Introduction

The purpose of this document is to serve as a guide for information security teams who wish to roll out web application scanning capability to development teams at their organization.

Qualys Web Application Scanning (WAS), can be used at any stage of the software development lifecycle (SDLC) to identify vulnerabilities and weaknesses in web applications. The only requirement is to have a running instance of the application. Application scans historically have been performed by information security personnel just prior to the web application moving to production.

However, identifying and fixing application vulnerabilities earlier in the SDLC (known as "moving left") has many benefits. Vulnerabilities can be addressed quickly by developers prior to the application code being promoted from the development stage. Once code is promoted, the cost of addressing security issues goes up significantly because of the different teams and number of people who need to get involved. Communication (or miscommunication) between parties represents a source of inefficiency and can cause the entire release process to slow down.

About the Self-Service Model

With a self-service model, application scanning responsibilities are given to the individual development teams who are building the applications. The information security team then focuses on administering the overall program, including oversight, training, metrics, and day-to-day or routine tasks.

A self-service model is desirable not only for reasons of cost, but also because information security teams are often understaffed and overloaded with work. The security team may simply not have enough resources to provide coverage for all the applications that need to be tested.

When development teams are engaged in a self-service model, they take ownership of application security scanning. Scans are done earlier in the development process and issues can be remediated quickly as they are identified. A greater number of applications can be tested because scanning responsibilities are distributed. Another key benefit is that fewer vulnerabilities exist in later stages of the SDLC, such as QA, UAT, staging, and production.

Prerequisites

To establish a self-service model, there are a number of prerequisites.

Authority

The information security team needs to have the authority to roll out a scanning program to development teams at the company. Without this, the initiative is destined to fail because development teams are not likely to perform the scanning. The authority may come from the CIO or other high-ranking executive at the company.
Support from Development Leadership

Developers will naturally push back or grumble about being given the responsibility to perform application scans. Therefore the software development leadership at the company (VPs of Development, Development Managers, Team Leads, etc.) needs to be aware of the scanning initiative and be supportive of it. The development organization as a whole must understand what is expected of them and also that the information security team has the authority to administer and oversee the scanning program.

Application Inventory

An inventory of in-scope web applications needs to be available. The more complete and detailed the inventory, the more successful the self-service scanning model will be. The inventory needs to be accurate and updated as changes occur.

The inventory, at a minimum, should include:

- Application name
- Description / purpose
- Business criticality rating
- Responsible business unit, group, and/or team
- Name of owner or point of contact
- URL for scanning, along with environment description

Training/Education Material

The security team needs to create a place for development teams to go, such as an Intranet site, that provides guidance, training, and other useful material around what they are expected to do. Most developers have never used a security testing tool like Qualys WAS before. They will need to be given step-by-step instructions on how to log in, configure authentication, perform scans, view results, etc.

A person on the security team should be designated and promoted as the point of contact for all questions. Consider creating a dedicated email address (e.g., WAS@company.com) where developers can send requests and ask questions.

Preparation

To prepare for a self-service scanning model, several setup tasks are required to be done up front. These tasks are typically carried out by the information security team.

Roles Setup

A role within WAS is a collection of permissions. Tags on the other hand determine what is visible to users once they log in.

Qualys recommends creating a very precise, customized role tailored for members of development teams. There are certain capabilities that only the information security team should
have. For example, it doesn't make sense for developers to have the ability to create web applications in WAS. The web application list would eventually become a haphazard mess or WAS licenses consumed quickly. Likewise, developers should not be able to mark findings as "ignore", edit option profiles to exclude certain tests, or edit the severity of findings.

