UNIS XScan-G 系列漏洞扫描系统

用户 FAQ

目 录

本文档介绍漏洞扫描系统中用户常见问题及解答。

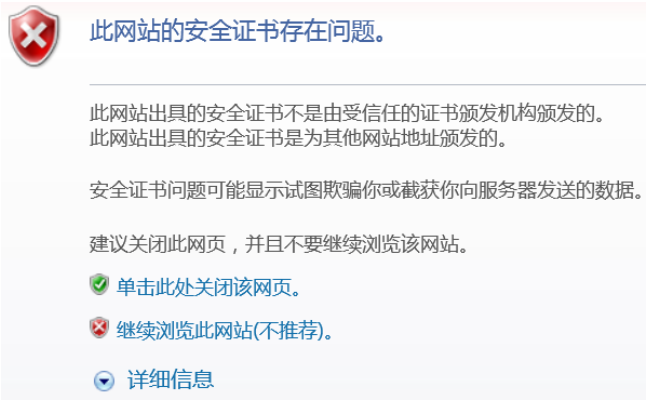
1 常用配置类 FAQ

浏览器打开地址链接后显示证书存在安全问题。

解决方法：

点击继续浏览此网站即可。

图1 点击继续浏览此网站

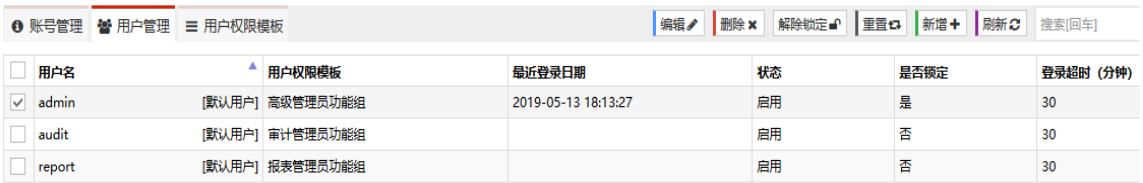


admin账户登录密码忘记，账户被锁定。

解决方法：

登录 account 账户，在用户管理找到 admin 进行编辑，解除锁定或重置密码。

图2 解锁账号



内网的地址无法管理设备，可Ping通，Web界面和SSH均不能登录。

解决办法：

一般此类情况是某些用户添加了对应信任 IP 导致，只允许特定网段 IP 访问，需要直连设备，使用默认的 192.168.0.1 地址登录，删除信任 IP 或者添加 0.0.0.0/0 的信任 IP 即可解决该问题。

图3 配置信任 IP

邮件告警或短信告警接收人无法添加。

原因：系统针对任务建立告警信息，不支持添加固定的告警信息接受人。

解决办法：添加多目标任务，可选择批量导入或者回车换行导入，选择检测结束发送邮件或发送短信，并添加告警接收人（接收人邮箱建议加白，否则漏洞结果告警太多容易被拉黑）。

图4 告警接收人配置

SSH登录的admin账户如何修改密码？

解决办法：

使用 SSH 连接工具，连接主机 IP 地址后，登录 admin 账户，使用键盘输入用户身份验证方式，点击确定后输入 admin 用户的密码，此时登录到 admin 账户，可以通过 **changepass** 命令更改 admin 账户的密码。修改后，下次 SSH 登录 admin 账户的密码为修改后的密码。（注意：admin 账户 Web 登录密码与 SSH 方式登录密码可不一致，请注意保存密码，以免遗忘）。示意如下。

[root]$ changepass

Input the new password:

Input the new password again:

[root]$

添加多个任务后，部分任务处于排队阶段。

解决办法：

系统为了防止同时多个任务执行影响设备性能导致系统异常，对并发任务数有限制，此情况一般由于正在运行的任务总数或 IP、站点总数达到了并发上限，导致平台新的任务出于排队等待状态，待执行的任务结束后，排队的任务会被执行。

系统检测结果中无检测详情

解决办法：

部分漏洞检测详情内容较多，导致报表内容冗长，故默认不保存漏洞检测详情，如需保存，在任务中心>新建任务>系统扫描>检测选项>开启保存漏洞检测详情。

图5 开启保存漏洞检测详情

选择特定模板后，系统扫描结果中仍存在其它类别的漏洞。

解决办法：

系统扫描选定指定模板后，为保证扫描效果，默认会检测相关联的其它漏洞。如不必要，可在任务中心>新建任务>系统扫描>检测选项>开启执行相关联漏洞，关闭该功能。

图6 开启执行相关联漏洞

2 业务功能类 FAQ

添加扫描任务有几种方式?

