Webアプリケーションスキャン

はじめにガイド

2024年8月2日

Qualys, Inc.
919 E Hillsdale Blvd 4階
フォスターシティ、カリフォル
ニア州 944041 (650) 801 6100

目次

WAS へようこそ 4

はじめに 7

さあ始めましょう 7
ウェブアプリの設定を追加 8
ダッシュボードから最新のセキュリティ状況を確認 10
検出を管理 11
Seleniumスクリプトを使用したスキャン 12
まず発見スキャンをお勧めします 13
次に脆弱性スキャンを実施 15
サイトマップを確認 19
ヒント：-スキャンを自動実行するようにスケジュール設定 21
ダッシュボードから最新のセキュリティ状況を確認 22
カタログについて教えてください 24
検出結果を管理 25
Burp の検出結果をインポートしますか 25
Bugcrowdとの連携 26
フルスキャンを実行せずに複数の検出結果を再テスト 27
認証テスト 27
Webアプリケーションの高ボリュームスキャン 28
Seleniumスクリプトを使用したスキャン 29
仮想パッチサポート 30

レポート 31

レポート作成の手順 31
サンプルWebアプリケーションレポート 33
サンプルスコアカードレポート 34
& のヒントとコツ 35
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 41

よくある質問（FAQ） 48

WASモジュールにアクセスできないのはなぜですか 48

ヘルプ 50

WAS へようこそ

Qualys Web Application Scanning (WAS) は、組織が攻撃者を寄せ付けず、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、集中管理、統合機能を提供します。Qualys WASにより、組織はWebアプリケーションの脆弱性を評価、追跡、修正できます。

Qualys WASは、欠陥注入テストを用いて脆弱性を検出する自動スキャナです。アプリケーションのフォームフィールドに特別に作成された文字列を挿入します。その後、WASはWebアプリケーションからの応答を分析し、脆弱性の存在を判定します。送信内容とアプリケーションの応答は
WASのレポート機能で確認できます。

Qualys WASは、組織がWebアプリケーションの脆弱性をスキャンすることを可能にします。Webアプリケーションの脆弱性を評価、追跡、修正します。Qualys WASは、組織がWebアプリケーションの脆弱性を評価、追跡、修正することを可能にします

主な機能

- ウェブアプリケーション（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インタラクティブなUI

- 機密データや秘密データのウェブアプリケーション上での取り扱い状況を特定

- カスタマイズ：ブラックリスト/ホワイトリスト、robots.txt、sitemap.xml など

- 一般的な認証方式をサポート

- 推奨されるセキュリティコーディングプラクティスと構成に関するレポートを表示

堅牢でスケーラブルなスキャン機能

- JavaScriptおよび埋め込みFlashを含むHTMLウェブアプリケーションのスキャンをサポート

- OWASPトップ10脆弱性を含むカスタムWebアプリケーション脆弱性の包括的検出

- 単純な情報漏洩と悪用可能な欠陥注入問題を区別

- カスタムWebアプリケーションの動作をプロファイリング

- カスタマイズ可能なパフォーマンスレベルによるスキャン性能の設定

Qualys Cloud Platform - ユーザーにとっての利点

Javaベースのバックエンドに実装された新技術は、ユーザーに多くの利点を提供します：

- 動的でインタラクティブなインターフェース、ウィザード、および多様な表示オプションを備えたスキャンデータを提示する新しいレポートテンプレートを備えたUI。

- WASと統合された統合ダッシュボード（UD）。UDは、すべてのQualysアプリケーションからの情報を1か所に集約し、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、様々な形式（html、pdf、暗号化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た、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、パラメータセット）に関連する、いくつかの広範な Qualys データセットの高速検索。

- Web アプリケーションをグループ化および整理するためのタグ（静的および動的）を作成および管理します。

- 大規模ネットワークのスキャンを最適化するため、利用可能性と負荷に基づいて複数のスキャナーに動的にスキャンを分散し、大規模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削減します。

REST API スキャン、CI/CD 統合、その他

Swagger バージョン 2.0 をサポートしており、DevOps チームは REST API の評価を効率化し、モバイルアプリケーションのバックエンドやモノのインターネット (IoT) サービスのセキュリティ態勢をより迅速に把握することができます。さらに、Jenkins 用の新しいネイティブプラグインにより、人気のある継続的インテグレーション/継続的デリバリー (CI/CD) ツールを使用しているチームのために、Web アプリケーションの脆弱性スキャンを自動化します。同時に、お客様は、新しい Qualys Browser Recorder（無料の Google Chrome ブラウザ拡張機能）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 REST (Representational State Transfer) API のスキャン - Qualys WAS は、SOAP (Simple Object Access Protocol) Web サービスのスキャンに加え、REST API のテストに Swagger 仕様を活用しています。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から参照可能であ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APIスキャン - PostmanはREST APIの機能テストに広く利用されるツールです。Postmanコレクションとは、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できる、ツールからエクスポート可能なファイルです。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におけるPostmanコレクションサポートのリリースにより、お客様は自社のAPI向けにPostmanコレクションを使用してAPIスキャンを設定する選択肢を得ました。

- ジェンキンスプラグイン - Qualys WAS ジェンキンスプラグインにより、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。このようにスキャンを統合することで、SDLC の早い段階でアプリケーションのセキュリティテストを実施し、セキュリティ上の欠陥を発見して排除することができるため、SDLC の後半で対応する場合に比べ、修正コストを大幅に削減することができます。プラグインはこちらからダウンロードしてください。

- Qualys Browser Recorder – この新しい Chrome 拡張機能により、ユーザーは Web ブラウザのアクティビティを記録し、スクリプトを保存して、繰り返し可能な自動テストを行うことができます。スクリプトは Qualys WAS で再生され、スキャンエンジンが複雑な認証やビジネスワークフローを正常にナビゲートできるようにします。Qualys Browser Recorder 拡張機能は無料で、Chrome Web Store から Qualys のお客様だけでなく、どなたでもご利用いただけます。

の開始方法

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。

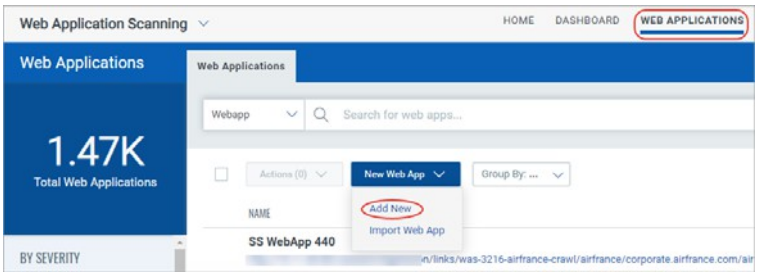
注記：新しいWAS UIでは、Webアプリケーション、認証、オプションプロファイル、検索リスト、パラメータセット、検出機能のみをサポートしています。本ガイドではこれらの機能の概要を説明します。詳細については、WASオンラインヘルプを参照してください。新しいWAS UIで利用できない機能については、従来のWAS UIバージョンへ誘導します。

さあ、 を始めましょう！

ログイン後、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」を選択してください。

新しいWASビューに切り替えるをクリック！

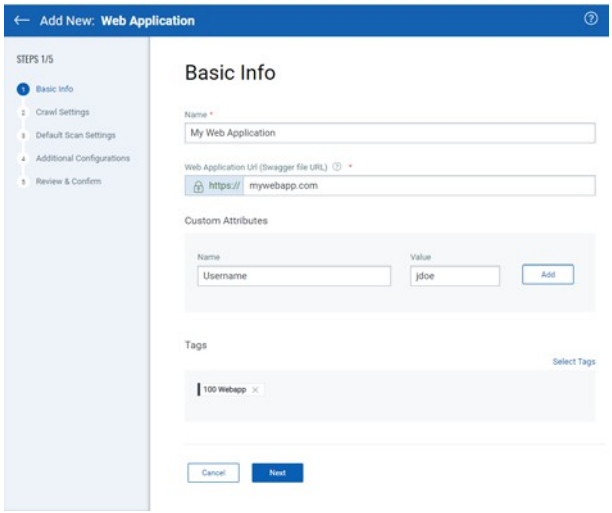
スキャンしたいWebアプリケーションについてお知らせください - **「Webアプリケーション」**＞**「新規Webアプリ」**をクリックするだけです。



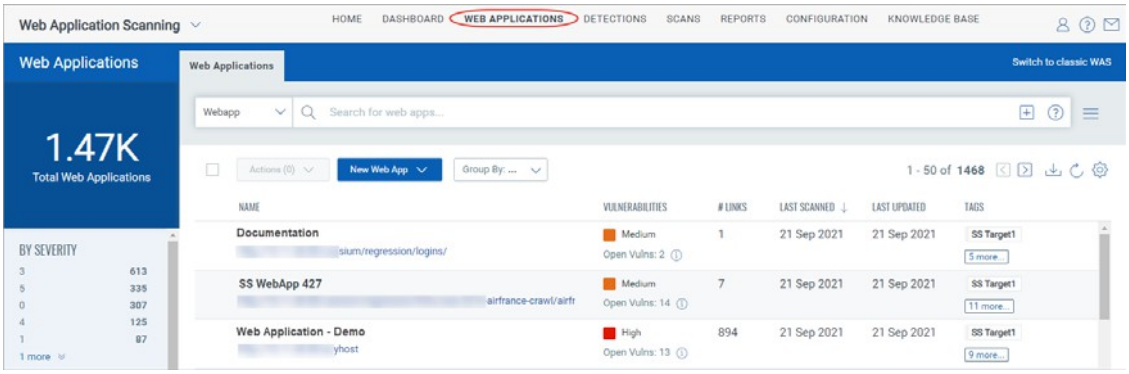
の設定を追加

新規にWebアプリを追加する際は、Webアプリケーション名とURLの入力が必須です。

外部サイトのマルウェアスキャンをご希望ですか？マルウェア監視を有効にするだけで、毎日自動的にマルウェアスキャンを実行します。



追加したWebアプリケーションは「Webアプリケーション」タブに表示され、設定編集やスキャン実行が可能です。



認証を使用する理由認証を使用することで、当社のサービスはクロール処理中にウェブアプリケーションの全領域にアクセスできます。これにより、より詳細な評価を実施可能です。多くのウェブアプリケーションでは、主要機能の利用に認証アクセスが必要です。ログインページなどのHTMLフォームやサーバーベース認証（HTTP Basic、Digest、NTLM、SSLクライアント証明書）に対して、認証スキャンを設定できます。認証タブに移動し、「新規レコード」を選択して、アクセス認証情報を含む認証レコードを設定してください。必要に応じてフォーム認証とサーバー認証を組み合わせることが可能です。セッション状態を監視し、クロール全体を通じて認証済みスキャンが認証された状態を維持します。

認証情報を提供する必要がありますか？

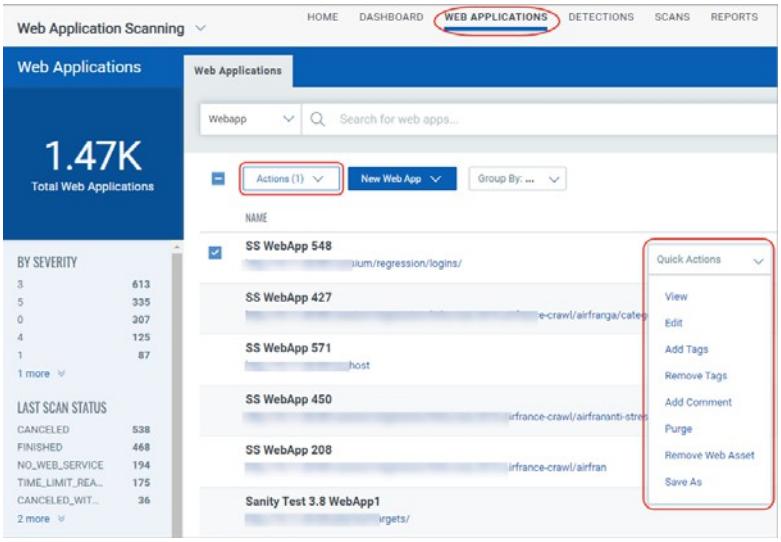
このWebアプリケーションの機能にアクセスするには認証が必要ですか？ 必要な場合は必ず認証レコードを選択してください。

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、スキャン設定オプションのセットです。開始には「初期WASオプション」をお勧めします。プロファイル内のオプションを編集することで、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

クイックアクションメニューを使用して個々のアプリケーションに対して操作を実行します。Webアプリケーションを選択またはホバーし、矢印をクリックするとクイックアクションメニューのオプションが表示されます。クイックアクション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・削除、Webアセットのスキャンデータの削除を行います。また、サブスクリプションや関連モジュールからWebアセットを削除したり、「名前を付けて保存」オプションを使用して同じ設定で新しいWebアセットを作成したりすることもできます。複数のWebアプリケーションに対しては、一括操作メニューを使用して操作を実行できます。



知っておくと良いこと

どのような脆弱性チェックがテストされますか？オプションプロファイルで特定脆弱性（確認済み、潜在的、情報収集）にスキャンを制限しない限り、ナレッジベースに記載されている全脆弱性チェック（QID）をスキャンします。新たなセキュリティ情報が公開されるたびにナレッジベースは随時更新されます。上部メニューの「ナレッジベース」をクリックしてください。

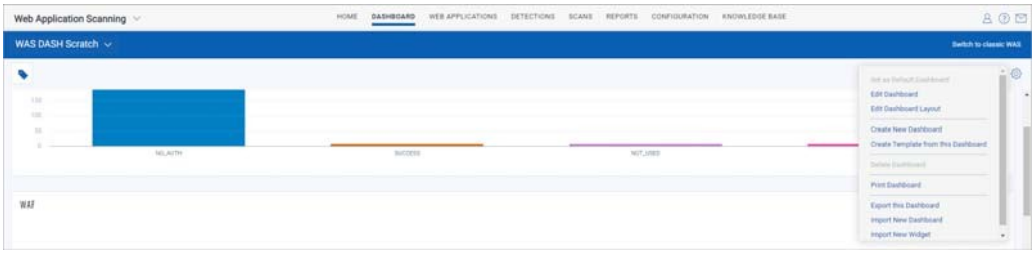
深刻度とは？ 各QIDには、当社サービスにより以下の深刻度レベルが割り当てられます：確認済み脆弱性（赤）、潜在的脆弱性（黄）、情報収集（青）。

ダッシュボードで最新のセキュリティ状況を確認

ダッシュボードではセキュリティ状態を一目で確認でき、常に最新情報が反映されます。ウェブアプリケーションとその検知状況を可視化するのに役立ちます。当社はWASにUnified Dashboard（UD）を統合しました。UDは全Qualysアプリケーションの情報を一元的に可視化します。UDは強力な新ダッシュボード基盤とプラットフォームサービスを提供し、既存ダッシュボード機能を強化するため、他の全製品で利用・活用されます。

右上の歯車アイコンをクリックすると、ダッシュボードの作成、編集、印刷が可能です。検索クエリ付きのウィジェットを追加し、関心のある情報を正確に表示するオプションもあります。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/インポートでき、アカウント間やQualysコミュニティ内で共有できます。

複数のダッシュボードを作成し、切り替えてデータの異なるビューを確認できます。



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、エクスポートが可能です。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) ダッシュボードの「ウィジェットを追加」ボタンをクリックして開始します。

2) 当社のウィジェットテンプレートから選択するか、独自のウィジェットを作成してください。

3) 右上の歯車アイコンをクリックし、メニューから設定をjson形式のファイルにエクスポートすることも可能です。これにより、アカウント間やQualysコミュニティ内でウィジェットを共有できます。

ヒント:

- デフォルトダッシュボードのウィジェット作成方法が知りたいですか？ウィジェットメニュー＞編集を選択すると設定を確認できます。

検出の管理

すべての検出結果を一元管理。検出タブはアプリケーションセキュリティ脆弱性の検出・管理・情報の中核領域として機能します。検出タブにはすべての検出結果（Qualys、Burp、Bugcrowd）が表示されます。

