



漏洞扫描服务

常见问题

文档版本 03

发布日期 2019-07-12

华为技术有限公司



版权所有 © 华为技术有限公司 2019。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <http://e.huawei.com>

目录

1 操作类	1
1.1 哪些网站不能使用漏洞扫描服务？	1
1.2 如何对网站进行域名认证？	1
1.3 如何将认证文件上传到网站根目录？	3
1.4 为什么域名认证失败？	6
1.5 如何解决网站扫描失败报连接超时的问题？	7
1.6 创建网站扫描任务或重启任务不成功时如何处理？	7
1.7 域名认证完成后网站根目录下面的认证文件可以删除吗？	8
1.8 什么场景下需要进行高级扫描设置？	9
1.9 为什么购买漏洞扫描服务失败了？	10
1.10 网站漏洞扫描一次需要多久？	10
1.11 如何设置定时扫描？	11
1.12 如何查看漏洞修复建议？	11
2 计费类	15
2.1 价格体系	15
2.2 续费	15
2.3 退订	16

1 操作类

1.1 哪些网站不能使用漏洞扫描服务？

请确保网站可以正常访问，并且内容遵守国家相关法律法规。

符合以下任一条款的网站都不能使用漏洞扫描服务：

- 未取得ICP备案号的网站不允许使用。
- 网站打不开或无任何实际内容，导致无法判断网站运营范围的网站。
- 相关机构提示网页有威胁的，有非法信息的。
- 医院类型网站（流产，皮肤病，性病等医院），未获得卫生部资质的网站。
- 网站主体内容含有色情（视频交友，一夜情交友）、违法（办假证，贩卖仿真枪）、黑客（非技术交流网站）、钓鱼网站、游戏私服、游戏外挂、网赚（传销性质网站）、成人用品、保健用品（减肥药）、两性、美女贴图 and 动漫贴图（尺度过大）、赌博（含贩卖赌博工具）等低俗内容。
- 网站存在恶意流氓广告（存在非法内容视频链接，非法网页内容链接）。
- 网站内容存在版权风险的网站（视频，小说，音乐网站）。
- 网站含有药品销售、保健品销售，但未取得资质的，或严重夸大药效事实。
- 网站主要业务为向非法网站提供支付、交易平台、担保，代理中国以外金融理财（炒股，炒现货，炒黄金）等服务。
- 网站中大量存在影响社会和谐稳定的内容的网站（涉嫌攻击国家，攻击领导人，攻击人民，言论煽动性质的网站）。

1.2 如何对网站进行域名认证？

执行以下步骤进行域名认证：

步骤1 登录管理控制台。

步骤2 选择“安全 > 漏洞扫描服务 > 资产列表”，进入“资产列表”界面。

步骤3 在需要认证的域名所在行的操作列中，单击“前往认证”。

步骤4 弹出“认证域名”对话框，有两种域名认证方式，“上传证书认证”和“云上租户一键认证”。

方法一：选择“上传证书认证”，如[图1 上传证书失败](#)所示。

图 1-1 上传证书失败



1. 单击“下载认证文件”。
2. 将下载的认证文件上传到网站根目录，保证能成功访问链接“目标网址/hwwebscan_verify.html”。
3. 勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”。
4. 单击“完成认证”，进行域名认证。

执行完成后，该域名的状态为“已认证”。

方法二：选择“云上租户一键认证”，如[图2 云上租户一键认证](#)所示。

图 1-2 云上租户一键认证



勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”，单击“完成认证”，进行域名认证。

执行完成后，该域名的状态为“已认证”。

---结束

1.3 如何将认证文件上传到网站根目录？

域名认证时，需要将下载的认证文件上传到网站根目录（即网站首页index文件的同级目录下），然后进行认证。用户使用的服务器不同，文件上传的位置有所不同，请参照以下方法完成认证文件的上传。

Tomcat、Apache、IIS 服务器

如果网站所使用的服务器是Tomcat、Apache、IIS服务器，请执行以下操作步骤。

步骤1 登录网站所使用的服务器。

如果是非root用户，登录后，执行**su -root**命令切换到root用户。

步骤2 找到网站所使用的服务器的根目录，即“index”文件的同级目录。常见服务器的根目录如**表1-1**所示。

表 1-1 常见服务器的根目录

网站所使用的服务器	根目录
tomcat	tomcat的部署地址/webapps/ROOT/
apache	默认为“/var/www/html”，请以实际情况为准
IIS	默认为“C:\inetpub\wwwroot”，请以实际情况为准

