UNIS XScan-G 系列漏洞扫描系统

典型配置举例

目 录

1 简介

本文档介绍 UNIS 漏洞扫描系统典型配置举例

2 配置前提

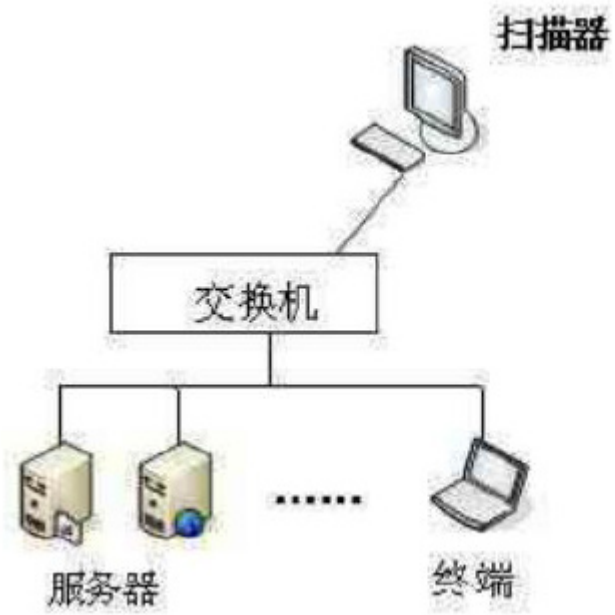
本文档不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

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。

3 主机扫描配置举例

3.1 组网需求

图1 配置组网图

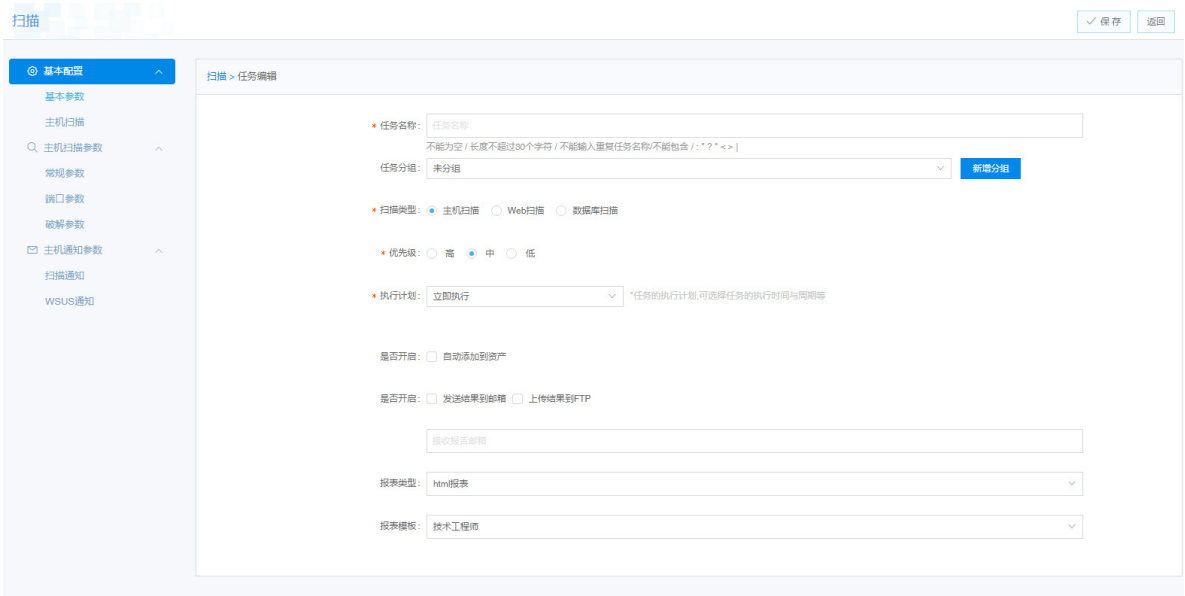


UNIS 漏洞扫描系统属于网络旁路设备，可以部署在核心交换机上（原则上可达即可扫），并对应不同的网络分配不同的网口地址，定期地对网络中多个不同的网段的主机进行全面、深入的检测，同时生成相应的漏洞解决方案，用户根据这些解决方案来对目标系统和应用做相应的加固和防护，及时将网络的安全风险降到最低。