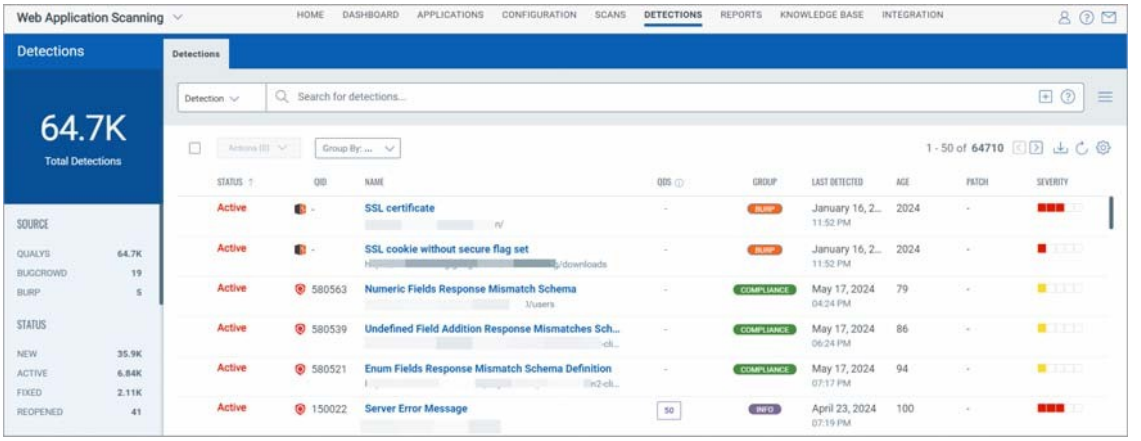
左ペインには検索を強化し検出タイプを素早く特定するためのフィルターを用意しています。一般的なフィルターに加え、検索トークンを使用して複雑な検索式を構築し、要件に合致する検出結果を見つけられます。例：10日以上経過したBURP検出結果を表示するには、検索バーに次の検索式を入力してください：vulnerability.source:"BURP" and vulnerability.age>10。

リストに表示されるアイコンで検出タイプを区別できます。

 - Qualys検出

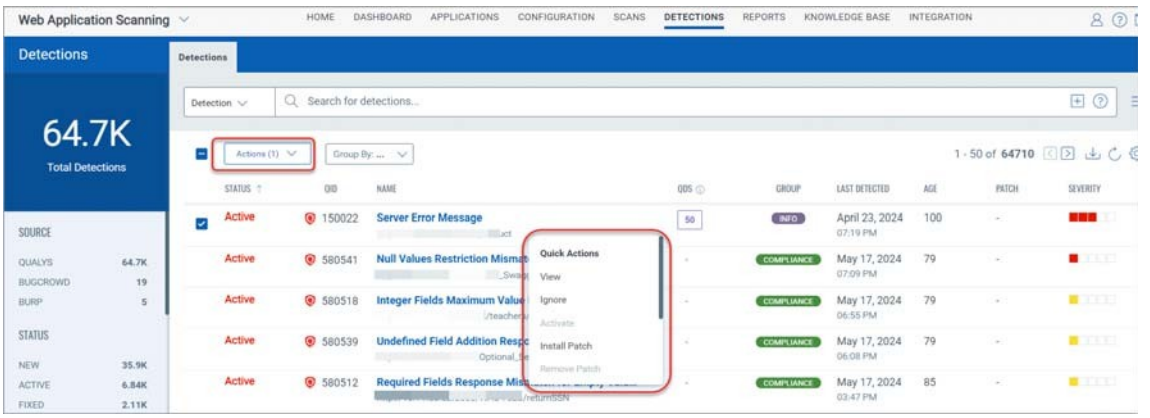
 - Burpの問題

- Bugcrowdの報告



検出項目に対するアクションの実行

クイックアクションメニューを使用して個々の検出項目に対してアクションを実行します。検出項目を選択またはホバーし、矢印をクリックするとクイックアクションメニューのオプションが表示されます。クイックアクションメニューを使用して、編集、無視、無視した検出項目の再有効化を行います。検出項目の深刻度レベルの編集や復元、検出項目へのコメント追加も可能です。アクションメニューを使用して複数の検出項目に対してアクションを実行できます。



Seleniumを使用したスキャン スクリプト

Qualys Browser Recorder（QBR）を使用してSeleniumスクリプトを作成できます。QBRは、ウェブアプリケーションの自動テスト用スクリプトを記録・再生する無料のブラウザ拡張機能（Google Chromeブラウザ用）です。QBRでは、ブラウザ内のWeb要素をキャプチャし操作を記録することで、自動テストケースを迅速かつ容易に生成・編集・再生できます。また、ブラウザに現在表示されているページからUI要素を選択し、パラメータ付きSeleniumコマンドのリストから選択することも可能です。これらのスクリプトをWASで使用することで、スキャナがWebアプリケーション内の複雑な認証プロセスや業務ワークフローをナビゲートするのを支援できます。

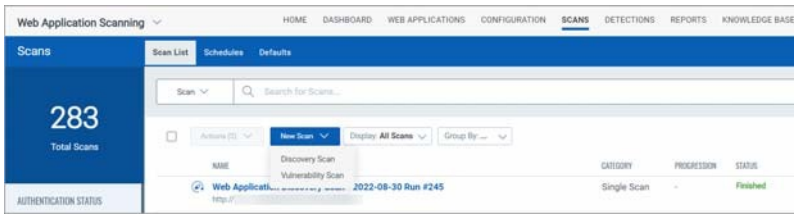
Webアプリケーションで一般的に使用される認証メカニズムにシングルサインオン（SSO）があります。これは複雑さを伴い、Qualys WASでの認証とスキャン時に混乱を招く可能性があります。QBRを使用することで、スキャナー向けの認証メカニズムを簡素化できます。詳細な手順については、当社のブログ記事を参照してください。

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ではテストデータを含むフォームが送信されます。これを望まない場合は、ブラックリスト設定、POSTデータブラックリスト設定を追加するか、オプションプロファイル内でGETメソッドのみを選択してください。これらの設定を使用する場合、Webアプリケーションの特定領域のテストは対象外となり、該当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留意してください。

最初に検出スキャンを実行することを推奨します

発見スキャンは、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を収集します。これは、スキャンがどこを調査するか、また脆弱性スキャン用にブラックリスト登録すべきURIがあるかどうかを理解するのに有効な方法です。

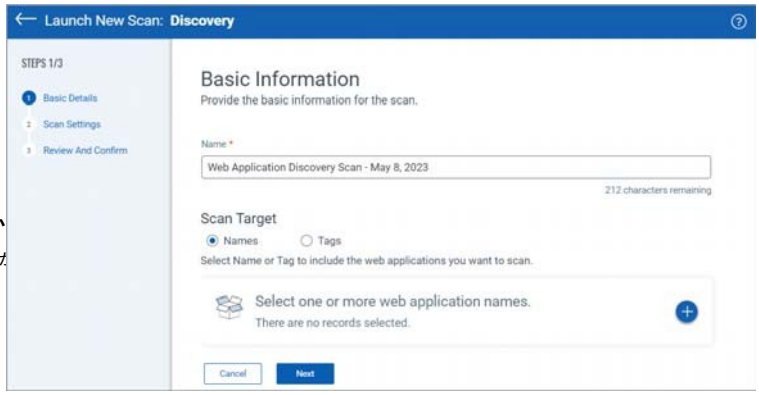
[スキャン] ＞ **[スキャン一覧]** に移動し、[**新規スキャン**] ＞ [**ディスカバリースキャン**] をクリックします。



スキャンウィザードが手順を案内します。

スキャン対象のWebアプリケーションを指定し、スキャン設定を選択してください（*は必須項目）。

スキャンを開始する準備ができましたか？「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、スキャン設定オプションのセットです。開始には「初期WASオプション」をお勧めします。プロファイル内のオプションを編集することで、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。

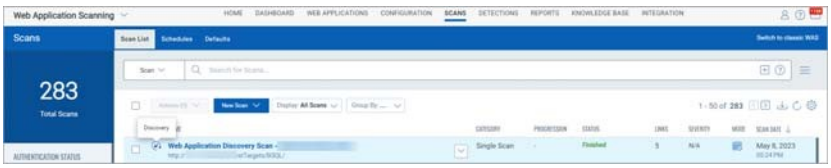
認証情報を提供する必要がありますか？

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？必要な場合は、必ず認証レコードを選択してください。

スキャナー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では、ネットワーク境界での外部スキャン用にクラウドスキャナーを提供しています。内部スキャンにはスキャナーアプライアンス（物理または仮想）の設定が必要です。VM/VMDR ＞ スキャン ＞ アプライアンスに移動し、新規メニューからオプションを選択すると、手順を案内します。（Express Liteをご利用ですか？アカウントには外部スキャン、内部スキャン、または両方が有効化されている可能性があります）。

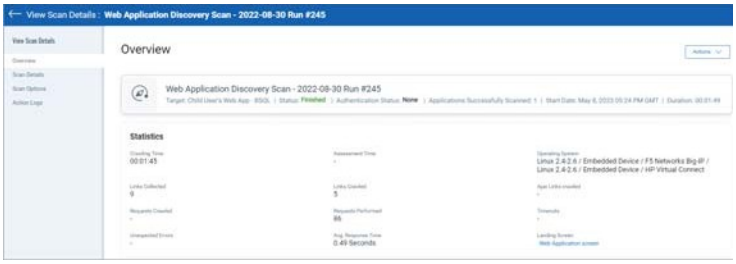
完了したスキャンをダブルクリックするとスキャンビューが表示されます。



スキャンビュー

概要ではスキャン結果の概要を確認できます。

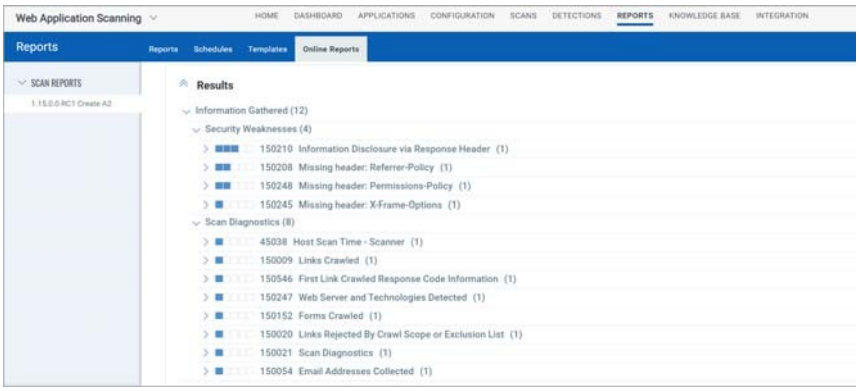
完全なスキャンレポートを表示したいですか？「レポートを表示」ボタンをクリックするだけです。



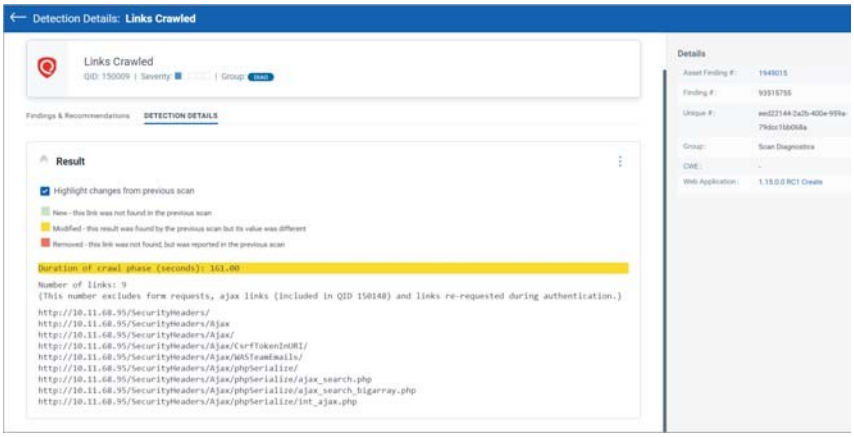
完全なスキャンレポート

各QIDは実施したセキュリティチェックと収集した情報です。詳細を確認するには行をクリックしてください。

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



QID 150009 [クロールされたリンク] の結果には、クロールされたリンクの一覧が表示されます。



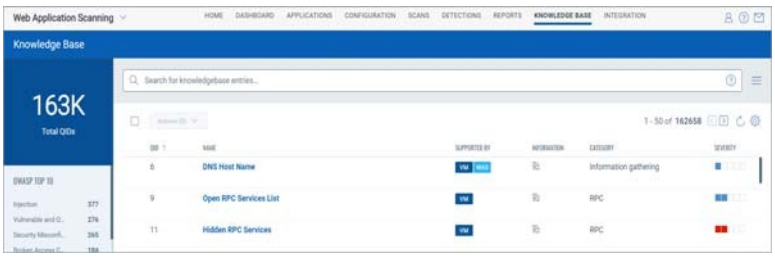
脆弱性に関する次回スキャン

脆弱性スキャン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態を把握します。

知っておくと良いこと

どのような脆弱性チェックが実施されますか？オプションプロファイルで特定脆弱性（確認済み、潜在的、情報収集対象）にスキャンを限定しない限り、ナレッジベースに記載されている全脆弱性チェック（QID）をスキャンします。新たなセキュリティ情報が公開されるたびにナレッジベースは随時更新されます。

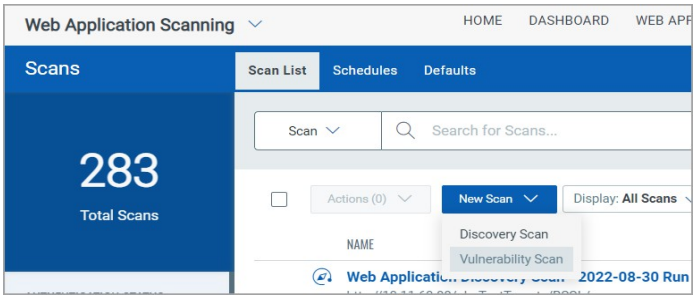
トップメニューの「ナレッジベース」をクリックしてください。



深刻度とは？各QIDには、当社サービスにより以下の深刻度レベルが割り当てられます：確認済み脆弱性（赤）、潜在的脆弱性（黄）、情報収集（青）。

スキャンを開始する

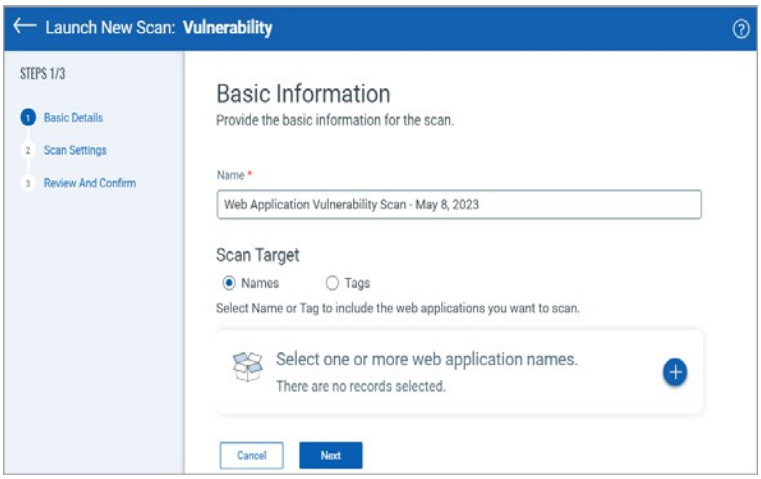
トップメニューの「スキャン」に移動し、「新規スキャン」＞「脆弱性スキャン」を選択してください。



起動スキャンウィザードが手順を案内します。

脆弱性スキャン対象のWebアプリケーションを指定し、スキャン設定を選択してください。

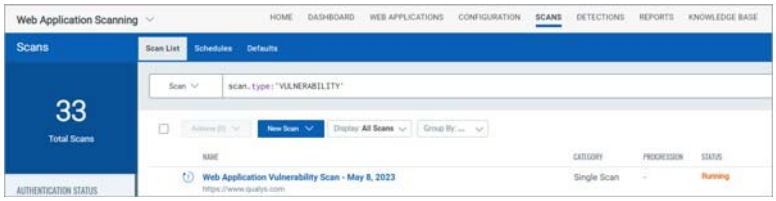
スキャンを開始する準備はできましたか？「続行」をクリックし、設定を確認してから「完了」をクリックしてください。



