# 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、复制本文档内容的部分或全部,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 旁路部署网络约	吉构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	置4
<b>3.2.3</b> 结果验证	E6
3.2.4 导出报表	長6
3.3 分布式部署网约	各结构8
3.4 分布式部署配置	置8
3.4.1 配置 IP:	地址8
3.4.2 配置分布	市式扫描引擎9
3.4.3 配置分布	<b>节</b> 式扫描管控中心
3.4.4 配置策略	各10
3.4.5 结果验证	E 13
3.4.6 导出报表	長
4 会话录制配置举例…	
4.1 组网需求	
4.2 配置步骤	
4.3 验证配置	
5 Web cookie 录制扫描	苗配置举例19
5.1 组网需求	
5.2 配置步骤	
5.3 验证配置	
6 Web Form 认证扫描	配置举例
6.1 组网需求	
6.2 配置步骤	
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。

# 1 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。

# **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。



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	管理配置
-----------	------

UNIS	漏洞扫描系统						account 👻
条 系統管理 <	⇒ IP管理配置 A 接口配置	☆ 路由配置 ■ DNS配置			自动DHCP +	新増+ N新2 提案[回年]	0
账号管理 网络接口	VLAN名称	IP地址	子网掩码	Mtu	状态	操作	
外发配置 告誓配置	MngtVlan	192.168.0.1 172.16.102.153 2001.fecd:ba23:cd1f:dcb1:1010:9234:4088	255.255.255.0 255.255.255.0 0	1500	应用	\$\$\$€ <b>/</b> ∰9≥×	
分布式部會 日期/时间	总计1条记录						< 1 →

再点击"下一步"调过 VLAN 基本配置。

VLAN接口配置				×
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		2 接口IP	地址配置	
1 1 1 1 1				_
VLAN编号	1		* [系统内置VLAN编号为1 新增VIAN号语输入[2-4094]之间,目不同于已有VIAN号的教字 ]	
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	٣	*	
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	按口IP地址配置	
新增+			
支持IPv4以及IPv6网络地址 IPv6示例: 2001:fecd:ba23:cd1f:dcb1	1:1010:9234:4088 IPv6前缀范围: 0-128		
IP地址	▲ 子阿擁码	操作	
192.168.7.253	255.255.255.0	<b>保存+</b> 取得-	
192.168.0.1	255.255.255.0	翻訳全来	
192.168.13.177	255.255.255.0	間目空末	
_			
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 A 接口配置	▲ ② 路由配置 ■ DNS配置		新増+ 刷新ご 推察(回车)
目的地址	▼ 子网编码/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年记录			< 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



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"。

日 新建任务				
基本配置 高级选项				
新建任务类型	✔ 系统扫描 Web扫描	□令攝解 □ 仅存活探测 *提示:如勾选仅做基础探测,则不进行器测扫描,仅探测资产存活状态和满口开放情况		
扫描目标方式	<ul> <li>● 手动输入</li> <li>○ 使用资产</li> </ul>	社会会入		
扫描目标	192.168.7.79	* 日播目标编写规范: IPV与劳制:92.168.1.100.JPV与予制: xxxxcxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		
任务名称		*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		
系统漏洞模板	全部属同扫描	* "提示:请选择漏洞插件模板		
检测模式	杨树田	秋春扫描:款以选择标准满口的满口范围,采用主机疗活利断,满口扫描,服务判断,漏房附试的步骤对扫描目标进行完整的安全扫描 快速扫描:快速的扫描目标进行主机疗法,减日服务劳服, 完全扫描:款以选择全部满口的调口范围,采用主机疗活利断,满口扫描,服务补断,漏用附试的步骤对扫描目标进行完整的安全扫描 深度扫描:利用能量好的用户名都另列解对主机进行复发后的全名出描		
调试模式	✓	若开启,则记录目标详细描件执行日志。		
执行优先级别	中	* "提示:当任务达到并发上限时,排队等待中"级别简的任务将优先执行		
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 local: 系统将会选择本地引擎		
告警模板	无	* * 提示: 告營次送配置, 请到系统管理>任务告答)下设置		
	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"。

<b>0</b> 任	务列表	■ 工作列表				新增+	刷新ご	至	全部任务	* 搜索回	\$1
	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
	30	> 192.168.7.79	系统扫描	192.168.7.79	● 商(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: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

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"。

日 新建任务			
基本配置 高级选项			
新建任务类型	系统扫描 ✓ Web扫描	□ 令靖解 □ 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
扫描目标方式	④ 手动绘入 (使用资产)	批量导入 〇会话录制	
扫描目标	http://172.16.101.74		* 13曲目転填写現在: IPA式等時192.168.1.100.IPv6示例: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
任务名称	http://172.16.101.74		*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	
WEB漏洞插件模板	全部WEB漏洞	* 提示: 请选择漏洞插件模板	
执行优先级别	<b>中</b>	* #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	ŕ
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 local:系统	将会选择 <mark>本地引擎</mark>
告警模板	无	▼ *提示:告警发送配置,请到[系统管理>任务告警]下设置	
	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"。

