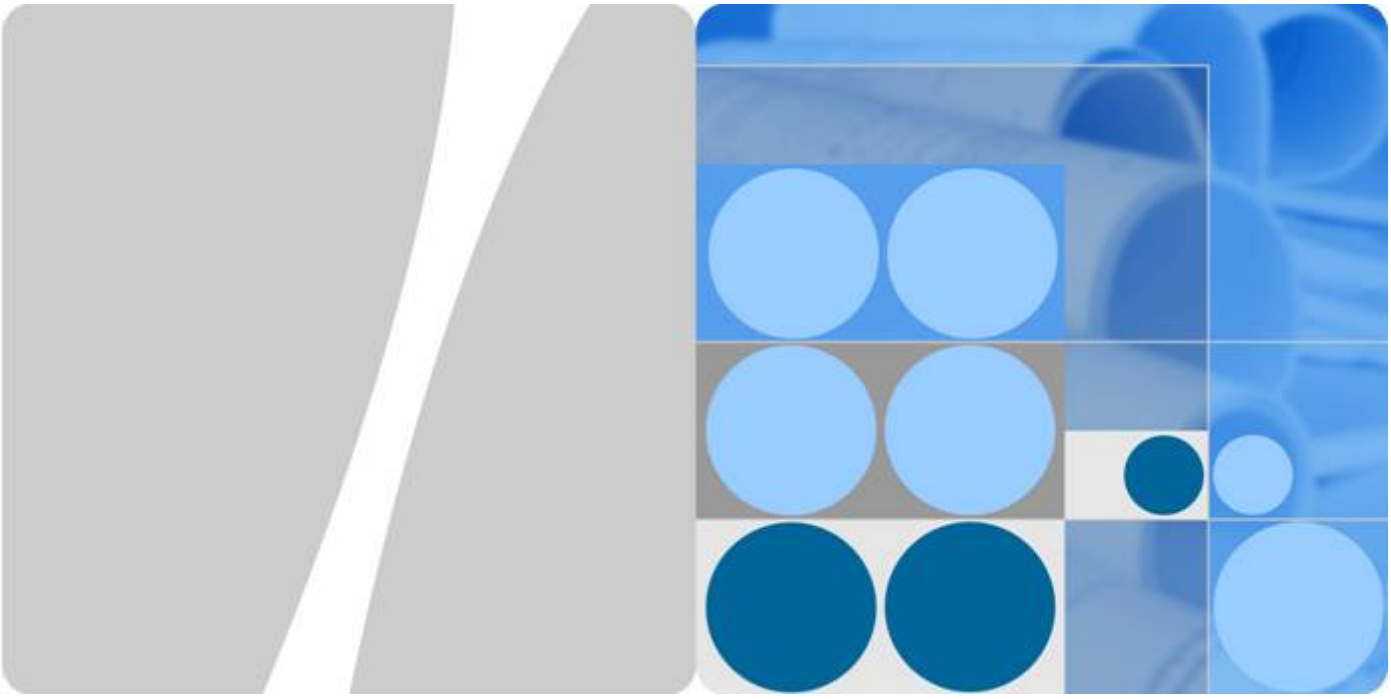


Vulnerability Scan Service

User Guide

Issue 03

Date 2019-07-12

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI 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: http://e.huawei.com

Contents

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**.

Table 1-1 Functions and specifications

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
Professional	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**.

NOTE

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)

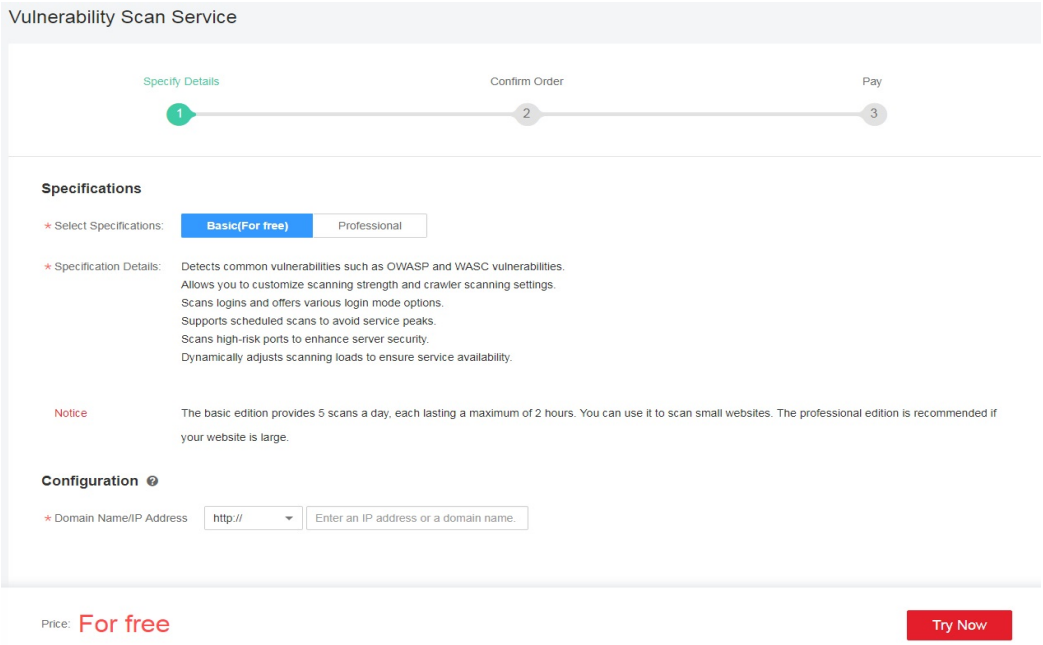


Figure 1-2 Edition selection (professional edition)

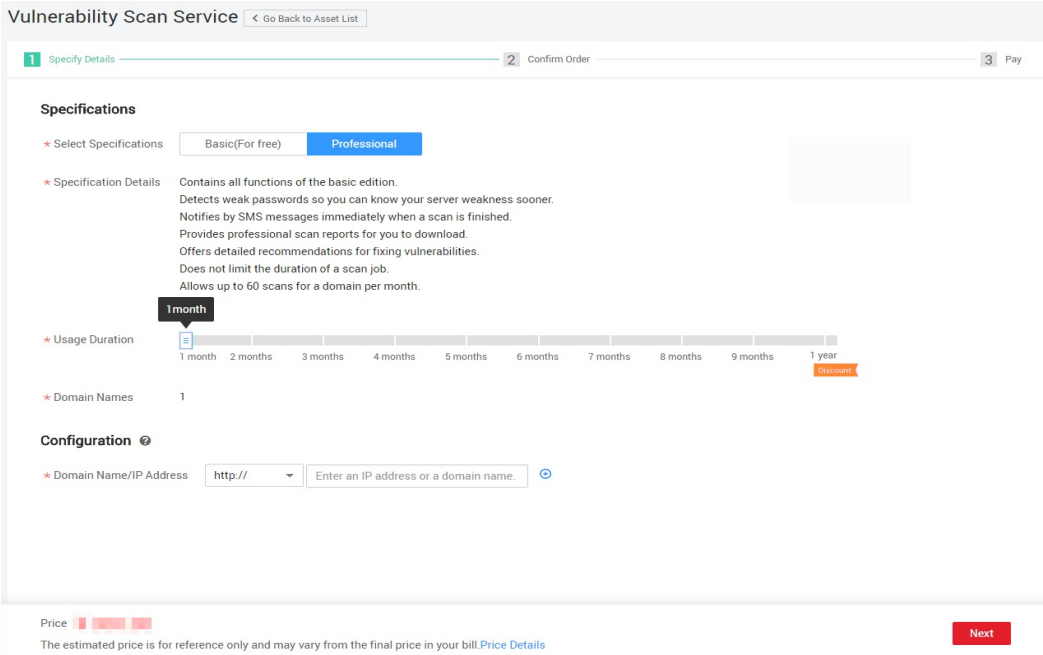


Table 1-2 Parameter description

Parameter	Description
Select Specifications	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**.