スキャン進捗の確認

ステータス列には状態（この場合は実行中）が表示されます。

詳細を確認するには、スキャン行をダブルクリックしてください。



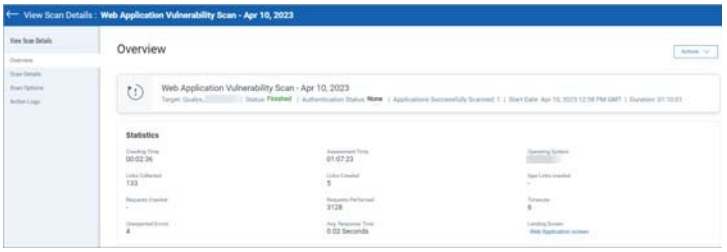
するとスキャン進行状況バーが表示され、スキャン終了予定時刻の目安を確認できます。

スキャン表示

表示方法：スキャンにカーソルを合わせ、クイックアクションメニューから「表示」を選択します。

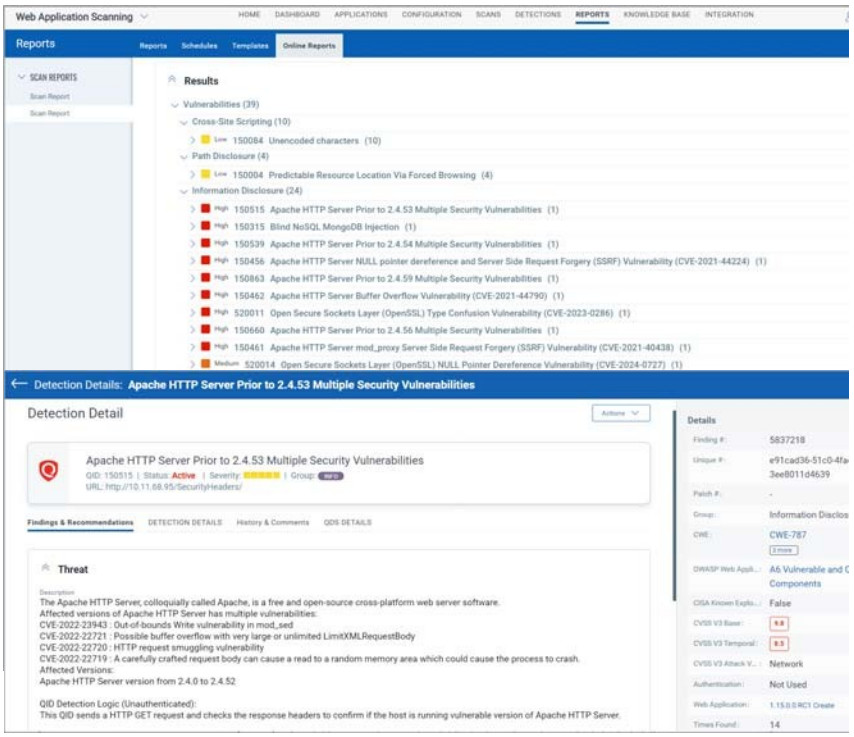
概要ではスキャン結果の概要が表示されます。

完全なスキャンレポートを確認したいですか？「レポートを表示」ボタンをクリックするだけです。

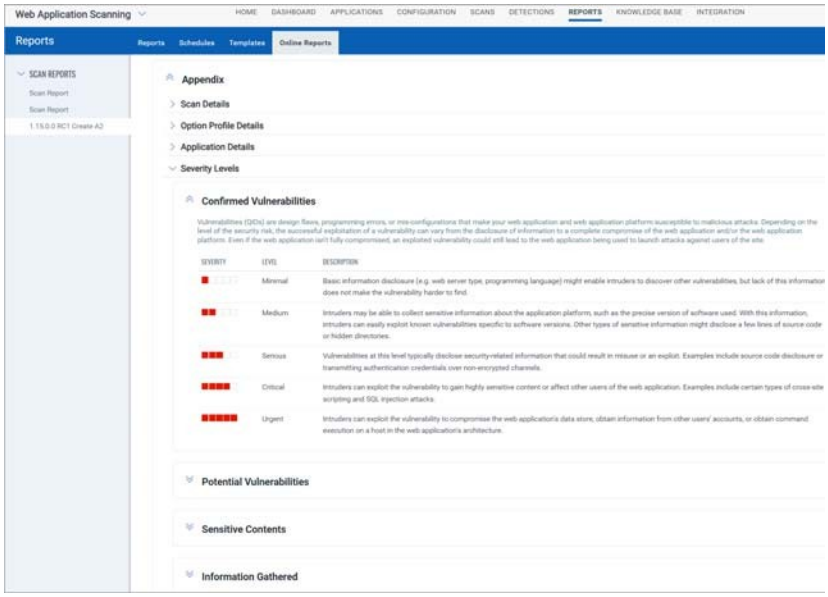


完全なスキャンレポート

脆弱性は
グループ別に分類されています。

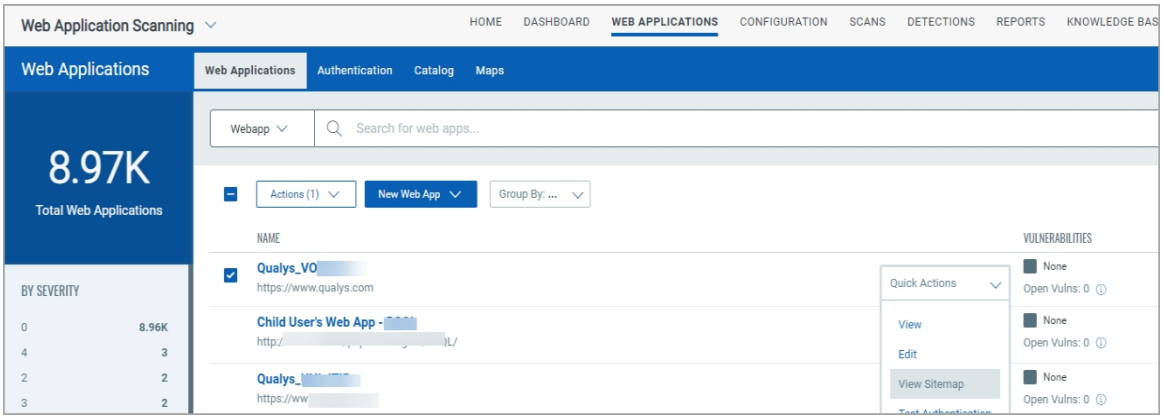


深刻度のレベルが意味する内容を簡単に確認するには、付録を参照してください。

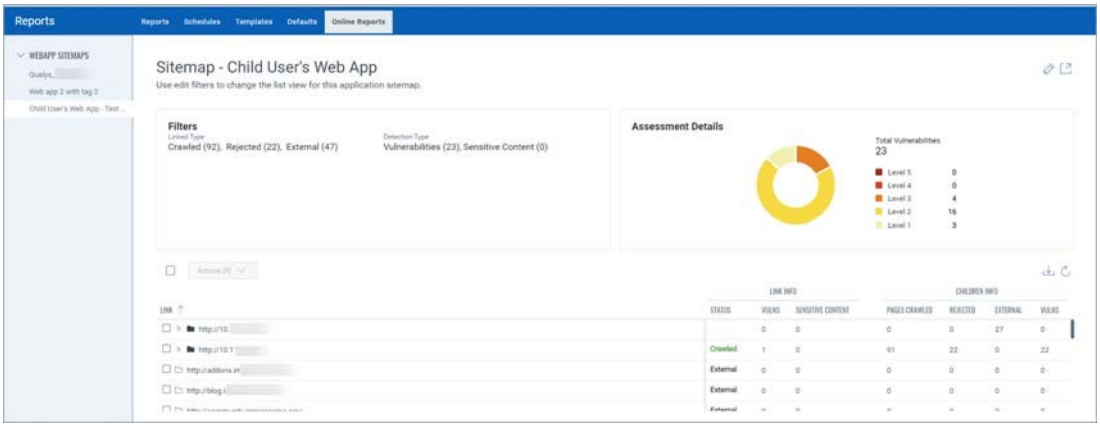


サイトマップをご覧ください

Webアプリケーションサイトマップは、クロールされたリンク、検出された脆弱性、および機密コンテンツを把握しながら、スキャンされた全ページ/リンクの一覧を簡単に取得する方法を提供します（Webアプリケーションに移動し、対象のWebアプリを選択後、クイックアクションメニューから「サイトマップを表示」を選択してください）。



以下は、合計271ページがクロールされ、306件の脆弱性と8件の機密コンテンツ検出があったWebアプリケーションのサイトマップ例です。

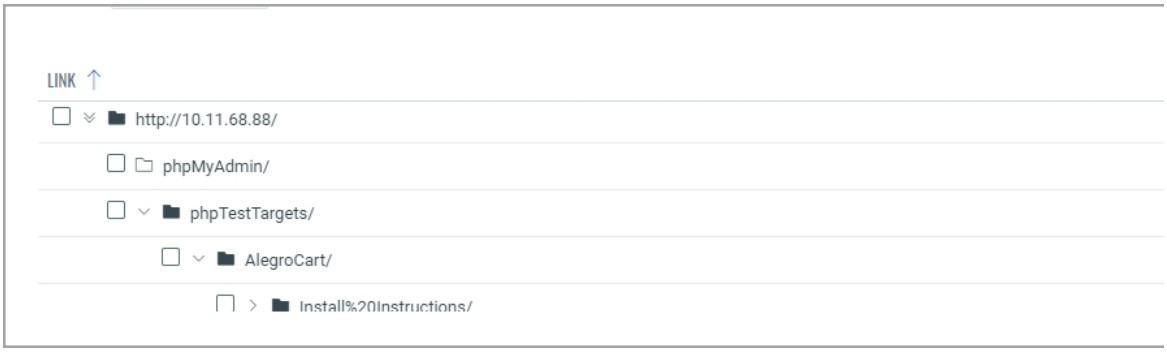


サイトマップのフィルタリング

編集アイコンをクリックするとページフィルターが表示されます。例：現在の脆弱性については「脆弱性」を選択。

ネストされたリンクを表示するにはドリルダウンしてください

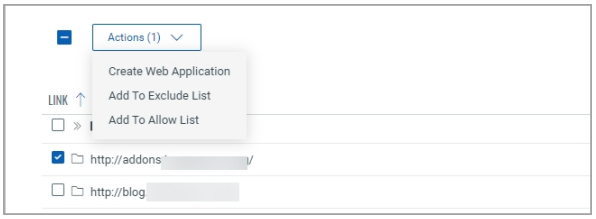
これにより、アプリケーションの異なる部分のセキュリティを調査できます。親フォルダーをダブルクリックすると子リ



ンクが表示されます。

Web アプリリンクに対してアクションを実行する

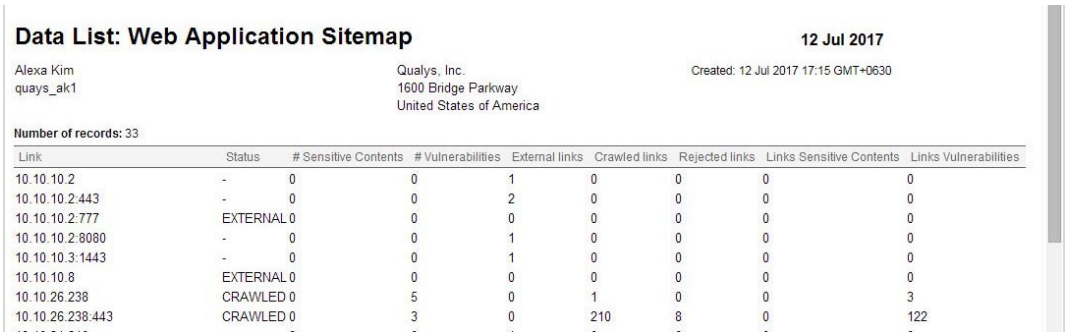
リンクから新しいWebアプリケーションを作成するか、リンクをブラックリストまたはホワイトリストに追加します。ブラウザでリンクを表示するには、該当行を選択し、詳細パネル（右側）のリンクをクリックしてください。



ウェブアプリリンクを簡単にエクスポート

検出データ付きのスキャン済みリンクを複数形式でダウンロード

ダウンロードレポートでは、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

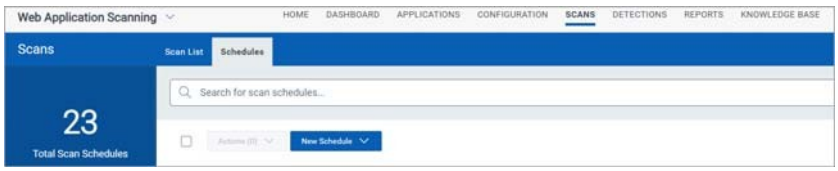
Number of records: 33

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

ヒント - スキャンを自動実行するようにスケジュール設定してください

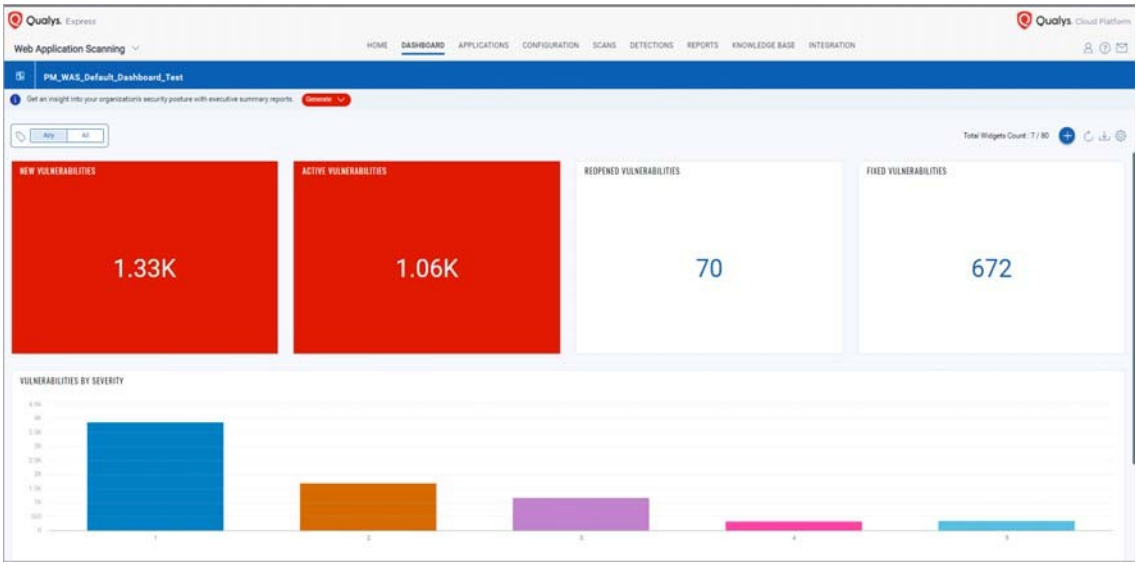
スキャンを繰り返し実行するスケジュールを設定することをお勧めします。これにより、組織にとって都合の良い時間帯に（毎日、毎週、または毎月）自動的に結果を取得できます。

[スキャン] > [スケジュール] に移動し、[新しいスケジュール] を選択してください。



ダッシュボードで最新のセキュリティ状況を確認

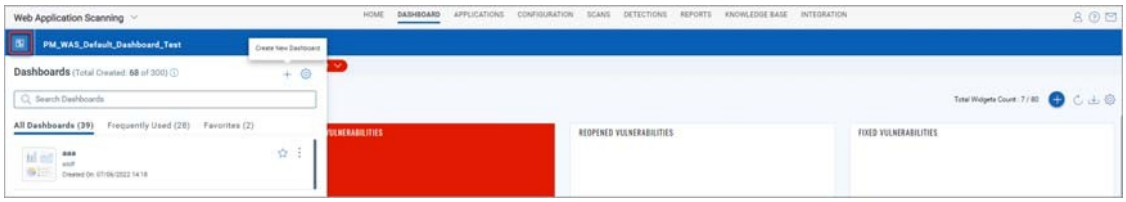
ダッシュボードではセキュリティ状態が一目で確認でき、最新のスキャン結果で常に更新されます。非常にインタラクティブで、セクションやリンクをクリックするだけで詳細情報を確認できます。