三种：

- 手动输入：可一次输入单个或多个主机。
- 使用资产列表。
- 批量导入：下载 Excel 表格，按照模板填写上传。

添加扫描地址后，任务几秒钟就结束，扫描结果无信息。

解决方法：

当主机不存在或者地址不可达，导致扫描不到信息。在提交任务前请仔细核对任务地址。

图7 扫描任务异常

Web靶机确实存在此漏洞，但是扫描不出来该漏洞。

解决方法：

(1) Web 靶机存在的漏洞链接通过 IP 或域名访问不到，或者不可跳转该链接，通过直接添加存在问题的域名和 URL 来扫描。

(2) 规则库内没有该条漏洞的规则，需要升级最新规则库后重新扫描。

漏洞模版上显示的漏洞数量少，没有要查询的规则名称。

解决方法：

规则库版本较老，升级到最新的规则库后即可。

主机确认存在扫描无结果，扫描结束。

原因：地址不可达；主机防火墙开启；（主要为 Windows 防火墙）。

解决办法：

(1) 地址不可达，可能是由于扫描器本身的网络配置原因导致，或者扫描器所在网络禁止访问被扫描主机，更换到对应主机网络区，重新配置网络后即可。

图8 业务地址配置

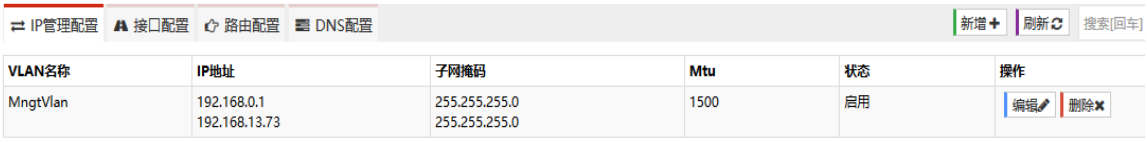


图9 路由配置

(2) 关闭主机防火墙。

Linux 防火墙

开启： service iptables start 关闭： service iptables stop

图10 Windows 防火墙

图11 启用或关闭 Windows 防火墙

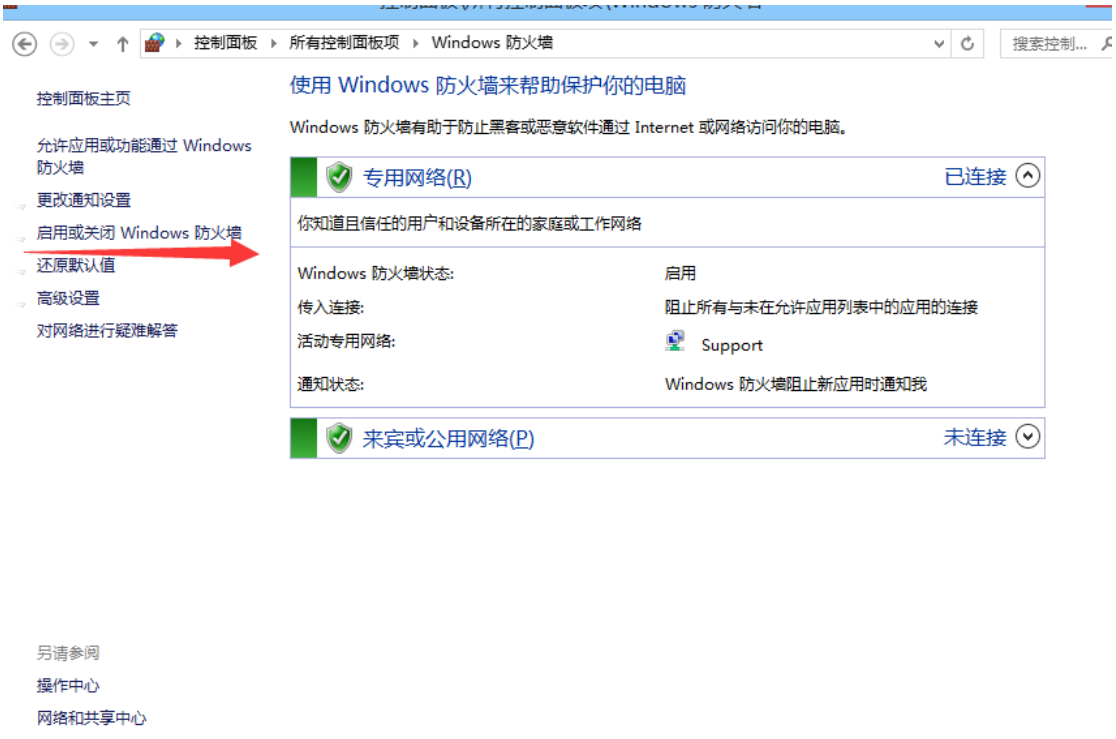
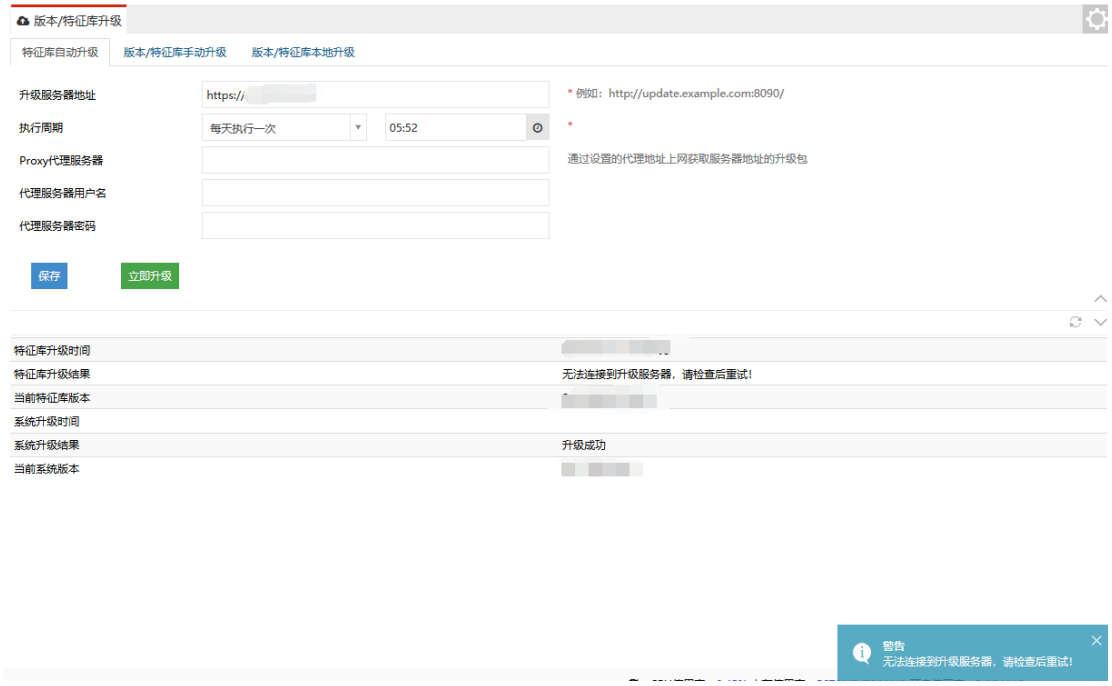