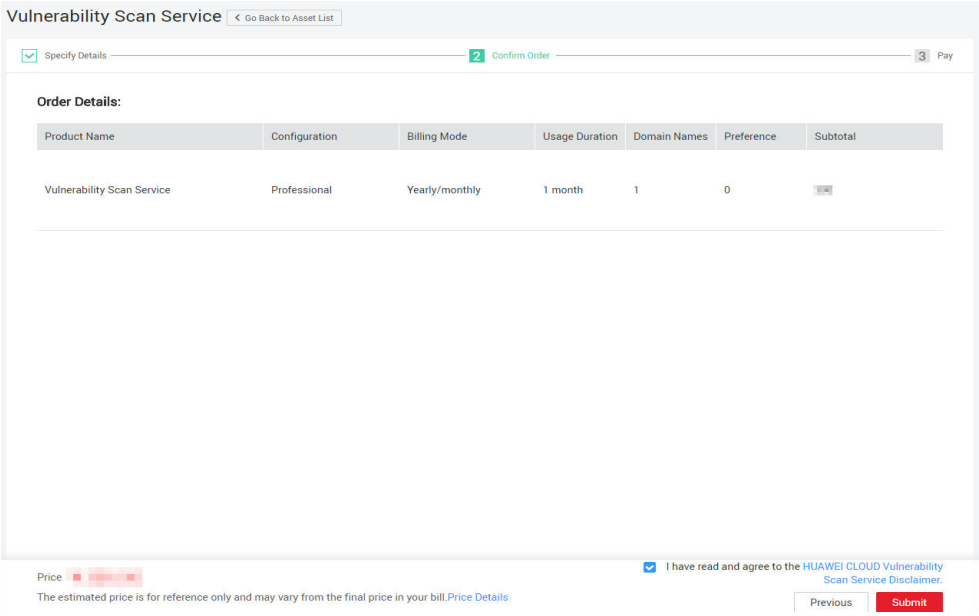
NOTE

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



Step 7 On the **Pay** page, select a payment method to pay for your order.

----End

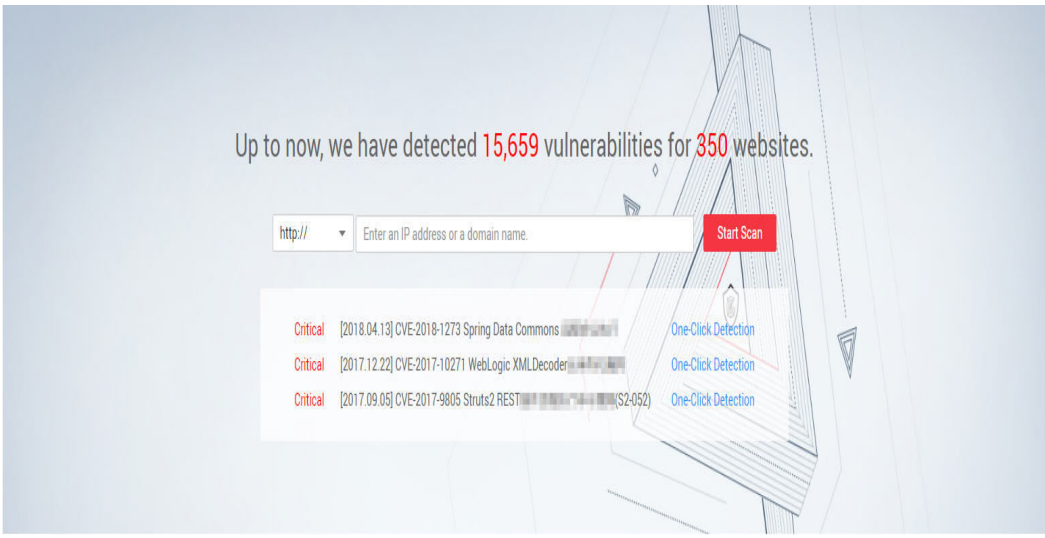
2 One-Click Scan

This section guides new users to experience VSS for free.

Procedure

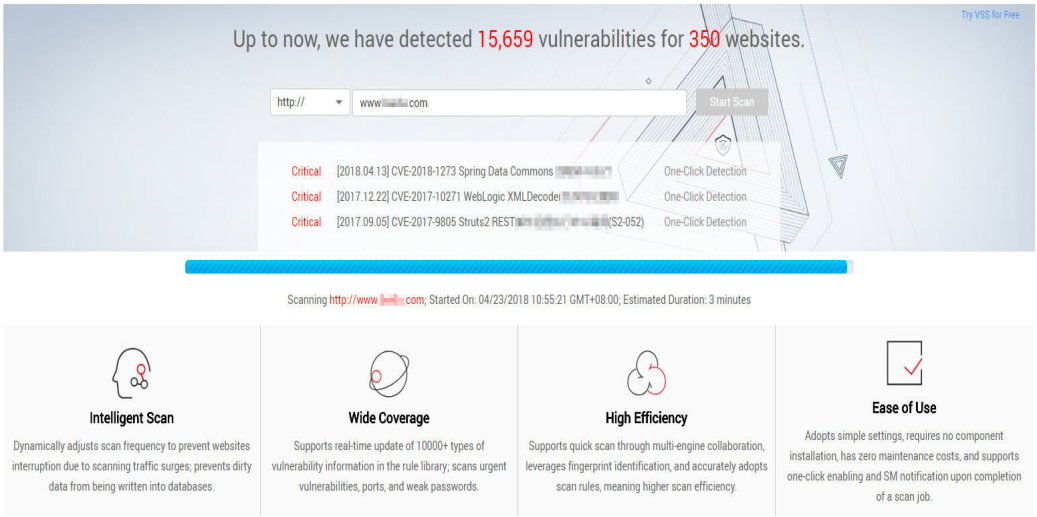
Step 1 Enter an IP address or a domain name to be scanned, and click **Start Scan**.

Figure 2-1 New user experience page



Step 2 View the scan progress.