3.2 配置步骤

通过【扫描】>【新增任务】创建一个主机扫描任务。

图2 新建任务



基本参数，配置任务名称，其他参数默认。

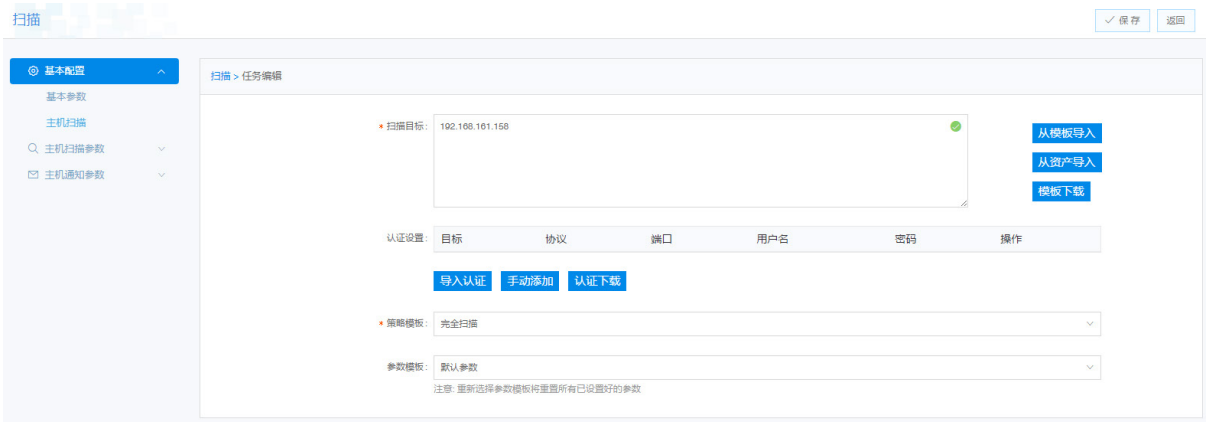
配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】。

