UNIS XSCAN-CN60 漏洞扫描系统

典型配置举例

目 录

1 产品简介

随着网络技术的成熟和发展，网络环境也日益复杂，网络与信息化以不可阻挡之势渗透到大众生产生活的方方面面，各国政府都愈加重视网络安全规划布局。

同时随着网络技术的成熟，一方面使用者越来越多，使用者也从最初的简单机械化操作变得依赖性更强，人们不仅依赖网络来传递信息，传播新闻动态，也利用网络来进行金钱交易。与此同时，由于国民网络安全普及度还不够广，暴露在网络环境下的各个网络单元就会变成不法分子的“猎物”。

据 CNNVD 统计分析称，网络环境中暴露的漏洞数量在逐年增加，而且严重和高危漏洞占据很大比例，其中网站漏洞中，跨站脚本和 SQL 注入类传统类别的漏洞依旧占据了相当大的比重，漏洞检查越来越有必要。

UNIS XSCAN-CN60 漏洞扫描系统通过对系统漏洞、服务后门、网页挂马、SQL 注入漏洞以及跨站脚本等攻击手段多年的研究积累，总结出了智能主机服务发现、智能化爬虫和 SQL 注入状态检测等技术，可以通过智能遍历规则库和多种扫描选项组合的手段，深入准确的检测出系统和网站中存在的漏洞和弱点。最后根据扫描结果，提供测试用例来辅助验证漏洞的准确性，同时提供整改方法和建议，帮助管理员修补漏洞，全面提升整体安全性。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

注意

扫描任务中若检测到 1 个扫描目标在线，则会占用 1 个 IP 数量授权，占用后无法释放，请在配置时按计划合理使用。

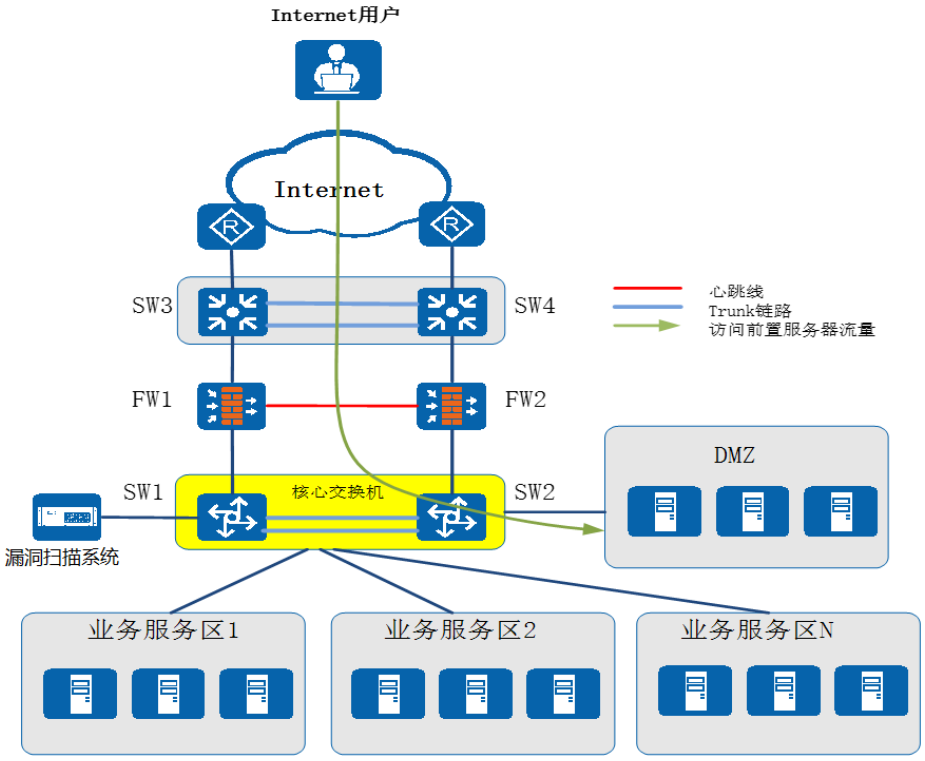
3 使用限制

无

4 典型组网

4.1 旁路部署网络结构

UNIS XSCAN-CN60 漏洞扫描系统旁路方式部署在某一个区域进行单区域扫描，或者是核心交换机旁边进行全网扫描。



4.2 旁路部署配置

4.2.1 配置 IP 地址

用账号(account)登录设备，在“系统管理>网络接口>IP 地址管理”中，选择 MngtVlan,点击“编辑”按钮。

说明

漏扫中配置的 vlan 是内部网桥的一个 vlan，发出去的包不带标签，从交换机上插根网线就能通，对交换机没有要求。默认出厂时所有口均在一个网桥中。

图4-1 IP 管理配置

再点击“下一步”调过 VLAN 基本配置。

点击“新增”增加 192.168.7.253 的 IP 地址，子网掩码 255.255.255.0，然后点击“保存”，最后点击完成，“完成”配置。

配置路由

在“系统管理>网络接口>路由配置”中，点击“新增”按钮，添加下一跳为 192.168.7.1 的默认路由，然后点击“提交”。

IP 管理配置

参数	说明
VLAN名称	网桥口的名称
IP地址/子网掩码	网桥的IP地址、掩码
状态	设置网桥接口的启用或禁用
操作	对网桥口做删除或编辑的操作

4.2.2 策略配置

> ⚠ 注意
>
> 扫描任务中若检测到 1 个扫描目标在线，则会占用 1 个 IP 数量授权，占用后无法释放，请在配置时按计划合理使用。

系统扫描配置

用账号(admin)登录设备“任务中心>新建任务>系统扫描”中，选择手动输入，先在扫描目标中填写需要防护的 IP 或者 IP 网段，本例为 192.168.7.79，然后填写任务名称，再选择“提交”。

任务添加完成后可以在“任务中心>任务列表”中查看系统扫描任务的执行进度。添加完任务之后，在前几秒任务显示为“排队等待中”，之后任务正常扫描时为“正在执行中”。

系统扫描

配置信息	说明
扫描目标方式	选择扫描目标的方式，包括手动输入、使用资产、批量导入列表
扫描目标	输入的内容有[单个主机]和[主机组]两种，多个之间以英文逗号(,)或换行分隔 * 单个主机示例：192.168.1.100 也可使用域名：www.example.com * IPv6示例：2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 * 主机组示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 * 排除某个IP：192.168.1.0/24!192.168.1.100
任务名称	输入任务名称

配置信息	说明
执行方式	选择立即执行或者定时执行
检测模式	完全扫描：采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描 强制扫描：使用强制手段对扫描目标进行主机存活、端口服务探测 登录审计：利用配置好的用户名密码列表对主机进行登录后的本地审计
漏洞插件模板	选择不同的漏洞插件模板
分布式引擎	默认：系统将根据引擎的负载情况，智能选择工作引擎。 local：系统将会选择本地引擎。
执行优先级别	当任务达到并发上限时，'排队等待中'级别高的任务将优先执行
检测结束发送邮件	扫描结束后发送邮件，需配置邮件
检测结束发送短信	扫描结束后发送短信，需配置短信网关