Figure 2-2 Scanning



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

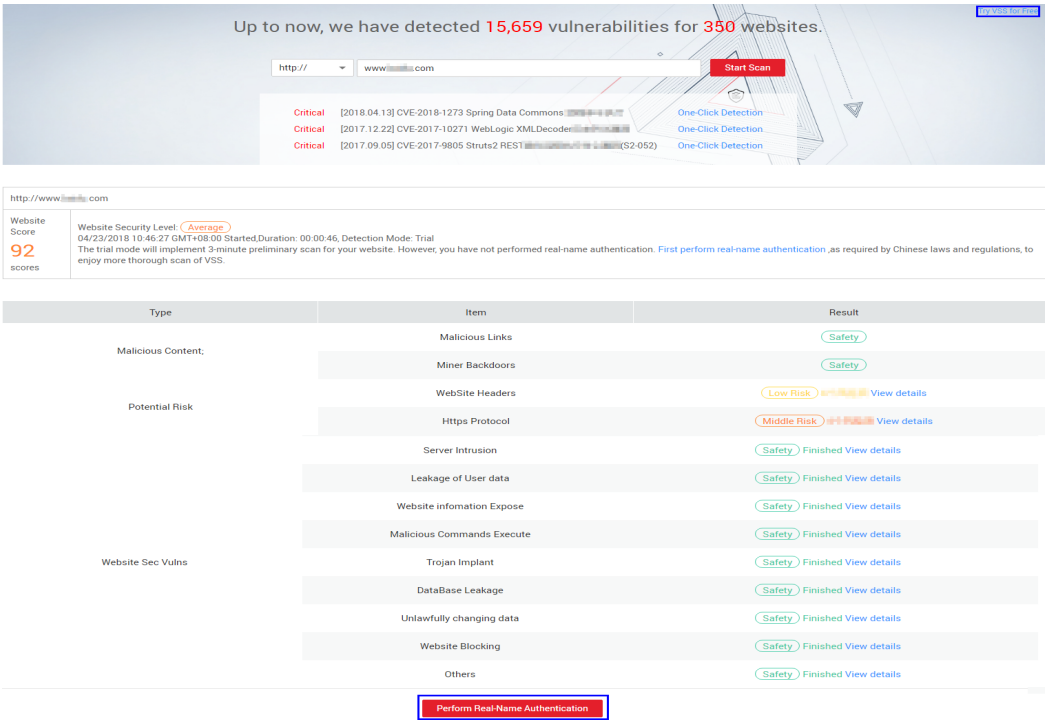


Table 2-1 Scan results

Area	Description	Operation
Type	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

