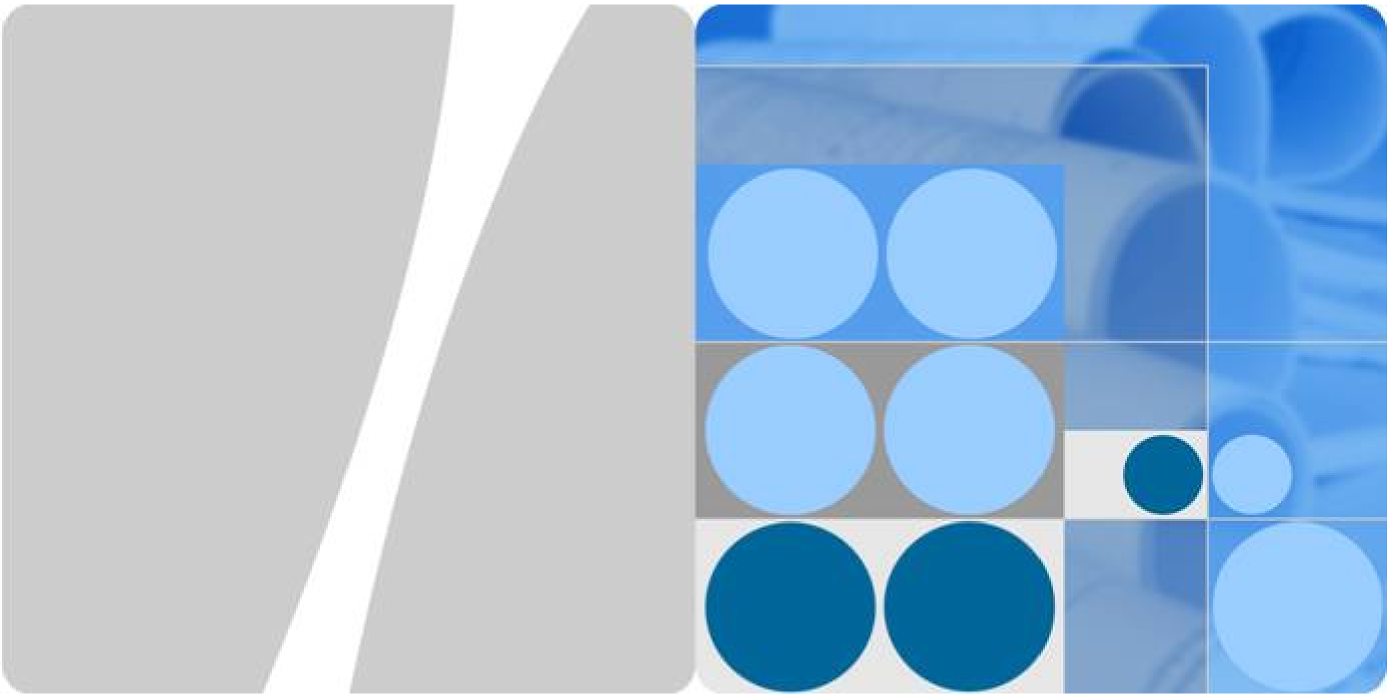


Vulnerability Scan Service

FAQ

Issue	**03**
Date	**2019-07-12**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 About Operations

1.1 Which Websites Are not Supported by VSS?

VSS does not support websites that are not accessible or do not comply with laws and regulations.

A website meeting any of the following conditions does not support VSS:

- Websites that do not have Internet Content Provider (ICP) registration number.
- Websites that cannot be opened or do not have enough content for VSS to determine their scope of operation.
- Websites that have threats or illegal information on their web pages.
- Hospital websites not certified by the Ministry of Health.
- Websites primarily contain pornographic content (video dating and one night stand), illegal content (making fake certificates and selling simulation guns), hackers (non-technical exchange websites), phishing websites, private game servers, game plug-ins, websites that make money online (pyramid sale websites), adult products, health care products (diet pills), bisexual content, obscene pictures of beauties and cartoons, as well as gambling (including sale of gambling tools).
- Websites contain malicious advertisements, video links of illegal content, and links of illegal websites.
- Websites contain copyright risk content, including video, novel, and music websites.
- Websites involve sales of medicines and health care products that obtain no qualification or overstate effects.
- Websites that serve as payment and transaction platforms, provide guarantee for illegal websites, or sell non-China financial (stock, physical, and gold trading) services.
- Websites contain a lot of content that has impact on social harmony and stability, for example, attacking the nation, leaders, and people, and promoting seditious speech.

1.2 How Do I Authenticate the Domain Name of a Website?

Perform the following operations:

Step 1 Log in to the management console.

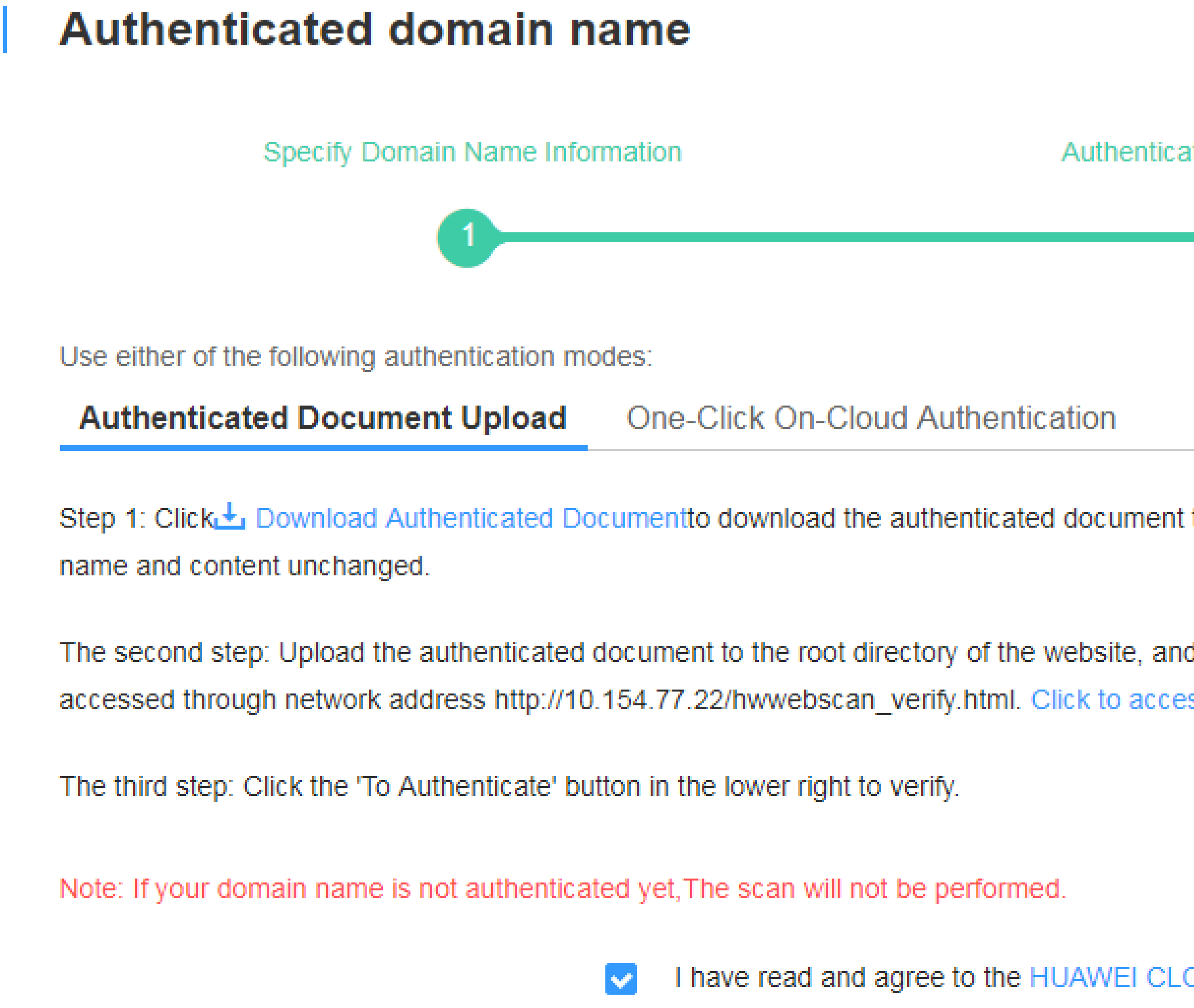
Step 2 Choose **Security** > **Vulnerability Scan Service** > **Asset List**.