添加 Web 扫描任务

用账号(admin)登录设备，在“任务中心>新建任务>系统扫描”中，选择手动输入，先在扫描目标中填写需要防护的 URL 地址，本例为 http:// 172.16.101.74，然后填写任务名称，再选择“提交”。

任务添加完成后可以在“任务中心>任务列表”中查看系统扫描任务的执行进度。刚添加完任务之后，在前几秒任务显示为“排队等待中”，之后任务正常扫描时为“正在执行中”。

WEB 扫描

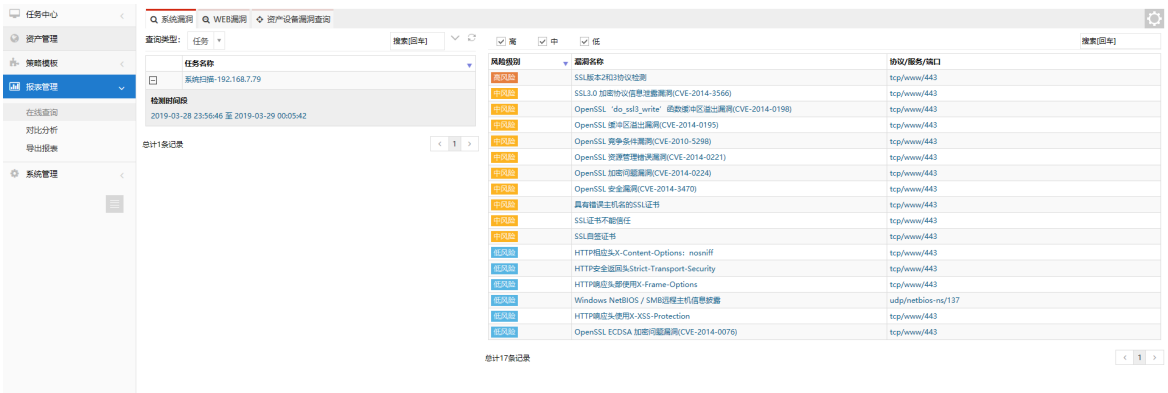
配置信息	说明
扫描目标方式	选择扫描目标的方式，包括手动输入、使用资产、批量导入列表和会话录制

配置信息	说明
扫描目标	URL地址：http://www.example.com/ 或 https://www.example.com/ URL地址：http://192.168.1.100/ 或 https://192.168.1.100/ IPv6 URL示例：http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/ 多个URL以英文逗号(,)或回车分隔
任务名称	输入任务名称
执行方式	选择立即执行或者定时执行
漏洞插件模板	选择不同的漏洞插件模板
分布式引擎	默认：系统将根据引擎的负载情况，智能选择工作引擎。同时也可以指定引擎
执行优先级别	当任务达到并发上限时，'排队等待中'级别高的任务将优先执行
检测结束发送邮件	扫描结束后发送邮件，需配置邮件
检测结束发送短信	扫描结束后发送短信，需配置短信网关

4.2.3 结果验证

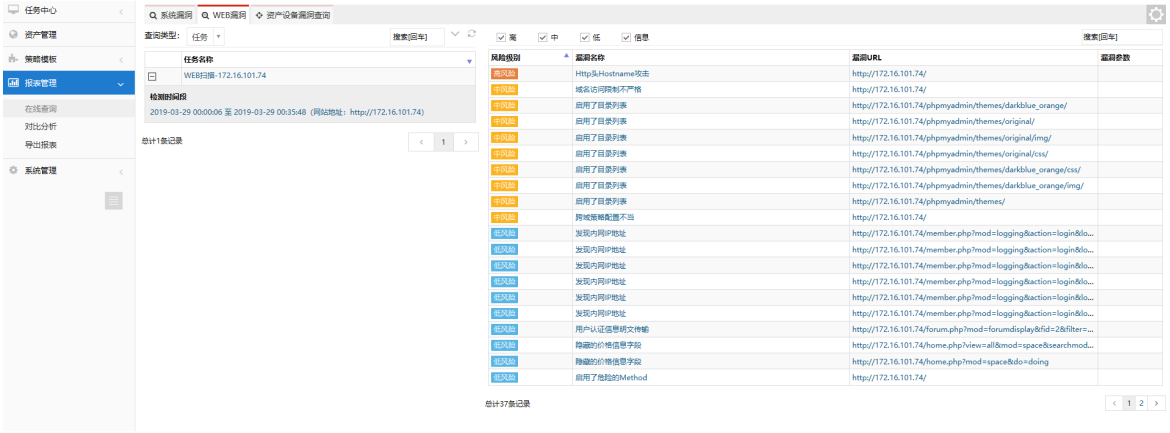
查看系统漏洞

添加的系统扫描任务执行结束后，可以在“报表管理>在线查询>系统漏洞”中，查看系统扫描的详细结果。



查看 Web 漏洞

添加的 Web 扫描任务执行结束后，可以在“报表管理>在线查询>Web 漏洞”中，查看 Web 扫描的详细结果。



4.2.4 导出报表

导出系统漏洞报表

添加的系统扫描任务执行结束后，可以在“报表管理>导出报表”中，选择“系统扫描资产”，然后选择“指定资产”、“检测任务时间段”和“导出格式”，最后点击“导出”按钮导出报表。

导出 Web 漏洞报表

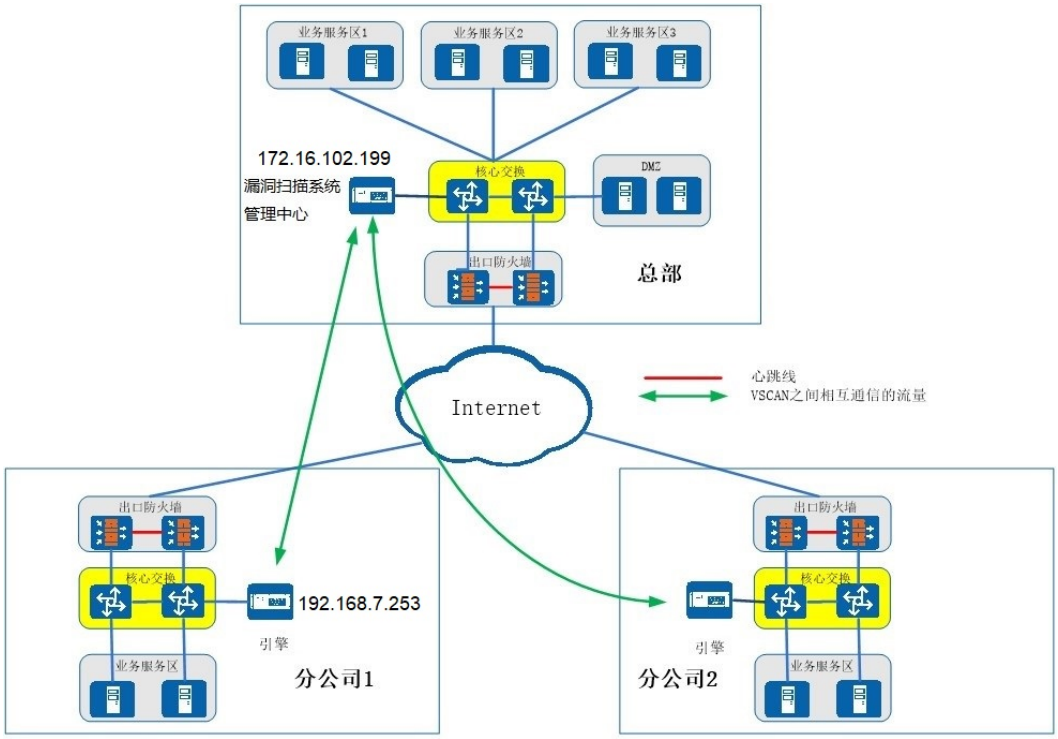
添加的系统扫描任务执行结束后，可以在“报表管理>导出报表”中，选择“Web 扫描资产”，然后选择“指定资产”、“检测任务时间段”和“导出格式”，最后点击“导出”按钮导出报表。