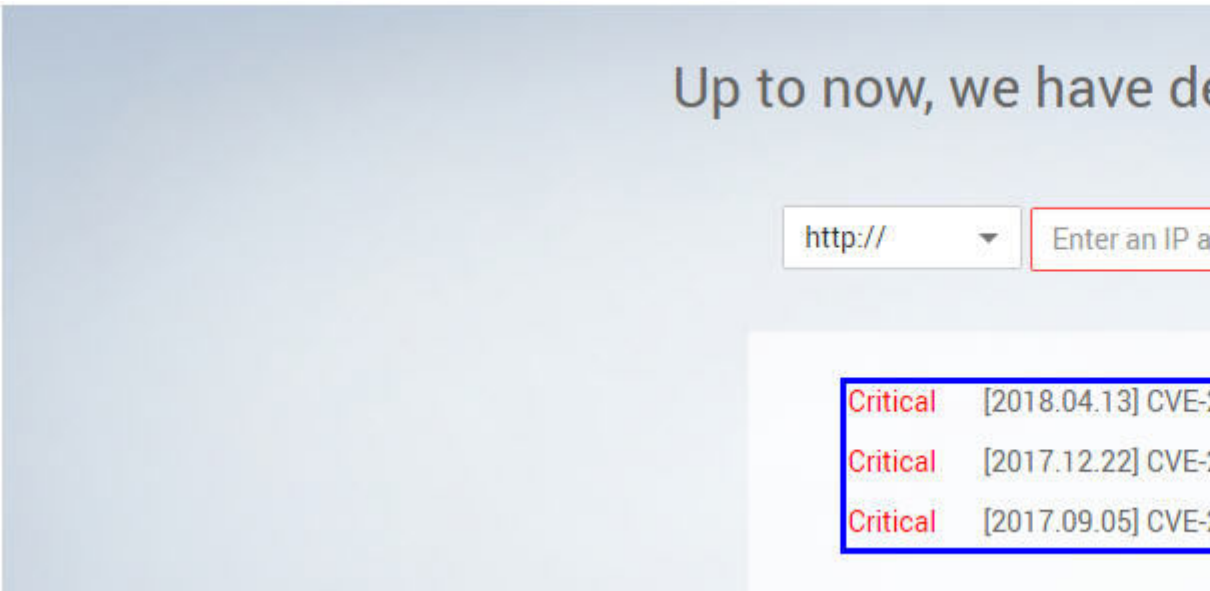


Figure 3-2 One-click detection of the latest critical vulnerability

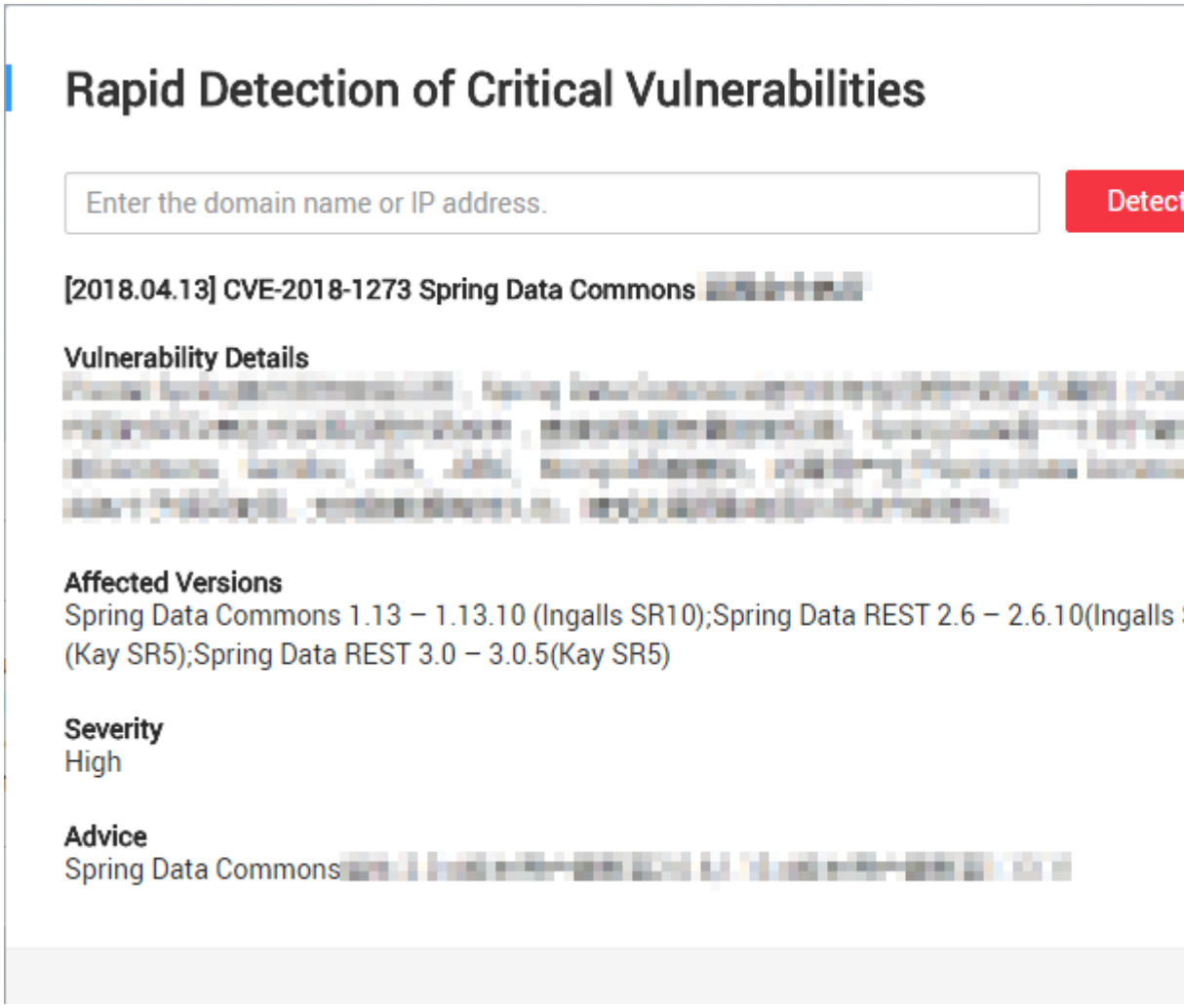


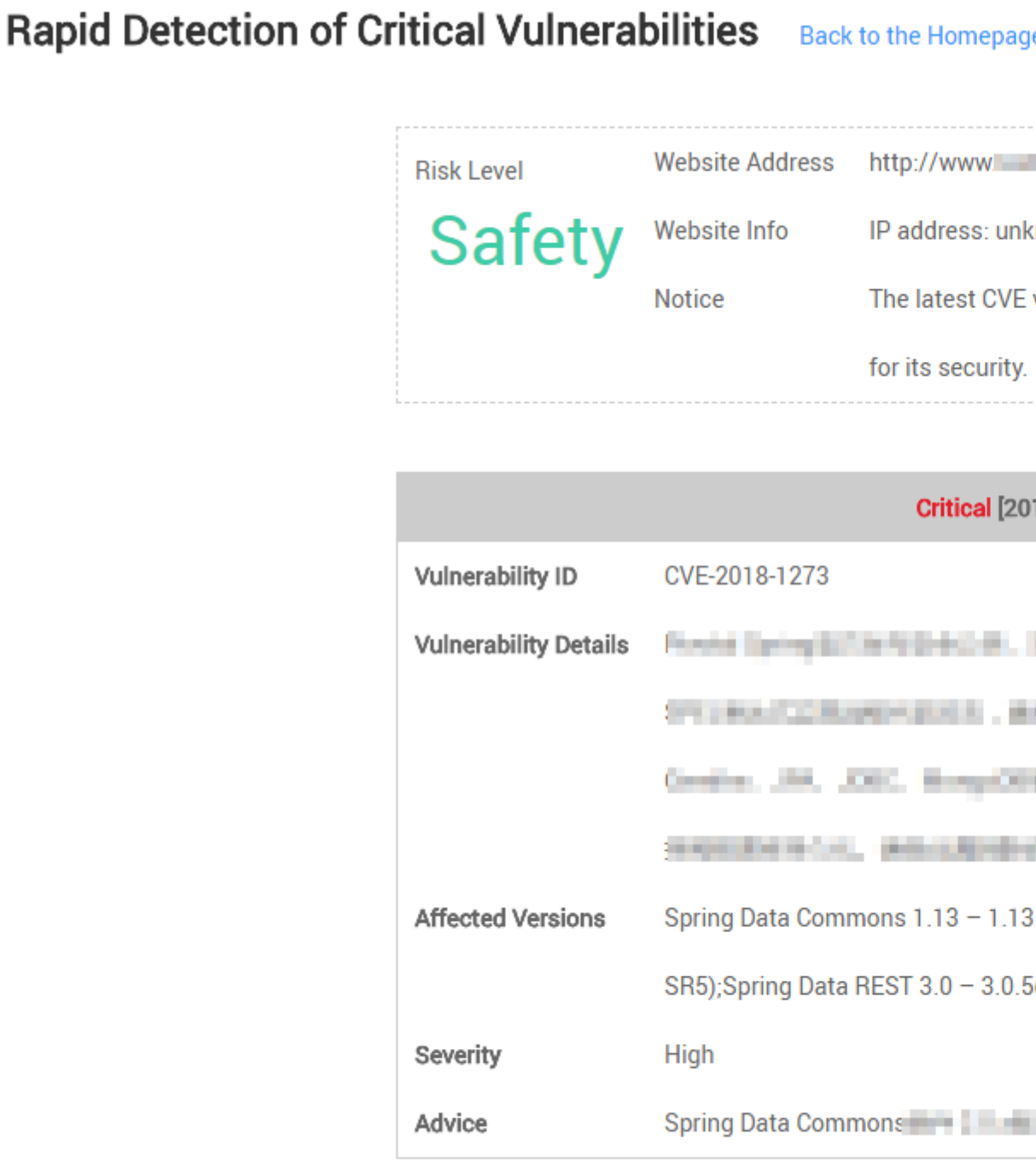
Table 3-1 Detection results

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



----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**.

NOTE

- 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

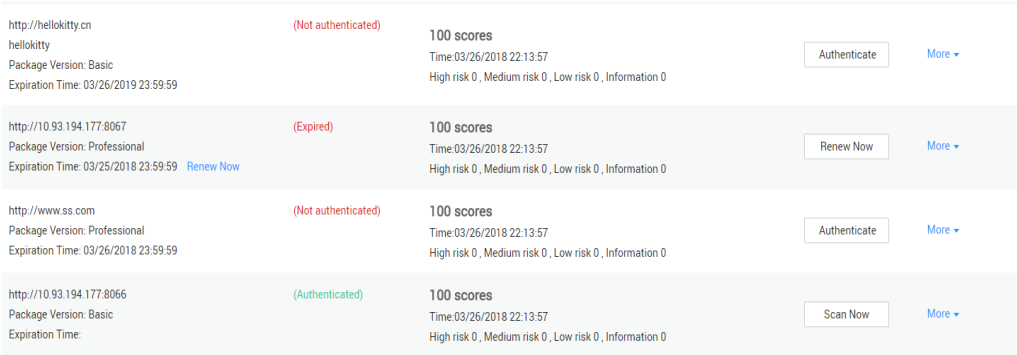


Table 4-1 Parameter description

Parameter	Description
Domain Information	● *Domain name/IP address and authentication status* – 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 *Vulnerability Scan 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.

----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.

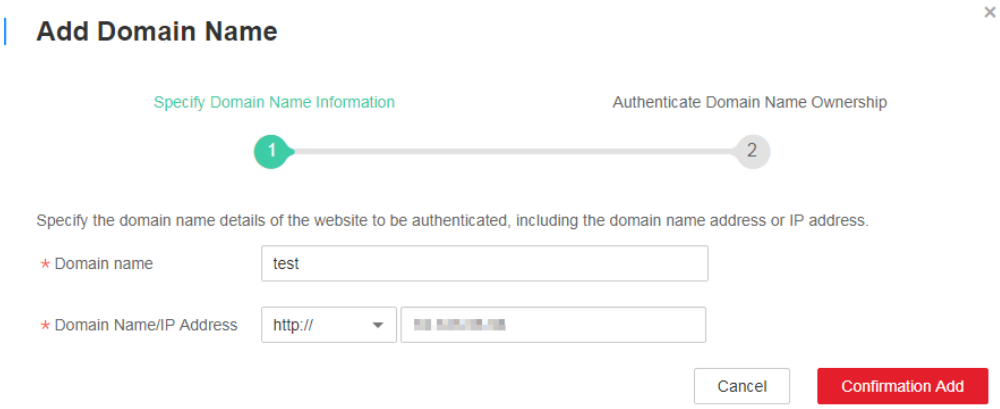
Procedure

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



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.

