

UNIS XSCAN-CN80 系列漏洞扫描系统

典型配置

Copyright © 2023 紫光恒越技术有限公司 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、复制本档容的部分或全部，并不得以任何形式传播。

除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

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 典型组网	1
3.1 旁路部署网络结构	1
3.2 旁路部署配置	2
3.2.1 配置 IP 地址	2
3.2.2 策略配置	4
3.2.3 结果验证	6
3.2.4 导出报表	6
3.3 分布式部署网络结构	8
3.4 分布式部署配置	8
3.4.1 配置 IP 地址	8
3.4.2 配置分布式扫描引擎	9
3.4.3 配置分布式扫描管控中心	10
3.4.4 配置策略	10
3.4.5 结果验证	13
3.4.6 导出报表	13
4 会话录制配置举例	14
4.1 组网需求	14
4.2 配置步骤	15
4.3 验证配置	17
5 Web cookie 录制扫描配置举例	19
5.1 组网需求	19
5.2 配置步骤	19
5.3 验证配置	21
6 Web Form 认证扫描配置举例	22
6.1 组网需求	22
6.2 配置步骤	22
6.3 验证配置	25

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 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。

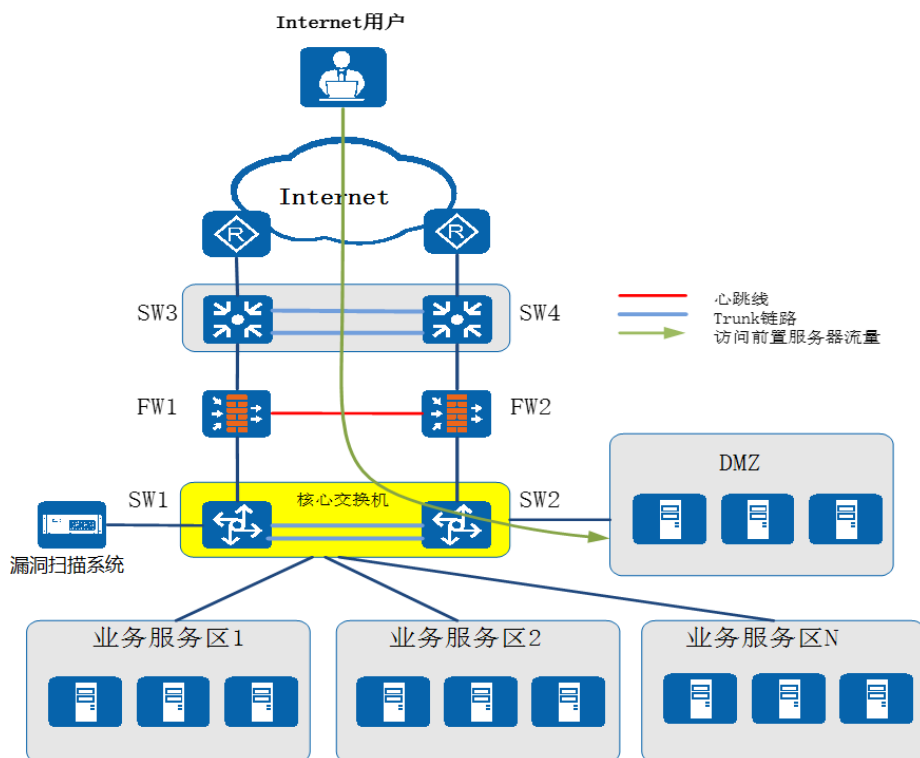


扫描任务中若检测到 1 个扫描目标在线，则会占用 1 个 IP 数量授权，占用后删除资产可以释放授权，E6202P04 版本以及之后版本支持资产删除。

3 典型组网

3.1 旁路部署网络结构

UNIS 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。



3.2 旁路部署配置

3.2.1 配置 IP 地址

用账号(account)登录设备，在“系统管理>网络接口>IP 管理配置”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3-1 IP 管理配置

UNIS 漏洞扫描系统						
系统管理	IP管理配置	接口配置	路由配置	DNS配置	自动DHCP+	新增+
账号管理					刷新	搜索(回车)
网络接口						
外发配置						
报警配置						
分布式部署						
日期/时间						
VLAN名称	IP地址	子网掩码	Mtu	状态	操作	
MngtVlan	192.168.0.1	255.255.255.0	1500	启用	编辑	删除
	172.16.102.153	255.255.255.0				
	2001:fece:bba2:3cd1:fdcb1:1010:9234:4088	0				
总计1条记录						

再点击“下一步”调过 VLAN 基本配置。

VLAN接口配置

1 基本配置

2 接口IP地址配置

VLAN编号

1

* [系统内置VLAN编号为1
新增VLAN号请输入[2-4094]之间，且不同于已有VLAN号的数字]

