

UNIS XSCAN-CN60 漏洞扫描系统

典型配置举例

Copyright © 2022 紫光恒越技术有限公司及其许可者版权所有，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。本文档中的信息可能变动，恕不另行通知。

目 录

1 产品简介	1-1
2 配置前提	1
3 使用限制	1
4 典型组网	1
4.1 旁路部署网络结构	1
4.2 旁路部署配置	2
4.2.1 配置 IP 地址	2
4.2.2 策略配置	4
4.2.3 结果验证	6
4.2.4 导出报表	7
4.3 分布式部署网络结构	8
4.4 分布式部署配置	9
4.4.1 配置 IP 地址	9
4.4.2 配置分布式扫描引擎	11
4.4.3 配置分布式扫描管控中心	11
4.4.4 配置策略	12
4.4.5 2.4.4 结果验证	14
4.4.6 2.4.5 导出报表	15
5 会话录制配置举例	16
5.1 组网需求	16
5.2 配置步骤	16
5.3 验证配置	20
6 Web cookie 录制扫描配置举例	21
6.1 组网需求	21
6.2 配置步骤	22
6.3 验证配置	23
7 Web Form 认证扫描配置举例	25
7.1 组网需求	25
7.2 配置步骤	25
7.3 验证配置	28

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。



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。

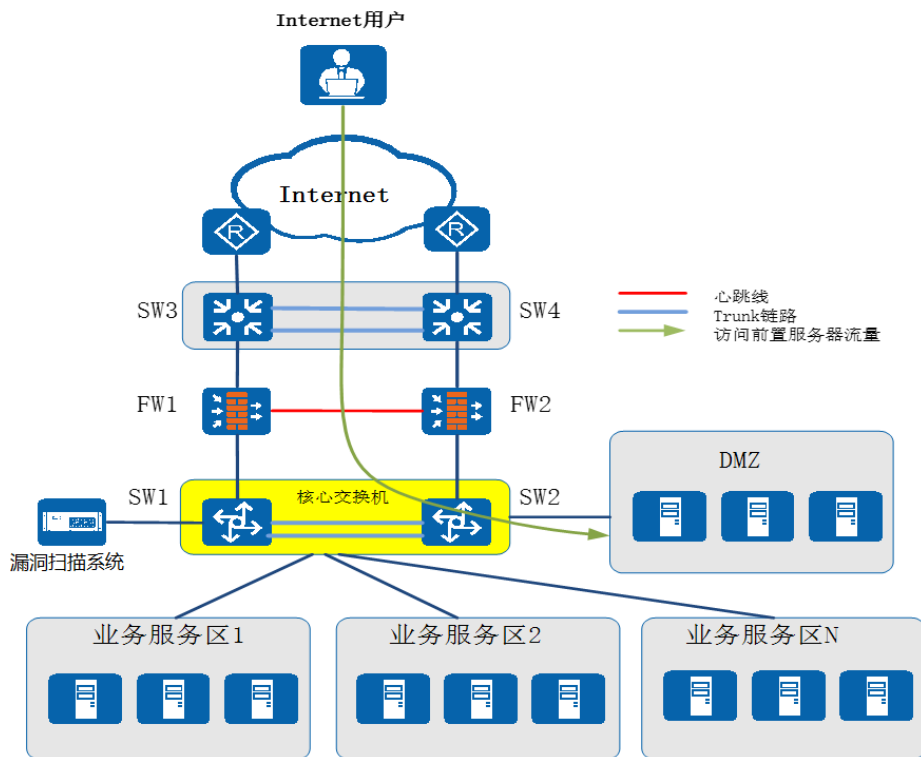
3 使用限制

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

IP管理配置						新增 +	刷新
VLAN名称	IP地址	子网掩码	Mtu	状态	操作		
MngtVlan	192.168.0.1 192.168.7.253	255.255.255.0 255.255.255.0	1500	应用	编辑 ✎	删除 ✕	

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 Management Configuration			
☐	Static IP	Subnet Mask / Subnet Length	Next Hop
☒	0.0.0.0	0.0.0.0	192.168.7.1
			Metric
			0

IP Management Configuration

Parameter	Description
VLAN Name	Name of the bridge interface
IP Address / Subnet Mask	IP address and subnet mask of the bridge
Status	Enable or disable the bridge interface
Operation	Delete or edit the bridge interface

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	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”。

The screenshot shows the 'New Task' configuration page for 'System Scan'. The 'Scan Target' field is set to 'http://172.16.101.74'. The 'Task Name' is 'WEB扫描-172.16.101.74'. The 'Execution Method' is 'Manual Input'. The 'Vulnerability Plugin Template' is 'All Web Vulnerabilities'. The 'Distributed Engine' is 'Default'. The 'Execution Priority' is 'Medium'. The 'Send Email' and 'Send SMS' checkboxes are both checked. The 'Submit' button is highlighted in blue.

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”。

The screenshot shows the 'Task List' interface. It displays a table with columns: Task Name, Execution Method, Start Time, End Time, Detection Time, Progress, and Actions. Two tasks are listed: 'WEB扫描-172.16.101.74' (Manual Input, 2019-03-29 00:00:06, 2 seconds, 0 vulnerabilities found) and '系统扫描-192.168.7.79' (Manual Input, 2019-03-28 23:56:46, 3 minutes 22 seconds, 1 vulnerability found). The 'Actions' column contains 'Pause' and 'Stop' buttons for each task.

