Web アプリケーションスキャニング スタートガイド バージョン 6.14

2020 年 9 月 18 日

Copyright 2011-2024 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

無断複写・転載を禁じます。2023-2024 年 クォリスジャパン株式会社

目次

無断複写・転載を禁じます。2023-2024 年 クォリスジャパン株式会社

WAS へようこそ

Qualys Web Application Scanning(WAS)は、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、統合機能を組織に提供します。Qualys WAS は、Web アプリケーションの脆弱性を評価、追跡、修復することを可能にします。

主な機能

- 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、脆弱性をスキャンする
- 柔軟なワークフローとレポートを備えた完全にインタラクティブな UI
- Web アプリケーションによる機密データや機密データの取り扱いを特定する
- カスタマイズ:ブラック/ホワイトリスト、ロボット.txt、サイトマップ.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
-

堅牢でスケーラブルなスキャン機能

- JavaScript と埋め込み 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挿入の問題を単純な情報漏えいから区別
- 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ース、ウィザード、新しいレポートテンプレートを備えた UI により、幅広いプレゼンテーションオプションでスキャンデータを表示します。
- カスタマイズ可能なテンプレート駆動型の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。
- スキャン結果、資産データ、スキャンプロファイル、ユーザ、脆弱性など、複数の広範な Qualys データセットを高速に検索します。
- 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、大規模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を完了するため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脆弱性スキャンを自動化します。また、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 の一般的なアプリケーション セキュリティ上の欠陥が自動的にテストされます。

- Postman サポートによる API スキャンの強化 - 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、関連する要求 (API エンドポイント) をまとめて他のユーザ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 の早い段階で行われ、セキュリティ上の欠陥を検出して排除できるため、SDLC の後半で行う場合と比較して、修復のコストを大幅に削減できます。 プラグインのダウンロードはこちらから。

- Qualys Browser Recorder –この新しい Chrome 拡張機能を使用すると、ユーザは Web ブラウザーのアクティビティを記録し、スクリプトを保存して反復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 ウェブストアから誰でも(Qualys のユーザだけでなく)利用できます。

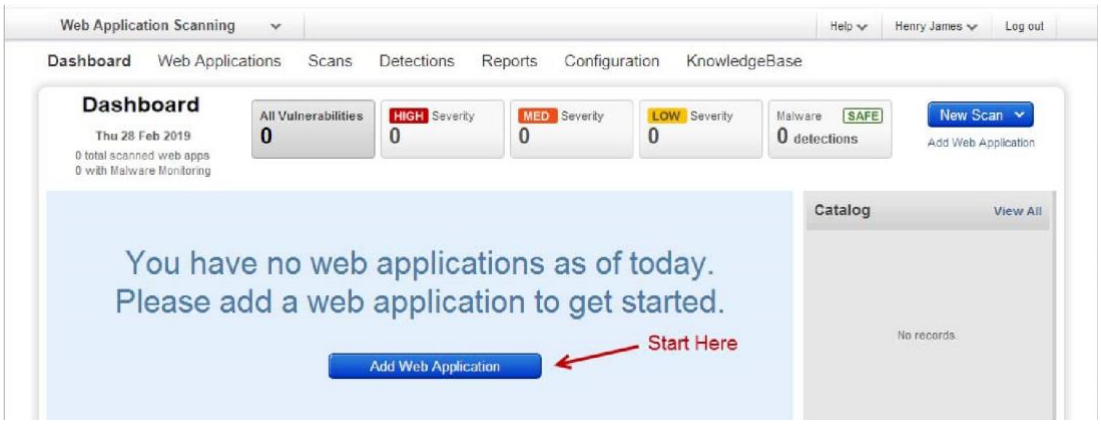
はじめに

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。

さあ始めましょう！

ログインして WAS を選択する

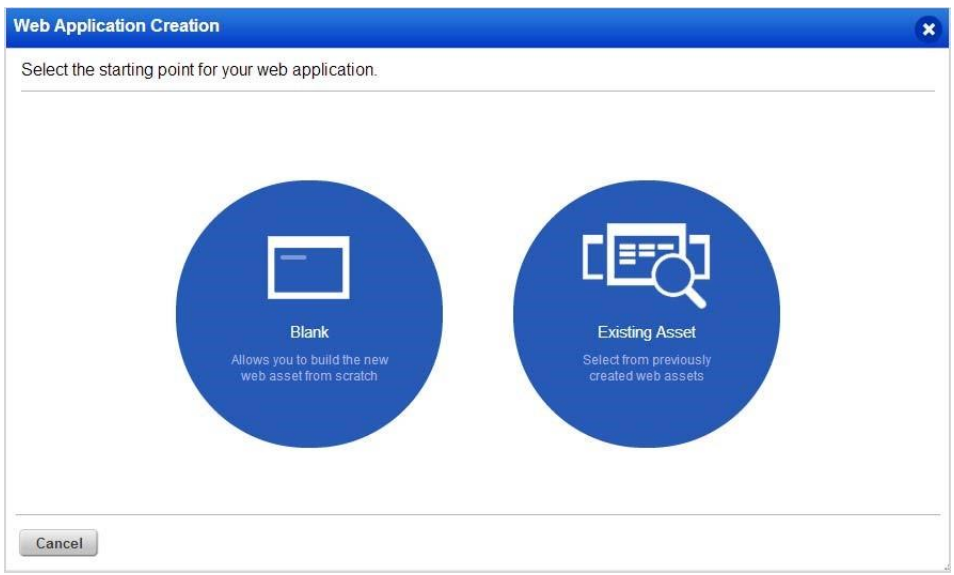
まず、スキャンする Web アプリケーションについてお知らせください - [Web アプリケーションの追加]をクリックするだけです。 (以下はクラッシック WAS View です)



スタート地点を選ぶ

[Blank] を選択すると、新しい Web アセットを最初から構築できます。

サブスクリプションに Web アセットを既にお持ちですか? WAF アプリケーション用にすでに定義している場合は、そうすることができます。「はい」の場合は、「既存のアセット（Existing Asset）」を選択するだけで、時間を節約できます。名前、URL、タグなどの設定を再入力する必要はありません。 (以下はクラッシック WAS View です)

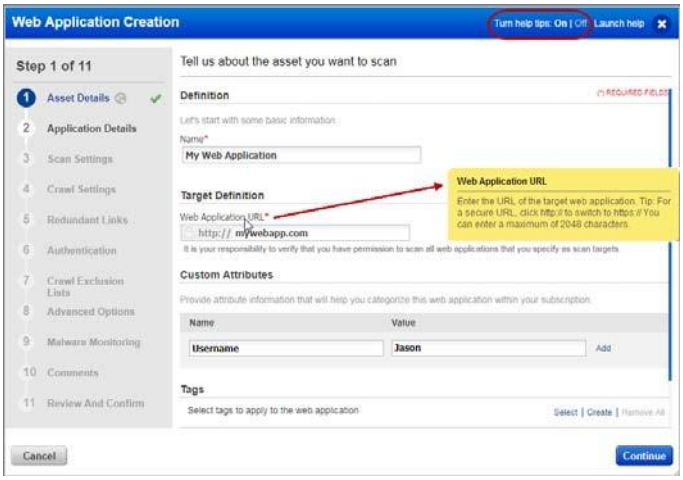


Web アプリの設定を追加する

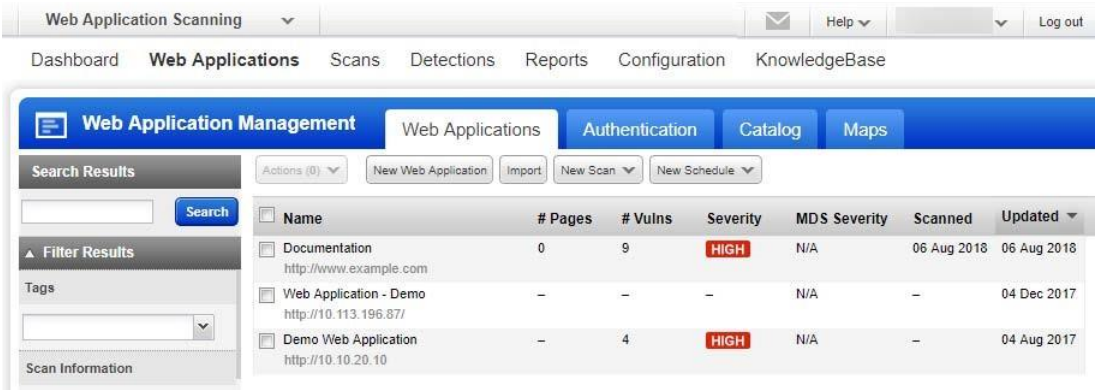
Web アプリケーションの名前と URL は、Web アプリを最初から追加するときに必要です。既存のアセットから追加する場合は、これらが自動的に入力されます。

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、毎日のマルウェアスキャンが自動実行されます。

ヘルプのヒント - (タイトルバーで)これをオンにして、フィールドにカーソルを合わせると、各設定のヘルプが表示されます。



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、スキャンを開始したりできます。



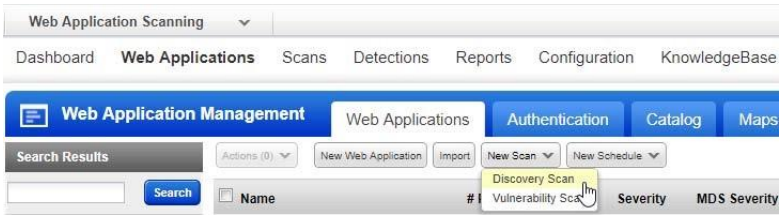
認証を使用する理由 認証を使用すると、クロール プロセス中に Web アプリケーションのすべての箇所にアクセスできるようになります。このようにして、Web アプリケーションのより詳細な評価を実行できます。一部の Web アプリケーションでは、その機能の大部分に対して認証されたアクセスが必要です。認証スキャンは、ログインページやサーバーベースの認証(HTTP 基本、ダイジェスト、NTLM、または SSL クライアント証明書)などの HTML フォームに対して構成できます。[認証] タブに移動し、[新しいレコード] を選択して、アクセス資格情報を使用して認証レコードを構成するだけです。フォーム認証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 - セッション状態を監視して、認証されたスキャンがクロール全体で認証されたままであることを確認します。

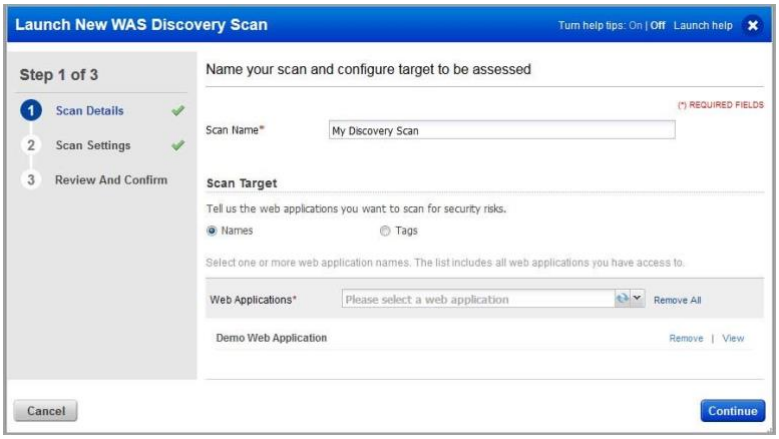
スキャンとその潜在的な影響に関する警告 Web アプリケーション・スキャンは、テスト・データを含むフォームを送信します。これが望ましくない場合は、ブラックリスト、POST データブラックリストの設定を追加するか、オプションプロファイル内で GET のみの方法を選択する必要があります。これらの構成を使用する場合、Web アプリケーションの特定の領域のテストは含まれず、これらの領域に存在する脆弱性が検出されない可能性があることに注意してください。

最初に検出(Discovery)スキャンを行うことをお勧めします

検出スキャンでは、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か、および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のに適した方法です。
(上部のメニューの)[Web アプリケーション]に移動し、[新しいスキャン]>[Discovery スキャン]を選択します。



スキャンの起動ウィザードは、順を追って説明します。スキャンする Web アプリケーションを入力し、スキャン設定を選択します(*は必須を意味します)。
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、「終了」をクリックします。



オプションプロファイルについて

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、「Initial 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、クロールとスキャンのパラメーターをカスタマイズできます。

認証の詳細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ために認証は必要ですか?「はい」の場合は、必ず認証レコードを選択してください。

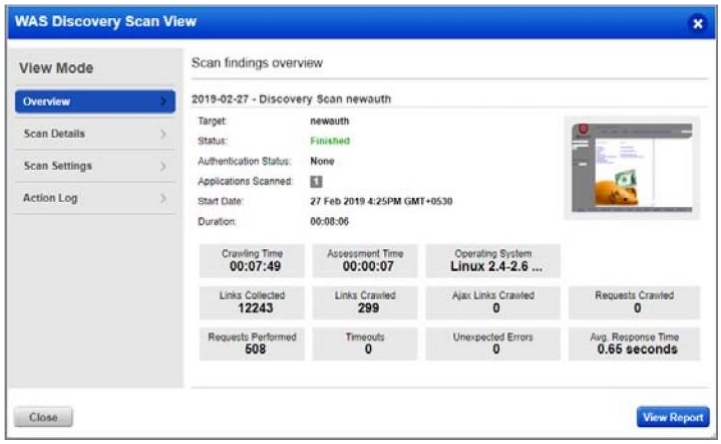
Scanner Appliance は必要ですか?