VLAN名称

MngtVlan

VLAN名称，不定义名称则默认命名为：VLAN编号

Mtu

1500

*

状态

启用

*

下一步

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。

VLAN接口配置

1 基本配置

2 接口IP地址配置

新增

支持IPv4以及IPv6网络地址
IPv6示例：2001:feceb3:2cd1:fdcb1:1010:9234:4088 IPv6前缀范围：0-128

IP地址	子网掩码	操作
192.168.7.253	255.255.255.0	保存 取消
192.168.0.1	255.255.255.0	删除
192.168.13.177	255.255.255.0	删除

完成

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

接口配置

路由配置

DNS配置

新增 刷新 搜索[回车]

自始地址	子网掩码/子网前缀长度	下一跳	Metric
☐ 0.0.0.0	0.0.0.0	192.168.13.1	0

总计1条记录

< 1 >

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

3.2.2 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，占用后删除资产可以释放授权，E6202P04 版本以及之后版本支持资产删除。

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: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

配置信息	说明
	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”。

任务ID	任务名称	扫描类型	扫描目标	检测结果	执行方式	优先级	任务状态	操作
31	http://172.16.101.74	WEB漏洞扫描	http://172.16.101.74	高(0) 中(0) 低(0) 信息(0)	立即执行	中	排队	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

配置信息	说明
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

3.2.3 结果验证

查看漏洞类别

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>漏洞类别”中，查看系统扫描的详细结果。

任务中心

资产管理

策略模板

系统管理

资产漏洞查询

全部资产 搜索...[回车键可搜索]

资产组 ...

漏洞等级 ...

查询 重置

导出Excel

漏洞列表

资产	漏洞等级	漏洞名称	漏洞数量	漏洞类别	端口/服务	漏洞评分
172.18.0.49	高风险	Microsoft Windows SMB服务器多个漏洞 (ms17-010) 【原理扫描】	1	默认探测	445/microsoft-ds	9.3
172.18.0.49	高风险	检测到目标操作系统已停止维护 【原理扫描】	1	默认探测	445/microsoft-ds	10
172.18.0.49	高风险	Oracle Database SQL注入漏洞 (CVE-2005-0297)	1	SQL注入	1521/oracle-tns	7.5
172.18.0.49	高风险	Oracle数据库服务器MDSYS.SDO_CS软件包远程溢出漏洞 (CVE-200...	1	缓冲区溢出	1521/oracle-tns	8.5
172.18.0.49	高风险	Oracle数据库服务器Listener组件未明安全漏洞 (CVE-2010-0911)	1	其它	1521/oracle-tns	7.8
172.18.0.49	高风险	Oracle Database Server Core RDBMS组件远程安全漏洞 (CVE-201...	1	其它	1521/oracle-tns	7.1
172.18.0.49	高风险	null	1		1521/oracle-tns	0.0
172.18.0.49	高风险	Microsoft Windows SMB服务器多个漏洞 (ms17-010) 【原理扫描】	1	默认探测	445/microsoft-ds	9.3
172.18.0.49	高风险	Oracle Database SQL注入漏洞 (CVE-2005-0297)	1	SQL注入	1521/oracle-tns	7.5
172.18.0.49	高风险	Oracle数据库服务器MDSYS.SDO_CS软件包远程溢出漏洞 (CVE-200...	1	缓冲区溢出	1521/oracle-tns	8.5
172.18.0.49	高风险	Oracle数据库服务器Listener组件未明安全漏洞 (CVE-2010-0911)	1	其它	1521/oracle-tns	7.8
172.18.0.49	高风险	Oracle Database Server Core RDBMS组件远程安全漏洞 (CVE-201...	1	其它	1521/oracle-tns	7.1
172.18.0.203	高风险	OpenSSL 信息泄露漏洞 (CVE-2016-2183) 【原理扫描】	1	默认探测	5989/https	7.5
172.18.0.203	高风险	OpenSSL 缓冲区溢出漏洞 (CVE-2017-3731)	1	缓冲区溢出	443/vmware esxi se...	7.5
172.18.0.203	高风险	OpenSSL 代码问题漏洞 (CVE-2017-3730)	1	代码问题	443/vmware esxi se...	7.5
172.18.0.203	高风险	多款VMware产品缓冲区溢出漏洞 (CVE-2017-4903)	1	缓冲区溢出	443/vmware esxi se...	8.8