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:fece: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	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。

任务名称	风险等级	漏洞详情	协议/端口
系统漏洞-192.168.7.79	高危	SSL/TLS 协议实现缺陷	tcp/www/443
	高危	SSL/TLS 加密协议实现缺陷(CVE-2014-3566)	tcp/www/443
	高危	OpenSSL 'sha256_verify' 函数缓冲区溢出漏洞(CVE-2014-0198)	tcp/www/443
	高危	OpenSSL 缓冲区溢出漏洞(CVE-2014-0199)	tcp/www/443
	高危	OpenSSL 竞争条件漏洞(CVE-2010-5286)	tcp/www/443
	高危	OpenSSL 资源管理缺陷漏洞(CVE-2014-0221)	tcp/www/443
	高危	OpenSSL 加密问题漏洞(CVE-2014-0234)	tcp/www/443
	高危	OpenSSL 安全漏洞(CVE-2014-3470)	tcp/www/443
	高危	具有错误主机名的SSL证书	tcp/www/443
	高危	SSL证书不信任	tcp/www/443
	高危	SSL自签名证书	tcp/www/443
	高危	HTTP响应头X-Content-Options: none	tcp/www/443
	高危	HTTP安全响应头Strict-Transport-Security	tcp/www/443
	高危	HTTP响应头使用X-Frame-Options	tcp/www/443
	高危	Windows NetBIOS / SMB远程主机信息暴露	udp/netbios-ng/137
	高危	HTTP响应头使用X-XSS-Protection	tcp/www/443
	高危	OpenSSL ECDSA 加密问题漏洞(CVE-2014-0076)	tcp/www/443

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。

任务名称	风险等级	漏洞名称	漏洞URL	漏洞参数
WEB扫描-172.16.101.74	高危	Http&Hostname攻击	http://172.16.101.74/	
	高危	域名沙箱限制不严格	http://172.16.101.74/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/original/fmg/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/original/cos/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/cos/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/fmg/	
	高危	使用了目录列表	http://172.16.101.74/phpmyadmin/themes/	
	高危	跨域策略配置不当	http://172.16.101.74/	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&id=...	
	高危	用户认证逻辑文件传输	http://172.16.101.74/forum.php?mod=forumdisplay&fid=2&filter=...	
	高危	隐藏的价格信息字段	http://172.16.101.74/home.php?view=all&mod=space&searchmod=...	
	高危	隐藏的价信息字段	http://172.16.101.74/home.php?mod=space&do=doing	
	高危	使用了危险的Method	http://172.16.101.74/	

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。

任务中心 资产管理 策略模板 报表管理 在线查询 对比分析 导出报表 系统管理	导出报表 选择导出对象 指定资产组 检测任务时间段 导出格式 导出方式 漏洞状态 漏洞标题 导出文件名 自定义HTML详细报表 自定义公司信息 设置压缩包密码 导出	系统扫描资产组 WEB扫描资产组 2019-03-29 00:00:06 至 2019-03-29 00:35:48 HTML WPS PDF ET XML 详细报表 新建 误报 已修复 漏洞扫描安全评估报告 WEB扫描-172.16.101.74资产 自定义HTML详细报表 自定义公司信息 设置压缩包密码 导出	提示：数据库检测，勾选请解任务都属于系统扫描范围 提示：仅显示已检测过的资产组 提示：开始时间-至-结束时间 提示：请选择导出方式 提示：必须，注释：漏洞默认状态为“新建”，用户可以在漏洞详情页更新漏洞状态 提示：请填写报表标题，限制：[4-30]字符之间，限制字符：\ / : * " < > [.] , ' . ! , 提示：请填写导出的文件名称，限制：[1-42]字符之间，限制字符：\ / : * " < > [.] , ' . ! ,
---	---	---	---

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。

任务中心

资产管理

策略模板

报告管理

在线查询

对比分析

导出报表

系统管理

导出报表

报表列表

输出报表

选择导出对象

系统扫描资产组

WEB扫描资产组

WEB扫描-172.16.101.74资产

2019-03-29 00:00:06 至 2019-03-29 00:35:48

HTML

WPS

PDF

ET

XML

详细报表

统计报表

新建

误报

已修复

漏洞扫描安全评估报告

导出文件名

WEB扫描-172.16.101.74资产

自定义HTML详细报表

自定义公司信息

设置压缩包密码

导出

提示：数据库检测、口令猜解任务都属于系统扫描范畴

提示：仅显示已检测过的资产组

提示：开始时间-至-结束时间

提示：请选择导出方式

提示：必选。注释：漏洞默认状态为“新建”，用户可以在漏洞详情页更新漏洞状态

提示：请填写报表标题。限制：[4-30]字符之间。限制字符：\/:?* "< > | . () , ' []

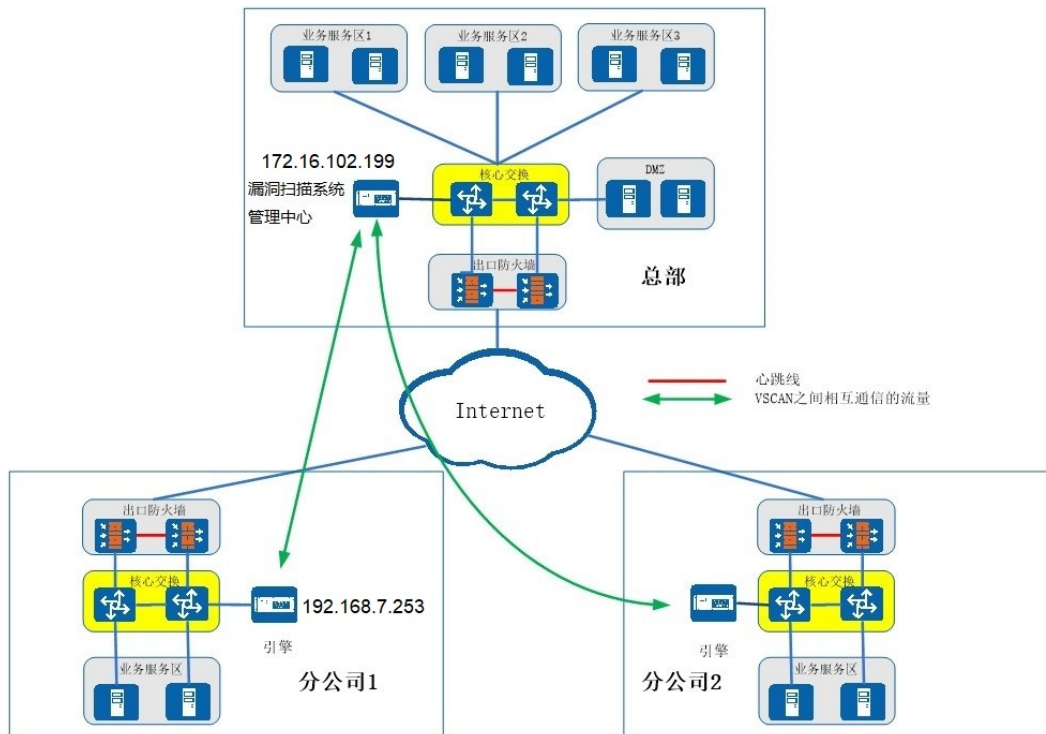
提示：请填写导出文件名。限制：[1-42]字符之间。限制字符：\/:?* "< > | . () , ' []

