

Vulnerability Scan Service

User Guide

lssue 03 Date 2019-07-12



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

Website: <u>http://e.huawei.com</u>

Contents

1 Enabling VSS	1
1.1 Functions and Specifications of Different VSS Versions	1
1.2 Buying VSS	2
2 One-Click Scan	5
3 One-Click Risk Identification	8
4 Asset List	11
4.1 Viewing the Asset List	11
4.2 Adding a Domain Name	12
4.3 Authenticating a Domain Name	13
5 Job List	
5.1 Creating a Scan Job	17
5.2 Viewing Scan Details	21
6 Overview	
6.1 Taking an Overview	
6.2 Vulnerability List	
6.2.1 Viewing the Vulnerability List	
6.2.2 Viewing Details of a Vulnerability	
6.2.3 Marking Vulnerabilities as Ignored	
A Change History	33

1 Enabling VSS

1.1 Functions and Specifications of Different VSS Versions

VSS provides the basic edition and professional edition. The basic edition is free of charge, but it provides a limited set of functions and specifications. The profession edition is available on a pay-per-use basis. For details, see **Table 1-1**.

Edition	Charging Mode	Function	Specifications
Basic	Free	 Vulnerability detection Re-scanning Scheduled scanning Port scanning Customization of login methods Scanning of Web 2.0 crawlers 	 Number of domain names: 5 Number of scans per day: 5 Duration of a single job: 2 hours Job priority: low

Edition	Charging Mode	Function	Specifications
Professio nal	Pay-per- use	 Vulnerability detection Re-scanning Scheduled scanning Port scanning Customization of login methods Scanning of Web 2.0 crawlers Short message notification (SMN) upon job completion Query of vulnerability fixing suggestions Download of scanning reports Weak password scan 	 Number of domain names: purchase-per-use Number of scans per domain per month: 60 Duration of a single job: unlimited Job priority: high

1.2 Buying VSS

This section describes how to buy the VSS professional edition. If you are a new user, perform the pre-scan first. For details, see section "One-Click Scan" in the *Vulnerability Scan Service User Guide*.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Asset List.
- Step 3 In the upper right corner, click Purchase VSS Professional.

Alternatively, choose **Security** > **Vulnerability Scan Service** > **Dashboard**. On the **Dashboard** page that is displayed, click **Purchase VSS Professional**.

Step 4 On the Specify Details page, configure the parameters based on Table 1-2.

Figure 1-1 Edition selection (basic edition)

Vulnerability Scan S	ervice		
Specify	Details	Confirm Order	Pay 3
Specifications * Select Specifications: * Specification Details:	Basic(For free) Professional Detects common vulnerabilities such as OWASP sllows you to customize scanning strength and cr cans logins and offers various login mode option supports scheduled scans to avoid service peaks scans high-risk ports to enhance server security. ynamically adjusts scanning loads to ensure ser	and WASC vulnerabilities. rawler scanning settings. ns. 5. rvice availability.	
Notice	he basic edition provides 5 scans a day, each la our website is large.	isting a maximum of 2 hours. You can use it to	scan small websites. The professional edition is recommended if
* Domain Name/IP Address	http:// • Enter an IP address or	a domain name.	
Price: For free			Try Now

Figure 1-2 Edition selection (professional edition)

Specify Details		2 Confirm Order		3 P
Specifications				
* Select Specifications	Basic(For free) Professional			
* Specification Details	Contains all functions of the basic edition.			
	Detects weak passwords so you can know your server weakn	iess sooner.		
	Notifies by SMS messages immediately when a scan is finisi Provides professional scan reports for you to download	led.		
	Offers detailed recommendations for fixing vulnerabilities.			
	Does not limit the duration of a scan job.			
	Allows up to 60 scans for a domain per month.			
	month			
10 10 10 10 10 10 10 10 10 10 10 10 10 1				
* Usage Duration	I month 2 months 2 months 4 months 5 months	6 months 7 months 9 mont	he 0 months 1 year	
		o montria o montria	Discount (
* Domain Names	1			
Configuration @				
2				
* Domain Name/IP Addr	ess http:// - Enter an IP address or a domain na	ame. 💿		
Price				_

Table 1-2 Parameter description

Parameter	Description
Select Specification s	Currently, only the professional edition needs to be purchased. The basic edition can be used for free.

Parameter	Description
Usage Duration	One month to one year can be set.
Domain Names	Specifies the number of configured domain names or IP addresses.
Domain Name/IP Address	 Specifies the domain name configured for vulnerability scan. Click () to add multiple domain names. Only one domain name can be configured at a time for the basic edition. Up to 10 domain names can be configured for the professional edition.

Step 5 In the lower right corner of the page, click Next.

ΠΝΟΤΕ

For any doubt about the pricing, click **Price Details**.

