



# 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

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

Qualys および Qualys ロゴは Qualys, Inc. の登録商標です。その他の商標は、それぞれの所有者に帰属します。

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 .....	
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 .....	
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 .....	
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（インターネット、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サポートによる強化された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kinsスプラグイン - Qualys WAS ジェンkins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。

始めましょう  
さあ、始め  
ましょう！

## 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。

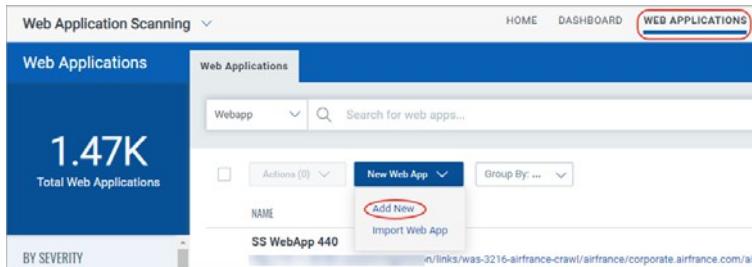
The screenshot shows the Qualys WAS application picker. It is organized into several sections:

- Modules** dropdown menu.
- COMPLIANCE (3)**
  - PC** Policy Compliance: Define, Audit and Document IT Security Compliance.
  - PCI** PCI Compliance: Achieve compliance with the PCI Data Security Standard (DSS).
  - FIM** File Integrity Monitoring: Monitor changes on file systems.
- APPLICATION SECURITY (5)**
  - WAS** Web Application Scanning: Automated Web Application Security Assessment and Reporting. This item is highlighted with a red box.
  - WAF** Web Application Firewall: Detect attacks and protect your web applications.
  - MD** Web Malware Detection: Scan and Monitor Your Sites for Malware Infections.
  - SECURE Seal**: PLEASE NOTE! Secure Seal will be retired on December 31, 2020.
  - AS** API Security: Assess the security posture of your APIs throughout the SDLC.
- SENSOR MANAGEMENT (1)**
  - CA** Cloud Agent: Stay updated with network security by deploying agents on your hosts.
- UTILITIES**
  - Administration**: Manage Application Users and Permissions.
  - UD** Unified Dashboard: Build multiple widgets from your Qualys apps in a single dashboard.

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。

A screenshot of the 'Add New: Web Application' form. The left sidebar shows the steps: 1. Basic Info (which is active and highlighted in blue), 2. Crawl Settings, 3. Default Scan Settings, 4. Additional Configurations, and 5. Review & Confirm. The main panel is titled 'Basic Info' and contains fields for 'Name' (set to 'My Web Application') and 'Web Application Url (Swagger file URL)' (set to 'https:// mywebapp.com'). There are also sections for 'Custom Attributes' (with a 'Username' field set to 'jdoe') and 'Tags' (with a single tag '100 Webapp' listed). At the bottom are 'Cancel' and 'Next' buttons.

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。

The screenshot shows the 'Web Applications' section of the interface. On the left, there's a summary card with '1.47K Total Web Applications'. Below it is a chart titled 'BY SEVERITY' showing counts for severity levels 3, 5, 0, 4, and 1. The main area is a table listing three web applications: 'Documentation', 'SS WebApp 427', and 'Web Application - Demo'. Each row includes columns for Name, Vulnerabilities (with a breakdown of Medium, High, and Critical), #Links, Last Scanned, Last Updated, and Tags.

NAME	VULNERABILITIES	#LINKS	LAST SCANNED	LAST UPDATED	TAGS
Documentation	Medium: 1, Open Vulns: 2	1	21 Sep 2021	21 Sep 2021	SS Target1 5 more...
SS WebApp 427	Medium: 7, Open Vulns: 14	7	21 Sep 2021	21 Sep 2021	SS Target1 11 more...
Web Application - Demo	High: 894, Open Vulns: 13	894	21 Sep 2021	21 Sep 2021	SS Target1 9 more...

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できます。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

クリ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リックアクションメニューのオプションが表示されます。クリ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。

**Web Application Scanning**

**Web Applications**

**1.47K** Total Web Applications

**BY SEVERITY**

3	613
5	335
0	307
4	125
1	87
1 more	▼

**LAST SCAN STATUS**

CANCELED	538
FINISHED	468
NO_WEB_SERVICE	194
TIME_LIMIT_REA...	175
CANCELED_WIT...	36
2 more	▼

**Web Applications**

Search for web apps... Webapp Actions (1) New Web App Group By: ...

NAME

- SS WebApp 548
- SS WebApp 427
- SS WebApp 571
- SS WebApp 450
- SS WebApp 208
- Sanity Test 3.8 WebApp1

Quick Actions

- View
- Edit
- Add Tags
- Remove Tags
- Add Comment
- Purge
- Remove Web Asset
- Save As

### 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。

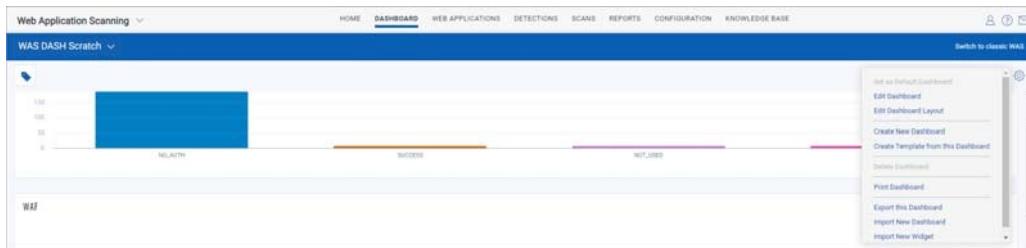
深刻度とは？各QIDには、当社サービスにより以下の深刻度レベルが割り当てられます：確認済み脆弱性（赤）、潜在的脆弱性（黄）、情報収集（青）。