图3 配置基本参数

主机扫描，输入扫描目标，显示认证设置配置功能。

配置路径：【扫描】>【新增任务】>【基本配置】>【主机扫描】。

图4 配置主机扫描

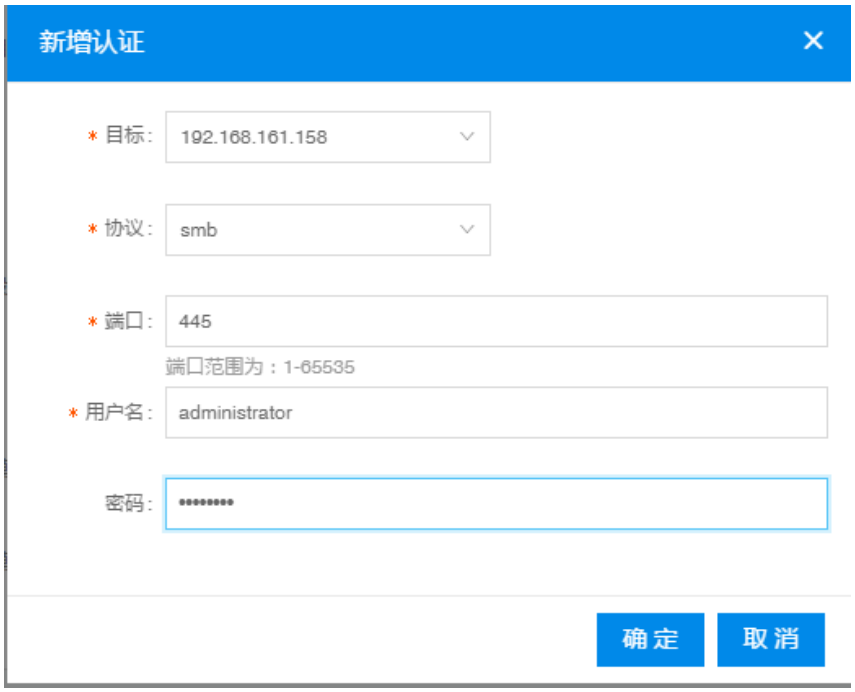


点击【手动添加】，弹出新增认证界面窗口。

图5 新增认证

配置扫描认证参数，选择目标、协议（支持 SMB、SSH、TELNET 三种协议认证）、端口、用户名、密码。

图6 新增认证



点击确定，完成新增认证配置

图7 完成配置

点击右上角【保存】按钮，即完成主机递进扫描任务创建

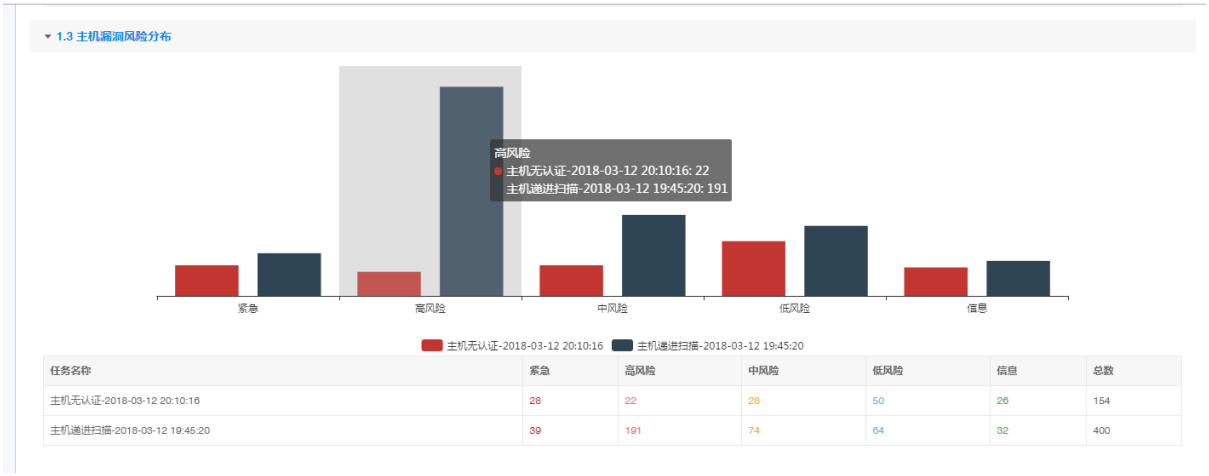
3.3 验证配置

(1) 新建主机扫描任务，未配置认证参数，其他参数与主机递进扫描任务一致。

(2) 扫描结束，2 个任务扫描结果，进行对比分析。

(3) 正常情况下扫描出来的主机递进扫描任务结果比未配置认证参数的扫描任务多。

图8 验证配置

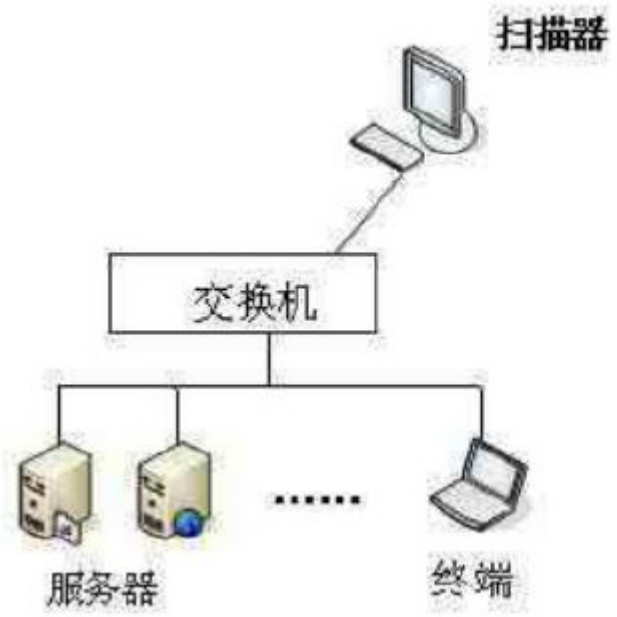


任务名称	紧急	高风险	中风险	低风险	信息	总数
主机无认证-2018-03-12 20:10:16	28	22	28	50	26	154
主机递进扫描-2018-03-12 19:45:20	39	191	74	64	32	400

4 主机弱口令扫描配置举例

4.1 组网需求

图9 配置组网图



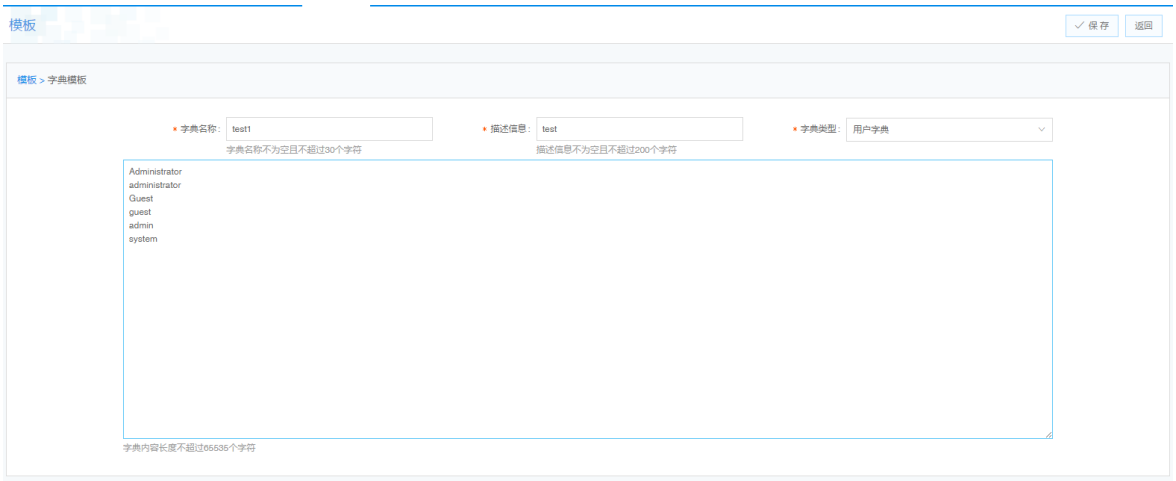
弱口令检测可以使用系统默认的模板也可以自定义弱口令模板，弱口令破解协议支持大部分常用协议如 SSH/SMB 等。

