Web アプリケーション スキャン

入門ガイド

August 2, 2024

Qualys, Inc.

919 E Hillsdale Blvd

4th Floor

Foster City, CA 94404

1 (650) 801 6100

Table of Contents

WAS へようこそ 5

はじめに 8

さあ始めましょう！ 8

ウェブアプリの設定を追加する 8

ウェブアプリの設定を追加する 10

ダッシュボードから最新のセキュリティス状況を取得する 12

検出の管理 13

Selenium スクリプトを使用したスキャン 14

最初にディスカバリースキャンをお勧めします 14

次の脆弱性スキャン 17

Tip -スキャンを自動的に実行するようにスケジュールする 22

ダッシュボードから最新のセキュリティ状態を取得する 23

カタログについて教えてください 25

検出の管理 26

Burp の結果をインポートしたいですか? 26

Bugcrowd との統合 27

フルスキャンを起動せずに複数の検出結果を再テストする 28

認証のテスト 28

Web アプリケーションの大量スキャン 29

Selenium スクリプトを使用したスキャン 30

仮想パッチのサポート 31

レポート 32

レポート作成手順 32

Web アプリケーションのサンプルレポート 34

スコアカードレポートのサンプル 35

Tips & Tricks 36

カスタマイズ可能なレポートテンプレート 38

スケジュールされたレポート 39
ユーザーの追加 40
ロール管理 43
よくある質問(FAQ) 46
WAS モジュールにアクセスできないのはなぜですか? 46
ヘルプの取得 48

WAS へようこそ

Qualys Web Application Scanning (WAS) は、攻撃者を寄せつけず、Web アプリケーションを安全に保つために必要な使いやすさ、一元管理、統合機能を組織に提供します。Qualys WAS を使用すると、組織は Web アプリケーションの脆弱性を評価、追跡、修復できます。

Qualys WAS は、フォールトインジェクションテストを使用して脆弱性を見つける自動スキャナーです。特別に細工された文字列がアプリケーションフォームフィールドに挿入されます。次に、WAS は Web アプリケーションからの応答を調べて、脆弱性の存在を判断します。送信された内容とアプリケーションがどのように応答したかは、WAS のレポート機能で確認できます。

主な特徴

- Web アプリケーション (イントラネット、インターネット) をクロールし、脆弱性をスキャン
- 柔軟なワークフローとレポート機能を備えた完全にインタラクティブな UI を提供
- Web アプリケーションによる機密データまたは秘密データの処理を特定する
- カスタマイズ： ブラック/ホワイトリスト、robots.txt、sitemap.xml など
- 一般的な認証スキームをサポート
- 推奨されるセキュリティコーディングの実践と構成を含むレポートを表示する

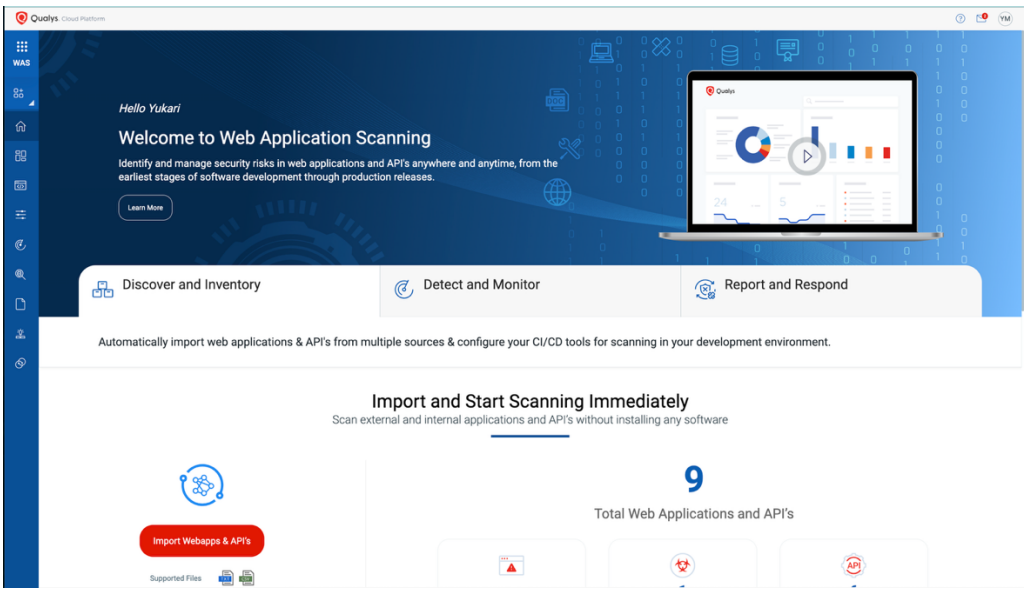
堅実でスケーラブルなスキャン機能

- JavaScript と組み込み Flash を使用した HTML Web アプリケーションのスキャンをサポート
- OWASP Top 10 Vulnerabilities を含むカスタム Web アプリケーションの脆弱性を包括的に検出
- 悪用可能なフォールト・インジェクションの問題と単純な情報漏えいを区別
- カスタム Web アプリケーションの動作をプロファイルする
- カスタマイズ可能なパフォーマンスレベルでスキャンパフォーマンスを構成

Qualys Cloud Platform - ユーザーにとってのメリット

Java ベースのバックエンドに実装された新しいテクノロジーは、ユーザーに多くのメリットをもたらします：

- 動的でインタラクティブなインターフェイス、ウィザード、新しいレポートテンプレートを備えた UI,スキャンデータを幅広いプレゼンテーションオプションで表示します。
- 統合ダッシュボード (UD) と WAS を統合。UD は、すべての Qualys アプリケーションからの情報を 1 か所にまとめて視覚化します。
- カスタマイズ可能なテンプレート駆動型レポートエンジンは、さまざまな形式(html、pdf、暗号化された pdf、ppt、xml、cvs)でレポートを出力します。
- 検索トークンを使用して、Web アプリケーション、検出、認証レコード、および構成 (オプション プロファイル、検索リスト、パラメーター セット) に関連するいくつかの広範な Qualys データセットを高速検索します。
- タグ (静的および動的) を作成および管理して、Web アプリケーションをグループ化および整理します。
- 可用性と負荷に基づいて複数のスキャナーにスキャンを動的に分散して、大規模なネットワークのスキャンを最適化し、大規模なスキャンジョブの完了に必要な全体的なスキャン時間を大幅に短縮します。



REST API スキャン、CI/CD 統合など

Swagger バージョン 2.0 をサポートしているため、DevOps チームは REST API の評価を合理化し、モバイル アプリケーション バックエンドとモノのインターネット (IoT) サービスのセキュリティ体制をより迅速に可視化できます。さらに、Jenkins 用の新しいネイティブ プラグインは、一般的な継続的インテグレーション/継続的デリバリー (CI/CD) ツールを使用して、チーム向けに Web アプリケーションの自動脆弱性スキャンを提供します。並行して、お客様は無料の Google Chrome ブラウザ拡張機能である新しい Qualys Browser Recorder を活用して、Web アプリケーションの複雑な認証やビジネスワークフローをナビゲートするためのスクリプトを簡単に確認できるようになりました。

- Swagger ベースの Representational State Transfer (REST) API のスキャン - Qualys WAS は、Simple Object Access Protocol (SOAP) Web サービスのスキャンに加えて、REST API のテストに Swagger 仕様を利用します。ユーザーは、Swagger バージョン 2.0 ファイル (JSON 形式) がスキャン サービスに表示されることを確認するだけで、API は一般的なアプリケーション セキュリティ上の欠陥について自動的にテストされます。
- Postman サポートによる強化された API スキャン - Postman は、REST API の機能テストに広く使用されているツールです。Postman コレクションは、関連するリクエスト (API エンドポイント) をまとめて他のユーザーと共有するツールからエクスポートできるファイルです。これらのコレクションは JSON 形式でエクスポートされます。Qualys WAS での Postman Collection サポートのリリースにより、お客様は API の Postman Collection を使用して API スキャンを構成するオプションを利用できます。
- Jenkins プラグイン - Qualys WAS Jenkins プラグインを使用すると、DevOps チームは既存の CI/CD プロセスにアプリケーションの脆弱性スキャンを組み込むことができます。この方法でスキャンを統合することで、アプリケーションセキュリティテストが SDLC の早い段階で実行され、セキュリティ上の欠陥を検出して排除するため、SDLC の後半で行う場合と比較して修復コストが大幅に削減されます。プラグインのダウンロードはこちらから。
- Qualys ブラウザ レコーダー – この新しい Chrome 拡張機能を使用すると、ユーザーは Web ブラウザのアクティビティを記録し、繰り返し可能な自動テストのためにスクリプトを保存できます。スクリプトは Qualys WAS で再生されるため、スキャン エンジンは複雑な認証とビジネス ワークフローを正常にナビゲートできます。Qualys Browser Recorder 拡張機能は無料で、Chrome ウェブストアから(Qualys の顧客だけでなく)誰でも利用できます。

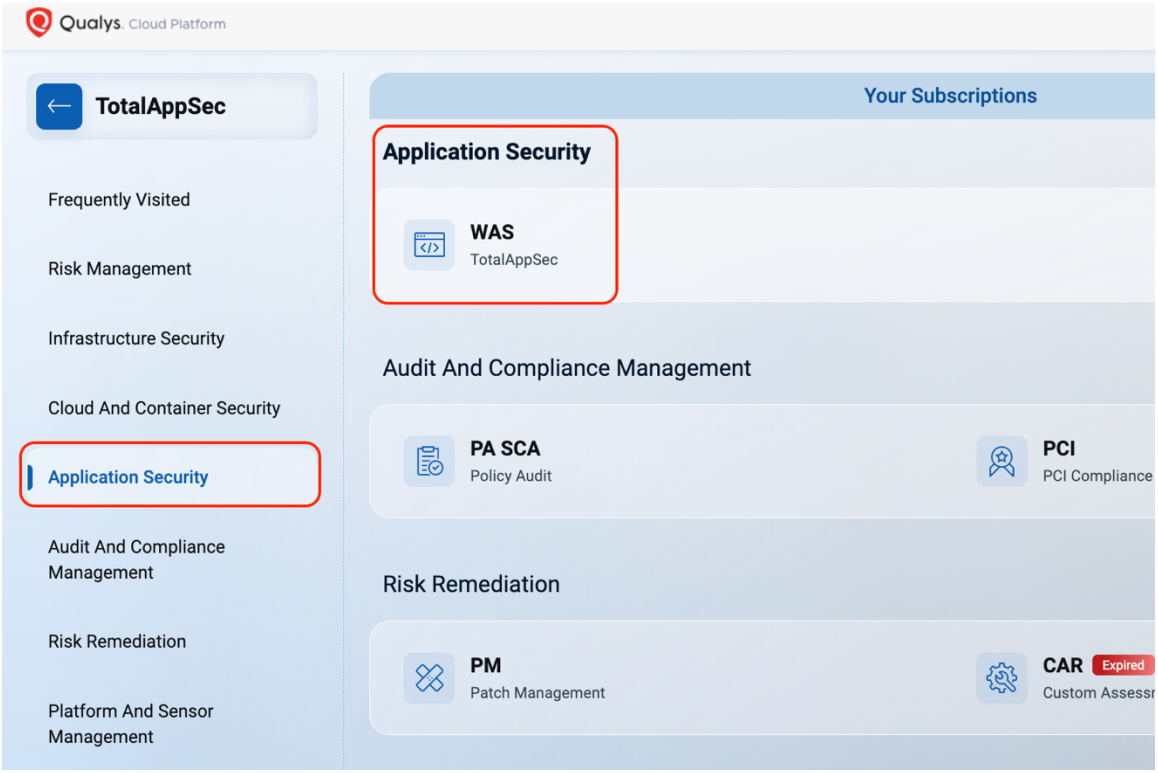
はじめに

Qualys WAS は、利用可能な最も強力な Web アプリケーションスキャナーです。

注: 新しい WAS UI は、Web アプリケーション、認証、オプション プロファイル、検索リスト、パラメータ セット、および検出機能のみをサポートします。このガイドでは、これらの機能の概要を説明します。詳細については、WAS オンライン ヘルプを参照してください。新しい WAS UI では使用できない機能については、クラシック WAS UI バージョンに移動します。

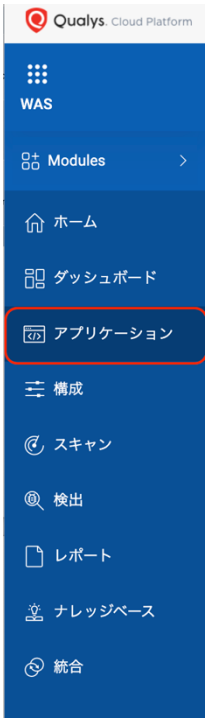
さあ始めましょう！

ログインして、アプリケーションピッカーから **Web アプリケーションスキャン** を選択します。　WAS の後継モジュール **TotalAppSec** が表示される場合はそちらを選択します。

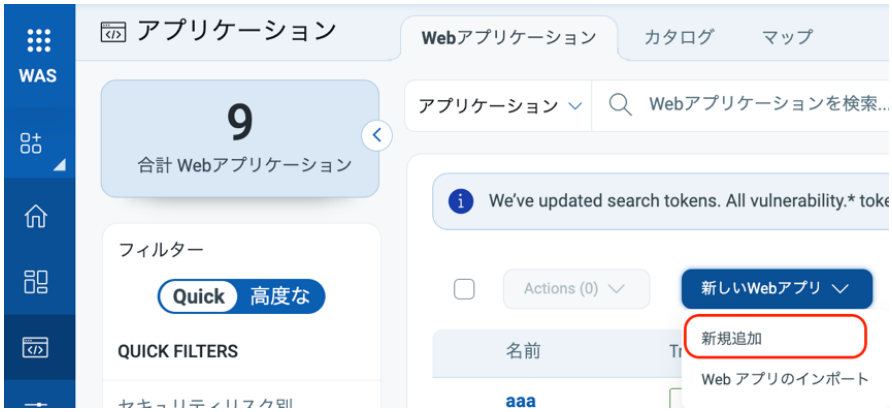


ウェブアプリの設定を追加する

WAS の View から**[アプリケーション]**を選択します。



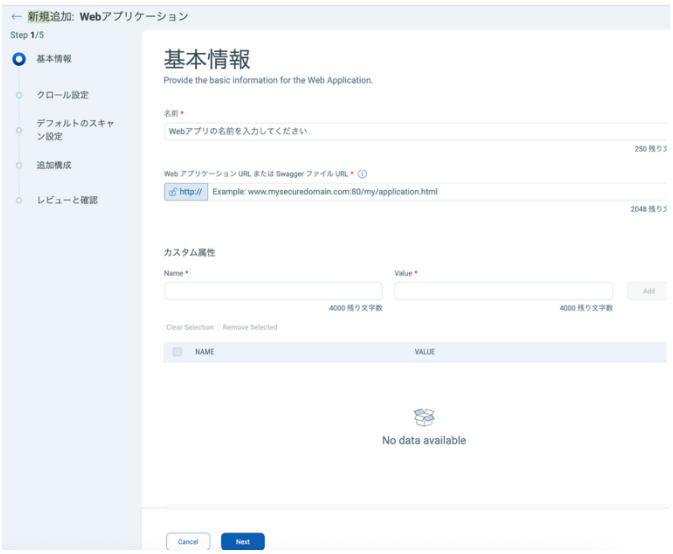
まず、スキャンする Web アプリケーションについてお知らせください - **[Web アプリケーション] > [新しい Web アプリ] > [新規追加]** をクリックします。



ウェブアプリの設定を追加する

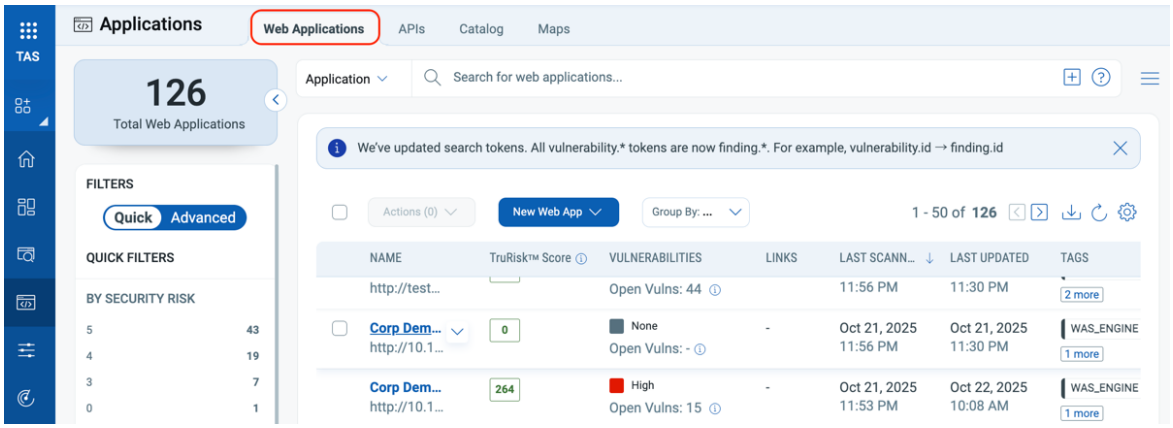
Web アプリケーション名と URL は、Web アプリを新規に追加する場合に必要です。

外部サイトをスキャンしてマルウェアを検出したいですか？ マルウェア監視をオンにするだけで、毎日自動的にマルウェアスキャンが実行されます。



ウェブアプリの設定を追加する

Web アプリケーションが **[Web アプリケーション]** タブに表示され、アプリケーション設定を編集したり、スキャンを起動したりできます。



認証を使用する理由

認証を使用すると、クロールプロセス中に Web アプリケーションのすべての部分にサービスがアクセスできるようになります。このようにして、Web アプリケーションのより詳細な評価を実行できます。一部の Web アプリケーションでは、その機能の大部分に対して認証されたアクセスが必要です。認証スキャンは、ログインページやサーバーベースの認証 **(HTTP Basic、Digest、NTLM、または SSL クライアント証明書)**などの HTML フォームに対して構成できます。**[認証] タブ**に移動し、**[新しいレコード]** を選択し、アクセス資格情報を使用して認証レコードを構成するだけです。フォーム認証とサーバー認証は必要に応じて組み合わせることができます - セッションの状態を監視して、認証されたスキャンがクロール全体を通して認証されたままであることを確認します。

認証の詳細を入力する必要がありますか?

