc.の商標です。

Mac OSは、米国および他の国々で登録されたApple Inc.の商標です。

Microsoftは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Excelは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Internet Explorerは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Internet Information Serverは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Officeは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Microsoft Wordは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Safariは、米国および他の国々で登録されたApple Inc.の商標です。

Windowsは、米国およびその他の国における米国Microsoft Corporationの登録商標です。

Windows Serverは、米国およびその他の国における米国Microsoft Corporationの商標です。

Windows NTは、米国およびその他の国における米国Microsoft Corporationの登録商標です。

Windows 10、Windows 8.1、Windows 8、Windows 7、Active Directory、Internet Explorerは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

Apache、Tomcatは、Apache Software Foundationの登録商標または商標です。

PostgreSQLは、PostgreSQLの米国およびその他の国における商標です。

Android™、AndroidロゴはGoogle Inc. の登録商標です。

OWASPは、OWASP財団の登録商標です。

PCI DSS（Payment Card Industry Data Security Standard）は、PCI Security Standards Councilの商標です。