CPU使用率: 0.00% 内存使用率: 2964M/7860M 硬盘使用率: 34G/1.8T

3.2.4 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

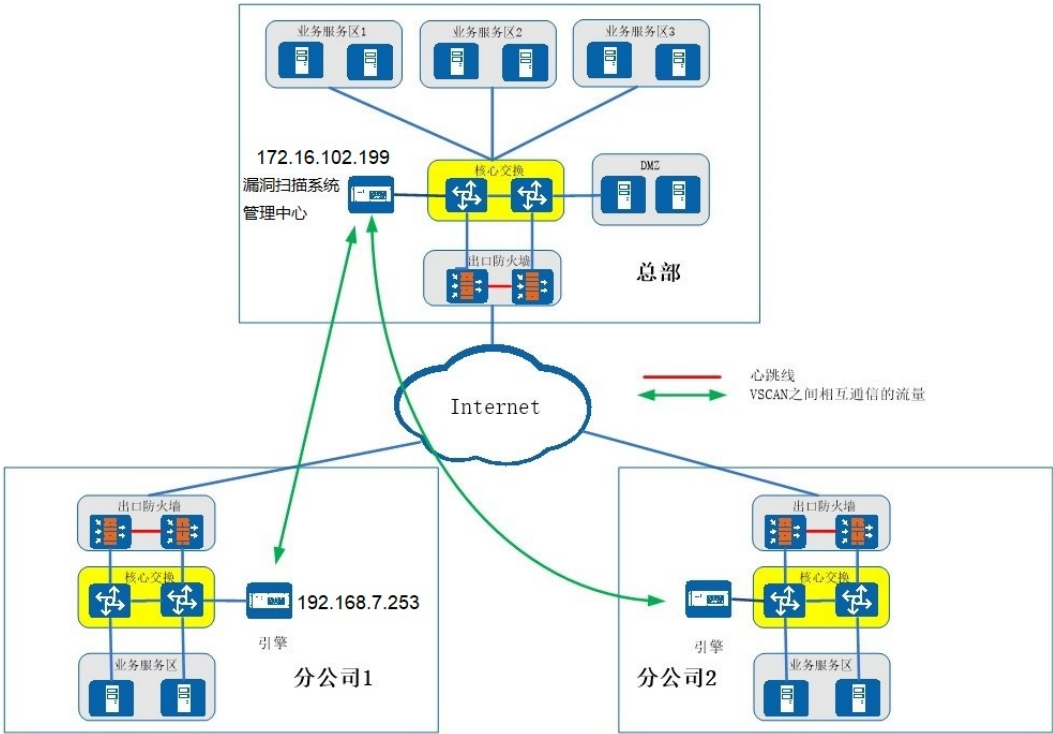
添加的系统扫描任务执行结束后，可以在“报表管理>导出报表”中，选择“Web 扫描资产”，然后选择“指定资产”、“检测任务时间段”和“导出格式”，最后点击“导出”按钮导出报表。

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、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

3.3 分布式部署网络结构

UNIS 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。



3.4 分布式部署配置

3.4.1 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。

VLAN接口配置

1 基本配置

2 接口IP地址配置

VLAN编号	1	* [系统内置VLAN编号为1 新增VLAN号请输入[2-4094]之间，且不同于已有VLAN号的数字]
VLAN名称	MngtVlan	VLAN名称，不定义名称则默认命名为：VLAN编号
Mtu	1500	*
状态	启用	*

下一步

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。

VLAN接口配置

1 基本配置

2 接口IP地址配置

新增+

支持IPv4以及IPv6网络地址
IPv6示例：2001:fece:ba23:cd1f:dc1:1010:9234:4088 IPv6前缀范围：0-128

IP地址	子网掩码	操作
192.168.7.253	255.255.255.0	保存+ 取消-
192.168.0.1	255.255.255.0	删除
192.168.13.177	255.255.255.0	删除

完成

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 网络接口配置 路由配置 DNS配置

新增+ 删除- 搜索[回车]

自始地址	子网掩码/子网前缀长度	下一跳	Metric
☐ 0.0.0.0	0.0.0.0	192.168.13.1	0

总计1条记录

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

3.4.2 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 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)

管理中心地址

提交

提示：开启后当前设备将只作为扫描工作引擎。

限制：长度在[5-32]之间。提示：分布式引擎建议使用IP地址组合的方式命名。例如：dist_192.168.1.100

提示：本机地址为127.0.0.1；其他管理地址需填写可达且有效的IP地址

注意：开启分布式的管理中心地址不能配置自己的管理地址！

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)

管理中心地址

提交

提示：开启后当前设备将只作为扫描工作引擎。

限制：长度在[5-32]之间。提示：分布式引擎建议使用IP地址组合的方式命名。例如：d

提示：本机地址为127.0.0.1；其他管理地址需填写可达且有效的IP地址

注意：开启分布式的管理中心地址不能配置自己的管理地址！

确定开启分布式？提示：提交后会重启设备，若无更改配置，则不会重启。

取消 确认

3.4.3 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。

SecPath 漏洞扫描系统

增加引擎地址

引擎IP地址

提交

提示：请在此IP地址，保证子引擎与主控管理中心正常通信

添加完成后，可以在引擎列表中看到新增的引擎。

分布式设置

引擎列表

增加引擎地址 +

删除 -

引擎名称	引擎类型	引擎IP	状态	自动同步策略	自动同步策略
local	WEB扫描引擎	127.0.0.1	启用	Yes	Yes
local	基础核查引擎	127.0.0.1	启用	Yes	Yes
local	系统扫描引擎	127.0.0.1	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