图12 关闭防火墙

规则库升级失败，提示升级失败。

图13 规则库升级失败

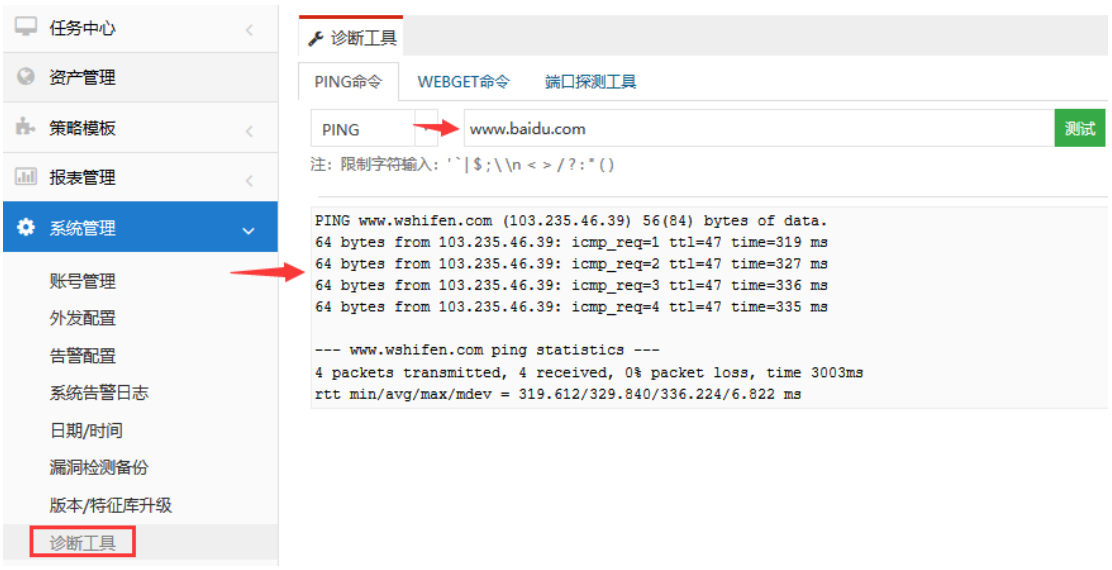


原因：网络地址不可达；升级服务器地址错误。

解决办法：

(1) 网络地址不可达：测试其它外网地址是否可达，如 www.baidu.com 或者 www.sina.com.cn，确定网络地址可达，并对升级地址进行可用性验证。