当社のセキュリティサービスは、ネットワーク境界で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、Scanner Appliance(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、[New] メニューからオプションを選択すると、手順が順を追って表示されます。(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

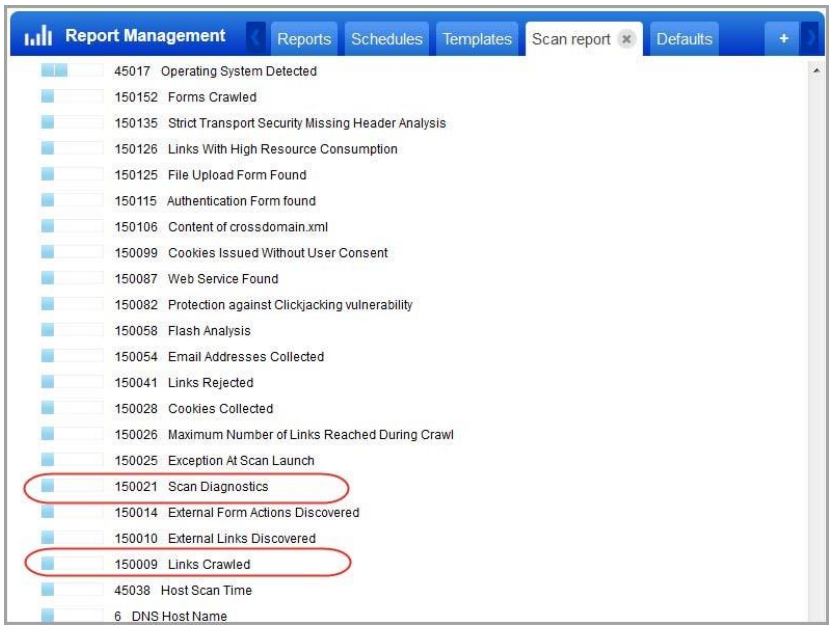
「概要(Overview)」には、スキャン結果の概要が表示されます。フル スキャン レポートを表示しますか?[レポートの表示] ボタンをクリックするだけです。



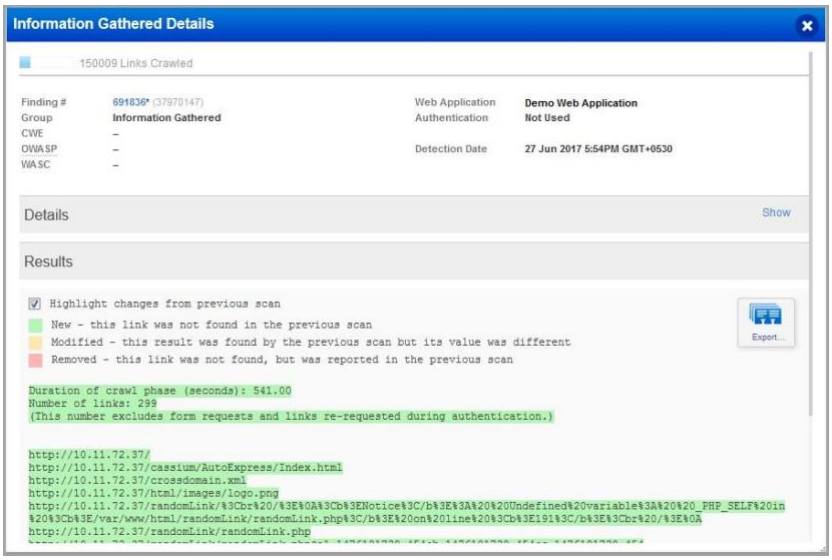
フル スキャン レポート

各 QID は、当社が実施し、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、必ず QID 150009 Links Crawled および QID 150021 Scan Diagnostics を確認してください。



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



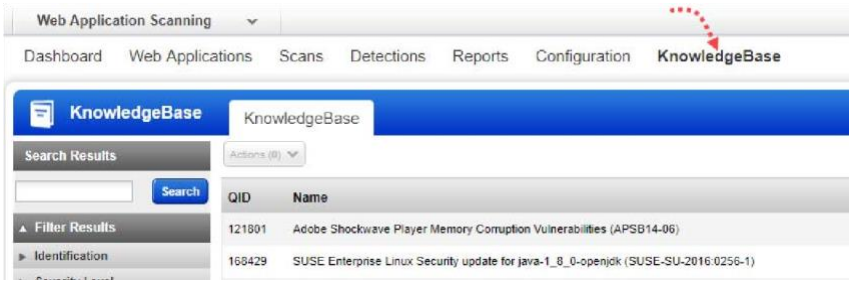
脆弱性スキャン

脆弱性スキャンでは、脆弱性チェックと機密コンテンツのチェックを実行して、Web アプリケーションのセキュリティ体制について通知します。

知っておくと良いこと

どのような脆弱性チェックがテストされますか?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)は、スキャンを特定の脆弱性(確認済み、潜在的な脆弱性、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、スキャンされます。ナレッジベースは、新しいセキュリティ情報が利用可能になると、常に更新されます。

トップメニューの[KnowledgeBase]をクリックします。

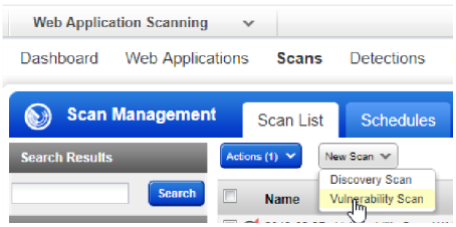


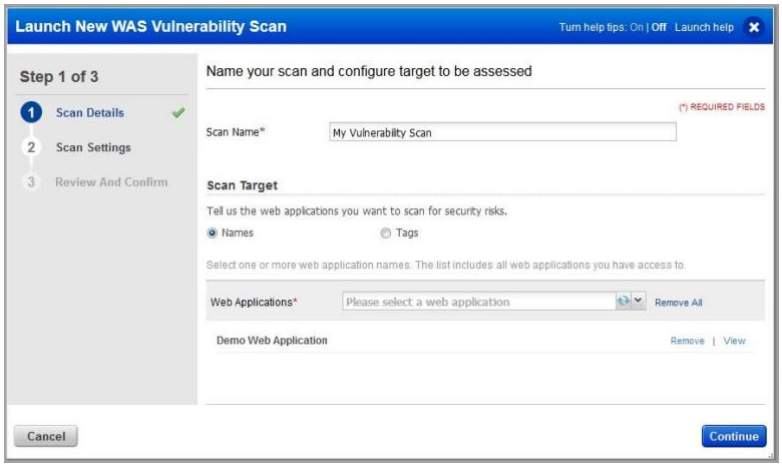
重大度とは何ですか?各 QID には、サービスによって重大度レベル(確認された脆弱性(赤)、潜在的な脆弱性(黄)、収集された情報(青))が割り当てられています。

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(Vulnerability)スキャン] を選択します。

スキャンの起動ウィザードは、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指定し、スキャン設定を選択します。



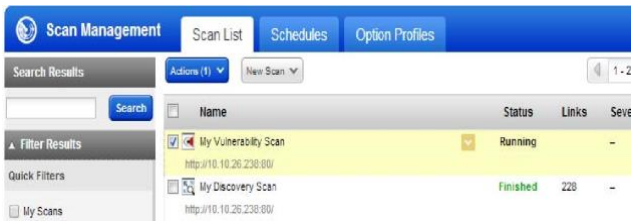


スキャンを開始する準備はできましたか?「続行」をクリックし、設定を確認してから、「終了」をクリックします。

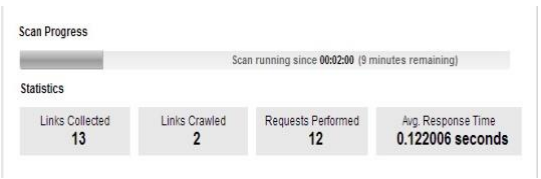
スキャンの進行状況を確認する

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。

もっと情報が必要ですか?スキャン行をダブルクリックします。

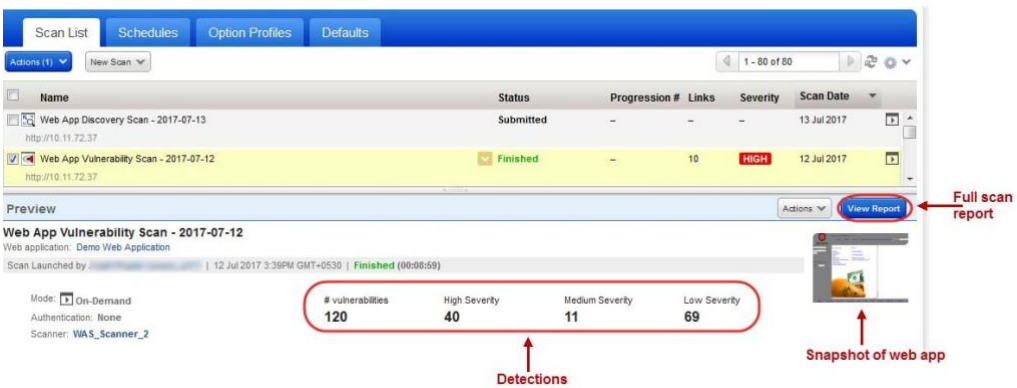


次に、スキャンの進行状況バーが表示され、スキャンがいつ終了するかの見積もりが表示されます。



スキャン結果

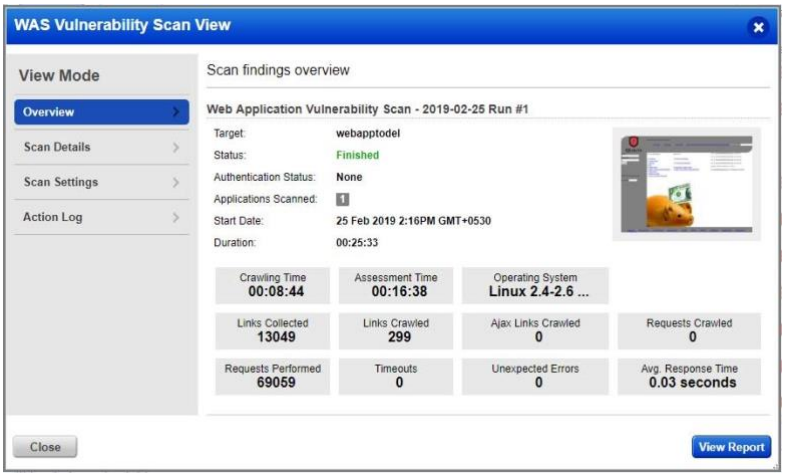
完了したスキャンを選択すると、スキャンのプレビューが表示されます(リストの下)。



スキャン・ビュー

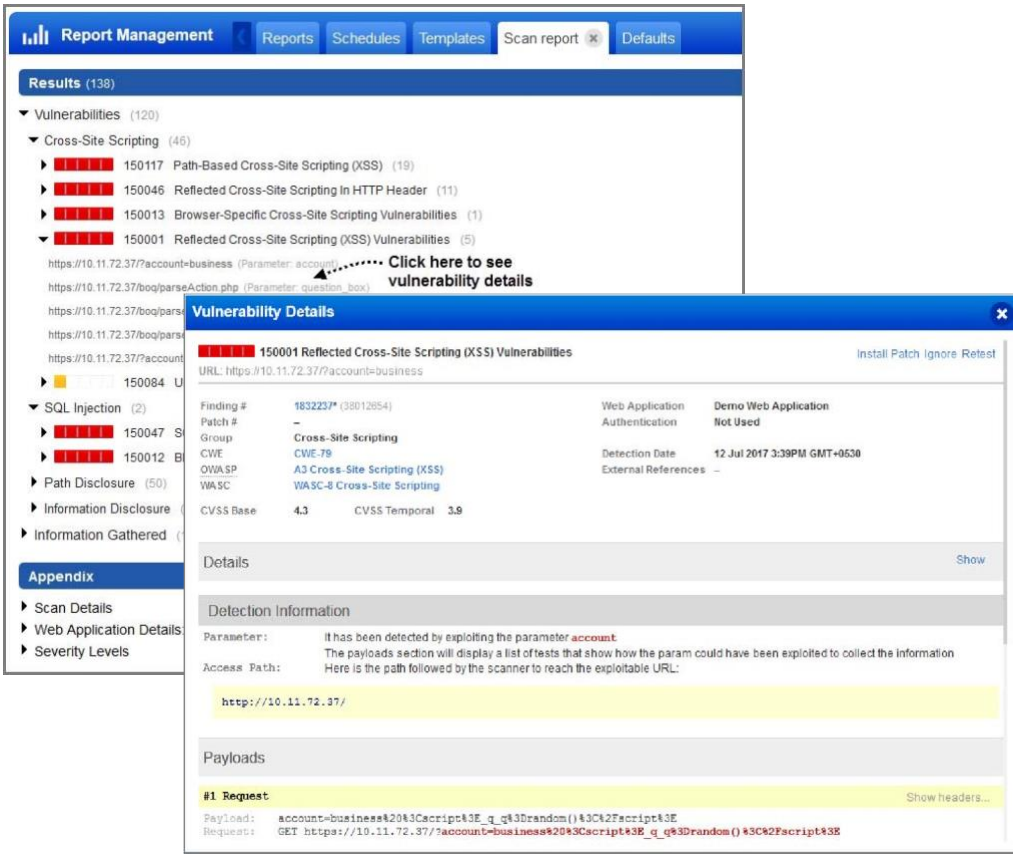
どうすればわかりますか?スキャンにカーソルを合わせ、「クイック・アクション」メニューから「表示」を選択します。
「概要」には、スキャン結果の概要が表示されます。