カスタムダッシュボードを簡単に作成し、ビューを切り替えられます

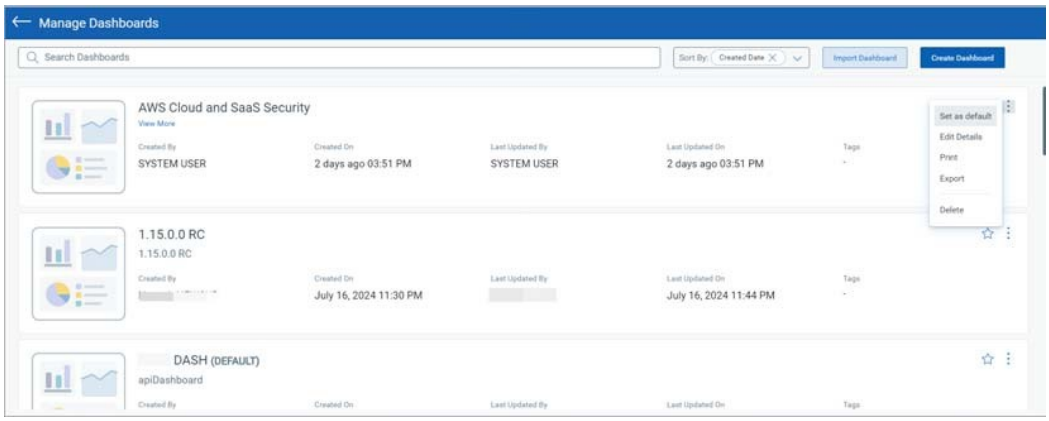
ダッシュボードを、関心のある領域、特定のWebアプリケーション、本番環境にいつでも集中させられます。カスタムダッシュボードをアカウントのデフォルトに設定することも可能です。

アイコンをクリック > 新規ダッシュボードを作成。



デフォルトのダッシュボードを変更できます。ハイライトされたアイコンをクリックし、ダッシュボードを管理します。

デフォルトダッシュボードを変更するには、ダッシュボード一覧から対象を選択し、「デフォルトに設定」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。カタログ内のエントリが実際にWASでスキャンすべきWebアプリケーションであるかどうかを判断するには、手動によるトリアージが必要です。

カタログエントリは、アカウント内の完了済みマップ、脆弱性スキャン、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リクエストに応答したWebサーバーです。
（カタログ機能はExpress Liteユーザーにはご利用いただけません。）

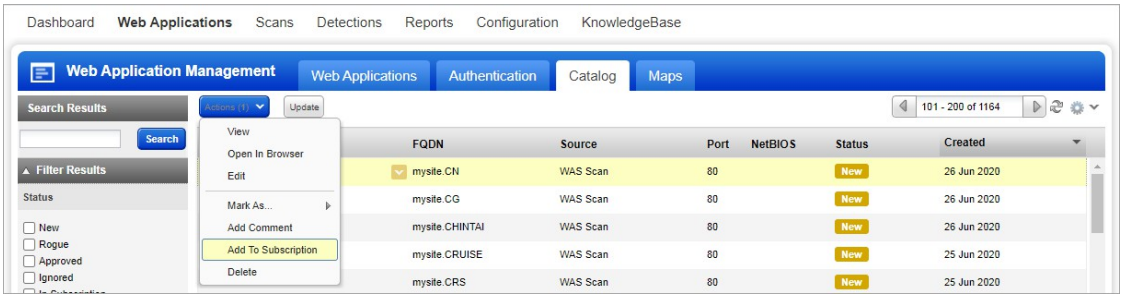
どのように始めればよいですか？

カタログは、ユーザー（または他のユーザー）がVMアプリケーションを使用してマップや脆弱性スキャンを実行するか、WASスキャンを実行するまで空の状態です。これらが完了すると、結果を処理する準備が整います。

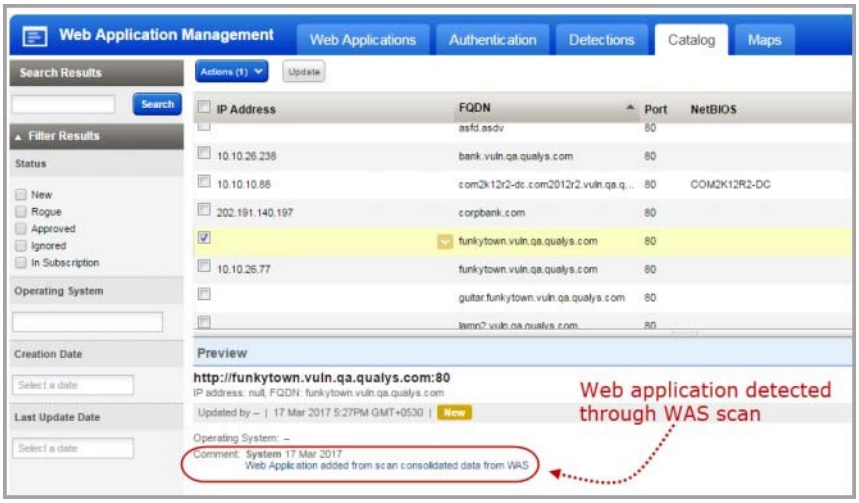
- スキャン結果の処理：Web Applications ＞ Catalog に移動し、リスト上部の「更新」をクリックします。

- プロセスマップ結果: [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。

新たに検出されたWebアプリケーションの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簡単に追加し、セキュリティリスクをスキャンできます。



ウェブアプリケーションの所在が不明な場合でも、その位置を特定できます。強化された検出手法により、サーバーで複数の仮想ホストが稼働している場合でも、存在するアプリケーションをより正確に識別し、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もののウェブ資産として追加されていないウェブアプリケーションで更新されます。



検出の管理

すべての検出結果を一元管理。検出タブはアプリケーションセキュリティ脆弱性の検出・管理・情報の中核領域として機能します。検出タブにはすべての検出結果（Qualys、Burp、Bugcrowd）を一覧表示します。

検出タイプを強化し、迅速に特定するためのフィルターを用意しています。一般的なフィルターに加え、検出タイプに応じて、各検出タイプ固有の追加フィルターが表示されます。例えば、検出タイプを「Burp」に選択すると、Burp関連の検出に適用可能なフィルターが有効化され、その他の非適用フィルターは無効化されます。

検出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検出
- Burpの問題
- Bugcrowdの提出

Burpの 検出結果をインポートしますか？

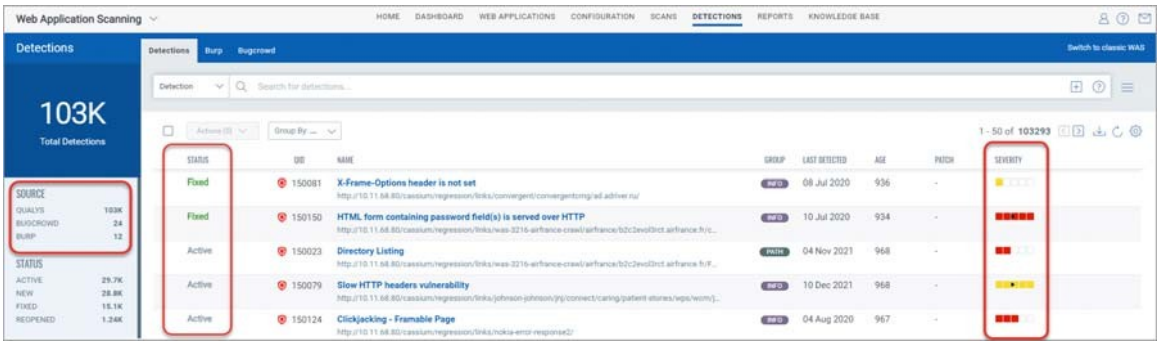
（この機能はExpress Liteユーザーには利用できません。）

Qualys WAS Burp拡張機能をお試しになることをお勧めします。これにより、WASの検出結果をBurp Repeaterに直接インポートし、脆弱性を手動で検証できます。この拡張機能はBurp Suite Professional版とCommunity Editionの両方で動作します。

Qualys WAS Burp拡張機能は、BAppストアの「Extender」タブから入手可能です。詳細については、Qualysコミュニティのブログ記事をご参照ください。

または、[検出] > [Burp] > [インポート] 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。

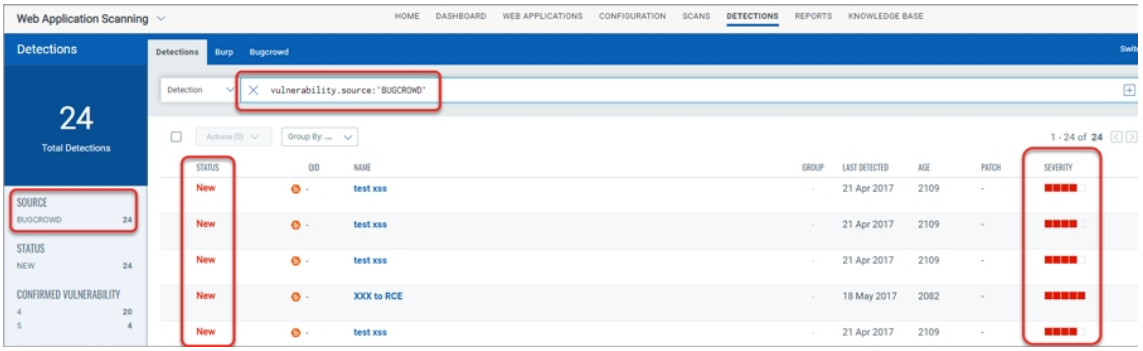
Burpレポートからインポートされた問題は「検出」リストに表示されます。「検出」>「検出」に移動し、検索フィルターの「検出タイプ」でBurpを選択すると、検出日時・ステータス・深刻度を含む詳細情報を確認できます。



との連携Bugcrowd

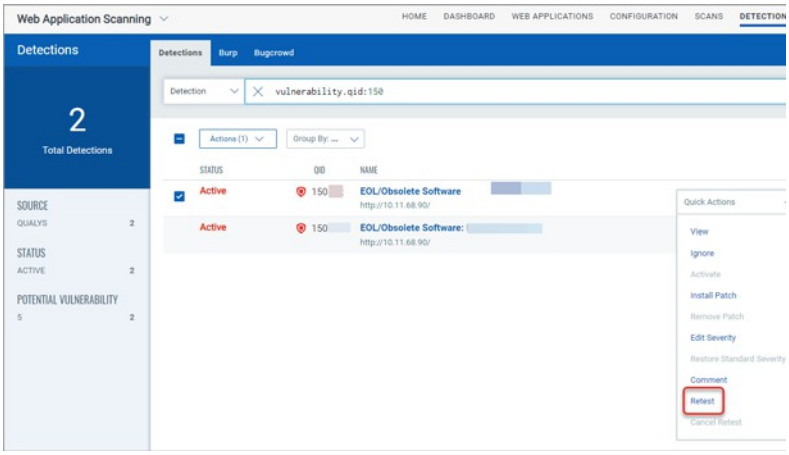
Bugcrowdのお客様は、承認済みのBugcrowd提出内容をWASアカウントにインポートすることも可能です。当社のBugcrowd連携機能により、WASによって特定された脆弱性と、Bugcrowdが管理するバグ報奨金プログラムを通じて発見された脆弱性を閲覧・報告する方法を提供します。

検出 > Bugcrowd > インポート 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、その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ファイルでインポートされた問題は、問題リストに表示されます。検出 > 検出 に移動します。



のフルスキャンを実行せずに複数の検出結果を再テストする

はい、選択した複数の検出結果に対してスキャンを実行することで、脆弱性の検出結果を簡単に再テストできます。再テスト可能なのは、潜在的な脆弱性、確認済み脆弱性、および機密コンテンツのみです。同じQIDおよびWebアプリケーションに属する複数の検出結果をまとめて、単一のバッチで再テストを実行できます。再テストスキャンでは、最新のスキャンで使用された設定がそのまま適用されます。いずれかの検出結果の再テストをキャンセルすると、そのバッチ全体の再テストスキャンがキャンセルされます。

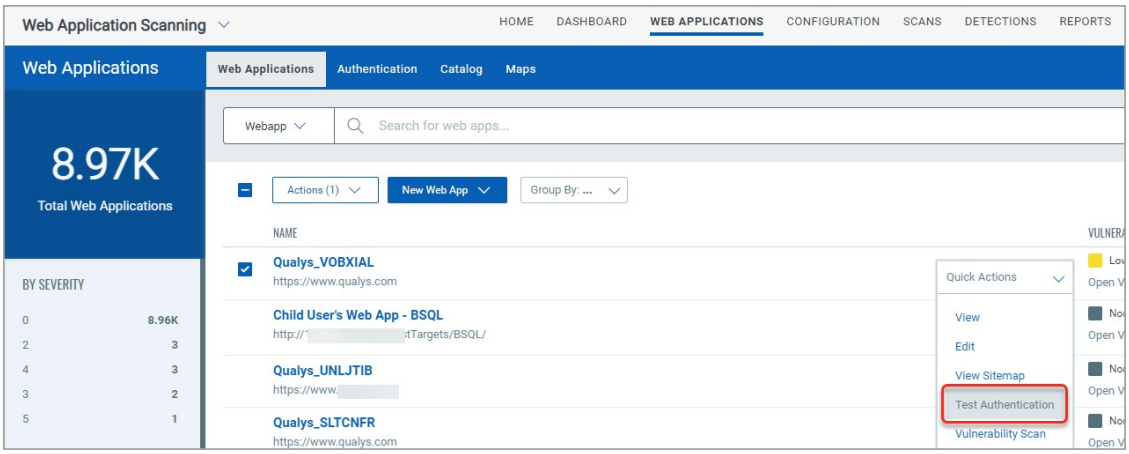


[検出] > [検出] に移動します。左ペインのフィルターを使用して、同じ QID および Web アプリケーションのすべての検出結果を表示できます。再テストする検出結果を選択します。[アクション] メニューから [再テスト] を選択します。確認すると、選択したすべての検出結果に対して再テストスキャンが一括で開始されます。

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せずにテストできます。Webアプリケーションの認証を迅速にテストし、スキャナーのWebアプリケーションへの認証能力を確認できます。

Web Applications > Web Applications に移動し、Web アプリケーションを選択します。クイックアクションメニューから「Test Authentication」を選択します。



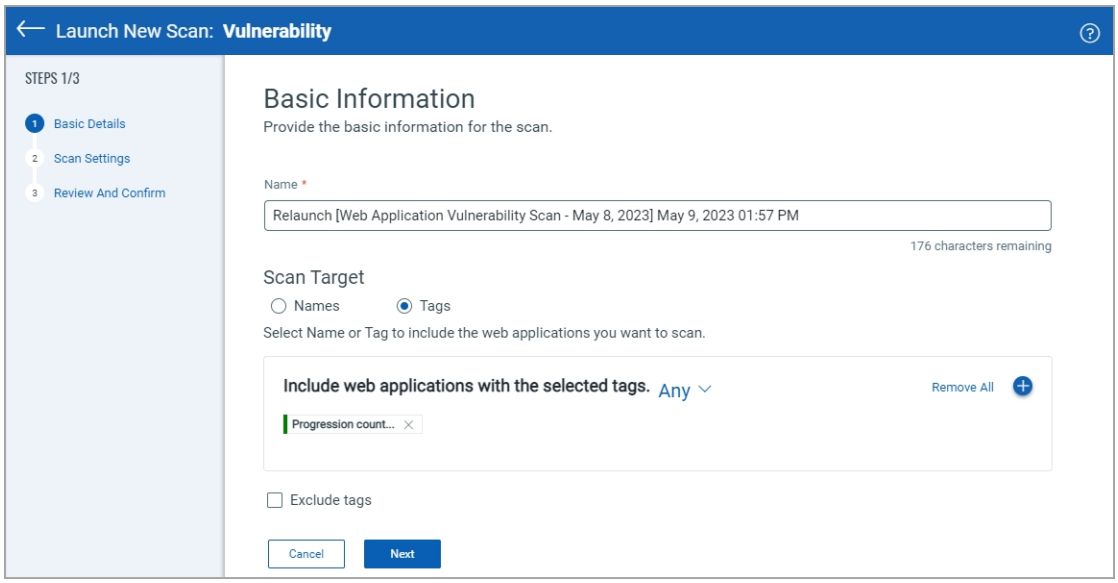
認証テストスキャンが完了状態になったら、クイックアクションメニューから「レポートを表示」を選択し、認証テストスキャンレポートを確認します。