この Web アプリケーションの機能にアクセスするには認証が必要ですか?「はい」の場合は、必ず認証レコードを選択してください。

オプションプロファイルについて教えてください

オプション・プロファイルは、スキャン構成オプションのセットです。開始するには**「イニシャル WAS オプション」**をお勧めします。プロファイルの編集オプションを使用すると、クロールおよびスキャンパラメータをカスタマイズできます。

Web アプリケーションに対するアクションの実行

[Quick Actions]メニューを使用して、個々のアプリケーションに対してアクションを実行します。Web アプリケーションを選択またはカーソルを合わせ、矢印をクリックして [Quick Actions] メニューのオプションを表示します。Quick Actions メニューを使用して、**Web アセットの詳細の表示、編集、Web アセットへのタグの追加と削除、Web アセットのスキャンデータのパージ**を行います。また、サブスクリプションおよびその他の関連モジュールから Web アセットを削除し、名前を付けて保存オプションを使用して、同じ構成で新しい Web アセットを作成することもできます。**[一括アクション] メニュー**を使用して、複数の Web アプリケーションに対してアクションを実行できます。

知っておきたいこと

どのような脆弱性チェックがテストされますか? スキャンを特定の脆弱性 (確認済み、潜在的、および/または収集された情報) に制限するようにオプション プロファイルを設定しない限り、ナレッジベースにリストされているすべての脆弱性チェック (QID) をスキャンします。新しいセキュリティ情報が利用可能になると、ナレッジベースを常に更新しています。トップメニューの **[ナレッジベース]** をクリックします。

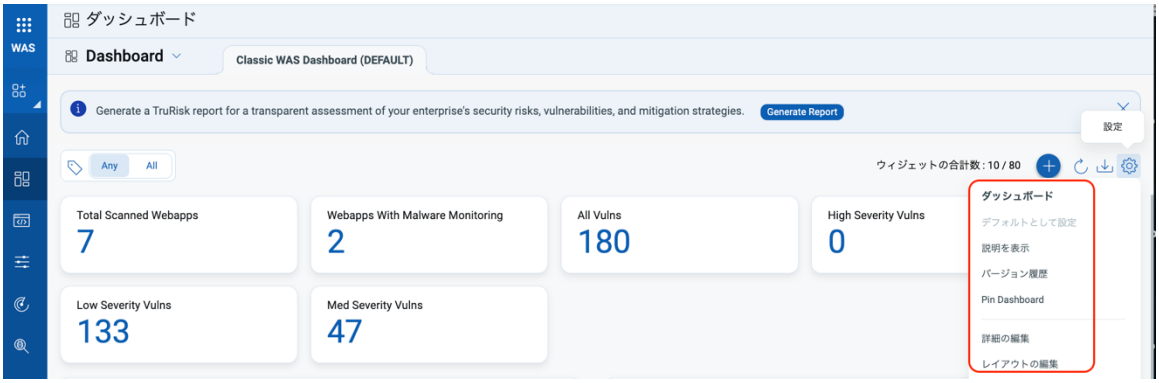
重大度とは何ですか? 各 QID には、当社のサービスによって重大度レベル (確認された脆弱性 (赤)、潜在的な脆弱性 (黄色)、収集された情報 (青) が割り当てられます。

ダッシュボードから最新のセキュリティス状況を取得する

ダッシュボードでは、セキュリティステータスが一目でわかり、常に最新の状態になります。ダッシュボードは、Web アプリケーションとその検出を視覚化するのに役立ちます。統合ダッシュボード (UD) を WAS と統合しました。UD は、すべての Qualys アプリケーションからの情報を 1 か所にまとめて視覚化します。UD は、既存のダッシュボード機能を強化するために、他のすべての製品で消費および使用されるプラットフォーム サービスとともに、強力な新しいダッシュボード フレームワークを提供します。

右上の歯車アイコンをクリックして、ダッシュボードを作成、編集、印刷します。検索クエリを含むウィジェットを追加して、興味のあるものを正確に確認するオプションもあります。また、ダッシュボードとウィジェットの設定を json 形式のファイルにエクスポートおよびインポートして、アカウント間または Qualys コミュニティ内で共有することもできます。

複数のダッシュボードを作成し、データのさまざまなビューに合わせてそれらを切り替えます。



「ウィジェット」メニューから、ウィジェットの編集、削除、複製、更新、およびエクスポートを行うことができます。ウィジェットからテンプレートを作成するオプションもあります。

ウィジェットの追加

1. まず、ダッシュボードの **[ウィジェットの追加]** ボタンをクリックします。
2. ウィジェットテンプレートの 1 つを選択するか、独自のテンプレートを作成します。
3. **右上の歯車アイコン**をクリックすると、メニューから構成を json 形式のファイルにインポートして、アカウント間または Qualys コミュニティ内でウィジェットを共有することもできます。

ヒント：

デフォルトのダッシュボードでウィジェットをどのように作成したのか気になりますか? **ウィジェットメニュー**を選択し**編集**を選択して設定を表示します。

検出の管理

すべての検出を 1 か所で管理します。**[検出] タブ**は、アプリケーション セキュリティの脆弱性の検出、管理、および情報の中心領域として機能します。すべての検出結果 (Qualys、Burp、Bugcrowd) が [検出] タブに一覧表示されます。

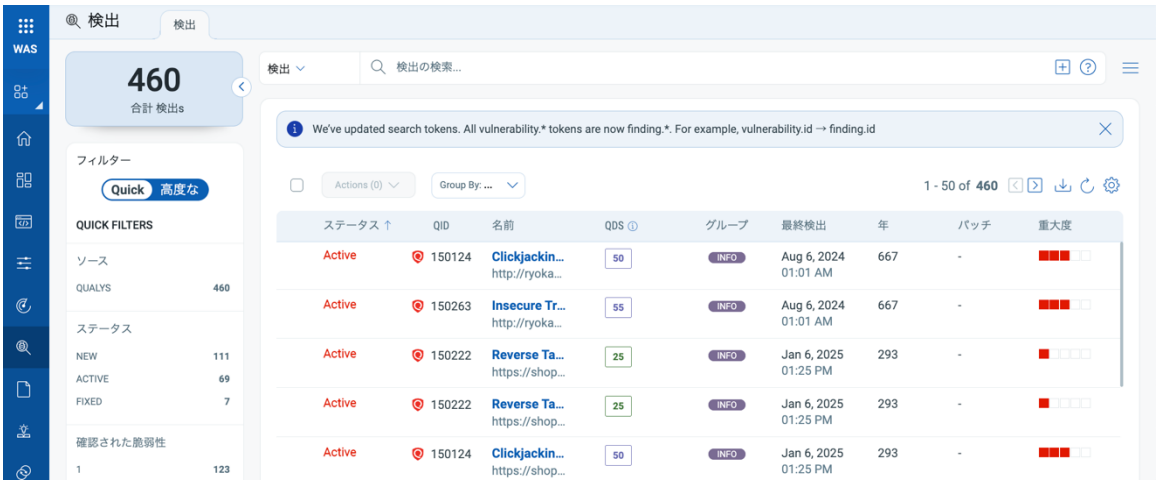
左側のペインには、検索を強化し、検出タイプをすばやく見つけるためのフィルターがあります。一般的なフィルターに加えて、検索トークンを使用して複雑な検索式を作成し、要件に固有の検出を見つけます。たとえば、10 日を超える経過時間の BURP 検出結果を表示するには、検索バーに vulnerability.source:"BURP" と vulnerability.age>10 という検索エクスプレスを入力します。

検出結果タイプは、リストに表示されるアイコンで区別できます。

- Qualys detections
- Burp issues

Scanning using Selenium scripts

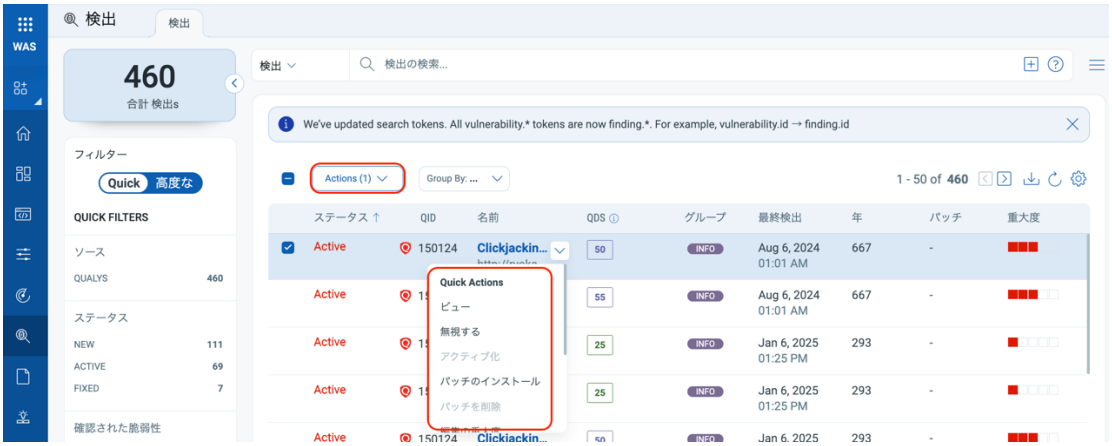
- Bugcrowd submissions



検出に対するアクションの実行

[Quick Actions] メニューを使用して、個々の検出に対してアクションを実行します 。検出を選択またはカーソルを合わせ、矢印をクリックして [Quick Actions] メニューのオプションを表示します。[Quick Actions] メニューを使用して、無視された検出を編集、無視、および再アクティブ化します。また、検出の重大度レベルを編集および復元したり、検出に

コメントを追加したりすることもできます。**[Actions] メニュー**を使用して、複数の検出に対してアクションを実行できます 。



Selenium スクリプトを使用したスキャン

Qualys Browser Recorder (QBR) を使用して、Selenium スクリプトを作成できます。QBR は、Web アプリケーション自動化テスト用のスクリプトを記録および再生するための無料のブラウザ拡張機能(Google Chrome ブラウザ用)です。QBR を使用すると、Web 要素をキャプチャし、ブラウザでアクションを記録できるため、自動テストケースをすばやく簡単に生成、編集、再生できます。また、ブラウザーの現在表示されているページから UI 要素を選択し、パラメーターを含む Selenium コマンドのリストから選択することもできます。これらのスクリプトを WAS で使用すると、スキャナーが Web アプリケーションの複雑な認証およびビジネスワークフローをナビゲートできます。

Web アプリケーションで使用される一般的な認証メカニズムは、シングル サインオン (SSO) です。これにより複雑になり、Qualys WAS を使用した認証とスキャンに関して混乱が生じる可能性があります。QBR を使用すると、スキャナーの認証メカニズムを簡素化できます。詳細な手順については、ブログ記事を参照してください。

スキャンとその潜在的な影響に関する警告 Web アプリケーション・スキャンは、テスト・データを含むフォームを送信します。これが望ましくない場合は、ブラックリスト、POST データブラックリストの設定を追加するか、オプションプロファイル内で GET のみの方法を選択する必要があります。これらの構成を使用する場合、Web アプリケーションの特定の領域のテストは含まれず、これらの領域に存在する脆弱性が検出されない可能性があることに注意してください。

最初にディスカバリースキャンをお勧めします

ディスカバリースキャンでは、脆弱性テストを実行せずに Web アプリケーションに関する情報が検出されます。これは、スキャンがどこに行くのか、脆弱性スキャンのためにブラッ

クリストに登録する必要がある URI があるかどうかを理解するための良い方法です。**[スキャン] > [スキャン リスト]** に移動し、**[新しいスキャン] > [デイスカバリースキャン]** をクリックします。

起動スキャンウィザードは、手順を順を追って説明します。

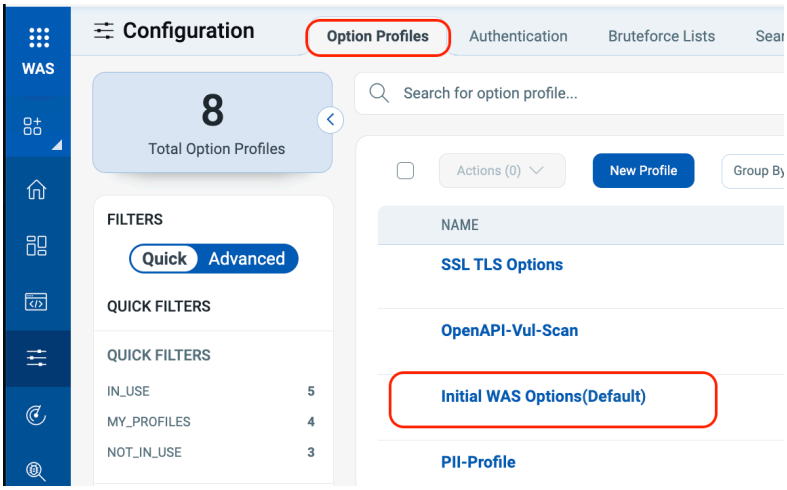
スキャンしたい Web アプリケーションをお知らせし、スキャン設定を選択します(*は必須という意味)。

スキャンを開始する準備はできましたか?

「続行」をクリックし、設定を確認してから、「完了」をクリックします。

オプションプロファイルについて教えてください

オプション・プロファイルは、スキャン構成オプションのセットです。開始するには「イニシャル WAS オプション」をお勧めします。プロファイルの編集オプションを使用すると、クロールおよびスキャンパラメータをカスタマイズできます。



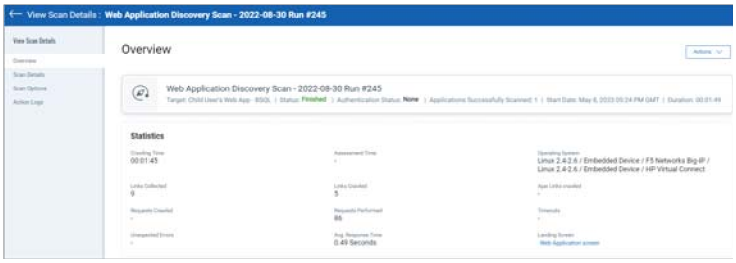
認証の詳細を入力する必要がありますか?

この Web アプリケーションの機能にアクセスするには認証が必要ですか?「はい」の場合は、必ず認証レコードを選択してください。

スキャナアプライアンスは必要ですか?