フル スキャン レポートをご覧になりたいですか?[レポートの表示] ボタンをクリックするだけです。

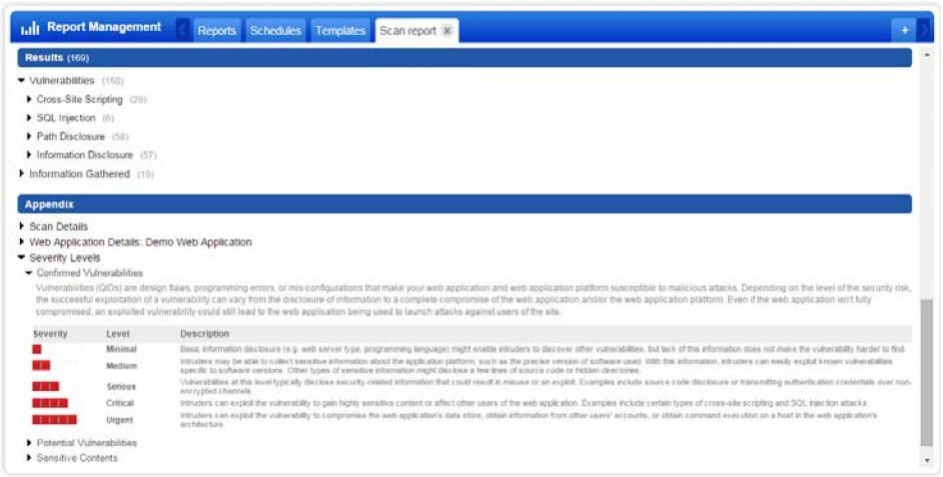


フル スキャン レポート

脆弱性はグループでソートされます。

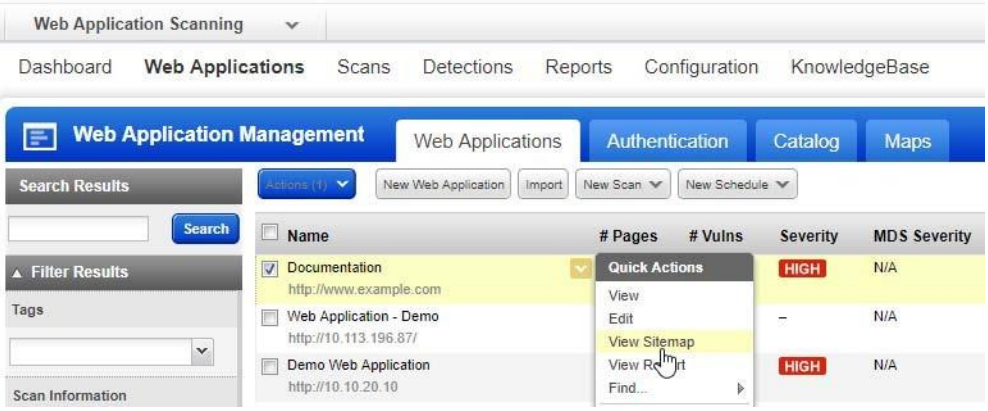


Appendix で重大度レベルが何を意味するかを簡単に確認できます。

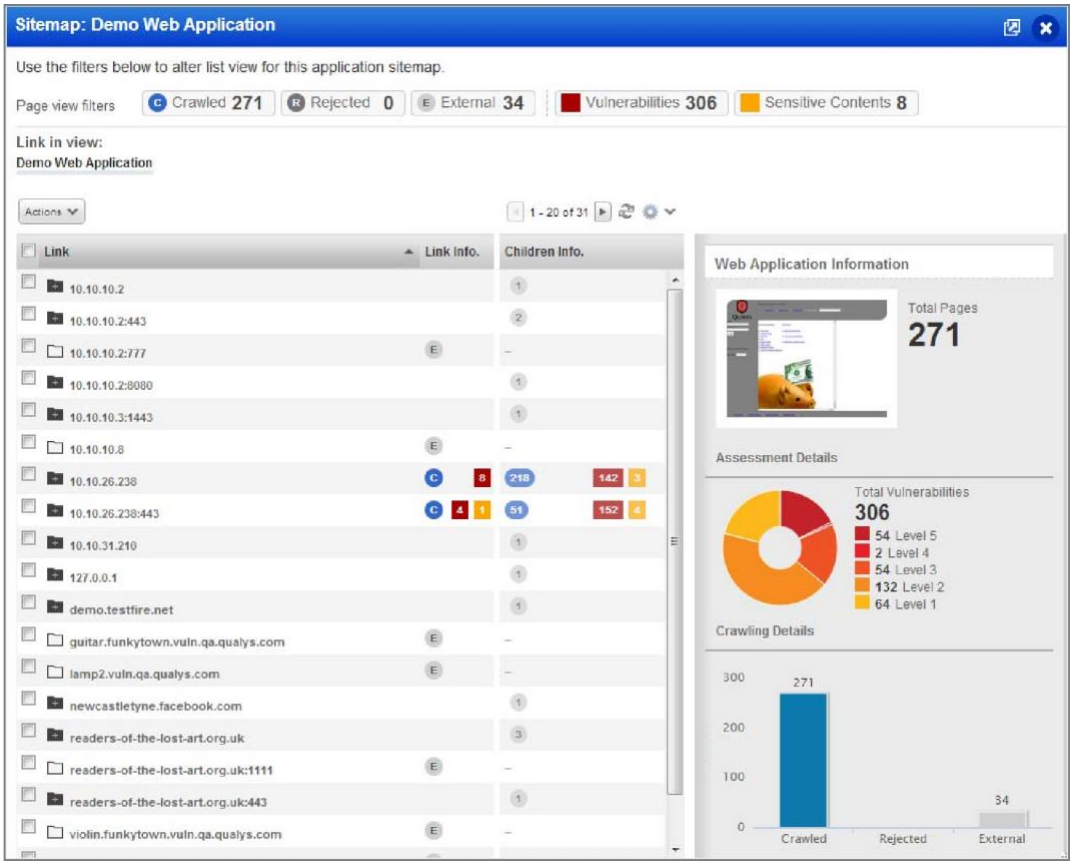


サイトマップを確認する

Web アプリケーションサイトマップは、クロールされたリンク、脆弱性、および検出された機密コンテンツ(Web アプリケーションに移動し、Web アプリを選択し、[クイックアクション]メニューから[サイトマップの表示])を表示して、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。



以下は、合計 271 ページのクロール、合計 306 の脆弱性、8 つの機密コンテンツの検出がある Web アプリケーションのサンプル サイトマップです。



サイトマップを新しいブラウザ ウィンドウに移動する

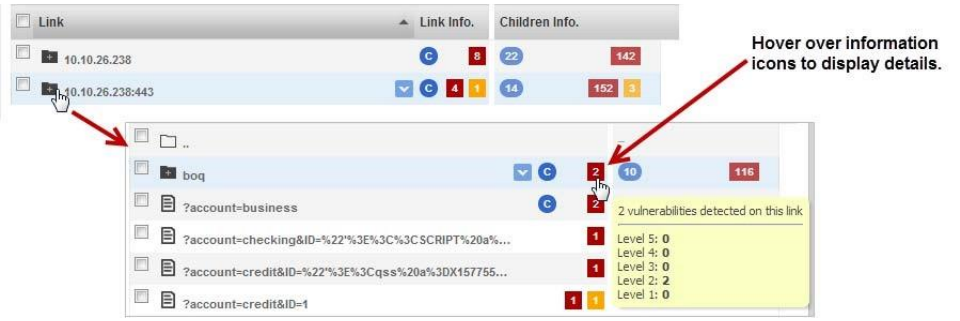
右上隅のアイコンをクリックして、サイトマップを新しいブラウザウィンドウに移動します。

サイトマップをフィルタリングする

ページビューフィルターの 1 つをクリックします。たとえば、現在の脆弱性の脆弱性です。

ドリルダウンしてネストされ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すると、子リンクが表示されます。



Web アプリの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するには、その行を選択し、詳細パネル(右側)の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

スキャンしたリンクとその検出データを複数の形式でダウンロードします。

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

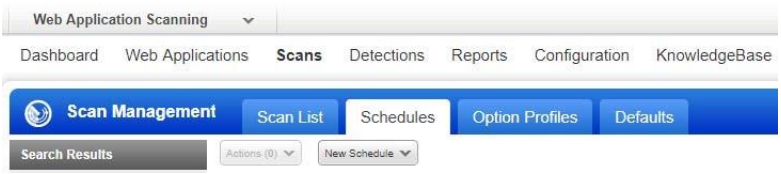
Number of records: 33

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

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

スキャン スケジュールは、繰り返し実行するように設定することをお勧めします。このようにして、結果を自動的に(毎日、毎週、または毎月)取得し、組織にとって都合の良い時間帯に取得できます。

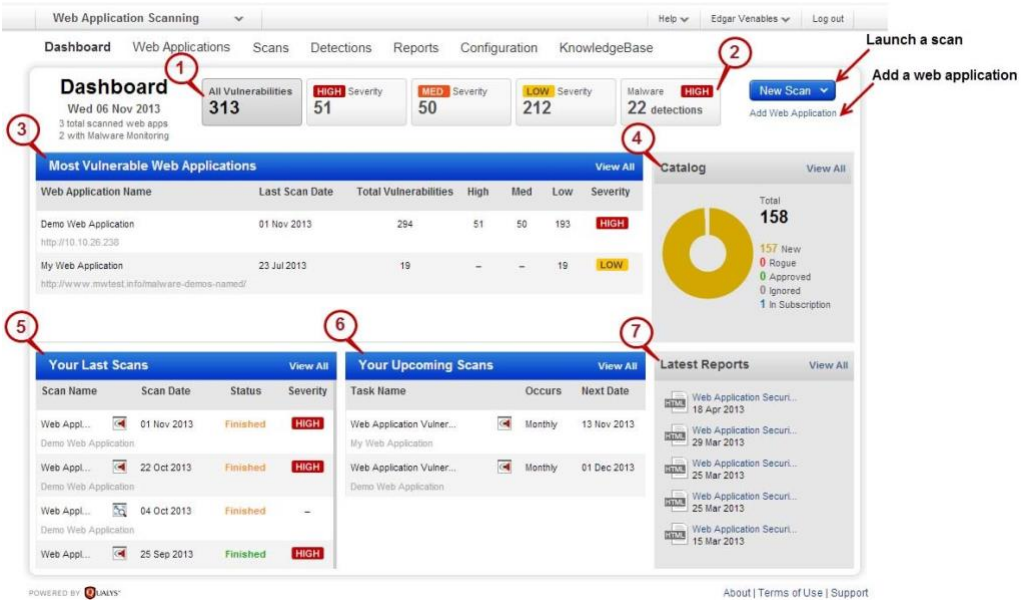
[スキャン]>に移動します
[スケジュール] をクリックし、[新しいスケジュール] を選択します。



Get the latest security status from your dashboard

ダッシュボードから最新のセキュリティステータスを取得

ダッシュボードにはセキュリティステータスが一目でわかり、常に最新のスキャン結果が表示されます。これは非常にインタラクティブです - セクション、リンクをクリックして、詳細を発見するだけです。



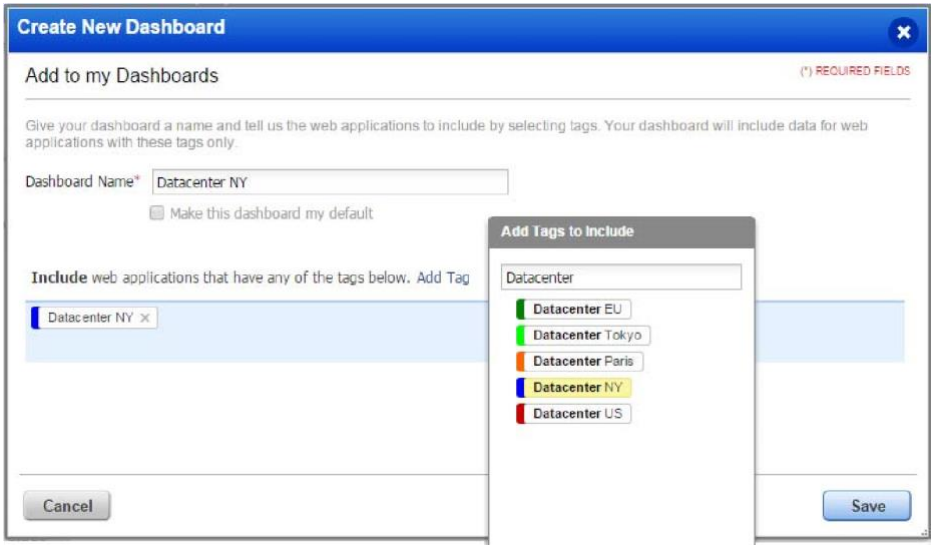
1) 現在の脆弱性数:深刻度高(レベル 4 および 5)、中(レベル 3)、低(レベル 1 および 2)。
2) マルウェア検出の数 (Web アプリのマルウェア監視を有効にした場合)。
3) 最も脆弱な Web アプリ。
4) 検出された Web アプリがカタログに登録されました(Express Lite ユーザは利用できません)。
5) 最新のスキャン(ヒント-スキャン日にカーソルを合わせると、それぞれの日付/時刻が表示されます)。
6) 今後のスキャン (スケジュール)。
7) 最新のレポートに簡単にアクセスできます。

カスタムダッシュボードを簡単に作成し、ビューを切り替えます

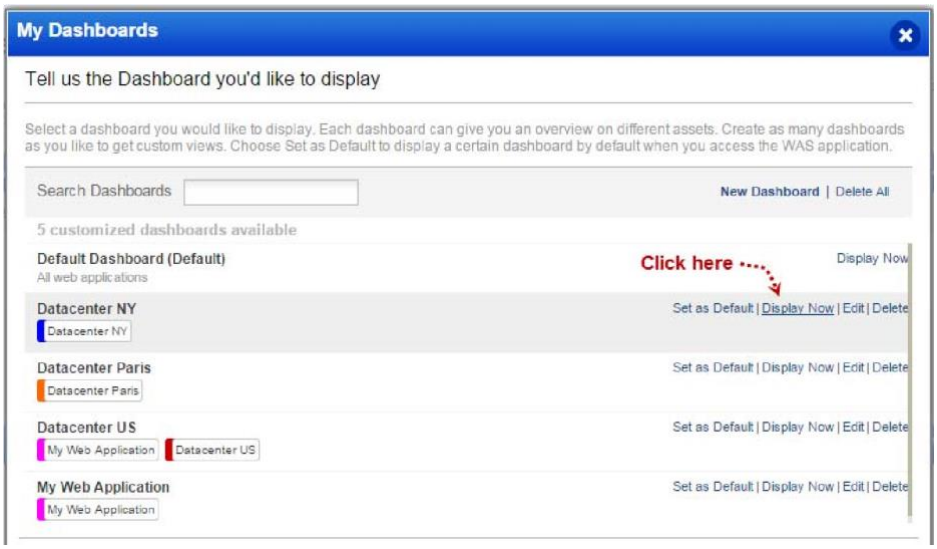
ダッシュボードは、関心のある分野、特定の Web アプリケーション、本番環境にいつでも焦点を当てることができます。カスタムダッシュボードをアカウントのデフォルトとして設定することもできます。

「ダッシュボード」にカーソルを合わせ、「変更...」をクリックします。

タグを選択して、各ダッシュボードに含める Web アプリを指定します。



[今すぐ表示] をクリックするだけで、ダッシュボードの表示を変更できます。とても簡単です!