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 1-1 Uploading an authenticated document



Authenticated domain name

Specify Domain Name Information

Authentica

1

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

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 acces

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 CLO

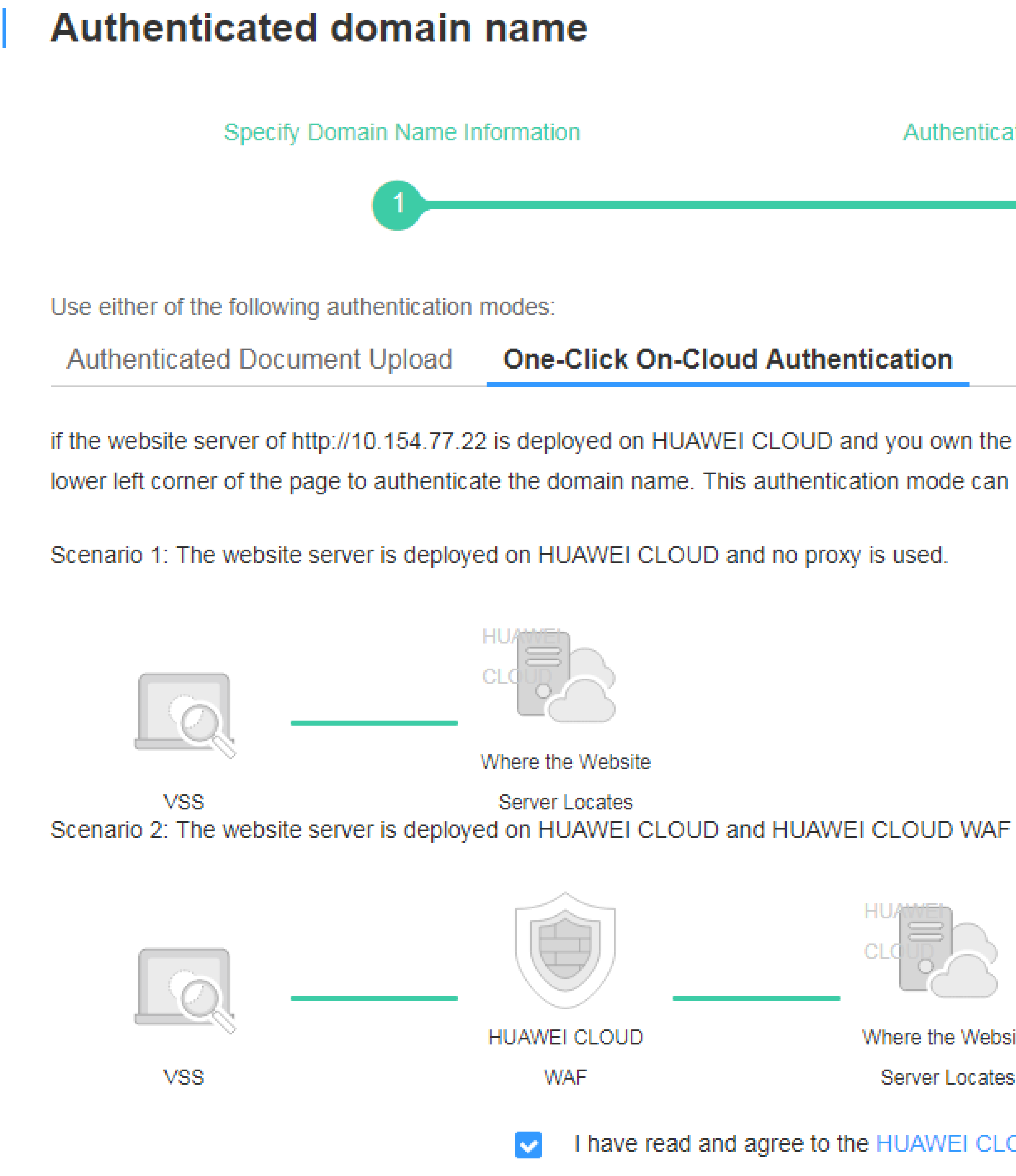
1. Click **Download Authenticated Document**.
2. Upload the document to the root directory of the website and ensure that the following network address can be accessed: **target network address/hwwebscan_verify.html**.

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 1-2 One-click on-cloud authentication



Authenticated domain name

Specify Domain Name Information

Authentica

1

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.

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

☑ I have read and agree to the HUAWEI CLC

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

1.3 How Do I Upload an Authentication Document to the Root Directory of a Website?

During domain name authentication, you need to upload the downloaded authentication file to the root directory of the website (that is, the directory at the same level as the index file on the homepage). The file upload location varies according to the server used by the user. To upload the authentication file, perform the following steps.

Tomcat, Apache, and IIS Servers

Perform the following steps:

Step 1 Log in to your web server.

If you are not the **root** user, run the **su -root** command to switch to the **root** user.

Step 2 Locate the root directory of the server, that is, the directory at the same level as the **index** file. **Table 1-1** lists the root directories of common servers.