3.4.4 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，占用后删除资产可以释放授权，E6202P04 版本以及之后版本支持资产删除。

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”。

任务中心

新建任务

任务列表

探测未知站点

安全基线检测

数据率检测

会话录制

资产管理

策略模板

报告管理

系统管理

基本配置

高级选项

新建任务类型

扫描目标方式

扫描目标

任务名称

执行方式

系统漏洞模板

检测模式

调试模式

执行优先级

分布式引擎

告警模板

☒系统扫描

☐Web扫描

☐口令破解

☐仅存活探测

☒手动输入

☐使用资产

☐批量导入

192.168.7.79

立即执行

全部漏洞扫描

标准扫描

☒

中

默认

无

* 提示：如勾选仅做基础探测，则不进行漏洞扫描，仅探测资产存活状态和端口开放情况

* 扫描目标填写规范：
IPv4示例：192.168.1.100/IPv6示例：xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
IP段示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254,192.168.1.*
域名示例：www.example.com
URL示例：http://192.168.1.100/https://www.example.com/
http://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]/
排除IP或IP段：!192.168.1.1/24,!192.168.1.1-255,!192.168.1.1
类似192.168.3.cc、192.168.bb.cc、192.aa.bb.cc格式将会被视为域名，请确认后提交
多个之间以英文逗号(,)或换行分隔

* 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

标准扫描：默认选择标准漏洞的漏洞范围，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
快速扫描：快速的对扫描目标进行主机存活、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
完全扫描：默认选择全部漏洞的漏洞范围，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
深度扫描：利用配置好的用户名密码列表对主机进行登录后的安全扫描
若开启，则记录目标详细操作执行日志。
* 提示：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
* 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
* 注意：下推口令破解任务若使用非默认字典，系统将会自动选择本地默认引擎
* 提示：告警发送配置，请到[系统管理>任务告警]下设置

提交

CPU使用率: 0.50% 内存使用率: 2954MB/7860MB 硬盘使用率: 34G/1.8T

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ID	任务名称	扫描类型	扫描目标	检测结果	执行方式	优先级	任务状态	操作
32	192.168.7.79	系统扫描	192.168.7.79	高(0) 中(0) 低(0) 信息(0)	立即执行	中	排队	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:dc11:1010:9234:4088 * 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。

配置信息	说明
	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”。

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: <code>http://www.example.com/</code> 或 <code>https://www.example.com/</code> URL地址: <code>http://192.168.1.100/</code> 或 <code>https://192.168.1.100/</code> IPv6 URL示例: <code>http://[2001:fece:ba23:cd1f:dcb1:1010:9234:4088]/</code> 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

配置信息	说明
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

3.4.5 结果验证

查看漏洞类别

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>漏洞类别”中，查看系统扫描的详细信息。

任务中心

资产管理

策略模板

系统管理

报表管理

数据查询

对比分析

导出报表

资产漏洞查询

全部资产 | 搜索... (回车键可搜索)

资产组 ...

漏洞等级 ...

查询

重置

导出Excel

资产	漏洞等级	漏洞名称	漏洞数量	漏洞类别	端口/服务	漏洞评分
172.18.0.49	高风险	Microsoft Windows SMB服务器多个漏洞 (ms17-010) 【原理扫描】	1	默认探测	445/microsoft-ds	9.3
172.18.0.49	高风险	检测到目标操作系统已停止维护 【原理扫描】	1	默认探测	445/microsoft-ds	10
172.18.0.49	高风险	Oracle Database SQL注入漏洞 (CVE-2005-0297)	1	SQL注入	1521/oracle-tns	7.5
172.18.0.49	高风险	Oracle数据库服务器MDSYS.SDO_CS软件包远程溢出漏洞 (CVE-200...	1	缓冲区溢出	1521/oracle-tns	8.5
172.18.0.49	高风险	Oracle数据库服务器Listener组件未明安全漏洞 (CVE-2010-0911)	1	其它	1521/oracle-tns	7.8
172.18.0.49	高风险	Oracle Database Server Core RDBMS组件远程安全漏洞 (CVE-201...	1	其它	1521/oracle-tns	7.1
172.18.0.49	高风险	null	1		1521/oracle-tns	0.0
172.18.0.49	高风险	Microsoft Windows SMB服务器多个漏洞 (ms17-010) 【原理扫描】	1	默认探测	445/microsoft-ds	9.3
172.18.0.49	高风险	Oracle Database SQL注入漏洞 (CVE-2005-0297)	1	SQL注入	1521/oracle-tns	7.5
172.18.0.49	高风险	Oracle数据库服务器MDSYS.SDO_CS软件包远程溢出漏洞 (CVE-200...	1	缓冲区溢出	1521/oracle-tns	8.5
172.18.0.49	高风险	Oracle数据库服务器Listener组件未明安全漏洞 (CVE-2010-0911)	1	其它	1521/oracle-tns	7.8
172.18.0.49	高风险	Oracle Database Server Core RDBMS组件远程安全漏洞 (CVE-201...	1	其它	1521/oracle-tns	7.1
172.18.0.203	高风险	OpenSSL 信息泄露漏洞 (CVE-2016-2183) 【原理扫描】	1	默认探测	5989/https	7.5
172.18.0.203	高风险	OpenSSL 缓冲区错误漏洞 (CVE-2017-3731)	1	缓冲区溢出	443/vmware-essl se...	7.5
172.18.0.203	高风险	OpenSSL 代码问题漏洞 (CVE-2017-3730)	1	代码问题	443/vmware-essl se...	7.5
172.18.0.203	高风险	多款VMware产品缓冲区错误漏洞 (CVE-2017-4903)	1	缓冲区溢出	443/vmware-essl se...	8.8