### 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。

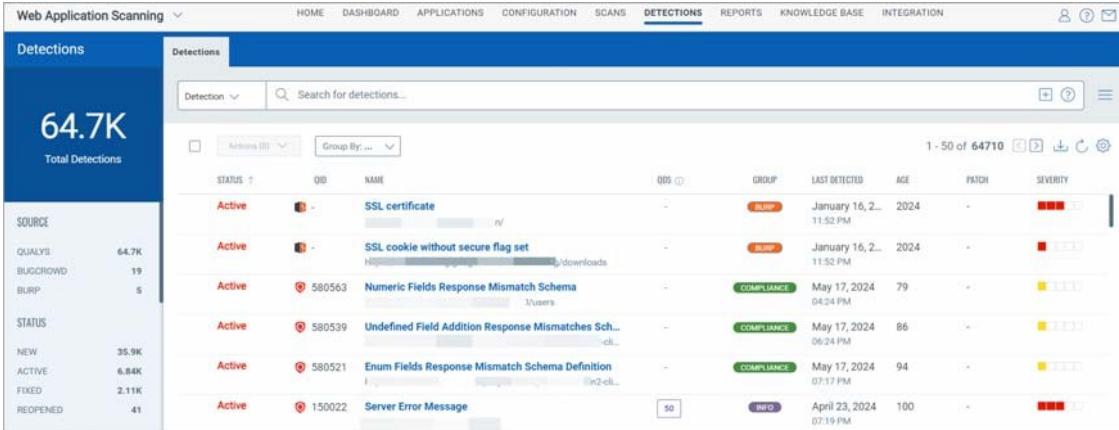


- Qualys検出



- Burpの問題

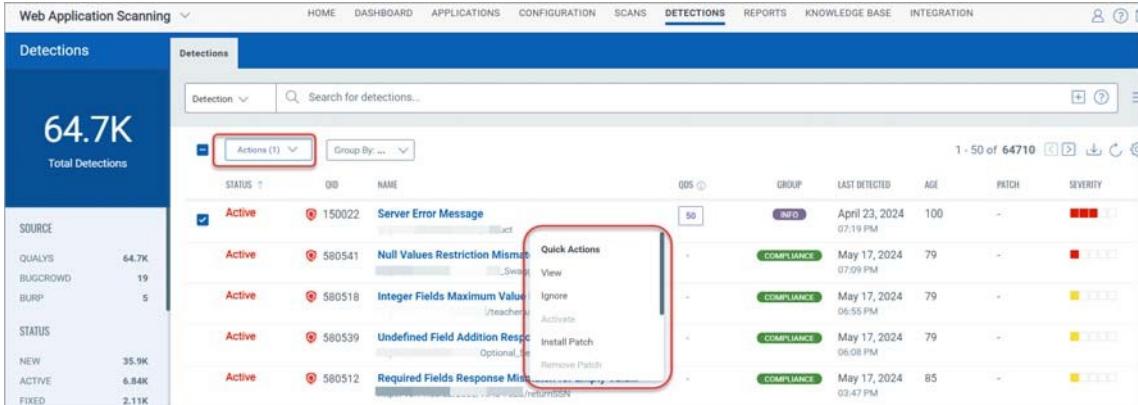
 - Bugcrowdの報告



STATUS	ID	NAME	QBR	GROUP	LAST DETECTED	AGE	PATCH	SEVERITY
Active	-	SSL certificate	-	BURP	January 16, 2024 11:52 PM	-	-	■■■
Active	-	SSL cookie without secure flag set	-	BURP	January 16, 2024 11:52 PM	-	-	■■■
Active	580563	Numeric Fields Response Mismatch Schema	-	COMPLIANCE	May 17, 2024 04:24 PM	79	-	■■■
Active	580539	Undefined Field Addition Response Mismatches Sch...	-	COMPLIANCE	May 17, 2024 06:24 PM	86	-	■■■
Active	580521	Enum Fields Response Mismatch Schema Definition	-	COMPLIANCE	May 17, 2024 07:17 PM	94	-	■■■
Active	150022	Server Error Message	50	INFO	April 23, 2024 07:19 PM	100	-	■■■

### 検出項目に対するアクションの実行

クリ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リックアクションメニューのオプションが表示されます。クリ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。



STATUS	ID	NAME	QBR	GROUP	LAST DETECTED	AGE	PATCH	SEVERITY
Active	150022	Server Error Message	50	INFO	April 23, 2024 07:19 PM	100	-	■■■
Active	580541	Null Values Restriction Mismat...	-	COMPLIANCE	May 17, 2024 07:09 PM	79	-	■■■
Active	580518	Integer Fields Maximum Value	-	COMPLIANCE	May 17, 2024 06:55 PM	79	-	■■■
Active	580539	Undefined Field Addition Respo...	-	COMPLIANCE	May 17, 2024 06:08 PM	79	-	■■■
Active	580512	Required Fields Response Mis...	-	COMPLIANCE	May 17, 2024 03:47 PM	85	-	■■■

### 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、設定を確認したら「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、クローク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。

**Result**

- Highlight changes from previous scan
- New - this link was not found in the previous scan
- Modified - this result was found by the previous scan but its value was different
- Removed - this link was found, but was reported in the previous scan

Duration of crawl phase (seconds): 161.00

Number of Links: 9 (This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

```

http://10.11.48.95/SecurityHeaders/
http://10.11.48.95/SecurityHeaders/Ajax/
http://10.11.48.95/SecurityHeaders/Ajax/CarTokenInURL/
http://10.11.48.95/SecurityHeaders/Ajax/JSFromEmails/
http://10.11.48.95/SecurityHeaders/Ajax/JSFromEmails/
http://10.11.48.95/SecurityHeaders/Ajax/phpSerialize/ajax_search.php
http://10.11.48.95/SecurityHeaders/Ajax/phpSerialize/ajax_search_bigarray.php
http://10.11.48.95/SecurityHeaders/Ajax/phpSerialize/int_ajax.php

```

## 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。

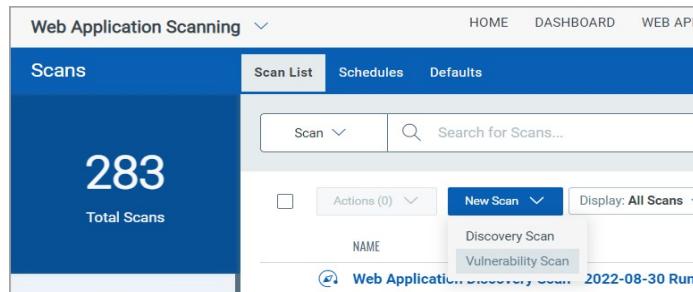
トップメニューの「ナレッジベース」をクリックしてください。

ID	NAME	SUPPORTED BY	INFORMATION	CATEGORY	SEVERITY
6	DNS Host Name	VM, Cloud	名	Information gathering	■■■■■
9	Open RPC Services List	VM	名	RPC	■■■■■
11	Hidden RPC Services	VM	名	RPC	■■■■■

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。

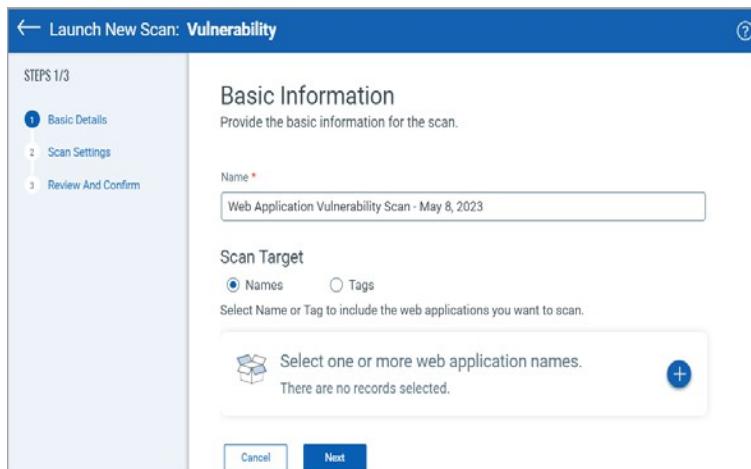


The screenshot shows the 'Web Application Scanning' interface. At the top, there are tabs for 'HOME', 'DASHBOARD', and 'WEB APP'. Below that is a 'Scans' section with a large blue background. In the center of the blue area, it says '283 Total Scans'. To the right of this, there are buttons for 'Scan List', 'Schedules', and 'Defaults'. Below these buttons is a search bar with a magnifying glass icon and the placeholder 'Search for Scans...'. Further down are buttons for 'Actions (0)', 'New Scan', and 'Display: All Scans'. A dropdown menu under 'Display' shows 'Discovery Scan' and 'Vulnerability Scan', with 'Vulnerability Scan' being highlighted. At the bottom of the blue area, there is a link 'Web Application Discovery Scan 2022-08-30 Run'.