4.2 配置步骤

新建自定义用户和密码字典。

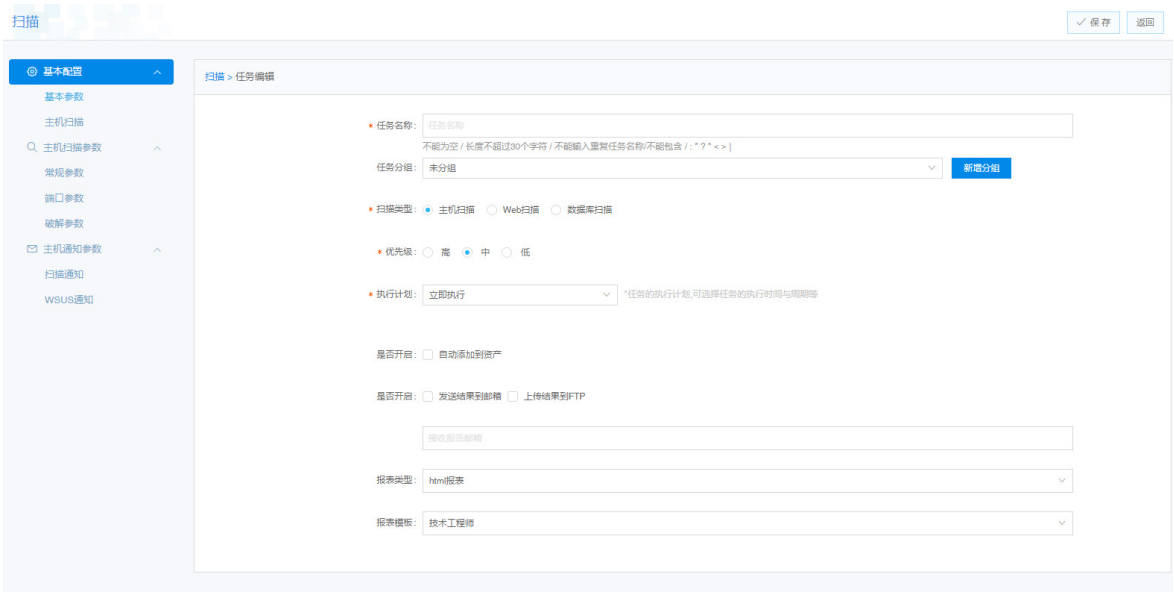
配置路径：【模板】>【数据字典】>【新建字典】。

图10 新建字典



通过【扫描】>【新增任务】创建一个主机扫描任务。

图11 新增任务



基本参数，配置任务名称，其他参数默认。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】。

图12 配置基本参数

主机扫描，输入扫描目标， 策略模板选择<账户密码检测>。

配置路径：【扫描】>【新增任务】>【基本配置】>【主机扫描】。

图13 主机扫描

破解参数，勾选 SMB 密码破解，密码字典和用户字典选择步骤（1）创建的字典。

配置路径：【扫描】>【新增任务】>【主机扫描参数】>【破解参数】。

图14 破解参数

点击右上角【保存】按钮，即完成主机弱口令扫描任务创建

4.3 验证配置

在账户页面可以看到弱口令账户密码信息。

图15 验证配置

5 WEB cookie 录制扫描配置举例

5.1 组网需求

图16 配置组网图

WEB cookie 录制后可以记录页面授权信息，扫描结果更详细全面，可用于扫描需要登录验证的 web 网页。

5.2 配置步骤

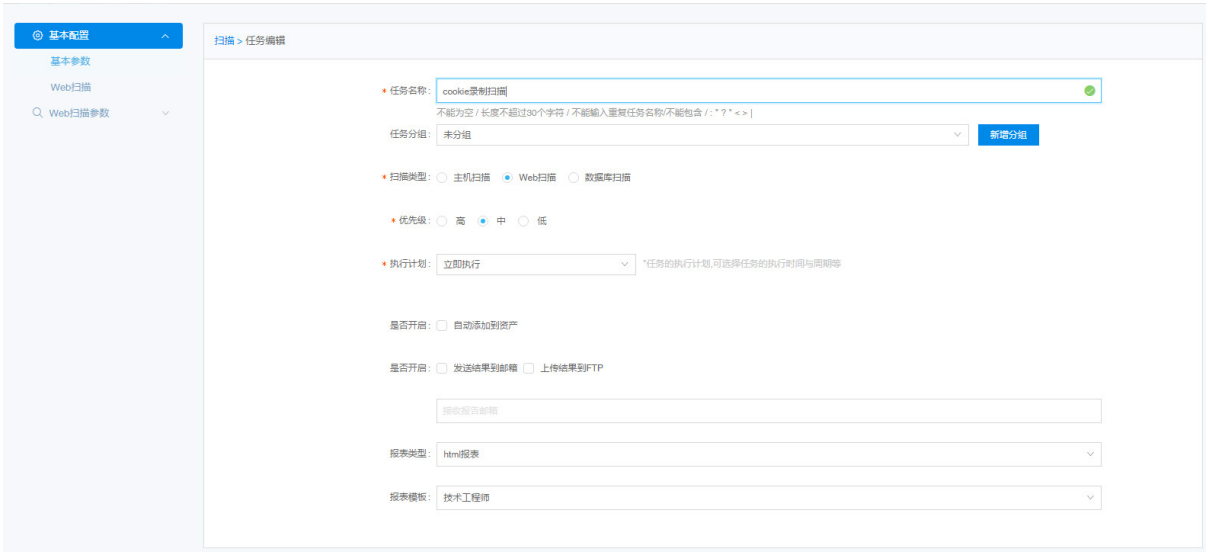
通过【扫描】>【新增任务】创建一个 WEB 扫描任务。

图17 新增任务

基本参数，配置任务名称，扫描类型选择 WEB 扫描，其他参数默认。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】。