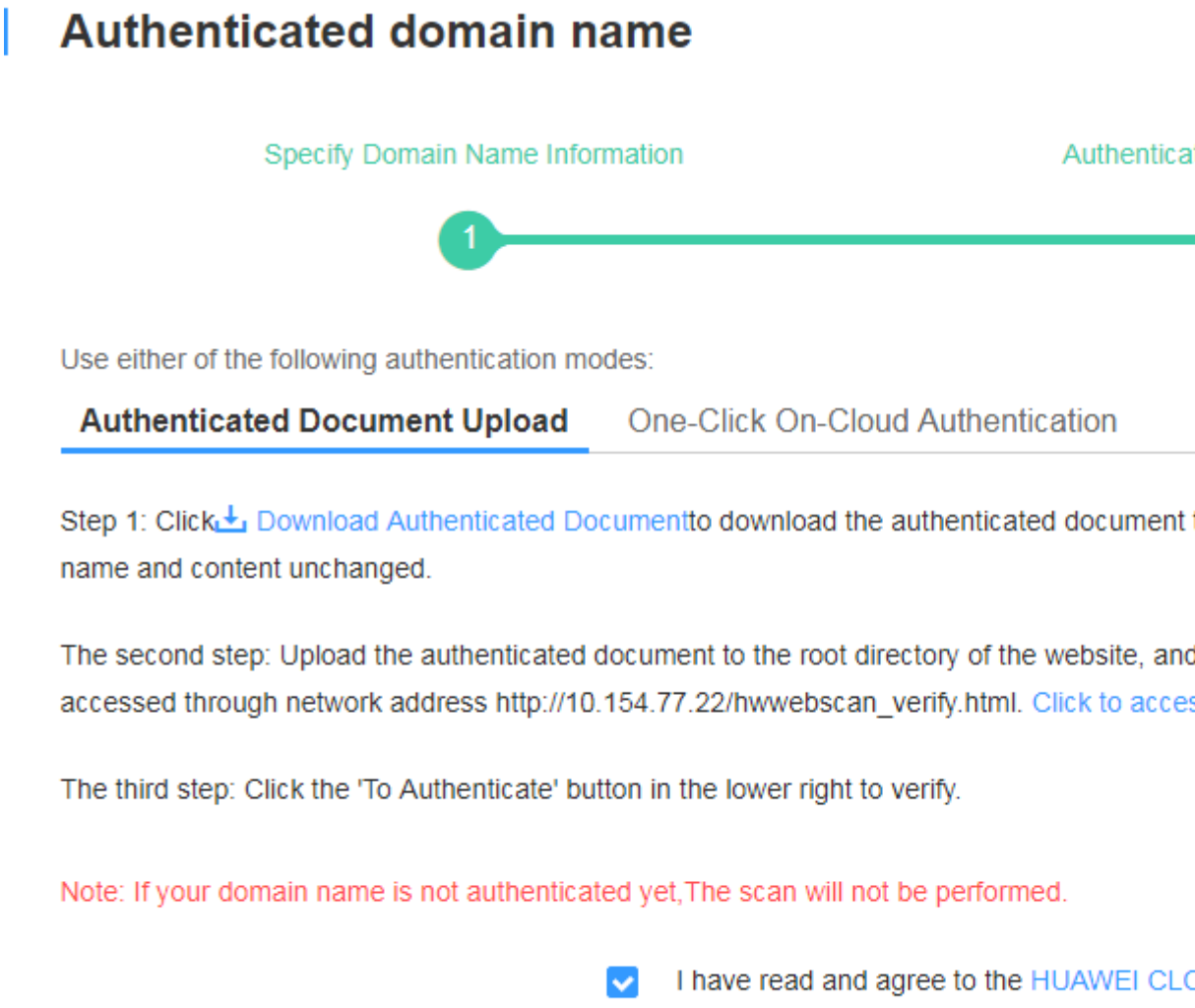
Step 2 Choose **Security** > **Vulnerability Scan Service** > **Asset List**.

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

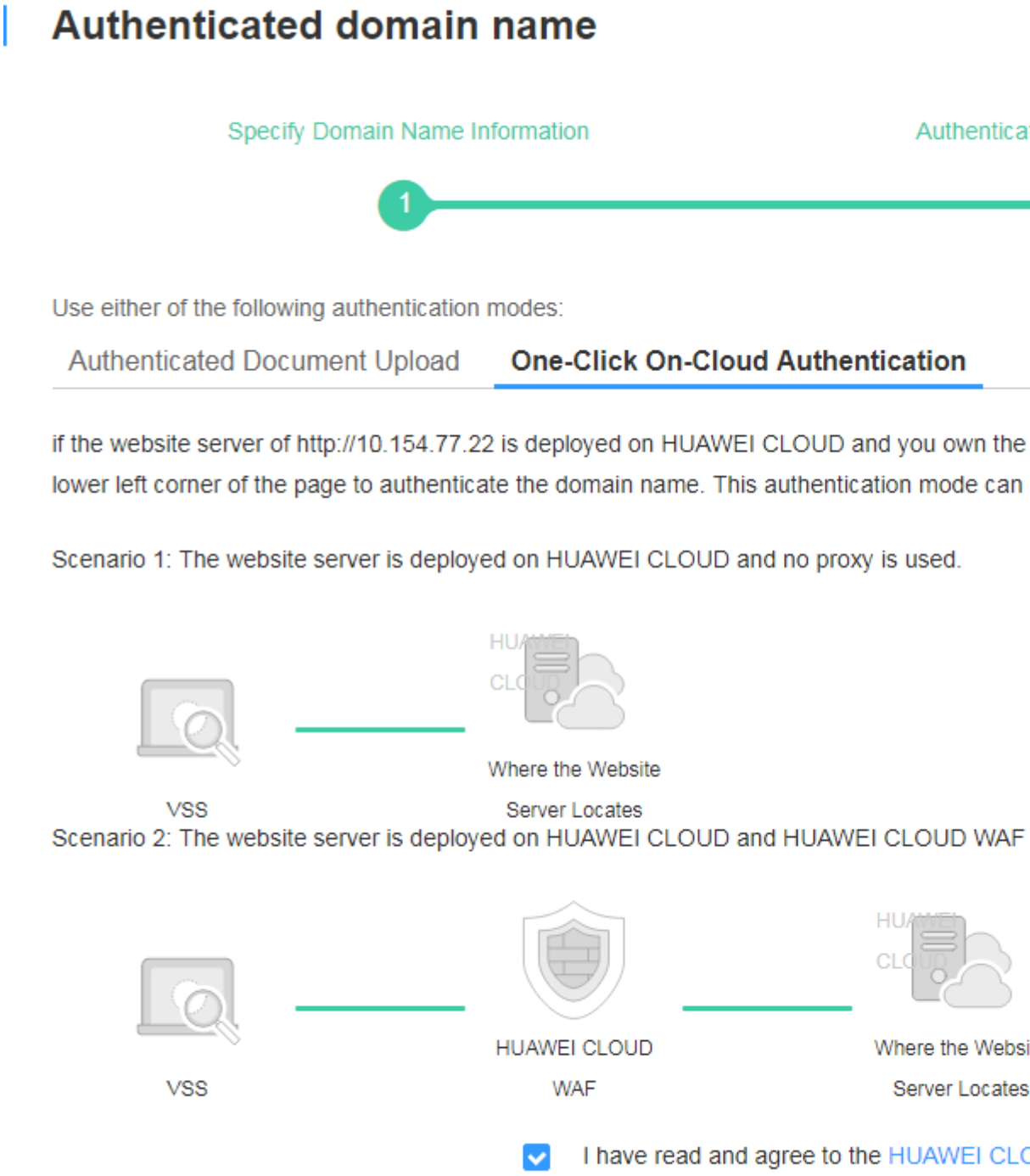


1. Click **Download Authenticated Document**.
2. Upload the document to the root directory of the website and ensure that the following network address can be accessed: **target network address/hwwebscan_verify.html**.
3. Select **I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer**.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

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

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

Figure 4-4 One-click on-cloud authentication



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

5 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.