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。

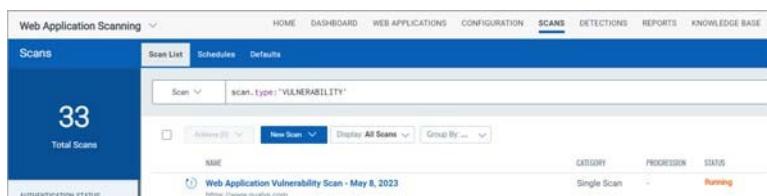


The screenshot shows the first step of the 'Launch New Scan: Vulnerability' wizard. It has a title bar with a back arrow and a help icon. On the left, there's a sidebar with 'STEPS 1/3' and three numbered steps: 1. Basic Details (which is selected), 2. Scan Settings, and 3. Review And Confirm. The main area is titled 'Basic Information' with the sub-instruction 'Provide the basic information for the scan.' Below this is a 'Name \*' field containing 'Web Application Vulnerability Scan - May 8, 2023'. Under 'Scan Target', there are two radio buttons: 'Names' (selected) and 'Tags'. A note below says 'Select Name or Tag to include the web applications you want to scan.' Below this is a list box with a placeholder 'Select one or more web application names.' and a note 'There are no records selected.' At the bottom are 'Cancel' and 'Next' buttons.

## 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。



The screenshot shows the 'Scans' dashboard. At the top, there are tabs for 'HOME', 'DASHBOARD', 'WEB APPLICATIONS', 'CONFIGURATION', and 'SCANS' (which is selected). Below that is a 'Scan List' section with a large blue background. In the center of the blue area, it says '33 Total Scans'. To the right of this, there are buttons for 'Actions (0)', 'New Scan', and 'Display: All Scans'. A dropdown menu under 'Display' shows 'Discovery Scan' and 'Vulnerability Scan', with 'Vulnerability Scan' being highlighted. At the bottom of the blue area, there is a link 'Web Application Vulnerability Scan - May 8, 2023' with the URL 'https://www.qualys.com'.

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。



The screenshot shows the 'Scan Progress' details for a specific scan. At the top, it says 'Scan Progress' and 'Scan report due 19:00:07 (2 minutes remaining)'. Below this is a 'Scan Phase' section with a progress bar showing 'Scanning' and 'Completed'. There are also sections for 'Statistics' and 'Details'.

## 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。

The screenshot shows the 'View Scan Details' interface for a 'Web Application Vulnerability Scan - Apr 10, 2023'. The 'Overview' tab is selected. Key statistics displayed include:

- Scanning Time: 00:02:36
- Links Collected: 123
- Requests Tracked: 1
- Assessed Errors: 8
- Assessment Time: 01:07:23
- Links Checked: 5
- Resources Performed: 3728
- Time taken: 0.02 Seconds
- Scanning Status: In Progress
- Number of Issues: 8
- Landing Screen: Web Application screen

## 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。

The screenshot shows the 'Reports' section of the application. The 'Results' tab is active, displaying a hierarchical list of vulnerabilities:

- Vulnerabilities (39)
  - Cross-Site Scripting (10)
    - Low: 150084 Unencoded characters (10)
  - Path Disclosure (4)
    - Low: 150004 Predictable Resource Location Via Forced Browsing (4)
  - Information Disclosure (24)
    - High: 150515 Apache HTTP Server Prior to 2.4.53 Multiple Security Vulnerabilities (1)
    - High: 150315 Blind NoSQL MongoDB Injection (1)
    - High: 150539 Apache HTTP Server Prior to 2.4.54 Multiple Security Vulnerabilities (1)
    - High: 150415 Apache HTTP Server NULL pointer dereference and Server Side Request Forgery (SSRF) Vulnerability (CVE-2021-44224) (1)
    - High: 150818 Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities (1)
    - High: 150462 Apache HTTP Server Buffer Overflow Vulnerability (CVE-2021-44790) (1)
    - High: 520011 Open Secure Sockets Layer (OpenSSL) Type Confusion Vulnerability (CVE-2023-0286) (1)
    - High: 150616 Apache HTTP Server Prior to 2.4.56 Multiple Security Vulnerabilities (1)
    - High: 150461 Apache HTTP Server mod\_proxy Server Side Request Forgery (SSRF) Vulnerability (CVE-2021-40438) (1)
    - Medium: 520014 Open Secure Sockets Layer (OpenSSL) NULL Pointer Dereference Vulnerability (CVE-2024-0727) (1)

The screenshot shows the 'Detection Details' page for a specific vulnerability:

**Apache HTTP Server Prior to 2.4.53 Multiple Security Vulnerabilities**

**Detection Detail**

**Details**

- Finding #: 5837218
- Unique #: e91cad36-51c0-4fae-8ee8-01d4659
- Patch #:
- Group: Information Disclos
- CWE: CWE-787
- CVSS Web Appl.: A6 Vulnerable and Components
- CVSS Known Exploit: False
- CVSS V3 Base: 8.8
- CVSS V3 Temporal: 8.8
- CVSS V3 Attack Vector: Network
- Authentication: Not Used
- Web Application: 1.15.0.5 RC1 Create
- Times Found: 14

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。

The screenshot shows a web-based application scanning interface. At the top, there's a navigation bar with links like HOME, DASHBOARD, APPLICATIONS, CONFIGURATION, SCANS, DETECTIONS, REPORTS, KNOWLEDGE BASE, and INTEGRATION. The REPORTS link is underlined, indicating it's the active section. Below the navigation, there's a sidebar with options like SCAN REPORTS, Reports, Schedules, Templates, and Online Reports. Under SCAN REPORTS, there are entries for Scan Report and 1.15.0 RC1 Greater A2. The main content area is titled 'Confirmed Vulnerabilities'. It includes a legend for severity levels: Minimal (1 red square), Medium (2 red squares), Serious (3 red squares), Critical (4 red squares), and Urgent (5 red squares). The 'Minimal' level is described as basic information disclosure that might enable intruders to discover other vulnerabilities but doesn't make the vulnerability harder to find. The 'Medium' level is described as intruders being able to collect sensitive information about the application platform. The 'Serious' level is described as intruders being able to exploit known vulnerabilities specific to software versions. The 'Critical' level is described as intruders being able to compromise the web application's data store or obtain command execution. The 'Urgent' level is described as intruders being able to gain highly sensitive content or affect other users of the web application. Below this, there are sections for 'Potential Vulnerabilities', 'Sensitive Contents', and 'Information Gathered', each with a small icon and a descriptive title.

## 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、スキャナされた全ページ/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）。

The screenshot shows the 'Web Application Scanning' interface. In the top navigation bar, 'WEB APPLICATIONS' is selected. Below it, the 'Web Applications' section displays a total of 8.97K web applications. A summary table shows the count by severity: 0 (8.96K), 4 (3), 2 (2), and 3 (2). On the right, a list of applications is shown, including 'Qualys\_V0' (https://www.qualys.com) and 'Child User's Web App' (http://...). Each application entry includes a 'Quick Actions' dropdown menu with options like 'View', 'Edit', and 'View Sitemap'. A sidebar on the left provides navigation links for 'Reports', 'Schedules', 'Templates', 'Defaults', and 'Online Reports'.

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。

This screenshot shows a detailed sitemap for 'Child User's Web App'. It includes a sidebar for 'WEBAPP SITEMAPS' and a main panel for 'Sitemap - Child User's Web App'. The main panel displays filters for 'Linked Type' (Crawled, Rejected, External) and 'Detection Type' (Vulnerabilities, Sensitive Content). The 'Assessment Details' section features a donut chart showing the distribution of vulnerabilities across levels: Level 5 (0), Level 4 (0), Level 3 (4), Level 2 (16), and Level 1 (23). Below the chart is a table of 'LINK INFO' and 'CHILDREN INFO' with data for four categories: Crawled, External, and two unnamed categories with 'n' status. The sidebar also lists 'Reports', 'Schedules', 'Templates', 'Defaults', and 'Online Reports'.