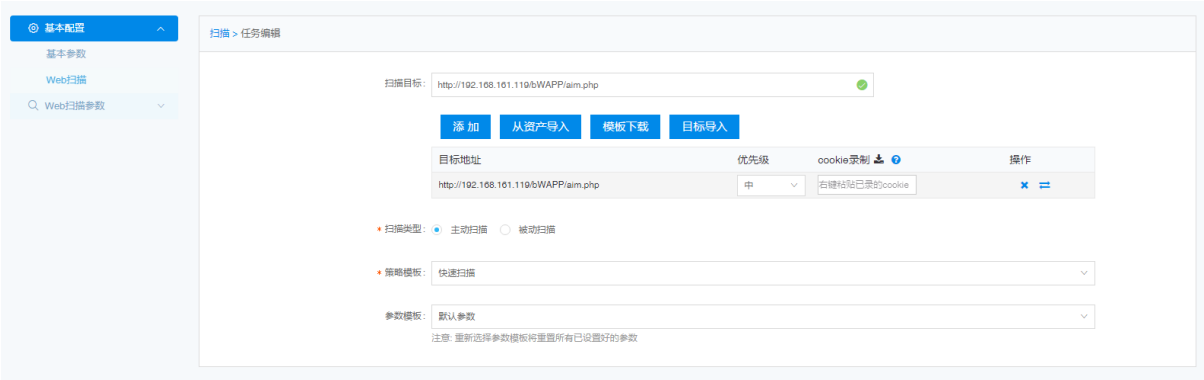
图18 配置基本参数



WEB 扫描，输入扫描目标 ， 点击添加。

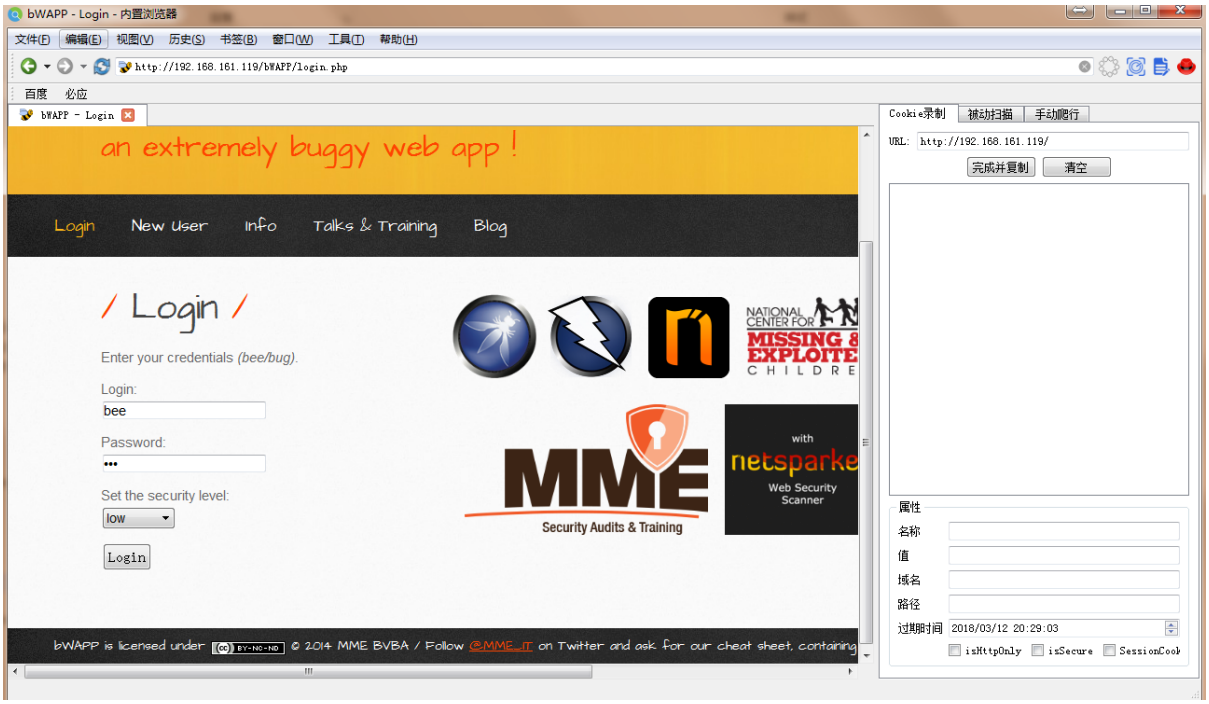
配置路径：【扫描】>【新增任务】>【基本配置】>【WEB 扫描】。

图19 Web 扫描



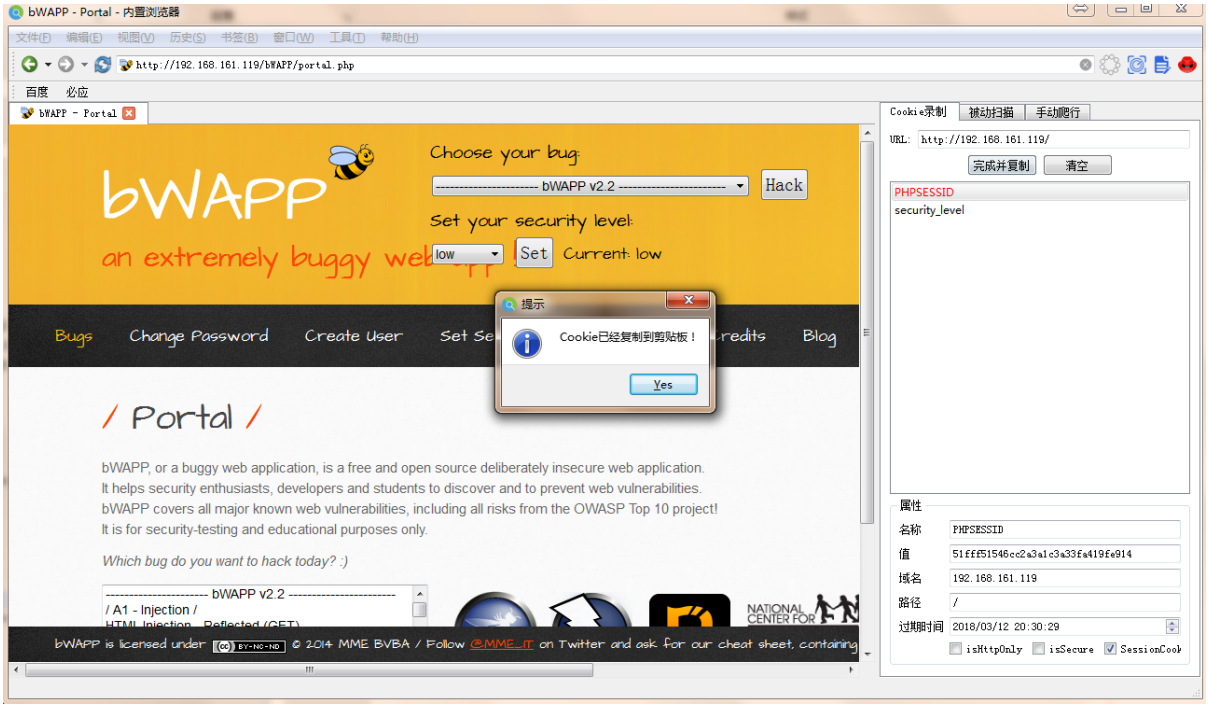
打开内置浏览器，在地址栏输入要录制 cookie 的目标 URL，回车并在网页上输入正确用户名密码登录。