Table 1-1 Root directories of common servers

Server Used by a Website	Root Directory
Tomcat	*Tomcat deployment address*/**webapps/ROOT/**
Apache	The default value is **/var/www/html**. Set the directory based on the site requirements.
IIS	The default value is **C:\inetpub\wwwroot**. Set the directory based on the site requirements.

Step 3 Save the authentication document to the directory found in **Step 2**.

NOTE

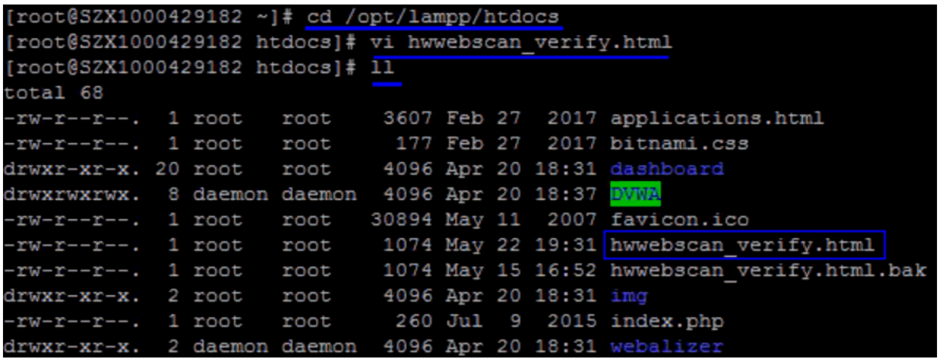
The directory must be in the same level as the **index** file.

Example:

1. Run the **cd root directory** command to go to the root directory of the server.
2. Run the **vi hwwebscan_verify.html** command to create a file with the same name as the authentication file.
3. Run **i** to enter the edit mode.

   Paste the content of the authentication file here.
4. Press **Esc** to exit the editing mode, and then run the **:wq** command to save the settings and exit.
5. Run **ll** to check whether the authentication file is successfully uploaded.

Figure 1-3 Example



```
[root@SZX1000429182 ~]# cd /opt/lampp/htdocs
[root@SZX1000429182 htdocs]# vi hwwebscan_verify.html
[root@SZX1000429182 htdocs]# ll
total 68
-rw-r--r--.  1 root   root    3607 Feb 27  2017 applications.html
-rw-r--r--.  1 root   root     177 Feb 27  2017 bitnami.css
drwxr-xr-x. 20 root   root    4096 Apr 20 18:31 dashboard
drwxrwxrwx.  8 daemon daemon  4096 Apr 20 18:37 DVWA
-rw-r--r--.  1 root   root   30894 May 11  2007 favicon.ico
-rw-r--r--.  1 root   root    1074 May 22 19:31 hwwebscan_verify.html
-rw-r--r--.  1 root   root    1074 May 15 16:52 hwwebscan_verify.html.bak
drwxr-xr-x.  2 root   root    4096 Apr 20 18:31 img
-rw-r--r--.  1 root   root     260 Jul  9  2015 index.php
drwxr-xr-x.  2 daemon daemon  4096 Apr 20 18:31 webalizer
```

Step 4 Enter *domain name*/**hwwebscan_verify.html** in the address box of the browser to check whether the authentication file is uploaded. If the file can be accessed, the upload is successful.

----End

Nginx Servers

Perform the following steps to redirect the access to hwwebscan_verify.html to a local file:

Step 1 Log in to the Nginx server.

If you are not the **root** user, run the **su -root** command to switch to the **root** user.

Step 2 Upload the authentication document to any directory (the Nginx process only has the read permission on this directory). The following uses the **/opt/mock** directory as an example.

Example:

1. Run the **cd /opt/mock** command to open the **/opt/mock** directory.
2. Run the **vi hwwebscan_verify.html** command to create a file with the same name as the authentication file.
3. Run **i** to enter the edit mode.

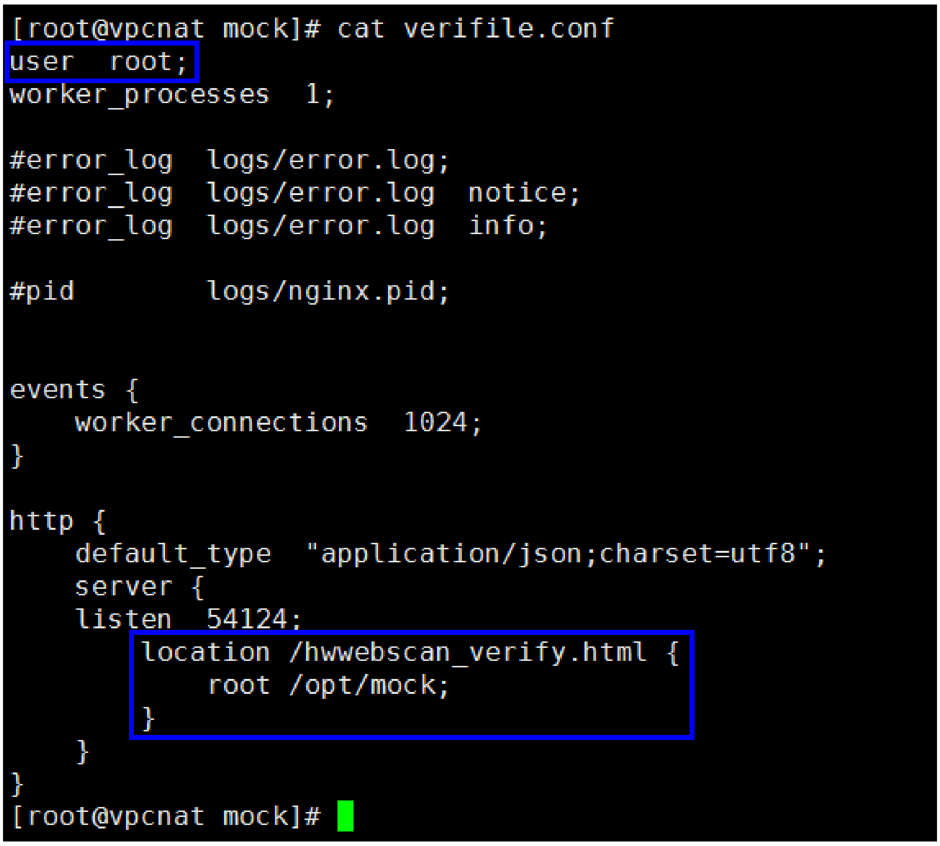
   Paste the content of the authentication file here.
4. Press **Esc** to exit the editing mode, and then run the **:wq** command to save the settings and exit.

Step 3 Open the **nginx.conf** file and configure the location information of the HTTP module of Nginx. After the configuration is successful, you can read the authentication file from the **/opt/mock** directory.