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

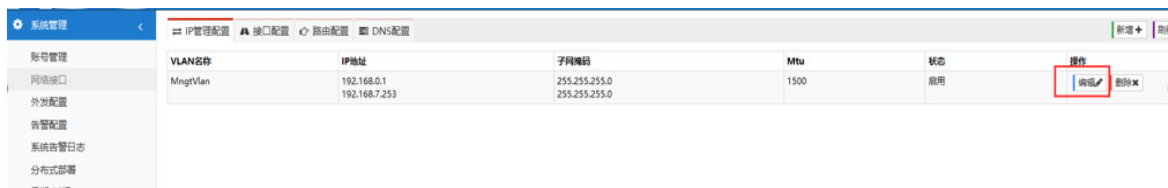
UNIS XSCAN-CN60 漏洞扫描系统支持分布式部署，集中管控中心既可作为管理端，也可以作为扫描引擎，统一下发扫描任务至下级引擎，并在管控中心统一分析、统一展示。



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。

IP地址	子网掩码	操作
192.168.0.1	255.255.255.0	删除 ✕
192.168.7.253	255.255.255.0	删除 ✕

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			
☐	目的地址	子网掩码/子网前缀长度	下一跳
☒	0.0.0.0	0.0.0.0	192.168.7.1
			Metric
			0

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。

分布式设置 引擎列表

基本选项

作为分布式引擎 ☒

引擎名称(别名) fenbushi * 提示：分布式引擎建议以IP地址组合的方式命名。例如：dist_192.168.1.100

管理中心地址 172.16.102.199 * 提示：本机地址为127.0.0.1；其他管理地址需填可达且有效的IP地址

提交

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。

分布式设置 引擎列表

基本选项

作为分布式引擎 ☒

引擎名称(别名) fenbushi * 提示：分布式引擎建议以IP地址组合的方式命名。例如：dist_192.168.1.100

管理中心地址 172.16.102.199 * 提示：本机地址为127.0.0.1；其他管理地址需填可达且有效的IP地址

提交

是否立即重新启动？重新启动后配置才能生效！

取消 确认

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。

分布式设置 引擎列表

增加引擎地址

引擎IP地址 192.168.7.253 * 提示：信任此IP地址，保证子工作引擎与主管理通信正常

提交

引擎名称 local

引擎名称 local

引擎名称 local

自动同步规则 Yes

自动同步规则 Yes

自动同步规则 Yes

添加完成后，可以在引擎列表中看到新增的引擎。

引擎名称	引擎类型	引擎IP	状态	自动同步策略	自动同步规则
local	WEB扫描引擎	127.0.0.1	启用	Yes	Yes
fenbushi	口令破解引擎	192.168.7.253	启用	Yes	Yes
local	系统扫描引擎	127.0.0.1	启用	Yes	Yes
fenbushi	WEB扫描引擎	192.168.7.253	启用	Yes	Yes
local	口令破解引擎	127.0.0.1	启用	Yes	Yes

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”。

系统扫描

WEB扫描

数据库检测

口令破解

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

扫描目标方式

手动输入

使用资产

批量导入

扫描目标

192.168.7.79

* 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:fece:ba23:cd1f:dc61:1010:9234:4088
 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

系统扫描-192.168.7.79

* 提示：请填写任务名称，长度在[1-40]字符之间

执行方式

立即执行

* 提示：请选择执行方式

检测模式

完全扫描

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

全部漏洞扫描

* 提示：请选择漏洞插件模板

分布式引擎

fenbushi

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

中

当任务达到开发上限时，'排队等待'中'级别高'的任务将优先执行。

检测结束发送邮件

✖

检测结束发送短信

✖

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”。

任务名称	执行方式	开始时间	结束时间	检测耗时	进度	操作
系统扫描-192.168.7.79	手动执行	2019-03-28 23:56:46		1秒	发现漏洞数: 0 发现主机数: 0	暂停 停止

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:fece: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	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”。

系统扫描 WEB扫描 数据库检测 命令解释

扫描基本配置 自主选择插件 引擎配置 检测选项

扫描目标方式 ☒ 手动输入 ☐ 使用资产 ☐ 批量导入 ☐ 会话复制

扫描目标

任务名称

执行方式

漏洞插件模板

分布式引擎

执行优先级

检测结束发送邮件 ☒

检测结束发送短信 ☒

* 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:fece:ba23:cd1f:dcb1:1010:9234:4088]/
 多个URL以英文逗号(,)或回车分隔

* 提示：请填写任务名称，长度在[1-40]字符之间

* 提示：请选择执行方式

* 提示：请选择漏洞插件模板

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

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。

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”。

任务列表

工作列表

新建 +

刷新

全部任务

搜索[回车]

每页显示

25

☐ 任务名称	执行方式	开始时间	结束时间	检测耗时	进度	操作
☐ WE扫描-172.16.101.74	手动执行	2019-03-29 00:00:06		2秒	发现漏洞数: 0 检测网页数: 0	查看 停止
☐ 系统扫描-192.168.7.79	手动执行	2019-03-28 23:56:46		3分22秒	漏洞数: 1 主机数: 1 剩余时间: 大于1小时	查看 停止