CPU使用率: 0.00% 内存使用率: 2964MB/7860MB 硬盘使用率: 34G/1.8T

3.4.6 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。

导出报表

报表列表

报表模板

选择导出模式

任务名称

导出格式

导出方式

导出文件名

设置压缩包密码

报表模板

导出

按任务

按资产

选择任务

HTML

WORD

PDF

EXCEL

XML

详细报表

默认模板

提示: 请选择需要导出的任务 (支持多选, 不支持全选任务)

提示: 包含基础任务时, 不可导出PDF格式

提示: 请选择导出方式。基础任务仅支持统计报表导出

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

提示: 请选择报表模板

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、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

4 会话录制配置举例

4.1 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。

4.2 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4-1 会话录制



2、输入要录制的域名>点击“开始录制”。

表4-1 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4-2 输入要录制域名



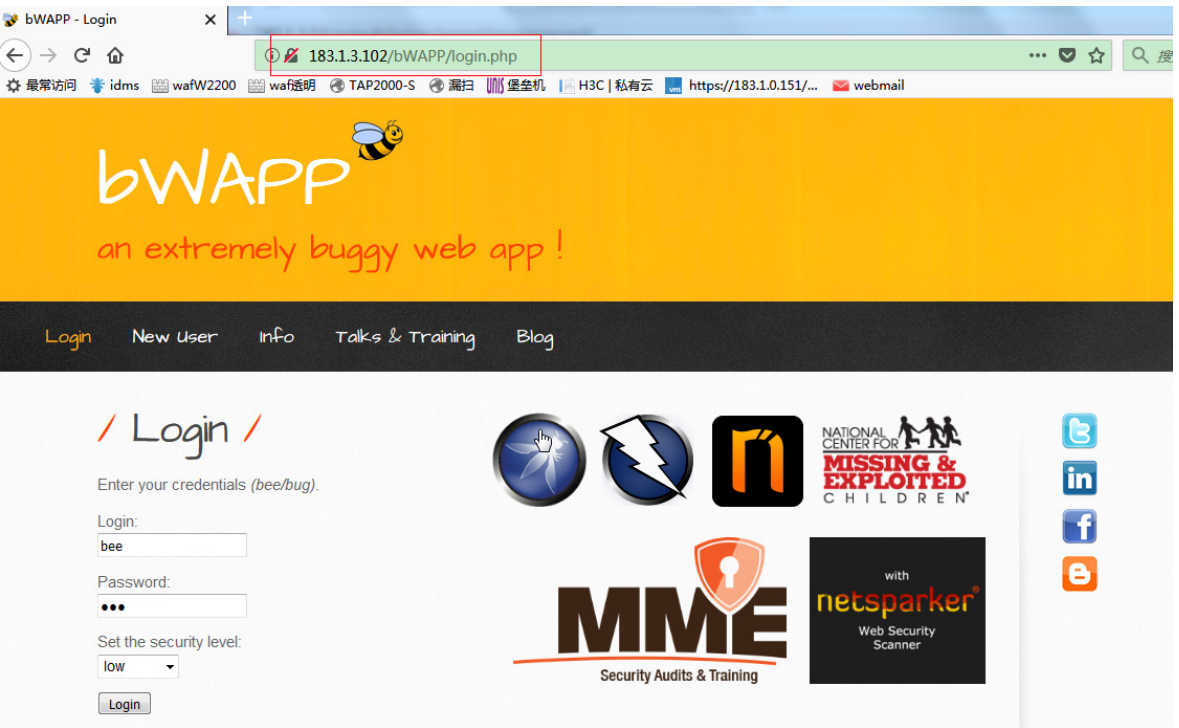
3、使用火狐浏览器做代理配置，进入“选项>常规>网络代理>设置”，配置手动代理设置，“HTTP代理”填入漏扫设备地址，端口填写 8080，点击确定。

图4-3 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4-4 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4-5 代理服务器拒绝连接