Step 6 Confirm your order and read the *Vulnerability Scan Service Disclaimer*. If you agree with the disclaimer, select I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer and click Submit.

If the order is incorrect, click **Previous** to go back to the last step and modify your order.

Figure 1-3 Confirming an order

Specify Details		2 Con	firm Order				
Order Details:							
Product Name	Configuration	Billing Mode	Usage Duration	Domain Names	Preference	Subtotal	
Vulnerability Scan Service	Professional	Yearly/monthly	1 month	î	0	38	
					d and agree to the	HUAWELCLOUD Vols	
Price				M Thave leave	a and agree to the	Soon Service Die	ali



----End

2 One-Click Scan

This section guides new users to experience VSS for free.

Procedure

Step 1 Enter an IP address or a domain name to be scanned, and click Start Scan.

Figure 2-1 New user experience page

Up to not	v, we have detected 15,659 vulnerabilities for 350 websites.
http://	Enter an IP address or a domain name. Start Scan
Criti	cal [2018.04.13] CVE-2018-1273 Spring Data Commons One Click Detection

Step 2 View the scan progress.

Figure 2-2 Scanning

Up t	Conow, we have detected 15,65 http:// • www.mate.com Ortical [2018.04.13] CVE-2018-1273 Spring Data C Critical [2017.12.22] CVE-2017-10271 WebLogic XI Critical [2017.09.05] CVE-2017-10271 WebLogic XI	59 vulnerabilities for 350 websi Start San ommons MLDecoder (\$2-052) One-Click Detection One-Click Detection	try VSS for Free
	Scanning http://www beam com; Started On: 04/23/20	18 10:55:21 GMT+08:00; Estimated Duration: 3 minutes	
		B	
Intelligent Scan	Wide Coverage	High Efficiency	Ease of Use
Dynamically adjusts scan frequency to prevent websites interruption due to scanning traffic surges; prevents dirty data from being written into databases.	Supports real-time update of 10000+ types of vulnerability information in the rule library; scans urgent vulnerabilities, ports, and weak passwords.	Supports quick scan through multi-engine collaboration, leverages fingerprint identification, and accurately adopts scan rules, meaning higher scan efficiency.	Adopts simple settings, requires no component installation, has zero maintenance costs, and supports one-click enabling and SM notification upon completion of a scan job.

Step 3 After the scan is complete, click Try VSS for Free in the upper right corner of the page. On the displayed Asset List page, complete domain name authentication. Alternatively, click Perform Real-Name Authentication at the bottom of the page to perform domain name authentication.

Figure 2-3 Scan details

	Up t	o now,	we have detected 15,659 vulnerabil	ities for 350 websites.		
	· · · ·					
		http://	www .com Start Scan			
		Critica	al [2018.04.13] CVE-2018-1273 Spring Data Commons			
		Critica	[2017.12.22] CVE-2017-10271 WebLogic XMLDecoder One-Click Detection			
		Critica	1 [2017.09.05] CVE-2017-9805 Struts2 RES1 (S2-052) One Click Detection			
http://www.	com					
Website Score 92 scores	Website Security Level: <u>Average</u> 04/23/2018 10:46:27 GMT+08:00 Started,Du The trial mode will implement 3-minute prelin enjoy more thorough scan of VSS.	ration: 00:00 minary scan	246, Detection Mode: Trial for your website. However, you have not performed real-name authentic performance.	ation. First perform real-name authentication , as required by Chinese laws and regulations, to		
	Туре		Item	Result		
	Malicious Content-		Malicious Links	Safety		
	maileidus content,		Miner Backdoors	Safety		
	Detertici Dich		WebSite Headers	Low Risk		
			Https Protocol	Middle Risk View details		
			Server Intrusion	Safety Finished View details		
			Leakage of User data	Safety Finished View details		
			Website infomation Expose	Safety Finished View details		
			Malicious Commands Execute	Safety Finished View details		
	Website Sec Vulns		Trojan Implant	Safety Finished View details		
			DataBase Leakage	Safety Finished View details		
			Unlawfully changing data	Safety Finished View details		
			Website Blocking	Safety Finished View details		
			Others	Safety Finished View details		
			Perform Real-Name Authentication			

Table 2-1 Scan results

Area	Description	Operation
Туре	The scan results are displayed by type.	N/A

Area	Description	Operation
Item	Items to be scanned, which are scan subtypes	N/A
Result	Scan results	 If your website is safe, the result is displayed as Safety. If there is a risk, the corresponding risk level is displayed. Click View details to view details. Low Risk View details
		displays the sample risk level.

----End

3 One-Click Risk Identification

This section guides new users to detect the latest critical vulnerabilities for free.

Old users can use this function by choosing **Security** > **Vulnerability Scan Service** > **Dashboard** and clicking **One-Click Detection** in the **What's New** area.