导出报表

配置信息	说明
选择导出对象	选择导出系统扫描资产或者WEB扫描资产，数据库检测、 口令猜解任务都属于系统扫描范畴
指定资产组	仅显示已检测过的资产组
检测任务时间段	开始时间-至-结束时间
导出格式	选择HTML、WPS、PDF、ET、XML格式
导出方式	选择详细报表或统计报表
报表标题	报表标题
导出文件名	导出文件名
导出CNNVD信息	若开启此按钮，系统详细报表中的系统漏洞中会包含CNNVD字段
自定义HTML详细报表	自定义HTML详细报表，可以自定义
自定义公司信息	自定义公司信息
设置压缩包密码	设置压缩包密码

4.3 分布式部署网络结构

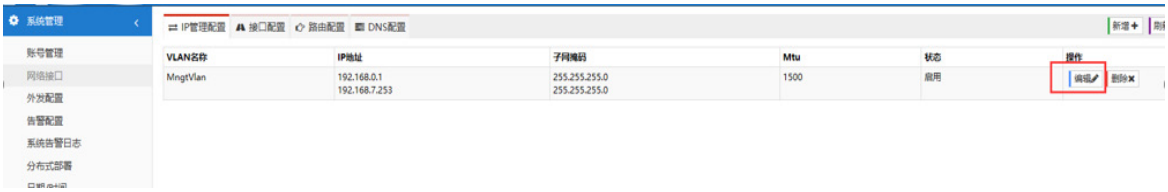
UNIS XSCAN-CN60 漏洞扫描系统支持分布式部署，集中管控中心既可作为管理端，也可以作为扫描引擎，统一下发扫描任务至下级引擎，并在管控中心统一分析、统一展示。



4.4 分布式部署配置

4.4.1 配置 IP 地址

用账号(account)登录设备，在“系统管理>网络接口>IP 地址管理”中，选择 MngtVlan,点击“编辑”按钮。



再点击“下一步”调过 VLAN 基本配置。

点击“新增”增加 192.168.7.253 的 IP 地址，子网掩码 255.255.255.0，然后点击“保存”，最后点击完成，“完成”配置。

配置路由

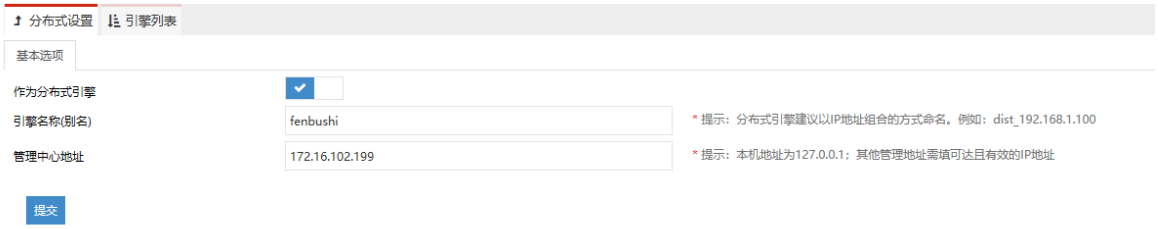
在“系统管理>网络接口>路由配置”中，点击“添加”按钮，添加下一跳为 192.168.7.1 的默认路由，然后点击“提交”。

IP 管理配置

参数	说明
VLAN名称	网桥口的名称
IP地址/子网掩码	网桥的IP地址、掩码
状态	设置网桥接口的启用或禁用
操作	对网桥口做删除或编辑的操作

4.4.2 配置分布式扫描引擎

用超级管理员账号(account)登录设备，在“系统管理>分布式部署>分布式配置”中，点击“作为分布式引擎”按钮，将 UNIS XSCAN-CN60 漏洞扫描系统改成引擎模式，然后进行配置，选择对应的管控中心。本例管控中心 IP 为 172.16.102.199。

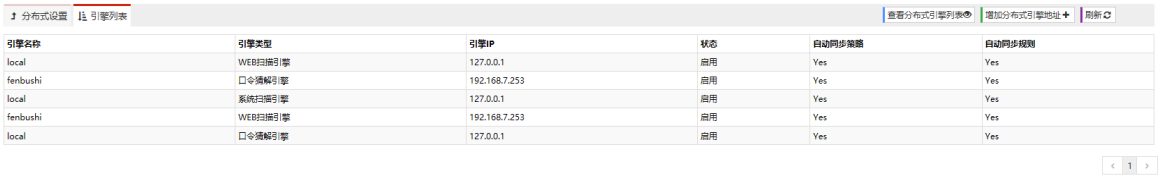


配置成功后，点击“提交”系统会自动重启。重启完成后，即可作为一个引擎使用。每次修改完引擎的配置后，都需要重启分布式引擎配置才会生效。

4.4.3 配置分布式扫描管控中心

用超级管理员账号(account)登录管控中心漏扫地址，在“系统管理>分布式部署>引擎列表”中，点击“增加引擎地址”按钮，填写引擎的地址，然后点击“提交”按钮。本例引擎 IP 为 192.168.7.253。

添加完成后，可以在引擎列表中看到新增的引擎。



注：引擎加载到管控中心漏扫中需要时间，请耐心等待

4.4.4 配置策略

注意

扫描任务中若检测到 1 个扫描目标在线，则会占用 1 个 IP 数量授权，占用后无法释放，请在配置时按计划合理使用。

系统扫描配置

用账号(admin)登录管理中心（172.16.102.199）“任务中心>新建任务>系统扫描”中，选择手动输入，先在扫描目标中填写需要防护的 IP 或者 IP 网段，本例为 192.168.7.79，然后填写任务名称，再选择“提交”。