## 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。

This dialog box allows users to edit search filters. It has two sections: 'Edit Filters' and 'Detection Type'. Under 'Edit Filters', there are checkboxes for 'Linked Type': 'Crawled' (unchecked), 'Rejected' (unchecked), 'External' (unchecked). Under 'Detection Type', there are checkboxes for 'Vulnerabilities' (checked) and 'Sensitive Content' (unchecked). At the bottom are 'Cancel' and 'Edit' buttons.

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

The screenshot shows a hierarchical site map. At the top is a link to 'http://10.11.68.88/'. Below it is 'phpMyAdmin/'. Under 'phpTestTargets/' there are two more links: 'AlegroCart/' and 'Install%20Instructions/'. This illustrates how the tool allows users to drill down into different parts of the application to analyze security.

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。

A context menu is open over a selected link. The menu includes options like 'Actions (1) ▾', 'Create Web Application', 'Add To Exclude List', and 'Add To Allow List'. The 'Actions (1)' dropdown is expanded, showing a single item: 'http://addons...' with a checked checkbox. Another link, 'http://blog...', is also visible below it.

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ヤン済みリンクを複数形式でダウンロード

The screenshot displays a report table with columns for STATUS, VULNS, SENSITIVE CONTENT, PAGES CRAWLED, REJECTED, EXTERNAL, and VULNS. There are two rows of data, both labeled 'External'. The first row has values: 0, 0, 0, 0, 0, 0. The second row has values: 0, 0, 0, 0, 1, 0. On the left side of the table, a list of URLs is shown with checkboxes next to them: 'http://www.webspell.org/' (unchecked), 'http://www.myspace.com/' (unchecked), 'http://www.impressoms.org/' (unchecked), 'http://www.google.com/' (unchecked), and 'http://www.yahoo.com/' (unchecked). A 'Download' button is located at the top right of the table area.

はじめましょう

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  
ましょう

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	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	0
10.10.26.238	CRAWLED 0	5	0	1	0	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

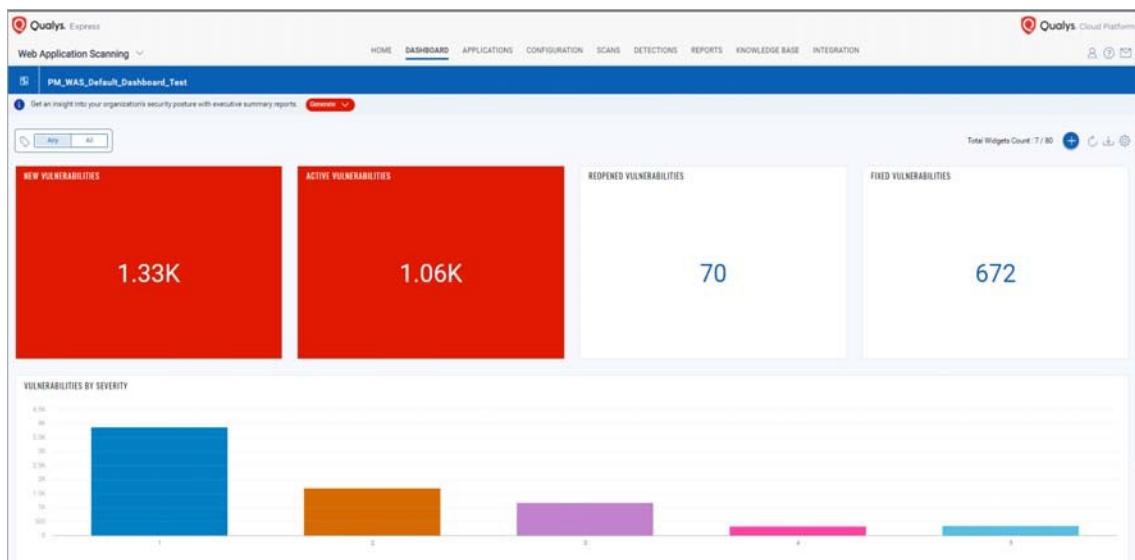
スキャンを繰り返し実行するスケジュールを設定することをお勧めします。これにより、組織にとって都合の良い時間帯に（毎日、毎週、または毎月）自動的に結果を取得できます。

[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。

The screenshot shows the Qualys Web Application Scanning interface. At the top, there's a navigation bar with links for HOME, DASHBOARD, APPLICATIONS, CONFIGURATION, SCANS, DETECTIONS, REPORTS, and KNOWLEDGE BASE. The 'SCANS' link is underlined, indicating it's the active section. Below the navigation, there's a blue header bar with tabs for 'Scans' (which is the current view) and 'Schedules'. A search bar says 'Search for scan schedules...'. Below the header, a large blue area displays the number '23' and the text 'Total Scan Schedules'. At the bottom of this area are buttons for 'Actions (0)' and 'New Schedule'.

## 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。



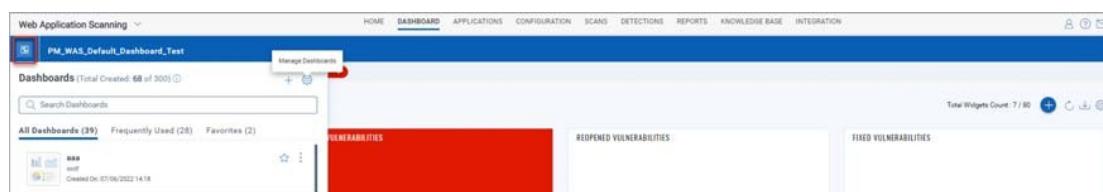
カスタムダッシュボードを簡単に作成し、ビューを切り替えられます

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。

The screenshot shows the 'Manage Dashboards' page with three dashboards listed:

- AWS Cloud and SaaS Security**  
Created By: SYSTEM USER  
Created On: 2 days ago 03:51 PM  
Last Updated By: SYSTEM USER  
Last Updated On: 2 days ago 03:51 PM  
Tags: [empty]
- 1.15.0.0 RC**  
1.15.0.0 RC  
Created By: [redacted]  
Created On: July 16, 2024 11:30 PM  
Last Updated By: [redacted]  
Last Updated On: July 16, 2024 11:44 PM  
Tags: [empty]
- DASH (DEFAULT)**  
apiDashboard  
Created By: [redacted]  
Created On: [redacted]  
Last Updated By: [redacted]  
Last Updated On: [redacted]  
Tags: [empty]

A context menu is open over the second dashboard ('1.15.0.0 RC'), showing options: Set as default, Edit Details, Print, Export, and Delete.

## 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。

The screenshot shows the 'Web Application Management' interface with the 'Catalog' tab selected. On the left, there's a search bar and a filter section with checkboxes for 'New', 'Rogue', 'Approved', and 'Ignored'. The main area is a table with columns: FQDN, Source, Port, NetBIOS, Status, and Created. The first row is highlighted. A context menu is open over this row, with 'Add To Subscription' highlighted in yellow.