Procedure

Step 1 Click One-Click Detection to go to the Rapid Detection of Critical Vulnerabilities page.

Figure 3-1 One-click risk identification

U	p to now,	we	have de
	http://	•	Enter an IP a
	Critical	[20]	18.04.13] CVE-
	Critical	[20	17.12.22] CVE-
	Critical	[20	17.09.05] CVE-





 Table 3-1 Detection results

Area	Description
Vulnerability Details	Details about the current critical vulnerability
Affected Versions	Affected versions
Severity	Vulnerability severity
Advice	Recommended actions

- Step 2 Enter your domain name or IP address and click Detect Now.
- **Step 3** Click **Perform Real-Name Authentication** at the bottom of the page to complete domain name authentication (For details, see **Authenticating a Domain Name**) if there is a risk, and then get a deep scan.

Figure 3-3 Vulnerability detection results

Rapid Detection of Critical Vulnerabilities Back to the Homepage

Risk Level	Website Address	http://www
Safetv	Website Info	IP address: unk
	Notice	The latest CVE
		for its security.

	Critical [20
Vulnerability ID	CVE-2018-1273
Vulnerability Details	Presid Spring Bill Market Action.
	PERMITSION - R
	Gentles, J.M. 2007, Borge001
	STREET, MARKET
Affected Versions	Spring Data Commons 1.13 – 1.13
	SR5);Spring Data REST 3.0 – 3.0.5
Severity	High
Advice	Spring Data Commons

----End

4 Asset List

4.1 Viewing the Asset List

This section describes how to view the asset list.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Choose Security > Vulnerability Scan Service > Asset List.

- In the row containing the desired domain name, click **More** in the **Operation** column to edit, scan, or delete a domain name.
- For the professional edition, only an expired domain name can be deleted.

Figure 4-1 Asset list

http://hellokitty.cn hellokitty Package Version: Basic Expiration Time: 03/26/2019 23:59:59	(Not authenticated)	100 scores Time 03/26/2018 22:13:57 High risk 0 , Medium risk 0 , Low risk 0 , Information 0	Authenticate	More 🗸
http://10.93.194.177:8067 Package Version: Professional Expiration Time: 03/25/2018 23:59:59 Renew Now	(Expired)	100 scores Time 03/26/2018 22:13:57 High risk 0 , Medium risk 0 , Low risk 0 , Information 0	Renew Now	More 🗸
http://www.ss.com Package Version: Professional Expiration Time: 03/26/2018 23:59:59	(Not authenticated)	100 scores Time 03/26/2018 22:13:57 High risk 0 , Medium risk 0 , Low risk 0 , Information 0	Authenticate	More 🗸
http://10.93.194.177:8066 Package Version: Basic Expiration Time:	(Authenticated)	100 scores Time 03/26/2018 22:13:57 High risk 0, Medium risk 0, Low risk 0, Information 0	Scan Now	More 🗸

Parameter	Description
Domain	• Domain name/IP address and authentication status
Information	 Authenticated The target domain name has been authenticated. You can click Scan Now in the Operation column to create a scan job. For details, see Creating a Scan Job.
	 Not authenticated The target domain name has not been authenticated. You can click Authenticate in the Operation column to authenticate the domain name. For details, see Authenticating a Domain Name.
	 Expired and cannot be renewed If the purchase duration of the professional edition has expired, Expired and cannot be renewed is displayed. Click Re-purchase to renew the domain name. For details, see the <i>Vulnerability Scan</i> Service Purchase Guide.
	• Job name
	• Package Version : Indicates the current VSS edition, which can be either Basic or Professional .
	• Expiration time
	 When you are using the basic edition, the expiration time is displayed.
	 When you are using the professional edition, the actual expiration time is displayed. If the purchased service has expired, click Re- purchase.
Latest Scan Details	Displays information about the latest scan job of the domain name, including the score, time, and number of vulnerabilities at each level.

Table 4-1	Parameter	description
-----------	-----------	-------------

----End

4.2 Adding a Domain Name

This section describes how to add a domain name.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Asset List.
- Step 3 Click Add Domain Name or +Add Domain Name.

Figure 4-2 Adding a domain name

Add Domain Nan	ne	X
Specify Doma	in Name Information	Authenticate Domain Name Ownership
	1	2
Specify the domain name detai	Is of the website to be authenticated, includin	ng the domain name address or IP address.
* Domain name	test	
* Domain Name/IP Address	http://	
		Cancel Confirmation Add

Step 4 Click OK.

The Authenticated domain name page is displayed. For details, see Authenticating a Domain Name.

NOTE

You can also add domain names through **Purchase Service** in the upper right corner on the **Dashboard** page.

----End

4.3 Authenticating a Domain Name

This section describes how to authenticate a domain name.