任务添加完成后可以在“任务中心>任务列表”中查看系统扫描任务的执行进度。添加完任务之后，在前几秒任务显示为“排队等待中”，之后任务正常扫描时为“正在执行中”。

系统扫描

配置信息	说明
扫描目标方式	选择扫描目标的方式，包括手动输入、使用资产、批量导入列表
扫描目标	输入的内容有[单个主机]和[主机组]两种，多个之间以英文逗号(,)或换行分隔 * 单个主机示例：192.168.1.100 也可使用域名：www.example.com * IPv6示例：2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 * 主机组示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 * 排除某个IP：192.168.1.0/24!192.168.1.100
任务名称	输入任务名称
执行方式	选择立即执行或者定时执行
检测模式	完全扫描：采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描 强制扫描：使用强制手段对扫描目标进行主机存活、端口服务探测 登录审计：利用配置好的用户名密码列表对主机进行登录后的本地审计
漏洞插件模板	选择不同的漏洞插件模板
分布式引擎	默认：系统将根据引擎的负载情况，智能选择工作引擎。 local：系统将会选择本地引擎。
执行优先级别	当任务达到并发上限时，'排队等待中'级别高的任务将优先执行
检测结束发送邮件	扫描结束后发送邮件，需配置邮件
检测结束发送短信	扫描结束后发送短信，需配置短信网关

添加 Web 扫描任务

用账号(admin)登录设备，在“任务中心>新建任务>系统扫描”中，选择手动输入，先在扫描目标中填写需要防护的 URL 地址，本例为 http://172.16.101.74，然后填写任务名称，再选择“提交”。

任务添加完成后可以在“任务中心>任务列表”中查看系统扫描任务的执行进度。刚添加完任务之后，在前几秒任务显示为“排队等待中”，之后任务正常扫描时为“正在执行中”。

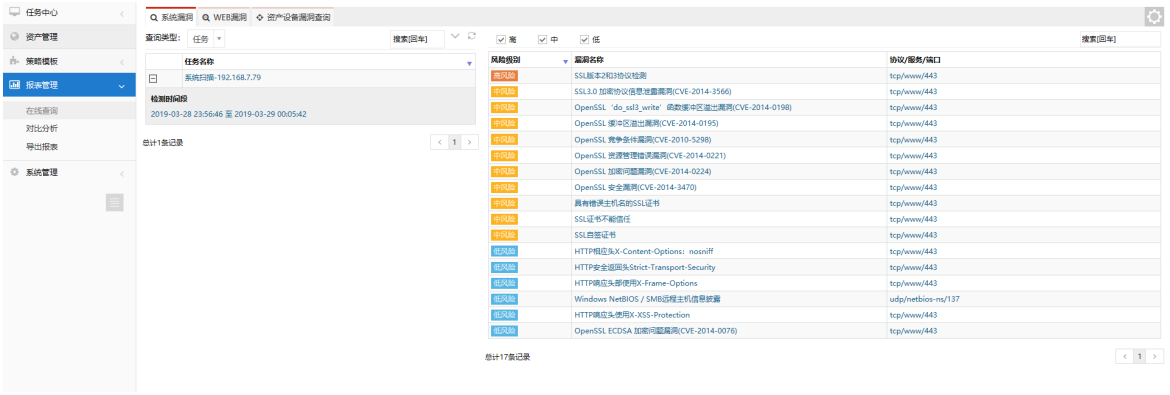
WEB 扫描

配置信息	说明
扫描目标方式	选择扫描目标的方式，包括手动输入、使用资产、批量导入列表和会话录制
扫描目标	URL地址：http://www.example.com/ 或 https://www.example.com/ URL地址：http://192.168.1.100/ 或 https://192.168.1.100/ IPv6 URL示例：http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/ 多个URL以英文逗号(,)或回车分隔
任务名称	输入任务名称
执行方式	选择立即执行或者定时执行
漏洞插件模板	选择不同的漏洞插件模板
分布式引擎	默认：系统将根据引擎的负载情况，智能选择工作引擎。同时也可以指定引擎
执行优先级别	当任务达到并发上限时，'排队等待中'级别高的任务将优先执行
检测结束发送邮件	扫描结束后发送邮件，需配置邮件
检测结束发送短信	扫描结束后发送短信，需配置短信网关

4.4.5 2.4.4 结果验证

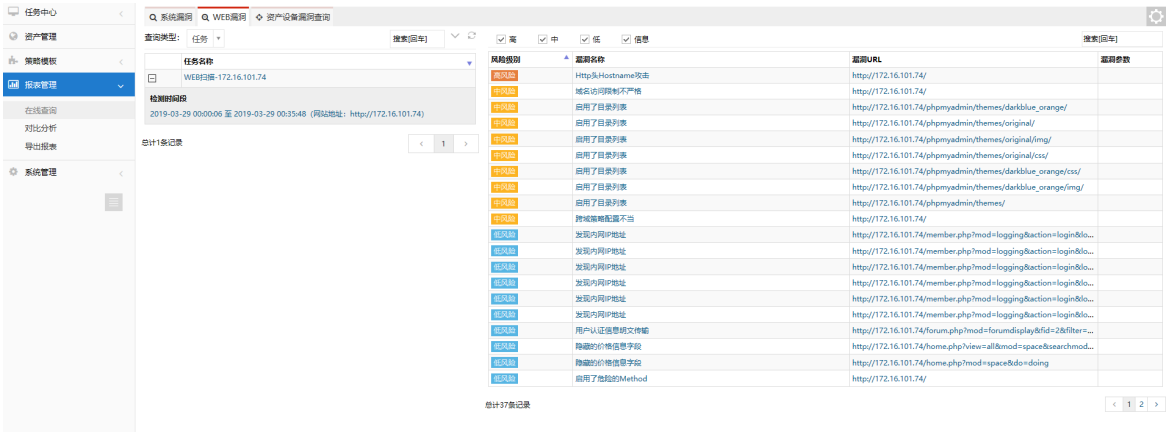
查看系统漏洞

添加的系统扫描任务执行结束后，可以在“报表管理>在线查询>系统漏洞”中，查看系统扫描的详细结果。



查看 Web 漏洞

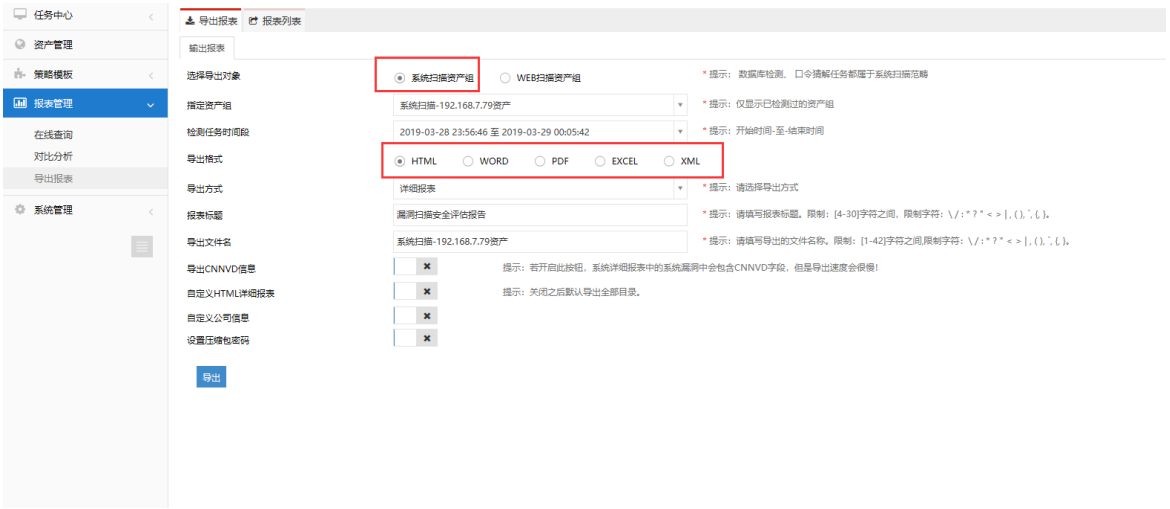
添加的 Web 扫描任务执行结束后，可以在“报表管理>在线查询>Web 漏洞”中，查看 Web 扫描的详细结果。