当社のセキュリティサービスは、**ネットワーク境界の外部スキャン用のクラウドスキャナーを提供します。内部スキャンの場合は、スキャナアプライアンス(物理または仮想)をセットアップする必要があります。[VM/VMDR] > [Scans] >]Appliances]** に移動し、**[新規]** メニューからオプションを選択すると、手順が説明されます。(Express Lite はありますか? アカウントは、外部スキャン、内部スキャン、またはその両方で有効になっている場合があります)。

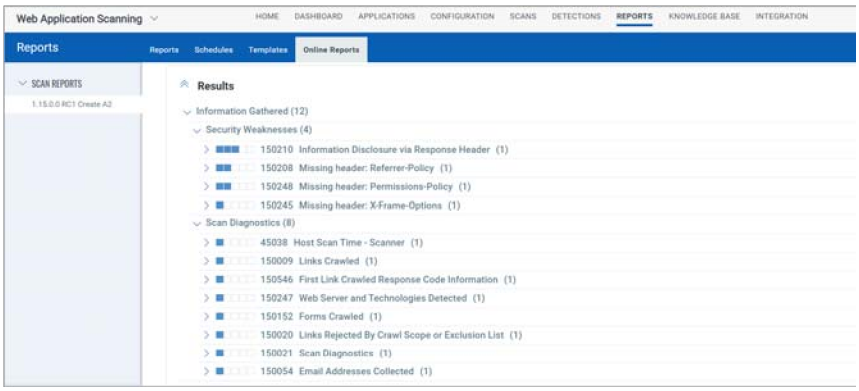
スキャンビュー



「Overview」には、スキャン結果の概要が表示されます。

完全なスキャンレポートを表示したいですか?[レポートの表示]ボタンをクリックするだけです。

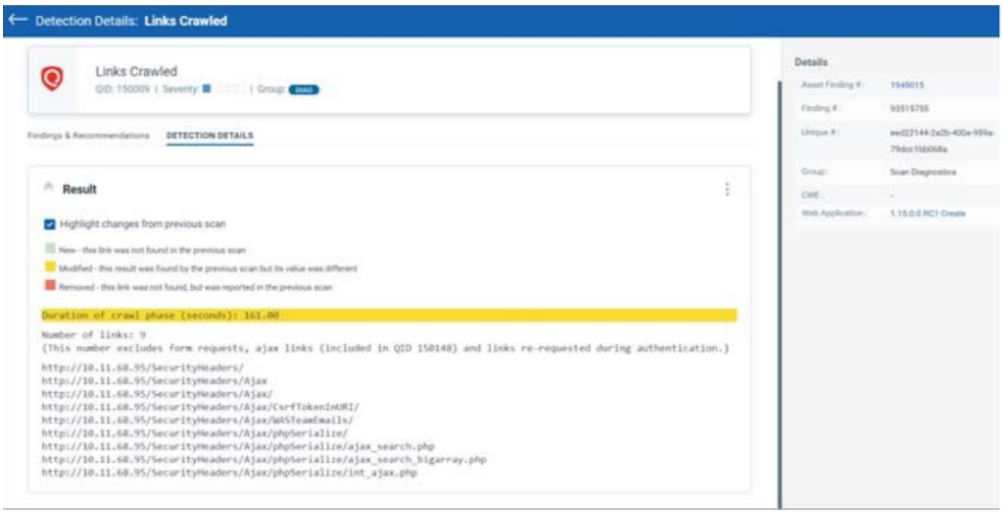
完全なスキャン レポート



各 QID は、私たちが実行し、情報を収集したセキュリティチェックです。行をクリックするだけで詳細が表示されます。

スキャンに関する重要なデータを確認するには、クロールされた QID 150009 リンクと QID 150021 スキャン診断を確認してください。

クロールされた QID 150009 リンク の結果が表示され、クロールされたリンクのリストが表示されます。



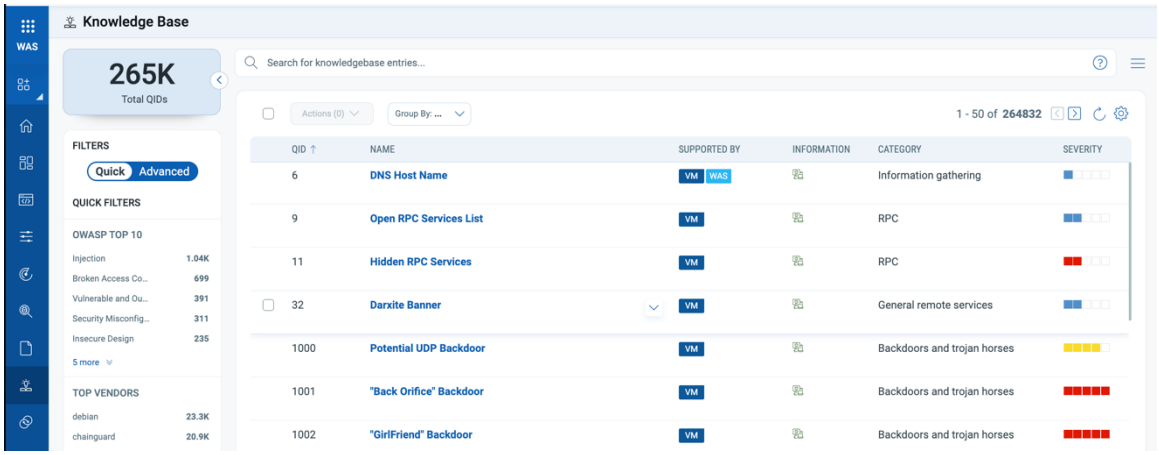
次の脆弱性スキャン

脆弱性スキャンでは、脆弱性チェックと機密コンテンツチェックを実行し、Web アプリケーションのセキュリティ状況を把握できます。

知っておきたいこと

どのような脆弱性チェックがテストされますか? スキャンを特定の脆弱性 (確認済み、潜在的、および/または収集された情報) に制限するようにオプション プロファイルを設定しない限り、ナレッジベースにリストされているすべての脆弱性チェック (QID) をスキャンします。新しいセキュリティ情報が利用可能になると、ナレッジベースを常に更新しています。

重大度とは何ですか?
各 QID には、当社のサービスによって重大度レベル (確認された脆弱性 (赤)、潜在的な脆弱性 (黄色)、収集された情報 (青) が割り当てられます。



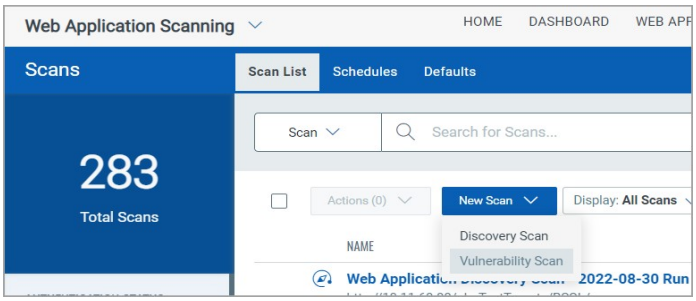
スキャンを開始する

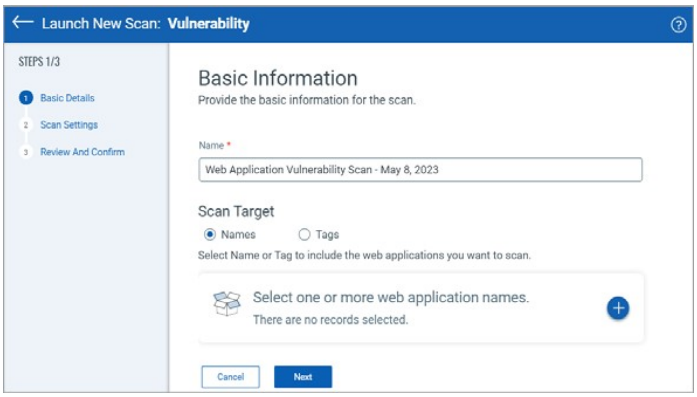
トップメニューの[スキャン]に移動し、[新しいスキャン]>[脆弱性スキャン]を選択します。

起動スキャンウィザードは、手順を順を追って説明します。

脆弱性をスキャンする Web アプリケーションを教えて、スキャン設定を選択してください。

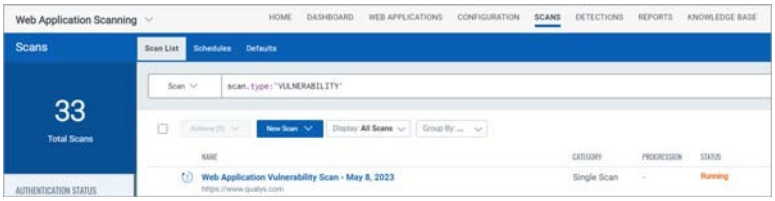
スキャンを開始する準備はできましたか?「続行」をクリックし、設定を確認してから、「完了」をクリックします。





スキャンの進行状況を確認する

ステータス列には、ステータス (この場合は実行中) が表示されます。



さらに詳しい情報が必要ですか?スキャン行をダブルクリックします。

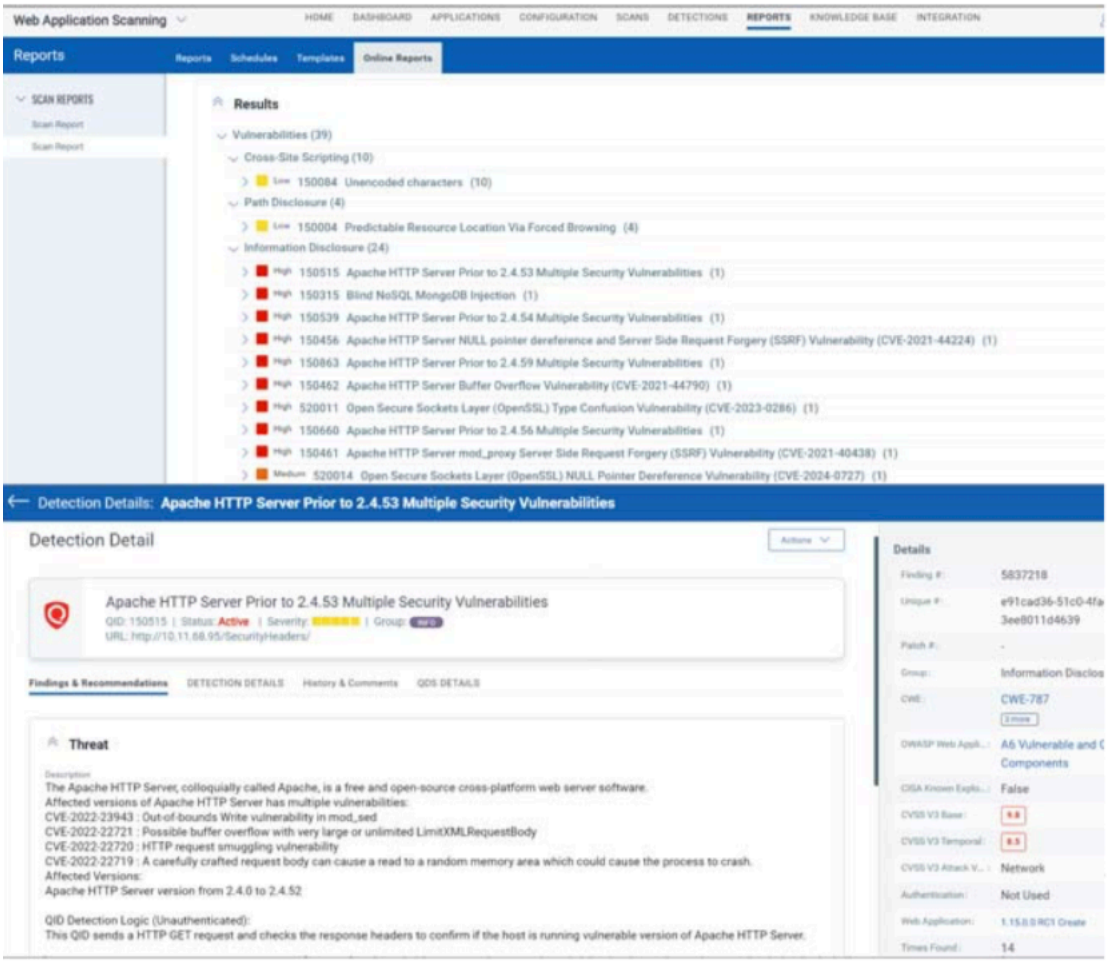
次に、スキャンの進行状況バーが表示されます - これにより、スキャンがいつ終了するかの推定値が表示されます。

スキャン表示

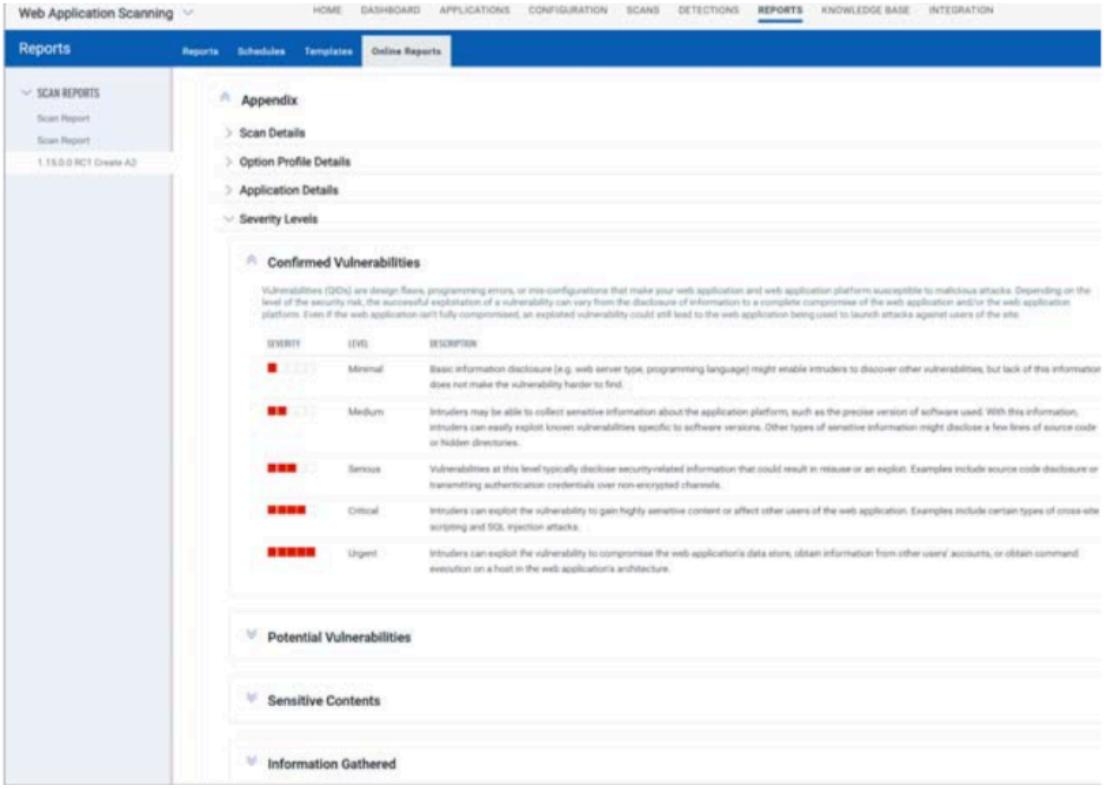
これをどのように見ればよいですか? スキャンにカーソルを合わせ、**[Quick Actions]** メニューから **[View]** を選択します。**[Overview]**には、スキャン結果の概要が表示されます。

フル スキャン レポート

完全なスキャンレポートを見たいですか? **[レポートの表示]** ボタンをクリックするだけです。脆弱性は、グループ別にソートされます。

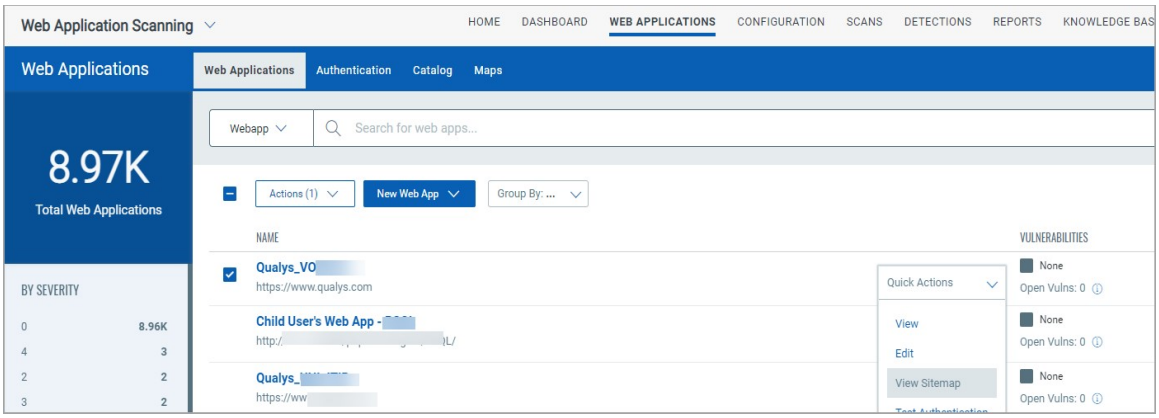


付録の重大度レベルの意味を簡単に確認できます。

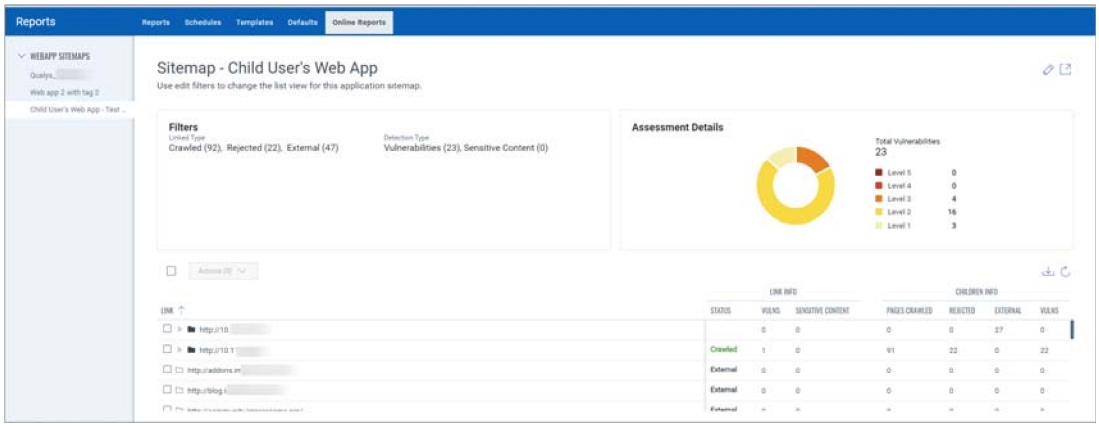


サイトマップを確認する

Web アプリケーションサイトマップを使用すると、クロールされたリンク、脆弱性、検出された機密コンテンツのビューでスキャンされたすべてのページ/リンクのリストを取得する便利な方法を提供します (Web アプリケーションに移動し、Web アプリを選択してから、**[Quick Actions]** メニューから **[サイトマップを表示]** を選択します)。



これは、クロールされた合計 271 ページ、合計 306 の脆弱性、8 つの機密コンテンツ検出がある Web アプリケーションのサンプル サイトマップです。



サイトマップをフィルタリングする

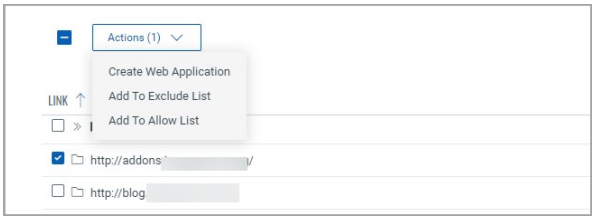
編集アイコンをクリックして、ページ・フィルターを表示します。たとえば、現在の脆弱性の脆弱性などです。