Prerequisites

- An account and its password have been obtained for logging in to the management console.
- The domain name status is **Not authenticated**.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Asset List.
- Step 3 In the Operation column of the desired domain name to be authenticated, click Authenticate.
- Step 4 Choose the method for domain name authentication, Authenticated Document Upload or One-Click On-Cloud Authentication in the displayed Authenticated domain name dialog box.

Method 1: Click Download Authenticated Document.

Figure 4-3 Uploading an authenticated document

Authenticated domain name

Specify Domain Name Information

Authentica

Use either of the following authentication modes:

Authenticated Document Upload One-Click On-Cloud Authentication

Step 1: Click Download Authenticated Documentto download the authenticated document in name and content unchanged.

The second step: Upload the authenticated document to the root directory of the website, and accessed through network address http://10.154.77.22/hwwebscan_verify.html. Click to access

The third step: Click the 'To Authenticate' button in the lower right to verify.

Note: If your domain name is not authenticated yet, The scan will not be performed.

I have read and agree to the HUAWEI CLC

- 1. Click Download Authenticated Document.
- 2. Upload the document to the root directory of the website and ensure that the following network address can be accessed: target network address/hwwebscan_verify.html.
- 3. Select I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer.
- 4. Click Authenticate.

After the operations are complete, the domain name status becomes Authenticated.

Method 2: Click One-Click On-Cloud Authentication.



Authenticated domain name

Specify Domain Name Information

Authentica

Use either of the following authentication modes:

Authenticated Document Upload

One-Click On-Cloud Authentication

if the website server of http://10.154.77.22 is deployed on HUAWEI CLOUD and you own the lower left corner of the page to authenticate the domain name. This authentication mode can

Scenario 1: The website server is deployed on HUAWEI CLOUD and no proxy is used.



VSS



Where the Website

Server Locates

Scenario 2: The website server is deployed on HUAWEI CLOUD and HUAWEI CLOUD WAF



Select I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer and click Authenticate.

After the operations are complete, the domain name status becomes Authenticated.

----End

$\mathbf{5}_{\mathsf{Job\ List}}$

5.1 Creating a Scan Job

This section describes how to create a scan job.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Task List.
- Step 3 Click Create Job.

Figure 5-1 Creating a job

Create Job			
Job Name	Scan	Score	Vulnerability Le
wpz_eipff	http://10.154.76.159	100	🛑 High risk 0 (
111	http://10.154.76.159	100	🔵 High risk 0 (



Table 5-1 Parameter description

Parameter	Description
Job Name	The value is specified by the user.
Target Network Address	Enter the website or IP address to be scanned. Select an authenticated domain name from the drop-down list.
receive notifications	After this function is enabled, the user will receive an SMS notification when the scan job is complete.

Figure 5-2 Scan settings

Scanning Settings @			
* Job Name:	test		
* Target Network Address:	http://		
receive notifications:	\bigcirc		
Advanced Settings ¥			
		Timing	02/11/2018

Step 5 (Optional) Expand Advanced Settings. Set parameters by referring to Table 5-2.



	Advanced S	ettings *			
	~ Mor	re Scan Settings			
		Scan Strength: 😮	1	2	3
		Port Scan:	—		
		Weak Password Sca	an: 🗡		
	∧ We	bsite Login Setti	ngs 🕜		
		Login Page:			
		Username:			
		Password:			
		Confirm Password:			
	∧ Cra	wler			
		Simulate Browser:	Firefox		
		Exclude Link: 😮			
			🕀 You can add 4 r	nore entries.	
	∧ Self	f-Define HTTP R	equest Heade	r	
		Example:X-GIT-TOP Example:Cookie: ph	KEN: dsfsdfsadfasdfs psessionid=asdfsadf	adfasdfsadfsdaf sadfsadfsadf; sdfs	s=asdfasdfasdf; uid='
Issue 03 (2019-07-12)	(Copyright © Huawei Techr	nologies Co., Ltd.		19
		Name:			Value:
		You can add 4 m	ore entries.		

Parameter	Description	Configuration
More Scan Setti	ngs	
Scan Strength	The higher the scan strength, the stronger the detection capability, but the longer the time required.	N/A
Port Scan	You can enable or disable port scan.	enabled
Weak Password Scan	You can enable or disable weak password scan.	: disabled
Website Login S	ettings	
NOTE:		
Some pages cann provide the follow	ot be accessed unless you have lowing information.	ogged in. If you want to scan these pages,
Login Page	Address of the website login page	N/A
Username	Username for logging in to the website	N/A
Password	Password of a user	N/A
Confirm Password		
Crawler		
Simulate Browser	Web browser used by crawlers	Select a browser from the drop-down list box. Currently, only Firefox and Chrome are supported.
Exclude Link	Links to pages that you do not	You can add a maximum of five links.