カタログについて教えてください

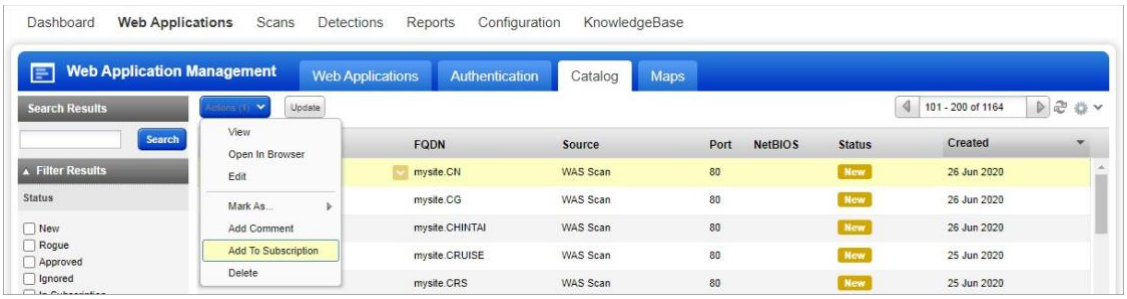
カタログは、サブスクリプションに追加することを選択できる Web アプリケーションのステージング領域です。カタログでは、どのエントリが WAS でスキャンする必要がある本当に Web アプリケーションであるかを知るために、手動でトリアージする必要があります。
カタログエントリは、アカウント内の完了したマップ、脆弱性スキャン、および WAS スキャンから処理されます。カタログエントリは必ずしも Web アプリケーションではなく、特定のポートで HTTP リクエストに応答した Web サーバーです。 (カタログ機能は Express Lite をご利用いただけません。

どのように始めればよいですか?

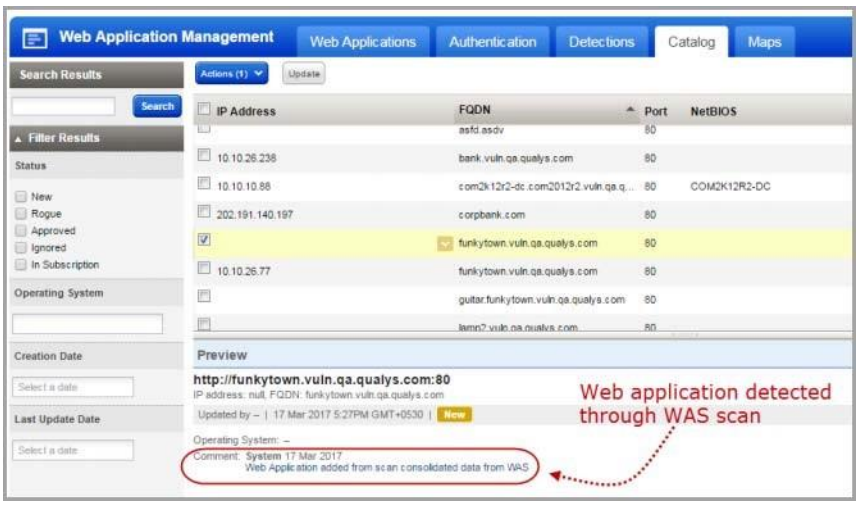
カタログは、自分(または別のユーザ)がマップ、VM アプリケーションを使用した脆弱性スキャン、または WAS スキャンを起動するまで空になります。完了すると、結果を処理する準備が整います。

- スキャン結果の処理: 「Web 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。
- マップの結果の処理: [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、[結果の処理] 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について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い場合でも、Web アプリケーションを見つけることができます。強化された検出方法により、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 スキャンによって検出されたが、Web 資産として追加されていない 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、および情報の中心的な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表示されます。たとえば、[Finding Type] を [Burp] として選択すると、Burp 関連の検出結果に適用可能なフィルターが有効になり、他の適用されないフィルターは無効になります。
リストに表示されるアイコンで検出結果タイプを区別できます。

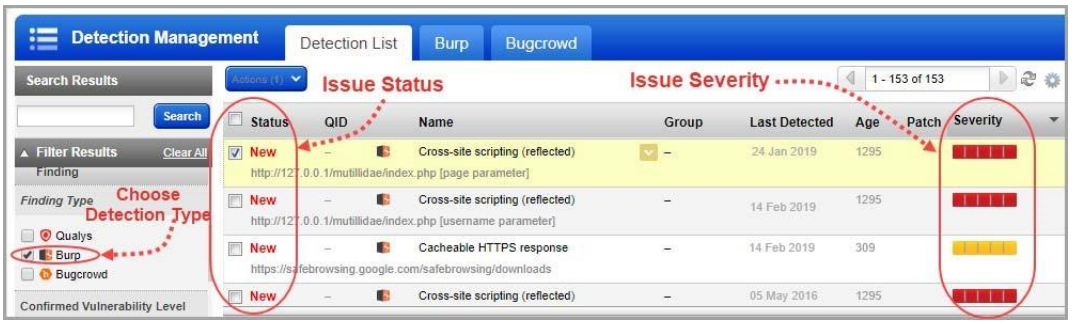
- Qualys 検出
- Burp の問題
- Bugcrowd の提出

Burp の所見をインポートしたいですか?

(Express Lite をご利用の方はご利用いただけません。)

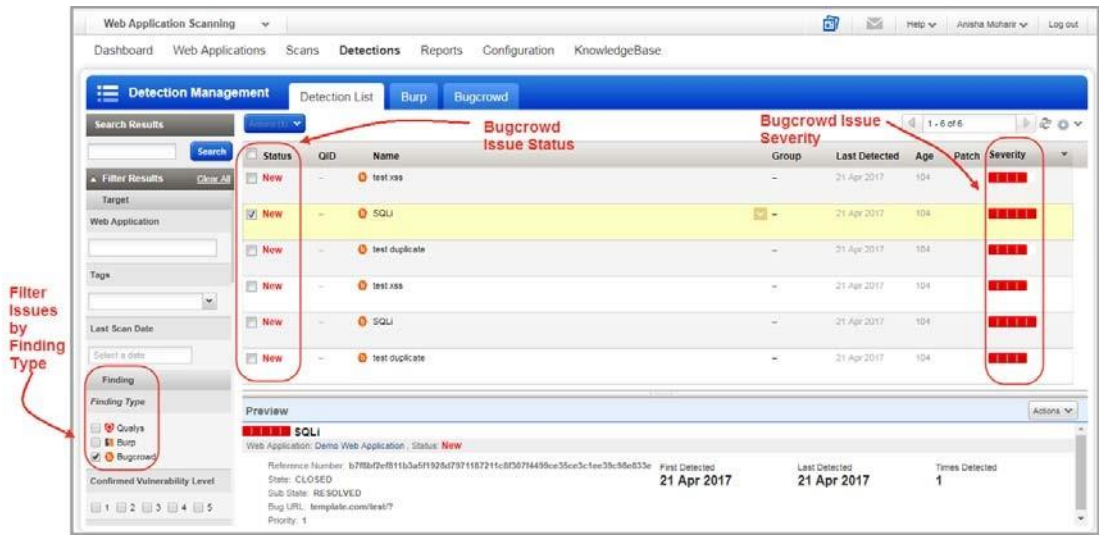
Qualys WAS Burp 拡張機能を試して、WAS 検出結果を Burp Repeater に直接インポートし、脆弱性を手動で検証することをお勧めします。この拡張機能は、Burp Suite Professional Edition と Burp Suite Community Edition の両方で動作します。

Qualys WAS Burp 拡張機能は、BApp ストアの [Extender] タブから入手できます。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、[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 レポートを適用する 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 [検出] リストに表示されます。[検出] > [検出リスト] に移動します。検索フィルターの [検出結果タイプ] で [Burp] を選択すると、検出日、ステータス、重大度など、問題を詳細に表示できます。



Bugcrowd との統合

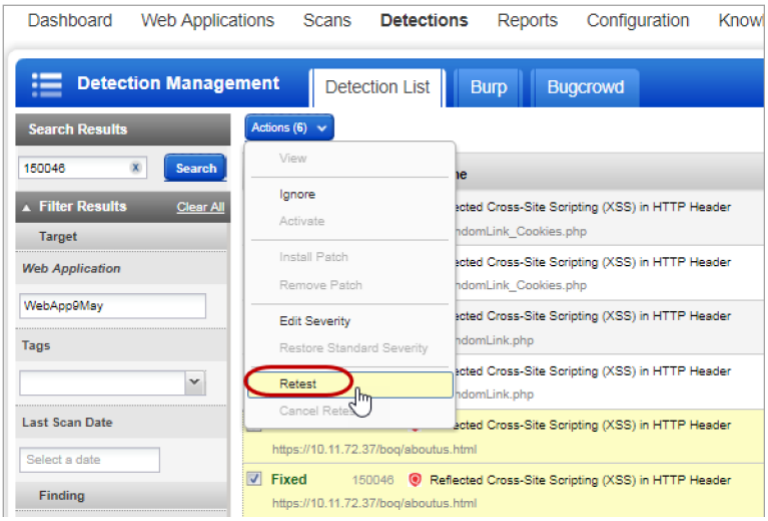
Bugcrowd のお客様は、承認された Bugcrowd の提出物を WAS アカウントにインポートすることもできます。Bugcrowd 統合により、WAS によって特定された脆弱性と、Bugcrowd が管理するバグ報奨金プログラムによって検出された脆弱性を表示および報告する方法が提供されます。
[Detections > Bugcrowd > Import に移動し、ローカルファイルシステムから CSV 形式の Bugcrowd ファイルを選択し、Bugcrowd ファイルを適用する Web アプリケーションを選択します。Bugcrowd ファイルとともにインポートされた課題が課題リストに表示されます。[検出] > [検出リスト] に移動します。



Retest multiple findings without launching a full scan

フルスキャンを開始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、検出結果の脆弱性を簡単に再テストできます。再テストの対象となるのは、潜在的な脆弱性、確認された脆弱性、および機密性の高いコンテンツのみです。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グループ化し、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も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取り消すと、検出結果のバッチ全体について再テスト・スキャンが取り消されます。

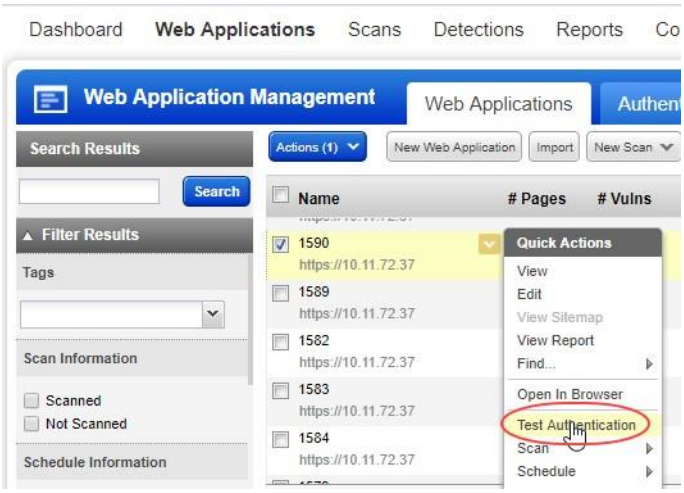


[検出] > [検出リスト] に移動します。左ペインのフィルターを使用して、同じ QID と Web アプリケーションのすべての結果を表示できます。再テストする結果を選択します。「アクション」メニューから、「再テスト」を選択します。確認すると、選択したすべての検出結果に対して再テスト スキャンが一度に開始されます。

認証テスト

定義した Web アプリケーションの認証レコードは、検出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すばやくテストし、スキャナーが Web アプリケーションに対して認証できるかどうかをテストできます。

「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て、クイック・アクション・メニューから「認証のテスト」を選択します。



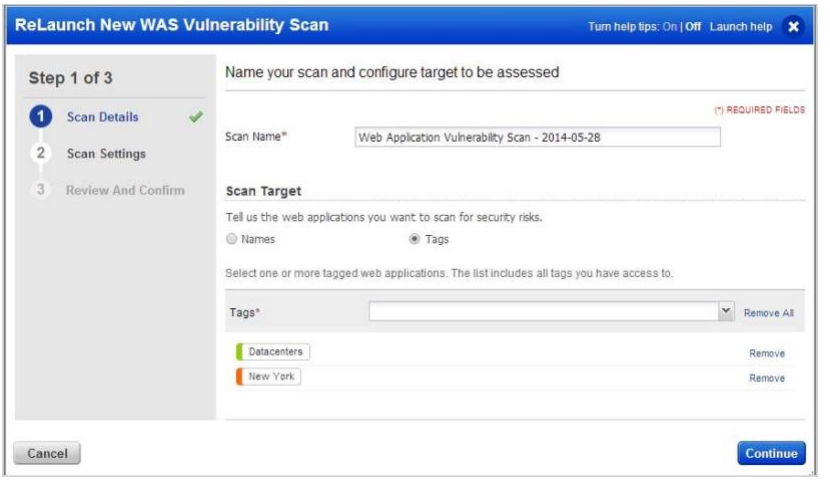
認証テスト・スキャンが「完了」状態になったら、クイック・アクション・メニューから「レポートの表示」を選択し、「認証テスト・スキャン」レポートを表示します。

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。任意の数の Web アプリケーションをマルチスキャンとして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、企業内にある数百または数千の Web アプリケーションをスキャンして、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。