5、在访问结束后点击“停止录制”。

图4-6 会话录制



5、点击保存会话。

图4-7 保存会话



4.3 验证配置

在会话录制列表中可查看保存的会话。

图4-8 查看保存会话

会话录制						录制 +	删除 -	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		

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4-9 会话录制方式下发任务

任务中心

新建任务

任务列表

探测未知站点

安全基线检测

数据源检测

会话录制

资产管理

策略模板

报告管理

系统管理

新建任务

高级选项

☐ 系统扫描

☒ Web扫描

☐ 口令破解

☐ 仅存活探测

* 提示：如勾选仅做基础探测，则不进行漏洞扫描，仅探测资产存活状态和端口开放情况

☐ 手动输入

☐ 使用资产

☐ 批量导入

☒ 会话录制

* 提示：录制新会话，请前往会话录制

会话录制

* 提示：录制新会话，请前往会话录制

立即执行

* 提示：请选择执行方式

全部WEB漏洞

* 提示：请选择漏洞插件模板

中

* 提示：当任务达到开发上限时，'排队等待中'级别的任务将优先执行

默认

* 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

* 注意：下发口令破解任务若使用非默认字典，系统将自动选择本地默认引擎

无

* 提示：告警发送配置，请到[系统管理>任务告警]下设置

提交

CPU使用率: 1.00% 内存使用率: 2970MB/7860MB 硬盘使用率: 34G/1.8T

18

5 Web cookie 录制扫描配置举例

5.1 组网需求

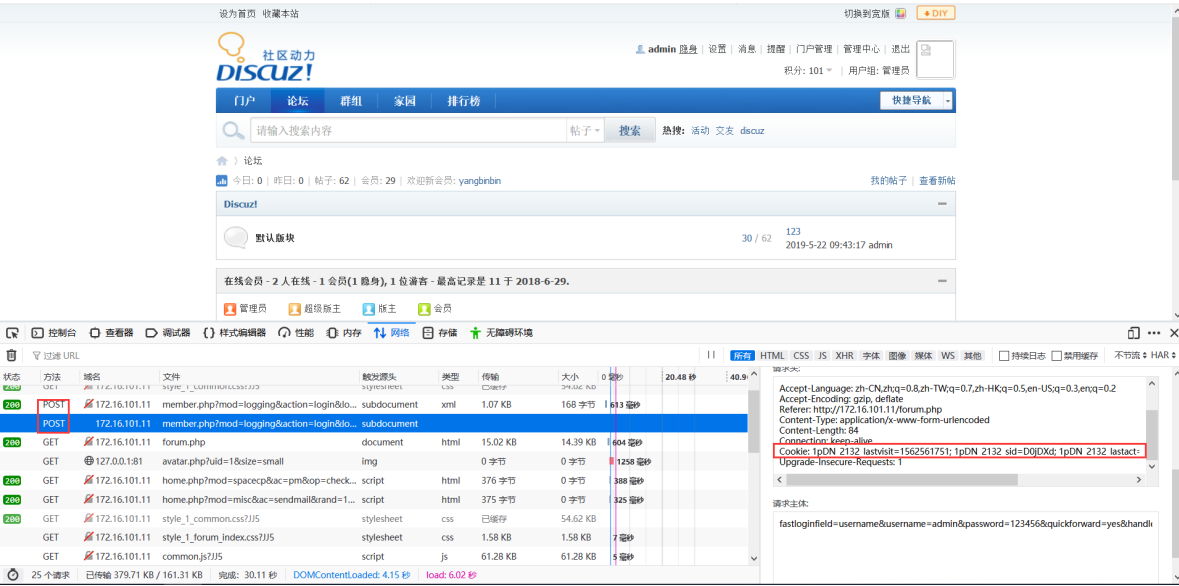


Web 站点设置了主页登录，认证等方式，需要拿到登录认证对应的信息才能扫描到更多的结果。常见的 Web 登录方式绝大多数以 Cookie 认证、Form 认证为主；较少使用的 Web 登录方式有 Basic 认证；NTLM 认证是比较早期的认证技术，目前很少使用。本配置介绍了 Cookie 认证扫描配置方法。

5.2 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5-1 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5-2 新增 web 资产



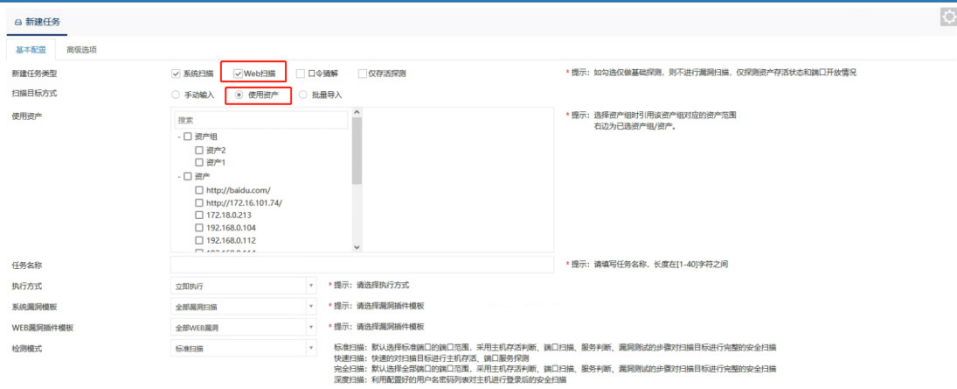
3、选择此新增站点，进入“资产详情>WEB 资产属性”界面，登录认证方式选择 Cookie/Session 认证，将步骤 1 中复制的内容，补充到起始 URL 后面，填入提交 URL 中，提交数据格式如下图中所示。