Table 5-2 Parameter	description	of advanced	settings
---------------------	-------------	-------------	----------

Self-Define HTTP Request Header

NOTE:

Some pages have further authentication requirements (such as requiring the user to enter a verification code). If you want to scan these pages, enter HTTP request headers.

Click \bigcirc to add links and \bigcirc to

remove them.

NT		
and click 🖸 to	remove them.	
A maximum of fi	ve request headers can be added.	Click 🕒 to add HTTP request headers

Name	Name of an HTTP request header	Example: Cookie
------	--------------------------------	-----------------

want to include in the scan

Parameter	Description	Configuration
Value	Value of an HTTP request header	Example: phpsessionid=asdfsadfsadfsadfsadf; sdfs=asdfasdfasdf; uid=1

- **Step 6** After the settings are complete, select **Timing** for a scheduled scan or click **Start Scan** to immediately start a scan.
 - Scheduled scan

Select Timing and set the scan time. Then, click Start Scan.

The system starts the job at the scheduled time.

Immediate scan

Click Start Scan.

After the job is successfully created, a page displaying the job details is displayed.

If the server is not fully occupied, the newly created job can be performed immediately and the job status is **In progress**.

If the server is fully occupied, the job waits in the queue and its status is Waiting.

----End

5.2 Viewing Scan Details

This section describes how to view scan details.

Prerequisites

- An account and its password have been obtained for logging in to the management console.
- At least one scan job has been created.

Procedure

Step 1 Log in to the management console.

Step 2 Choose Security > Vulnerability Scan Service > Task List.

Step 3 Click the name of a job.

Figure 5-4 Job name

Job Name	Scan	Score	Vulnerability Level	Started	Scan Duration	Status	Progress	Operation
(asakat)	http://10.175.47.113:8080/wavsep/activ	0	● High risk 31 ● Medium risk 0 ● Low risk 0 ● Information 0	02/06/2018 15:3	00:03:49	Complete	100%	Restart Cancel Edit

Step 4 The page displaying details of the job is displayed, including the **Scan Details** tab. **Table 5-3** describes each part of the page.

In the upper right corner, click download Report to download the job report in HTML format.

Figure 5-5 Scan details

Job List > wx:sectrain.cn_1522170841000					
What Does the Score Mean? V	Why is a Job Automatically Canceled in	the Job Scan Process? How Do I View Vulnerability Fixing Suggestions?	More common problems Comments and Suggestions		
Target Network Add	dress: https://wx.sectr	ain.cn 😣 Authenticate Now More 🕶		土 Download Report	
Score:			Complete:10)0%~	
	Website Security Level: Safety				
100 _{scores}	Total: 0 🔸 H	ligh risk 0 🛛 🔴 Medium risk 0 💛 Low risk 0 💿 Information 0			
	Scan Details: Target Ne	twork Address: https://wx.sectrain.cn Started: 03/28/2018 01:14:01 GM	AT+08:00 Scan Duration: 00:00:16 Scan Strength2 (Weaker strength	but faster speed)	
	Stanresuits. Tou cant	nny nave a seminare premininary scan because your domain name is not a	autrenituateu, ejease autrenituate your uoritain name in the assectiat a	ina ger a deep, fuil soan.	
Scan Details Vulnerabili	ty List Port List Site Structu	re			
-					
Туре		Item	Result		
Malicious Content;		Malicious Links	Safety View details		
Miner Backdoors (Safety) View details					
Dotential Rick		WebSite Headers	(Safety) View details		
Potentiai Risk		Https Protocol	(Safety) View details		

Table 5-3 Parameter description

Area	Description	Operation
Scan Address	The default value is the Target Network Address value that you set when creating the job.	 Click next to the target website to view the following basic information about the website: IP Server Language

Area	Description	Operation
Job Information	 Displays basic information about a job, including: Score: score of the host. The initial score is 100, which will be deducted according to the numbers and levels of vulnerabilities discovered. If no vulnerability is detected, the score remains 100. Website Security Level: Determine the website security level based on the scan results. If no vulnerability is detected, Website Security Level is displayed as Safety. If vulnerabilities are found, it is displayed as medium risk, high risk, or low risk. Total: total number of vulnerabilities and number of vulnerabilities of different levels Started: time to start the scan job Scan Duration: time consumed to complete the scan Scan strength: scan strength of the website selected when you create a scan job. The deeper the scan strength is, the slower the scan speed is. Scan results: result of a scan job, scanned successfully or failed 	 Click Scan Again or Cancel to re-scan or cancel the scan job. Click More to perform the following operations: Query details of advanced settings. Edit the scan job.
Scan Details	Displays the scan types, specific scan items, and the scan result of each scan item.	 Scan result: Safety Danger. In this case, click View details. Scan fails as the domain name is not authenticated. Click Authenticate Now.

Step 5 Click **View details** to learn more if the scan result is safety. If there is a risk (such as mediumand high-risk), click View details to check the risk.