步骤3 将认证文件保存在**步骤2**中找到的目录下。

 **说明**

以下的操作仅为示例，请以实际情况为准，总之，将认证文件放到“index”文件的同级目录即可。

示例：

1. 进入网站所使用的服务器的根目录：**cd** 根目录
2. 新建一个同域名认证文件同名的文件：**vi** hwwebscan_verify.html
3. 进入编辑模式：**i**
将准备好的认证文件内容粘贴到此处。
4. 保存并退出编辑模式：按Esc退出编辑，输入 **:wq**保存并退出。
5. 查看认证文件是否上传成功：**ll**

图 1-3 示例

```
[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 DWTB
-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
```

步骤4 在浏览器中输入“[目标网址/hwwebscan_verify.html](#)”，验证认证文件是否上传成功，如果能成功访问，则表示上传成功。

----结束

Nginx 服务器

如果网站所使用的服务器是Nginx，可以通过配置nginx.conf文件，将hwwebscan_verify.html的访问重定向到本地的某个文件，具体操作请执行以下步骤。

步骤1 登录Nginx服务器。

如果是非root用户，登录后，执行**su -root**命令切换到root用户。

步骤2 将认证文件上传到任意目录下（Nginx进程对此目录有只读权限）。以下以“/opt/mock”目录为例。

示例：

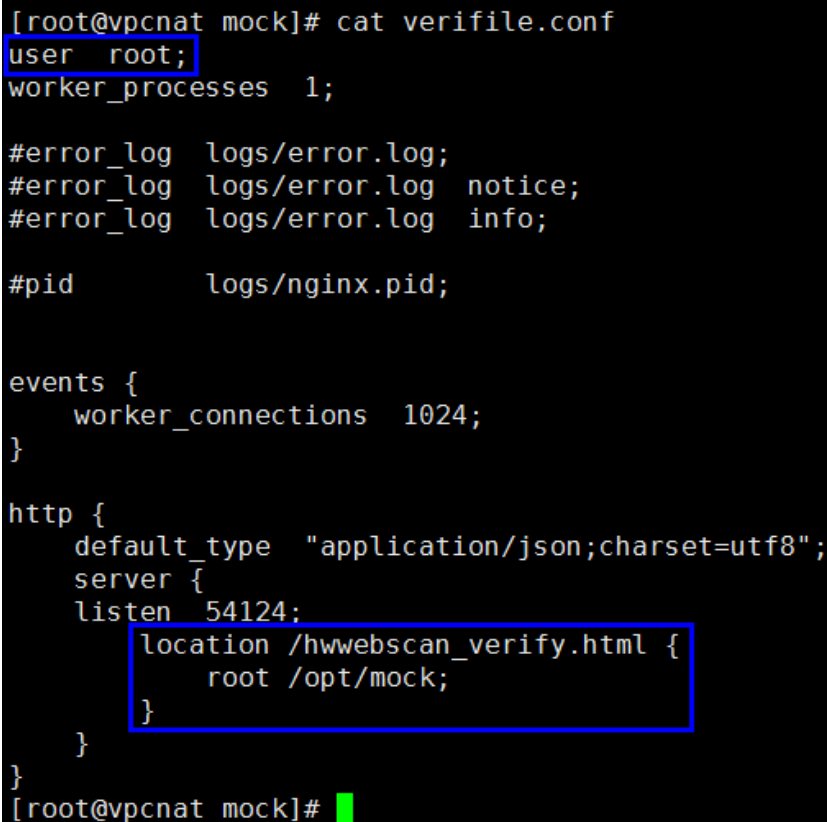
1. 打开任意目录：**cd /opt/mock**
2. 新建一个同域名认证文件同名的文件：**vi hwwebscan_verify.html**
3. 进入编辑模式：**i**
将准备好的认证文件内容粘贴到此处。
4. 保存并退出编辑模式：按Esc退出编辑，输入 **:wq**保存并退出。