<b>9</b> (1	务列表	■ 工作列表			新増+ 刷新の	至	全部任务	▼ 搶麥[回	车]	¢
	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: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

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。

★ 書询 重置
₽₩EXCEL × ©
漏洞评分
9.3
10
7.5
8.5
7.8
7.1
0.0
9.3
7.5
8.5
7.8
7.1
7.5
7.5
7.5
8.8
se

#### 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。

▲ 导出报表 <>> 提表列表	▲ 报表模板		
输出报表			
选择导出模式	<ul> <li>接任务</li> <li>按资产</li> </ul>		
任务名称	调选择任务	* 撮え	示: 请选择需要导出的任务 (支持多选, 不支持存活任务)
导出格式	🖲 HTML 🕤 🛛 WORD W 🔷 PDF 📐	C EXCEL 🗙 C XML 🚾 * 慶	示:包含基线任务时,不可导出PDF格式
导出方式	详细报表	· "提示:请选择导动方式。基线任务反支持统计报表导动	
寻出文件名		*提示: 请填写导出的文件名称。限制: [1-42]字符之间,限制字符: \/:*?"	<>   , (), `, ( ).
设置压缩包密码	×		
<b>&amp;表欄板</b>	默认模板	★ *提示: 请选择报表模板	
合田			

#### 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 < <p>E 报表列表 ♣ 报表</p>	5模板		
输出报表			
选择导出模式	<ul> <li>接任务</li> <li>按资产</li> </ul>		
任务名称	× 192.168.7.79		*提示:请选择需要导出的任务 (支持多选,不支持存活任务)
任务历史执行时间	×		*提示:默认导出各子任务最近一次扫描结果,可自定义选择历史扫描结果
导出格式	🖲 HTML 👩 🛛 WORD 🚺 🔿 PDF 📐	🗆 EXCEL 🔀 🛛 XML 🔜	*提示:包含基线任务时,不可导出PDF格式
导出方式	详细报表	▼ *提示:请选择导出方式。基线任务仅支持统计报表导出	
导出文件名	192.168.7.79	*提示:请填写导出的文件名称。限制: [1-42]字符之间,限制字符:	//:*?*<> ,(),`,(),
设置压缩包密码	×		
报表模板	默认模板	<ul> <li>* 提示: 请选择报表模板</li> </ul>	
9.41			

#### 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。

UNIS	漏洞扫描系统						
秦 系統管理 <	⇒ IP管理配置 A 接口配置	☆ 路由配置 ■ DNS配置			自动DHCP+	新増+ 刷新こ 捜索[回车]	0
账号管理 网络按口	VLAN名称	IP地址	子网掩码	Mtu	状态	操作	
外发配置 告警配置	MngtVlan	192.168.0.1 172.16.102.153 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088	255.255.255.0 255.255.255.0 0	1500	启用	siti.∕ ∰sx	
分布式部署 日期/时间	总计1条记录						< 1 →

再点击"下一步"调过 VLAN 基本配置。

VLAN接口配置		× 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	v ž
下─歩 ⊙		

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:fecd:ba23:cd1f:dcb1	1:1010:9234:4088 IPv6前缀范围: 0-128	
IP地址	▲ 子同擁码	操作
192.168.7.253	255.255.255.0	保存+ 取満-
192.168.0.1	255.255.255.0	BHR9=
192.168.13.177	255.255.255.0	删除来
完成 ④		

#### 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	A 接口配置	◇ 路由配置	■ DNS配置			新雄+	刷新ご	搜索[回车]	0
目的地址			*	子间掩码/子网前缀长度	丙一丙	м	etric		
0.0.00				0.0.0.0	192.168.13.1	0			
息计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

#### 3.4.2 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。

<b>1</b> 分布式设置 追引擎列表		
基本选项		
作为分布式引擎	<b>~</b>	*提示:开启后当前设备将只作为扫描工作引擎。
引擎名称(別名)	local11	* 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
管理中心地址	172.18.0.58	* 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 注意:开会分布式的管理中小地址不能都蛋自己的管理地址I
	_	

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。

t 分布式设置 11 引擎列	表	
基本选项		
作为分布式引擎		*提示:开启后当前设备将只作为扫描工作引擎。
引擎名称(别名)	local11	*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
管理中心地址	172.18.0.58	*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 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!
	提交	
	确定开启分布式。	? 提示:提交后会 <mark>重启</mark> 设备,若无更改配置,则不会重启。
		ROH MISA