图20 录制 cookie



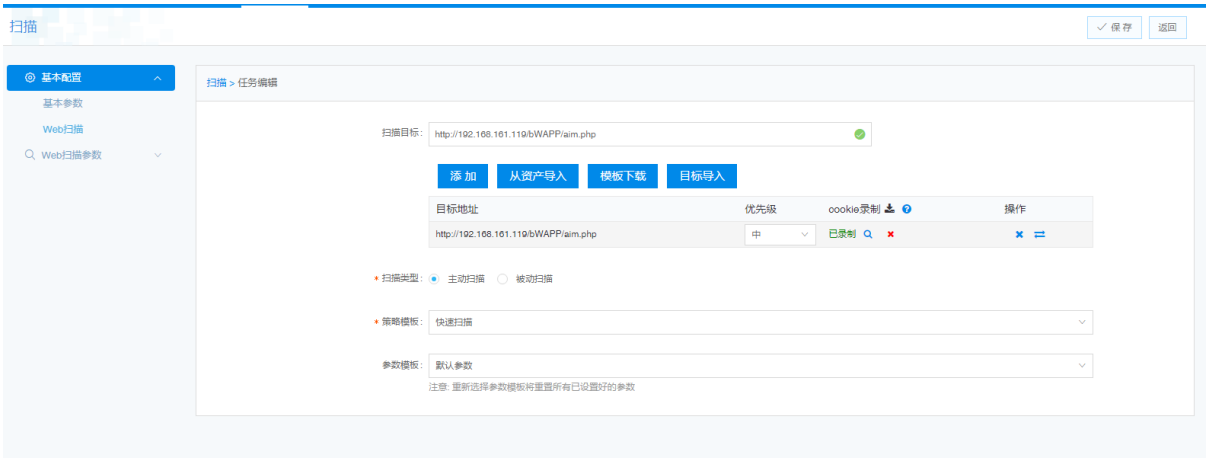
点用户登录目标站点进行扫描录制，点击【完成并复制】按钮。

图21 完成并复制



将保存好的录制粘贴到下表对应的 cookie 录制项下。

图22 粘贴到 cookie 录制项



点击右上角【保存】按钮，即完成扫描任务创建，注意：扫描过程不要关闭内置浏览器，关闭会影响扫描结果

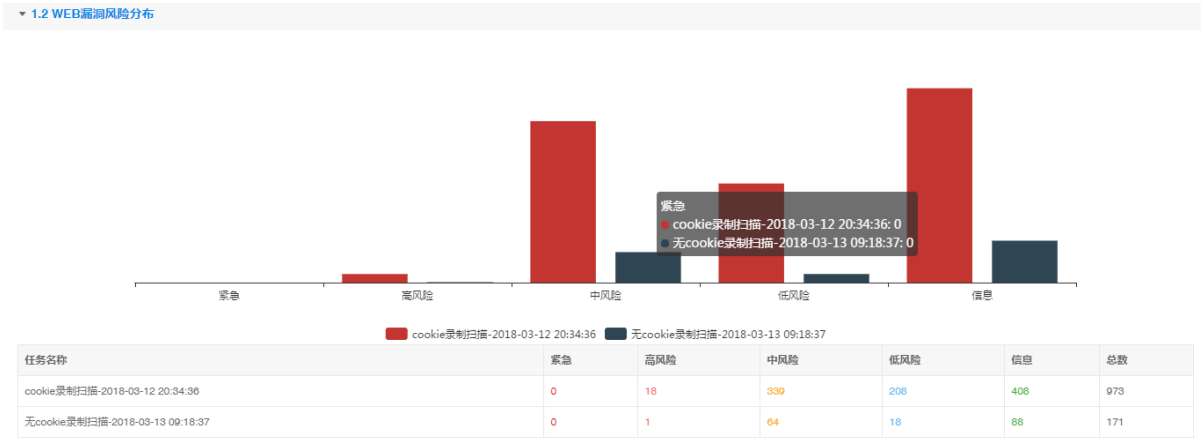
5.3 验证配置

(1) 新建 WEB 扫描任务，未进行 cookie 录制，其他参数与 cookie 录制扫描任务一致。

(2) 扫描结束，2 个任务扫描结果，进行对比分析。

3、查看 2 个任务对比结果，正常情况下扫描出来的 cookie 录制扫描任务结果比未配置 cookie 录制扫描的扫描任务多。