步骤3 打开nginx.conf文件，配置Nginx的http模块的location信息，配置成功后，可以从“/opt/mock”目录下读取认证文件。

1. 找到并打开nginx.conf文件：**vi nginx.conf**
2. 根据具体场景，把以下的内容修改后替换nginx.conf的原http模块，如**图1-4**所示。

```
http {
    default_type "application/json;charset=utf-8";
    server {
        listen ${your website port};#根据具体场景替换
        location /hwwebscan_verify.html {
            ${user} /opt/mock;
        }
    }
}
```

图 1-4 配置 location 信息



```
[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;
        }
    }
}
```

步骤4 完成配置后执行命令**nginx -s reload**刷新配置。

步骤5 在浏览器中输入“*目标网址*/hwwebscan_verify.html”，验证认证文件是否上传成功，如果能成功访问，则表示上传成功。

---结束

1.4 为什么域名认证失败？


为什么要进行域名认证

华为云漏洞扫描服务不同于一般的扫描工具，因为VSS的扫描原理是基于自动化渗透测试（对被扫描的对象发送非恶意的“攻击报文”），因此需要确保用户扫描的网站的所有权是用户自己。

VSS 支持的认证方式

- 下载鉴权文件上传到网站根目录的“文件认证”方式。
- 华为云租户“一键认证”。

“文件认证”方式失败的原因

- 认证文件没有放在网站根目录下
请参照[如何将认证文件上传到网站根目录？](#)将认证文件放在网站根目录后重新进行认证。
 - 获取证书失败
获取证书失败一般有三种可能：
 - 网站不可用，单击访问“http://{your website}/hwwebscan_verify.html”该页面，如果不能正常访问，则表示该网站不可用。
 - 网站有Web应用防火墙之类的防护，需要将VSS的IP加入到网站访问的白名单中，具体方法请参见[如何解决网站扫描失败报连接超时的问题？](#)
 - 证书放错了位置或者网站做了映射，访问证书会返回404，请将 *hwwebscan_verify.html*放在与首页（*index.php/index.jsp/index.html*）的同级目录下，再访问证书。
 - 证书校验失败
错误提示“证书校验失败”说明已经可以访问证书文件了。
校验失败的原因一般有两种可能：
 - 证书内容不对，先比较自己上传的*hwwebscan_verify.html*的内容与访问“http://{your website}/hwwebscan_verify.html”获取到的内容是否一致，如果不一致，建议将已有的“hwwebscan_verify.html”文件删除，重新下载“hwwebscan_verify.html”文件后再重新上传，再次验证域名能否认证通过，如果仍然验证失败，建议查看“http://{your website}/hwwebscan_verify.html”该页面的页面源代码（右键单击“查看页面源代码”），如果出现标签信息，则说明上传的证书文件被篡改了。
-  **说明**
- 建议直接将*hwwebscan_verify.html*文件放入服务器首页index文件的同级目录，不要通过复制粘贴文件内容的方式传输证书，
 - 网站有Web应用防火墙之类的防护，需要将VSS的IP加入到网站访问的白名单中，具体方法请参见[如何解决网站扫描失败报连接超时的问题？](#)
- 域名信息违规
该类网站不能使用漏洞扫描服务，参见[哪些网站不能使用漏洞扫描服务？](#)查看哪些网站不能使用漏洞扫描服务。

华为云“一键认证”失败的原因

华为云一键认证的功能只针对两种用户：

- 使用了华为云WAF的用户。
- 客户要扫描的网址对应的EIP是华为云华北、华东、华南、东北局点的EIP。

因此认证失败可能有以下原因：

- 用户不是上述的两种用户。
- 用户是华为云WAF的用户，但该WAF和VSS不在一个账户下，则认证会失败，因为只有购买WAF的账户才能查看WAF的回源IP。
- 用户要扫描的EIP不是在该账户下购买的，因为系统是根据该账户去查询用户已经购买的EIP，然后和输入的EIP进行比对，所以不在同一个账号下无法一键认证。
- 域名信息违规
该类网站不能使用漏洞扫描服务，参见[哪些网站不能使用漏洞扫描服务？](#) 查看哪些网站不能使用漏洞扫描服务。