Figure	5-6	Scan	Details
--------	-----	------	---------

Scan Details Vulnerability List Port List Site Struct	ure	
Туре	Item	Result
Mallalan October	Malicious Links	(Safety) View details
Malicious Content;	Miner Backdoors	Safety View details
	WebSite Headers	Safety View details
Potential Hisk	Https Protocol	Safety View details
	Server Intrusion	Safety View details
	Leakage of User data	Safety View details
	Website infomation Expose	Safety View details
	DataBase Leakage	Safety View details
Website Sec Vulns	Trojan Implant	(Safety) View details
	Phishing Fraud	Safety View details
	Unlawfully changing data	Safety View details
	Website Blocking	Safety View details
	Others	(Safety) View details

Step 6 Click the Vulnerability List tab.

Figure 5-7 Vulnerability List

Scan Details Vulnerability List Po	rt List Site Structure				
					View
Vulnerability ID	Discovered	Level	Status	Туре	Target Network Address
c7dc1a03b5930f73be7da656eb99f53e	04/03/2018 22:56:09 GMT+08:00	Medium	Not fixed	Cross-Site Request	http://122.112.198.43:9091/vulnerabilities/sqli/?id=98
07e2a0c37379b62c361cfdf5f920222b	04/03/2018 22:56:06 GMT+08:00	Medium	Not fixed	Cross-Site Request	http://122.112.198.43:9091/vulnerabilities/xss_r/?nam
a3139f92e55e3865c72430f04f70ddd2	04/03/2018 22:56:05 GMT+08:00	Medium	Not fixed	Cross-Site Request	http://122.112.198.43:9091/vulnerabilities/view_sourc
7c90cc86db32697c3d164b9d6cc89a4a	04/03/2018 22:56:04 GMT+08:00	Medium	Not fixed	Cross-Site Request	http://122.112.198.43:9091/vulnerabilities/exec/
69db89eb54413f58b75c643b52a8151f	04/03/2018 22:56:03 GMT+08:00	Medium	Not fixed	Cross-Site Request	http://122.112.198.43:9091/vulnerabilities/view_help.p.

5 🔻 Total Records: 14 < 1 2 3 >

Shows vulnerabilities detected in a job. One page displays five entries. You can go to the next page for more entries.

- Click View to view the vulnerability list.
- Click a vulnerability ID to view the vulnerability details.

Step 7 Click the Port List tab.

Port information of the target website is displayed.

Figure 5-8 Port List

Scan Details Vulnerability	List Port List Site Structu	ILE	
Port	Status	Protocol	Service
22	Close	ТСР	NetBIOS Session Service1
23	Open	UDP	NetBIOS Session Service2
22	Open	ТСР	NetBIOS Session Service2
22	Open	TCP	NetBIOS Session Service2
22	Open	TCP	NetBIOS Session Service2
5 Total Records: 6 <	1 2 >		

Step 8 Click the Site Structure tab.

ΠΝΟΤΕ

The **Site Structure** tab page shows locations of vulnerabilities in the target website. If no vulnerabilities have been detected, this page is empty.

The tab page displays basic information about the target website, including:

- IP Address: IP address of the target website
- Server: name of the server used for deploying the target website (for example, Tomcat, Apache httpd, and IIS)
- Language: development language used by the target website (for example: PHP, Java, and C#.)

Figure 5-9 Site Structure

Scan Details Vulnerability List Port List Site Structure

122.112.198.43:9091	^ Vulnerability1	^
📮 🔚 vulnerabilities	in the second	
🗖 🔚 sqli	Vulnershilty Detaile	
?id=985&Submit=Submit	vulnerability Details	
view_source.php?id=csrf&security=high	Vulnerability ID: 7a5ed613b3df64c6776bbef107b2cc1d	
🗖 🔚 fi	Vulnerability Type: Directory Traversal	
?page=include.php	Vulnerability description:Attackers can browse any file in a web page directory to leak the file structure and sensitive files of the website.	
🖾 🔚 csrf	vullerability Level. Medium fisk	
📮 🔚 sqli_blind		
🚦 ?id=419&Submit=Submit		
🗖 🔚 xss_r		
?name=131		
🛃 exec		
view_help.php?id=csrf&security=high		
📮 🔚 dvwa		
js		
CSS		
📴 images		
	*	-

----End

6 Overview

6.1 Taking an Overview

This section describes the **Dashboard** page, which displays the vulnerability overview, latest vulnerability news, vulnerability type, vulnerability level, vulnerability list, latest scan information, and product information.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

- Step 1 Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Dashboard.
- **Step 3** View the information on the **Dashboard** page. **Table 6-1** describes each part of the page.

You can select an authenticated domain name from the domain name drop-down list box on the upper left and view its vulnerability statistics measured by VSS.