1. Run the **vi nginx.conf** command to open the **nginx.con** file.
2. Modify the following content based on the site requirements and overwrite the original HTTP module. See **Figure 1-4**.

```
http {
default_type "application/json;charset=utf-8";
server {
Replace listen ${your website port};# with the actual value.
location /hwwebscan_verify.html {
${user}  /opt/mock;
}
}
}
```

Figure 1-4 Configuration of location information



```
[root@vpcnat mock]# cat verifile.conf
user  root;
worker_processes  1;

#error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;

#pid        logs/nginx.pid;


events {
    worker_connections  1024;
}

http {
    default_type  "application/json;charset=utf8";
    server {
    listen  54124;
        location /hwwebscan_verify.html {
            root /opt/mock;
        }
    }
}
[root@vpcnat mock]#
```

Step 4 Run the **nginx -s reload** command to update the configuration.

Step 5 Enter *domain name*/**hwwebscan_verify.html** in the address box of the browser to check whether the authentication file is uploaded. If the file can be accessed, the upload is successful.

----End

1.4 Why Does Domain Name Authentication Fail?

Why Is Domain Name Authentication Required?

Different from conventional scanning tools, VSS assessments are performed based on automatic penetration testing, that is, sending non-malicious **attack packets** to the target. Therefore, ensure that you own the website to be scanned.

Authentication Methods Supported by VSS

- **Document Authentication**: upload the authentication document to the root directory of the website.
- **One-Click Authentication**: for tenants on HUAWEI CLOUD

Reasons for Failure of Document Authentication

- The authentication document is not saved in the root directory of the website.

Upload the authentication document to the root directory of the website by referring to **How Do I Upload an Authentication Document to the Root Directory of a Website?** and perform authentication again.

- Failed to obtain the certificate file.

  The possible causes are as follows:

  - The website is unavailable. Access **http://{your website}/hwwebscan_verify.html**. If the website cannot be accessed, the website is unavailable.
  - The website is using Web Application Firewall (WAF). Whitelist the VSS IP addresses. For details, see **What Should I Do When a Website Scan Fails with a Message Displayed Indicating Connection Timeout?**.
  - The certificate file is placed in the wrong directory or the website is mapped. In this case, error code 404 is returned when accessing the certificate file. Place **hwwebscan_verify.html** in the directory as the same level as **index.php/index.jsp/index.html** and then access the certificate file again.

- Failed to verify the certificate.

  If the system displays a message indicating that certificate verification fails, the certificate file can be accessed.

  The possible causes are as follows:

  - The certificate content is incorrect. Check whether the content of the uploaded **hwwebscan_verify.html** file is consistent with that obtained from accessing **http://{your website}/hwwebscan_verify.html**. If not, delete the **hwwebscan_verify.html** file, and download and upload it again. Then check whether you are verified for the website. If the verification still fails, you are advised to view the source code of the **http://{your website}/hwwebscan_verify.html** page (right-click **View page source**). If the tag information is displayed, the uploaded certificate file has been tampered with.

    NOTE

    - You are advised to place the **hwwebscan_verify.html** file in the same directory as the index file. Do not copy and paste the file content.

  - The website is using Web Application Firewall (WAF). Whitelist the VSS IP addresses. For details, see **What Should I Do When a Website Scan Fails with a Message Displayed Indicating Connection Timeout?**.

- The domain name information does not comply with rules and regulations.

  This type of website cannot use VSS. For details, see **Which Websites Are not Supported by VSS?**.

Reasons for Failure of One-Click Authentication

One-click authentication applies only to the following two types of users:

- Users who are using WAF
- Users whose websites' EIPs are those of HUAWEI CLOUD North China, East China, South China, and Northeast China

The possible causes are as follows:

- You are not one of the two types of users.
- You are a WAF user but WAF and VSS are not subscribed using the same account, the authentication fails because only the WAF account can be used to view the back-to-source IP address of WAF.

- The EIP to be scanned is not purchased using the VSS account.
- The domain name information does not comply with rules and regulations.

  This type of website cannot use VSS. For details, see **Which Websites Are not Supported by VSS?**.

1.5 What Should I Do When a Website Scan Fails with a Message Displayed Indicating Connection Timeout?

The possible causes and solutions are as follows:

1. Your website is unstable. Open the website and check whether the connection is normal. Try scanning again.
2. Your website cannot be accessed from the Internet.
3. A firewall or another security policy has been configured for your website. As a result, the IP addresses of VSS (49.4.54.27, 49.4.8.50, 114.116.12.185, 114.115.159.33, 114.116.50.141, 114.116.50.142, 114.116.91.55, 114.115.175.79, 117.78.49.197, 117.78.49.29, 114.115.215.94, 114.115.211.231, 114.115.168.226, 114.115.129.201, 117.78.41.118, 117.78.41.126, 117.78.46.77, and 43.254.3.176) are mistakenly intercepted. Whitelist these IP addresses.

   NOTE

   If your website cannot be accessed, check whether it is working properly. If you have any questions, feel free to send your problem on the VSS console.

1.6 What Should I Do If a Website Scan Job Fails to Be Created or Restarted?

Perform the following operations:

Step 1 Log in to the management console.

Step 2 Click **Service List** at the top of the page and choose **Security** > **Vulnerability Scan Service**. In the navigation pane, choose **Asset List**. The **Asset List** page is displayed. Check whether the domain name has been authenticated.

- If yes, contact technical support.
- If no, perform **Step 3** to **4** to authenticate the domain name.

Step 3 In the **Authentication Status** column of the target domain name, click **Authenticate Now**.

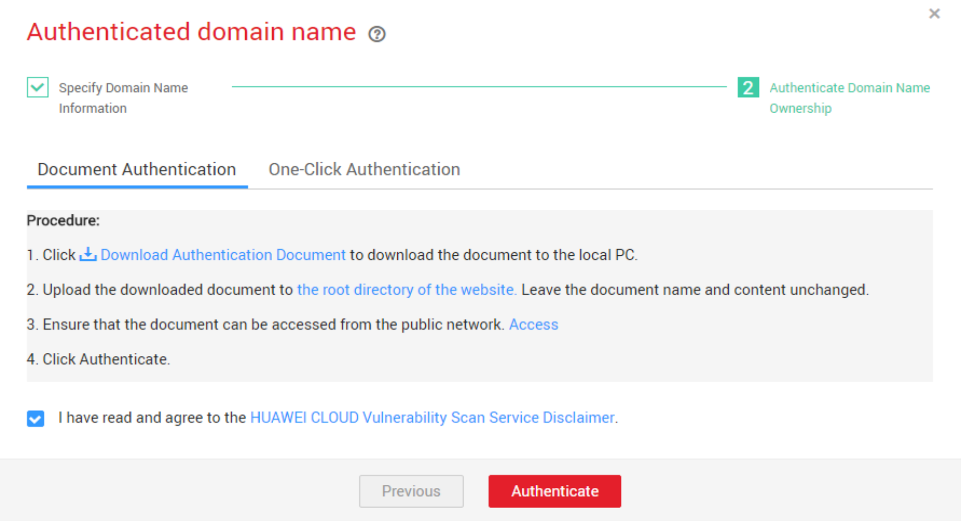
Step 4 In the **Authentication Status** column of the target domain name, click **Authenticate Now**. In the displayed **Authenticate Domain Name** dialog box, select an authentication method to complete domain authentication.