#### 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 漏洞拮	]描系统			▲ 接触上傳	accou
t 分布式设置	增加引擎地址		×	增加引擎地址+	RIN D
引擎名称	引擎IP地址		*提示:信任此P地址,保证子工作引擎与主控管理中心正常通信	自动同步规划	
local		提交		Yes	
local				Yes	

添加完成后,可以在引擎列表中看到新增的引擎。

t 分布式设置 Li 引擎列表					就加引擎地址+ 刷新C
引擎名称	引擎奥型	▼ SI罪IP	秋恋	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
local	基线核查引擎	127.0.0.1	启用	Yes	Yes
local	系统扫描引擎	127.0.0.1	启用	Yes	Yes
local	口令强解引擎	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



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			Ċ
新建任务 基本配置 高级选项			
任务列表 探测未知站点 新建任务类型 安全基项检测 扫描目标方式	<ul> <li>✓ 系統闫猫 (Web闫猫 □ 口令張峰 □ 仅存活探測</li> <li>● 手动輸入 ○ 使用资产 ○ 批量号入</li> </ul>	· 揭示: ba0)進伏維基維粹則,則不进行產幣目標,仅原则進产等活快率到滿口开放情況	
較還岸检測 扫描目标 会话录制	192.168.7.79	* 13編目标編号規模: IP4-研修192.168.1.100JP46元号: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
<ul> <li>◎ 资产管理</li> </ul>		潮電示明: www.example.com URL示例: http://192.168.1100/.https://www.example.com/ http://jcoocooccoocoocooccooccooccooccoocc)/	
♪● 策略模板 <		振行の意味後: 192.168.1.1/24/192.168.1.1-255/192.168.1.1  検拭192.168.3.cc、192.168.bb.cc、192.aabb.cc悟式将全被视为域名, 清晴认后提交  多个之间以英文道号()成成片分隔	
過 报表管理         <           任务名称		* 揭示: 请填写任务名称,长度在[1-40]字符之间	
系統管理 < 执行方式	立即执行 ▼ * 提示: 请选择执行方式		
系统漏洞模板	全部漏洞扫描 * 推示: 请选择漏洞插作	構版	
检测模式	标准扫描 ▼ 标准扫描: 默认选择社	准满口的端口范围,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 #P=F=#===10==== #==10=====	
	(代題:194) (代題:1037) 完全[1時] 默认选择: 深度[1時: 利用配量)	海国防田口士14行药,第二酸药用何 新闻口助用口石器,积土机疗者对新新,黄口曰黑,服务判断,漏洞除成的步骤对归扁目标进行完整的安全归庸 的用户省器将列唤对主机进行量表面的安全归庸	
调试模式	✓ 若开启,则记录目标:	细插件执行日志。	
执行优先级别	中 * 提示: 当任务达到并2	上限时,排队等待中"级别离的任务将优先执行	
分布式引擎	戦认 ▼ * 戦 认: 緊 応 ド 根 溜 引 り * 注 巻: 下 发 口 令 満 解 4	的负数情况, <mark>智能</mark> 选择工作引擎 local: 系统序合选择本 <mark>地引擎</mark> 务者使用非新认字典,系统场自动选择本地默认引擎	
告警機板	无 ▼ *提示:告警发送配置.	请到[系统管理>任务告署]下设置	
	<u>我</u>		

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"。

o f	<del>I</del> 务列表	■ 工作列表			新増+ 刷新の	至	全部任务	• 推察[[]	[]年]	¢
	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	腺作	
	32	> 192.168.7.79	系统扫描	192.168.7.79	● 商(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: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。

配置信息	说明
	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"。

日 新建任务			
基本配置 高级选项			
新建任务类型	系统扫描 ✓ Web扫描	□令猜解 □ 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
扫描目标方式		批量导入 〇会话录制	
扫描目标	http://172.16.101.74		* 13曲目を填写規范: IPv4元第192.168.1.100.IPv6元労): xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
任务名称	http://172.16.101.74		*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	
WEB漏洞插件模板	全部WEB漏洞	▼ *提示: 请选择漏洞插件模板	
执行优先级别	<b></b>	▼ *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	ŕ
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 local:系统	将会选择 <mark>本地引擎</mark>
告警模板	无	▼ *提示:告警发送配置,请到[系统管理>任务告警]下设置	
	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"。

<b>0</b> fi	务列表	■ 工作列表			新增+ 刷新 2	至	全部任务	* 搜索[[]]	1	¢
	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扫描	http://172.16.101.74	●斎(0) ●中(0) ●低(0) ●信息(0)	立即执行	中	排队	(B))	