ドリルダウンして入れ子になったリンクを表示する

これにより、アプリケーションのさまざまな部分のセキュリティを調べることができます。親フォルダをダブルクリックして、子リンクを表示します。

Web アプリ リンクに対するアクションの実行

リンクから新しい Web アプリケーションを作成するか、ブラック リストまたはホワイト リストへのリンクを追加します。ブラウザでリンクを表示できます - その行を選択し、詳細パネル (右側) でリンクをクリックするだけです。

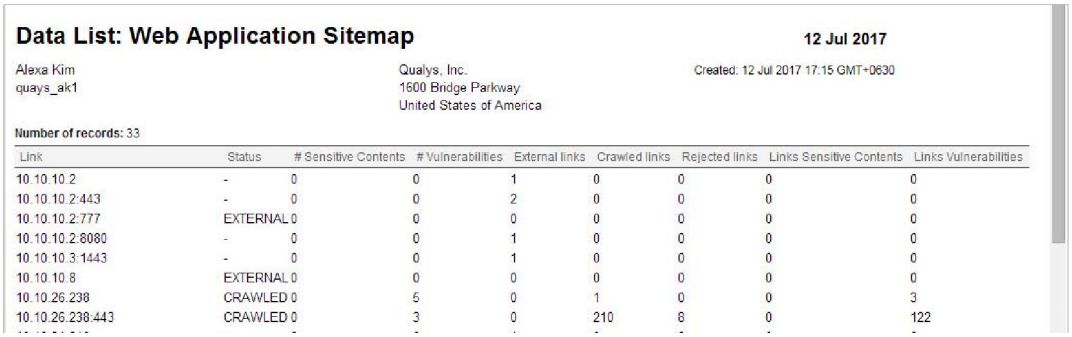


Web アプリのリンクを簡単にエクスポート

検出データでスキャンされたリンクを複数の形式でダウンロードします。

ヒント - スキャンを自動的に実行するようにスケジュールする

ダウンロードレポートには、リンクごとのスキャン結果が表示されます。



Data List: Web Application Sitemap

12 Jul 2017

Alexa Kim
quays_ak1

Qualys, Inc.
1600 Bridge Parkway
United States of America

Created: 12 Jul 2017 17:15 GMT+0630

Number of records: 33

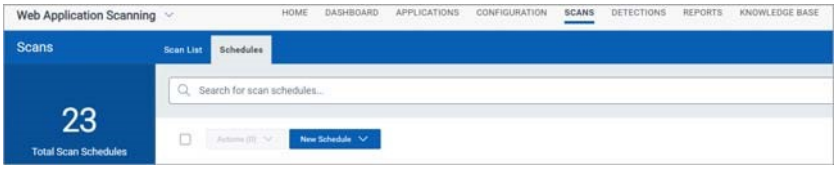
Link	Status	# Sensitive Contents	# Vulnerabilities	External links	Crawled links	Rejected links	Links Sensitive Contents	Links Vulnerabilities
10.10.10.2	-	0	0	1	0	0	0	0
10.10.10.2:443	-	0	0	2	0	0	0	0
10.10.10.2:777	EXTERNAL	0	0	0	0	0	0	0
10.10.10.2:8080	-	0	0	1	0	0	0	0
10.10.10.3:1443	-	0	0	1	0	0	0	0
10.10.10.8	EXTERNAL	0	0	0	0	0	0	0
10.10.26.238	CRAWLED	0	5	0	1	0	0	3
10.10.26.238:443	CRAWLED	0	3	0	210	8	0	122

Tip -スキャンを自動的に実行するようにスケジュールする

スキャンスケジュールを繰り返し実行するように設定することをお勧めします。これにより、組織にとって都合の良い時間枠内に、自動的に (毎日、毎週、または毎月) 結果が得られます。

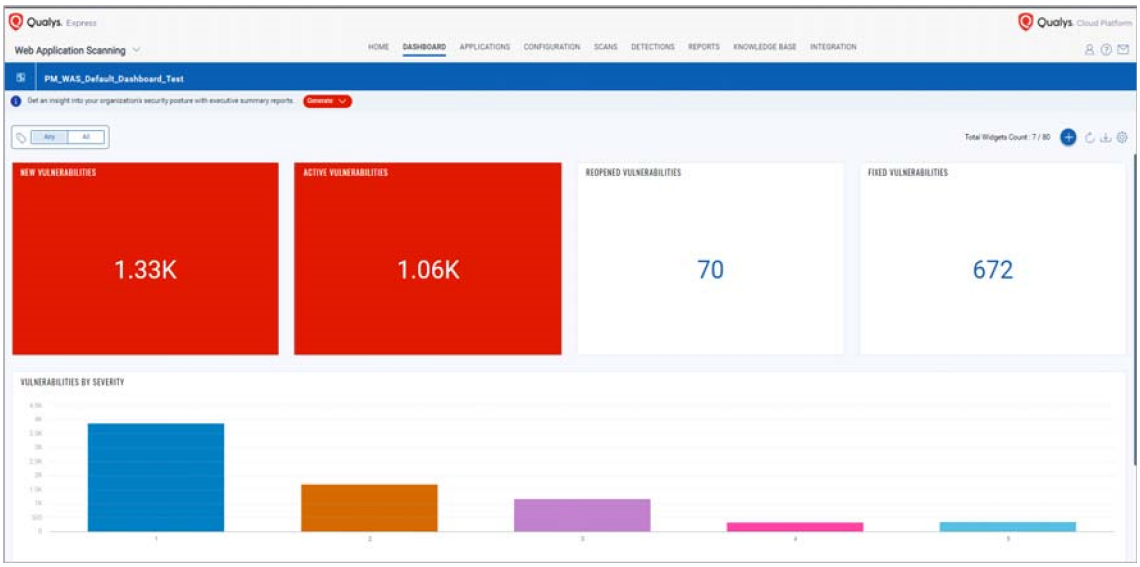
スキャンに移動します

[スケジュール] を選択し、**[新しいスケジュール]** を選択します。



ダッシュボードから最新のセキュリティ状態を取得する

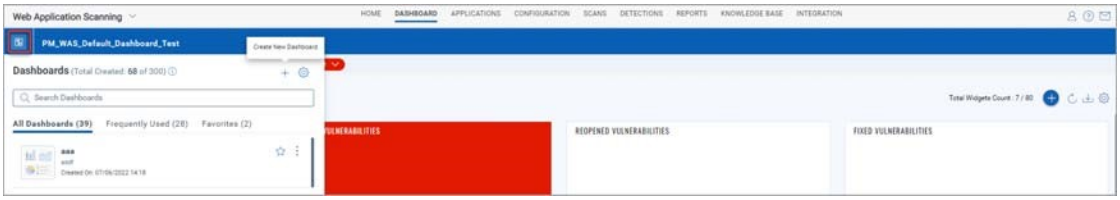
ダッシュボードでは、セキュリティステータスが一目でわかり、最新のスキャン結果が常に最新の状態になります。これは非常にインタラクティブです - セクションやリンクをクリックするだけで、詳細を確認できます。



カスタムダッシュボードを簡単に作成し、ビューを切り替える

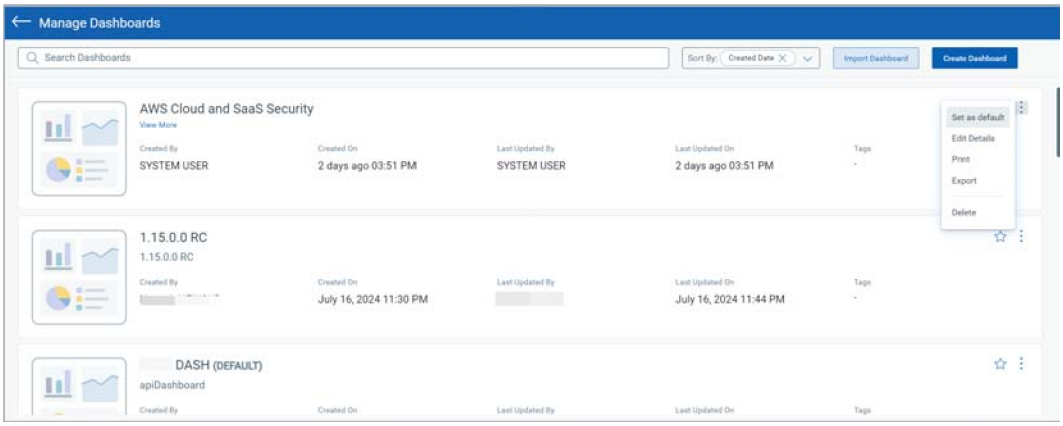
ダッシュボードは、関心のある領域、特定の Web アプリケーション、および本番環境にいつでも集中できます。カスタムダッシュボードをアカウントのデフォルトとして設定することもできます。

[新しいダッシュボードの作成] アイコンをクリックします。



デフォルトのダッシュボードを変更できます。**[ダッシュボードの管理]** から強調表示されたアイコンをクリックします。

デフォルトのダッシュボードを変更するには、ダッシュボードのリストからダッシュボードを選択し、「デフォルトとして設定」をクリックします。



カタログについて教えてください

カタログは、サブスクリプションに追加することを選択できる Web アプリケーションのステージング領域です。カタログでは、WAS でスキャンする必要があるエントリが本当に Web アプリケーションであるかどうかを判断するために、手動でトリアージする必要があります。

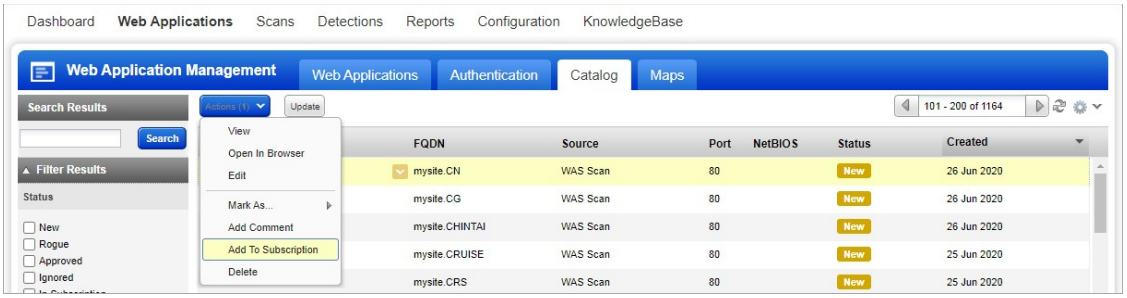
カタログエントリは、**アカウント内の完了したマップ、脆弱性スキャン、および WAS スキャンから処理されます**。カタログエントリは必ずしも Web アプリケーションではなく、特定のポートで HTTP 要求に応答した単なる Web サーバーです。(カタログ機能は Express Lite ユーザーはご利用いただけません。)

どうすれば始めればいいですか?

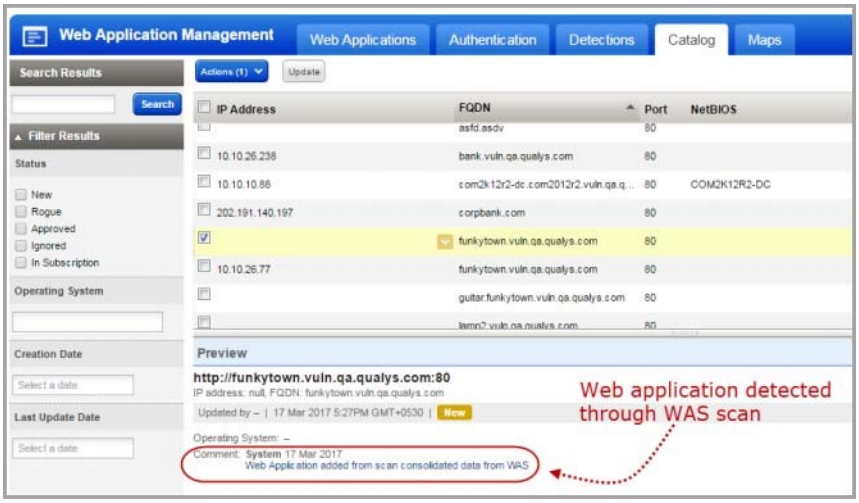
カタログは、あなた (または別のユーザー) がマップ、VM アプリケーションを使用した脆弱性スキャン、または WAS スキャンを起動するまで空になります。完了したら、結果を処理する準備が整います。

- プロセス・スキャン結果: **[Web アプリケーション] >[カタログ]**に移動し、「更新」(リストの上)をクリックします。
- プロセスマップの結果: **[Web アプリケーション] > [マップ]** に移動し、1 つ以上のマップを選択してから、**[プロセス結果]** を選択します。

新しく検出された Web アプリケーションの**新しいカタログ エントリ**が表示されます。これらの Web アプリケーションをアカウントに追加し、セキュリティ リスクがないかスキャンすることを簡単に選択できます。



また、Web アプリケーションがどこにあるかわからなくても、Web アプリケーションを見つけることもできます。強化された検出方法を使用すると、サーバーが複数の仮想ホストを実行している場合、存在するアプリケーションをより適切に識別し、それらを WAS カタログに追加できます。WAS カタログは、WAS スキャンで検出されたが、Web アセットとして追加されない Web アプリケーションで更新されます。



検出の管理

すべての検出を 1 か所で管理します。 **[検出] タブ**は、アプリケーション セキュリティの脆弱性の検出、管理、および情報の中心領域として機能します。すべての検出結果 (Qualys、Burp、Bugcrowd) が [検出] タブに一覧表示されます。

検索を強化し、検出タイプをすばやく見つけるためのフィルターがあります。一般的なフィルターに加えて、検出結果タイプに応じて、各検出結果タイプに固有のフィルターがさらに表示されます。例えば、[Finding Type] を [Burp] にすると、Burp 関連の検出結果に適用できるフィルターが有効になり、他の適用できないフィルターは無効になります。

検出結果タイプは、リストに表示されるアイコンで区別できます。

- Qualys detections
- Burp issues
- Bugcrowd submissions

Burp の結果をインポートしたいですか?

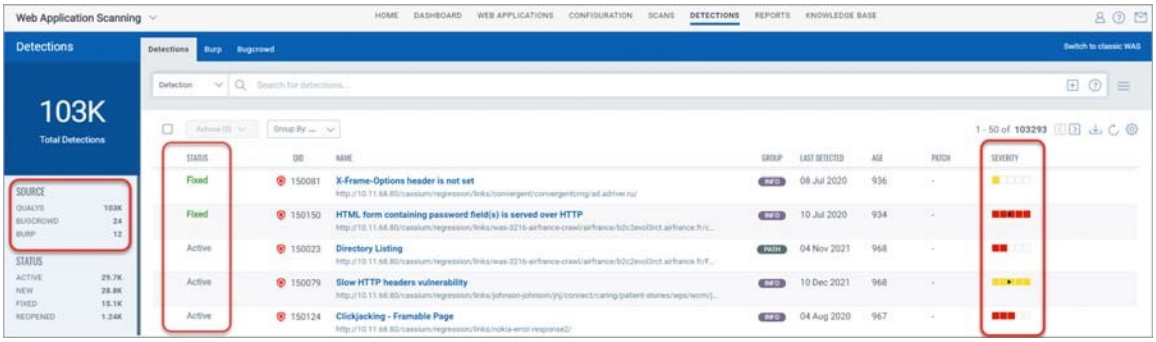
(この機能は、Express Lite ユーザーは利用できません。)

Qualys WAS Burp 拡張機能を試して、WAS 検出結果を Burp Repeater に直接インポートして、脆弱性を手動で検証することをお勧めします。この拡張機能は、Burp Suite Professional と Burp Suite Community Edition の両方で動作します。

Qualys WAS Burp 拡張機能は、BApp ストアの [エクステンダー] タブにあります。Qualys WAS Burp 拡張機能の詳細については、Qualys コミュニティのこのブログ記事を参照してください。

または、**[Detections] > [Burp] > [Import]** に移動します。ローカルファイルシステムから XML 形式の Burp ファイルを選択し、Burp レポートが適用される Web アプリケーションを選択します。

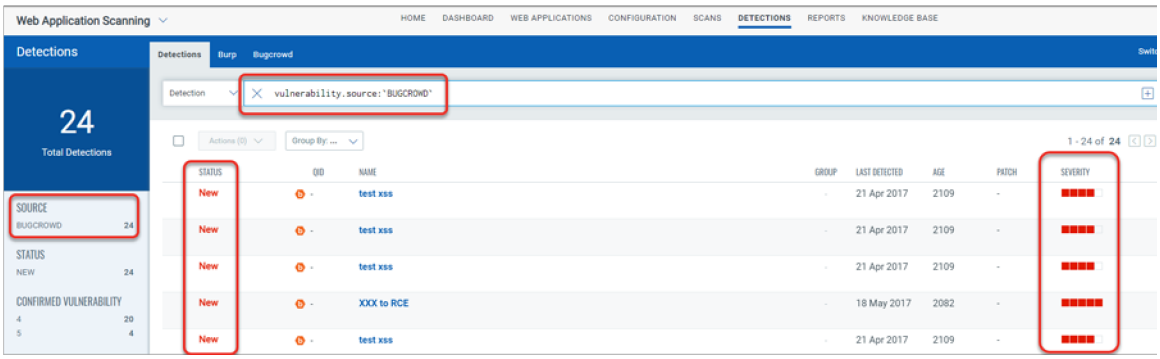
Burp レポートでインポートされた問題が [Detection] リストに表示されます。[Detections] > [Detections] に移動します。検索フィルターの [検出結果の種類] で [Burp] を選択すると、検出日、ステータス、重大度などの問題を詳細に表示できます。