图14 诊断工具



(2) 升级服务器地址填写错误：检查填写的升级服务器地址是否正确，填写正确的升级服务器地址。默认升级服务器地址为：https://47.92.55.33/。

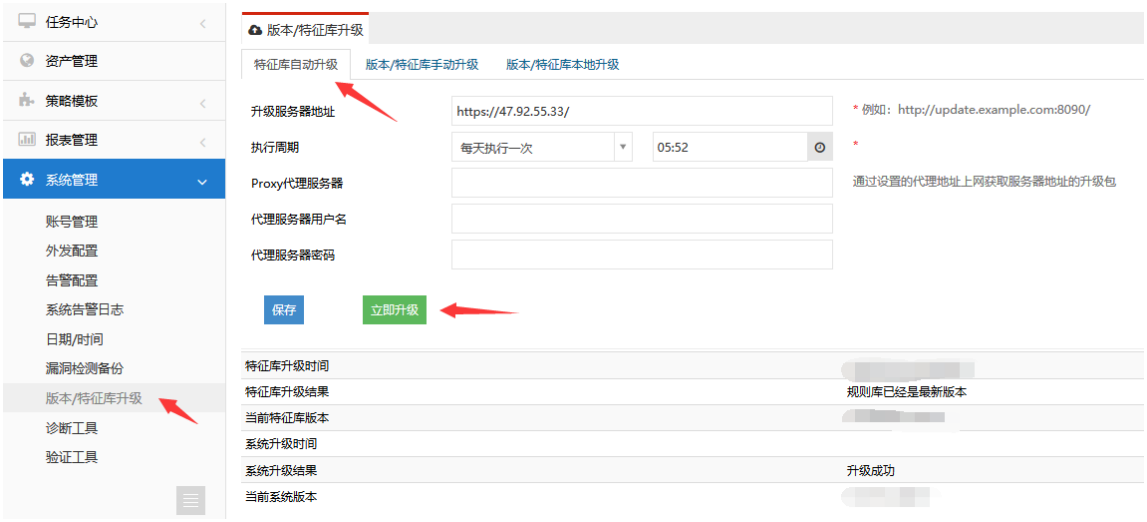
如何进行升级。

解决方法：

(1)　自动升级规则库

在 admin 账户下登录，选择**系统管理>版本/版本库升级>版本/版本库升级**。

图15 自动升级规则库



(2)　界面手动升级规则库和系统版本

在本地搭建 Ftp（3CDaemon 软件）环境，关闭本地主机防火墙，选择对应的升级路径和文件，进行升级。

命令：ftp://user:pass@ip:port/包名.img

图16 搭建 Ftp(3CDaemon 软件)环境

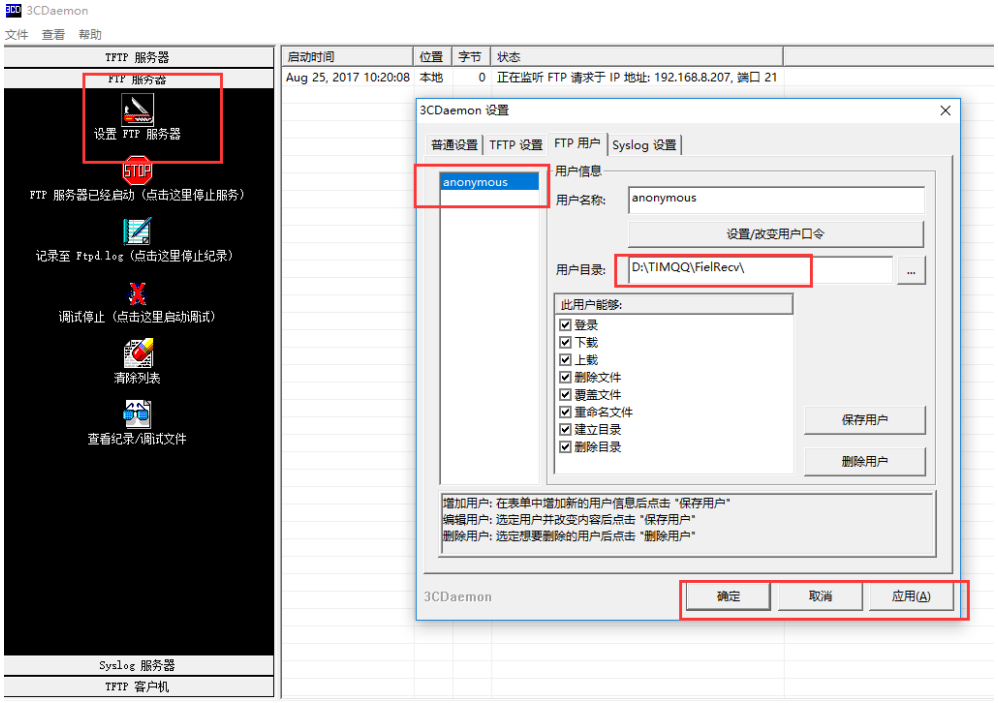


图17 手动升级

(3) 界面本地升级

点击导入的按钮，选择本地的升级文件直接导入即可。

图18 界面升级

(4) 后台升级

打开终端管理软件，如 putty，使用 ssh2 协议登录后台，初始用户名/密码：admin/admin

本地搭建 Ftp（3CDaemon 软件）环境，关闭本地主机防火墙，选择对应的升级路径和文件。

后台执行命令：

特征库升级： sigup ftp://ip/包名.img

系统升级： patchall ftp://ip/包名.img

口令猜解无法添加任务问题。

原因：在无资产组信息的条件下，无法添加口令猜解任务。

解决办法：添加资产组后,勾选相应的服务类型和数据库类型提交任务。

图19 资产组管理

图20 新增资产

图21 口令猜解配置

对系统扫描的个别主机信息和漏洞信息报告不准确。

原因：主机地址可能是 NAT 或者映射之类的地址，导致服务识别与漏洞测试过程中可能出现主机信息及服务被代理或者代理主机端口转换，和多端口多服务多主机情况存在导致的信息返回紊乱。此情况是主要由网络原因导致。