#### 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				

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结果。

🖵 任务中心		◆ 资产漏洞查询						¢
◎ 资产管理		全部资产 * 搜索[回车键可搜索]		资产组 *	漏洞等级		,	≫ 直询 重置
┢- 策略模板	<	★ 漏洞列表						
■ 报表管理	~		101014-0		1010041-00			Ş≝EXCEL ♥ ₽
数据查询		20 <sup>14</sup>	<b>准</b> 洞零级	<b>進過名称</b>	進利数量	<b>温洞</b> 奕別	端山/服务	温润评分
对比分析		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
导出报表		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
系統管理		172.18.0.49	高风险	Oracle Database SQL注入漏洞(CVE-2005-0297)	1	SQLI主入	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软件包运程溢出漏洞(CVE-200	1	織沖区溢出	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	織冲区溢出	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产品缓冲区错误漏洞(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	2964MB/7860MB 硬曲使用	察: 34G/1.8T

#### CPU使用率: 0.00% 内中使用率: 2904WB/7800WB 被重使用率: 343/1.81

#### 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 ピ 报表列表 🔥	报表模板		
输出报表			
选择导出模式	● 按任务 ○ 按资产		
任务名称	请选择任务		*提示: 请选择需要导出的任务 (支持多选,不支持存活任务)
导出格式	🖲 HTML 😈 🛛 WORD 👿 🔷 PDF	ڬ 🔿 excel 🔀 🔿 XML 🚧	* 提示:包含基线任务时,不可导出PDF格式
导出方式	计如报表	· "提示:" 崩透挥导山方式。 基线任务仪文持统计报表导动	
导出文件名		*提示: 请填写导出的文件名称。限制: [1-42]字符之间,限制字符:	: \/:*?*<> ,(),`,{},
设置压缩包密码	×		
报表模板	默认横板	<ul> <li>* 提示: 请选择报表模板</li> </ul>	
母田			

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	

# 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

新速任労	
探测未知站点 没有检索到数据	
安全要決約第         ・ 步骤1: 第4項写置要表示的討伐4. 点击开始投稿开始表明           影響雪地滑         感討の影記業           ・雪響: 第2本意見小ー小讨赏意識電加工の代稿。「道路方32方位音音12次目前第3000           ・雪響: 第2本意見小ー小讨赏意識電力の行為第二次目前通知	
<ul> <li>         ・</li></ul>	
□ · · · · · · · · · · · · · · · · · · ·	
THOMAS -	

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

占求利		
城名	183.1.3.102	li.
•步骤1:	首先填写需要录制的域名,点击开始按钮开始录制	111.
<ul> <li>步骤2:</li> <li>步骤3:</li> </ul>	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 然后在配置了http代理的浏览器上,依次访问需要录制的url	
<ul> <li>注:域</li> <li>注: 此)</li> </ul>	5対字符限制: ヽ/ い 、 い 、 ヽ ! ' 、 ' \$' 、 ' ; ' 、 ' / ' 、 ' \ n' 、 ' <' 、 ' >' 、 ' / ' 、 ' ?' 、 ' : ' 、 ' "' 、 ' (' 、 ') ' 、 ' ' 、 '	
•注:会ì	活動的使用请确认使用的两个消览器没有同时开启代理,避免出现相互代理的情况。推荐使用火狐消览器和谷歌消览器。	
当衆制的UF	L	>

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

		连接设置	×
<ul> <li>☆ 常規</li> <li>Q 搜索</li> <li>▲ 隐私与安全</li> </ul>	<ul> <li>检查更新,但田忠</li> <li>不检查更新(不指</li> <li>自动更新搜索引导</li> </ul>	<b>配置访问国际互联网的代理服务器</b> <ul> <li>不使用代理服务器(Y)</li> <li>自动检测此网络的代理设置(W)</li> <li>使用系统代理设置(U)</li> </ul>	*
じ Firefox 账户	性能	● 手动代理配置( <u>M</u> ) 端口设置为	18080
	✓ 使用推荐的性能设	HTTP代理(X) 183.1.3.13 编目设备地址 端口(P) 8080	•
	自动选择适合此电脑	✓ 为所有协议使用相同代理服务器( <u>S</u> )	=
	_	SSL代理 183.1.3.13 端口(Q) 8080	×
	浏览	<u>F</u> TP代理 183.1.3.13 端口(E) 8080	
	<ul> <li>✓ 使用自动滚屏(A)</li> <li>● 使用平滑滚动(M)</li> </ul>	SO <u>C</u> KS 主机 183.1.3.13 端口(I) 8080 ● SOC <u>K</u> S v4 ● SOCKS <u>v</u> 5 不使用代理(N)	v
	<ul> <li>✓ 始终使用方向键在</li> <li>若在文本框外输入</li> </ul>	I	
	网络代理	例如:.mozilla.org, .net.nz, 192.168.1.0/24 自动代理配置的 URL ( PAC ) file:///E:/proxv.pac 軍新载入	(E) •
⑦ Firefox 帮助	配置 Firefox 如何连接	确定 取消 帮	<sup>§</sup> 助( <u>H</u> )