图23 验证配置

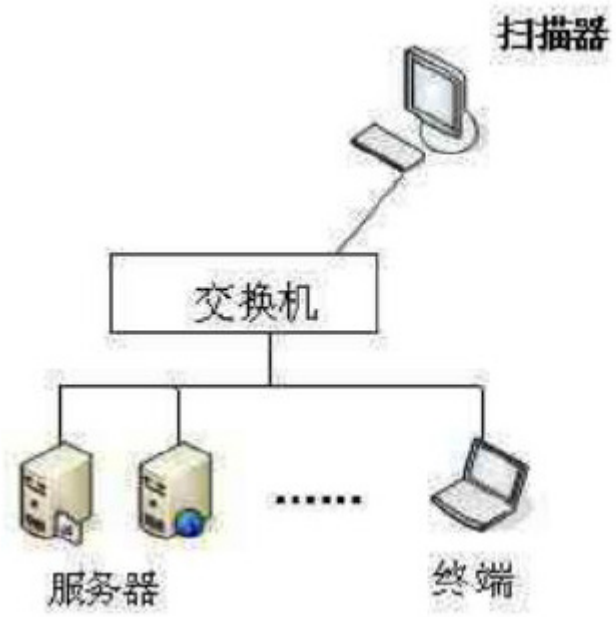


任务名称	紧急	高风险	中风险	低风险	信息	总数
cookie录制扫描-2018-03-12 20:34:36	0	18	339	208	408	973
无cookie录制扫描-2018-03-13 09:18:37	0	1	64	18	88	171

6 WEB 手动爬行扫描配置举例

6.1 组网需求

图24 配置组网图



对手动点击提交的 URL 以及爬虫引擎爬取到的 URL 进行扫描，主要用于对爬虫引擎做补充。

6.2 配置步骤

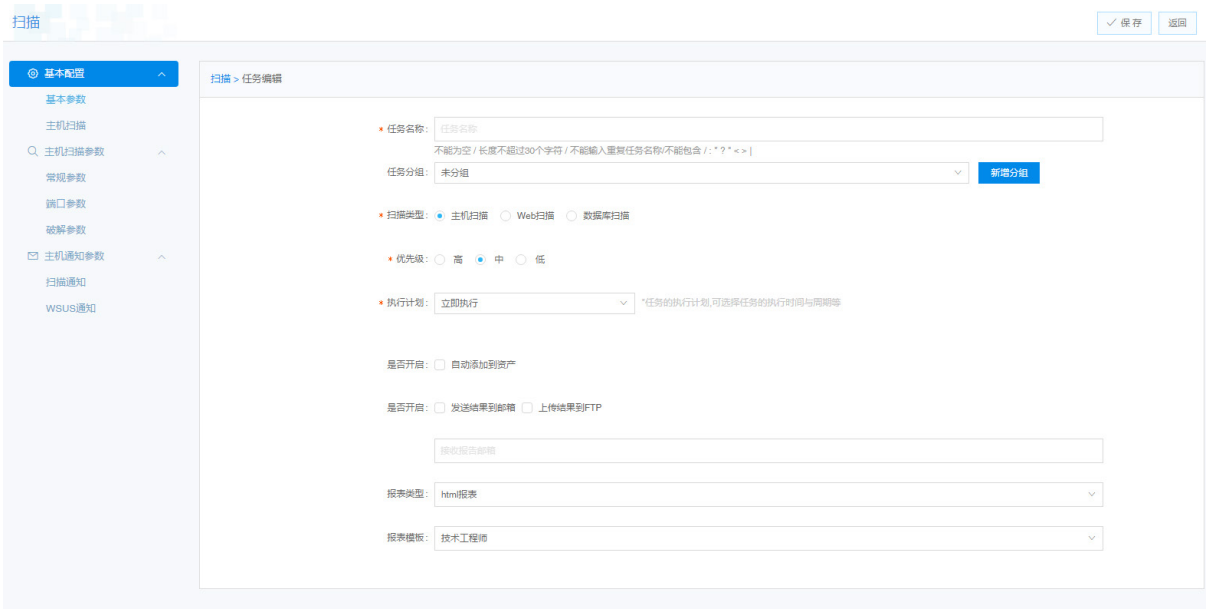
通讯配置，设置扫描器与产品提供内置端浏览器通信地址，使用当前访问的扫描器 IP 地址