Figure 6-1 Dashboard

6 Overview

Dashboard @ For any question or suggestion, please click here to let us know. Select domain name * What's New [2018.04.13] CVE-2018-1273 Spring Data Commons... - vulnerabilities have - of them are high-risk vul One-Clic [2017.12.22] CVE-2017-10271 WebLogic XMLDecod... One-Click [2017.09.05] CVE-2017-9805 Struts2 REST The Recent 6 Scans Overview (!)[:] No data available No data available Latest Scan Information Job Name: Vulnerability Level Vulnerability Type Score: Total Vulnerabilities: 🗕 High risk – Medium risk -Low risk -Information [:] [:] Status: No data available No data available Started: Duration: Vulnerability List View Product Information Target Network Address Vulnerability ID Discovered Level Status Type Web Application Firewall . Ne Prevent Web attack, CC, horse, to escort your business website ed Anti-DDoS , New arrival $\left[\cdot \right]$ Big traffic DDoS attacks for games, finance, website and other b. Security Assessment Service , New Product 30% Discount on Bi... No data available Nationally certificated security experts are ready to do "pulse fe... Host security service , New arrival Special defense against cloud host intrusion, violent cracking, Tr...

Table 6-1 Page description

Area	Description	Operation
The Recent 6 Scans Overview	Shows the distribution of different- level vulnerabilities of the latest six scans by time for the selected domain name in a line chart.	To hide data about a vulnerability level, click the corresponding legend on the right. Click High risk to hide data about high-risk vulnerabilities.
Vulnerabili ty Type	Shows the vulnerability type distribution of the selected domain name.	To hide data about a vulnerability type, click the corresponding legend on the right. For example: Click SQL Injection to hide data
		about SQL injection vulnerabilities.

Area	Description	Operation
Vulnerabili ty List	Displays basic information about vulnerabilities for the selected domain name, such as its ID, discovery time, level, status, type, and URL.	 Click a vulnerability ID to view the vulnerability details. For more information about this operation, see Viewing Details of a Vulnerability.
		 Click View to go to the Vulnerability List page.
What's New	Displays information about the vulnerabilities that need to be handled by VSS.	Click One-Click Detection to go to the Rapid Detection of Critical Vulnerabilities page.
Latest Scan Informatio n	Shows information about the latest scan, including the job name, score, number of vulnerabilities of each level, job status, start time, and duration.	Click a job name to view details. For more information about this operation, see Viewing Scan Details.
Product Informatio n	Shows information about VSS or other related products.	N/A

----End

6.2 Vulnerability List

6.2.1 Viewing the Vulnerability List

This section describes how to view the list of detected vulnerabilities.

Prerequisites

An account and its password have been obtained for logging in to the management console.

Procedure

- **Step 1** Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Dashboard.
- Step 3 On the right of the Vulnerability List area, click View to go to the Vulnerability List page.

You can expand the **All statuses** or **Advanced Search** drop-down box to filter vulnerabilities to view. If you click **Advanced Search**, first set the discovery time, select items from **All vulnerabilities** drop-down list, set the vulnerability level, and then click **Search**. Click **Reset** to clear the search criteria.

Figure 6-2 Vulnerability List

Vulnerability List

Vulnerability ID	Discovered
1ceaccf3faf4144a4cae5311cf127c3e	03/31/2018 22:44:37 GMT+08:00
7a5ed613b3df64c6776bbef107b2cc1d	03/31/2018 22:44:37 GMT+08:00
b4dcdab661b13c5c3271a5ce8d7060cb	03/31/2018 22:44:37 GMT+08:00
3d9e625dfe96ac6952661f90c702e3c6	03/31/2018 22:44:06 GMT+08:00

Table 6-2 Vulnerability list parameters

Parameter	Description
Vulnerability ID	ID of a vulnerability You can click a vulnerability ID to view the vulnerability details.
Target Network Address	Page where the vulnerability is detected
Discovered	Time when a vulnerability is detected
Level	Level of a vulnerability. Possible values are:
	• High: high-risk
	• Medium: medium-risk
	• Low: low-risk
	• Info
Туре	Type of a vulnerability, including SQL injection, reflected XSS, and cross-site request forgery
Status	Status of a vulnerability. Possible values are:
	• Not fixed
	• Fixed
	• Ignored

----End

6.2.2 Viewing Details of a Vulnerability

This section describes how to view the details of a vulnerability.

Prerequisites

- An account and its password have been obtained for logging in to the management console.
- At least one vulnerability has been detected.

Procedure

- **Step 1** Log in to the management console.
- **Step 2** Choose **Security** > **Vulnerability Scan Service** > **Dashboard**.
- Step 3 On the right of the Vulnerability List area, click View to go to the Vulnerability List page.
- Step 4 Click the ID of the desired vulnerability.