FQDN	Source	Port	NetBIOS	Status	Created
mysite.CN	WAS Scan	80	New	26 Jun 2020	
mysite.CG	WAS Scan	80	New	26 Jun 2020	
mysite.CHINTAI	WAS Scan	80	New	26 Jun 2020	
mysite.CRUISE	WAS Scan	80	New	25 Jun 2020	
mysite.CRS	WAS Scan	80	New	25 Jun 2020	

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。

The screenshot shows the 'Web Application Management' interface. At the top, there are tabs for 'Web Applications', 'Authentication', 'Detections', 'Catalog', and 'Maps'. The 'Detections' tab is active. Below it, a 'Search Results' section includes a search bar, a 'Search' button, and a 'Update' button. A 'Filter Results' sidebar contains filters for 'Status' (New, Rogue, Approved, Ignored, In Subscription), 'Operating System', 'Creation Date', and 'Last Update Date'. The main table lists detected applications with columns for IP Address, FQDN, Port, and NetBIOS. One row is highlighted in yellow, showing 'funkytown.vuln.qa.qualys.com:80'. A 'Preview' panel for this entry shows the URL 'http://funkytown.vuln.qa.qualys.com:80', the IP address 'null', the FQDN 'funkytown.vuln.qa.qualys.com', and a note 'Updated by - | 17 Mar 2017 5:27PM GMT+0530 | New'. Below this, an 'Operating System' section shows a comment: 'Comment: System 17 Mar 2017 Web Application added from scan consolidated data from WAS'. A red arrow points from this comment to a callout box containing the text 'Web application detected through WAS scan'.

## 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[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。

The screenshot shows the Qualys WAS interface under the 'Detections' tab. On the left, there's a summary card for '103K Total Detections' with sections for 'SOURCE' (Qualys: 103K, Bugcrowd: 24, Burp: 12) and 'STATUS' (Active: 29.7K, New: 28.8K, Fixed: 15.1K, Reopened: 1.24K). The main area displays a table of detected vulnerabilities. A red box highlights the 'SOURCE' section of the summary card. Another red box highlights the search bar at the top of the detection list, which contains the query 'vulnerability.source:BUGCROWD'. The table columns include ID, NAME, GROUP, LAST DETECTED, AGE, PATCH, and SEVERITY. The severity scale is shown as a color gradient from yellow (low) to red (high).

## 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。

The screenshot shows the Qualys WAS interface under the 'Detections' tab. On the left, there's a summary card for '24 Total Detections' with sections for 'SOURCE' (Bugcrowd: 24) and 'STATUS' (New: 24). The main area displays a table of detected vulnerabilities. A red box highlights the 'SOURCE' section of the summary card. Another red box highlights the search bar at the top of the detection list, which contains the query 'vulnerability.source:BUGCROWD'. The table columns include ID, NAME, GROUP, LAST DETECTED, AGE, PATCH, and SEVERITY. The severity scale is shown as a color gradient from red (high) to green (low).

## 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ナを実行することで、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、单一のパッチで再テストを実行できます。再テストスキャナでは、最新のスキャナ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、そのパッチ全体の再テストスキャナ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ナ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、ディスクバリースキャナ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。クリックアクションメニューから「Test Authentication」を選択します。

認証テストスキャナが完了状態になったら、クリックアクションメニューから「レポートを表示」を選択し、認証テストスキャナ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。

← Launch New Scan: Vulnerability (?)

STEPS 1/3

1 Basic Details 2 Scan Settings 3 Review And Confirm

**Basic Information**  
Provide the basic information for the scan.

Name \*  176 characters remaining

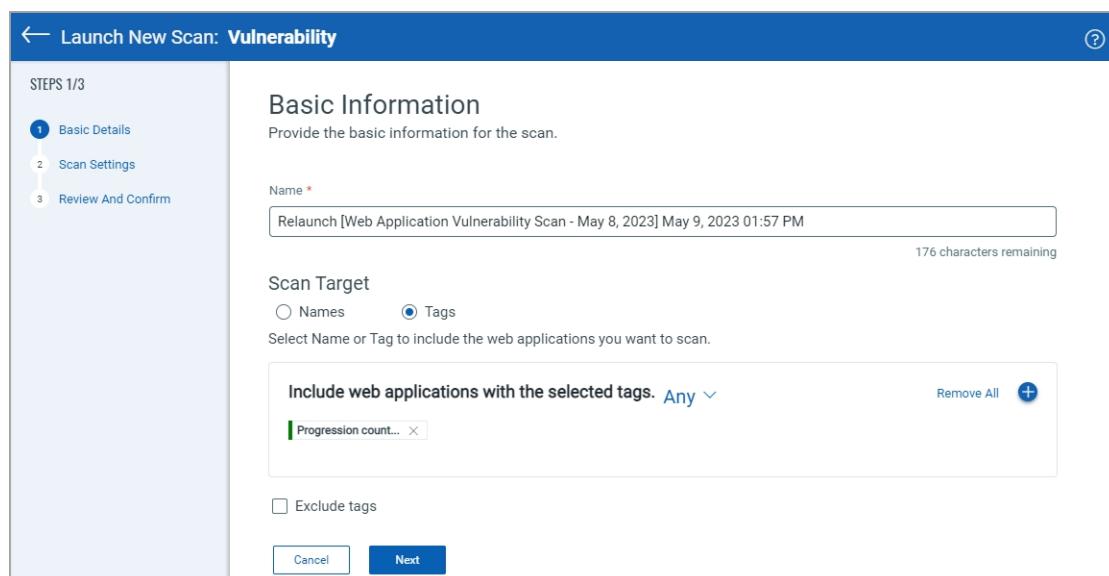
Scan Target  Names  Tags  
Select Name or Tag to include the web applications you want to scan.

Include web applications with the selected tags. Any ▼ Remove All +

X

Exclude tags

Cancel Next



## 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。

← Launch New Scan: Vulnerability

STEPS 2/3

1 Basic Details

2 Scan Settings

3 Review And Confirm

Scan Settings

Configure the scan settings.

Randomize Scanning

Select the check box to add randomization to the order of scanning web applications in a multi-scan scenario. This helps to prevent network slowdown and possible errors.

Randomize scan

Option Profile

Select an option profile.

Option Profile \*

AlegraCart OP

Use this profile if the web application has no default profile assigned       Use this profile for all web applications

Authentication

Use the default authentication record to scan each target web application, if authentication is required.

Use the default authentication record       Do not use an authentication record

Web applications without a default authentication record will be scanned without authentication.

Cancel Previous Next

## 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。

The screenshot shows the 'Web Application Scanning' interface with the 'Detections' tab selected. On the left, there's a summary section with '103K Total Detections'. Below it are sections for 'SOURCE' (QUALYS: 103K, BUGCROWD: 24, BURP: 12), 'STATUS' (ACTIVE: 29.7K, NEW: 28.8K, FIXED: 15.1K, REOPENED: 1.24K), and 'RETEST STATUS' (RETESTED: 128, CANCELING: 38, UNDER\_RETEST: 36, CANCELED: 27). The main area displays a table of detections with columns for STATUS, ID, NAME, GROUP, and LAST DETECTED. One row is selected, and a context menu is open over it, showing options like 'View', 'Ignore', 'Activate', 'Install Patch' (which is highlighted with a red box), 'Remove Patch', 'Edit Severity', 'Restore Standard Severity', 'Comment', 'Retest', and 'Cancel Retest'.

## 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。

The screenshot shows the 'Reports' section of the Web Application Scanning interface. It displays a summary of 47 total reports. Below this, there are search and filter options, and a list of reports with pagination at the bottom.

The screenshots show the 'Create New Report' wizard. Step 1/2: Basic Information. Report Type: Web Application Report. Step 2/2: Target. Include web applications with the selected tags: Any. WebAppTag10. There are no records selected.