图5-3 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5-4 配置 Form 认证资产建立 Web 扫描任务



5.3 验证配置

1、在“任务中心>任务列表”中，可查看 Web 扫描任务。

图5-5 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5-6 登录后扫描的网站 URL



图5-7 Cookie 认证和未认证对比

☐	13	> 192.168.1.123未登录	系统扫描	192.168.1.123	●高(86) ●中(123) ●低(17) ●信息(10)	立即执行	中	已完成	启动
☐	12	> 192.168.1.123-denglu	系统扫描	192.168.1.123	●高(85) ●中(123) ●低(13) ●信息(3)	立即执行	中	已完成	启动

6 Web Form 认证扫描配置举例

6.1 组网需求

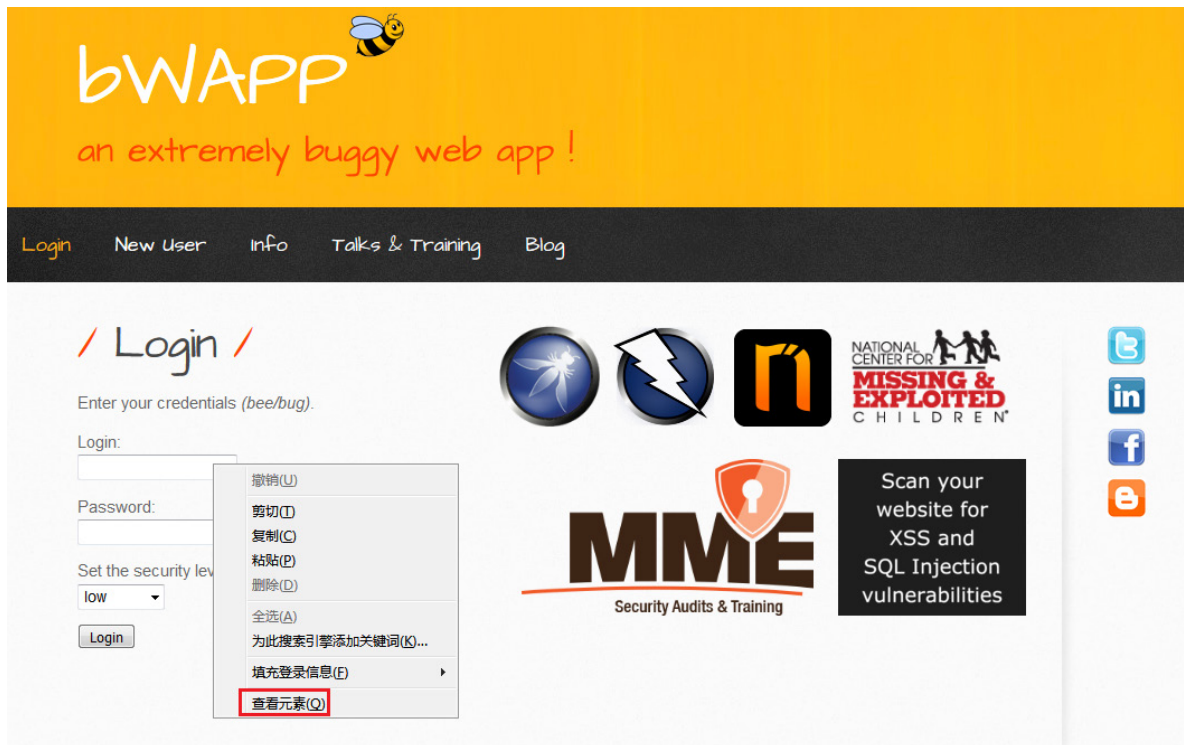


Web 站点设置了主页登录，认证等方式，需要拿到登录认证对应的信息才能扫描到更多的结果。常见的 Web 登录方式绝大多数以 Cookie 认证、Form 认证为主；较少使用的 Web 登录方式有 Basic 认证；NTLM 认证是比较早期的认证技术，目前很少使用。本配置介绍了 Form 登录认证扫描配置方法。

6.2 配置步骤

1、火狐浏览器登录需要扫描的网站，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6-1 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6-2 编辑和重发