1.5 如何解决网站扫描失败报连接超时的问题？

网站报连接超时，可能原因与解决办法如下。

1. 您的网站不稳定，请打开网站，确认是否正常连接，再尝试重新扫描。
2. 您的网站无法在外网访问，导致漏洞扫描服务无法正常访问到您的网站，为您的网站进行安全扫描。
3. 您的网站设置了防火墙或其他安全策略，导致漏洞扫描的扫描IP（49.4.54.27，49.4.8.50，114.116.12.185，114.115.159.33，114.116.50.141，114.116.50.142，114.116.91.55，114.115.175.79，117.78.49.197，117.78.49.29，114.115.215.94，114.115.211.231，114.115.168.226，114.115.129.201，117.78.41.118，117.78.41.126，117.78.46.77，43.254.3.176）被当成恶意攻击者而误拦截，请您将漏洞扫描的扫描IP添加至网站访问的白名单中。

说明

您的网站无法访问，请您检查网站是否正常工作。如有疑问，欢迎在漏洞扫描服务控制台中进行快速反馈。

1.6 创建网站扫描任务或重启任务不成功时如何处理？

请执行以下步骤进行处理。

- 步骤1** 登录管理控制台。
- 步骤2** 单击页面上方的“服务列表”，选择“安全 > 漏洞扫描服务”，在左侧导航树中，选择“资产列表”，进入“资产列表”界面。查看目标网址是否已完成域名认证。
 - 如果是，请联系华为技术支持。
 - 如果不是，请执行[步骤3~4](#)完成域名认证。
- 步骤3** 在目标域名的“认证状态”列，单击“前往认证”。
- 步骤4** 在需要认证的域名所在行的“认证状态”列中，单击“去认证”，弹出的“认证域名”对话框，选择域名认证方式完成域名认证。

 说明

如果待检测站点的服务器搭建在华为云上，且该服务器是您当前登录账号的资产，才可以选择“一键认证”的方式进行快速认证，否则只能选择“文件认证”的方式进行认证。

- 文件认证，参照图1-5中的验证步骤完成域名认证。

图 1-5 文件认证方式



- 一键认证，如图1-6所示。

图 1-6 一键认证方式



勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”，单击“完成认证”，进行域名认证，执行完成后，该域名的状态为“已认证”。