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、クリ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。

The screenshot shows the 'Scans' section of the Web Application Scanning interface. It displays a list of scans with various details like category, status, severity, and scan date. A context menu is open over a specific scan entry, with 'View Report' highlighted.

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。

The screenshot shows the 'Web Application Scanning' interface. On the left, there's a sidebar with a blue header '42 Total Web Applications'. Below it, there are two sections: 'BY SEVERITY' and 'LAST SCAN STATUS'. The 'BY SEVERITY' section has three rows: '5 High', '3 Medium', and '1 Low'. The 'LAST SCAN STATUS' section has three rows: 'FINISHED 7', 'NO WEB SERVICE 2', and 'ERROR 1'. The main area is titled 'APPLICATIONS' and contains a table of web applications. The table has columns: NAME, TruRisk™ Score, VULNERABILITIES, LINKS, LAST SCANNED, LAST UPDATED, and TAGS. One row is selected, and its details are shown in a modal overlay: 'Proxy WEBAPP' (http://[REDACTED]), TruRisk™ Score 332, 4 Vulnerabilities (High: 4, Medium: 6), Last Scan Report, Open In Browser, Discovery Scan, Vulnerability Scan, Retest Webapp. The 'VULNERABILITIES' column shows severity levels: High (red), Medium (orange), and Low (green). The 'TAGS' column shows 'WebAppTag1.0' for the selected application.

NAME	TruRisk™ Score	VULNERABILITIES	LINKS	LAST SCANNED	LAST UPDATED	TAGS
Proxy WEBAPP http://[REDACTED]	332	High: 4 Open Vulns: 21	4	July 18, 2024 04:25 PM	July 18, 2024 04:43 PM	-
WEBAPP BURP PROXY COLLECTION http://[REDACTED]	78	Medium: 6 Open Vulns: 11	6	July 18, 2024 04:25 PM	July 18, 2024 04:23 PM	WebAppTag1.0
WEBAPP POSTMAN COLLECTION http://[REDACTED]	83	High: 4 Open Vulns: 26	-	July 18, 2024 04:25 PM	July 18, 2024 04:23 PM	WebAppTag1.0
WEBAPP POSTMAN COLLECTION ENVIRON http://[REDACTED]	312	High: 10 Open Vulns: 39	10	July 18, 2024 04:24 PM	July 18, 2024 05:20 PM	WebAppTag1.0 1 more

## Webアプリケーション レポートのサンプル

Web Application Scanning ▾

HOME DASHBOARD APPLICATIONS CONFIGURATION SCANS DETECTIONS REPORTS KNOWLEDGE BASE INTEGRATION

Reports Reports Schedules Templates Online Reports

APPLICATION REPORTS Web Application Report

Web Application Report

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Targets Applications selected: Proxy WEBAPP

Filters Status: New, Active, Reopened  
Remediation: Do not include ignored findings, Include patched findings  
Detection Source: Qualys, Burp, Bugcrowd

Summary

High Security Risk	1 Applications	21 Vulnerabilities	0 Sensitive Contents	14 Information Gathered
--------------------	----------------	--------------------	----------------------	-------------------------

VULNERABILITIES BY SEVERITY

Severity	Count
High	5
Medium	14
Low	21

VULNERABILITIES BY STATUS

Status	Count
New	21

OWASP TOP 10 2021 VULNERABILITIES

Vulnerability	Count
A01.2021 Broken Access Control	8
A02.2021 Cryptographic Failures	1
A03.2021 Injection	2
A04.2021 Insecure Design	1
A05.2021 Security Misconfiguration	8
A06.2021 Vulnerable and Outdated Components	3
A07.2021 Identification and Authentication Failures	1
A08.2021 Software and Data Integrity Failures	1
A09.2021 Security Logging and Monitoring Failures	1
A10.2021 Server Side Request Forgery (SSRF)	1

APPLICATION	HIGH	MEDIUM	LOW	SENSITIVE CONTENTS	INFORMATION GATHERED
Proxy WEBAPP	5	2	14	0	14

Results

Proxy WEBAPP (35)

Appendix

Application Details

## サンプルスコアカード レポート

**Web Application Scanning** ▾      HOME DASHBOARD APPLICATIONS CONFIGURATION SCANS DETECTIONS **REPORTS** KNOWLEDGE BASE INTEGRATION 👤 🎊 📈 📧

**Reports** Reports Schedules Templates **Online Reports**

**APPLICATION REPORTS**  
Web Application Report

**SCORECARD REPORTS**  
Scorecard Report

**Scorecard Report**

Web applications are listed with the total number of findings sorted by severity.

**Targets**

Applications selected: WEBAPP, POSTMAN, COLLECTION, ENVIRONMENT, VARIABLE. Include Tags: WebAppTag1, 0. Include Tag Match Type: Any. [5 more]

**Summary**

<b>High</b> Security Risk	<b>6</b> Applications	<b>151</b> Vulnerabilities
------------------------------	--------------------------	-------------------------------

**VULNERABILITIES BY SEVERITY**

Severity	Count
High	~30
Medium	~70
Low	~40
Sensitive Contents	~5
Information Gathered	~160

**VULNERABILITIES BY GROUP**

Group	Count
Cross-Site Scripting	~15
Information Disclosure	~120
Path Disclosure	~10
SQL Injection	~5

**OWASP TOP 10 2021 VULNERABILITIES**

Vulnerability	Count
A01:2021 Broken Access Control	~14
A02:2021 Cryptographic Failures	~18
A03:2021 Injection	~22
A04:2021 Insecure Design	~9
A05:2021 Security Misconfiguration	~45
A06:2021 Vulnerable and Outdated Components	~45
A07:2021 Identification and Authentication Failures	~3
A08:2021 Software and Data Integrity Failures	~1
A09:2021 Security Logging and Monitoring Failures	~1
A10:2021 Server Side Request Forgery (SSRF)	~4

**APPLICATION**

APPLICATION	HIGH	MEDIUM	LOW	SENSITIVE CONTENTS	INFORMATION GATHERED
WEBAPP POSTMAN COLLECTION ENVIRONMENT VARIABLE	10	10	19	0	32
WEBAPP POSTMAN COLLECTION	1	14	7	0	33
WEBAPP SWAGGER 3.0 upload	1	1	1	0	16
WebApp2	14	29	10	0	35
WebApp3	7	13	3	0	18
WEBAPP BURP PROXY COLLECTION	0	9	2	0	24

**Results**

- › Cross-Site Scripting (15)
- › Information Disclosure (119)
- › Path Disclosure (13)
- › SQL Injection (4)

## ヒントとコツ

### 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

The screenshot shows the 'Web Application Report' page. On the left, there's a sidebar with 'APPLICATION REPORTS' (selected) and 'SCORECARD REPORTS'. The main area has a title 'Web Application Report' with a note: 'Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.' It includes 'Targets' (Proxy WEBAPP), 'Filters' (Status: New, Active, Reopened; Remediation: Do not include ignored findings, Include patched findings), and a 'Detection Source' section (Qualys, Burp, Bugcrowd). Below is a 'Summary' table:

High Security Risk	1 Applications	21 Vulnerabilities	0 Sensitive Contents	14 Information Gathered
--------------------	----------------	--------------------	----------------------	-------------------------

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ます、複数のレポートを同時に簡単に操作できます。

This screenshot is identical to the one above, showing the 'Web Application Report' page. The URL in the header bar is 'Web Application Scanning > Reports > Web Application Report'. The interface includes the sidebar, report title, targets, filters, detection source, and summary table.