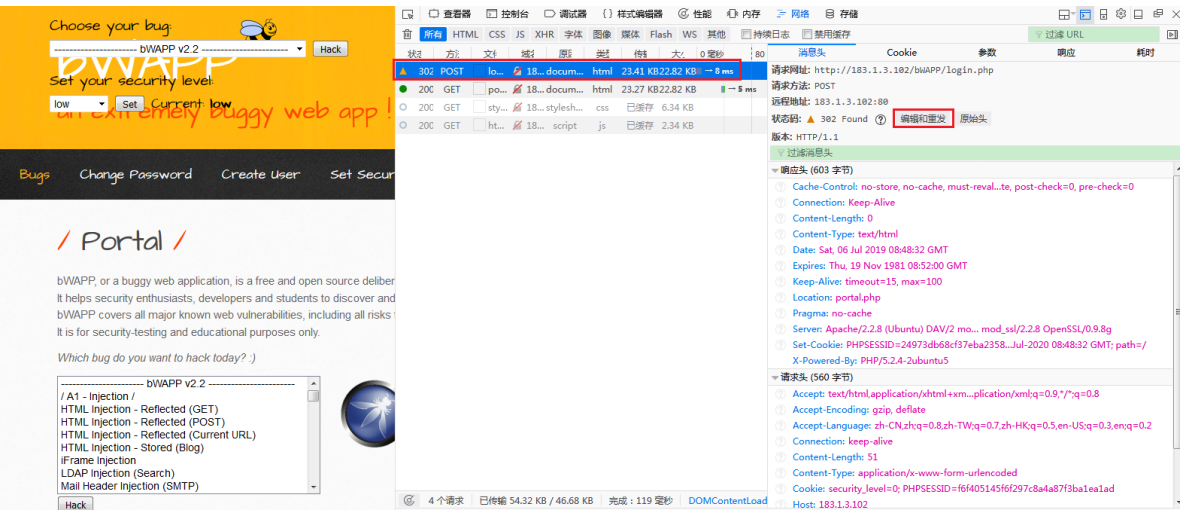
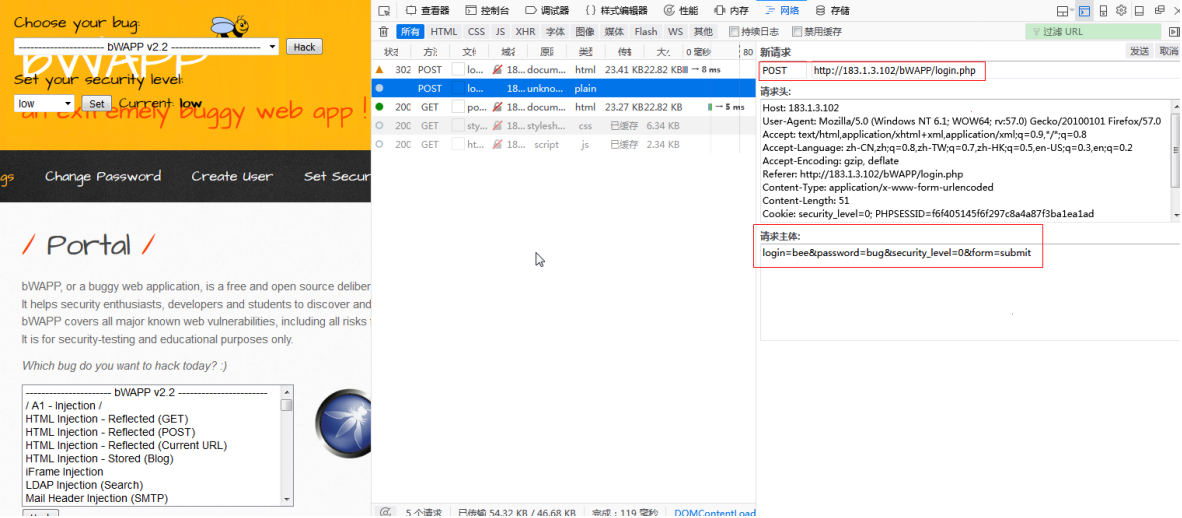


图6-3 请求主体内容复制



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6-4 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6-5 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6-6 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6-7 使用配置 Form 认证资产建立 Web 扫描任务

任务ID	任务名称	扫描类型	扫描目标	检测结果	执行方式	优先级	任务状态	操作
34	web扫描-from	WEB扫描	http://baidu.com/	高(0) 中(0) 低(0) 信息(0)	立即执行	中	排队	停止

2、扫描完成后可查看扫描结果。

图6-8 登录后扫描的网站 URL

任务列表									
工作列表									
新增 编辑 至 全部任务 搜索(回车)									
☐	任务ID	任务名称	扫描类型	扫描目标	扫描结果	执行方式	优先级	任务状态	操作
☐	34	web扫描-from	WEB扫描	http://baidu.com/	高(0) 中(0) 低(0) 信息(0)	立即执行	中	已停止	操作
子任务ID	任务类型	开始时间	结束时间	扫描耗时	结果信息	扫描进度			
49	WEB扫描	2022-05-31 17:13:25	2022-05-31 17:13:37	12秒	检测网页数: 0 漏洞: 0 中危: 0 低危: 0 信息: 0	已停止			