Web Application Scanning Subscription Setup Request



Copyright

Copyright 2007-2019. Secureworks®, Inc. All Rights Reserved.

This publication contains information that is confidential and proprietary to Secureworks and is subject to your confidentiality obligations set forth in your contract with Secureworks or affiliates thereof. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please report any errors to Secureworks in writing. Secureworks does not warrant that this publication or related hardware or software is error-free. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks and iSensor are registered trademarks of Secureworks. All other trademarks are the property of the respective owners.

# Table of Contents

[Table of Contents 3](#_Toc525643114)

[Web Application Basic Information 4](#_Toc525643115)

[Definition 4](#_Toc525643116)

[Target Definition 4](#_Toc525643117)

[Business Information 4](#_Toc525643118)

[Comments 4](#_Toc525643119)

[Web Application Details 5](#_Toc525643120)

[Target Scope 5](#_Toc525643121)

[Scan Settings 6](#_Toc525643122)

[Default Configuration 6](#_Toc525643123)

[Crawling Hints 6](#_Toc525643124)

[Authentication 7](#_Toc525643125)

[Authentication Record Definition 7](#_Toc525643126)

[Comments 7](#_Toc525643127)

[Form Records 7](#_Toc525643128)

[Standard Form Based Authentication 7](#_Toc525643129)

[Custom Form Based Authentication 7](#_Toc525643130)

[Custom Configuration 8](#_Toc525643131)

[Fields 8](#_Toc525643132)

[Masked Fields 8](#_Toc525643133)

[Server Authentication 9](#_Toc525643134)

[Basic Authentication Record 9](#_Toc525643135)

[Digest Authentication Record 9](#_Toc525643136)

[NTLM Authentication Record 9](#_Toc525643137)

[Black and White List 10](#_Toc525643138)

# Web Application Basic Information

Thank you for selecting SecureWorks Managed Security Services. This Service Activation Questionnaire is a tool used by SecureWorks to collect information for new Web Application Scanning subscription requests.

## Definition - Required

Please enter the information about the web site which you would like to scan for WAS scanning.

|  |  |
| --- | --- |
| Name: |  |

## Target Definition - Required

|  |  |
| --- | --- |
| Web Application URL |  |

## Business Information - Optional

Provide business information that will help you categorize your web application among your subscription.

|  |  |
| --- | --- |
| Business Function: |  |
| Business Location: |  |
| Business Description: |  |

## Comments

(Additional notes concerning your Web Application. 2048 characters maximum)

# Web Application Details

## Target Scope - Required

Controls how the scanner crawls and scans target web application. Select one of the scope value options below:

1. **Limit at or below URL Hostname:** Scope will be limited to the hostname within the URL, using HTTP or HTTPS and any port.
2. **Limit to content located at or below URL subdirectory:** Scope will be limited to all links starting with a URL subdirectory using HTTP or HTTPS and any port.
3. **Limit to URL hostname and specified sub-domain:** Scope will be limited to only the URL hostname and one specified sub-domain, using HTTP or HTTPS and any port.
4. **Limit to URL hostname and specified domains:** Scope will be limited to only the URL hostname and specified domains, using HTTP or HTTPS and any port.

|  |  |
| --- | --- |
| **Scope** |  |
| **Domain(s)** |  |

# Scan Settings

## Default Configuration - Required

|  |  |
| --- | --- |
| **Options Profile** | Initial WAS Options [Default Configuration] |
| **Scanner Appliance** | External |

**Option profiles provide the settings for web application scans – crawling, sensitive content detection, vulnerability detection and password brute forcing. When launching or scheduling a scan, you'll need to choose an option profile. If you don't have a WAS option profile in your account, we've provided one called "Initial WAS Options" with the recommended settings for web application scanning.**

## Crawling Hints - Required

If defined for your web application, Robots.txt/Sitemap.xml file contains links that may be included in your scan.

|  |  |
| --- | --- |
| **Use robots.txt \*** | **Yes  No** |
| **Use Sitemap.xml \*\*** | **Yes  No** |

**\* Robots.txt is a convention to prevent cooperating web spiders and other web robots from accessing all or part of a web site that is otherwise publicly viewable.**

**\*\* Sitemap.xml is an XML file that lists URLs for a site to inform search engines about URLs that are available for crawling.**

# Authentication – Optional

When entering authentication data below, populate either Standard OR Custom. **Do not populate both sections**.

Note: To maintain security please contact your Project Manager so you can provide the password over the phone.

## Authentication Record Definition

|  |  |
| --- | --- |
| Name |  |

## Comments

## Form Records

Enter the details for the login form. One of the easiest ways to find the form values is to view the source code and search for "<FORM”

There may be several forms on the page. Be sure to copy details from the form that contains the login fields.

## Standard Form Based Authentication

|  |  |
| --- | --- |
| Username |  |
| Password |  |
| Send authentication on SSL only (YES/NO) | **Yes**  **No** |

**Standard username and password Authentication record**

## Custom Form Based Authentication

|  |  |
| --- | --- |
| Form Action: |  |
| Send authentication on SSL only (YES/NO) | **Yes  No** |

**Allows you to enter other fields (example customerID0 apart from standard login credentials**

## Custom Configuration - Optional

Enter the login fields below. Login fields will commonly be User Name or Login and Password. There may be more fields and even hidden fields that do not show on the screen. If the form has fields that change depending on what you select we suggest you fill out the form entirely and then look at the source code of the page. See the Help for examples of form fields.

## Fields

|  |  |
| --- | --- |
| Name | Value |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Masked Fields

|  |  |
| --- | --- |
| Name | Value |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## When entering authentication data below, populate either Server, Basic OR Digest. Do not populate all three sections

## Server Authentication – Optional

**Server authentication is handled within the HTTP headers**

|  |  |
| --- | --- |
| Send authentication on SSL only (YES/NO) | **Yes  No** |

**Specify if credentials shall be sent only on secure connections**

## Basic Authentication Record - Optional

|  |  |
| --- | --- |
| Username |  |
| Password |  |
| Realm |  |

**The realm is the name associated with the protected area of the web application. It corresponds to the AuthName setting in a .htaccess file for Apache servers and to the Realm value set for IIS servers**

## Digest Authentication Record – Optional

|  |  |
| --- | --- |
| Username |  |
| Password |  |
| Realm |  |

## NTLM Authentication Record – Optional

|  |  |
| --- | --- |
| Username |  |
| Password |  |

# Black and White List – Optional

Set up a black list to prevent those URLs or their sub-directories from being scanned.

Any link that matches a black list entry will not be scanned unless it also matches a white list entry.

|  |  |
| --- | --- |
| Blacklist URL(s) |  |
| Whitelist URL(s) |  |

**Black/Whit**