4.4.6 2.4.5 导出报表

导出系统漏洞报表

添加的系统扫描任务执行结束后，可以在“报表管理>导出报表”中，选择“系统扫描资产”，然后选择“指定资产”、“检测任务时间段”和“导出格式”，最后点击“导出”按钮导出报表。



导出 Web 漏洞报表

添加的系统扫描任务执行结束后，可以在“报表管理>导出报表”中，选择“Web 扫描资产”，然后选择“指定资产”、“检测任务时间段”和“导出格式”，最后点击“导出”按钮导出报表。

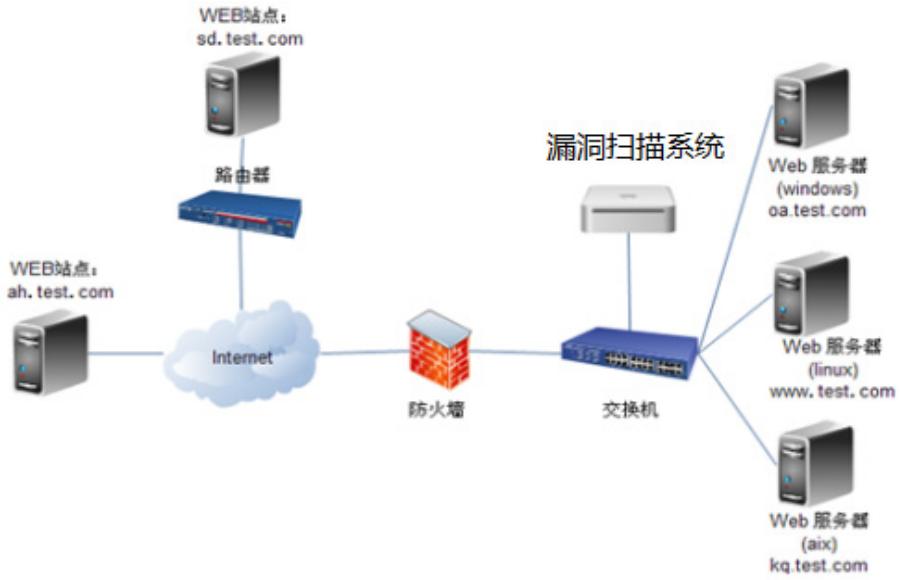
导出报表

配置信息	说明
选择导出对象	选择导出系统扫描资产或者WEB扫描资产，数据库检测、 口令猜解任务都属于系统扫描范畴
指定资产组	仅显示已检测过的资产组

配置信息	说明
检测任务时间段	开始时间-至-结束时间
导出格式	选择HTML、WORD、PDF、EXCEL、XML格式
导出方式	选择详细报表或统计报表
报表标题	报表标题
导出文件名	导出文件名
导出CNNVD信息	若开启此按钮，系统详细报表中的系统漏洞中会包含CNNVD字段
自定义HTML详细报表	自定义HTML详细报表，可以自定义
自定义公司信息	自定义公司信息
设置压缩包密码	设置压缩包密码

5 会话录制配置举例

5.1 组网需求



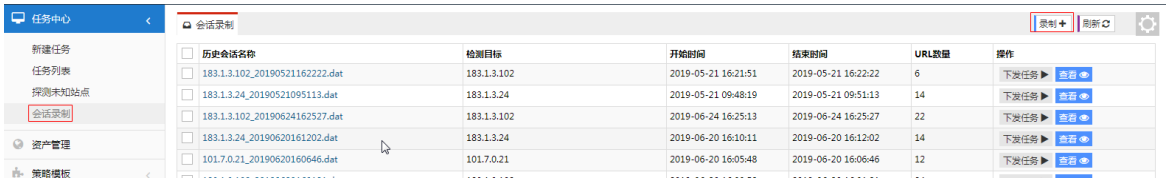
会话录制是设备自身开启代理服务器，由客户端配置代理后，通过记录代理请求中的 URL 信息形成记录的功能，可用于一些爬虫无法爬取，或者隐藏 URL 的站点扫描。