Qualys recommends creating a new role called "Development Team" with permissions assigned according to the table below.
Table 1 – Recommended permissions for "Development Team" role

<table>
<thead>
<tr>
<th>Qualys Module</th>
<th>Group</th>
<th>Recommended Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS</td>
<td>Access method</td>
<td>UI Access</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Burp Permissions</td>
<td>--- none ---</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Bugcrowd Permissions</td>
<td>--- none ---</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Configuration Permissions</td>
<td>Create DNS Override</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit DNS Override</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete DNS Override</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Remediation Permissions</td>
<td>Retest vulnerabilities and sensitive content</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Catalog Permissions</td>
<td>--- none ---</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Asset Permissions</td>
<td>Edit Web Asset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View/download Selenium sensitive contents</td>
</tr>
<tr>
<td>WAS</td>
<td>Scanner Appliance Permissions</td>
<td>--- none ---</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Scan Permissions</td>
<td>Launch WAS Scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cancel WAS Scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete WAS Scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Create WAS Schedule</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Schedule Permissions</td>
<td>Edit WAS Schedule</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete WAS Schedule</td>
</tr>
<tr>
<td>WAS</td>
<td>WAS Authentication Record</td>
<td>Create Authentication Record</td>
</tr>
<tr>
<td></td>
<td>Permissions</td>
<td>Update Authentication Record</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete Authentication Record</td>
</tr>
<tr>
<td>Reporting</td>
<td>Reporting Permissions</td>
<td>Create Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete Report</td>
</tr>
</tbody>
</table>

Note: Do not give developers pre-defined roles like WAS USER, WAS SCANNER, and WAS MANAGER. They were not designed for a self-service model.
Once complete, the Development Team role will look like this:

![Role Edit: Development Team](image)

You may want users with certain titles to have additional permissions. For example, let's say you want a Software Security Architect to have the "Ignore findings" permission. Simply create a new role with only that specific permission and assign it to the user in addition to the "Development Team" role.

**Tags Setup**

Tags are used to categorize objects and must be used to assure that users have the proper scope (visibility) once logged into WAS. Tags need to be created in a logical manner.

You will want to refer to your application inventory, and probably your company's organizational chart, when setting up the tags.
The tagging editor within the Qualys platform is located under the AssetView module as shown below. The tagging feature is shared functionality and used by all Qualys products.

![AssetView module](image)

First create a tag called "Everyone" (or similar). This tag will be assigned to all objects and users in WAS that need to have global visibility.

Tags can be nested. A parent tag can have any number of child tags. You may want to structure tags similar to your company's org chart.

Below is an example where tags were created for three business units (BU-1, BU-2, and BU-3). The BU-1 tag has been expanded to show that it has three child tags, one for each group in that business unit.

One of the tags ("ABC Group") has three child tags representing three different development teams in that group – Mercury, Pluto, and Saturn.
Web Applications Setup

The information security team, as the administrator of the scanning program, is responsible for managing the list of web applications within WAS. The infosec team creates, deletes, or purges web applications as needed. The application inventory (a prerequisite for a self-service model) can be used as the basis for creating web applications in a prioritized manner.

Categorize web applications logically using tags. This is needed because development teams should only be able to run scans and view results for web apps they are responsible for. Tags assure that users having the proper scope/visibility once they've logged in.

Below is a web application called "DVWA", which has been assigned to the "Saturn Team" as well as "ABC Group" and "BU-1".

Besides web applications, users, authentication records, and scanner appliances should be tagged appropriately as well.

Some objects, such as option profiles, should be assigned the "Everyone" tag because global visibility is permissible.
User Setup

As a Qualys WAS customer, you can create an unlimited number of users. Creating accounts for developers may be a somewhat tedious task at first. Each user needs to set up with the appropriate role(s) and scope.

Note: This document assumes that SAML/SSO or integration with Windows AD groups have not been implemented as part of your Qualys subscription.

To create a new user in Qualys, open the VM module and select Users. Click the "New" button and select "User…".

You need to know the name, title, phone number, and email addresses of the user. The email address is especially critical to get right, because that’s where the email with initial login instructions for the user will be sent.

Assuming the user should have access to WAS alone and no other modules in the Qualys platform, then configure the user as a "WAS-only" user as explained here: https://community.qualys.com/docs/DOC-4572.

Prior to creating a Qualys account for a developer, you need to know the development team they are on and which tag(s) they should be assigned. You should already have created the tags as described earlier.

Once the user has been created under the VM module, you must edit them under the Administration module, which is the last item in the main dropdown menu:
Find the user and select "Edit". Open the "Roles and Scopes" panel.