NOTE

If the server of your site to be detected is deployed on HUAWEI CLOUD and you own the server, you can select one-click authentication.

- Document authentication. See **Figure 1-5**.

Figure 1-5 Document authentication



Authenticated domain name

☑ Specify Domain Name Information

2 Authenticate Domain Name Ownership

Document Authentication | One-Click Authentication

Procedure:

1. Click Download Authentication Document to download the document to the local PC.

2. Upload the downloaded document to the root directory of the website. Leave the document name and content unchanged.

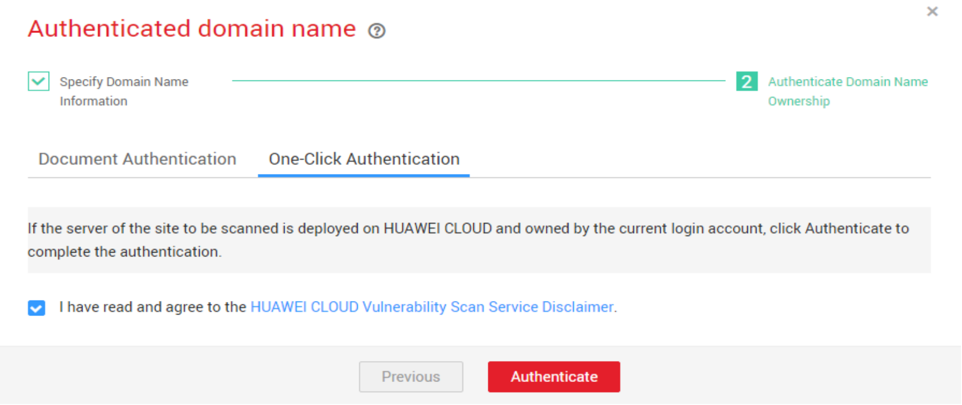
3. Ensure that the document can be accessed from the public network. Access

4. Click Authenticate.

☑ I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer.

- One-click authentication. See **Figure 1-6**.

Figure 1-6 One-click authentication



Authenticated domain name

☑ Specify Domain Name Information

2 Authenticate Domain Name Ownership

Document Authentication | One-Click Authentication

If the server of the site to be scanned is deployed on HUAWEI CLOUD and owned by the current login account, click Authenticate to complete the authentication.

☑ I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer.

Select **I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Disclaimer**, click **Authenticate**. The domain name is in the **Authenticated** status if authentication succeeds.

----End

1.7 Can the Authenticated Document in the Root Directory of the Website Be Deleted After Domain Name Authentication Is Complete?

No. VSS will read this document during subsequent scanning and check whether the ownership of the website is still valid.

If the authenticated document is deleted, a failure message is displayed when the domain name is scanned again.

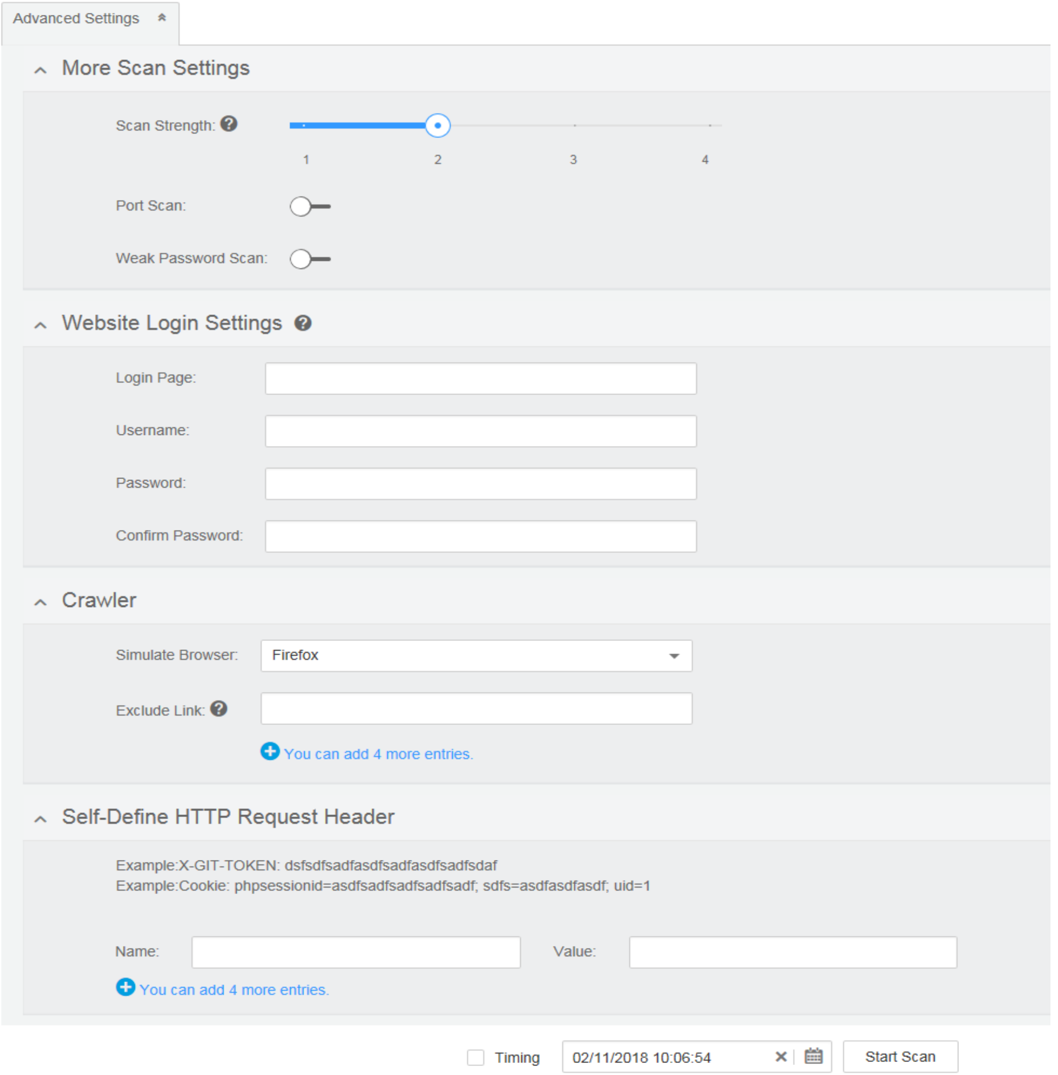
1.8 When Are Advanced Scan Settings Required?