该设备上还有其它设备映射过来的端口，则可能会检测到更多的特征，也会检测更多的系统。

解决方法：

避免由于网络的原因导致扫描结果不准确，可在局域网内进行系统漏洞扫描，跳过 NAT 设备、防火墙、代理类设备。同网段或者直连扫描结果准确性更高。

web扫描结果较少，Web站点需要登录扫描问题。

原因：Web 站点设置了主页登录，认证等方式，扫描器需要拿到对应的信息才能扫到更多的结果。

解决方法：

填写登录信息后进行扫描。

常见的登录认证方式：认证登录选型：有验证码的是 Cookie，无验证码 Form，用户名和密码写在 URL 里的是 Basic 认证。

(1) Cookie 认证信息获取

以火狐浏览器为例：登录上去后使用开发者工具，找到对应的 Cookie 信息。提交后重新扫描。

图22 Cookie 认证信息获取

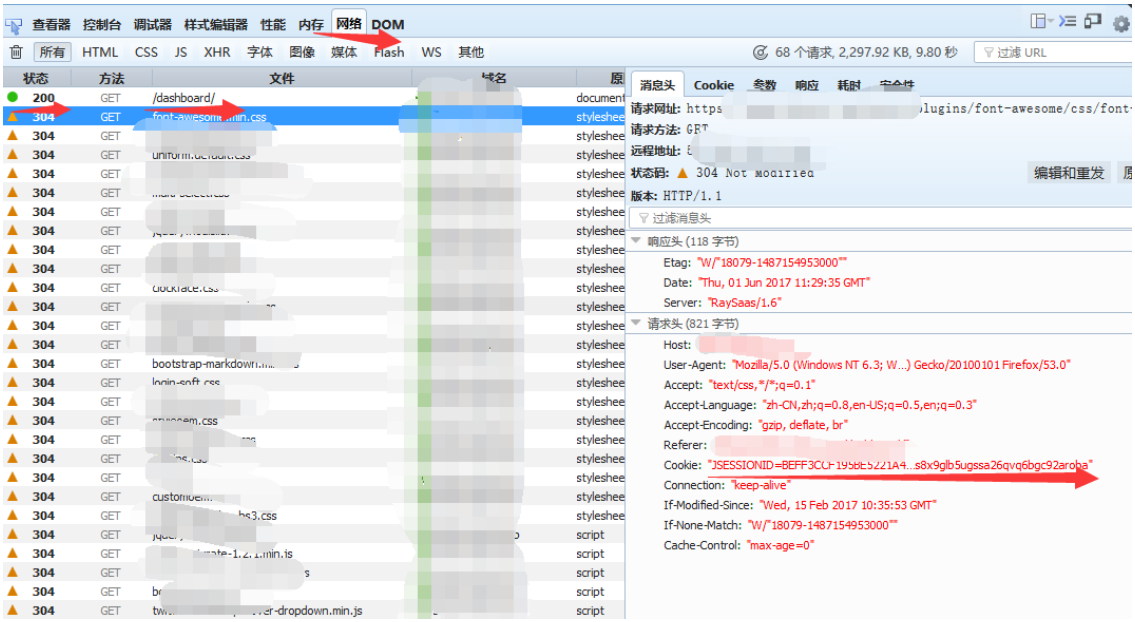
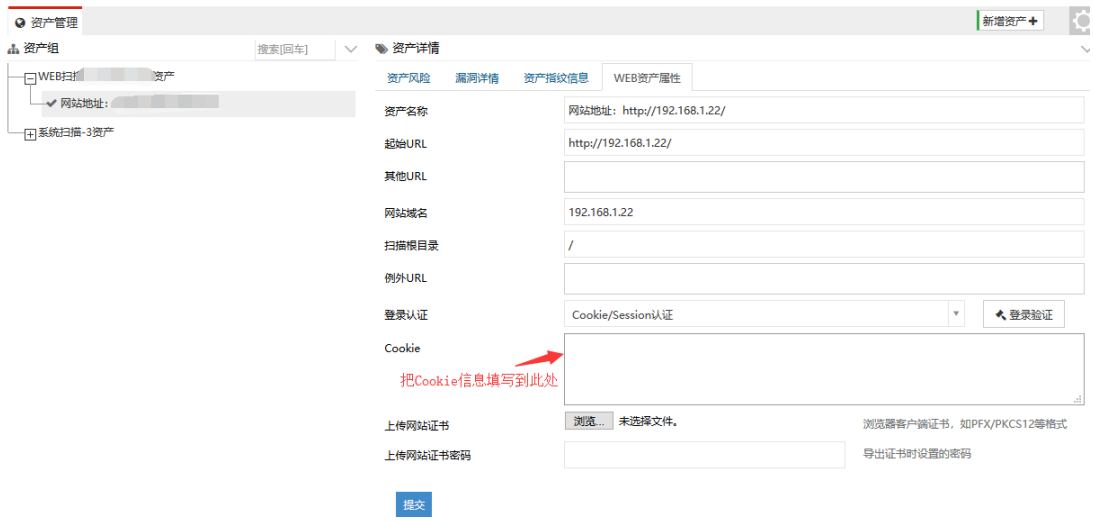