Web アプリケーションの高ボリュームスキャン

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し、大規模なWebアプリケーションスキャンプログラムのサポート能力を強化しました。この機能により、組織は自社内に存在する数百から数千ものWebアプリケーションをスキャンでき、どのスキャンが実行中か、どのスキャンが完了したかを詳細に把握できます。

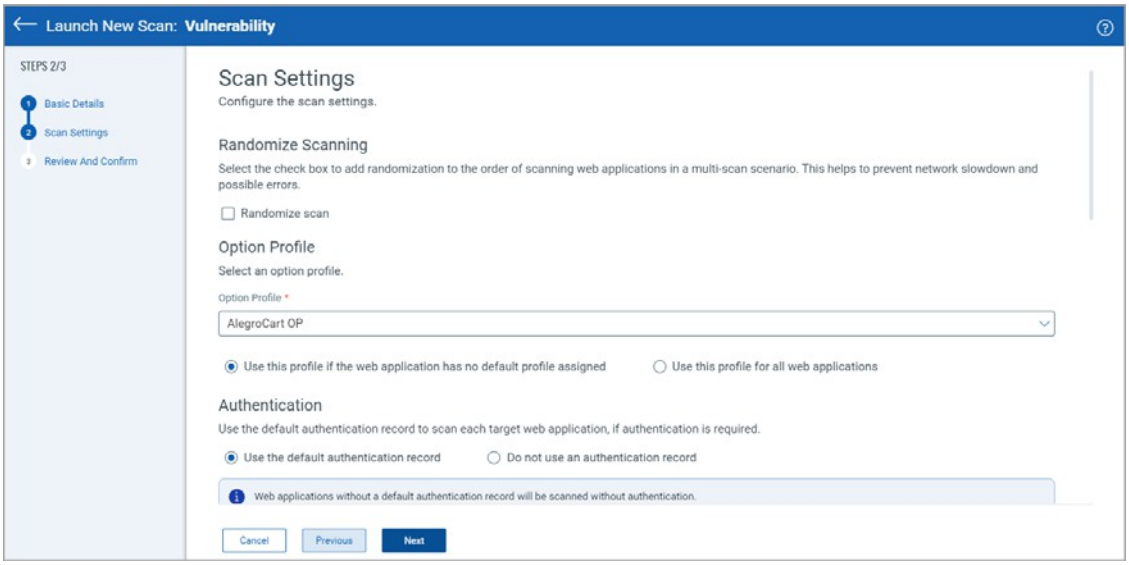
対象アプリケーションの選択 - 個別アプリまたはタグを選択

Qualysのアセットタグ付けを活用し、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すれば、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ない？問題ありません。ユーザーが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、スキャナーアプライアンス

マルチスキャン機能では、Webアプリケーションのデフォルト設定を受け入れるか、デフォルト設定を上書きするか、多くのオプションが提供されます。



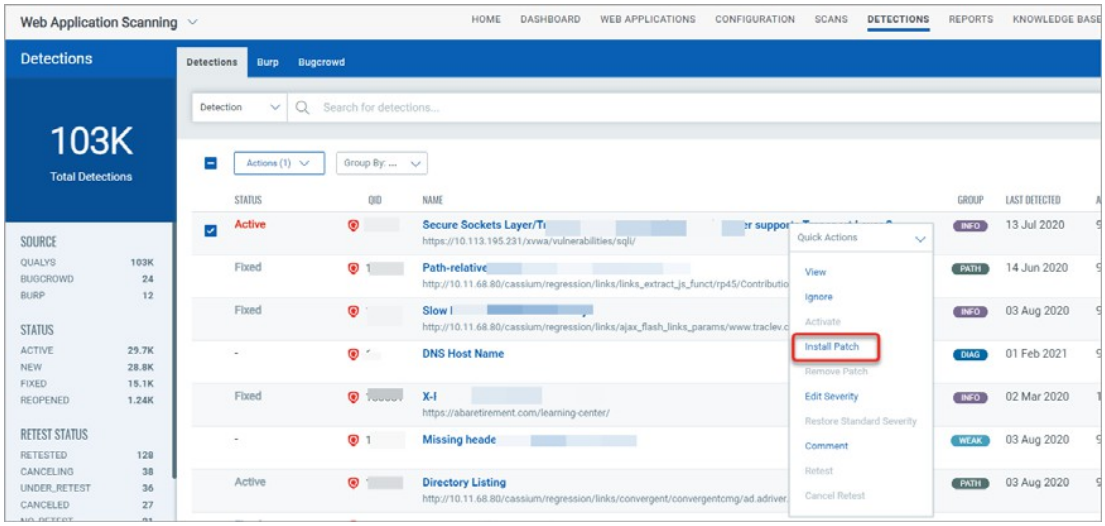
Seleniumを使用したスキャン スクリプト

Qualys Browser Recorder（QBR）を使用してSeleniumスクリプトを作成できます。QBRは、ウェブアプリケーションの自動テスト用スクリプトを記録・再生する無料のブラウザ拡張機能（Google Chromeブラウザ用）です。QBRでは、ブラウザ内のWeb要素をキャプチャし操作を記録することで、自動テストケースを迅速かつ容易に生成・編集・再生できます。また、ブラウザの現在表示ページからUI要素を選択し、パラメータ付きSeleniumコマンド一覧から選択することも可能です。これらのスクリプトをWASで活用すれば、スキャナがWebアプリケーション内の複雑な認証プロセスや業務ワークフローをナビゲートする際に役立ちます。

Webアプリケーションで一般的に使用される認証メカニズムにシングルサインオン（SSO）があります。これは複雑さを伴い、Qualys WASでの認証とスキャン時に混乱を招く可能性があります。QBRを使用することで、スキャナー向け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、当社のブログ記事を参照してください。

仮想パッチ サポート

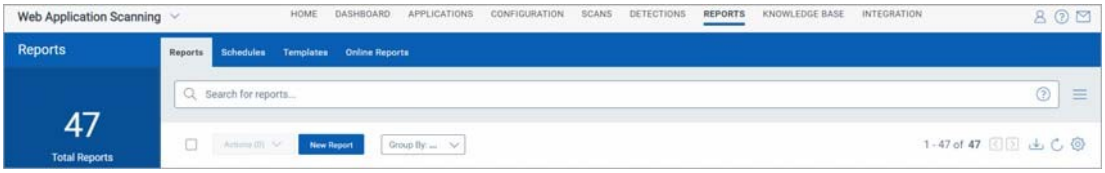
アカウントでWASとWAFが有効化されている場合、WASでは選択した脆弱性（検出項目）に対して仮想パッチをインストールできます。インストール後、選択した脆弱性の悪用をブロックするファイアウォールルールが自動的に追加されます。WAF APIに仮想パッチ管理を支援する機能が追加されました。

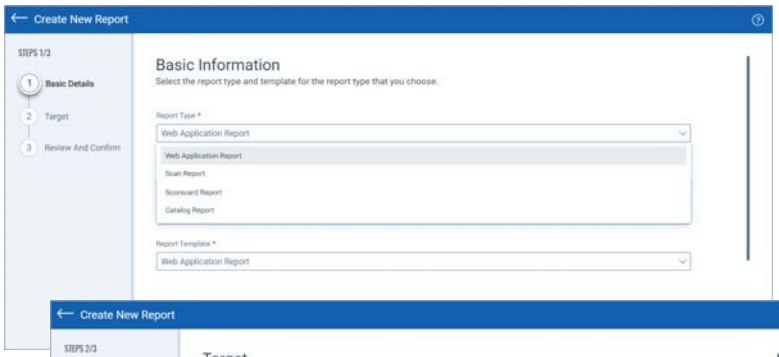


レポート機能

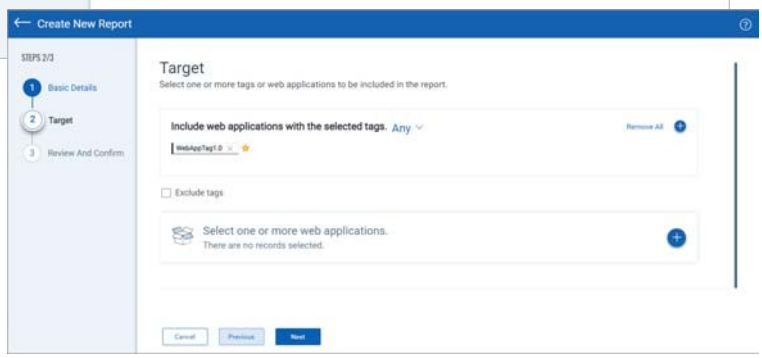
レポート作成手順

「新規レポート」を選択するか、右側の「+」ボタンをクリックします。



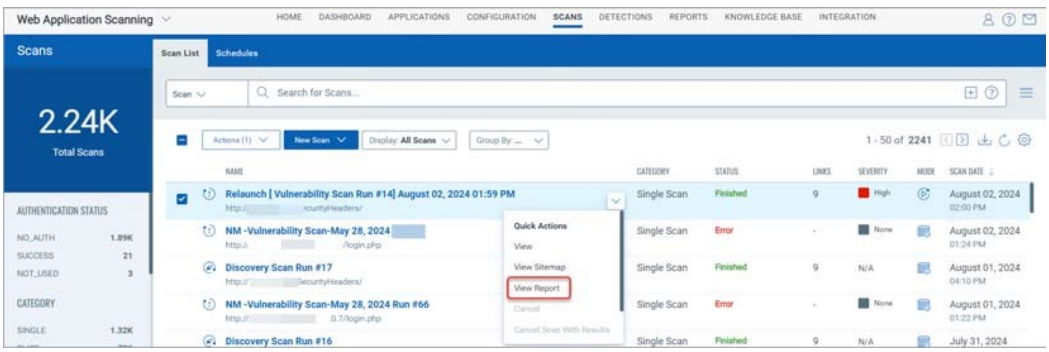


レポートの種類を選択してください。この場合は「Webアプリケーションレポート」です。

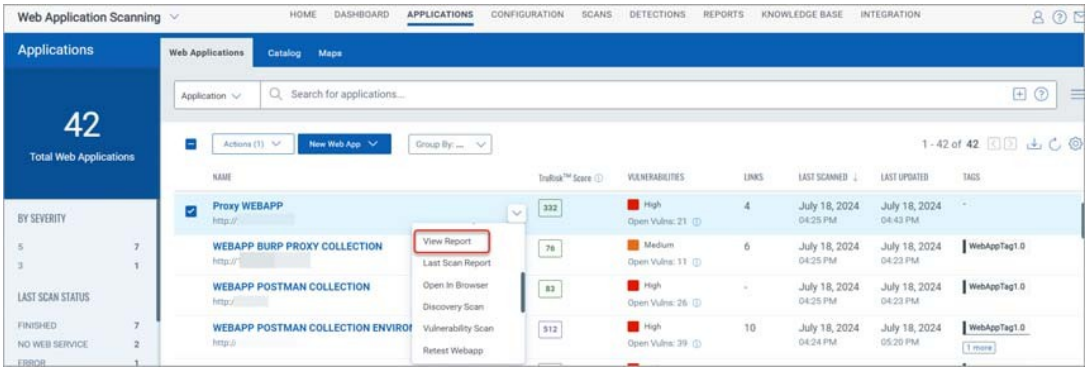


タグおよび/または名前でWebアプリケーションを選択

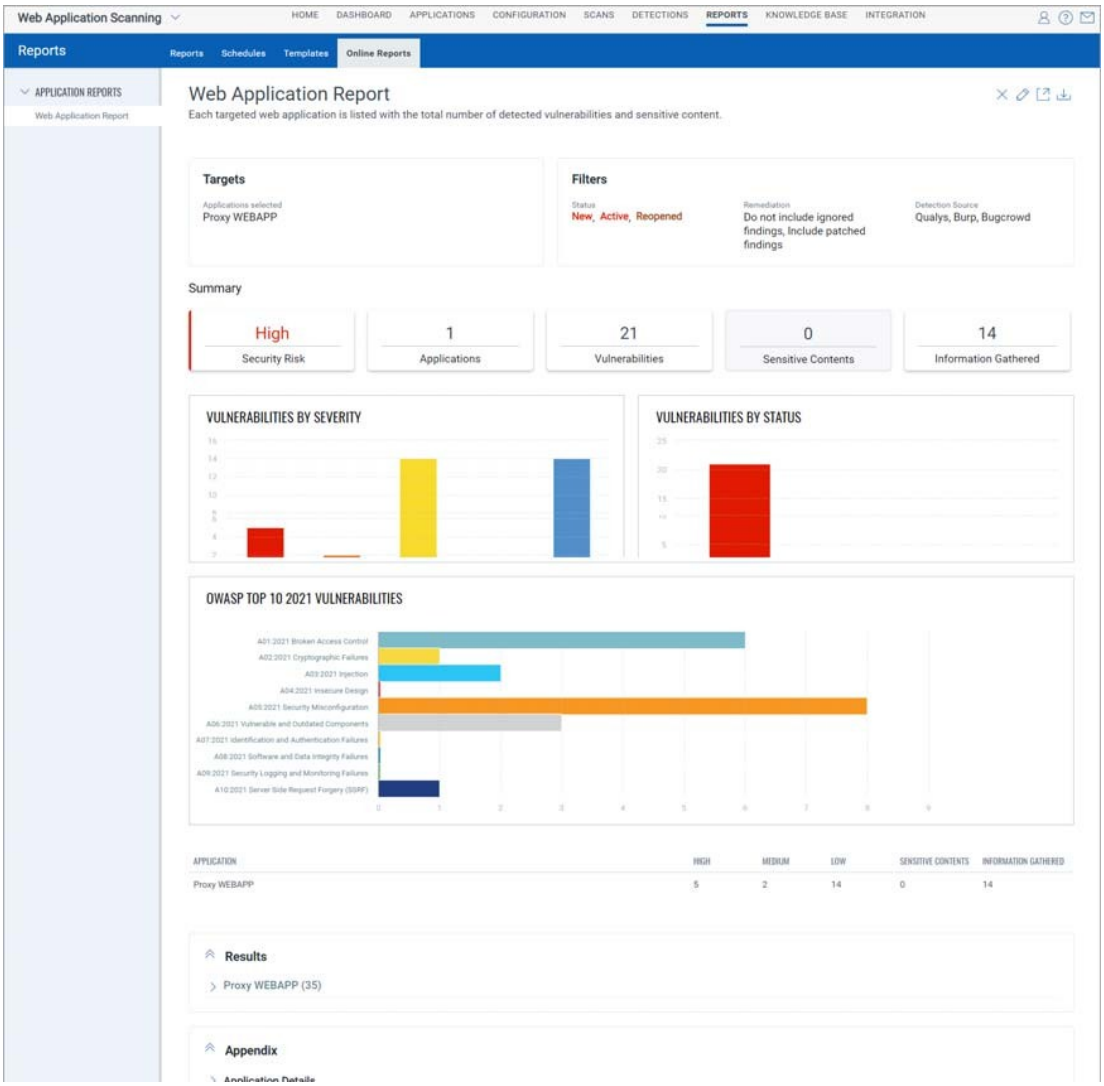
あるいは、スキャン一覧からスキャンを選択し、クイックアクションメニューの「レポートを表示」を選択することで、スキャンレポートを素早く生成できます。