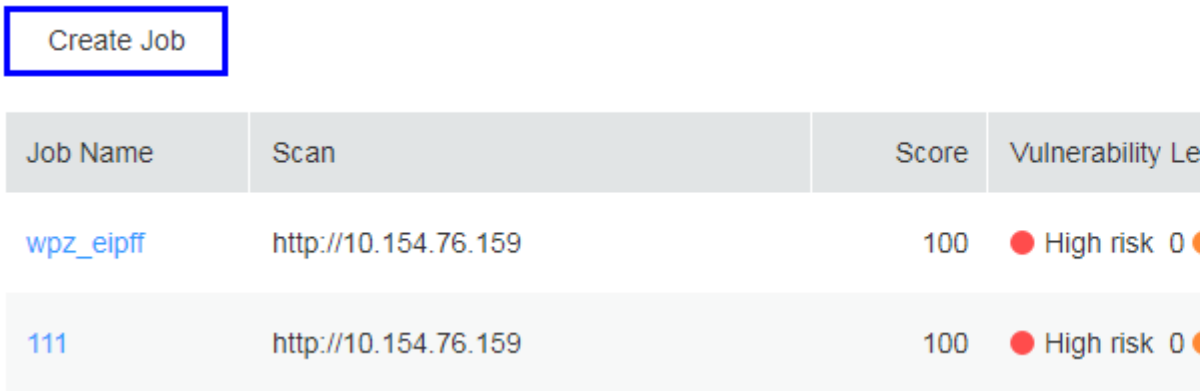
Procedure

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

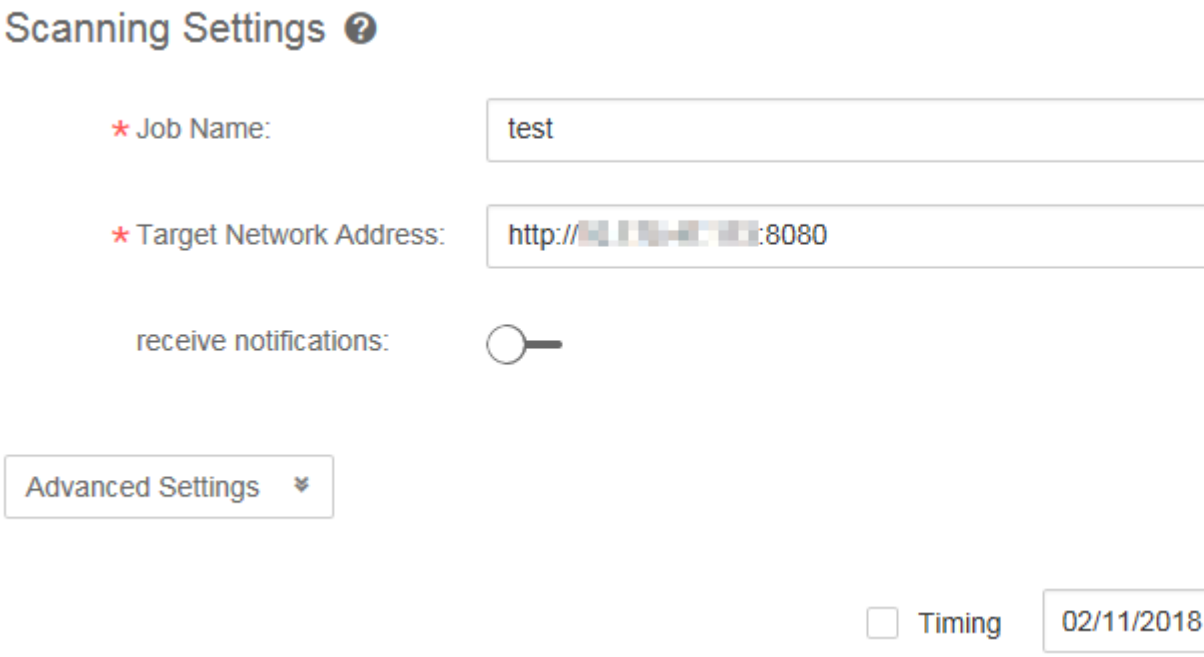


Step 4 Perform scan settings according to **Table 5-1**. **Figure 5-2** shows the result after setting.

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. ● : disabled ● : enabled

Figure 5-2 Scan settings



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

Figure 5-3 Advanced settings

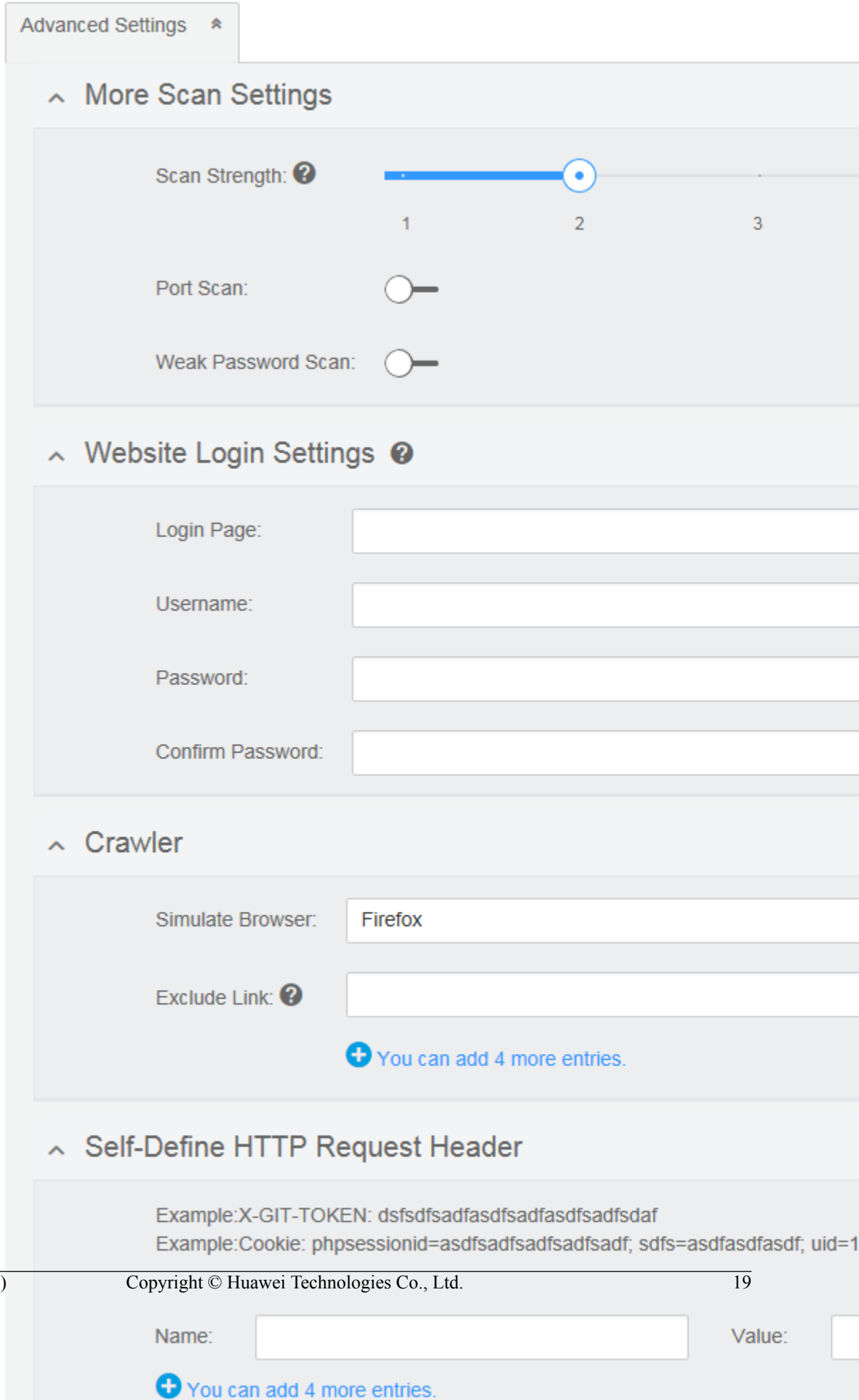


Table 5-2 Parameter description of advanced settings

Parameter	Description	Configuration
More Scan Settings		
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 : disabled
Weak Password Scan	You can enable or disable weak password scan.	
Website Login Settings NOTE: Some pages cannot be accessed unless you have logged in. If you want to scan these pages, provide the following information.		
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 want to include in the scan	You can add a maximum of five links. Click to add links and to remove them.
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. A maximum of five request headers can be added. Click to add HTTP request headers and click to remove them.		
Name	Name of an HTTP request header	Example: **Cookie**

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.