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:fece: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	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。

任务中心

资产管理

策略模板

资产管理

在线漏洞

对比分析

导出报表

系统管理

系统漏洞

WEB漏洞

资产设备漏洞查询

漏洞类型: 任务

搜索[回车]

☒ 有
☐ 中
☒ 低

搜索[回车]

任务名称

系统漏洞: 192.168.7.79

创建时间

2019-03-28 23:56:46 至 2019-03-29 00:05:42

总计1条记录

风险等级	漏洞名称	协议/服务/端口
高危	SSL脚本和协议检测	tcp/www/443
高危	SSL.0 加密协议信息暴露漏洞(CVE-2014-3560)	tcp/www/443
高危	OpenSSL 'do_ssl_write' 函数缓冲区溢出漏洞(CVE-2014-0198)	tcp/www/443
高危	OpenSSL 缓冲区溢出漏洞(CVE-2014-0195)	tcp/www/443
高危	OpenSSL 竞争条件漏洞(CVE-2010-5298)	tcp/www/443
高危	OpenSSL 堆栈管理缺陷漏洞(CVE-2014-0221)	tcp/www/443
高危	OpenSSL 加密问题漏洞(CVE-2014-0224)	tcp/www/443
高危	OpenSSL 安全漏洞(CVE-2014-3470)	tcp/www/443
高危	具有特权主机的SSL证书	tcp/www/443
高危	SSL证书不能信任	tcp/www/443
高危	SSL自签证书	tcp/www/443
高危	HTTP响应头X-Content-Options: nosniff	tcp/www/443
高危	HTTP安全响应头Strict-Transport-Security	tcp/www/443
高危	HTTP响应头不使用X-Frame-Options	tcp/www/443
高危	Windows NetBIOS / SMB进程主机信息暴露	udp/netbios-m/137
高危	HTTP响应头使用X-XSS-Protection	tcp/www/443
高危	OpenSSL ECDSA 加密问题漏洞(CVE-2014-0076)	tcp/www/443

总计17条记录

<

1

>

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。

漏洞名称	漏洞URL	漏洞参数
Httpk Hostname 攻击	http://172.16.101.74/	
域名访问限制不严格	http://172.16.101.74/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/original/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/original/img/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/original/css/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/css/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/darkblue_orange/img/	
应用了目录列表	http://172.16.101.74/phpmyadmin/themes/	
跨域策略配置不当	http://172.16.101.74/	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
发现内网IP地址	http://172.16.101.74/member.php?mod=logging&action=login&lo...	
用户认证信息明文传输	http://172.16.101.74/forum.php?mod=forumdisplay&fid=2&filter=...	
隐藏的敏感信息字段	http://172.16.101.74/home.php?view=all&mod=space&searchmod=...	
隐藏的敏感信息字段	http://172.16.101.74/home.php?mod=space&do=doing	
应用了危险的Method	http://172.16.101.74/	

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。

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

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

任务中心

新建任务

任务列表

探测未知站点

会话录制

资产管理

策略模板

会话录制

录制 +

刷新

设置

☐ 历史会话名称	检测目标	开始时间	结束时间	URL数量	操作
☐ 183.1.3.102_20190521162222.dat	183.1.3.102	2019-05-21 16:21:51	2019-05-21 16:22:22	6	下发任务 查看
☐ 183.1.3.24_20190521095113.dat	183.1.3.24	2019-05-21 09:48:19	2019-05-21 09:51:13	14	下发任务 查看
☐ 183.1.3.102_20190624162527.dat	183.1.3.102	2019-06-24 16:25:13	2019-06-24 16:25:27	22	下发任务 查看
☐ 183.1.3.24_20190620161202.dat	183.1.3.24	2019-06-20 16:10:11	2019-06-20 16:12:02	14	下发任务 查看
☐ 101.7.0.21_20190620160646.dat	101.7.0.21	2019-06-20 16:05:48	2019-06-20 16:06:46	12	下发任务 查看

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

会话录制

域名

183.1.3.102

步骤1：首先填写需要录制的域名，点击开始按钮开始录制

步骤2：其次在另外一个浏览器配置http代理,代理服务IP为此设备IP端口为8080

步骤3：然后在配置了http代理的浏览器上，依次访问需要录制的url

注：域名对字符限制：'\',' ','|','\$','%','\','\n','<','>','/','?','!','"','(',')',' '

注：此次录制只允许在本机所在的浏览器进行录制

已录制的URL

开始录制 ▶

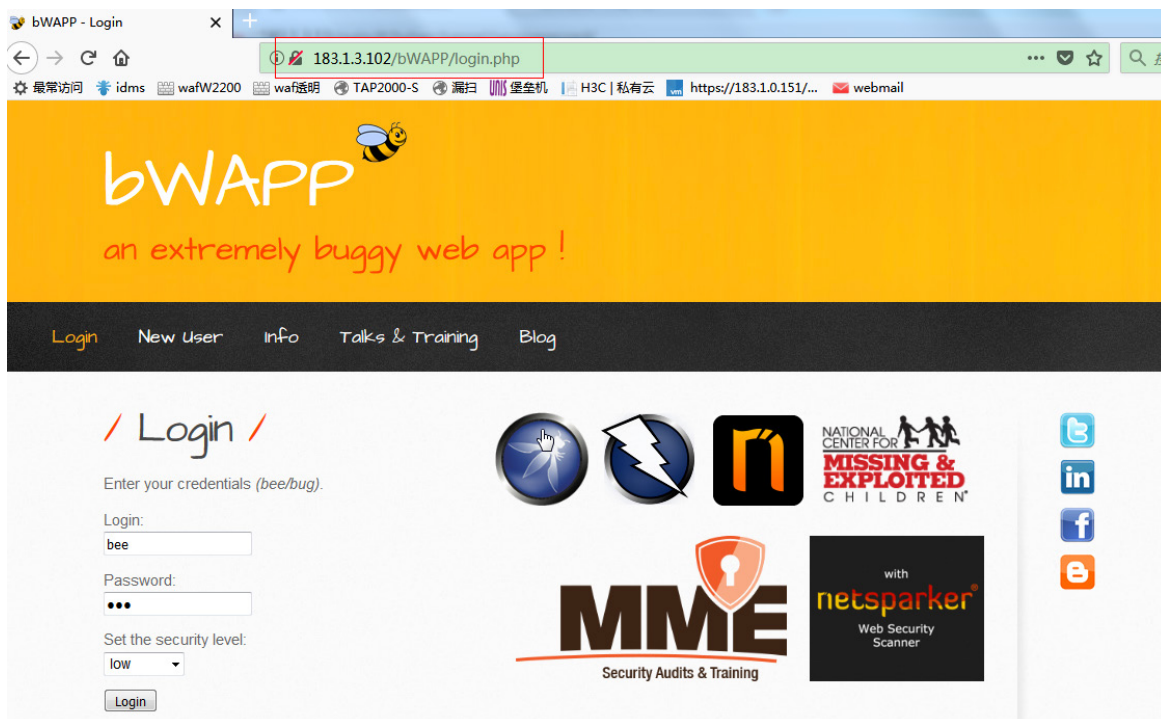
3、使用火狐浏览器做代理配置，进入“选项>常规>网络代理>设置”，配置手动代理设置，“HTTP代理”填入漏扫设备地址，端口填写 8080，点击确定。