## 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。

Web Application Report

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

**Targets**

Applications selected: Proxy WEBAPP

**Filters**

Status: New, Active, Reopened

Remediation: Do not include ignored findings, Include patched findings

Detection Source: Qualys, Burp, Bugcrowd

**Summary**

High Security Risk	1 Applications	21 Vulnerabilities	0 Sensitive Contents	14 Information Gathered
--------------------	----------------	--------------------	----------------------	-------------------------

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。

47 Total Reports

**STATUS**

- COMPLETE: 44
- RUNNING: 3

**REPORT TYPE**

- CATALOG REPORT: 4
- DATALIST REPORT: 3
- SCAN REPORT: 5

NAME	FORMAT	TYPE
APISEC record schedule	PDF Document	Web Application Report
tags.name:"A111"	Web Archive (HTML)	Web Application Report
tag 1 2 3	Web Archive (HTML)	Web Application Report
tags.name:"A111"	Web Archive (HTML)	Web Application Report
1.15.0.0 RC1 Create	Web Archive (HTML)	Web Application Report

### デフォルトのレポート形式を設定する

時間と効率を節約できます！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。

### Appendix

- ▶ Web Application Details
- ▼ Severity Levels
  - ▼ Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

Severity	Level	Description
<span style="color: #ccc;">■</span> <span style="color: #ccc;">□</span> <span style="color: #ccc;">□</span> <span style="color: #ccc;">□</span> <span style="color: #ccc;">□</span>	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find. Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.
<span style="color: #cc0000;">■</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span>	Medium	Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.
<span style="color: #cc0000;">■</span> <span style="color: #cc0000;">■</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span>	Serious	Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.
<span style="color: #cc0000;">■</span> <span style="color: #cc0000;">■</span> <span style="color: #cc0000;">■</span> <span style="color: #cc0000;">□</span> <span style="color: #cc0000;">□</span>	Critical	Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.
<span style="color: #cc0000;">■</span>	Urgent	
  - ▶ Sensitive Contents
  - ▶ Information Gathered

## 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。

Name	Owner	Type	Last Updated	Last Run Date	Number of Runs	Tags
Web Application Report	System	Web Application Report	30/01/2023	30/01/2023	6781	-
Scorecard report(Default)	System	Scorecard Report	30/01/2023	30/01/2023	621	-
Catalog report(Default)	System	Catalog Report	30/01/2023	30/01/2023	575	-
Scan Report(Default)	System	Scan report	30/01/2023	30/01/2023	2171	-
Template Exclude Individual Results		Web Application Report	29/01/2023	29/01/2023	248	-
		Web Application Report	24/01/2023	-	-	-

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

← Create New Report Schedule

STEPS 1/5

1 Basic Information

2 Target

3 Scheduling

4 Notification

5 Review And Confirm

Basic Information

Select a report type and format.

Name \*

 106 characters remaining

Choose a Focus

The report type you select defines the set of data (records, fields) available for the report. For the report template, select the default or a user-defined one.

Report Type \*

 Report Template \*

Report Format \*

ⓘ Report Format - Encrypted PDF is recommended for security reasons.



Tags

Select tags to apply to the schedule report.

Create Tag



Cancel

Next

### 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。

← Create New Report Schedule ⑦

STEPS 4/5

1 Basic Information  
2 Target  
3 Scheduling  
**4 Notification**  
5 Review And Confirm

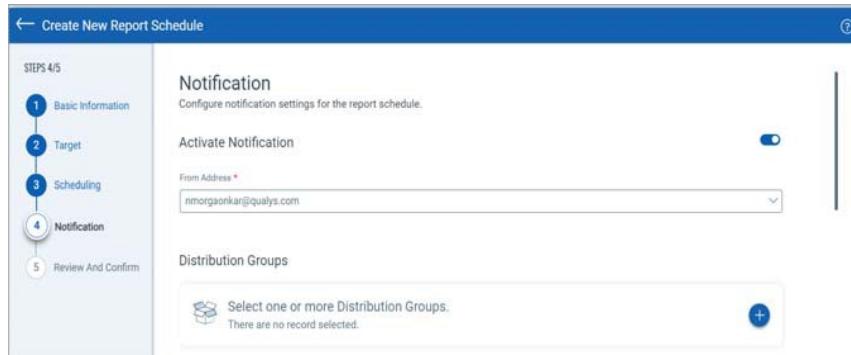
**Notification**  
Configure notification settings for the report schedule.

Activate Notification

From Address \*

Distribution Groups

Select one or more Distribution Groups.  
There are no record selected. +



## 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。

Username	Modules	First Name	Last Name	Email Address	Last Update Date	Last Login Date
quays_ak1 Unassigned Business Unit	ADMIN AM CA VM CM TP PC SAQ WAS WAF MD	Alex	Kim	eschamp@qualys....	15 Jul 2017	15 Jul 2017
quays_ch Unassigned Business Unit	AM CA VM CM TP	Christina	Hans	eschamp@qualys....	15 Jul 2017	-

新規ユーザーを編集します（ユーザーを選択し、クリ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スキャナ用の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、クリ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。

The screenshot shows the 'Role Management' tab selected in the navigation bar. A list of roles is displayed in a table with columns: Name, Description, and Modules. A context menu is open over the 'WAS SCANNER' row, listing actions: View, Edit, Add To Users, Remove From Users, Add Permissions, Remove Permissions, and Delete. The 'WAS SCANNER' row also has a 'Scanner User' note.

Name	Description	Modules
WAS USER	WAS User	WAS
<input checked="" type="checkbox"/> WAS SCANNER		WAS
WAS MANAGER		WAS
WAF Manager		
UNIT MANAGER		ADMIN AM
SCANNER	Scanner User	AM

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。

The screenshot shows the 'Role Management' tab selected. At the top, there's a summary: 'Total used roles' (9%) with breakdowns for Total (11), Used (1), and Not Used (10). Below this, a red arrow points from the text 'Click here to create a new custom role' to the 'New Role' button, which is highlighted with a red circle. The table below shows the 'WAS USER' role.

Name	Description	Modules
WAS USER	WAS User	WAS

たとえば「WASスキャナー」ロールを作成できます。

**Role Creation**

Step 1 of 3

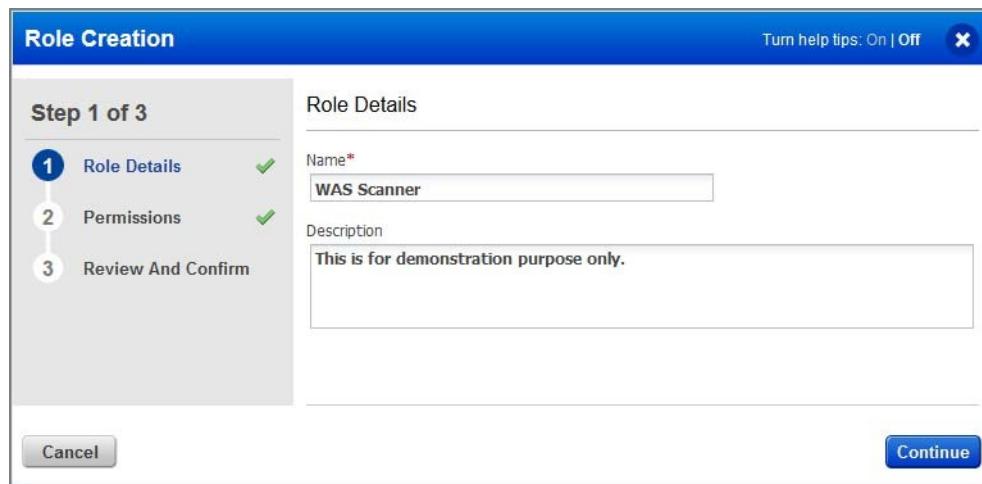
1 Role Details ✓  
2 Permissions ✓  
3 Review And Confirm

Role Details

Name\* WAS Scanner

Description This is for demonstration purpose only.