Advanced scan settings can be performed for special website pages that:

- Require port scan or weak password scan.
- Can only be accessed after authentication (username and password).
- Do not need to scan.
- Can only be accessed after a verification code is entered.

Figure 1-7 shows the advanced settings page. Table 1-2 describes the parameters.

Figure 1-7 Advanced settings



Simulate Browser: Firefox

Example:X-GIT-TOKEN: dsfsdfsadfasdfsadfasdfsadfsdaf
Example:Cookie: phpsessionid=asdfsadfsadfsadfsadf; sdfs=asdfasdfasdf; uid=1

□ Timing 02/11/2018 10:06:54

Table 1-2 Advanced settings parameters

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 for logging in to the website	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	A maximum of five links can be added. 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. You can add a maximum of five request headers. Click ⊕ to add headers and ⊖ 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**

1.9 Why Do I Fail to Buy VSS?

You may not have the required permission. Check your permissions.

To buy VSS, you must have the **te_admin**, **bss_adm**, **bss_pay**, or **bss_ops** permissions. To apply for such permissions, contact a user with Tenant Administrator permissions. For details, see *Identity and Access Management User Guide*.

1.10 How Long Does a Scan Take?

Duration of a website scan depends on the website size. Typically, scanning a 200-page website takes approximately 30 minutes.

A certain number of detection requests are sent to the website being scanned, slightly increasing website load.

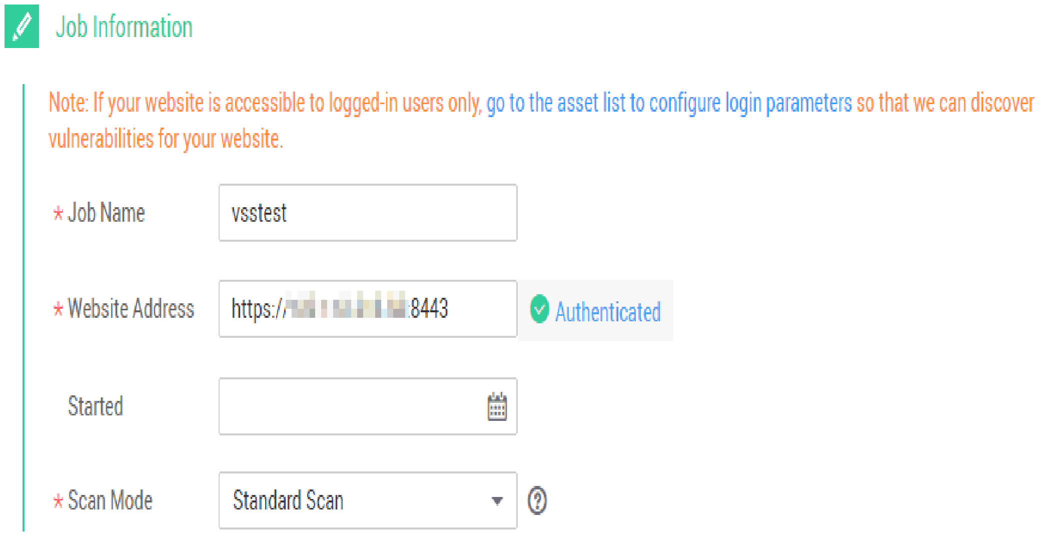
1.11 How Do I Set a Scheduled Scan?

When creating a job, set **Started**. The system will start the job at the set time. See **Figure 1-8**.

NOTE

The start time must be within the coming one week.

Figure 1-8 Setting a scheduled scan job



Job Information

Note: If your website is accessible to logged-in users only, go to the asset list to configure login parameters so that we can discover vulnerabilities for your website.

* Job Name: vsstest

* Website Address: https:/[redacted]8443 ✓ Authenticated

Started:

* Scan Mode: Standard Scan ▾

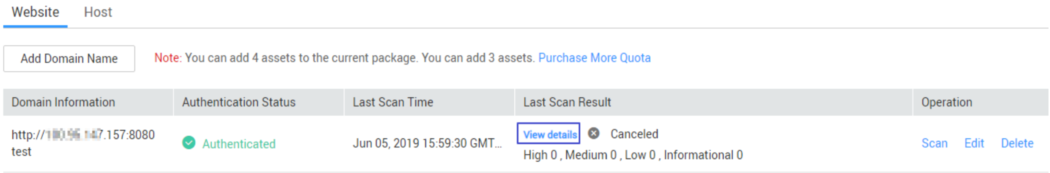
1.12 How Do I View Vulnerability Fixing Suggestions?

To view suggestions on how to fix website vulnerabilities, perform the following steps:

Step 1 Log in to the management console.

Step 2 In the navigation pane, choose **Asset List**. On the displayed page shown in **Figure 1-9**, click the **Website** tab. **Table 1-3** describes the related parameters.

Figure 1-9 List of websites



Website Host

Add Domain Name

Note: You can add 4 assets to the current package. You can add 3 assets. Purchase More Quota

Domain Information	Authentication Status	Last Scan Time	Last Scan Result	Operation
http://[redacted]7.157:8080 test	✓ Authenticated	Jun 05, 2019 15:59:30 GMT...	View details ⊗ Canceled High 0 , Medium 0 , Low 0 , Informational 0	Scan Edit Delete

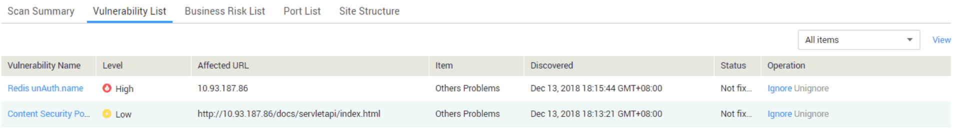
Table 1-3 Parameter description

Parameter	Description
Domain Information	● Domain name/IP address ● Customizable name for a domain
Authentication Status	● **Authenticated** The target domain name has been authenticated. ● **Not authenticated** The target domain name has not been authenticated. Click **Authenticate**. ● **Certificate expired** If the certificate is invalid, download the certificate file again and complete domain authentication.
Last Scan Time	Time when the last scan job begins
Last Scan Result	Information about the last scan job, including the score and number of vulnerabilities at each level. Click the score or **View details** to view scan details.

Step 3 In the **Last Scan Result** column of the target website, click the score or **View Details**. The job details page is displayed.

Step 4 Click the **Vulnerability List** tab. The **Vulnerability List** tab page is displayed, as shown in **Figure 1-10**.