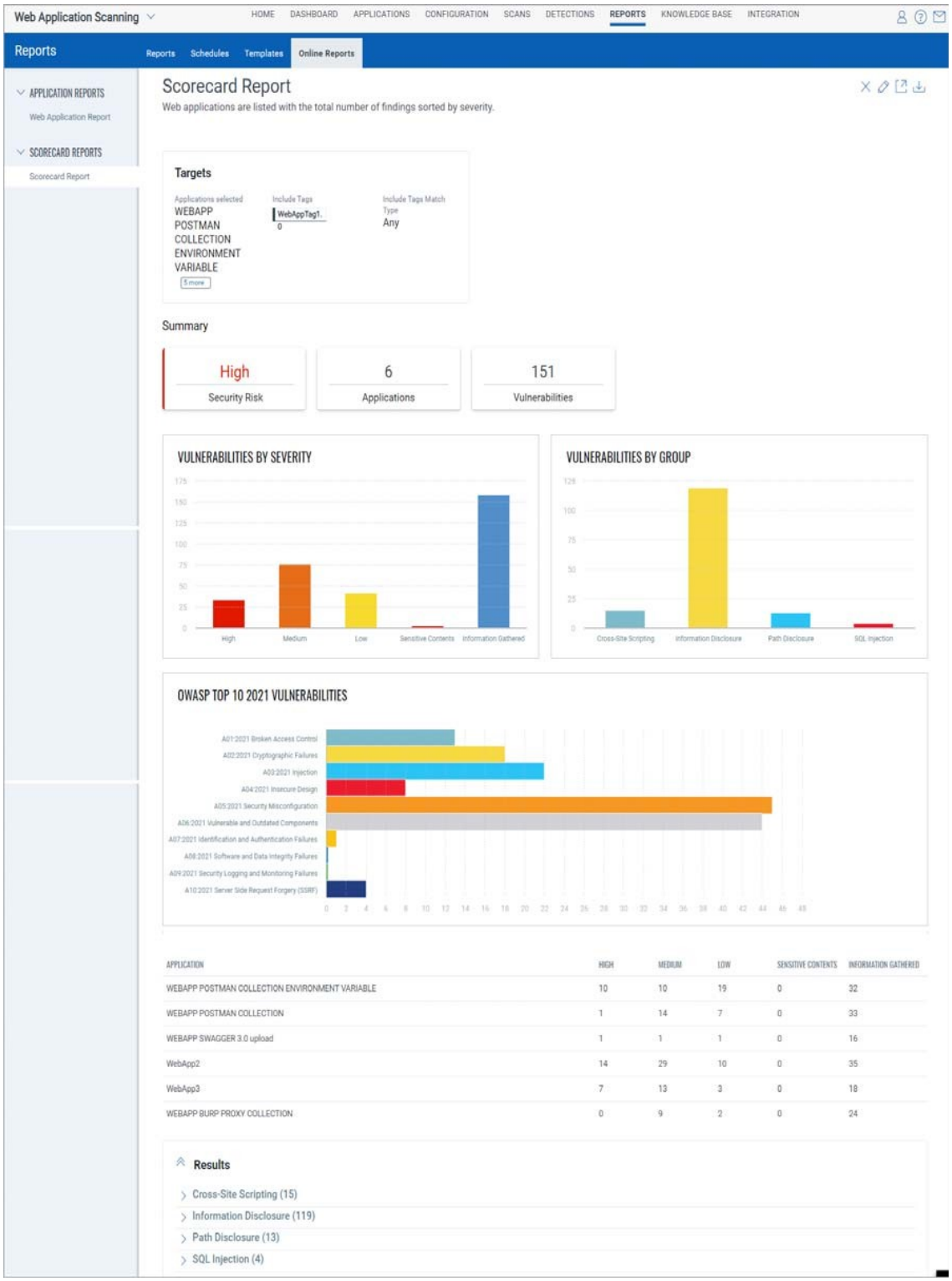
同様に、Webアプリケーションのクイックアクションメニューから「レポートを表示」を選択してWebアプリケーションレポートを生成することもできます。



Webアプリケーション レポートのサンプル



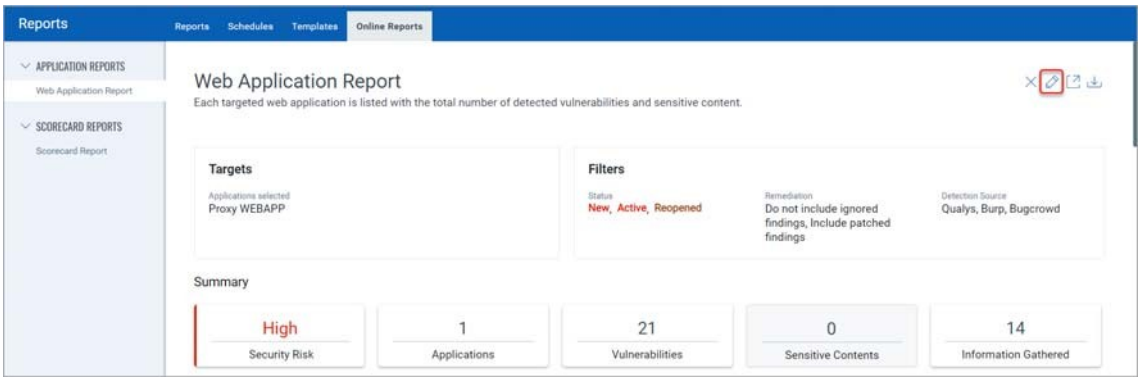
サンプル スコアカード レポート



ヒントと のコツ

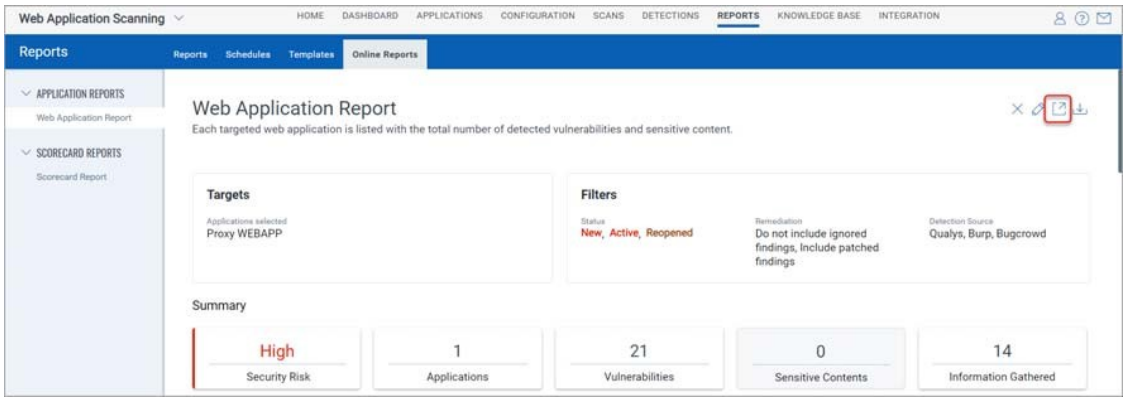
設定の表示、編集、繰り返し

レポートは反復的に更新されます。編集ボタンをクリックするだけでレポート設定を変更でき、変更内容を反映した最新版レポートを生成します。これにより、脆弱性やWebアプリケーションなど、レポート内容にフィルターを素早く適用できます。



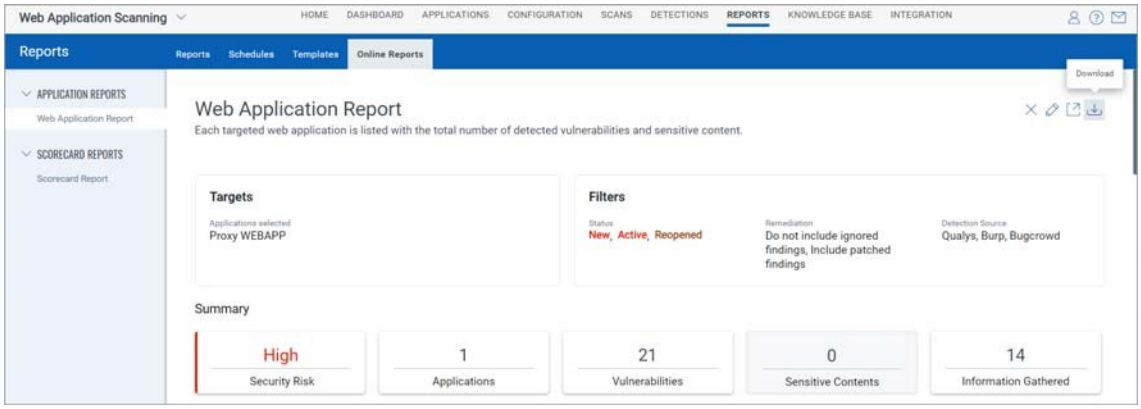
並列比較を行う

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、並列比較が可能になり、複数のレポートを同時に簡単に操作できます。

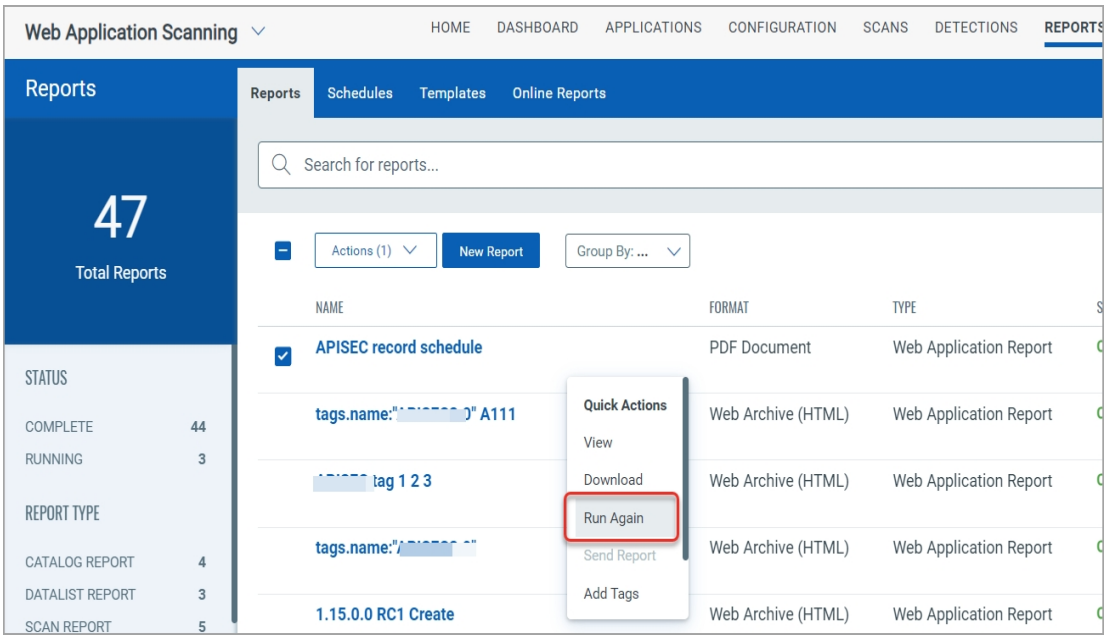


レポートの保存方法

「ダウンロード」オプションを使用すると、レポートをローカルマシンにダウンロードできるほか、アカウントにも保存されます。

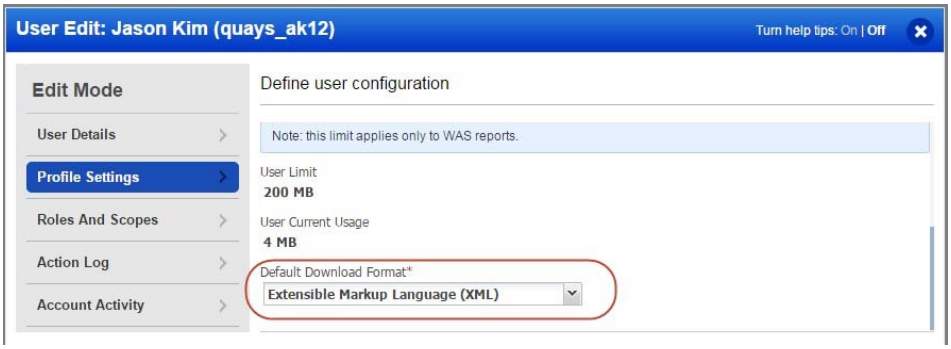


保存済みレポート一覧では、保存したレポートを確認できます。各レポート（概要）の表示、ダウンロード、再実行、タグの追加（他のユーザーとの共有用）が可能です。



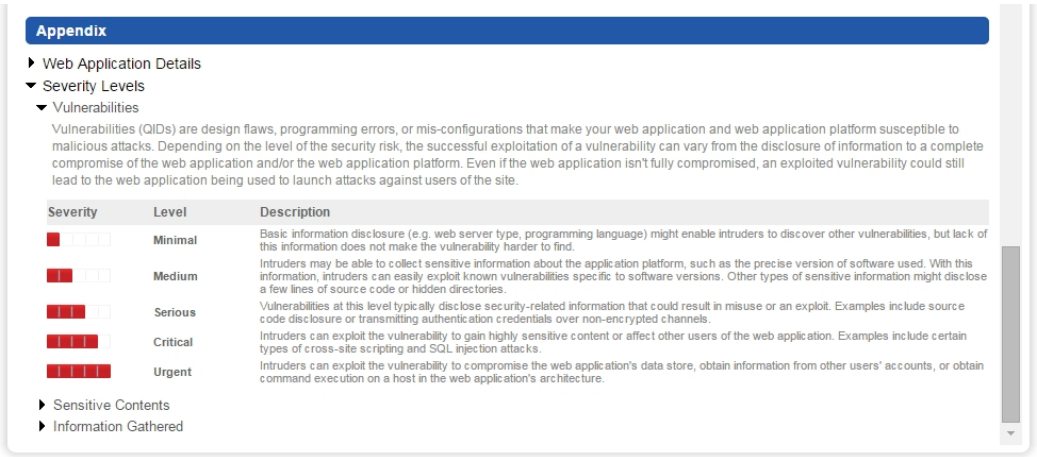
デフォルトのレポート形式を設定する

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好みの形式を選択する必要がなくなります。ユーザー名（画面右上）から「マイプロフィール」を選択し、プロフィール設定を編集してください。