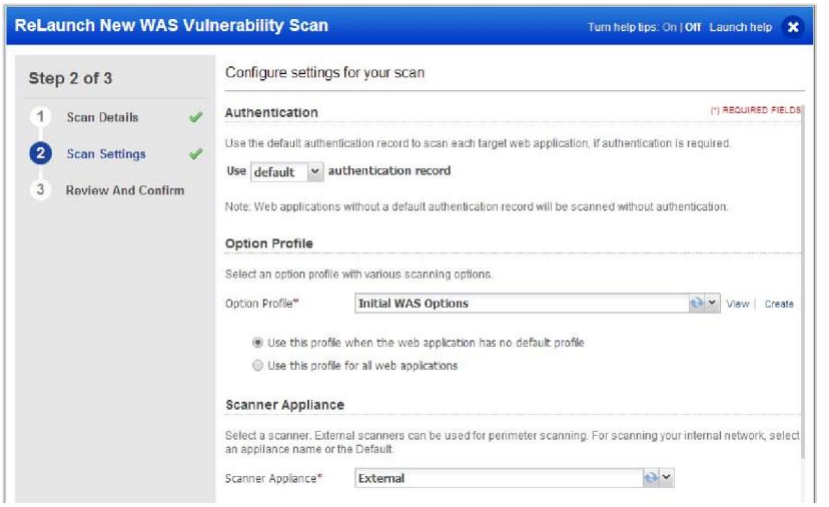
アプリケーションの選択 – 個々のアプリまたはタグを選択します

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 - ユーザはアプリケーション名を選ぶことができます。

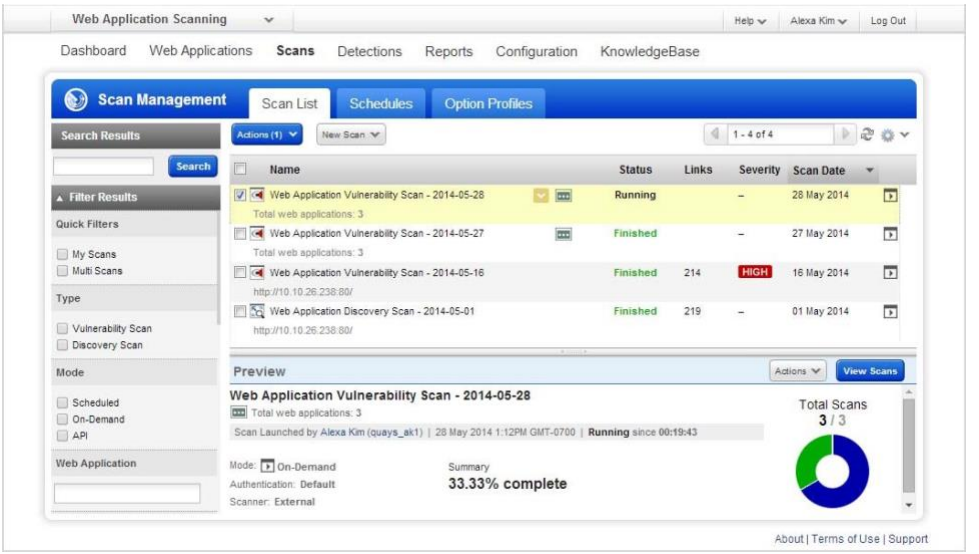


スキャン設定の選択(認証、オプションプロファイル、Scanner Appliance)

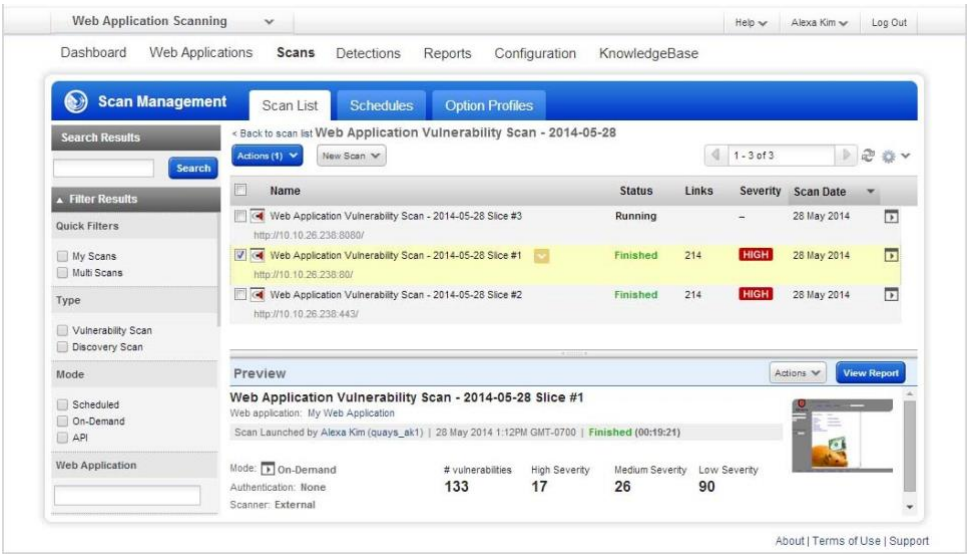
マルチスキャン機能には、Web アプリケーションのデフォルトを受け入れたり、デフォルトの Web アプリケーション設定を上書きしたりするための多くのオプションが用意されています。



マルチスキャンのスキャンステータスをプレビューペインで表示する



マルチスキャン内のすべてのスキャンのスキャンステータスの詳細を表示する



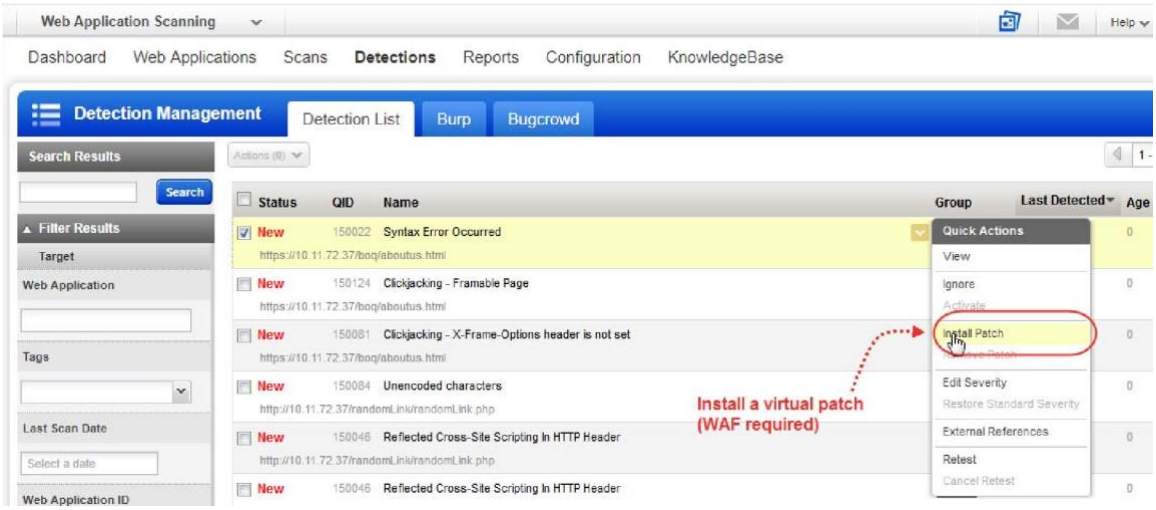
Selenium スクリプトを使用したスキャン

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、ブラウザーでアクションを記録して、自動テストケースをすばやく簡単に生成、編集、および再生できます。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 コマンドの一覧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するのに役立ちます。

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、複雑さが増し、Qualys WAS での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略化できます。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

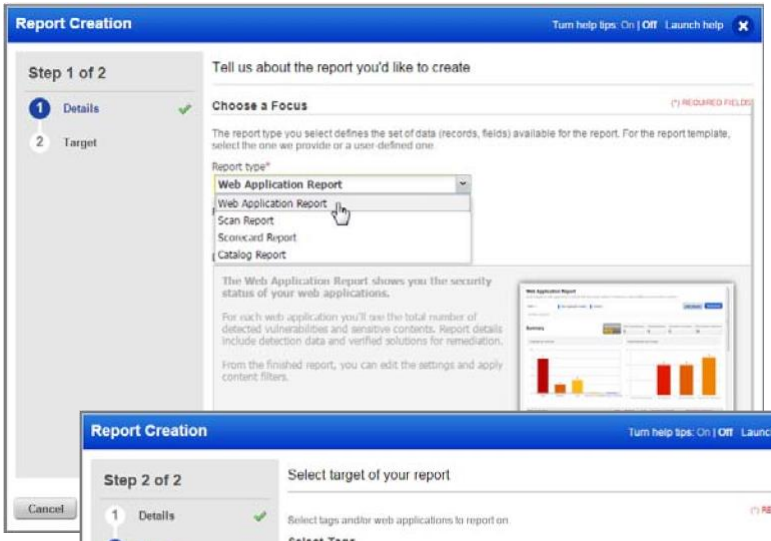
WAS では、アカウントで WAS と WAF が有効になっている場合に、選択した脆弱性(検出)の仮想パッチをインストールできます。インストールが完了すると、選択した脆弱性の悪用をブロックするファイアウォールルールが自動的に追加されます。WAF API に、仮想パッチの管理に役立つ機能が追加されました。