Bugcrowd との統合

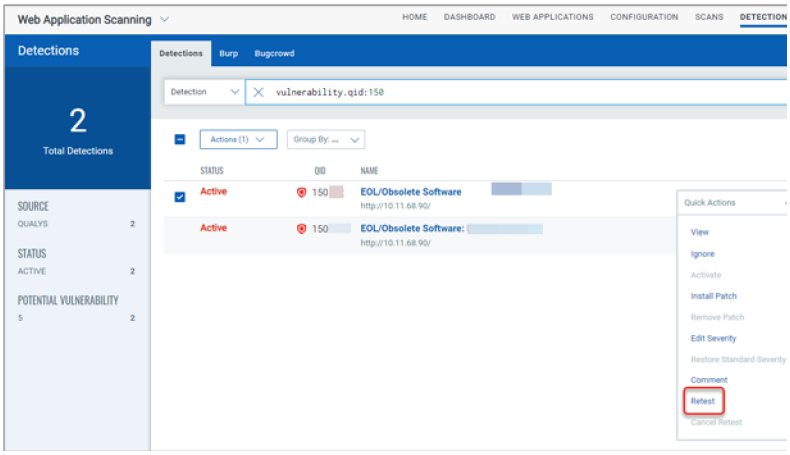
Bugcrowd のお客様は、承認された Bugcrowd の提出物を WAS アカウントにインポートすることもできます。Bugcrowd の統合により、WAS によって特定された脆弱性と、Bugcrowd が管理するバグ報奨金プログラムを通じて発見された脆弱性を表示および報告する方法が提供されます。

Bugcrowd > Import > Detections に移動し、ローカルファイルシステムから CSV 形式の Bugcrowd ファイルを選択し、Bugcrowd ファイルが適用される Web アプリケーションを選択します。Bugcrowd ファイルとともにインポートされた課題が課題リストに表示されます。[Detections] > [Detections] に移動します。



フルスキャンを起動せずに複数の検出結果を再テストする

はい、スキャンを開始して選択した複数の検出結果をテストすることで、脆弱性について検出結果を簡単に再テストできます。潜在的な脆弱性、確認された脆弱性、および機密コンテンツのみを再テストできます。同じ QID と Web アプリケーションに属する複数の検出結果をクラブ化し、1 つのバッチで再テストを開始できます。再テストスキャンでは、最新のスキャンで使用したのと同じ設定が使用されます。いずれかの検出結果の再テストをキャンセルすると、検出結果のバッチ全体に対して再テスト・スキャンが取り消されます。



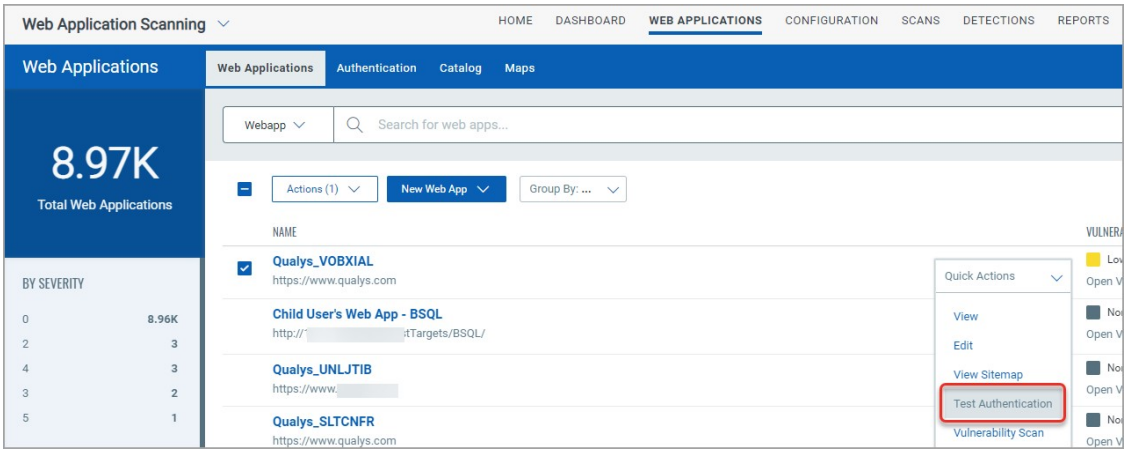
[Detections] > [Detections] に移動します。

左側のペインのフィルターを使用して、同じ QID と Web アプリケーションのすべての検出結果を表示できます。再テストする検出結果を選択します。**[Actions]** メニューから **[Retest]** を選択します。確認すると、選択したすべての検出結果に対して再テストスキャンが一度に開始されます。

認証のテスト

定義した Web アプリケーションの認証レコードは、ディスカバリー・スキャンを実行しなくてもテストできます。Web アプリケーションの認証をすばやくテストし、Web アプリケーションに対する認証を行うスキャナーの機能をテストできます。

[Web アプリケーション] > [Web アプリケーション] に移動し、Web アプリケーションを選択し、Quick Actions メニューから [認証のテスト] を選択します。



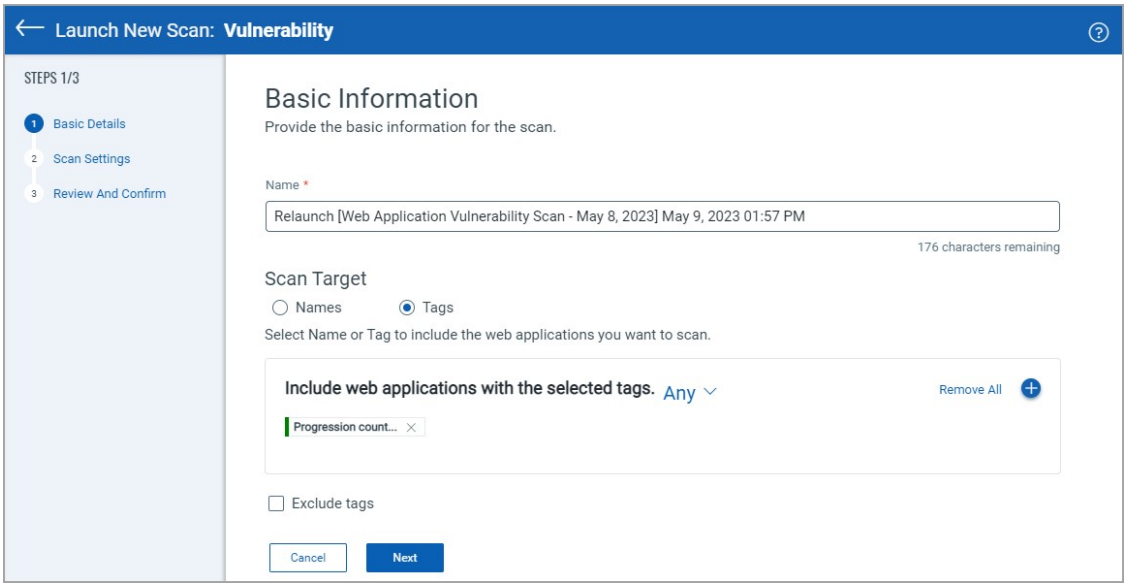
認証テストスキャンが「完了」状態になったら、Quick Actions メニューから「レポートの表示」を選択し、**認証テストスキャンレポート**を表示します。

Web アプリケーションの大量スキャン

Qualys WAS は、最もスケーラブルな Web アプリケーションスキャンソリューションです。マルチスキャンとして任意の数の Web アプリケーションをスキャンする機能を追加することで、大規模な Web アプリケーションスキャンプログラムをサポートする機能を強化しました。この機能により、組織は企業内に数百または数千の Web アプリケーションをスキャンし、どのスキャンが実行され、どのスキャンが完了しているかを詳細に把握できます。

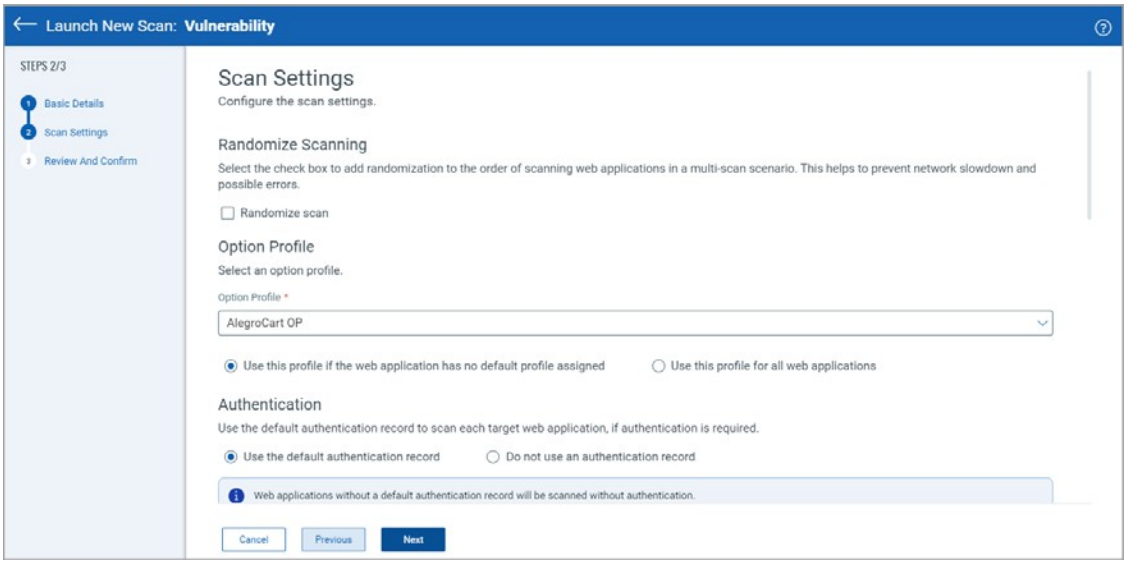
アプリケーションの選択 - 個々のアプリまたはタグを選択します

Qualys アセットのタグ付けを利用して、類似した属性を持つ可能性のあるアプリケーションを分類し、それらをまとめてスキャンできます。アプリケーションにタグを付ける時間がありませんか? 問題ありません - ユーザーはアプリケーション名を選択できます。



スキャン設定の選択 - 認証、オプションプロファイル、スキャナアプライアンス

マルチスキャン機能には、Web アプリケーションのデフォルトを受け入れたり、デフォルトの Web アプリケーション設定を上書きしたりするための多くのオプションが用意されています。



Selenium スクリプトを使用したスキャン

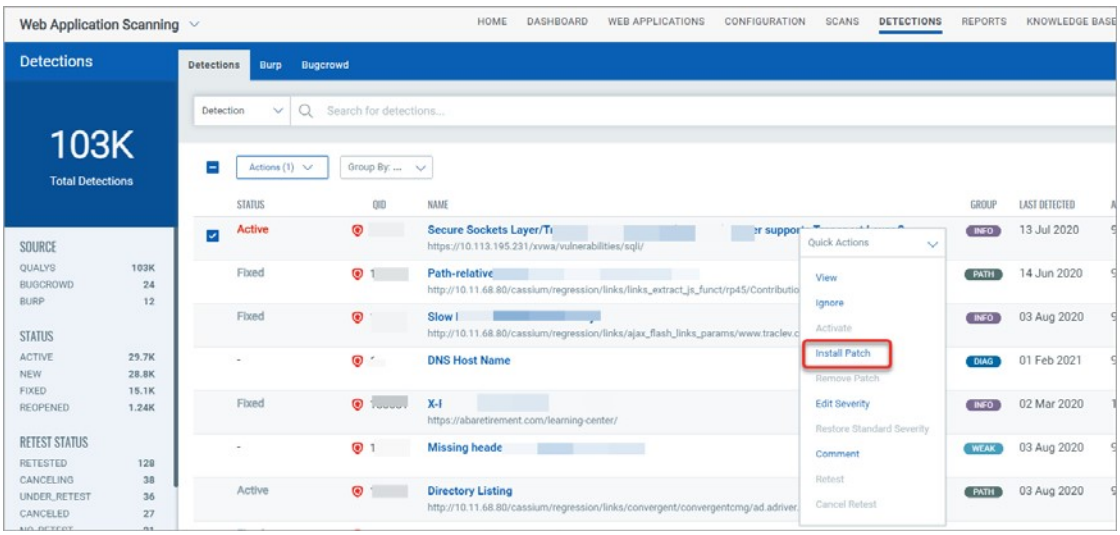
Qualys Browser Recorder (QBR) を使用して、Selenium スクリプトを作成できます。QBR は、Web アプリケーション自動化テスト用のスクリプトを記録および再生するための無料のブラウザ拡張機能(Google Chrome ブラウザ用)です。QBR を使用すると、Web 要素をキャプチャし、ブラウザでアクションを記録できるため、自動テストケースをすばやく

簡単に生成、編集、再生できます。また、ブラウザーの現在表示されているページから UI 要素を選択し、パラメーターを含む Selenium コマンドのリストから選択することもできます。これらのスクリプトを WAS で使用すると、スキャナーが Web アプリケーションの複雑な認証およびビジネスワークフローをナビゲートできます。

Web アプリケーションで使用される一般的な認証メカニズムは、シングル サインオン (SSO) です。これにより複雑になり、Qualys WAS を使用した認証とスキャンに関して混乱が生じる可能性があります。QBR を使用すると、スキャナーの認証メカニズムを簡素化できます。詳細な手順については、ブログ記事を参照してください。

仮想パッチのサポート

WAS では、アカウントで WAS と WAF が有効になっている場合に、選択した脆弱性(検出)に対して仮想パッチをインストールできます。インストールすると、選択した脆弱性の悪用をブロックするファイアウォールルールが自動的に追加されます。仮想パッチの管理に役立つ機能が WAF API に追加されました。