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

😵 bWAPP - Login	× +		
← → ⊂ ŵ	0 🔏 183.1.3.102/bWAPP/login.php	🛡 t	3Q捜
🗘 最常访问  脊 idm:	is 🔛 wafW2200 🔛 waf透明 🕜 TAP2000-S 🛞 漏扫 🍿 堡垒机 🔢 H3C   私有云 🔜 https://183.1.0.151/ 🔤 webmail		
b an	extremely buggy web app !		
Login I	New User Info Talks & Training Blog		
Enter	Login /	C in	
Login	CHILDREN'		
bee			
Pass	word:	B	
•••	necsparker		
Set th	he security level:		
low	Security Audits & Training		
Logi	in		

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

#### S 已录制的URL

GET	http://183.1.3.102:80/bWAPP/
GET	http://183.1.3.102:80/bWAPP/portal.php
GET	http://183.1.3.102:80/bWAPP/login.php
GET	http://183.1.3.102:80/bWAPP/stylesheets/stylesheet.css
GET	http://183.1.3.102:80/bWAPP/js/html5.js
GET	http://183.1.3.102:80/bWAPP/images/owasp.png
GET	http://183.1.3.102:80/bWAPP/images/zap.png
GET	http://183.1.3.102:80/bWAPP/images/netsparker.png
GET	http://183.1.3.102:80/bWAPP/images/mk.png
GET	http://183.1.3.102:80/bWAPP/images/mme.png
GET	http://183.1.3.102:80/bWAPP/images/netsparker.gif
GET	http://183 1 3 102:80/bWLPP/images/twitter ppg

#### 5、点击保存会话。

#### 图4-7 保存会话

#### ● 已录制的URL

GET	http://183.1.3.102:80/bWAPP/portal.php
GET	http://183.1.3.102:80/bWAPP/login.php
GET	http://183.1.3.102:80/favicon.ico
GET	http://183.1.3.102:80/phpmyadmin
GET	http://183.1.3.102:80/phpmyadmin/
GET	http://183.1.3.102:80/phpmyadmin/print.css
GET	http://183.1.3.102:80/phpmyadmin/phpmyadmin.css.php?lang=zh-utf-8&convcharset
GET	http://183.1.3.102:80/phpmyadmin/favicon.ico
GET	http://183.1.3.102:80/phpmyadmin/themes/original/img/b_info.png
GET	http://183.1.3.102:80/phpmyadmin/themes/original/img/logo_right.png
GET	http://183.1.3.102:80/phpmyadmin/themes/original/img/b_help.png
GFT	http://183 1 3 102-80/phpmuadmin/themes/original/img/s notice ppg

#### 保存会话 🗈 开始录制 🕨

## 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

□ 会活录制					尿制	+ 刷新ご	¢
历史会话名称	▼ 检测目标	开始时间	结束时间	URL設量	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 ~	8 新建任务		¢								
新建任务	<b>其中形型</b> 東明港兵										
任务列表 探测未知站点	新建任务类型	□ 系統当備   ☑ Web日始   □ 口令薄解   □ Q存进控制									
安全基线检测	扫描目标方式	○ 手动端入 ○ 使用资产 ○ 効果等入 ⑧ 会活業制									
数据库检测	历史会话	◆ "提示:我利斯会话,哪前往会话费制 在市政制									
新民族創	任务名称	* 提示: 请填写任务条称: 长度在[1-40]字符之间									
◎ 资产管理 <	执行方式	立期执行 * "现示:请选择执行方式									
ⅰ- 策略模板 <	WEB濃润播件模板	全部WE8篇词 * "提示: 请选择混词的件模板									
	执行优先级别	中         * 提示: 当任务达到并发上限时, 排队等待中级到簿的任务将优先执行									
副扱表管理 く	分布式引擎	取以 * 款は、系統将構造「壁的合変構成」、警範改基工作19世 [ooil:系統将占法統基本地計算 注意: 下足口合導解行為管理部状況と考慮、系統符合為的基本地批測引置									
◎ 系統管理 <	告警模板	光 ・ 提示: 告替対送取量,通列系統管理>任务告替)下设量									
		82									
		C CPU使用率: 1.00% 内存使用率: 2970MB/7860MB 硬血使用率: 34G/1.8T	^								