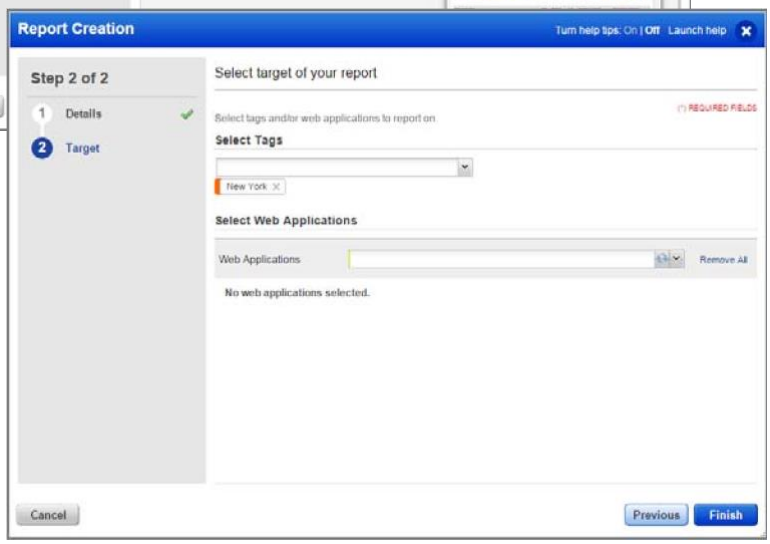
レポート

レポートの作成手順

[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。

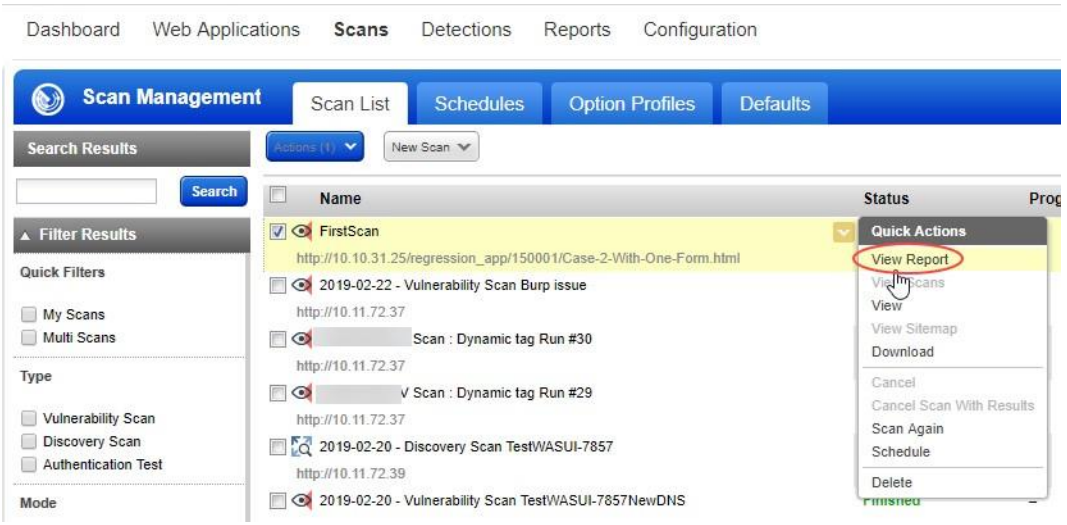


レポートの種類 (この場合は Web アプリケーションレポート) を選択します。

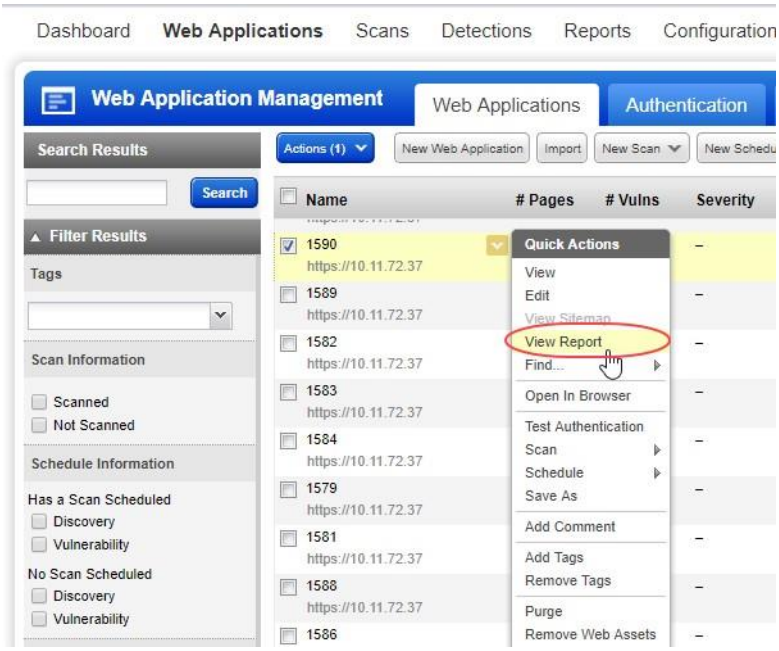


Web アプリケーションの選択を タグや名前を使用しておこないます。

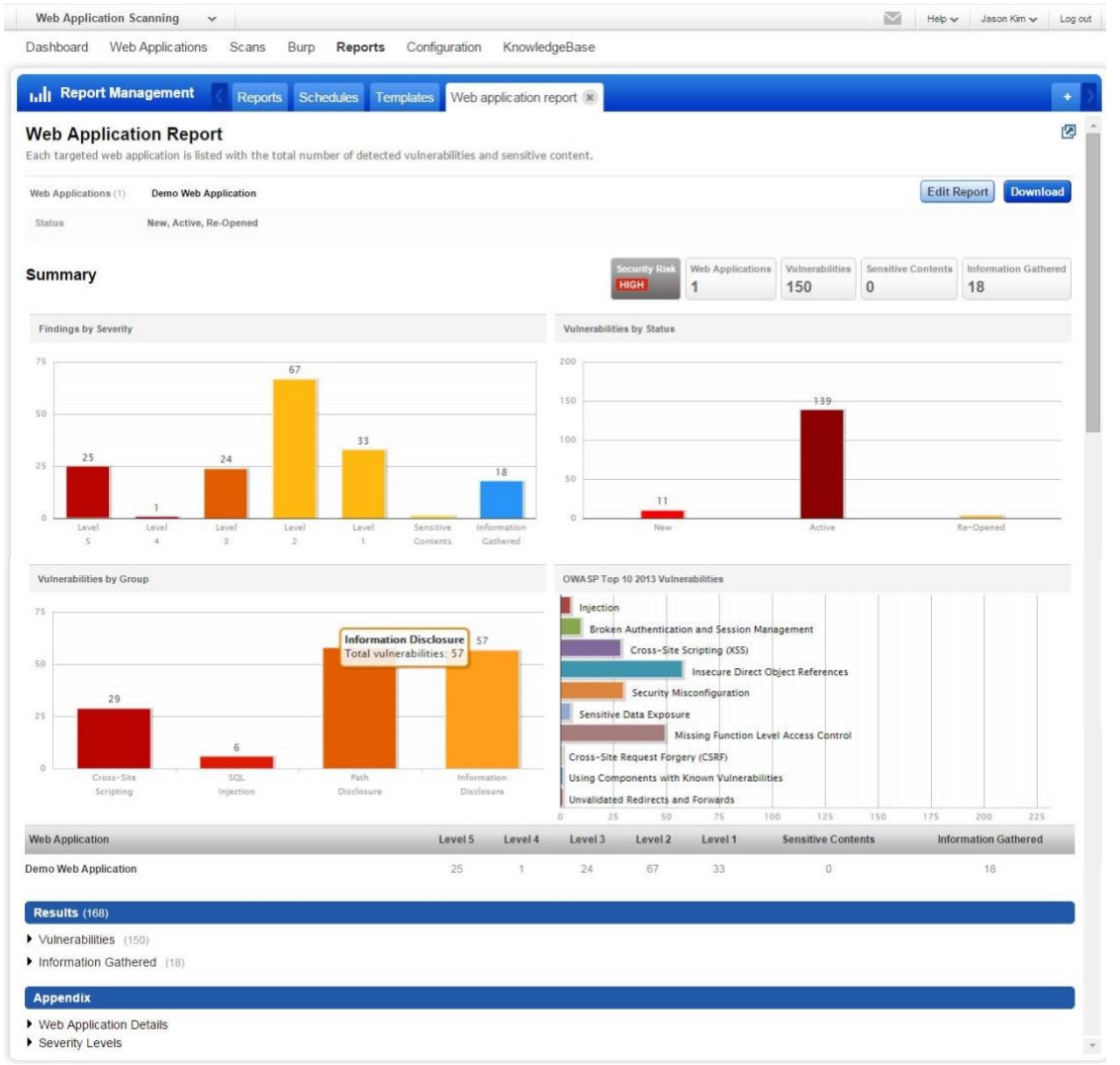
または、スキャン・リストからスキャンを選択し、クイック・アクション・メニューから「レポートの表示」を選択して、スキャン・レポートをすばやく生成することもできます。



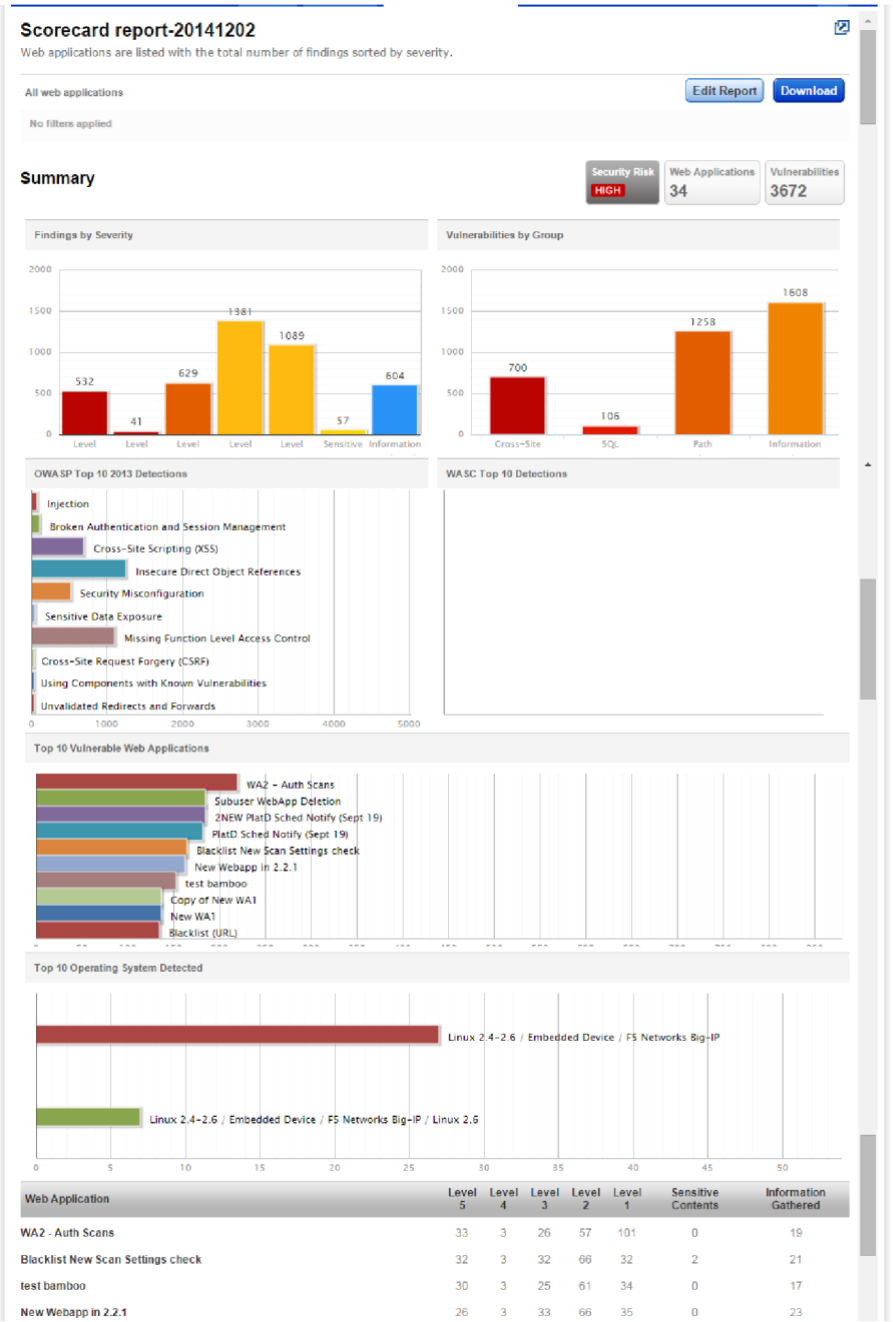
同様に、Web アプリケーションのクイックアクションメニューから [レポートの表示] を使用して Web アプリケーションレポートを生成できます。



サンプル Web アプリケーション レポート



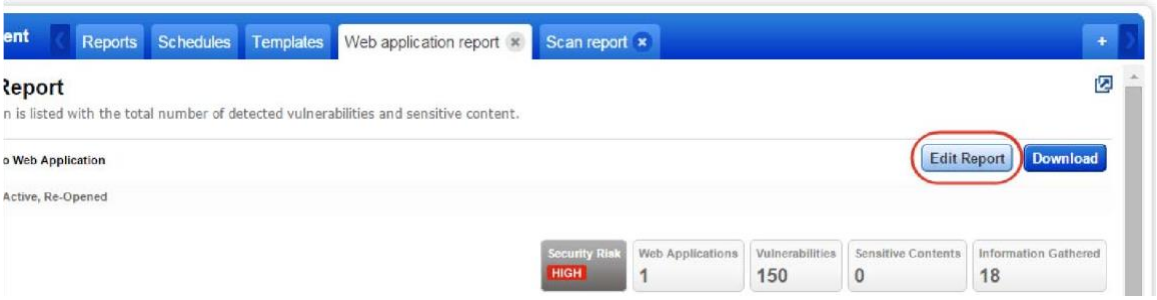
スコアカード レポートのサンプル



ヒントとコツ

設定を表示、編集し、繰り返す

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設定を変更するだけで、変更内容を反映した更新されたレポートが作成されます。これにより、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コンテンツにすばやく適用できます。



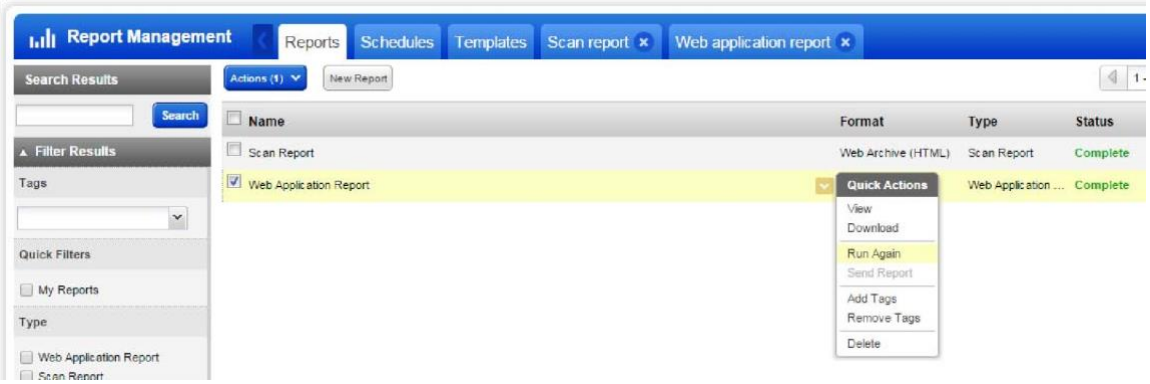
並べて比較する

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、並べて比較し、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いいですか?

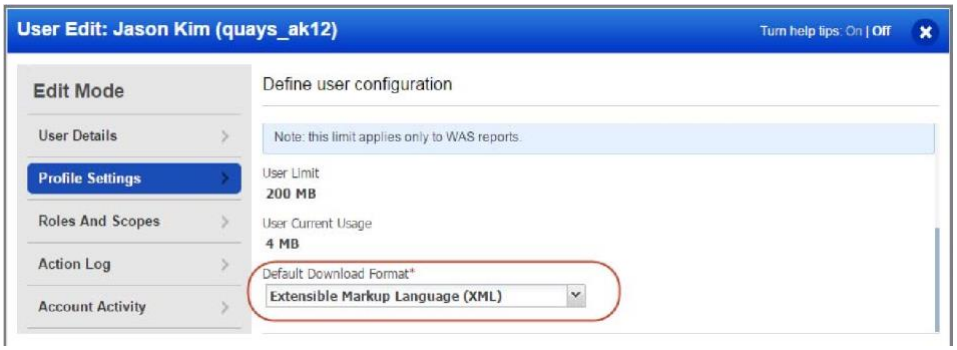
[ダウンロード] オプションを使用して、レポートをローカル マシンにダウンロードし、アカウントに保存します。

レポートリストには、保存したレポートを表示できる場所です。各レポート(概要)を表示し、ダウンロードし、再度実行し、タグを追加してレポートを他のユーザと共有できます。



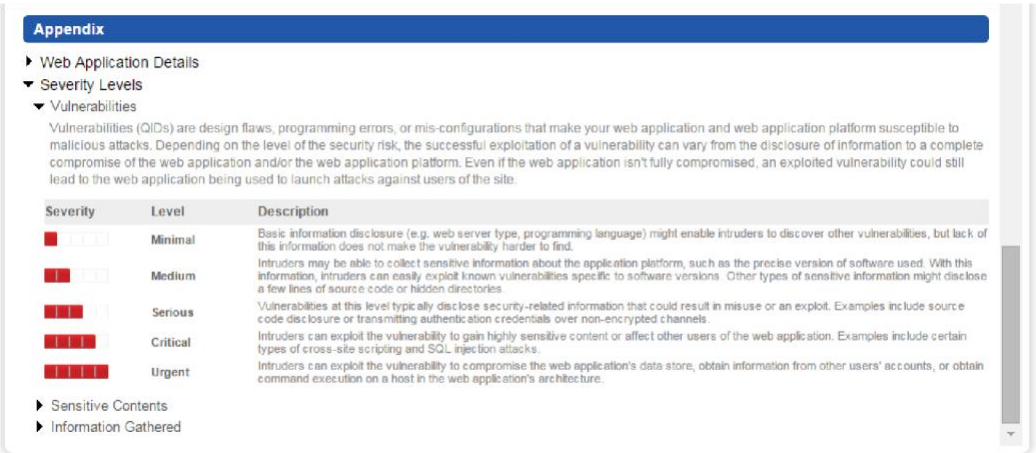
既定のレポート形式を設定する

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。



重大度とレベルは何を意味していますか?

付録に移動し、[重大度レベル]をクリックするだけです。各検出の種類 (脆弱性、機密性の高いコンテンツ、収集された情報) の重大度とレベルごとに説明があります。

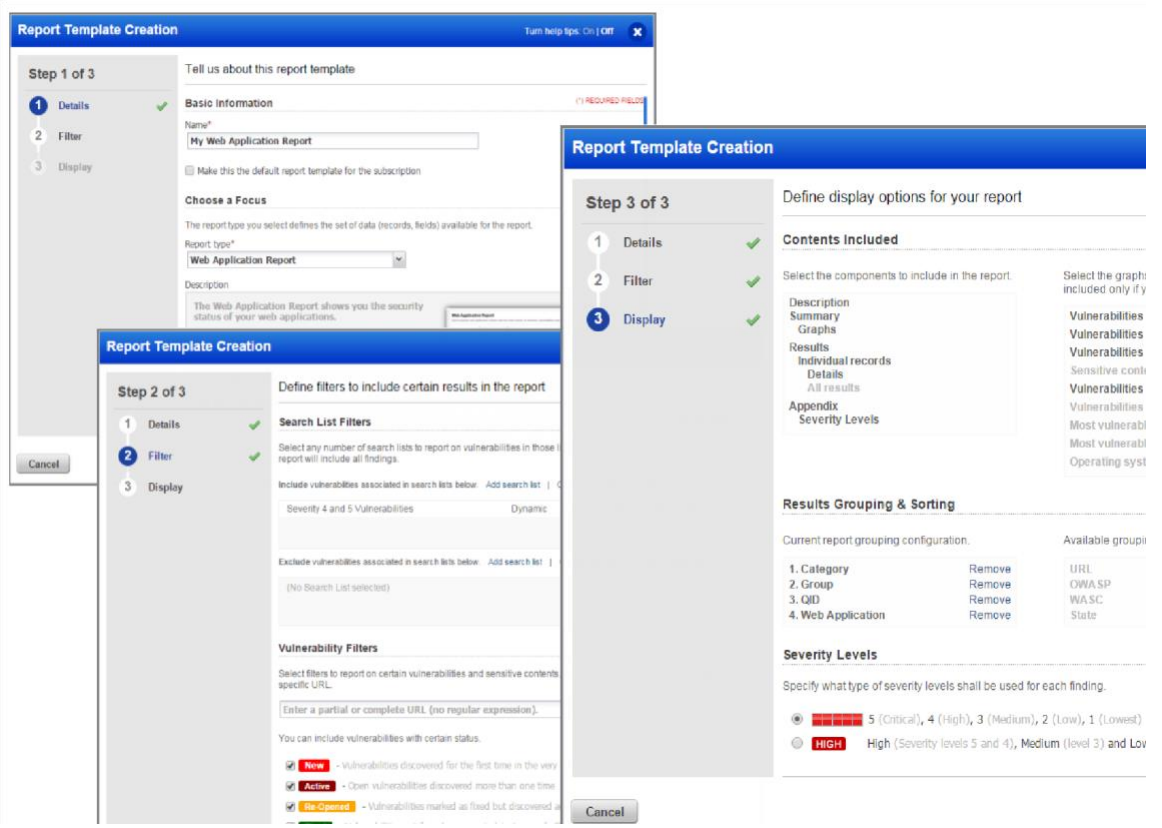


Customizable report templates

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、将来使用する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では、検索リスト、脆弱性検出、無視としてマークされた脆弱性などのフィルタや、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。