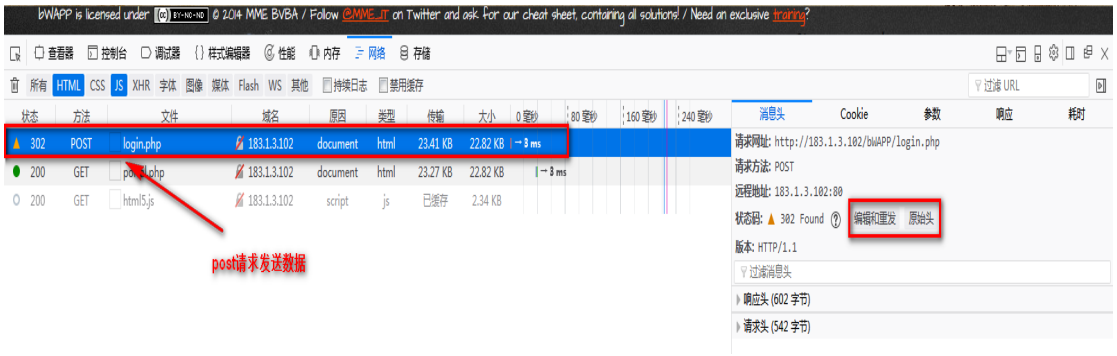
图23 Cookie 信息填写



(2) Form 认证信息获取

用火狐登录网站，F12 开发者视图可以看到登录采用的 Post 请求，点击编辑和重发可以看到请求头和请求体，点击原始头可以看到请求头和响应头。

图24 Post 请求发送数据

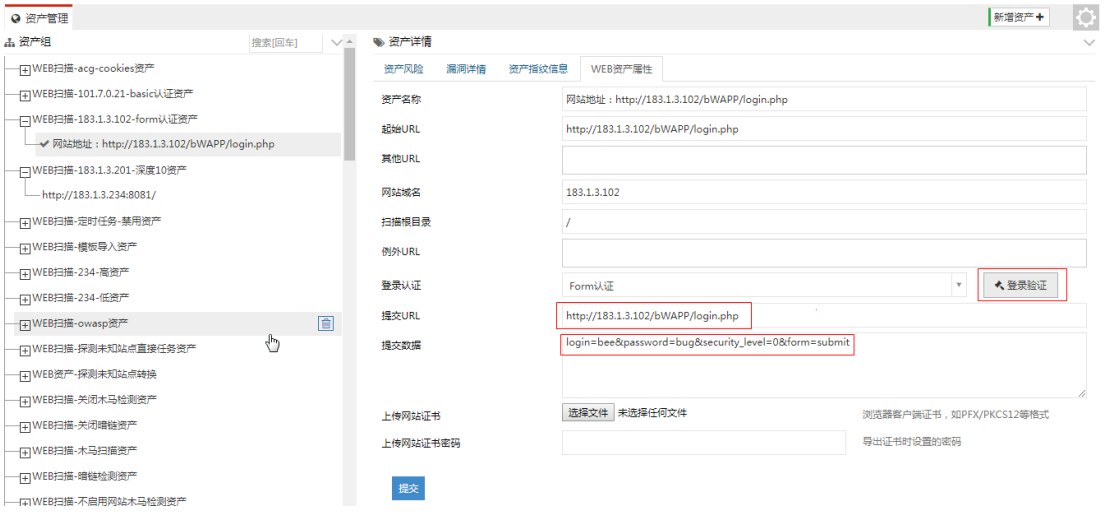


点击编辑和重发，看到 Post 请求头内容，可以用于网站认证时使用。

图25 请求头内容

资产管理/资产详情，选择登录认证方法为 Form 认证，把请求头内容复制到提交数据中，提交 URL 中写入登录 URL，提交数据格式如下图中所示

图26 Form 认证配置



(3) Basic 认证信息获取

可在提交的 URL 中获取到相应的用户名和密码，并填写到认证框内即可。

图27 Basic 配置

Web扫描扫不到页面。

解决办法：检查网络是否连通，地址是否可访问，是否有防护设备，是否开了防爬虫功能。

Ping不通，但是主机存活，系统扫描扫不到主机。

解决办法：判断网络是否连通，是否有防护设备，建议强制扫描，关闭“存活探测”。

Web扫描有页面数，没漏洞。

解决办法：

(1) 本身无漏洞。

(2) 爬虫爬取下来的页面解析后无漏洞。

(3) 发探测包解析的时候被防护设备拦截。

(4) 发测试包的前提是根据爬到的页面发对应的测试包，所以爬不到页面也就不会发测试包，不会去检测漏洞。

(5) 页面数太多，但没有漏洞，原因是超过系统超时时间，自动断开，还未判断出漏洞。

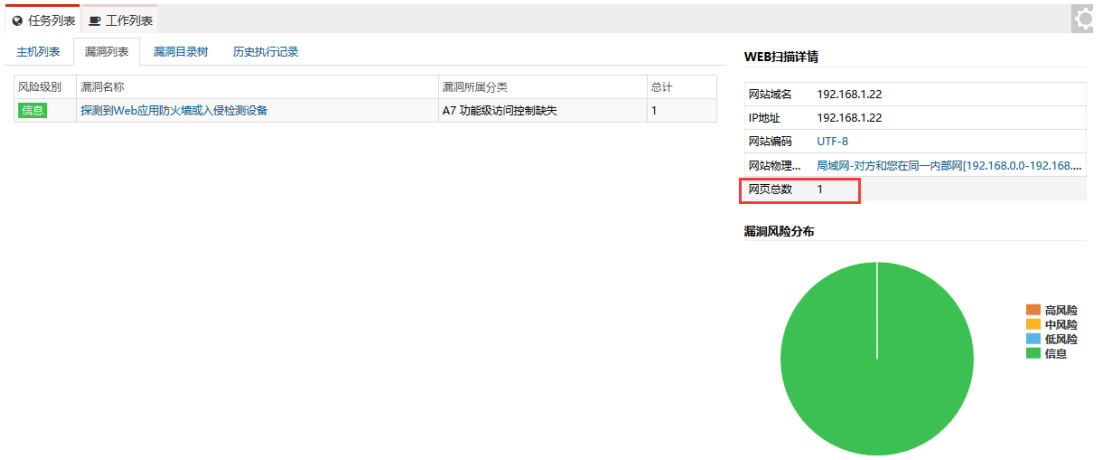
正常扫描和系统登录扫描（验证已登录成功），扫描结果没区别。

可能是系统本身是一个空系统，装的软件较少，开启的服务少，所以差别不大，对外提供的端口和服务都类似。