# 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

			设为首页 收藏本站								初換到宽版 📳 🔶 DIY 🔷
			O DISCUZ!					1 a	dmin <u>随身</u>	设置 消息	推羅 门戶管理 管理中心 進出 🔛 积分: 101 =  用戶組:管理员
			门户 论坛 群約	1 家园	排行	膀					快捷导航 -
			Q、 请输入搜索内容				帖子▼	捜索	热搜: 活动	h 交友 discus	z
				会员: 29   欢迎!	新会员: yar	ngbinbin					我的帖子   查看新帖
			Discuz!								-
			weil die to							30 /	62 123
			EA WARK W							507	2019-5-22 09:43:17 admin
			在线会员 - 2 人在线 - 1 会员(1	隐身),1位游客	- 最高记录	录是 11 于 2018-6	-29.				-
			□ 管理员 □ 超级版主	<b>同版主 </b>	会员						
R	▶ 控制台	○ 査看器 □ 調試器	{}样式編輯器 (2) 性能 (1) 内存	∓ 1L ⊠i≊ F	日存储・	★ 无障碍环境					v ח x
Û	▼ 过滤 URI				-					日二所有日	HTML CSS JS XHR 字体 图像 媒体 WS 其他 □ 持续日志 □ 禁用缓存 不节流 + HAR +
状态	方法	域名 文件		触发源头	类型	传输	大小	0 200	20.48 秒	40.9	mpre:
X60	GEI	ATTACADATA	commoncession	stylesneet	CSS .	C4817	34.02 ND	1		-	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 Accept-Encoding: gzip, deflate
200	POST	172.16.101.11 membe	er.pnprmod=loggingeaction=logineuo	subdocument	xmi	1.07 KB	108 子口	1613 999		_	Referer: http://172.16.101.11/forum.php Content-Type: application/x-www-form-urlencoded
200	GET	172.16.101.11 forum	nhn	document	html	15.02 KB	14 39 KB	604 (282			Content-Length: 84 Connection: keen-alive
_	GET	⊕127.0.0.1:81 avatar.	php?uid=1&size=small	ima		0 字节	0 字节	1258 👾			Cookie: 1pDN 2132 lastvisit=1562561751; 1pDN 2132 sid=D0jDXd; 1pDN 2132 lastact=
200	GET	# 172.16.101.11 home.c	php?mod=spacecp∾=pm&op=check	script	html	376 字节	0字节	388 200			< >>
200	GET	# 172.16.101.11 home.p	ohp?mod=misc∾=sendmail&rand=1	script	html	375 字节	0 字节	325 豪砂			22-42
200	GET	# 172.16.101.11 style_1	common.css?JJ5	stylesheet	CSS	已缓存	54.62 KB				in steps
	GET	# 172.16.101.11 style_1	forum_index.css?JJ5	stylesheet	CSS	1.58 KB	1.58 KB	7毫秒			rastrogrimeru – usernameckusername – aunimokpasswoli u = 12:34500kquicki oli wali u = yesokriali uli
	GET	#172.16.101.11 commo	on.js?JJ5	script	js	61.28 KB	61.28 KB	5 毫秒		~	
Ō	25 个请求	已传输 379.71 KB / 161.31	KB 完成: 30.11 秒 DOMContentLo	aded: 4.15 🕸	load: 6.02 €	9					

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 3	资产	×
资产目标		* 请填写资产目标,多个资产以逗号分隔。 主机资产填写示例:192.168.1.1, www.baidu.com web资产填写示例:http://www.baidu.com/
标签	液加	提示: 输入标签后按回车确定
	提交	

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

扫描根目录		
例外URL		
登录认证	Cookie/Session认证	▼ 《登录验证
Cookie		
上传网站证书	浏览) 未选择文件。	浏览器客户端证书,如PFX/PKCS12等格式
上传网站证书密码		导出证书时设置的密码

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。

日 新建任务					¢			
基本配量 高级选项								
新建任务类型	✓ 系统扫描 ✓ Web扫		· 仅存活探测	* 鐵示:如勾造仅做基础探测,则不进行漏洞扫描,仅探测资产存活状态和跳口开放情况				
扫描目标方式	<ul> <li>手动输入</li> <li>● 使用器</li> </ul>	町产 ○ 批量号	iک ا					
使用资产	後次 ^			* 提示: 选择资产相时引用该资产相对应的资产范围				
	- 」 奴 <sup></sup> 围 - 」 政产 - 〕 政产 - 〕 政产 - 」 政产 - 」 政产 - 」 1450/12416-001 - 1722-180.213 - 1922-1680.0104 - 1922-1680.0112 - 1922-1680.0112	v 1.74/						
任务名称				*提示:请编写任务名称,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					
系统漏洞模板	全部漏洞扫描	× *	提示:请选择漏洞插件模板					
WEB贏同插件模板	全部WEB羅問	* *	提示:请选择漏洞插件模板					
检测模式	iş krallı	¥	标准扫描:默认选择标准确口的确口范围,采 快速扫描:快速的对扫描目标进行主机存活。! 完全扫描:默认选择全部确口的确口范围,采	【符若非版,跳口当病,服务非断, 氟烷则试的步骤对当展目标进行冲器的安全扫描 【符洗等版 【存洗手版,跳口当病,服务非断,氟烷则试的步骤对当展目标进行冲器的安全日接 注意性的性心和出现				