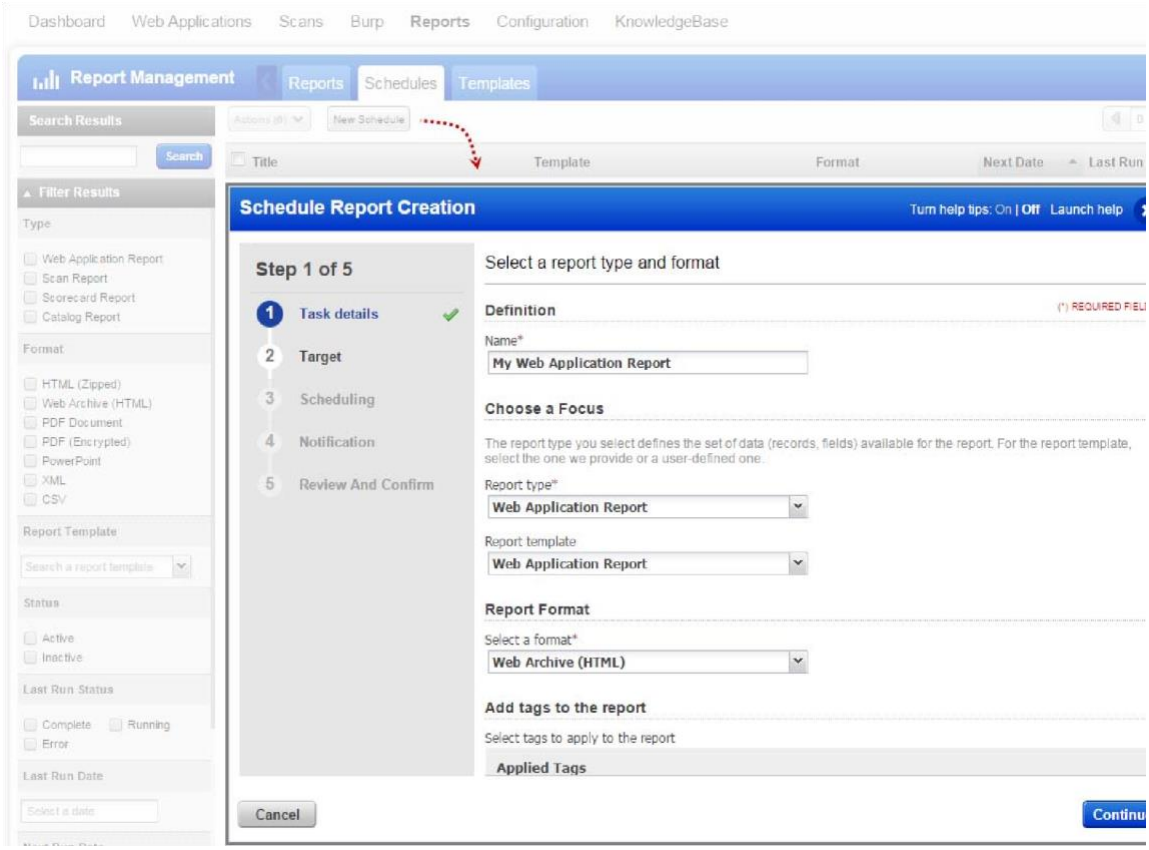


テンプレートを共有したいですか?他のオブジェクト(Web アプリケーション、レポートなど)と同様にタグを付け、ユーザスコープにタグを追加するだけです(管理ユーティリティを使用)。

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、他のユーザと共有するための優れた方法です。

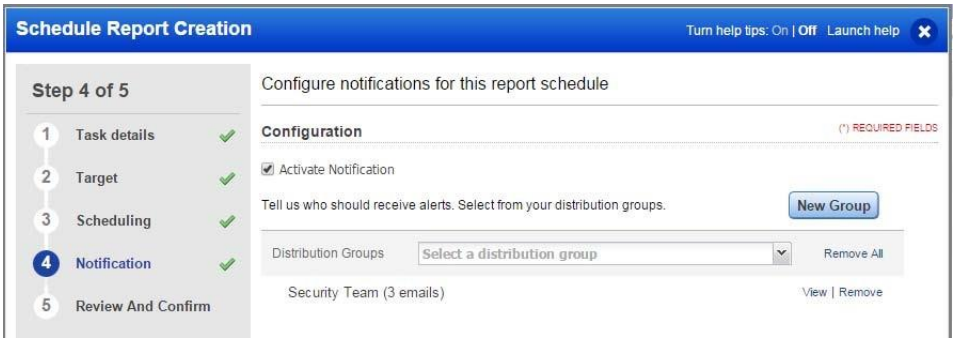
[Reports > Schedules] に移動し、[New Schedule] をクリックして開始します。



Scheduled Reporting

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、メール通知を受け取るユーザを指定するだけです。アラートは、レポートがダウンロードするためのリンクとともに完了するたびに、およびレポートの生成が失敗するたびに、ユーザに設定されます。


Schedule Report Creation
Turn help tips: On | Off Launch help
Step 4 of 5
1 Task details
2 Target
3 Scheduling
4 Notification
5 Review And Confirm
Configure notifications for this report schedule
Configuration
(*) REQUIRED FIELDS
Activate Notification
Tell us who should receive alerts. Select from your distribution groups.
New Group
Distribution Groups
Select a distribution group
Remove All
Security Team (3 emails)
View | Remove

ユーザの追加

Qualys サブスクリプションにユーザを追加し、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、マネージャーの役割が必要です。

新しいユーザ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・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] セクションに移動して新しいユーザを作成します。手順を順を追って説明します。

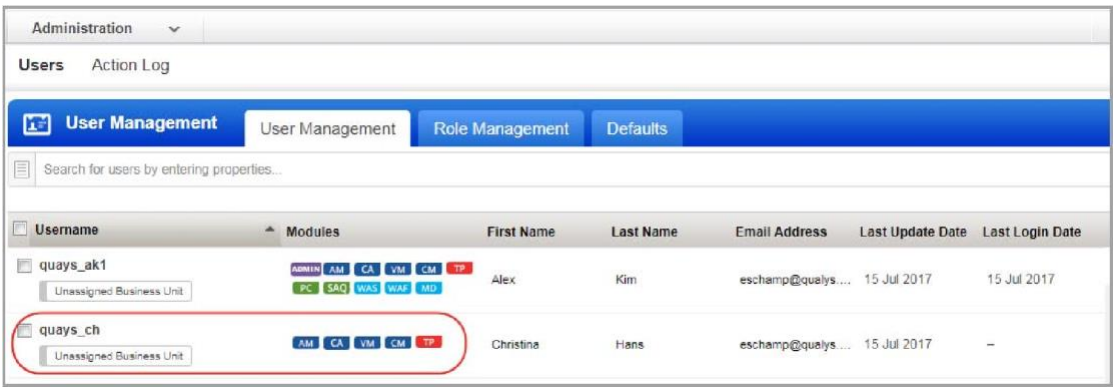
ユーザ、その役割、権限の表示

Qualys Cloud Platform UI には、サブスクリプション内のすべてのユーザ、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への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)には、WAS へのアクセスが自動的に付与されないことがわかります。

ユーザに WAS へのアクセス権を付与する方法

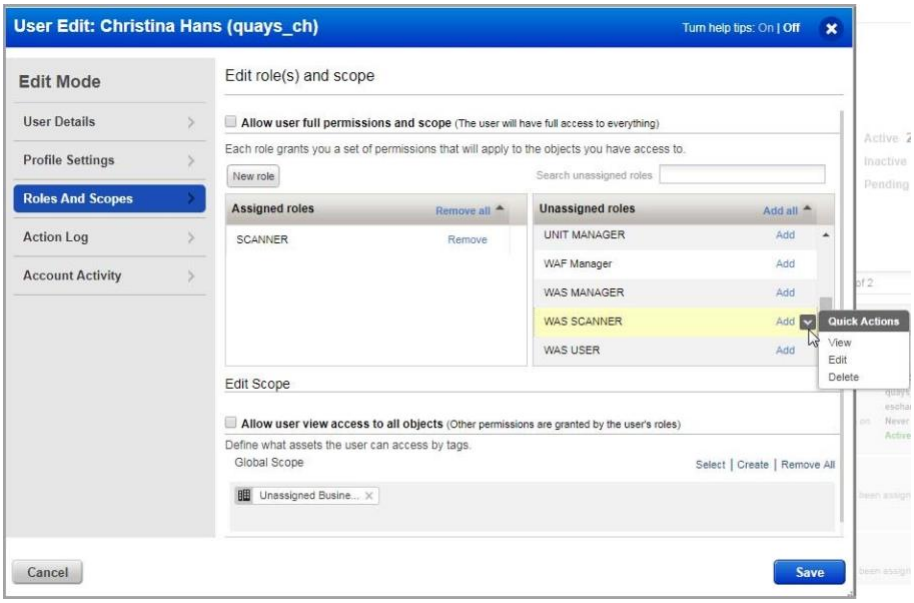
スキャナーの役割を持つ新しいユーザ Christina Hans を作成し、Christina が WAS を使用して Web アプリケーションのセキュリティ リスクをスキャンできるようにするとします。

Qualys Cloud Platform のアプリケーションに対する新しいユーザの権限を表示します。管理ユーティリティに移動します。新しいユーザの場合、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。

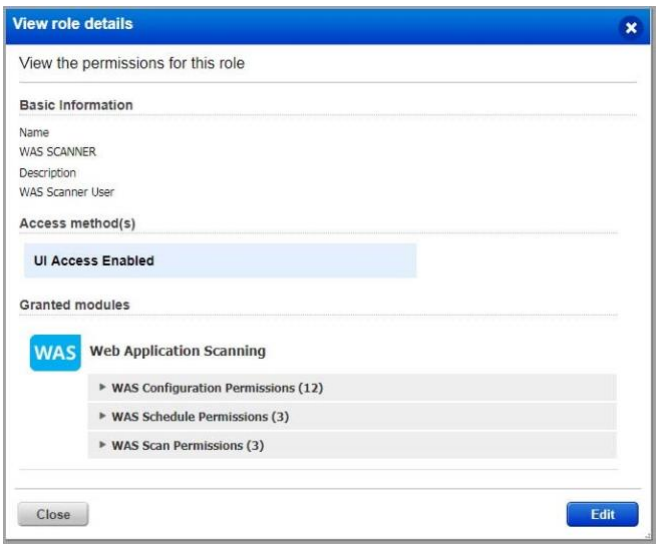


新しいユーザを編集します (ユーザを選択し、[クイック アクション] メニューから [編集] を選択します)。[ロールとスコープ] で、ユーザには VM や PC のスキャン用の SCANNER ロールが割り当てられます (サブスクリプション設定によって異なります)。

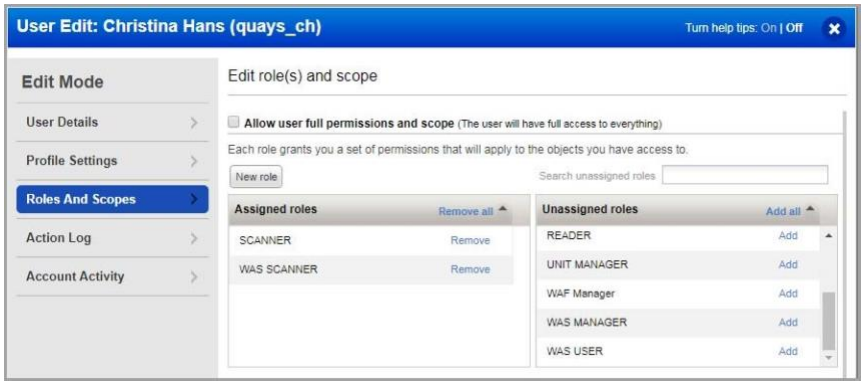
Qualys には、ユーザに WAS 権限を簡単に付与できるように、事前定義された WAS ユーザ ロールが用意されています。事前定義されたロールは、WAS MANAGER、WAS SCANNER、WAS USER です。



ユーザ Christina は SCANNER ロール (VM/PC 用) を持っているため、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/消去する権限を付与しません。



[閉じる] をクリックして、ユーザ設定を編集します。
[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。