Web扫描结束后，怎样可以看到单个站点的页面数。

解决办法：在任务列表里面点击对应主机，页面右边会显示该站点的网页数。

图28 查看站点网页数

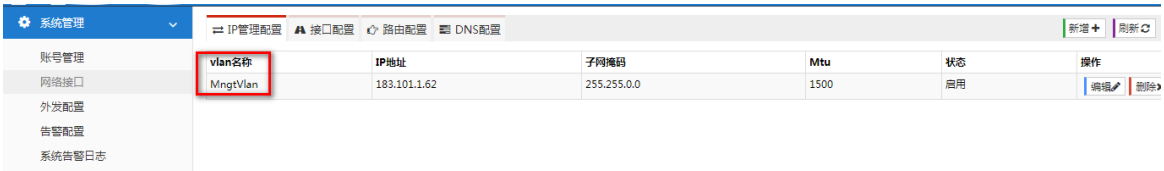


XSCAN-G10款型设备上插上四万兆插卡，web界面禁用万兆光口，显示为down的状态，但设备指示灯仍微亮。

X710&XL710 网卡芯片问题，物理实际为 down，可根据漏扫界面端口状态判断端口状态。

系统管理>网络接口，IP管理配置中vlan名称和默认MngtVlan表示为vlan还是网桥？

漏扫中表示为网桥的含义。



使用系统插件中自定义策略模板进行扫描时，为何还会扫描出非自定义策略中漏洞呢？

使用自定义策略模板扫描时，需要关闭任务配置中“检测选项>执行相关联漏洞”选项。


系统扫描
WEB扫描
数据库检测
口令猜解
扫描基本配置
自主选择插件
探测选项
检测选项
引擎选项
登录信息选项
最大限度报告漏洞
若选择开启，扫描结果中不是所有漏洞都经过原理扫描得出，会有一些根据版本信息推测出来的漏洞。
执行所有规则检测
若选择开启：检测耗时越久、对检测目标的覆盖面更广。
执行相关联漏洞
若选择开启：某些已例外的漏洞将加入到扫描结果当中。
保存漏洞检测详情
若选择开启：漏洞的详细打印信息将加入到扫描结果当中。
自适应网络
根据网络的反应速度，适当调整发包的速率，从而不至于将网络扫瘫痪，但会影响扫描速度
危险测试
包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用
停止探测无响应主机
如果扫描过程中发现扫描目标没有反应，停止对该目标的探测
随机顺序扫描
启用口令破解
使用默认字典对系统或服务的口令进行猜解
测试Oracle账号
启用Web检测
SMB信息探测