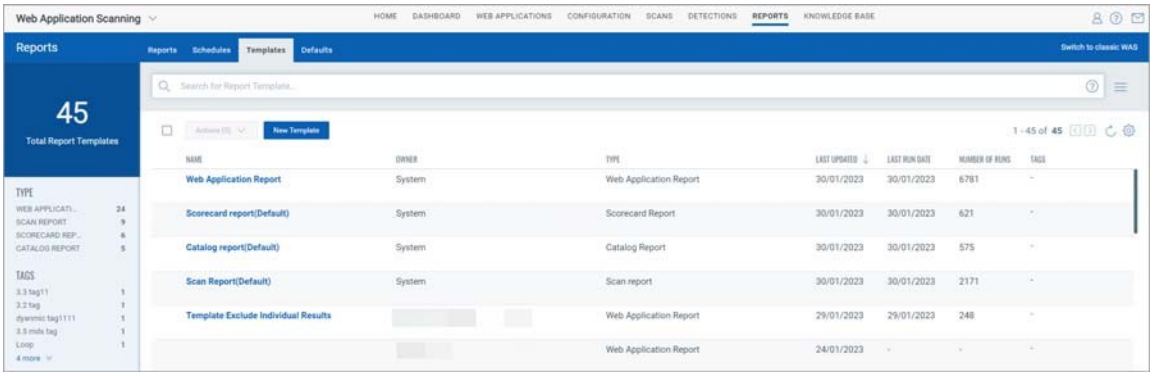
深刻度とレベルの意味は？

付録に移動し、「深刻度レベル」をクリックしてください。各検出タイプ（脆弱性、機密情報、収集された情報）ごとに、各深刻度とレベルの説明が表示されます。

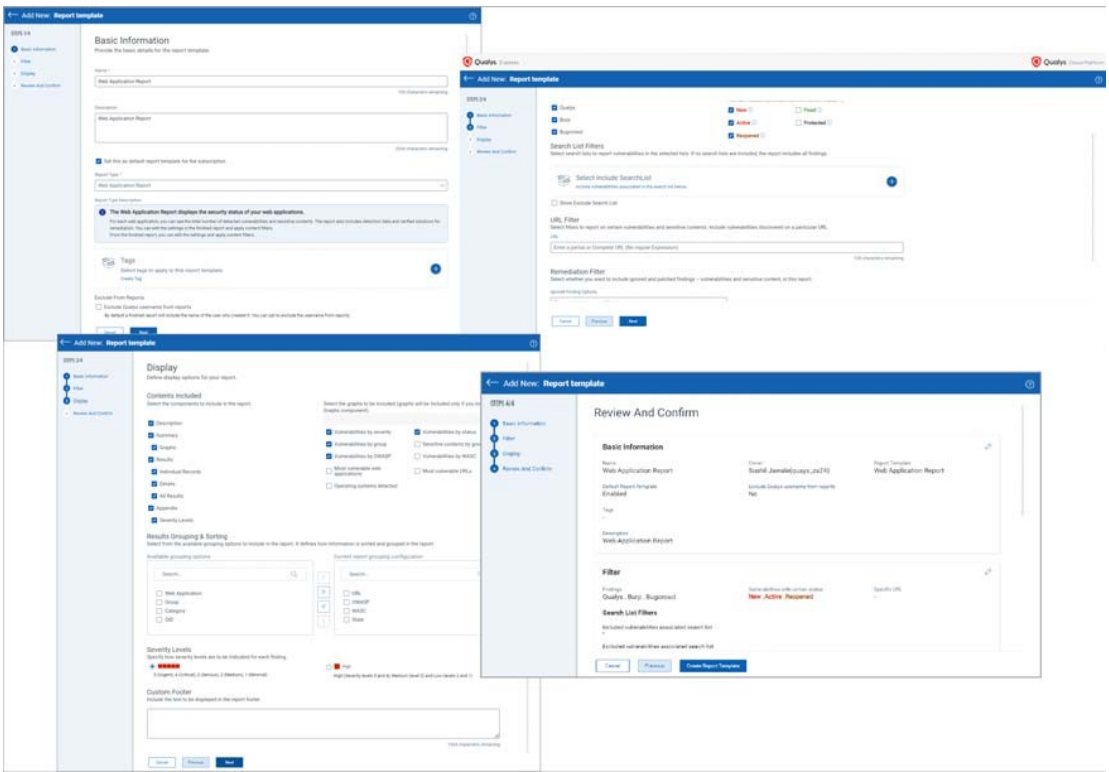


カスタマイズ可能なレポート テンプレート

関心のある特定の情報を含むテンプレートを作成しましょう。これにより、アプリケーションのステークホルダー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、将来の使用のため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、新規テンプレートボタンを選択して開始してください。



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、無視済みとしてマークされた脆弱性などのフィルターや、含めるコンテンツ、グループ化、並べ替えなどの表示設定を構成できます。

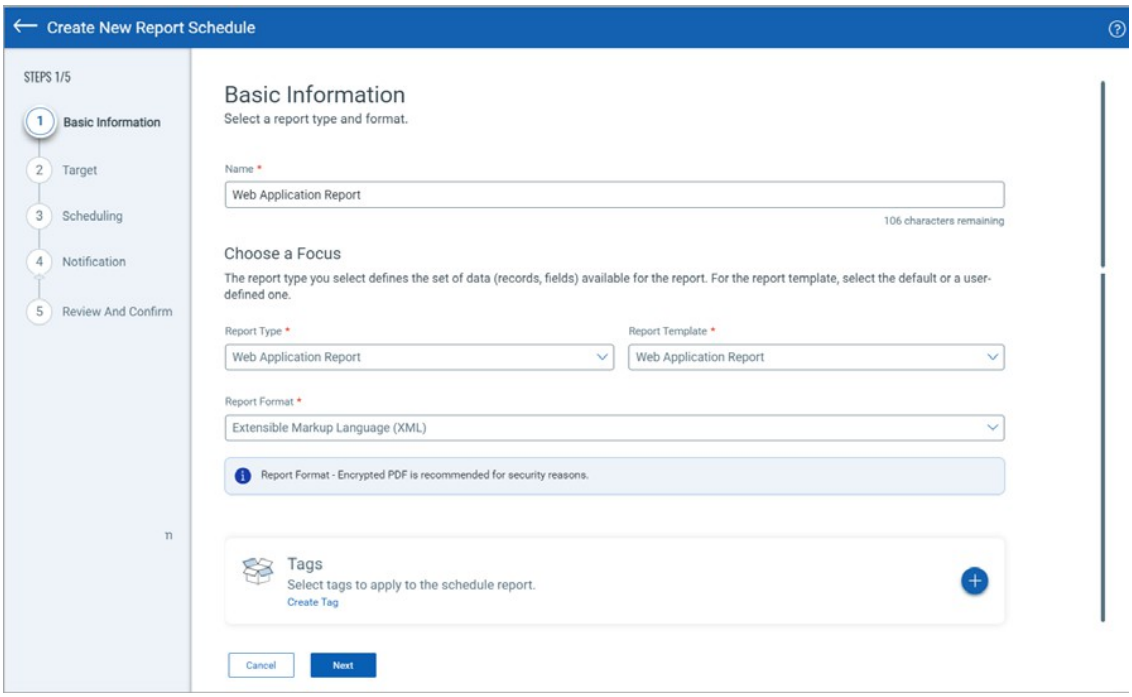


テンプレートを共有したいですか？問題ありません。他のオブジェクト（Webアプリケーション、レポートなど）と同様にタグを付け、ユーザースコープにタグを追加してください（管理ユーティリティを使用）。

レポートのスケジュール設定

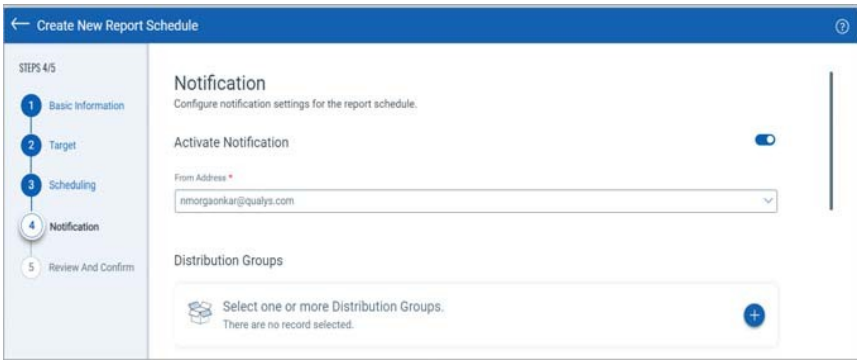
スキャンをスケジュールするのと同じ方法で、レポートを自動的に実行するようにスケジュールできます。レポートは毎日、毎週、毎月、または1回限りの実行をスケジュールできます。レポートのスケジュール設定は、最新のスキャン結果に基づくセキュリティ更新情報を取得し、他のユーザーと共有する優れた方法です。

[レポート] > [スケジュール] に移動し、[新規スケジュール] 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

通知を有効化を選択し、メール通知を受け取るユーザーを指定するだけです。レポートが完了するたびにダウンロードリンク付きのアラートがユーザーに送信され、レポート生成が失敗した場合にも通知が行われます。



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権限が必要です。

新規ユーザーを追加するには？

脆弱性管理アプリケーションで提供されている「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規ユーザーを作成します。手順を順を追って説明します。

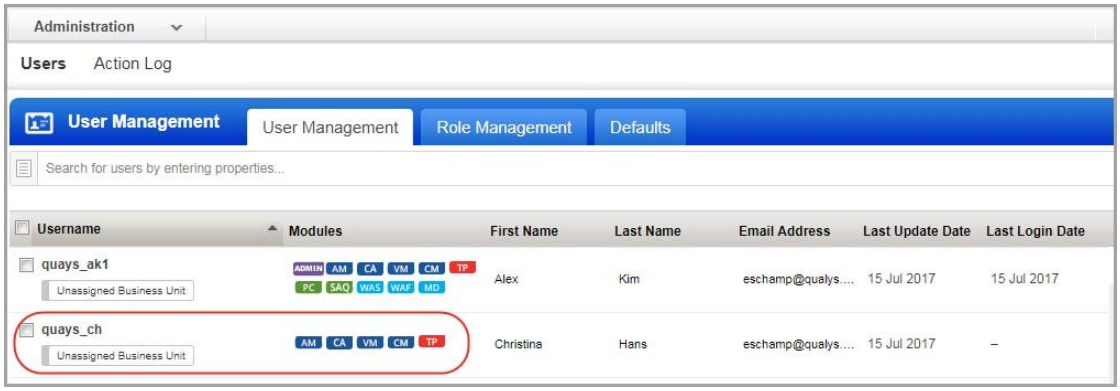
ユーザー、そのロールおよび権限の表示

Qualys Cloud Platform UIでは、サブスクリプション内の全ユーザー、割り当てられたロール、およびアカウントで有効化されている各種アプリケーションへのアクセス権限を確認できます。
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）には、WASへのアクセス権が自動的に付与されないことにご留意ください。

ユーザーにWASへのアクセス権を付与する方法

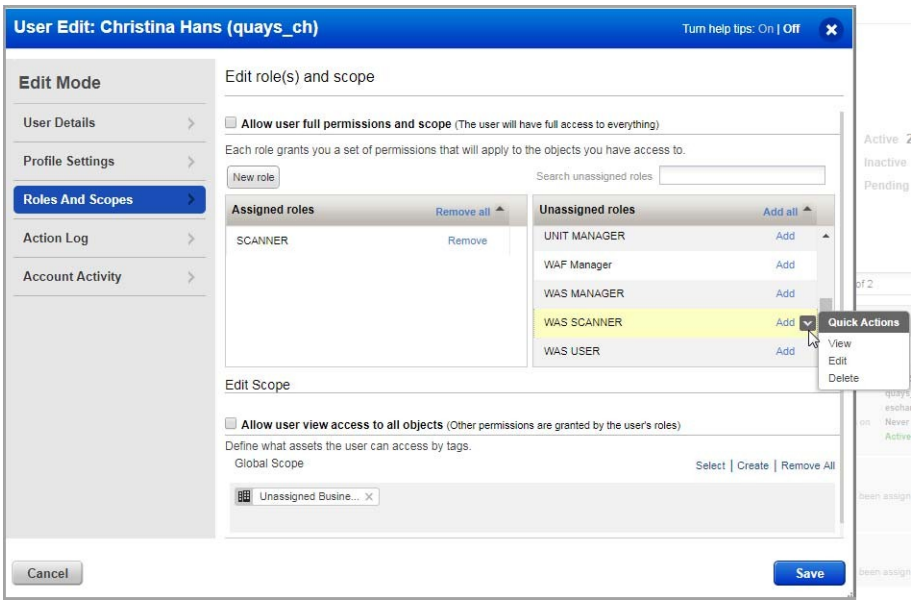
たとえば、スキャナーの役割を持つ新しいユーザー Christina Hans を作成し、Christina が WAS を使用して Web アプリケーションのセキュリティリスクをスキャンできるようにしたいとします。

Qualys Cloud Platformで新規ユーザーのアプリケーション権限を確認します。管理ユーティリティに移動してください。新規ユーザーにはWASアプリケーションがリストされていないことがわかります。

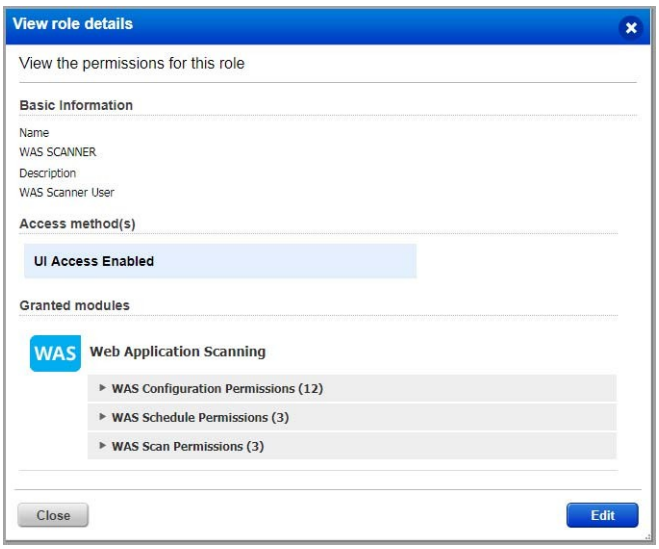


新規ユーザーを編集します（ユーザーを選択し、クイックアクションメニューから「編集」を選択）。「ロールとスコープ」で、ユーザーにVMおよび/またはPCスキャン用のSCANNERロールを割り当てます（サブスクリプション設定に応じて）。

Qualysは、ユーザーにWAS権限を簡単に付与できるよう、事前定義されたWASユーザーロールを提供します。事前定義ロールはWAS MANAGER、WAS SCANNER、WAS USERです。

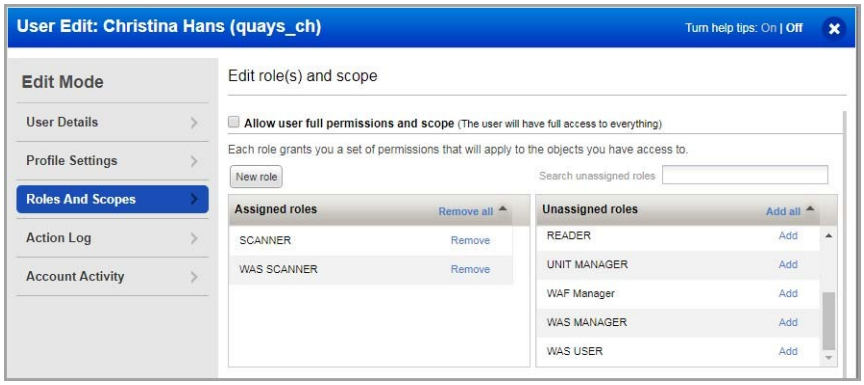


ユーザーChristinaにはSCANNERロール（VM/PC用）が付与されているため、彼女のアカウントにWAS SCANNERロールを追加します。WAS SCANNERを選択し、クイックアクションメニューから[表示]を選択してください。WAS SCANNERの権限グループが表示され、ロールの詳細を確認できます。このロールでは、例えばWebアプリケーションの追加/更新/削除などの権限は付与されません。



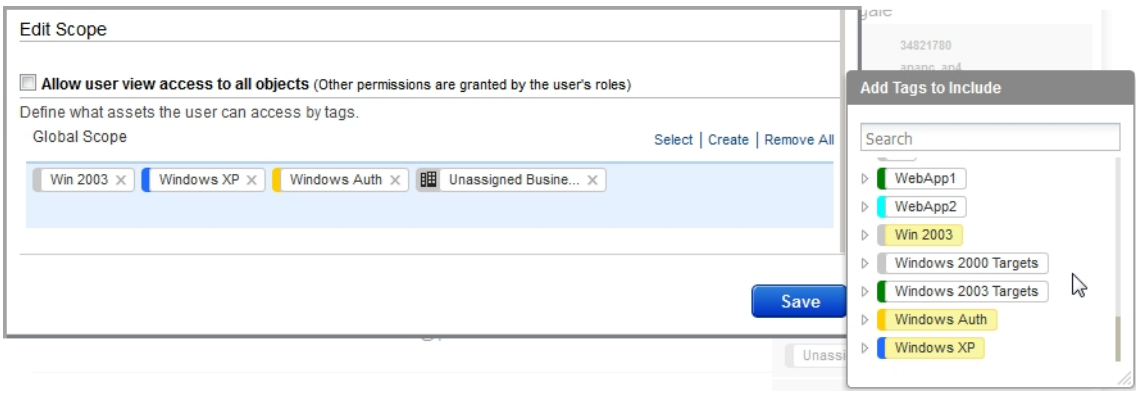
ユーザー設定を編集するには「閉じる」をクリックします。

WAS SCANNER ロールの横にある [追加] リンクをクリックし、ユーザーの割り当て済みロールに追加します。割り当て済みロールは以下のように表示されます。



編集範囲セクションを更新し、ユーザーに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します。デフォルトでは、ユーザーはWebアプリケーションやその他のWAS構成へのアクセス権を持ちません。いずれかのオプションを選択してください。