  NOTE

  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

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.

NOTE

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

Figure 5-5 Scan details

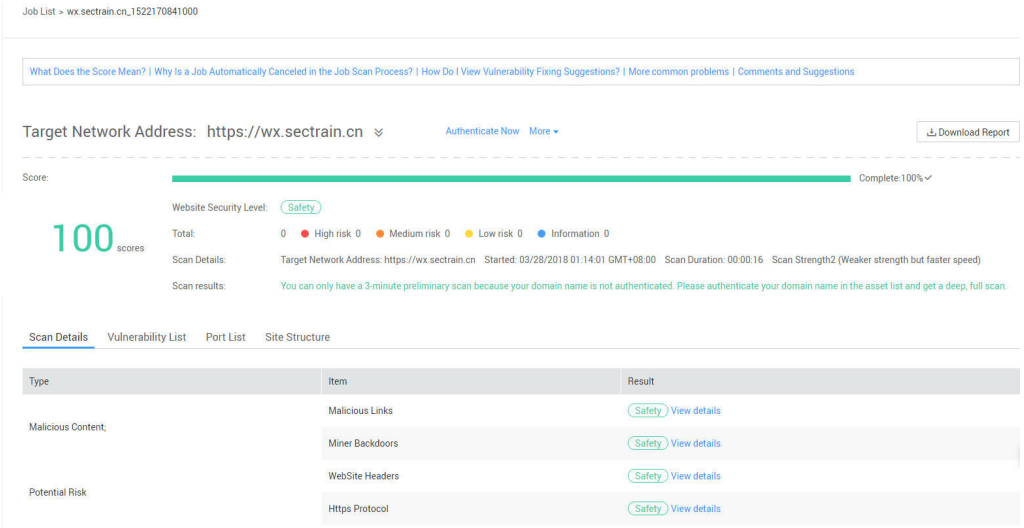


Table 5-3 Parameter description

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 medium- and high-risk), click View details to check the risk.

Figure 5-6 Scan Details

Scan Details | Vulnerability List | Port List | Site Structure

Type	Item	Result
Malicious Content;	Malicious Links	Safety View details
	Miner Backdoors	Safety View details
Potential Risk	WebSite Headers	Safety View details
	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 | Port List | Site Structure

View

Vulnerability ID	Discovered	Level	Status	Type	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

NOTE

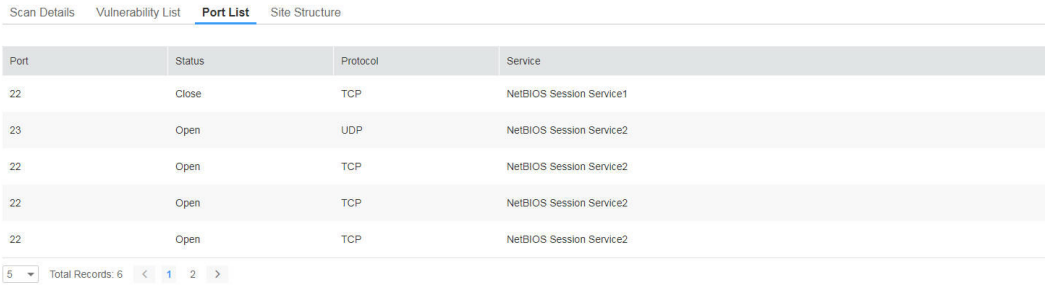
Shows vulnerabilities detected in a job. One page displays five entries. You can go to the next page for more entries.

- 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



Step 8 Click the **Site Structure** tab.

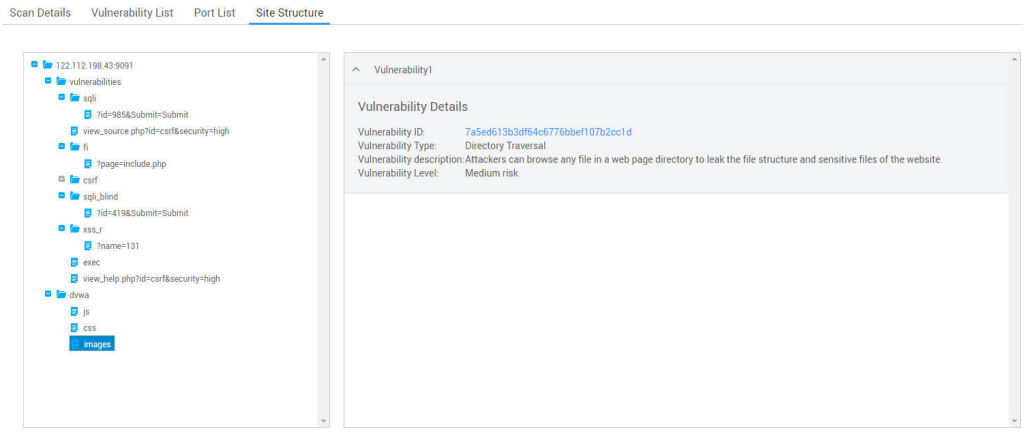
NOTE

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



----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.

NOTE

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

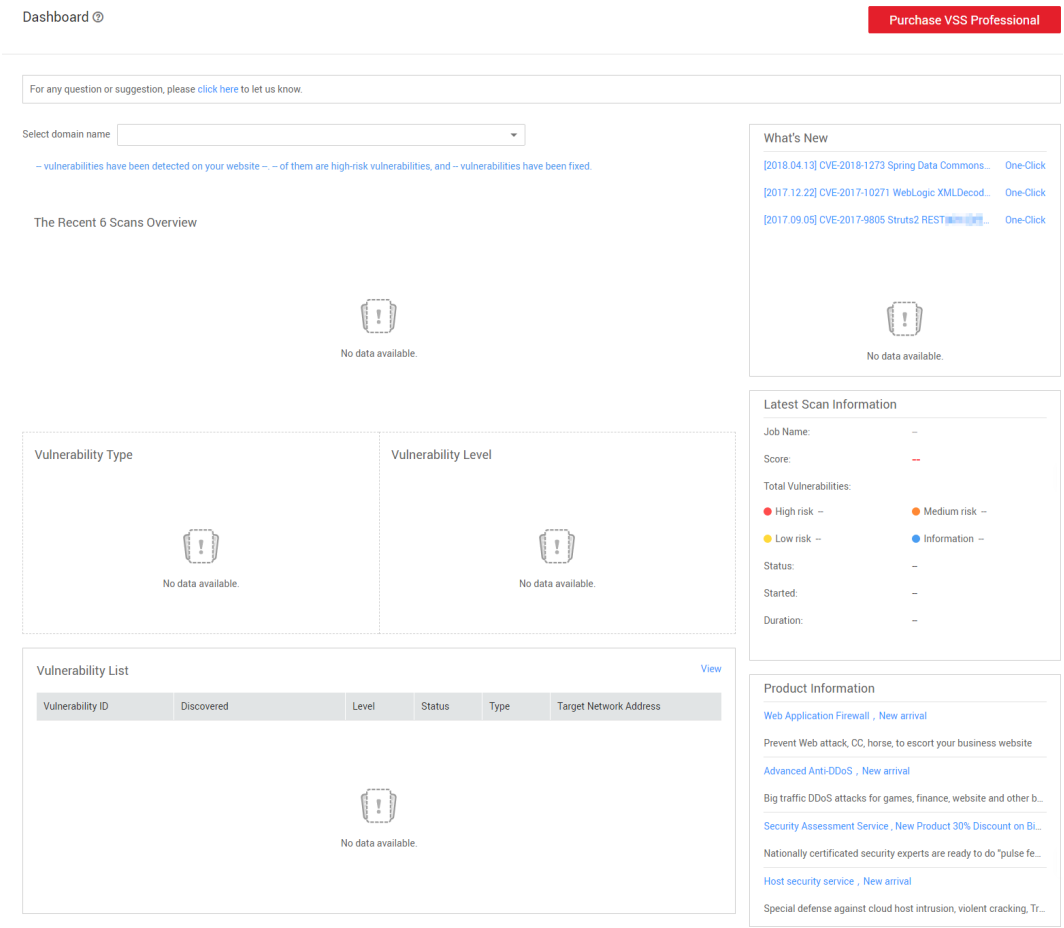


Table 6-1 Page description

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.
Vulnerability 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
Vulnerability 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 Information	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 Information	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.