---结束

1.7 域名认证完成后网站根目录下面的认证文件可以删除吗？

不可以。VSS在后续扫描过程中会读取该文件，验证网站的所有权是否仍然有效。

如果认证文件被删除，当再次对该域名进行扫描时，会提示失败。

1.8 什么场景下需要进行高级扫描设置？

对于有特殊要求的页面，可以进行高级扫描设置，例如：

- 需要进行端口扫描或弱密码扫描。
- 需要输入用户名和密码登录后才能访问的页面。
- 排除不需要扫描的页面。
- 需要输入验证码才能访问的页面。

高级扫描设置如[图1 高级设置](#)所示，相关参数请根据[表1 参数说明](#)进行设置。

图 1-7 高级设置

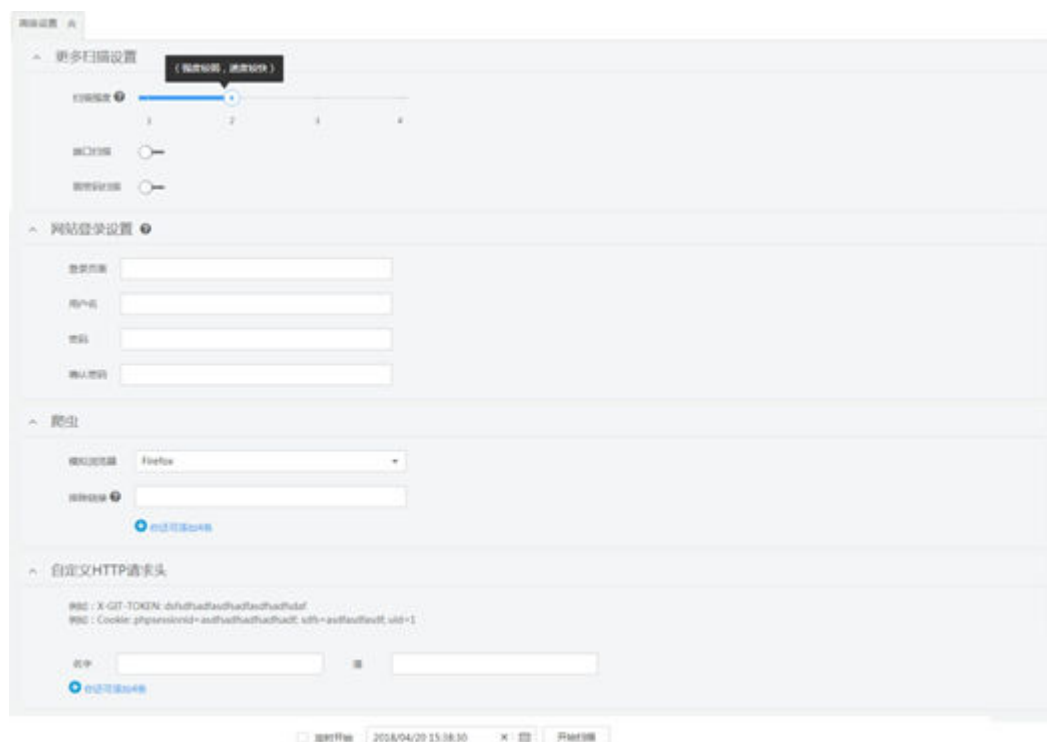


表 1-2 参数说明

参数	参数说明	设置
更多扫描设置		
扫描强度	扫描强度越高，检测能力越强，但是扫描耗时越久。	-
端口扫描	可以开启或关闭端口扫描。	<input checked="" type="checkbox"/> ：开启。
弱密码扫描	可以开启或关闭弱密码扫描。	<input type="checkbox"/> ：关闭。

参数	参数说明	设置
网站登录设置		
说明 登录后才可以访问的页面，需要提供该信息才能进行扫描。		
登录页面	网站登录页面的地址。	-
用户名	登录网站的用户名。	-
密码	用户名的密码。	-
确认密码		
爬虫设置		
模拟浏览器	爬虫所使用的浏览器。	根据下拉框进行选择，目前支持 Firefox 和 Chrome。
排除链接	可以排除不需要进行扫描的页面。	最多可以添加 5 个链接，单击  可以添加多个链接，单击  可以删除添加的链接。
自定义 HTTP 请求头		
说明 对于有其他特殊访问要求的页面（例如需要输入验证码的页面），请填写 HTTP 请求头。 最多可以添加 5 个请求头，单击  可以添加多个 HTTP 请求头，单击  可以删除添加的请求头。		
名字	HTTP 请求头的名字。	示例： <i>Cookie</i>
值	HTTP 请求头的值。	示例： <i>phpsessionid=asdfsadfsadfsadfsadf; sdfs=asdfsadfsadfsadfsadf; uid=1</i>

1.9 为什么购买漏洞扫描服务失败了？

购买失败，可能是权限不足，请检查用户权限。

用户需要拥有te_admin、bss_admin、bss_pay或bss_ops权限才能购买漏洞扫描服务。如需开通该权限，请联系拥有Tenant Administrator权限的用户，开通权限，详细内容请参见《统一身份认证服务用户指南》。

1.10 网站漏洞扫描一次需要多久？

网站漏洞扫描的时间受网站大小影响，一般200个页面的网站完成一次漏洞扫描耗时约30分钟。

扫描的过程中会向网站发送一定数量的检测请求，可能会导致网站的负载小幅度增大。


1.11 如何设置定时扫描？

在创建任务时，设置“开始时间”，设置好启动时间后，系统会在用户设置的时间点启动该任务，如图1-8所示。

说明

启动时间必须在一周之内。

图 1-8 定时开始

创建任务 

您目前正在体验漏洞扫描服务企业版，支持漏洞检测、业务威胁检测、主机漏洞扫描、基线合规检测。

填写扫描信息

提示：如果您的网站需要登陆才能设置，请前往资产列表设置登陆信息，以便我们能为您的网站进行更好的扫描。

* 任务名称	<input type="text" value="消费者云测试https代理"/>
* 目标网址	<input type="text" value="https://[IP]50-8443"/> 已认证
开始时间	<input type="text" value=""/> 
* 扫描模式	<input type="text" value="快速扫描"/> 