图5-3 浏览器中代理配置



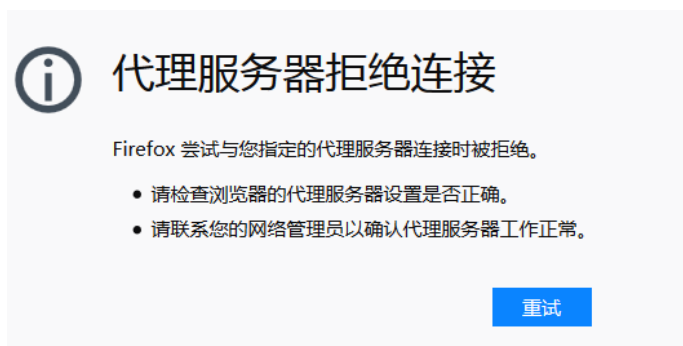
4、关闭火狐浏览器，重新打开，依次访问录制的域名。

图5-4 代理服务器访问域名



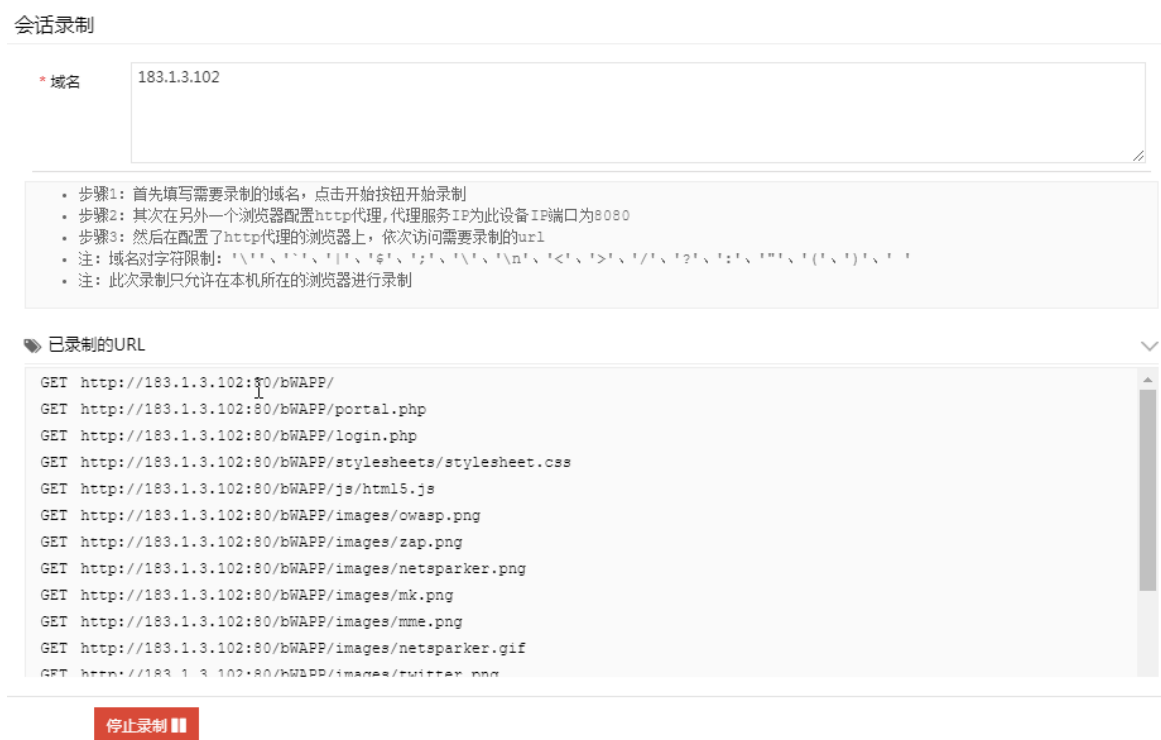
注意：若出现“代理服务器拒绝连接”，可多次点击重试即可。

图5-5 代理服务器拒绝连接



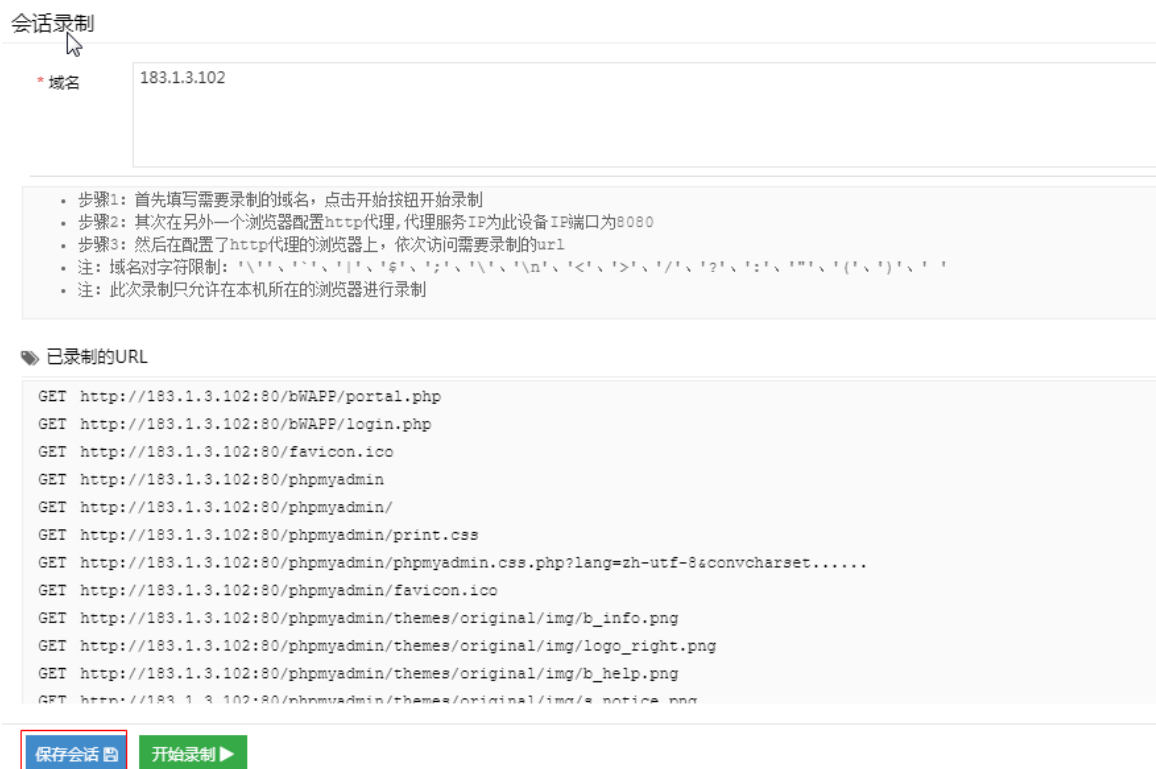
5、在访问结束后点击“停止录制”。

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

会话录制

录制 + 刷新

☐	历史会话名称	检测目标	开始时间	结束时间	URL数量	操作
☐	183.1.3.102_20190626192621.dat	183.1.3.102	2019-06-26 19:21:12	2019-06-26 19:26:21	25	下发任务 ▶ 查看
☐	183.1.3.102_20190521162222.dat	183.1.3.102	2019-05-21 16:21:51	2019-05-21 16:22:22	6	下发任务 ▶ 查看
☐	183.1.3.24_20190521095113.dat	183.1.3.24	2019-05-21 09:48:19	2019-05-21 09:51:13	14	下发任务 ▶ 查看
☐	183.1.3.102_20190624162527.dat	183.1.3.102	2019-06-24 16:25:13	2019-06-24 16:25:27	22	下发任务 ▶ 查看
☐	183.1.3.24_20190620161202.dat	183.1.3.24	2019-06-20 16:10:11	2019-06-20 16:12:02	14	下发任务 ▶ 查看
☐	101.70.21_20190620160646.dat	101.70.21	2019-06-20 16:05:48	2019-06-20 16:06:46	12	下发任务 ▶ 查看
☐	183.1.3.102_20190620160121.dat	183.1.3.102	2019-06-20 16:00:52	2019-06-20 16:01:21	24	下发任务 ▶ 查看
☐	183.1.3.102_20190521092353.dat	183.1.3.102	2019-05-21 09:22:13	2019-05-21 09:23:53	6	下发任务 ▶ 查看

总计8条记录

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

系统扫描		WEB扫描	安全基线检测	数据库检测	命令嗅探
扫描基本配置		自主选择插件	引擎配置	检测选项	
扫描目标方式	☐ 手动输入 ☐ 使用资产 ☐ 批量导入 ☒ 会话录制				
历史会话	183.1.3.102_20190626192621.dat				* 提示：录制新会话,请前往会话录制
任务名称	WEB扫描-				* 提示：请填写任务名称,长度在[1-40]字符之间
执行方式	立即执行				* 提示：请选择执行方式
漏洞插件模板	全部WEB漏洞				* 提示：请选择漏洞插件模板
分布式引擎	默认				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	中				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。
检测结果发送邮件	☐				
检测结果发送短信	☐				
提交					