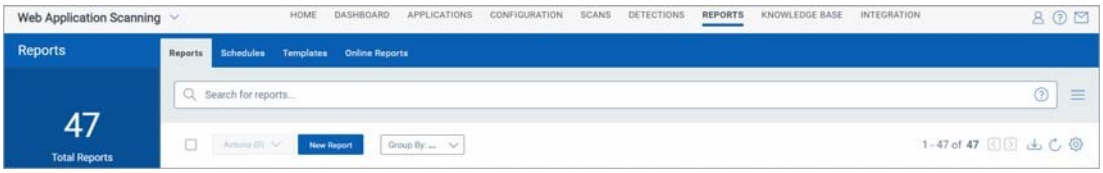


Steps to create reports

レポート

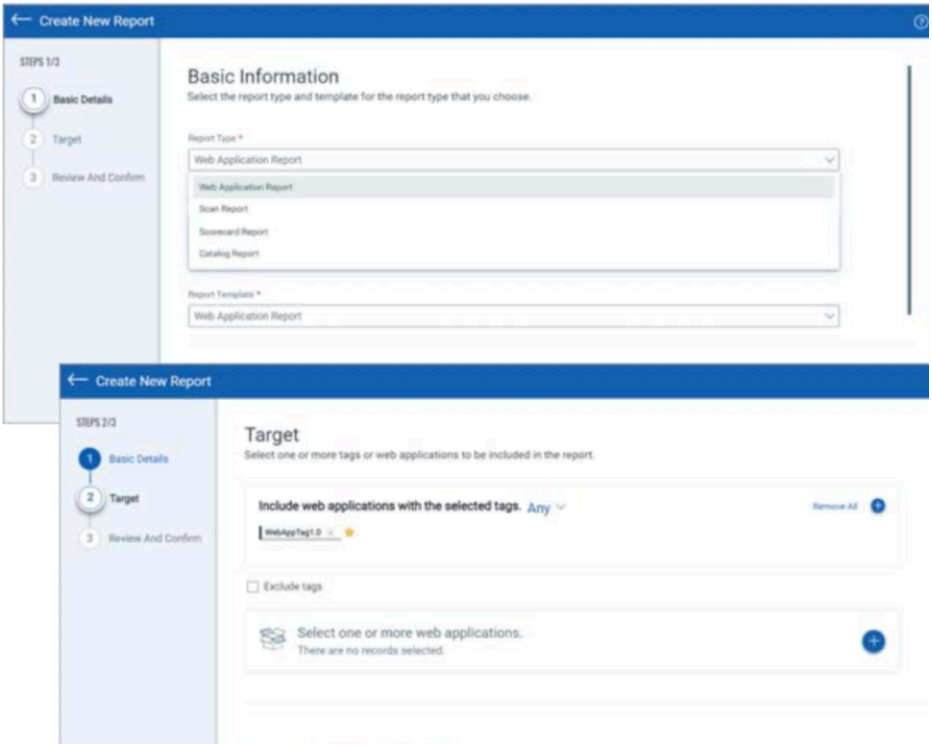
レポート作成手順

[新しいレポート] を選択するか、右側の [+] ボタンをクリックします。

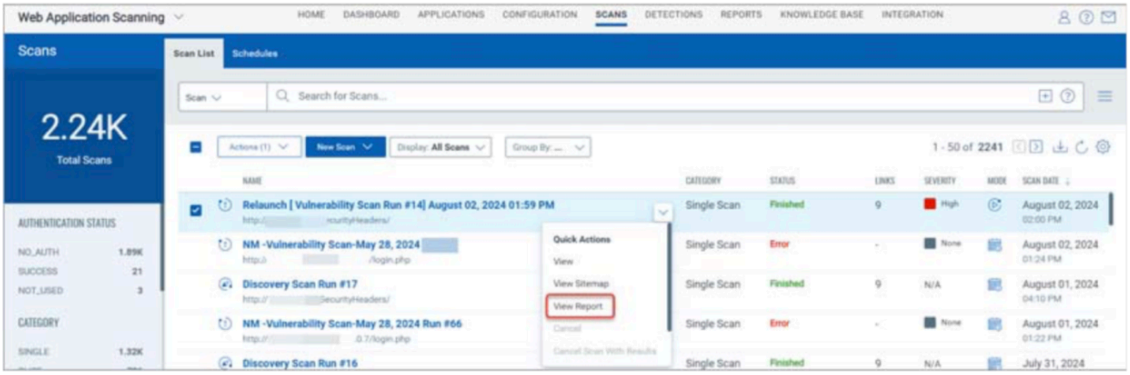


レポートタイプ(この場合は Web アプリケーションレポート)を選択します。

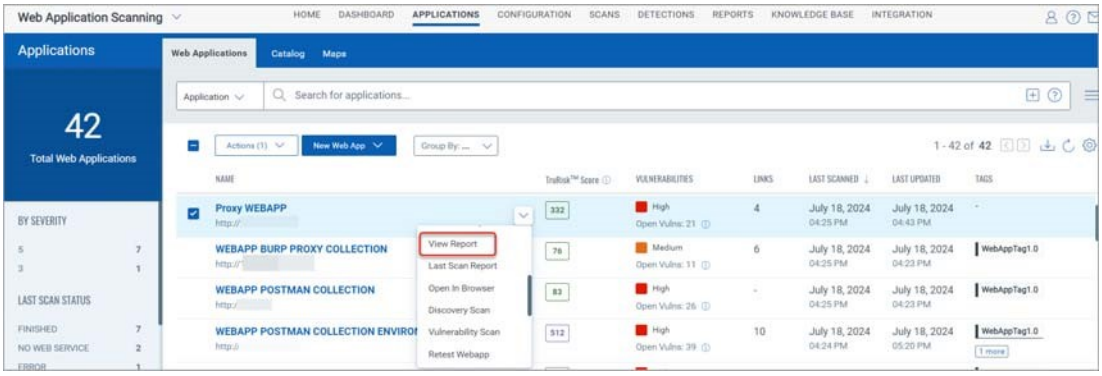
Tag または name によって Web アプリケーションを選択します。



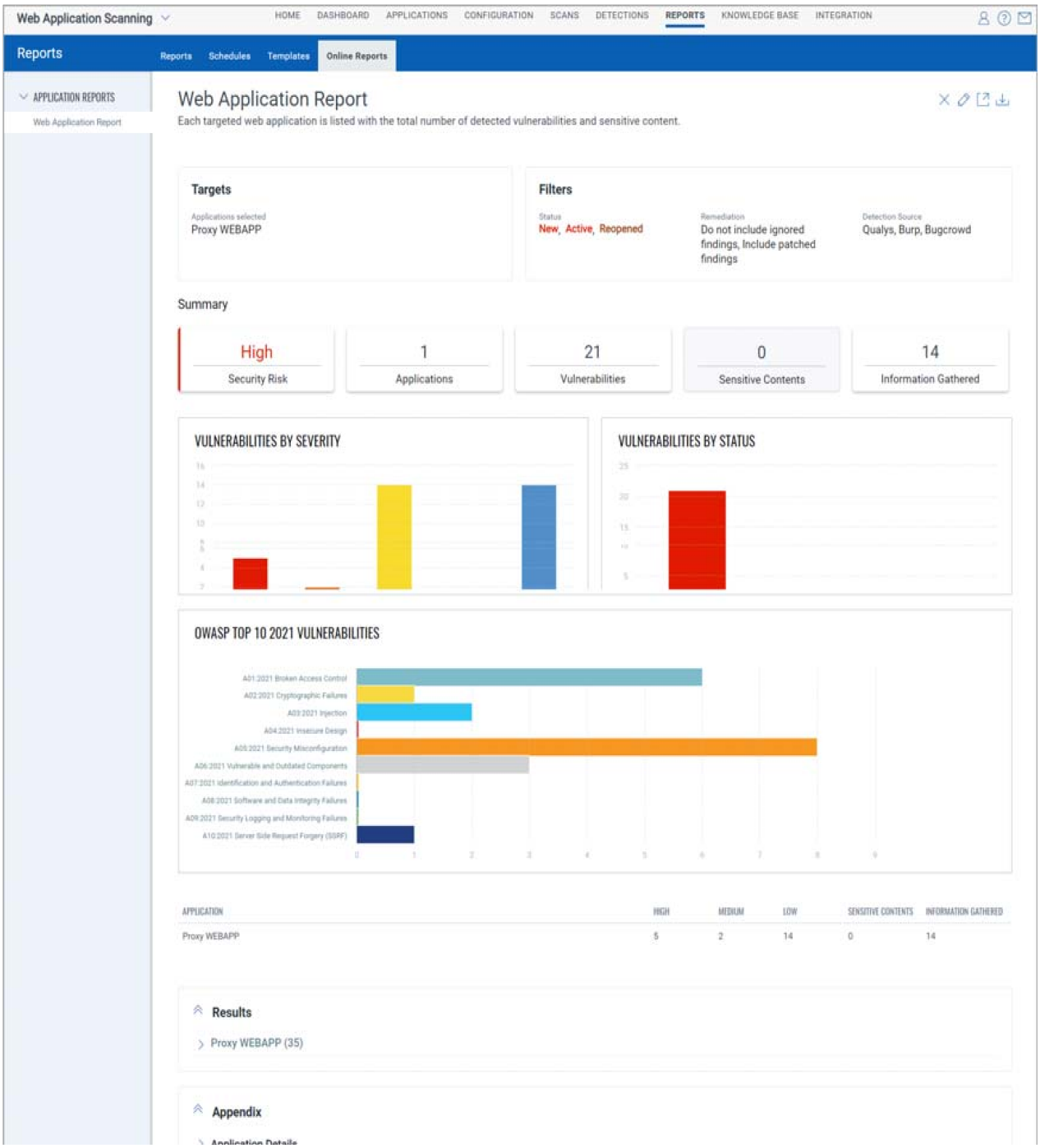
または、スキャン リストからスキャンを選択し、Quick Actions メニューから **[レポートの表示]** を選択して、スキャン レポートをすばやく生成することもできます。



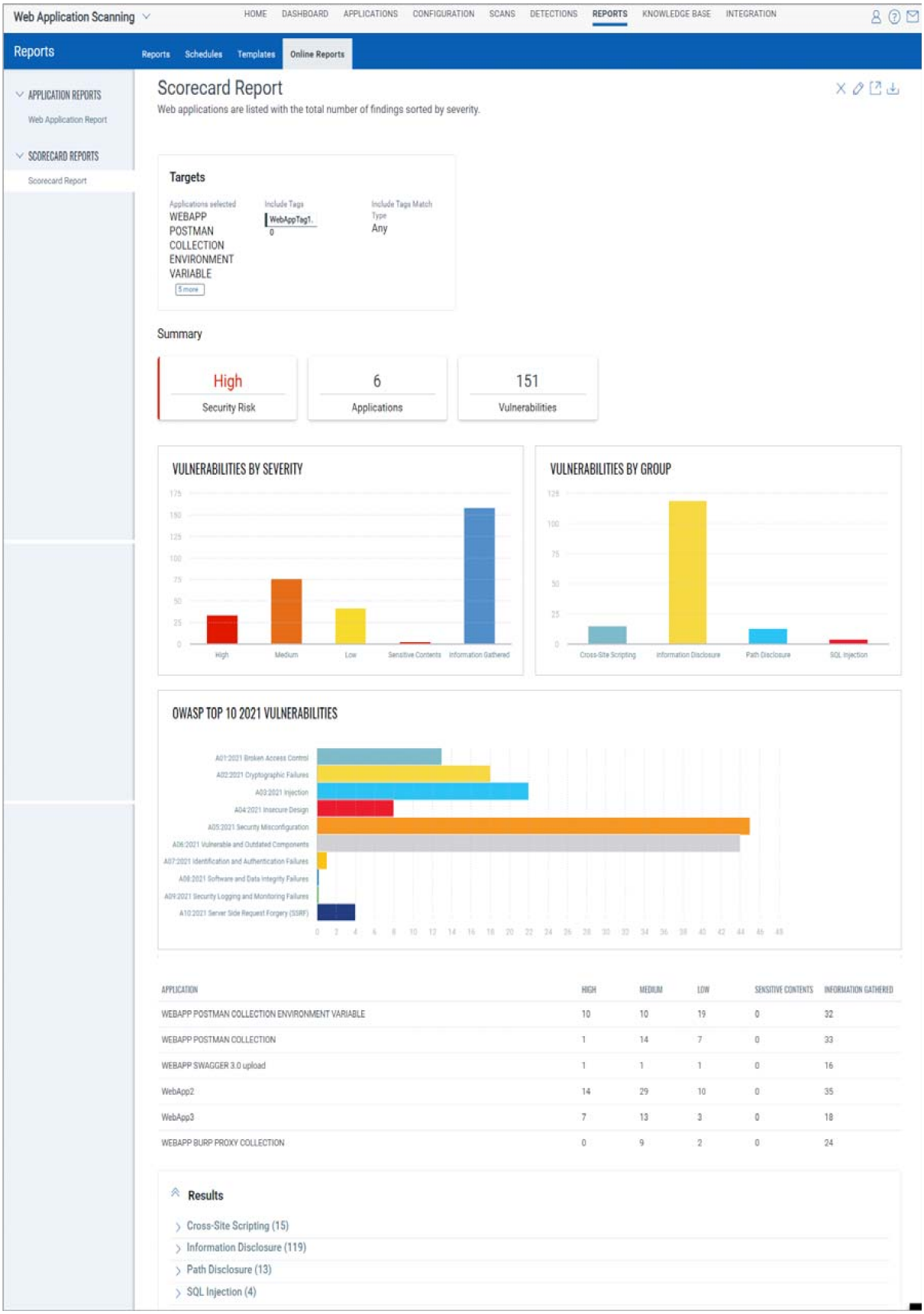
同様に、Web アプリケーションの Quick Actions メニューから [レポートの表示] を使用して Web アプリケーションレポートを生成できます。



Web アプリケーションのサンプルレポート



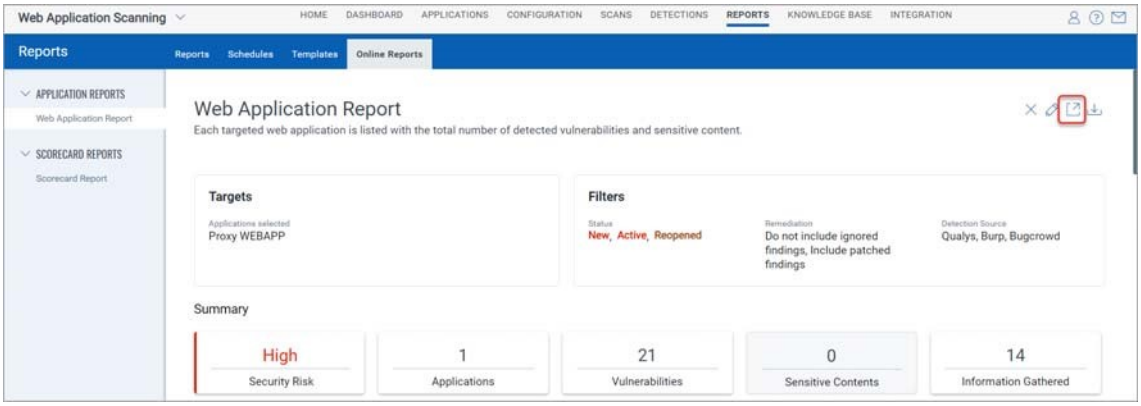
スコアカードレポートのサンプル



Tips & Tricks

設定の表示、編集、繰り返し

私たちのレポートは反復的です。[レポートの編集] ボタンをクリックしてレポートの設定を変更するだけで、変更内容を含む更新されたレポートが作成されます。これにより、どの脆弱性や Web アプリケーションなどのフィルターをレポートの内容にすばやく適用できます。

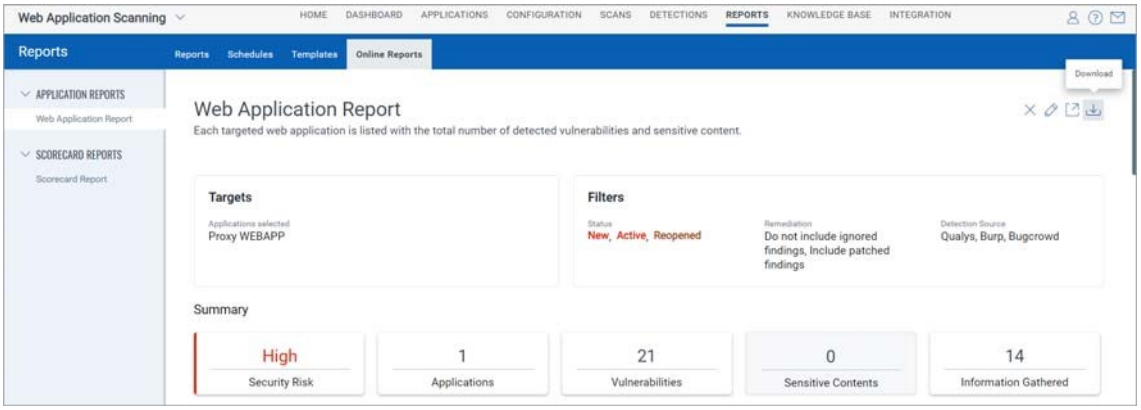


並べて比較する

レポートヘッダーのアイコンをクリックするだけで、レポートが新しいウィンドウで開きます。これにより、並べて比較を行い、一度に複数のレポートを簡単に操作できます。

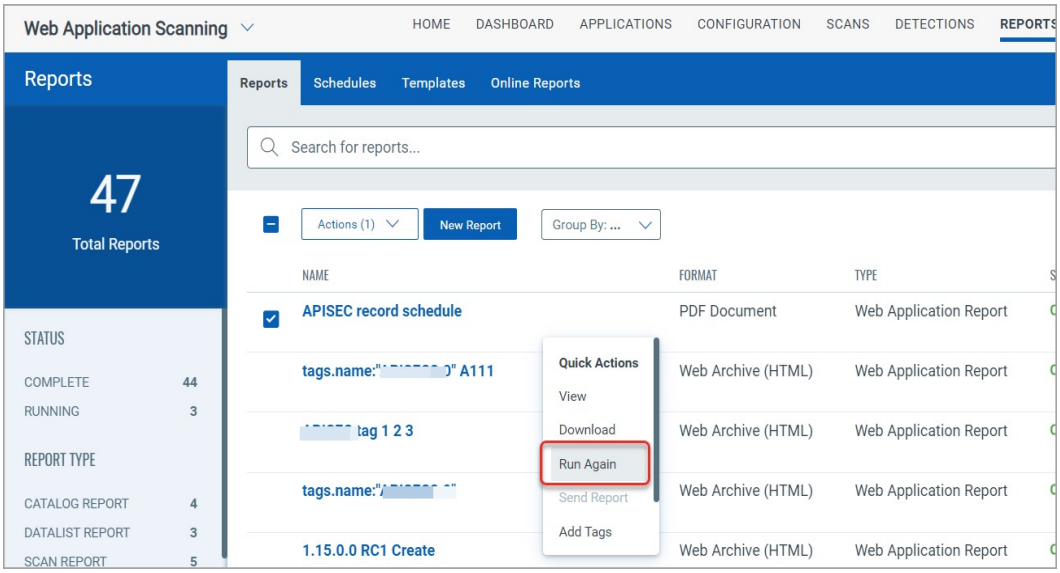
レポートを保存するにはどうすればよいですか?