1.12 如何查看漏洞修复建议？

网站扫描查看漏洞修复建议的方法。

步骤1 登录管理控制台。

步骤2 在左侧导航树中，选择“资产列表”，进入“资产列表”界面，选中“网站”页签，查看网站资产列表，如图1-9所示，相关参数说明如表1-3所示。

图 1-9 网站资产列表

域名信息	认证状态	上一次扫描时间	上一次扫描结果	操作
新增域名 <small>温馨提示：您当前套餐共可添加1个资产，因计费模式升级，多余资产可按专业版规格正常使用。 购买更多扫描配额</small>				
http://[IP]200.8000 yiftest	已认证	2019/01/23 11:14:30 GMT+08:00	已失败 高危0个，中危0个，低危0个，提示0个	扫描 编辑 删除
http://[IP] 229.247:18080 业务风险检测	证书失效 去认证	2018/12/17 15:57:47 GMT+08:00	17分 已完成 高危0个，中危4个，低危21个，提示0个	扫描 编辑 删除

表 1-3 网站资产列表参数说明

参数	参数说明
域名信息	<ul style="list-style-type: none"> ● 域名/IP地址 ● 域名名称
认证状态	<ul style="list-style-type: none"> ● “已认证” 目标域名已完成域名认证。 ● “未认证” 目标域名未完成域名认证。单击“去认证”进行域名认证。 ● “证书失效” 如果证书失效，请重新下载证书文件并完成域名认证。
上次扫描时间	域名最近一次扫描任务的时间。
上一次扫描结果	域名最近一次扫描结果信息，包括得分和各等级的漏洞数量。单击分数或者“查看详情”，进入“扫描详情”界面查看扫描概况。

步骤3 在目标网站所在行的“上一次扫描结果”列，单击分数或者“查看详情”，进入“任务详情”界面。

步骤4 单击“漏洞列表”页签，进入“漏洞列表”界面，如图1-10所示。

图 1-10 漏洞列表



步骤5 单击漏洞名称，查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”，如图1-11所示，用户可以根据修复建议修复漏洞。

图 1-11 网站漏洞详情

漏洞详情

漏洞编号	73291d953babfc33f5f6d7c7e6d96344	漏洞等级	● 低危	漏洞状态	未修复 忽略
发现时间	2018/11/30 00:35:29 GMT+08:00	漏洞名称	内容安全策略	所属域名	ddd
目标网址	http://[redacted]200.8080/DVWA/login.php				

漏洞简介

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

修复建议

Content-Security-Policy是为了页面内容安全而制定的一系列防护策略，通过在响应头中配置Content-Security-Policy头以及相应的策略，可指定可信的内容来源，排除各种跨站点注入，包括跨站点脚本编制等建议搭配使用

🔗 Web应用防火墙 WAF

命中详情

Content-Security-Policy

请求详情

```
GET http://[redacted]200:8080/DVWA/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN;zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: 114.116.9.200:8080
```

响应详情

```
HTTP/1.1 200 OK
Date: Thu, 29 Nov 2018 16:20:39 GMT
Server: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2j PHP/7.0.18 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/7.0.18
```

----结束

主机漏洞扫描查看漏洞修复建议的方法。

步骤1 登录管理控制台。

步骤2 在左侧导航树中，选择“资产列表”，进入“资产列表”界面，选中“主机”页签，如图1-12所示。

图 1-12 主机列表

网站 主机

全部分组 + × 名称/IP Q C

温馨提示：为了能为您的主机发现更全面、完整的安全风险，请您对主机进行扫描授权

主机信息	所在分组/区域/操作...	跳板机/接收信息	上一次扫描时间	上一次扫描结果	操作
<input type="checkbox"/> IP: 192.168.1.122 主机名称: ecs-lac23f VPC: vpc-705f	系统分组	-	2019/01/24 17:31:37 GMT+08:00	查看详情 ● 已失败 漏洞总数: 0 ● 高危 0 ● 中危 0 ● 低危 0 ● 提示 0	扫描 编辑 更换分组 删除