5.2 配置步骤

本配置以谷歌浏览器访问漏扫地址，火狐浏览器做代理服务器举例介绍。

1、谷歌浏览器访问漏扫地址，用账号(admin)登录设备，在“任务中心>会话录制”中，点击“录制”按钮。

图5-1 会话录制



2、输入要录制的域名>点击“开始录制”。

表5-1 会话录制配置参数

参数	说明
域名	填写需要录制的域名信息

图5-2 输入要录制域名

3、使用火狐浏览器做代理配置，进入“选项>常规>网络代理>设置”，配置手动代理设置，“HTTP代理”填入漏扫设备地址，端口填写 8080，点击确定。

图5-3 浏览器中代理配置

4、关闭火狐浏览器，重新打开，依次访问录制的域名。

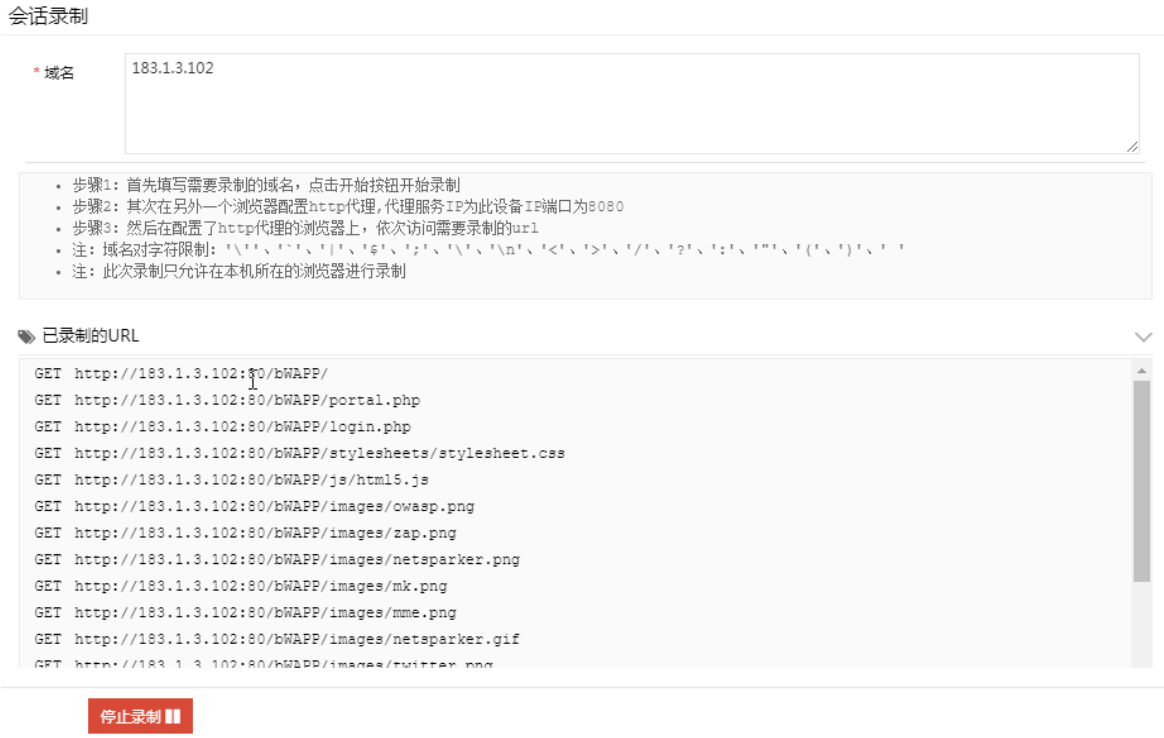
图5-4 代理服务器访问域名

注意：若出现“代理服务器拒绝连接”，可多次点击重试即可。

图5-5 代理服务器拒绝连接

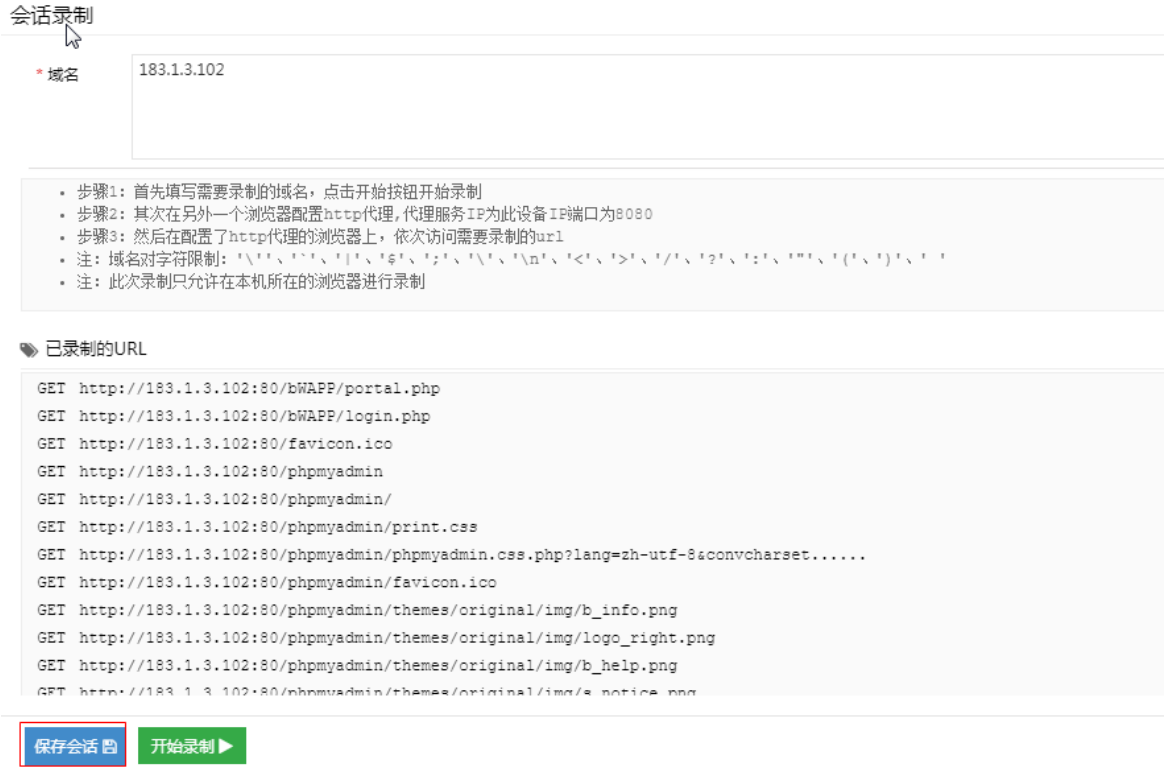
5、在访问结束后点击“停止录制”。

图5-6 会话录制



5、点击保存会话。

图5-7 保存会话



5.3 验证配置

在会话录制列表中可查看保存的会话。

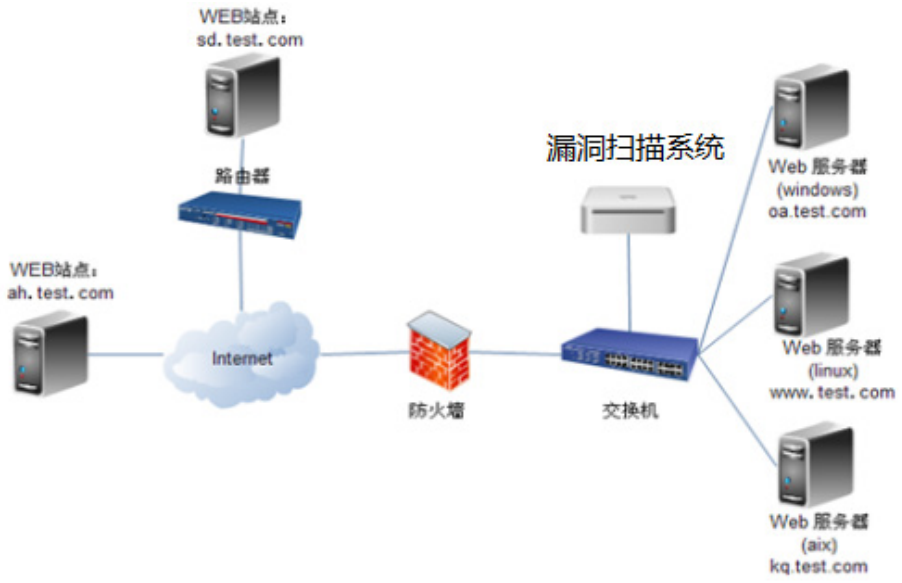
图5-8 查看保存会话

在会话录制列表的会话后点击“下发任务”，直接跳转到任务中心列表，可直接使用此会话建立扫描任务，其它配置可参考 4.2。

图5-9 会话录制方式下发任务

6 Web cookie 录制扫描配置举例

6.1 组网需求

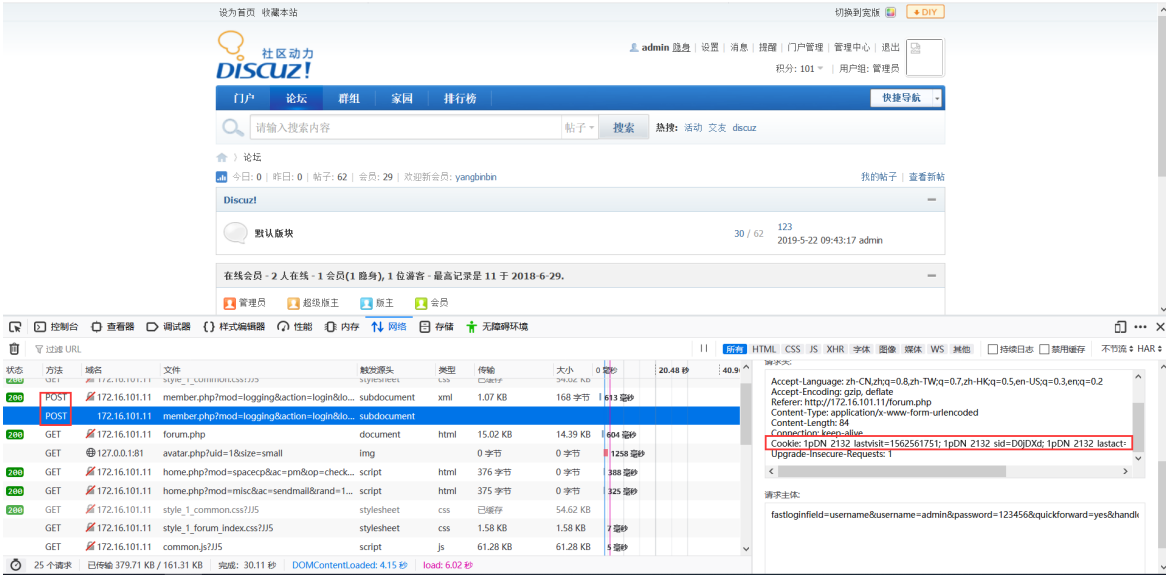


Web 站点设置了主页登录，认证等方式，需要拿到登录认证对应的信息才能扫描到更多的结果。常见的 Web 登录方式绝大多数以 Cookie 认证、Form 认证为主；较少使用的 Web 登录方式有 Basic 认证；NTLM 认证是比较早期的认证技术，目前很少使用。本配置介绍了 Cookie 认证扫描配置方法。