Figure 1-10 Vulnerability List tab page



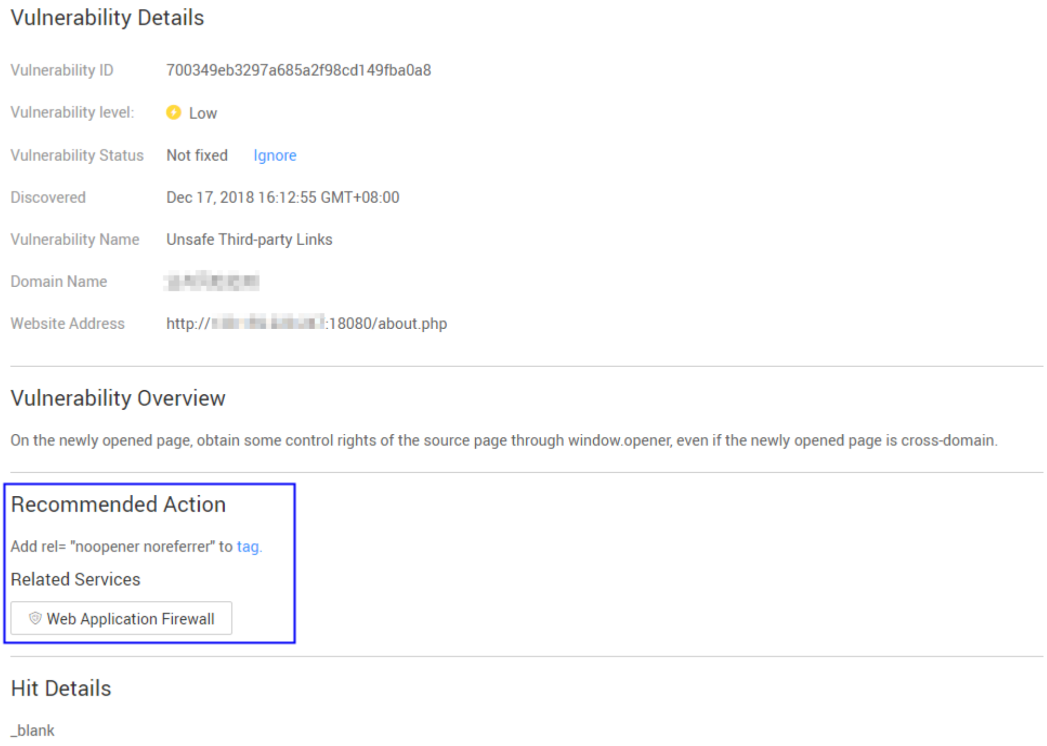
Scan Summary Vulnerability List Business Risk List Port List Site Structure

All items View

Vulnerability Name	Level	Affected URL	Item	Discovered	Status	Operation
Redis unAuth.name	High	10.93.187.86	Others Problems	Dec 13, 2018 18:15:44 GMT+08:00	Not fix...	Ignore Unignore
Content Security Po...	Low	http://10.93.187.86/docs/servletapi/index.html	Others Problems	Dec 13, 2018 18:13:21 GMT+08:00	Not fix...	Ignore Unignore

Step 5 Click a vulnerability name to view **Vulnerability Details**, **Vulnerability Overview**, and **Recommended Action**. See **Figure 1-11**.

Figure 1-11 Vulnerability details



Vulnerability Details

Vulnerability ID	700349eb3297a685a2f98cd149fba0a8
Vulnerability level:	● Low
Vulnerability Status	Not fixed Ignore
Discovered	Dec 17, 2018 16:12:55 GMT+08:00
Vulnerability Name	Unsafe Third-party Links
Domain Name	[redacted]
Website Address	http://[redacted]:18080/about.php

Vulnerability Overview

On the newly opened page, obtain some control rights of the source page through window.opener, even if the newly opened page is cross-domain.

Recommended Action

Add rel= "noopener noreferrer" to tag.

Related Services

Hit Details

_blank

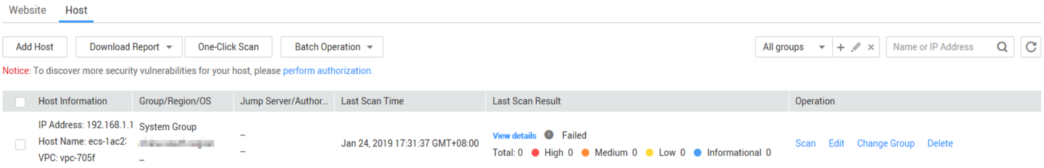
----End

To view suggestions on how to fix host vulnerabilities, perform the following steps:

Step 1 Log in to the management console.

Step 2 In the navigation pane, choose **Asset List**. On the displayed page, click the **Host** tab. See **Figure 1-12**.

Figure 1-12 Host tab page

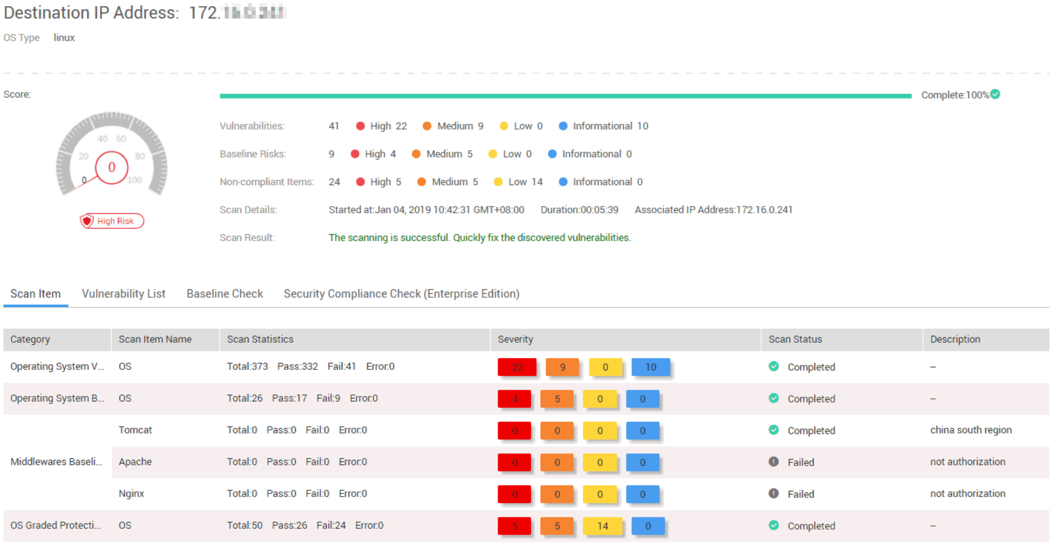


Notice: To discover more security vulnerabilities for your host, please perform authorization.