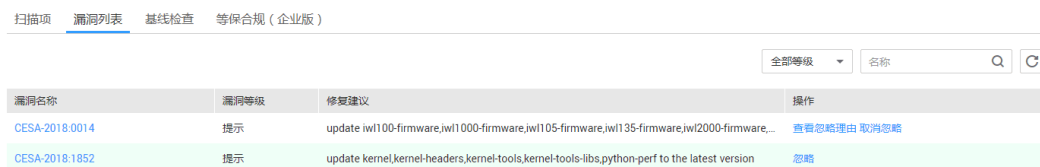
步骤3 在目标主机所在行的“上一次扫描结果”列，单击“分数”或者“查看详情”，进入“任务详情”界面，如图1-13所示。

图 1-13 查看主机扫描详情



步骤4 单击“漏洞列表”页签，进入“漏洞列表”的详情列表界面，如图1-14所示。

图 1-14 漏洞列表界面

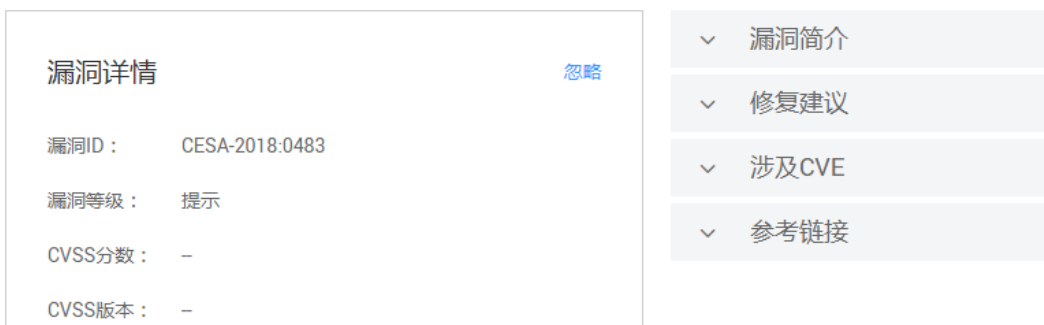


说明

在目标漏洞所在行的“操作”列，单击“忽略”，可以忽略该漏洞。

步骤5 单击漏洞名称，进入“漏洞详情”页面，查看漏洞修复建议，如图1-15所示，用户可以根据修复建议修复漏洞。

图 1-15 主机漏洞详情



----结束

2 计费类

2.1 价格体系

漏洞扫描服务的专业版扫描服务根据申请的域名数量和时长进行收费，您可以根据实际情况选择购买量。

详细的服务资费费用标准请参见[产品价格详情](#)。

2.2 续费

操作场景

该任务为您介绍当漏洞扫描服务即将到期时，您如何续费。续费后，您可以继续使用漏洞扫描服务的专业版功能。

前提条件

已获取管理控制台的登录账号与密码。

说明

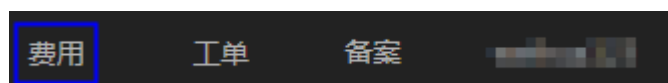
如果您使用的是子账号，需要主账号对子账号赋予BSS Administrator操作权限后，才可以使用子账号执行续费操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击界面右上方的“费用”，进入“费用中心”界面，如[图2-1](#)所示。

图 2-1 费用中心入口



步骤3 在左侧导航树上，选择“续费管理”。

步骤4 在对应页面根据页面提示完成续费。

详细续费操作请参见[续费管理](#)。

----结束

2.3 退订

操作场景

该任务为您介绍如何退订漏洞扫描服务的专业版功能。

前提条件

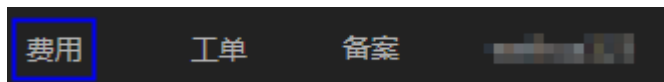
已获取管理控制台的登录帐号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 单击界面右上方的“费用”，进入“费用中心”界面，如[图2-2](#)所示。

图 2-2 费用中心入口



步骤3 在左侧导航树上，选择“退订与变更 > 退订管理”。

步骤4 在对应页面根据页面提示完成退订。

详细退订操作和退订限制请参见[退订管理](#)。

----结束