6.2 配置步骤

1、火狐浏览器登录需要扫描的网站，登录上去后按 F12 进入开发者工具视图，点击网络。Login 与 Password 登录框输入用户密码，登录认证，开发者视图中查看 POST 提交信息，查看“请求头”获取提交 Cookie 信息。

图6-1 Cookie 值复制

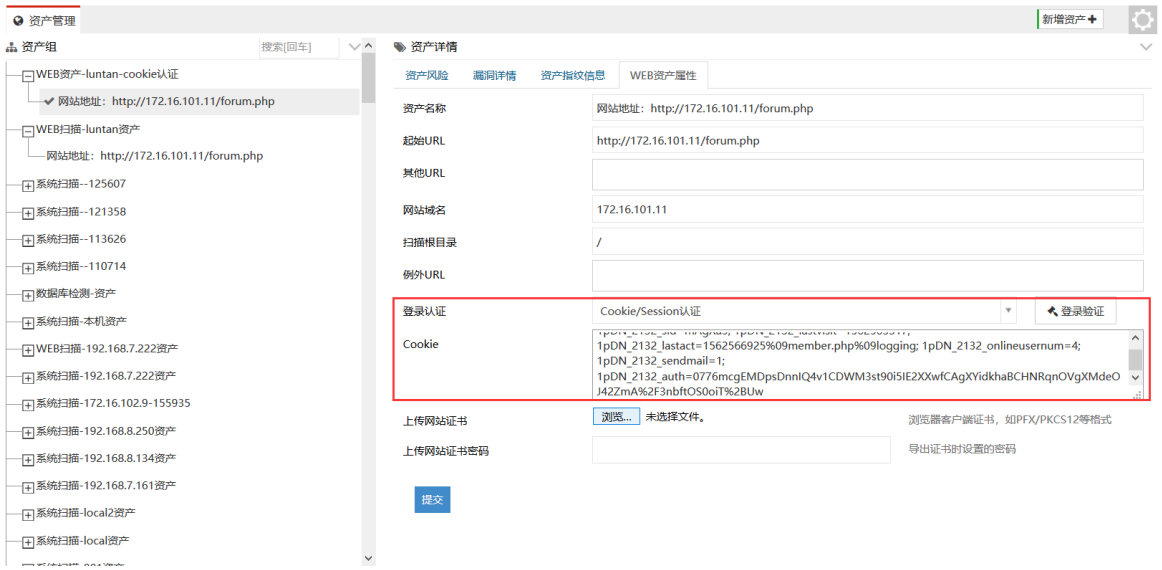


2、访问漏扫地址，用账号(admin)登录设备，在“资产管理”中，点击“新增资产”按钮，填入 web 扫描站点信息，点击提交。

图6-2 新增 web 资产

3、选择此新增站点，进入“资产详情>WEB 资产属性”界面，登录认证方式选择 Cookie/Session 认证，将步骤 1 中复制的内容，补充到起始 URL 后面，填入提交 URL 中，提交数据格式如下图中所示。

图6-3 Cookie 认证登录信息填入



5、在“任务中心>新建任务>WEB 扫描”中，选择“使用资产”，使用刚建立的资产，配置任务名称，点击提交。

图6-4 配置 Form 认证资产建立 Web 扫描任务

6.3 验证配置

1、在“任务中心>任务列表”中，可查看 Web 扫描任务。

图6-5 使用配置 Cookie 认证资产建立 Web 扫描任务

2、扫描完成后可查看扫描结果。

图6-6 登录后扫描的网站 URL

图6-7 Cookie 认证和未认证对比

7 Web Form 认证扫描配置举例

7.1 组网需求

Web 站点设置了主页登录，认证等方式，需要拿到登录认证对应的信息才能扫描到更多的结果。常见的 Web 登录方式绝大多数以 Cookie 认证、Form 认证为主；较少使用的 Web 登录方式有 Basic 认证；NTLM 认证是比较早期的认证技术，目前很少使用。本配置介绍了 Form 登录认证扫描配置方法。