#### 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

S	ecPath 漏洞扫描系统									王务列表 admin
	<b>9</b> 任	务列表	■ 工作列表			新増+ 刷新で	至	全部任务	* 搜索回	\$1
		任务ID	▼ 任务名称	1 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
		33	> cookie	WEB扫描	http://baidu.com/	●商(0) ●中(0) ●低(0) ●信息(0)	立即执行	中	抑队	停止

#### 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

结果详情							返回任务列表
网站列表 漏洞列表 漏洞目录例 历史执行记录					WEB扫描详情		
da	$\sim$	风险级别	荒洞名称	总计	网站域名	http://192.168.1.123:8001/	
Shttp://192.168.1.123:8001/		英风险	Cybrotech CyBroHttpServer 1.0.3跨站調	本攻击漏洞 1	IP地址	192.168.1.123	
		中风脸	Tomcat證站-3	1	网站服务器	TornadoServer/6.1	
		中风脸	Tomcat跨站-4	1	网站编码	gb2312	
		中风脸	Tomcat證許(manager)	1	网站物理位置	局域网·对方和您在同一内部网[192.168.0.0-192.168.255.255]	
		中风脸	域名访问限制不严格	1	网页总数	1	
		低风险	启用了DEBUG方法	1	PERMOT		
		低风险	X-Frame-Options头未设置	1	3030/4927345		
		信息	服务器版本信息泄漏	1			
		总计8条记录		毎页显示 25 * < 1 >			高风险[1] 中风险[4] 低风险[2]

#### 图5-7 Cookie 认证和未认证对比

13	> 192.168.1.123-未登录	系統扫描	192.168.1.123	● 藏(186) ● 中(123) ● (版(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	● 商(185) ● 中(123) ● (訊(13) ● 信恩(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

bWA an extrem	RPR	app !		
Login New User / Login Enter your credentials Login:	Info Talks & Training s (bee/bug).	Blog	MATIONAL CENTERFOR MISSING & EXPLOITED C H I L D R E N	e in
Password: Set the security lev Iow	炒销(U) 剪切(T) 复制(C) 粘贴(P) 删除(D) 全选(A) 为此搜索引擎添加关键词(K) 填充登录信息(E) ● 查看元素(Q)	Security Audits & Training	Scan your website for XSS and SQL Injection vulnerabilities	•

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

CI	G O i	き おいちょう こう	] 控制台	口调	武器 {}	样式编辑器	④ 性能	① 内存	🖙 网络 🔒 存储	1			
Choose your bug:	<b>前</b> 所有	HTML C	SS JS	XHR 🖻	⊭体 图像	媒体 Fla	sh WS 其	他一持	读日志 🔲 禁用缓存			♥ 过滹 URL	Þ
bWAPP v2.2 + Hack	秋江	方; 文	1	12 IRI	. #1	传输	大/ 0毫	80	消息头	Cookie	参数	响应	#毛印寸
DVVAPP	🔺 302 P	OST Ic	💋	18 docu	m html	23.41 KB2	2.82 KBII →	8 ms	请求网址: http://1	.83.1.3.102/bWAPP/	login.php		
Set your security level:	200 0	GET D	o 🔏 🕯	18 docu	m html	23.27 KB2	2.82 KB	I → 5 ms	请求方法: POST				
low - Set Current low	0 200 0	SET d	- <i>6</i>	18 styles	h css	日焼ない	5 34 KB		远程地址: 183.1.3.	102:80			
un extremely buggy web app !	0 200 (			10			24 KD		状态码: 🔺 302 Fou	und ⑦ 编辑和重发	原始头		
	200 0		Lini // .	TO South	pr jo	LUSRIT -	CIDMIND		版本: HTTP/1.1		-		
									♀ 过滤消息头				
Buas Change Password Create User Set Secur									▽ 响应头 (603 字节)				
Buys charge rassion a create aser set seed									⑦ Cache-Control	no-store, no-cache,	must-revalte, p	oost-check=0, pre-ch	ck=0
									⑦ Connection: K	eep-Alive			
									⑦ Content-Lengt	h: 0			
Portal									⑦ Content-Type:	text/html			
									⑦ Date: Sat, 06 J	ul 2019 08:48:32 GMT	1		
									② Expires: Thu, 1	9 Nov 1981 08:52:00	GMT		
bWAPP, or a buggy web application, is a free and open source deliber	1								⑦ Keep-Alive: tin	neout=15, max=100			
It helps security enthusiasts, developers and students to discover and	1								② Location: port	al.php			
bWAPP covers all major known web vulnerabilities, including all risks									Pragma: no-ca	iche			
It is for security-testing and educational purposes only.									② Server: Apache	e/2.2.8 (Ubuntu) DAV	/2 mo mod_ssl	/2.2.8 OpenSSL/0.9.8ç	
Million have do a service of the forest day do a 20									③ Set-Cookie: PH	IPSESSID=24973db6	8cf37eba2358J	ul-2020 08:48:32 GMT	; path=/
vvnich bug do you want to nack today? .)									X-Powered-By	PHP/5.2.4-2ubuntus	5		
bWAPP v2.2 ^									▽ 请求头 (560 字节)				
/ A1 - Injection /									O Accept: text/h	tml,application/xhtml	+xmplication/>	cml;q=0.9,*/*;q=0.8	
HTML Injection - Reflected (GET)									② Accept-Encodi	ng: gzip, deflate			
HTML Injection - Reflected (POST)									⑦ Accept-Langua	ige: zh-CN,zh;q=0.8,2	:h-TW;q=0.7,zh-l	HK;q=0.5,en-US;q=0.3	,en;q=0.2
HTML Injection - Stored (Blog)									() Connection: k	eep-alive			_
iFrame Injection									Content-Lengt	n: 51			
Mail Header Injection (SMTP)									Content-Type:	application/x-www-1	orm-unencoded	07-9-4-97(2)-11-	
Linek	© 4↑	请求 已修	输 54.3	2 KB / 46.	68 KB 完	成:119 毫	b DOMO	ContentLoad	A Hosti 192121	uy_ievei=0, PHPSESSI	5-1014031431012	57004407150816818	· .
HdCk				/					most: 183.1.3.1	102			