特定のタグを割り当てる。

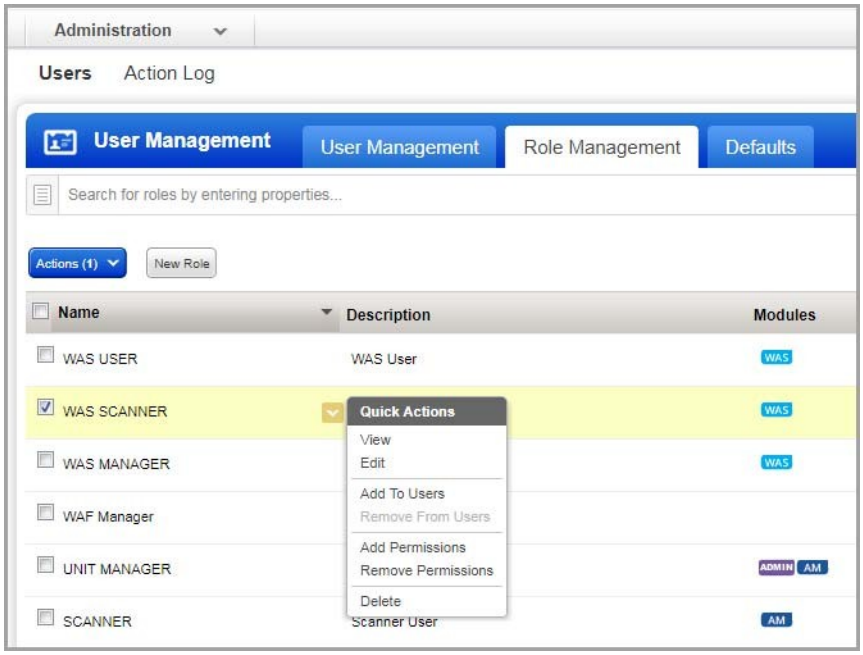


フルスコープ（すべてのタグ）を許可する

ユーザー設定を保存するには、[保存] をクリックします。

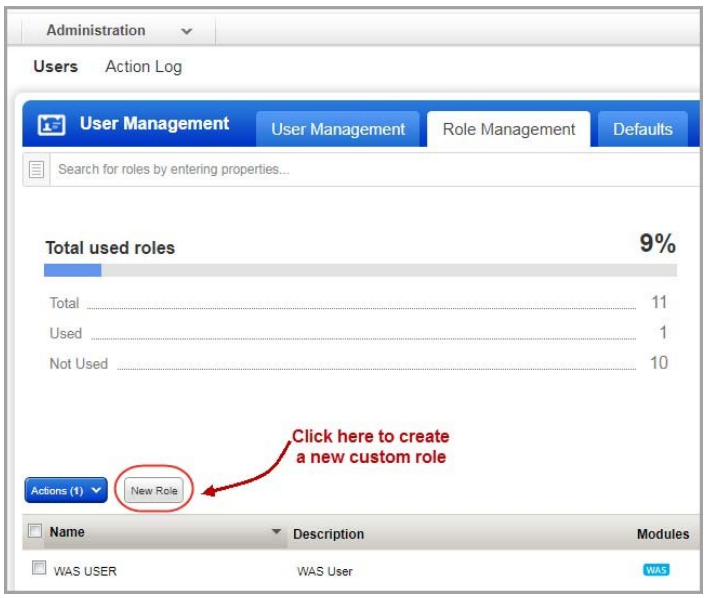
ロール管理

ロール管理セクションでは、サブスクリプション内のすべてのロールに関する情報を確認できます。

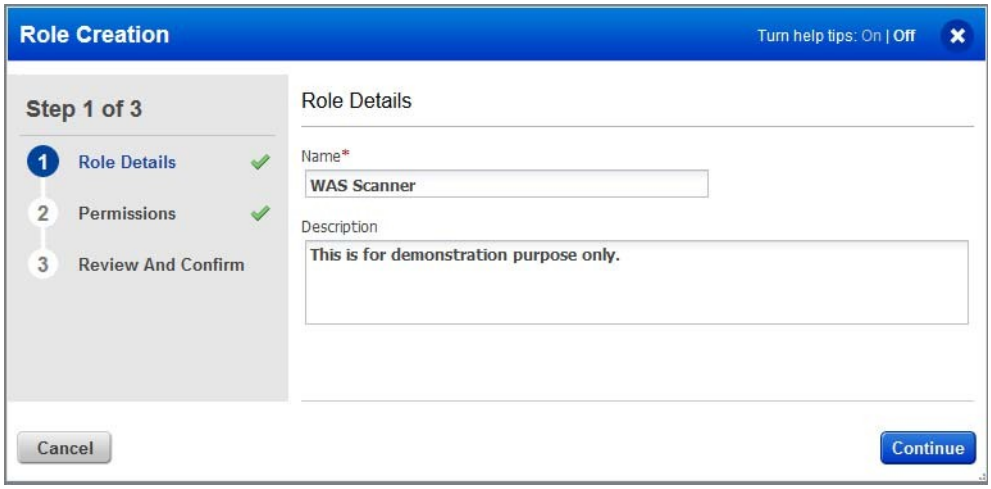


各ロールについて、詳細を確認したり、ユーザー追加、権限追加、権限削除などの操作を実行できます。

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。

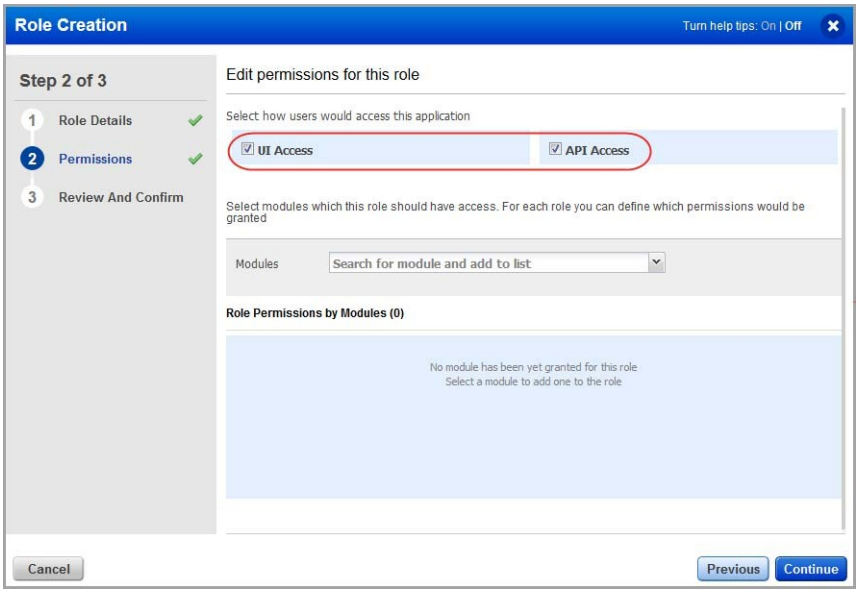


たとえば「WASスキャナー」ロールを作成できます。

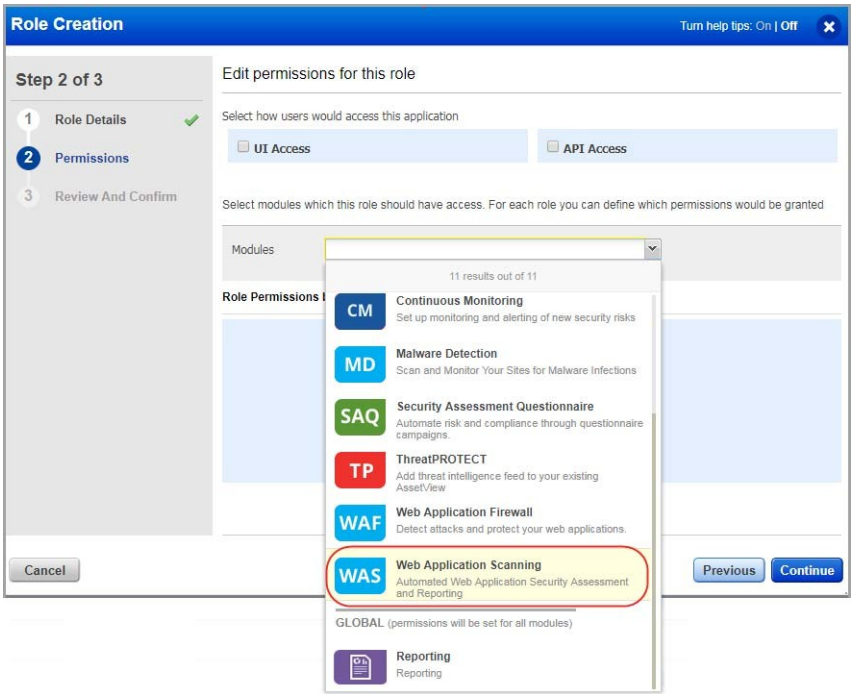


このロールにUIおよび/またはAPIへのアクセス権を付与します。

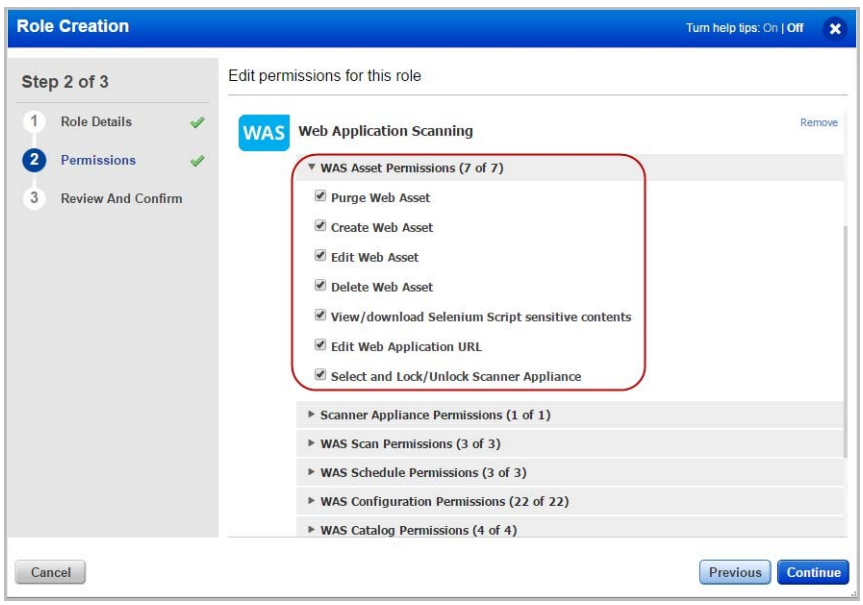
ロールの詳細で、ユーザーのアクセス方法を選択します。



WAS アプリへのアクセス権をロールに付与します。権限セクションで、提供されたメニューから WAS アプリを選択して追加します。



WASアプリ内でロールに権限を付与します。



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。管理者以外のユーザー（スキャナー、リーダー、ユニットマネージャー）は、WASアプリケーションおよび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限を付与される必要があります。管理者（または「ユーザー編集」権限を持つユーザー）は、管理ユーティリティを使用してユーザーの役割を設定できます。

ユーザーにロールを割り当てる手順は、こちらを参照してください。

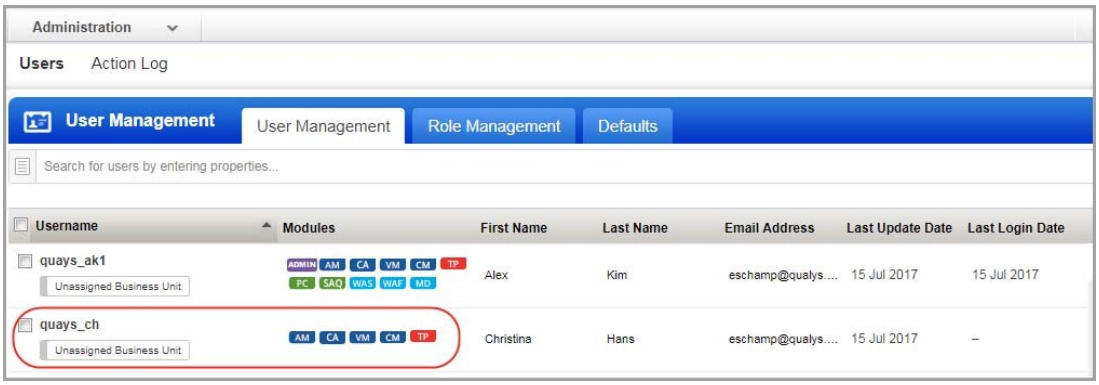
前提条件

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。

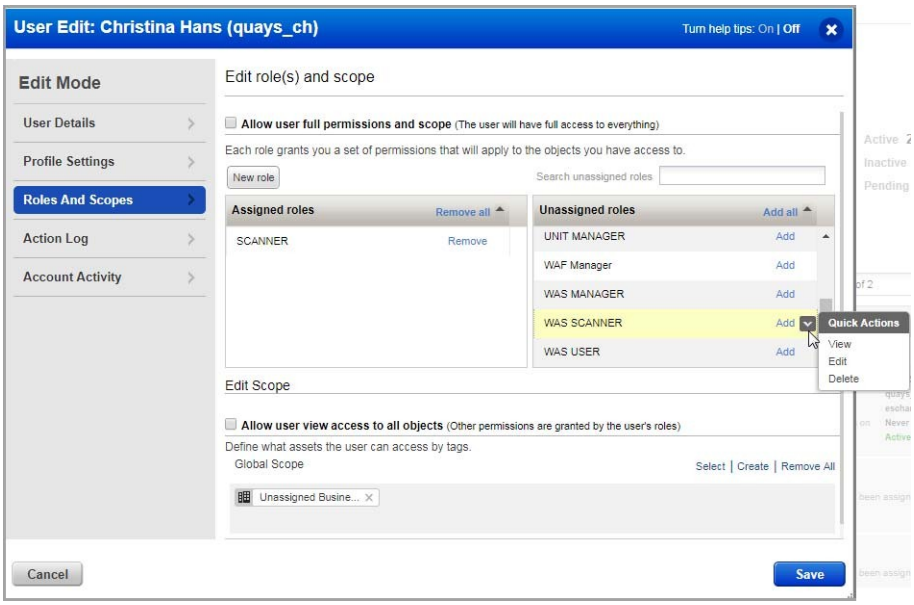
1) アカウント認証情報を使用して Qualys にログインします。

2) モジュールピッカーから「**管理**」モジュールを選択します。

3) ユーザー管理タブから、問題が発生しているユーザーを選択し、クイックアクションメニューから**編集を選択します**。



4) **「ロールとスコープ」**タブに移動し、要件に応じ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管理ユーティリティのオンラインヘルプにある「ユーザーロールの管理」トピック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、[**編集**]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、ユーザーのスコープにタグを追加します。

5) **[保存]**をクリックし、ユーザーに再度ログインするよう依頼します。

ヘルプの取得

Qualysは、お客様に最も徹底したサポートを提供することをお約束します。オンラインドキュメント、電話サポート、直接メールサポートを通じて、Qualysはお客様の質問に可能な限り迅速にお答えします。週7日、24時間体制でサポートいたします。オンラインサポート情報はhttps://success.qualys.com/customersupport/s/でご覧いただけます。

WASコミュニティ

WASに関する最新機能、ディスカッション、ドキュメント、動画の詳細については、Qualys WASコミュニティページをご覧ください。