7.2 配置步骤

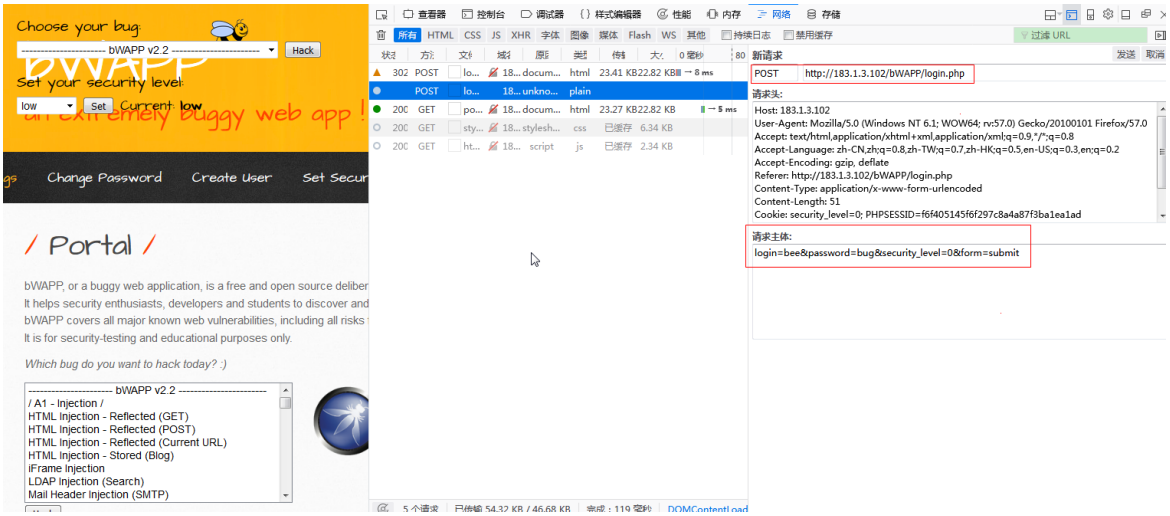
1、火狐浏览器登录需要扫描的网站，鼠标单击登录框，然后右键“查看元素”，点击即进入开发者模式。

图7-1 Form 信息获取

2、Login 与 Password 登录框输入用户密码，登录认证，开发者视图中查看 POST 提交信息，点击“编辑和重发”获取提交 URL 和提交数据信息。

图7-2 编辑和重发

图7-3 请求主体内容复制

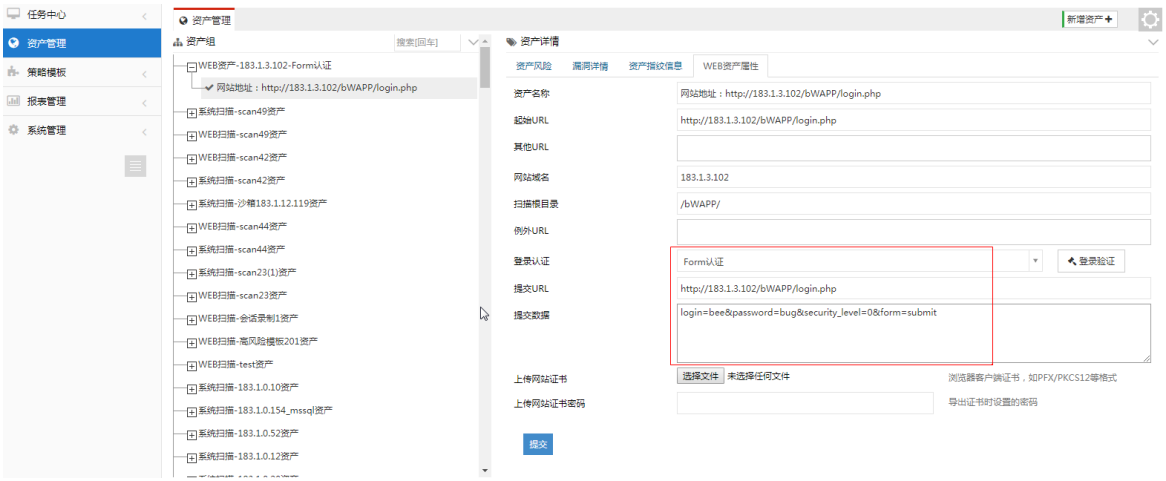


3、访问漏扫地址，用账号(admin)登录设备，在“资产管理”中，点击“新增资产”按钮，填入 web 扫描站点信息，点击提交。

图7-4 新增 web 资产

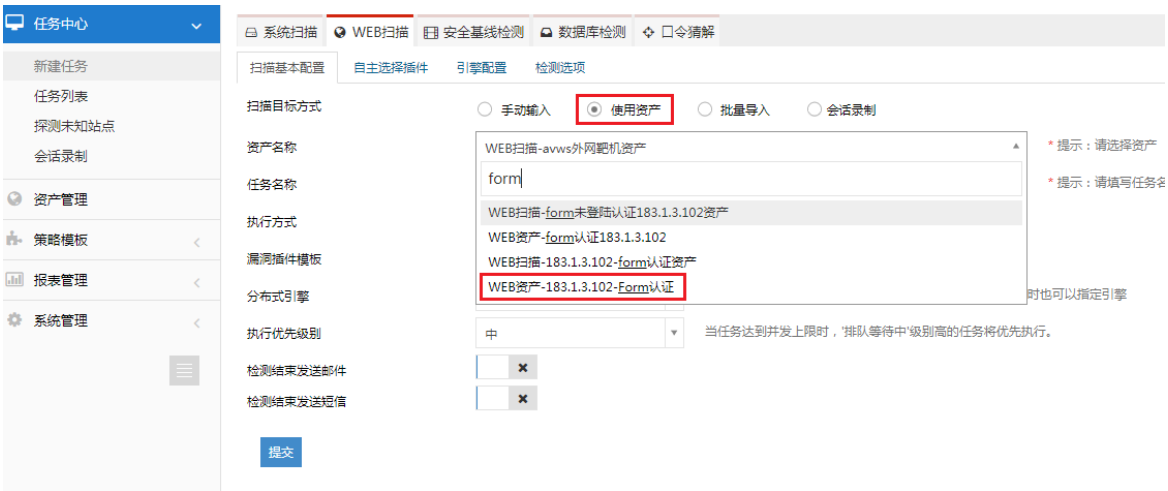
4、选择此新增站点，进入“资产详情>WEB 资产属性”界面，登录认证方式选择 Form 认证，将步骤 2 中复制的内容，补充到起始 URL 后面，填入提交 URL 中，提交数据格式如下图中所示。

图7-5 Form 认证登录信息填入



5、在“任务中心>新建任务>WEB 扫描”中，选择“使用资产”，使用刚建立的资产，配置任务名称，点击提交。

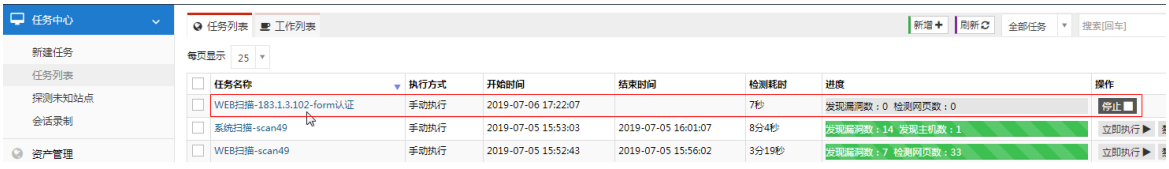
图7-6 配置 Form 认证资产建立 Web 扫描任务



7.3 验证配置

1、在“任务中心>任务列表”中，可查看 Web 扫描任务。

图7-7 使用配置 Form 认证资产建立 Web 扫描任务



2、扫描完成后可查看扫描结果。

图7-8 登录后扫描的网站 URL

图7-9 Form 认证和未认证对比