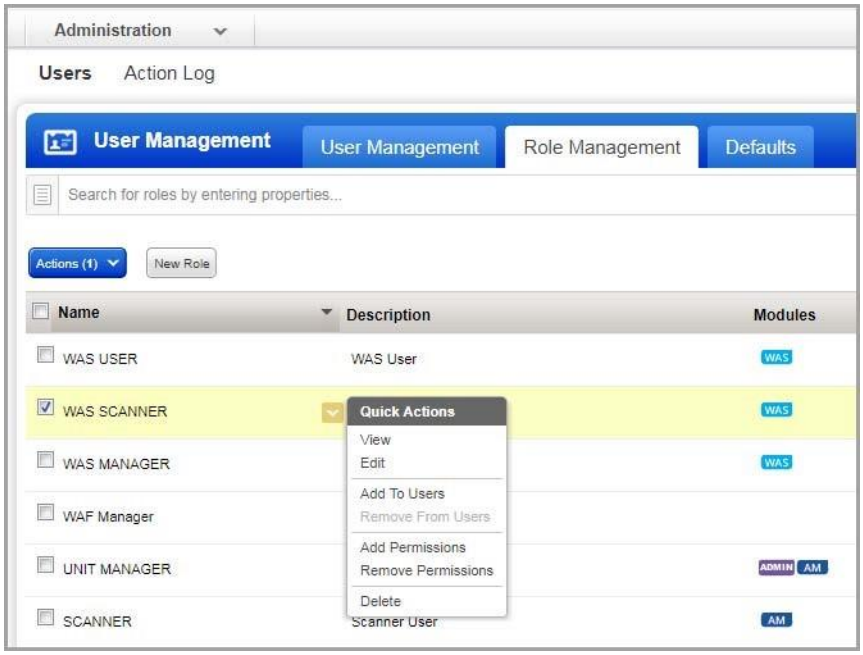
[スコープの編集] セクションを更新して、サブスクリプション内の Web アプリケーションへのアクセス権をユーザに付与します。既定では、ユーザは Web アプリケーションやその他の WAS 構成にアクセスできません。いずれかのオプションを選択します。
特定のタグを割り当てます。

フルスコープ(つまり、すべてのタグ)を付与する

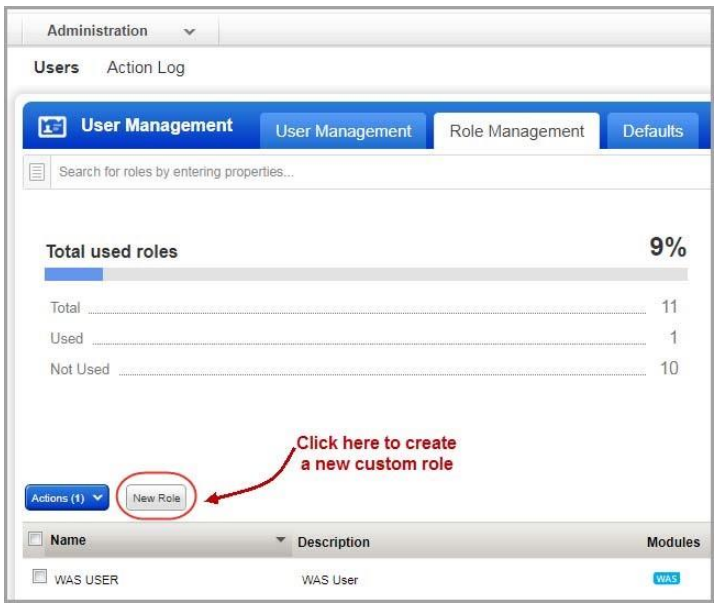
「保存」をクリックして、ユーザ設定を保存します。

ロール管理

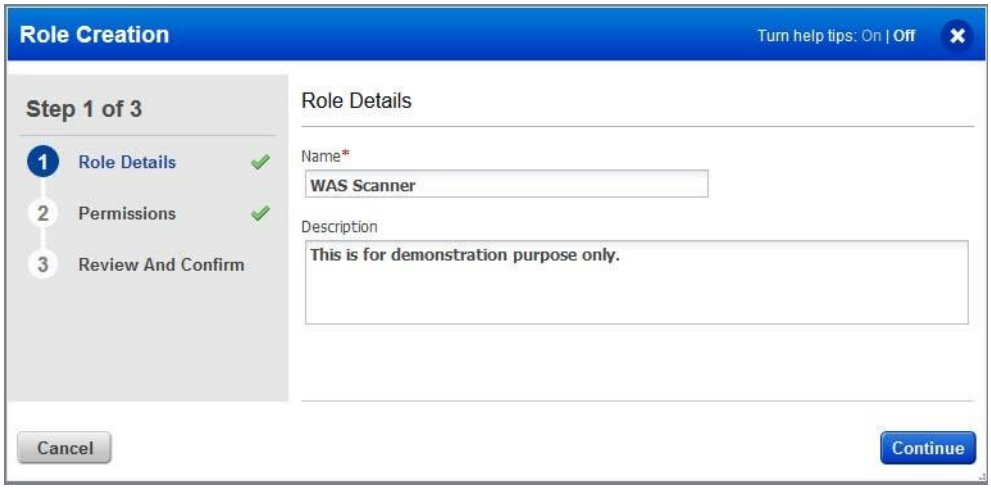
[ロール管理] セクションには、サブスクリプションのロールに関するすべての情報が表示されます。



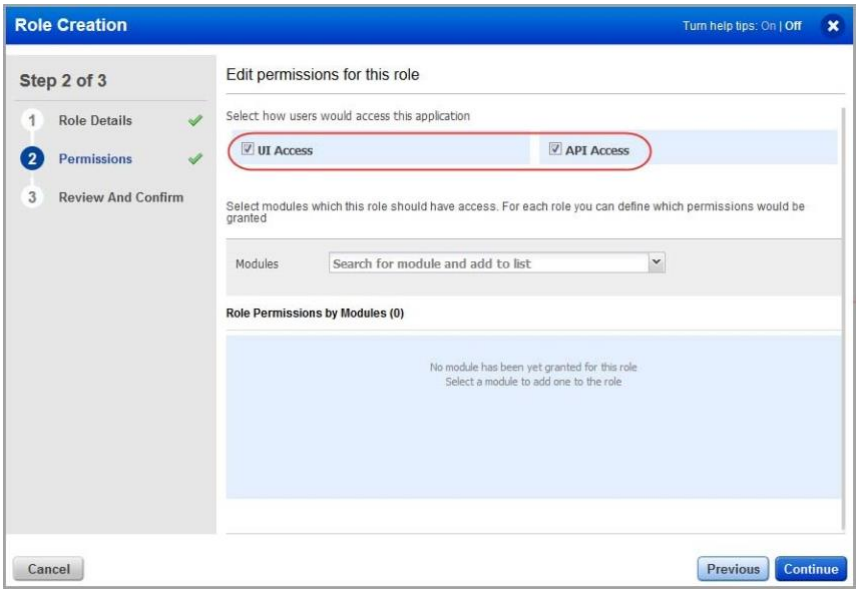
各ロールについて、詳細を表示し、ユーザへの追加、権限の追加、権限の削除などのアクションを実行できます。
「新規ロール」オプションを使用すると、必要な権限を正確に持つカスタム・ロールを作成できます。



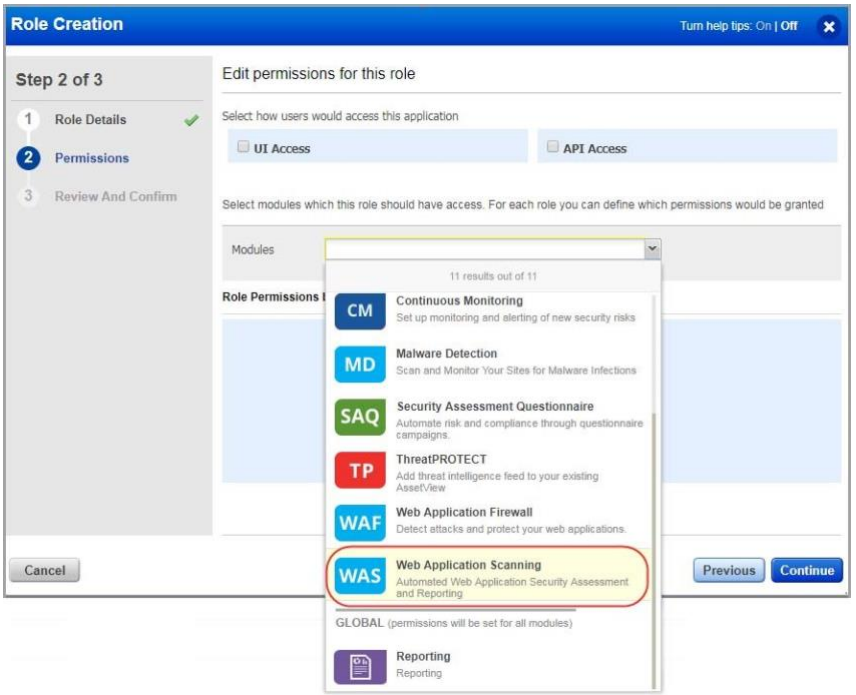
たとえば、ロール WAS Scanner を作成できます。



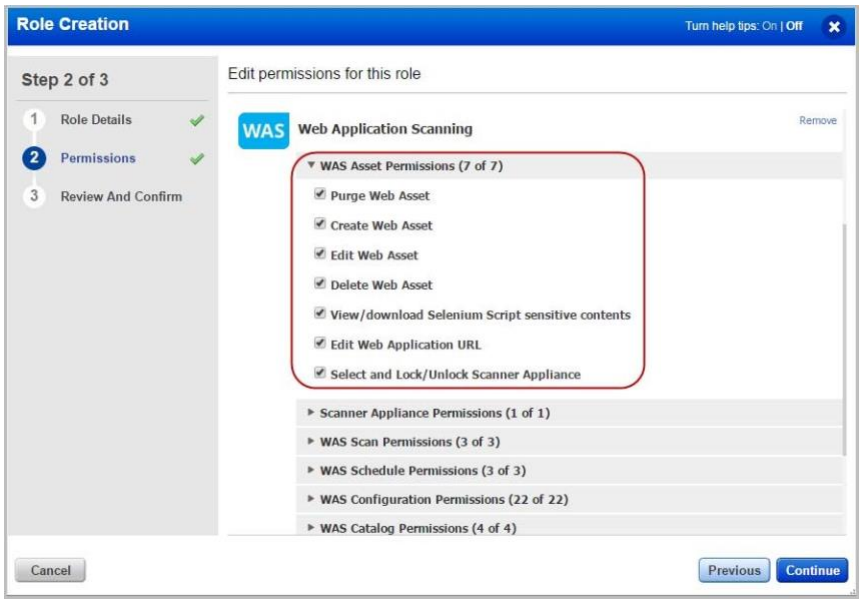
ロールに UI や API へのアクセス権を付与します。
ロールの詳細で、ユーザのアクセス方法を選択します。



ロールに WAS アプリへのアクセス権を付与します。[アクセス許可] 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?

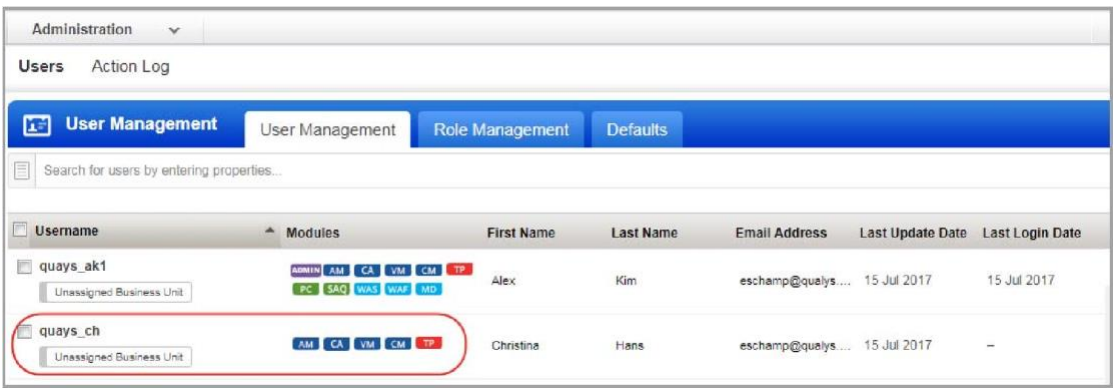
WAS モジュールにアクセスするには、十分な権限が必要です。管理者以外のユーザ (スキャナー、リーダー、ユニット マネージャー) には、サブスクリプション内の WAS アプリケーションと Web アプリケーションにアクセスするためのアクセス許可を付与する必要があります。マネージャ (または「ユーザの編集」権限を持つユーザ) は、管理ユーティリティを使用してユーザのロールを設定できます。

次に示す手順に従って、ユーザにロールを割り当てます。

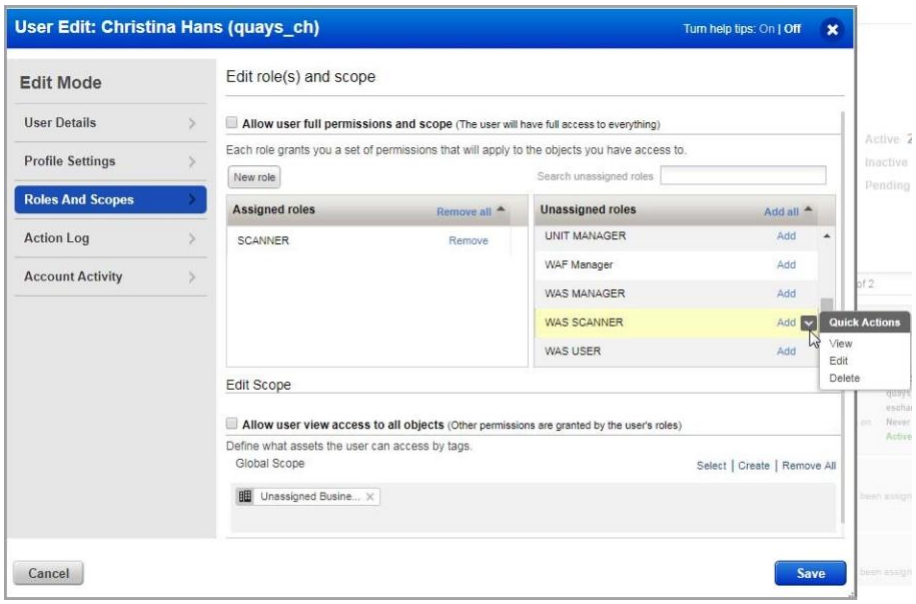
前提条件

この手順は、マネージャロールを持つユーザ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) 「ユーザ管理」タブで、問題に直面しているユーザを選択し、「クイック・アクション」メニューから「**編集**」を選択します。



4) [Roles and Scopes] タブに移動し、要件に従って、ユーザに適切な WAS Role & Scope を選択します。Qualys Administration Utility オンライン ヘルプの「ユーザ ロールの管理」の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、そのタグをユーザのスコープに追加します。

5) [**保存**] をクリックし、ユーザに再度ログインするように要求します。

ヘルプの入手

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、電話によるヘルプ、および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迅速に回答できるようにします。週 7 日、24 時間体制でサポートします。オンラインサポート情報には、ww.qualys.com/support/ から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、および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。