6 Web cookie 录制扫描配置举例

6.1 组网需求

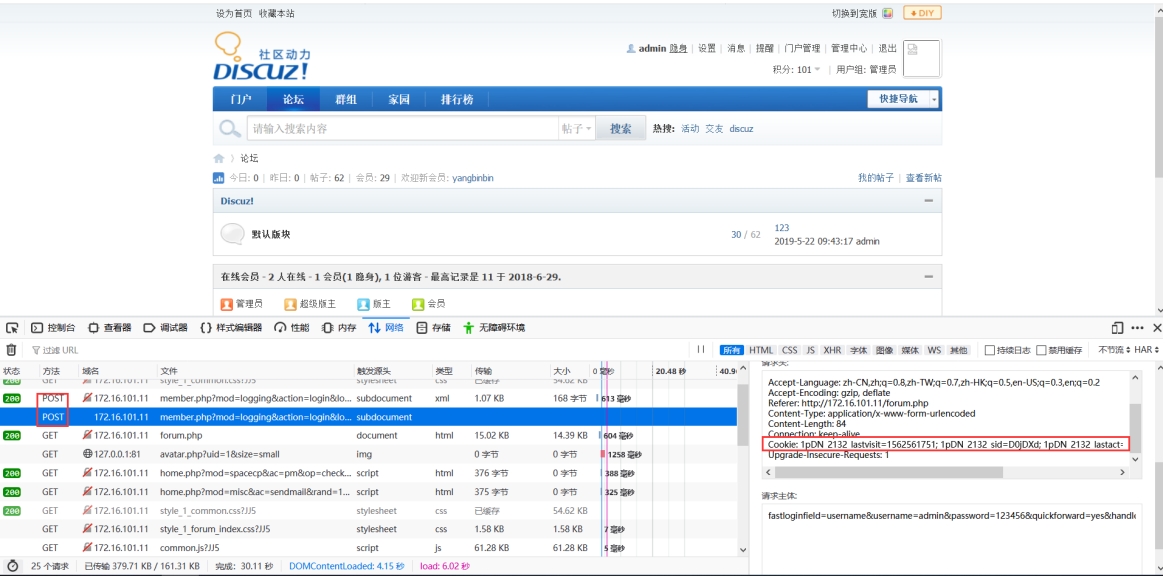


Web 站点设置了主页登录, 认证等方式, 需要拿到登录认证对应的信息才能扫描到更多的结果。常见的 Web 登录方式绝大多数以 Cookie 认证、Form 认证为主; 较少使用的 Web 登录方式有 Basic 认证; NTLM 认证是比较早期的认证技术, 目前很少使用。本配置介绍了 Cookie 认证扫描配置方法。

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



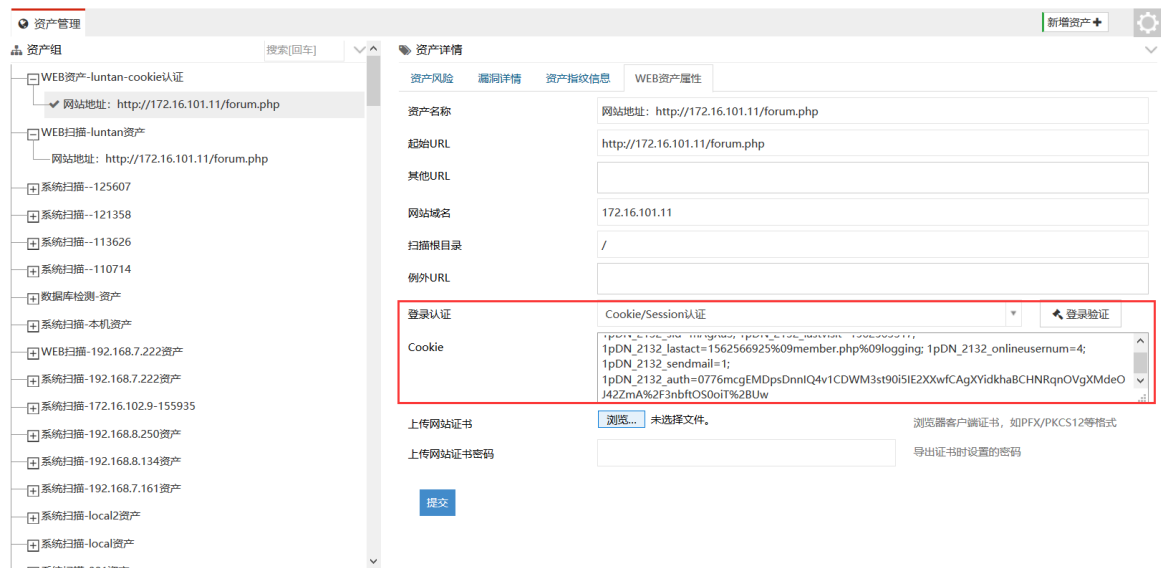
2、访问漏扫地址，用账号(admin)登录设备，在“资产管理”中，点击“新增资产”按钮，填入 web 扫描站点信息，点击提交。

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

任务列表							新增 +	刷新	全部任务	搜索[回车]	设置
每页显示 25											
☐	任务名称	执行方式	开始时间	结束时间	检测耗时	进度	操作				
☐	WEB扫描-luntan-cookie认证	手动执行	2019-07-08 14:30:16		12秒	发现漏洞数: 0 检测网页数: 0	暂停 停止				

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

任务列表 工作列表							
新增 + 刷新 全部任务 搜索[回车]							
每页显示 25							
任务名称	执行方式	开始时间	结束时间	检测耗时	进度	操作	
WEB扫描-luntan-cookie认证	手动执行	2019-07-08 16:32:25	2019-07-08 17:27:53	55分28秒	发现漏洞数: 145 检测网页数: 1698	立即执行 ▶	禁用 ⏻
WEB扫描-luntan	手动执行	2019-07-08 16:14:01	2019-07-08 16:34:07	20分6秒	发现漏洞数: 15 检测网页数: 401	立即执行 ▶	禁用 ⏻