Cancel Continue



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。

**Role Creation**

Step 2 of 3

1 Role Details ✓  
2 Permissions ✓  
3 Review And Confirm

Edit permissions for this role

Select how users would access this application

UI Access  API Access

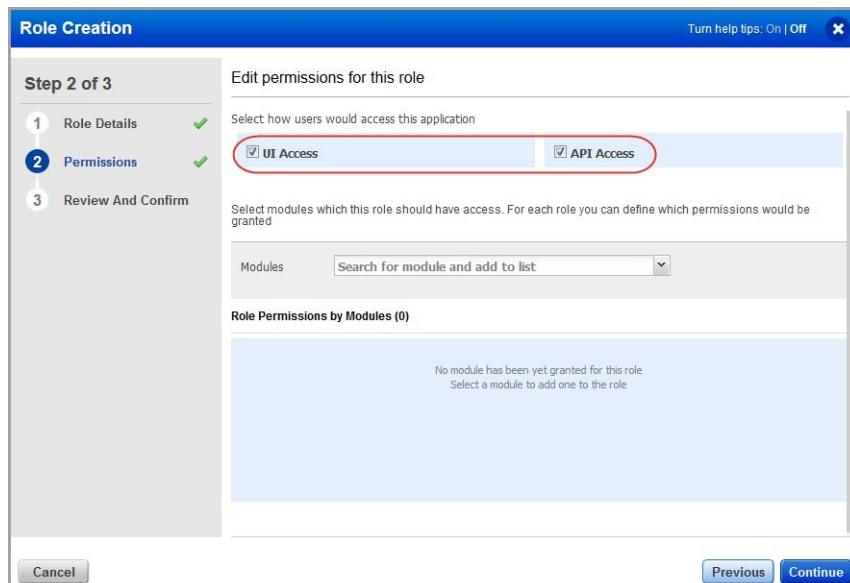
Select modules which this role should have access. For each role you can define which permissions would be granted

Modules Search for module and add to list

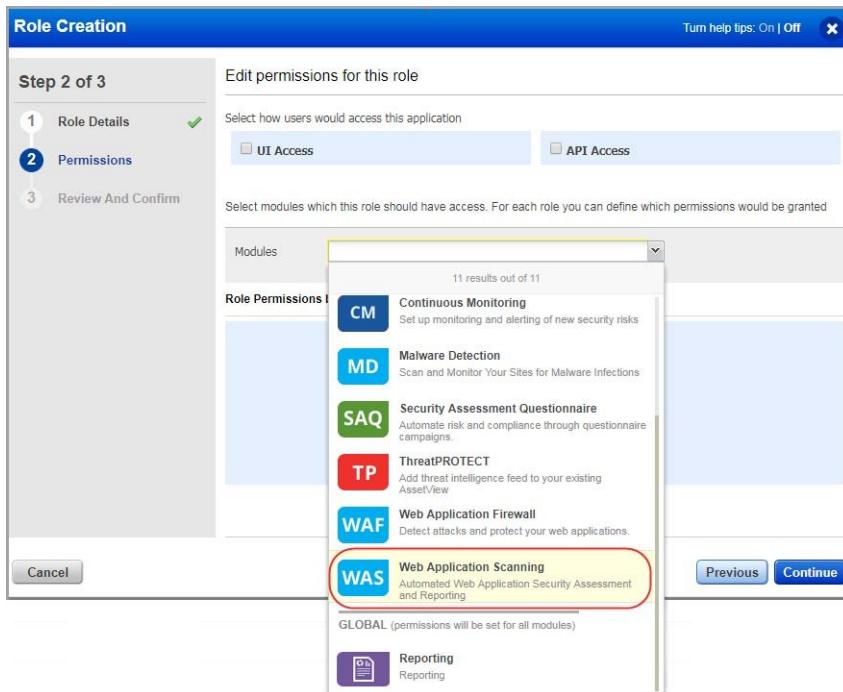
Role Permissions by Modules (0)

No module has been yet granted for this role  
Select a module to add one to the role

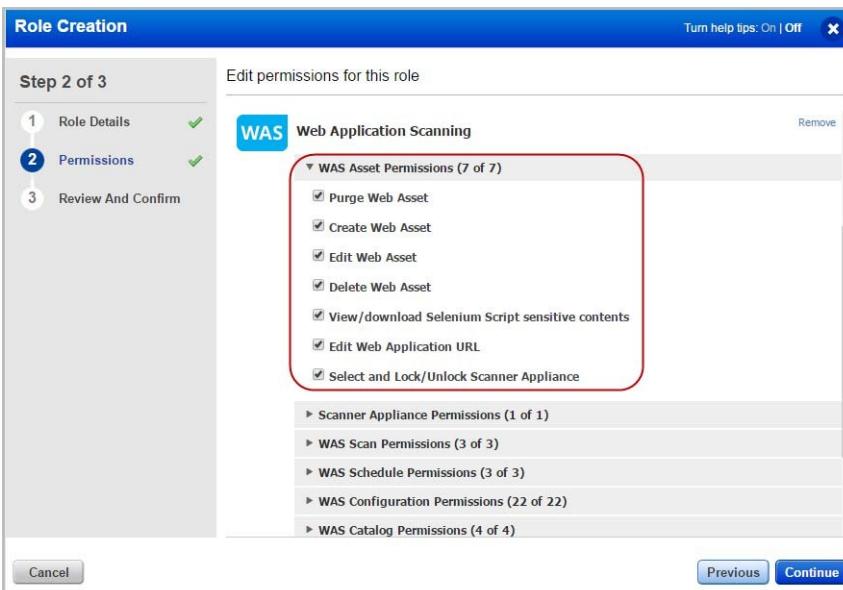
Cancel Previous Continue



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。

Username	Modules	First Name	Last Name	Email Address	Last Update Date	Last Login Date
quays_ak1 [Unassigned Business Unit]	ADMIN AM CA VM CM TP PC SAQ WAS WAF MD	Alex	Kim	eschamp@qualys....	15 Jul 2017	15 Jul 2017
quays_ch [Unassigned Business Unit]	AM CA VM CM TP	Christina	Hans	eschamp@qualys....	15 Jul 2017	-

- 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。

User Edit: Christina Hans (quays\_ch)

Edit Mode

User Details >

Profile Settings >

**Roles And Scopes** > **Assigned roles** Remove all

Action Log >

Account Activity >

Edit role(s) and scope

Allow user full permissions and scope (The user will have full access to everything)  
Each role grants you a set of permissions that will apply to the objects you have access to.

New role Search unassigned roles

Assigned roles	Remove	Unassigned roles	Add all
SCANNER	Remove	UNIT MANAGER	Add
		WAF Manager	Add
		WAS MANAGER	Add
		WAS SCANNER	Add
		WAS USER	Add

Edit Scope

Allow user view access to all objects (Other permissions are granted by the user's roles)  
Define what assets the user can access by tags.  
Global Scope Select | Create | Remove All

Unassigned Business... X

Cancel Save

サブクリプション内の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/>をご覧いただけます。

### 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。