Figure 6-3 Vulnerability ID

Vulnerability List						View
Vulnerability ID	Discovered	Level	Status	Туре	Target Network Address	
		No data availabl	e.			

Step 5 On the Vulnerability Details page, view details of the vulnerabilities.

Figure 6-4 Vulnerability Details

Vulnerability List > 1ceaccf3faf4144a4cae5311cf127c3e	
Vulnerability Details	 Recommended Action
Vulnerability ID:1ceaccf3faf4144a4cae5311cf127c3e	Modify the server configuration and disable the directory browsing function. Set the directory permission to prevent users from having the read permission during the running of the server. Add an index hum to the directory or nearby the directory and the server.
Vulnerability level:Medium risk	Recommendation
Vulnerability Status:Not fixed	Web Application Firewall Security Assessment Service Host Security Service
Discovered03/31/2018 22:44:37 GMT+08:00	. Lit Detaile
Vulnerability Type:Directory Traversal	^ Hit betails
Owning Domain Name:wpz_dvwa	 Request Details
Target Network Address:http://122.112.198.43:9091/dvwa	v Reenance Nataile
Vulnerability Overview	
Attackers can browse any file in a web page directory to leak the file structure and sensitive files of the website.	
*	

Area	Description	Operation
Vulnerabili ty Details	Displays the basic information about the hit vulnerability, including the vulnerability ID, vulnerability level, vulnerability status, discovery time, vulnerability type, owning domain name, URL, and vulnerability overview.	Click Mark as Ignored to ignore the vulnerability. NOTE After you mark a vulnerability as Ignored , you cannot change its status again and the system will no longer consider this vulnerability risky. You can click Unignore to bring back the vulnerability.
Recommen ded Action	Displays vulnerability rectification suggestions.	N/A
Hit Details	Shows the proof based on which a vulnerability is confirmed.	N/A
Request Details	Shows the request sent by VSS in order to simulate hacker probing and attacks on the website.	N/A
Response Details	Displays the response of the target website to the simulated request sent by VSS.	N/A

Table 6-3 Parameter descriptio

----End

6.2.3 Marking Vulnerabilities as Ignored

This section shows how to mark vulnerabilities as **Ignored**. Before the marking, make sure that the vulnerabilities are free of security risks.

After you mark a vulnerability as **Ignored**, you cannot change its status again and the system will no longer consider this vulnerability risky. You can click **Unignore** to bring back the vulnerability.

Prerequisites

- An account and its password have been obtained for logging in to the management console.
- At least one vulnerability has been detected.

Procedure

- Step 1 Log in to the management console.
- Step 2 Choose Security > Vulnerability Scan Service > Dashboard.
- Step 3 On the right of the Vulnerability List area, click View to go to the Vulnerability List page.
- Step 4 Select the vulnerabilities to be ignored and click Mark as Ignored.

Figure 6-5 Marking vulnerabilities as ignored

Mark	as Ignored		
	Vulnerability ID	Target Network Address	Disc
	c7dc1a03b5930f73be	http://122.112.198.43:9091/vulnerabilities/sqli/?i	04/(
	07e2a0c37379b62c36	http://122.112.198.43:9091/vulnerabilities/xss_r/	04/(
	a3139f92e55e3865c7	http://122.112.198.43:9091/vulnerabilities/view	04/(
	7c90cc86db32697c3d	http://122.112.198.43:9091/vulnerabilities/exec/	04/(
	69db89eb54413f58b7	http://122.112.198.43:9091/vulnerabilities/view	04/(
	49e33db0f8a74a6bf7	http://122.112.198.43:9091/vulnerabilities/csrf/?	04/0
	f535f64803018b4bc7	http://122.112.198.43:9091/vulnerabilities/csrf/?	04/(
	8e3667d14eadbe5a19	http://122.112.198.43:9091/vulnerabilities/fi/?pa	04/(
	d4cb3646ae2e7cc584	http://122.112.198.43:9091/vulnerabilities/sqli_bl	04/(
	1ceaccf3faf4144a4ca	http://122.112.198.43:9091/dvwa	03/3
10 👻	Total Records: 14 <	1 2 >	

- Alternatively, in the row containing the desired vulnerability, click **Ignore** in the **Operation** column to mark a vulnerability separately.
- You can also click **Ignore** on the page displaying the details of the vulnerability to mark a vulnerability.
- **Step 5** In the displayed **Ignore Vulnerability** dialog box, specify the mandatory fields, and then click **OK**.

----End



Released On	Description
2019-07-12	This is the third official release.
	 Added section "Enabling VSS."
	• Added FAQ "Pricing".
	 Added FAQ "Renewing an Account."
	• Added FAQ "Unsubscribing from VSS."
2019-07-08	This issue is the second official release.
	Optimized the content.
2018-05-10	This issue is the first official release.