[ダウンロード] オプションを使用して、レポートをローカル マシンにダウンロードし、アカウントに保存します。



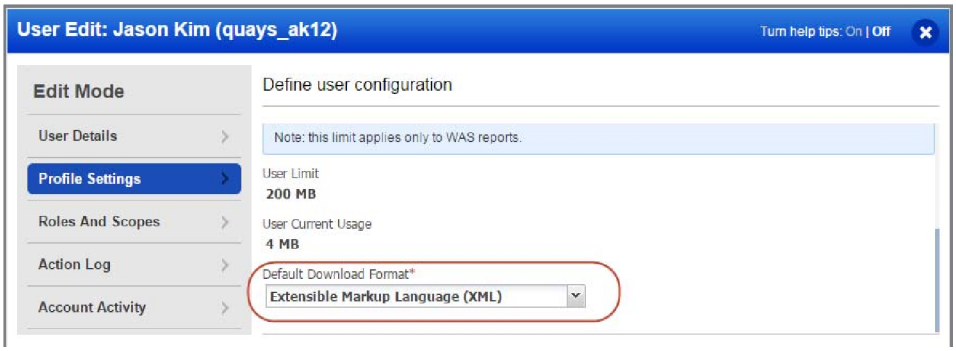
レポートリストでは、保存したレポートを表示できます。各レポート(概要)を表示できます

。ダウンロードして再度実行し、タグを追加してレポートを他のユーザーと共有します。



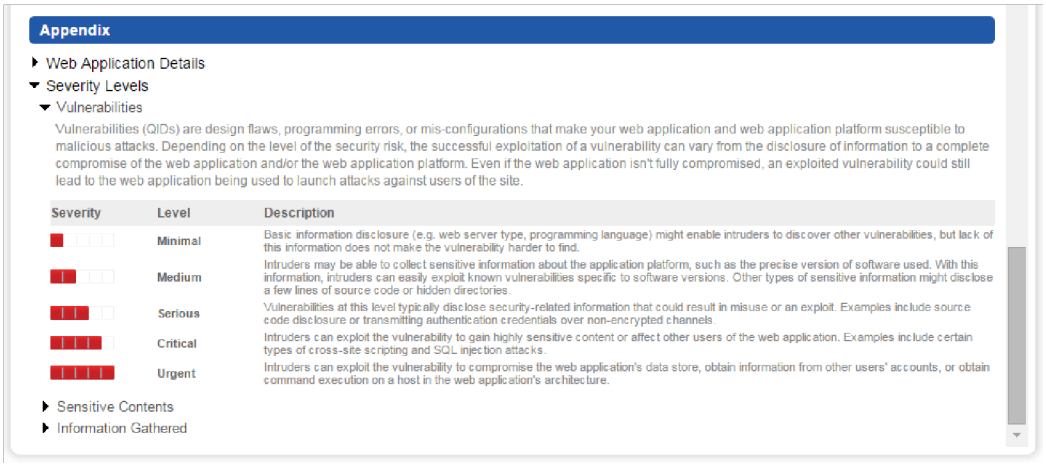
既定のレポート形式を設定する

これにより、時間を節約できます。レポートをダウンロードするたびに、お気に入りのレポート形式を選択する必要はありません。ユーザー名(右上隅)の下にある[マイプロファイル]を選択し、プロファイル設定を編集するだけです。



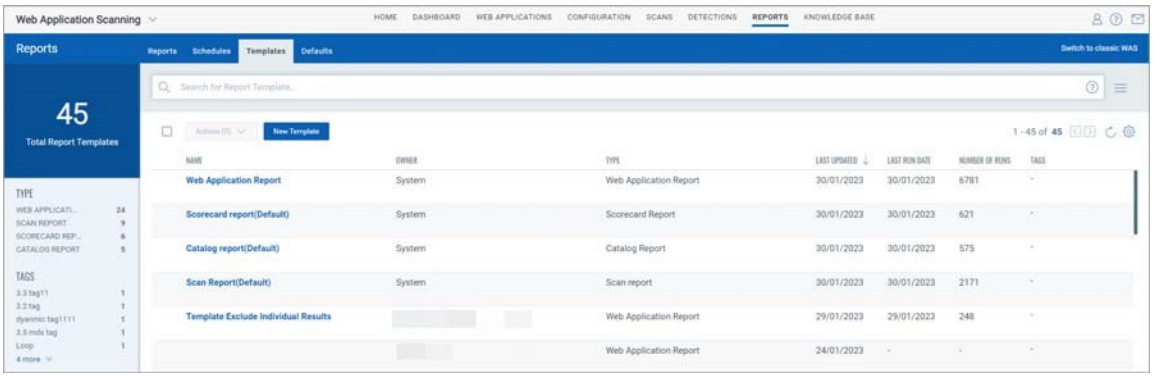
重大度とレベルはどういう意味ですか?

付録に移動して、**[重大度レベル]**をクリックします。各検出タイプ (脆弱性、機密コンテンツ、収集された情報) の重大度とレベルの説明が表示されます。

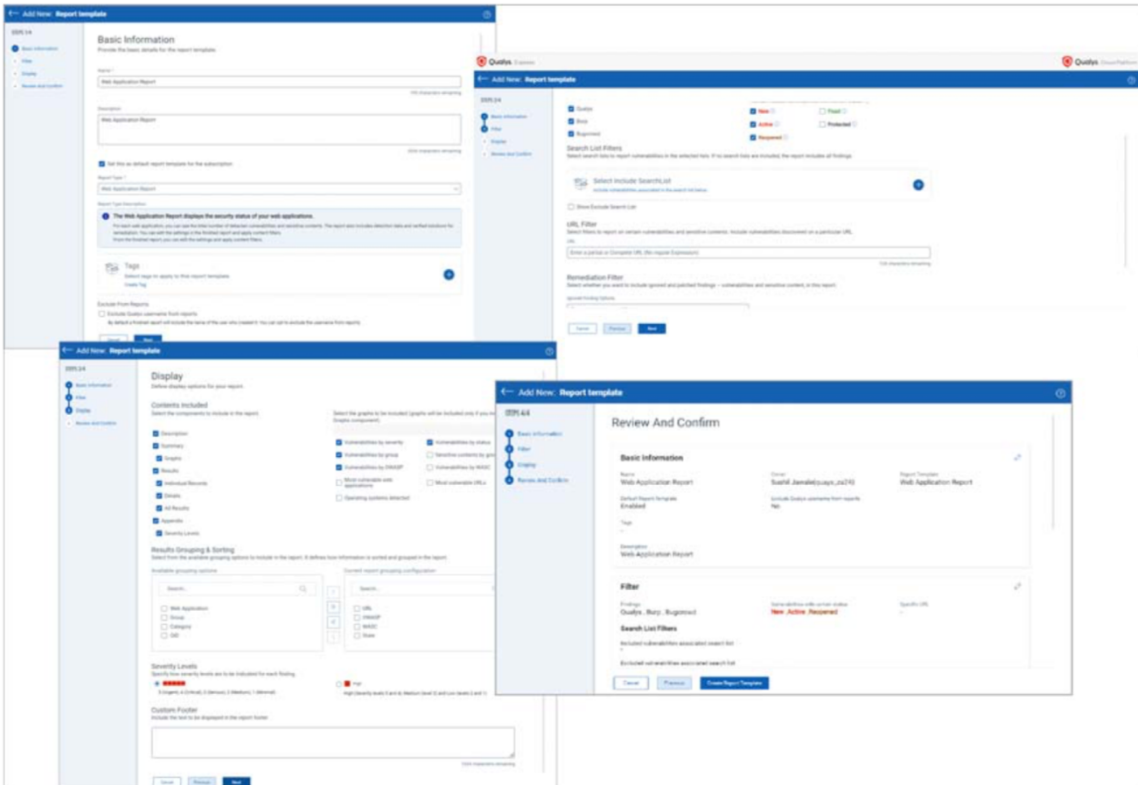


カスタマイズ可能なレポートテンプレート

関心のある特定の情報を含むテンプレートを作成します。これにより、アプリケーションの利害関係者に適切な情報を簡単に提供できます。すべてのカスタムテンプレートは、後で使用できるようにアカウントに保存されます。**[レポート] > [テンプレート]** に移動し、**[新しいテンプレート]** ボタンを選択して開始します。



多数のレポートテンプレート設定により、検索リスト、脆弱性検出、無視としてマークされた脆弱性、含めるコンテンツ、グループ化、並べ替えなどの表示設定などのフィルターを構成できます。

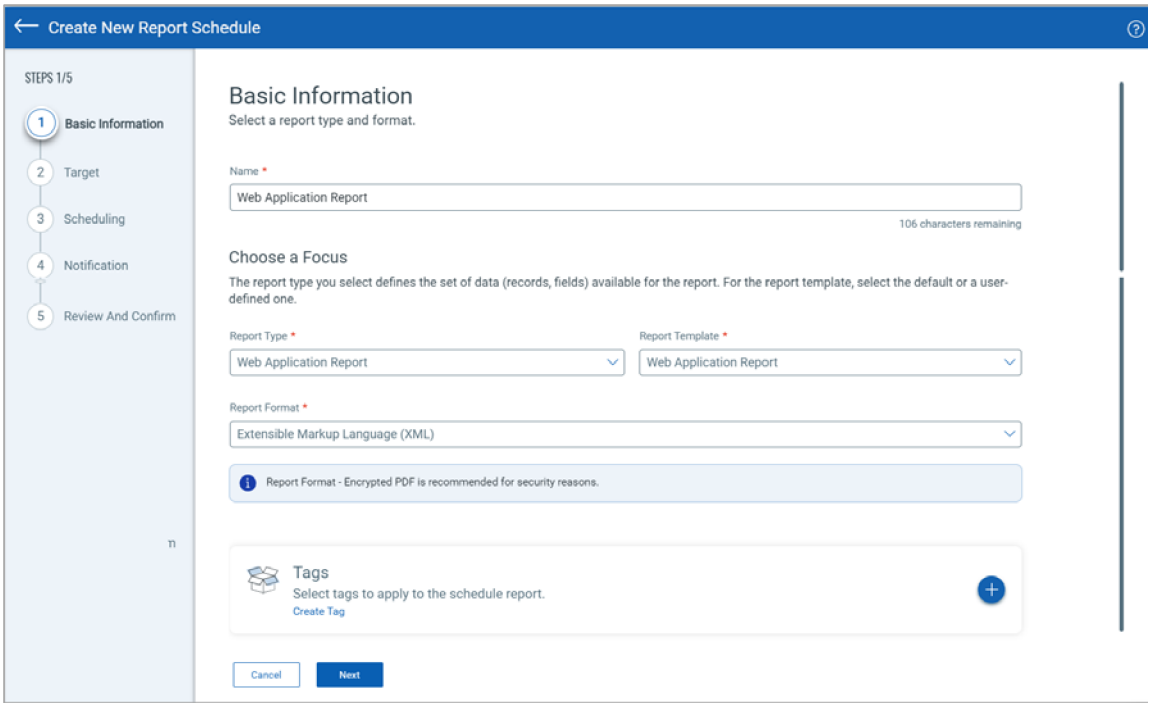


テンプレートを共有したいですか?　問題ありません - 他のオブジェクト (Web アプリケーション、レポートなど) の場合と同様に、タグをタグ付けし、タグをユーザー スコープに追加するだけです (管理ユーティリティを使用)。

スケジュールされたレポート

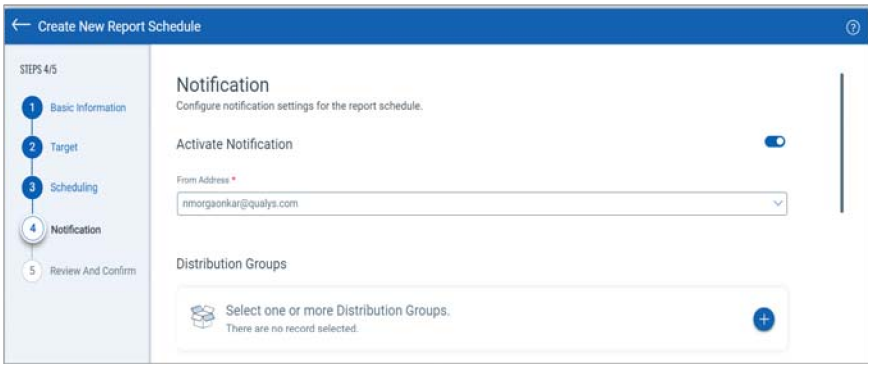
スキャンをスケジュールするのと同じ方法で、レポートが自動的に実行されるようにスケジュールします。レポートは、毎日、毎週、毎月、または 1 回だけ実行するようにスケジュールできます。レポートのスケジュール設定は、最新のスキャン結果に基づいてセキュリティ更新プログラムを取得し、他のユーザーと共有するための優れた方法です。

[レポート] > [スケジュール] に移動し、**[新しいスケジュール]** をクリックして開始します



レポート通知の設定は簡単です

[通知を有効にする] を選択し、電子メール通知を受信するユーザーをお知らせください。レポートが完了するたびに、レポートをダウンロードするためのリンクが記載されるたびに、およびレポートの生成が失敗するたびに、ユーザーにアラートが設定されます。



ユーザーの追加

Qualys サブスクリプションにユーザーを追加し、WAS へのアクセス権を付与するのは簡単です。これを行うには、マネージャー ロールが必要です。

新しいユーザーを追加するにはどうすればよいですか?

脆弱性管理アプリケーションで提供される新規ユーザーワークフローを使用します。アプリピッカーから [VM/VMDR] を選択し、[ユーザー] セクションに移動して新しいユーザーを作成します。手順を順を追って説明します。

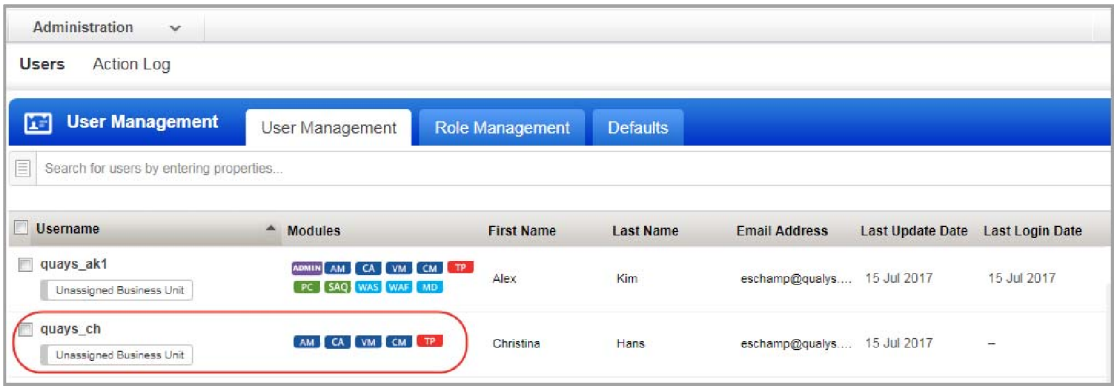
ユーザー、その役割、および権限の表示

Qualys Cloud Platform UI には、サブスクリプション内のすべてのユーザー、割り当てられたロール、およびアカウントで有効になっているさまざまなアプリケーションに対する権限が表示されます。新しく追加されたサブアカウント(スキャナー、リーダー、ユニットマネージャーなど)は、WAS へのアクセスを自動的に許可されないことに気付くでしょう。

ユーザーに WAS へのアクセス権を付与する方法

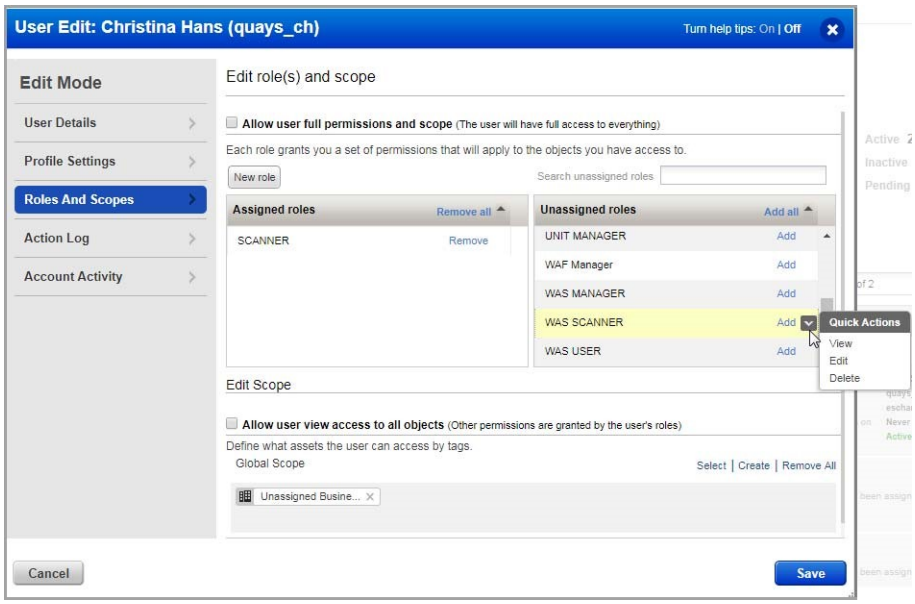
Scanner ロールを持つ新しいユーザー Christina Hans を作成し、Christina が WAS を使用して Web アプリケーションのセキュリティ リスクをスキャンできるようにするとします。

Qualys Cloud Platform を使用するアプリケーションに対する新しいユーザーの権限を表示します。Administration ユーティリティに移動します。新しいユーザーの WAS アプリケーションがリストされていないことに気付くでしょう。

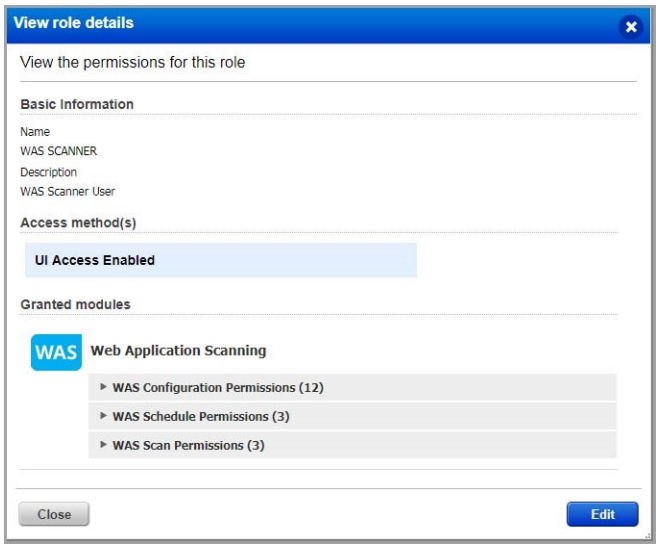


新しいユーザーを編集します (ユーザーを選択し、[Quick Actions] メニューから [編集] を選択します)。[ロールとスコープ] で、ユーザーには VM や PC スキャンの SCANNER ロールが割り当てられます (サブスクリプション設定によって異なります)。

Qualys には、ユーザーに WAS 権限を簡単に付与できるように、定義済みの WAS ユーザー ロールが用意されています。事前定義された役割は、WAS MANAGER、WAS SCANNER、WAS USER です。