Uncheck "Allow user full permissions and scope".

Assign the "Development Team" role to the user:

At the bottom of Roles and Scope, uncheck "Allow user view access to all objects". This is where you assign the appropriate tag(s) to set the scope of what this user will see when they log in. Be sure to assign the "Everyone" tag to every user.

Note: These tags are for setting the user's scope. Users themselves can have tags, which are set on the User Details panel, but aren't important for this discussion.

See example below, where the user's scope has been set to "Saturn Team" and "Everyone".

Upon login, this user sees only the "DVWA" web application, because that is the only one tagged with "Saturn Team".
It's probably not necessary for all developers on a team to have access to WAS. You may want to have each team decide for themselves who will be responsible for running scans. Then you can proceed to set up that person with a Qualys account.

You need to have an audit process so that people who leave the company are deactivated in Qualys. Remember Qualys is a SaaS product, so it can be accessed from anywhere.

**Option Profile Setup**

A variety of different option profiles should be pre-defined for developers. That way, they can just select one. Developers will not be editing option profiles in a self-service model.

Recommended option profiles include:

- **Authentication Test Only** (maximum 50 links in scope, lowest intensity, ignore binaries, SmartScan, no brute force)
- **Standard-lowest** (complete detection, max 1000 links, lowest intensity, ignore binaries, SmartScan, no brute force)
- **Standard-low** (complete detection, max 4000 links, low intensity, ignore binaries, SmartScan, no brute force)
- **Standard-medium** (complete detection, max 8000 links, medium intensity, ignore binaries, SmartScan, no brute force)
- **Standard-high** (complete detection, max 8000 links, high intensity, ignore binaries, SmartScan, no brute force)
- Specialty profiles, as desired:
  - CCN and SSN searches, plus any custom content search desired
  - Very high or disabled error/timeout thresholds
  - Brute force testing only
  - Severity 4 & 5 QIDs only
  - XSS tests only
Make sure to assign the "Everyone" tag to all option profiles so that all users can view and select the option profiles.

Note that all users can view the default option profile for your Qualys subscription, regardless of tags.

**Miscellaneous Setup**

Under Configuration—Appliances, assign the "Everyone" tag to all scanner appliances in your environment. Otherwise, users will not be able to launch scans using the scanners.

Under Configuration—Global Settings, Qualys recommends using the following regular expression, which will black-list images and font files.

```
^.*\.(jpg|jpeg|png|gif|ico|ttf|otf|woff|woff2).*$
```

These types of static files can be safely excluded from vulnerability testing.
Testing the Setup

After preparations have been completed, you should test your setup by creating a test user in Qualys. Use any valid email address (Gmail, Yahoo, etc.) to create an account and simulate a developer who is logging in to run a scan.

Create a test web application with appropriate tags. With this test account, put yourself in the developer's shoes. Confirm that permissions are correct and the visibility aligns with what is expected. The test user should see only those objects that have the same tag as the tags in the user's scope.

Verify that the user can launch a scan on the test web application and can view the results.

Pilot Phase

Conduct a pilot program before rolling out the self-service model to all teams. Identify one or two development teams who are willing to be the "guinea pig".

The pilot phase will be crucial to helping you identify and address any problems or difficulties.

Concurrent with the pilot and based on the questions or issues that arise, create relevant training material. Examples are an Intranet site or portal for the program, product training documents, a dedicated email address, authentication tips & tricks, etc.

It is important to have the training material ready prior to the broad, company-wide rollout.

Overseeing the Program

The information security team needs to oversee the program and server as a communications link. Ensure that development teams are running scans and things are working smoothly.

Verify that authentication is being used, if required as part of your program.

Prior to full rollout, or during the rollout, conduct a security "roadshow" for development teams. The roadshow is a series of onsite meetings (in-person) to introduce the program and to help dev teams understand the reasons behind it. Demonstrate Qualys WAS. Provide a walk-through of running a scan and viewing results.

Define the responsibilities/roles of the development teams and the information security team.

Inactivate developers within the Qualys platform if they leave the company.

Field questions from development teams as they arise.