□	Host Information	Group/Region/OS	Jump Server/Author...	Last Scan Time	Last Scan Result	Operation
□	IP Address: 192.168.1.1 Host Name: ecs-1ac2: VPC: vpc-705f	System Group [redacted] –	– –	Jan 24, 2019 17:31:37 GMT+08:00	View details ● Failed Total: 0 ● High 0 ● Medium 0 ● Low 0 ● Informational 0	Scan Edit Change Group Delete

Step 3 In the **Last Scan Result** column of the target server, click the score or **View details**. The job details page is displayed.

Figure 1-13 Job details page



Destination IP Address: 172.[redacted]

OS Type linux

Score:

Complete:100%

Vulnerabilities: 41 ● High 22 ● Medium 9 ● Low 0 ● Informational 10

Baseline Risks: 9 ● High 4 ● Medium 5 ● Low 0 ● Informational 0

Non-compliant Items: 24 ● High 5 ● Medium 5 ● Low 14 ● Informational 0

Scan Details: Started at:Jan 04, 2019 10:42:31 GMT+08:00 Duration:00:05:39 Associated IP Address:172.16.0.241

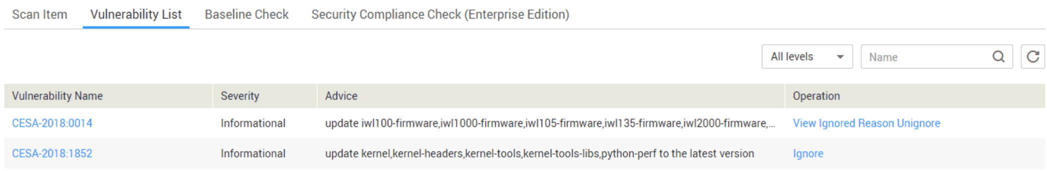
Scan Result: The scanning is successful. Quickly fix the discovered vulnerabilities.

Scan Item | Vulnerability List | Baseline Check | Security Compliance Check (Enterprise Edition)

Category	Scan Item Name	Scan Statistics	Severity	Scan Status	Description
Operating System V...	OS	Total:373 Pass:332 Fail:41 Error:0	22 9 0 10	✓ Completed	--
Operating System B...	OS	Total:26 Pass:17 Fail:9 Error:0	4 5 0 0	✓ Completed	--
Middlewares Baseli...	Tomcat	Total:0 Pass:0 Fail:0 Error:0	0 0 0 0	✓ Completed	china south region
	Apache	Total:0 Pass:0 Fail:0 Error:0	0 0 0 0	! Failed	not authorization
	Nginx	Total:0 Pass:0 Fail:0 Error:0	0 0 0 0	! Failed	not authorization
OS Graded Protecti...	OS	Total:50 Pass:26 Fail:24 Error:0	5 5 14 0	✓ Completed	--

Step 4 Click the **Vulnerability List** tab. The **Vulnerability List** tab page is displayed, as shown in **Figure 1-14**.

Figure 1-14 Vulnerability List tab page



Scan Item | Vulnerability List | Baseline Check | Security Compliance Check (Enterprise Edition)

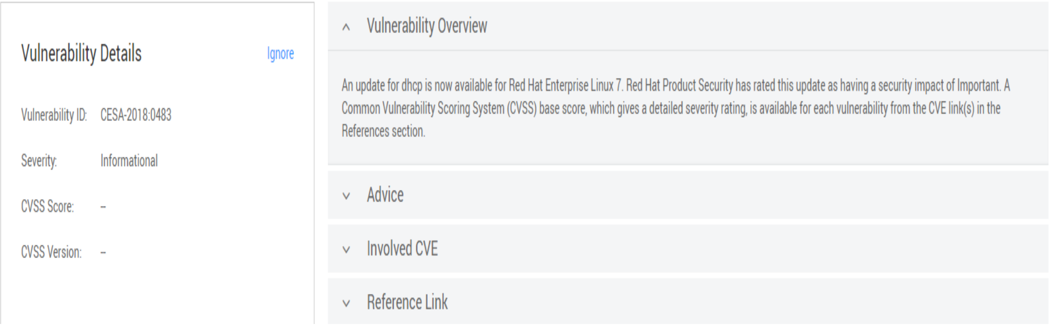
Vulnerability Name	Severity	Advice	Operation
CESA-2018:0014	Informational	update iwl100-firmware,iwl1000-firmware,iwl105-firmware,iwl135-firmware,iwl2000-firmware,...	View Ignored Reason Unignore
CESA-2018:1852	Informational	update kernel,kernel-headers,kernel-tools,kernel-tools-libs,python-perf to the latest version	Ignore

NOTE

To ignore a vulnerability, click **Ignore** in the **Operation** column of the target vulnerability.

Step 5 Click a vulnerability name. The vulnerability details page is displayed, as shown in **Figure 1-15**. You can rectify the vulnerability as recommended.

Figure 1-15 Vulnerability details



Vulnerability Details

Vulnerability ID: CESA-2018:0483

Severity: Informational

CVSS Score: -

CVSS Version: -

^ Vulnerability Overview

An update for dhcp is now available for Red Hat Enterprise Linux 7. Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

----End

2 About Pricing

2.1 Pricing

The VSS professional edition is billed by the number of domain names and duration.

For pricing details, see **Product Pricing Details**.

2.2 Renewing an Account

Scenario

This section describes how to renew VSS (professional edition) when it is about to expire. After the renewal, you can continue to use the VSS professional edition.

Prerequisites

You have obtained a username and its password to log in to the management console.

NOTE

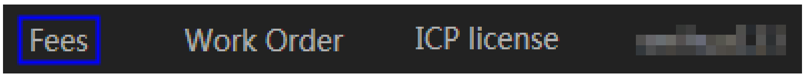
If you use a member account, grant the BSS Administrator permission to it so that you can renew the expired subscription using this member account.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Fees** in the upper right corner of the page.

Figure 2-1 Billing center entry



Step 3 In the navigation pane, choose **Renewal**.

Step 4 Complete the renewal as prompted on the corresponding page.

For details, see **Manually Renewing a Resource**.

----End

2.3 Unsubscribing from VSS

Scenarios

This section describes how to unsubscribe from VSS (professional edition).

Prerequisites

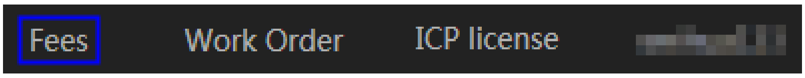
An account and its password have been obtained for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Fees** in the upper right corner of the page.

Figure 2-2 Billing center entry



Step 3 In the navigation pane, choose **Unsubscriptions and Changes** > **Unsubscriptions**.

Step 4 Complete the unsubscription operations as prompted on the corresponding page.

For details, see **Unsubscription Rules**.

----End