NOTE

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
Type	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

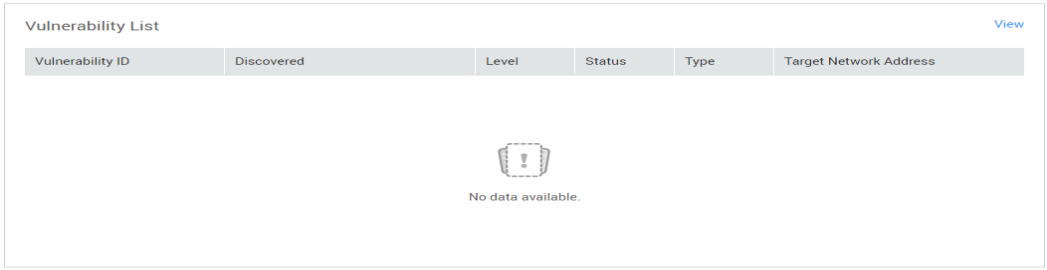
Step 1 Log in to the management console.

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



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

Figure 6-4 Vulnerability Details

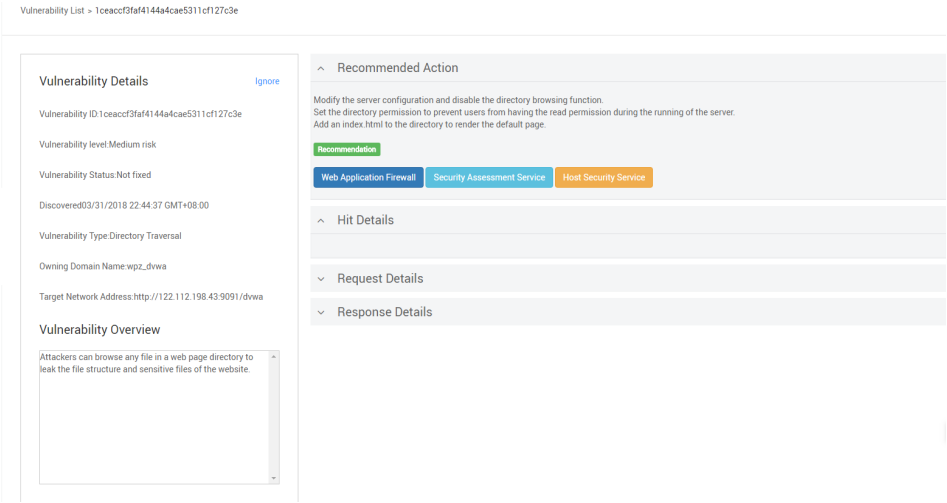


Table 6-3 Parameter description

Area	Description	Operation
Vulnerability 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.
Recommended 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

----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.

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.

Prerequisites

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

Procedure

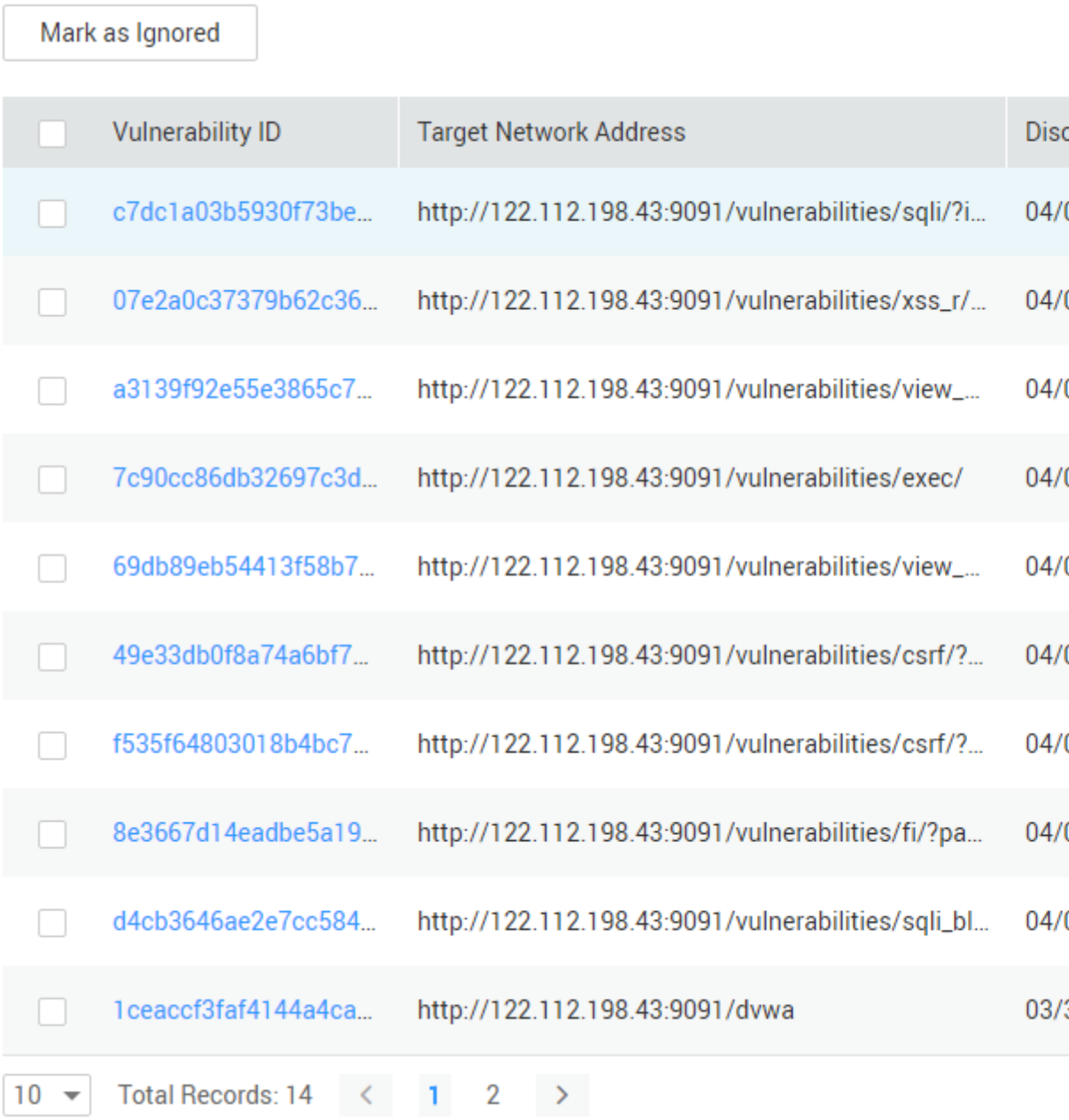
Step 1 Log in to the management console.

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



NOTE

- 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

A Change History

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.