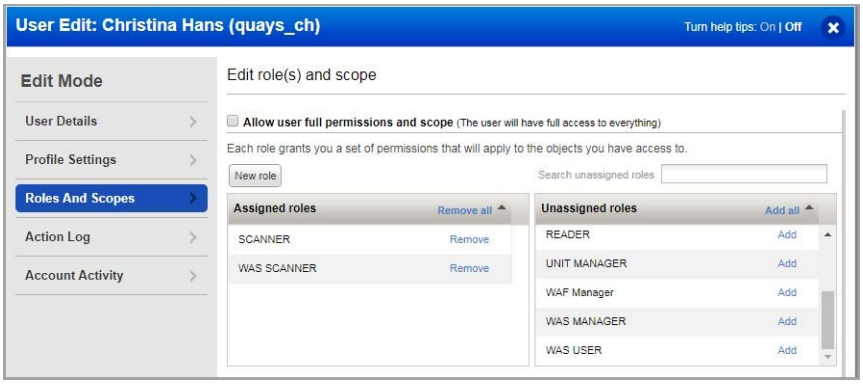


ユーザーの Christina は SCANNER ロール (VM/PC 用) を持っているため、WAS SCANNER ロールをアカウントに追加します。WAS SCANNER を選択し、Quick Actions メニューから表示を選択します。WAS SCANNER アクセス許可グループが表示され、ドリルダウンしてロールの詳細を確認できます。このロールは、たとえば Web アプリケーションを追加/更新/パージする権限を付与しません。

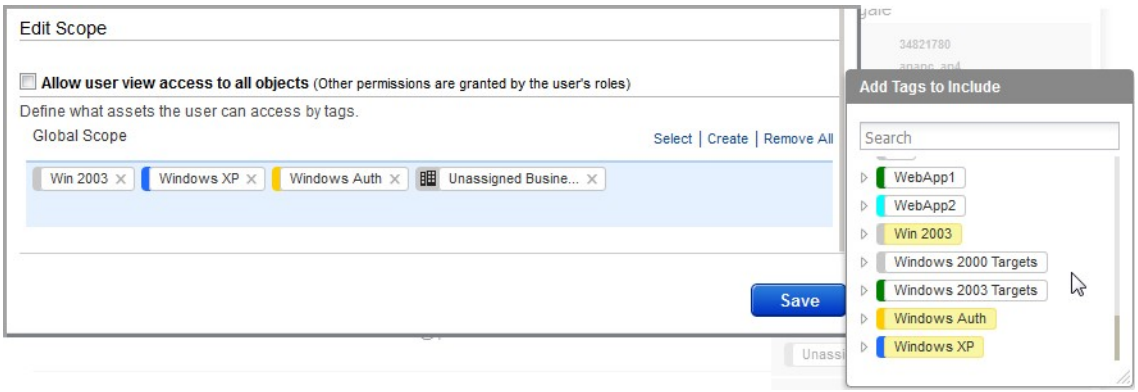


[閉じる] をクリックして、ユーザー設定を編集します。

WAS SCANNER ロールの横にある [追加] リンクをクリックして、ユーザーに割り当てられたロールに追加します。割り当てられたロールは次のようになります。



特定のタグを割り当てます。[スコープの編集] セクションを更新して、サブスクリプション内の Web アプリケーションへのアクセス権をユーザーに付与します。既定では、ユーザーは Web アプリケーションやその他の WAS 構成にアクセスできません。いずれかのオプションを選択します。

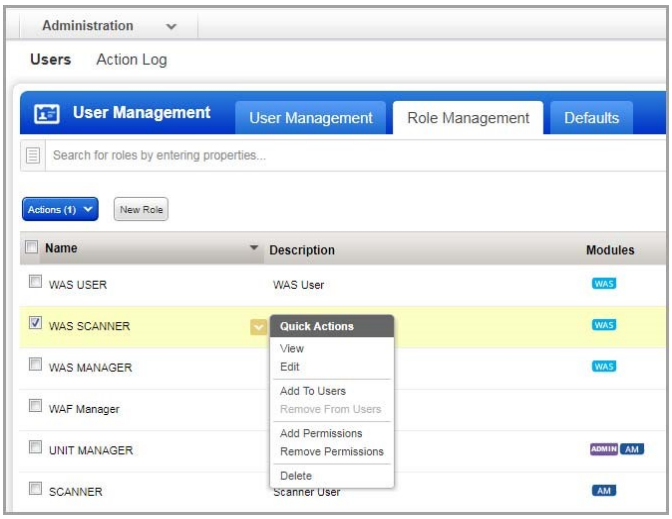


全範囲(すべてのタグ)を付与する

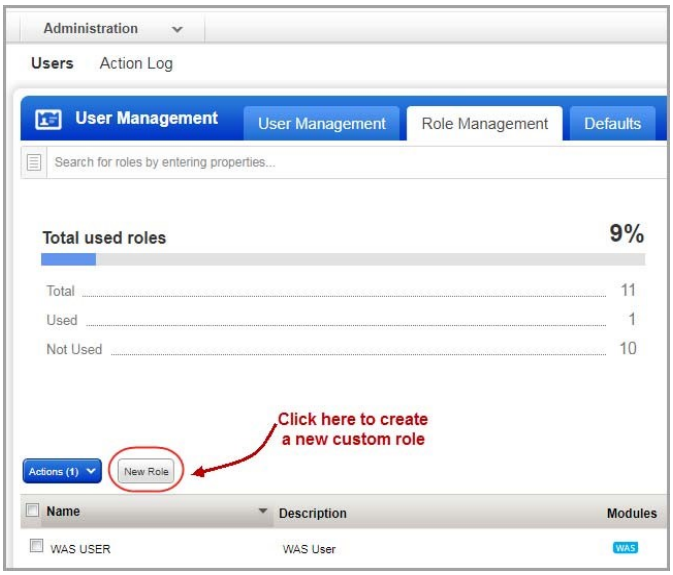
[保存] をクリックして、ユーザー設定を保存します。

ロール管理

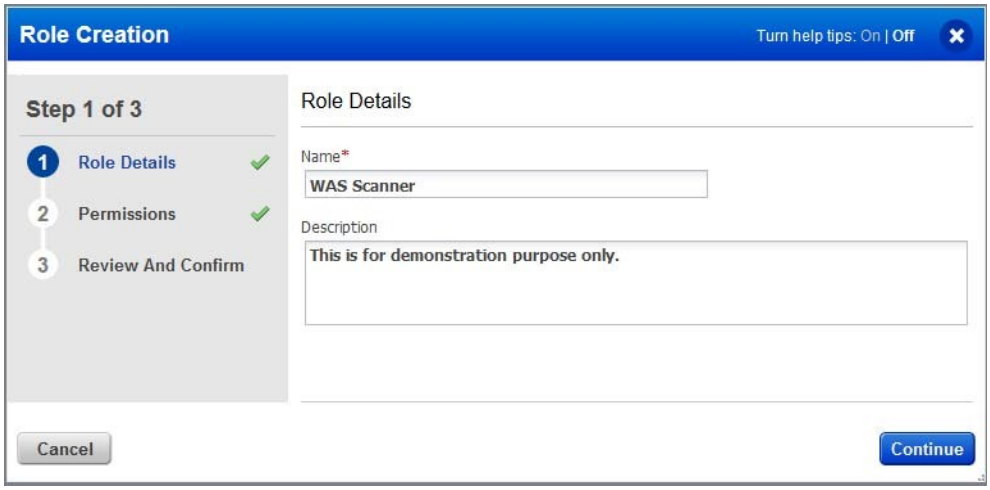
[Role Management] セクションには、サブスクリプションのロールに関するすべてが表示されます。



ロールごとに、詳細を表示し、ユーザーに追加したり、権限を追加したり、 権限の削除など [新しいロール] オプションを使用すると、必要な権限を正確に設定したカスタム ロールを作成できます。

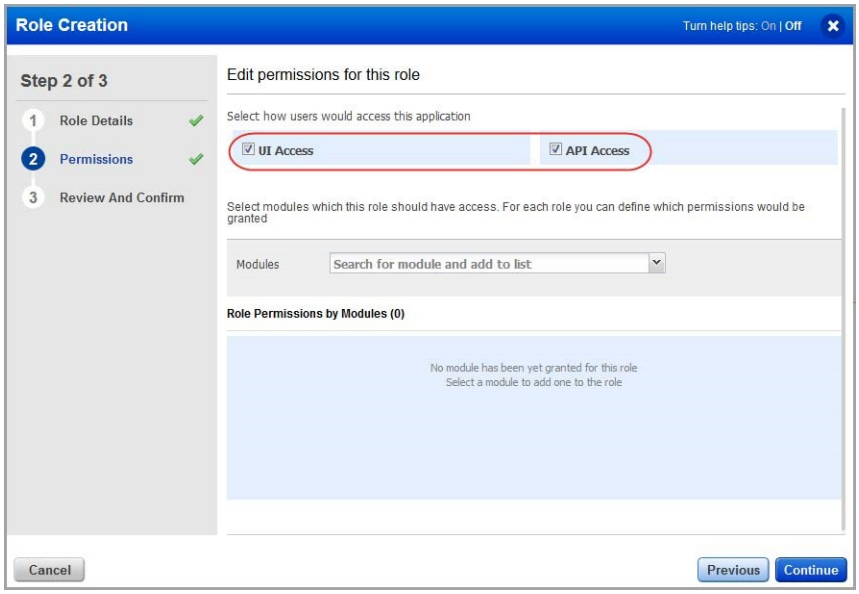


たとえば、 WAS スキャナーのロールを作成できます。

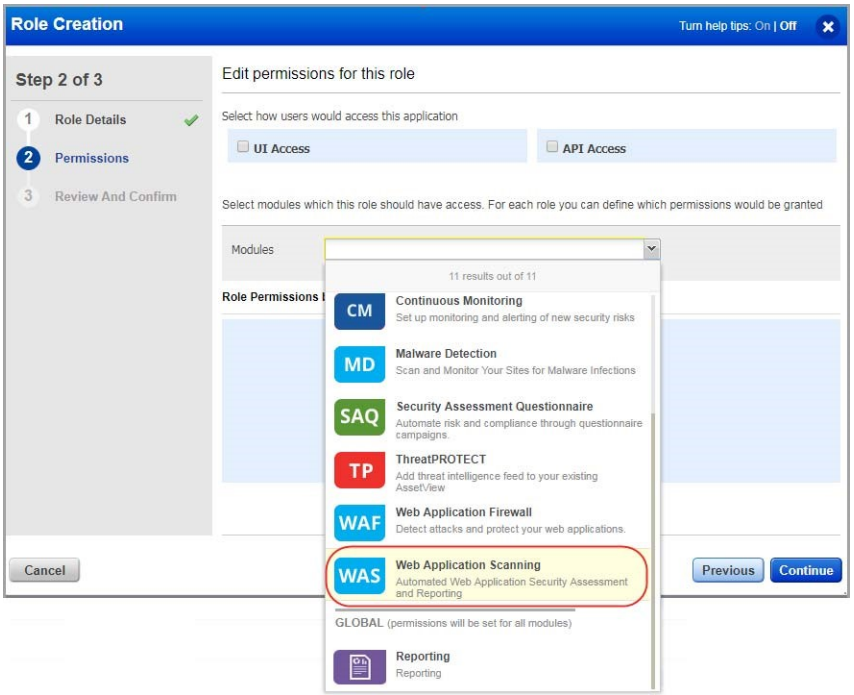


ロールに UI や API へのアクセス権を付与します。

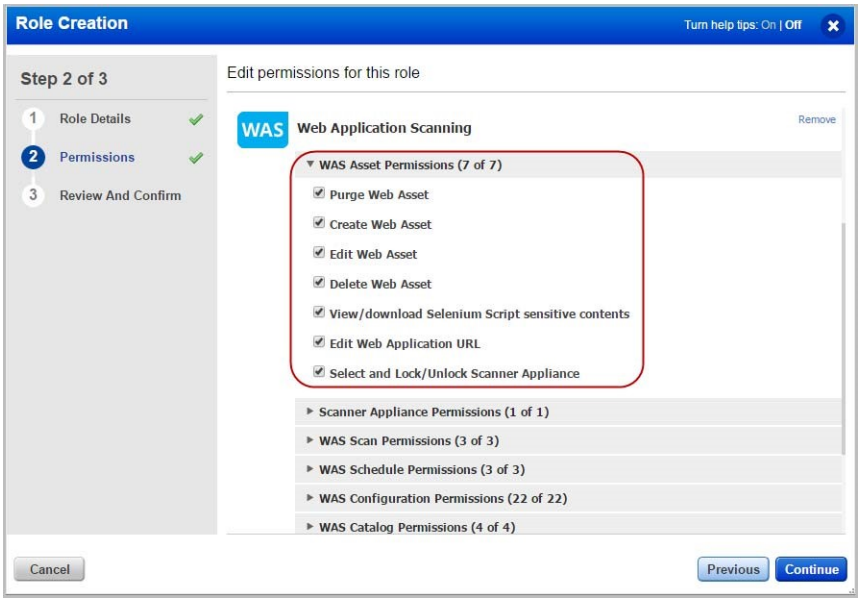
ロールの詳細で、ユーザーのアクセス方法を選択します。



ロールに WAS アプリへのアクセス権を付与します。[権限] セクションで、表示されたメニューから WAS アプリを選択します。



WAS アプリ内でロールのアクセス許可を付与します。



ユーザーアカウントを編集し、ロールを割り当てます。

よくある質問(FAQ)

WAS モジュールにアクセスできないのはなぜですか?

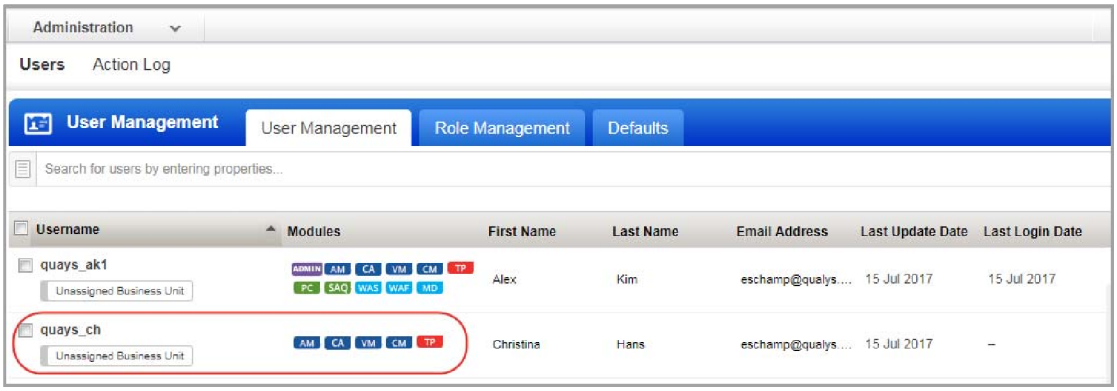
WAS モジュールにアクセスするには、十分な権限が必要です。マネージャー以外のユーザー (スキャナー、リーダー、ユニット マネージャー) には、サブスクリプション内の WAS アプリケーションと Web アプリケーションにアクセスするためのアクセス許可が付与されている必要があります。マネージャ(または「ユーザーの編集」権限を持つユーザー)は、「管理」ユーティリティーを使用して、ユーザーのロールを構成できます。

ここに記載されている手順に従って、ユーザーにロールを割り当てます。

前提条件

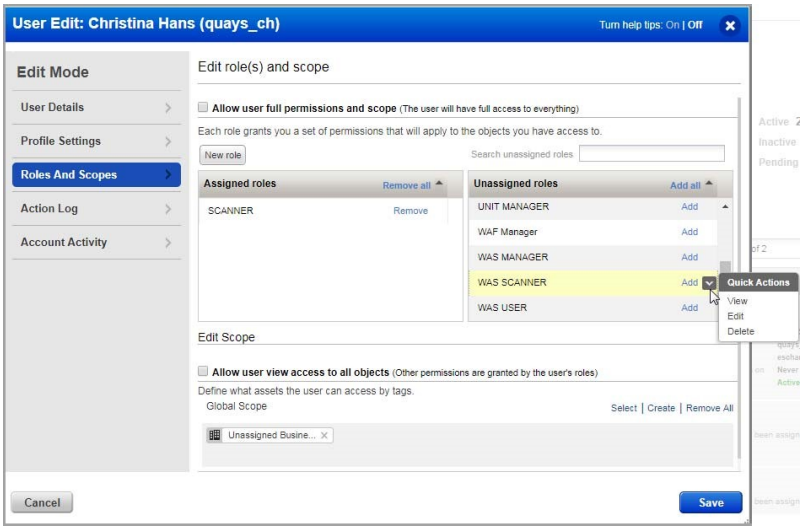
この手順は、マネージャー ロールを持つユーザーが実行する必要があります。

1. アカウントの資格情報を使用して Qualys にログインします。
2. モジュール ピッカーから、[Administration] モジュールを選択します。



3. [User Management] タブから、問題に直面しているユーザーを選択し、[Quick Actions] メニューから [Edit] を選択します。

4. **[Roles and Scopes]** タブに移動し、要件に従ってユーザーに適切な WAS ロールとスコープを選択します。Qualys Administration Utility オンラインヘルプの「Manage User Roles」を参照してください。



サブスクリプション内の Web アプリケーションへのアクセス権を付与する場合は、[Edit] セクションに移動し、[選択] リンクをクリックします。Web アプリケーションタグを選択し、そのタグをユーザーのスコープに追加します。

5. [Save] をクリックし 、ユーザーに再度ログインするように要求します。

ヘルプの取得

Qualys は、最も徹底したサポートを提供することをお約束します。Qualys は、オンライン ドキュメント、電話ヘルプ、直接の電子メール サポートを通じて、お客様の質問に可能な限り最速で回答することを保証します。週 7 日サポートし、

24 時間体制。h ttps://success.qualys.com/customersupport/s/ でオンラインサポート情報にアクセスしてください。

WAS コミュニティ

WAS に関連する最新の機能、ディスカッション、ドキュメント、ビデオの詳細については、Qualys WAS コミュニティ ページにアクセスしてください。