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

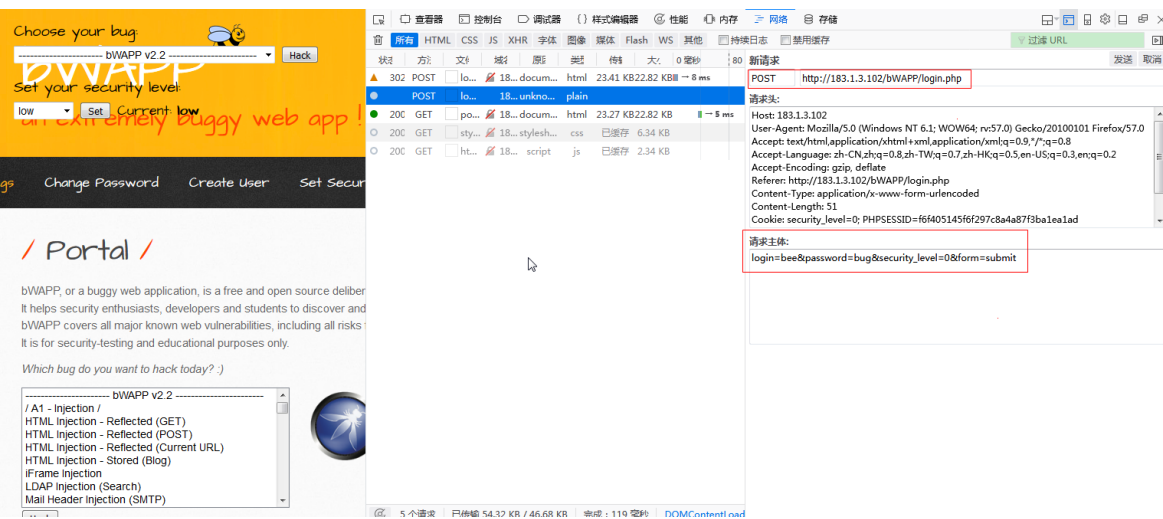


2、Login 与 Password 登录框输入用户密码，登录认证，开发者视图中查看 POST 提交信息，点击“编辑和重发”获取提交 URL 和提交数据信息。

图7-2 编辑和重发



图7-3 请求主体内容复制



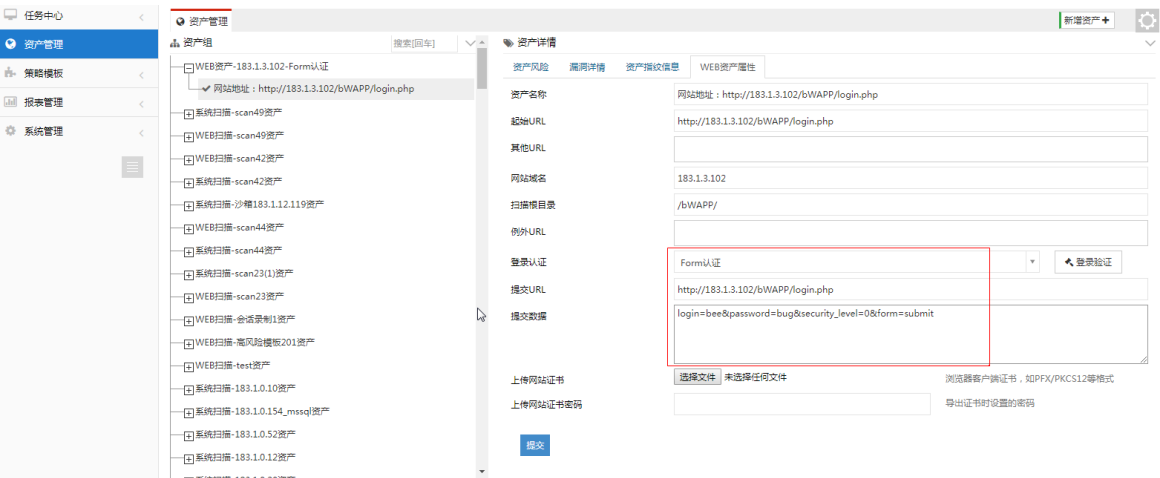
3、访问漏扫地址，用账号(admin)登录设备，在“资产管理”中，点击“新增资产”按钮，填入 web 扫描站点信息，点击提交。

图7-4 新增 web 资产



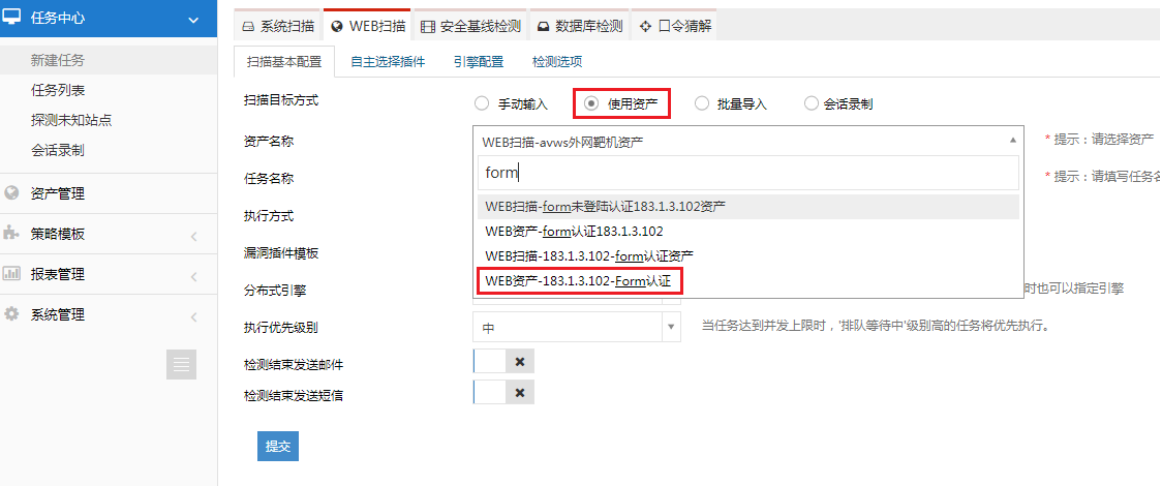
4、选择此新增站点，进入“资产详情>WEB 资产属性”界面，登录认证方式选择 Form 认证，将步骤 2 中复制的内容，补充到起始 URL 后面，填入提交 URL 中，提交数据格式如下图中所示。

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

每页显示 25

☐	任务名称	执行方式	开始时间	结束时间	检测耗时	进度	操作
☐	WEB扫描-183.1.0.102-未认证	手动执行	2019-07-06 17:59:48	2019-07-06 18:02:07	2分19秒	发现漏洞数: 65 检测网页数: 110	立即执行 ▶ 禁用 ⏻
☐	WEB扫描-183.1.3.102-form认证	手动执行	2019-07-06 17:22:07	2019-07-06 17:27:53	5分46秒	发现漏洞数: 149 检测网页数: 747	立即执行 ▶ 禁用 ⏻
☐	系统扫描-scan49	手动执行	2019-07-05 15:53:03	2019-07-05 16:01:07	8分4秒	发现漏洞数: 14 发现主机数: 1	立即执行 ▶ 禁用 ⏻