#### 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

	新增资产			×
	资产目标	1	* 请填写资产目标,多个资产以逗号分隔。 主机资产填写示例:192.168.1.1, www.baidu.com web资产填写示例:http://www.baidu.com/	
變	标签	添加一个标签	提示: 输入标签后按回车确定	
		提交		

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

白 新建任务	5				1
基本配置	高级选项				
系统扫描 WEB扫描 □令猜解 存活评测	登 <b>梁扫描</b> 引擎选项 检测选项	起始URL 開始URL 開始用意数 例外URL 整葉以近 確交以配 確交数調	fomikiji	< 123NE	
		上传网站证书 上传网站证书部词	<b>谢范</b>	运动器器和户间设计机,如PFX/PXC512等相比 导出设计和FraceS000存得	

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

基本配置  高级远项		_						
新建任务类型	■ 系統扫描 ✓ Web		3請解 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满口开放情				
扫描目标方式	○ 手动输入 💿 使用	適产 〇 株	温导入 〇 会话录制					
使用资产	志示 - □ 測学祖 - □ 測学祖 - □ 測学2 - □ 測学1 - □ 測学 - □ 測学 - □ 測学 - □ 計学/72.50.0724/ - □ 172.50.0714 - □ 172.50.0714 - □ 192.560.014		~	• 養示:過程是小量時间用度是小量時值的進产信息 前边为已過度小量(用个。				
任务名称				* 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	٧	*提示: 请选择执行方式					
WEB漏洞插件模板	全部WEB贏同	٣	*提示: 请选择震词插件模板					
执行优先级别	φ.	٧	*提示:当任务达到并发上限时,消队等待中`级别离的任务将优	先执行				
分布式引擎	默认	٧	* 默认:系统将根据引擎的负载情况。智能选择工作引擎 local:	₩选择工作引擎 local: 系统将会选择本地引擎				
(± \$25+#15)	Ŧ	*	*提示:告警发送配查,请到(系统管理>任务告警)下设置					

# 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

SecPath 漏洞扫描系统					6 新建任务	2 任务列表 admin ··
♀ 任务列表 ■ 工作列表			新端+ 刷新C	至	(回年)	
任务ID v 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	5 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

• 6	务列表	里 工作列表						i出+ 刷約c	至		全部任务	• RED	(¥)
	任务ID	• 任务名称		2	扫描目标		检测结果			执行方式	优先级	任务状态	腺性
	34	✓ web扫描-	from	扫描	http://baidu.co	m/	● 斎(0) ● 中(0)	● 低(0) ● 信息(0)		立即执行	中	已停止	启动
70	<b>祭ID</b>	任务类别	开始时间	私来的问	检测师的	结果信息			检测进度			_	操作
49		WEB扫描	2022-05-31 17:13:25	2022-05-31 17:13:37	1280	检测网页数: 0	高性:0 中性:0 任f	1:0 信息:0			E	柳止 0%	洋街