配置路径：【其它】>【系统配置】>【通讯配置】

图25 通讯配置

通过【扫描】>【新增任务】创建一个 WEB 扫描任务。

图26 新建任务



基本参数，配置任务名称，扫描类型选择 WEB 扫描，执行计划选择“暂不执行”，其他参数默认。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】

图27 配置基本参数

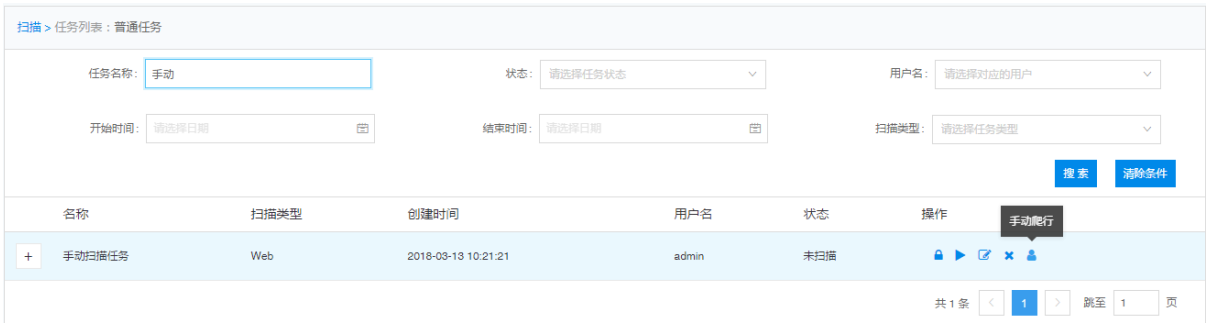
WEB 扫描，输入扫描目标，点击【添加】

配置路径：【扫描】>【新增任务】>【基本配置】>【WEB 扫描】

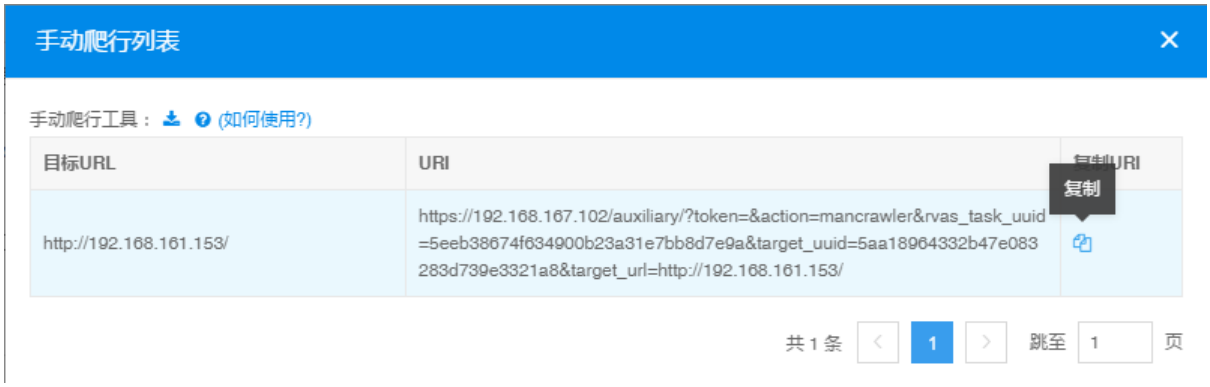
图28 Web 扫描

点击右上角【保存】按钮，查看扫描任务列表，点击该扫描任务右侧的【手动爬行】按钮，弹出手动爬行窗口

图29 手动爬行

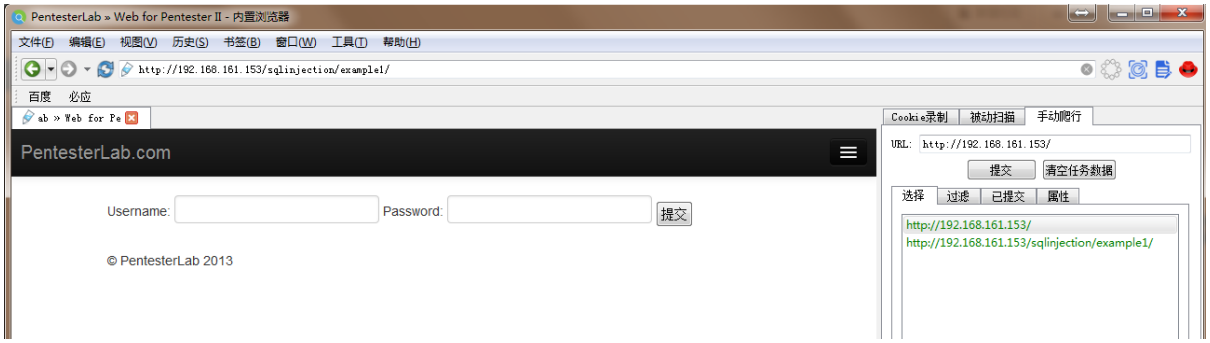


点击【复制】按钮，复制 URI 内容到剪贴板（一次只限一条）



将复制好的 URI 内容粘贴到内置浏览器的地址栏，并回车；通过内置浏览器用户进行手动点击想要检测页面的 URL，点击【提交】按钮，扫描器自动保存所有手动爬行的 URL，开始扫描任务。

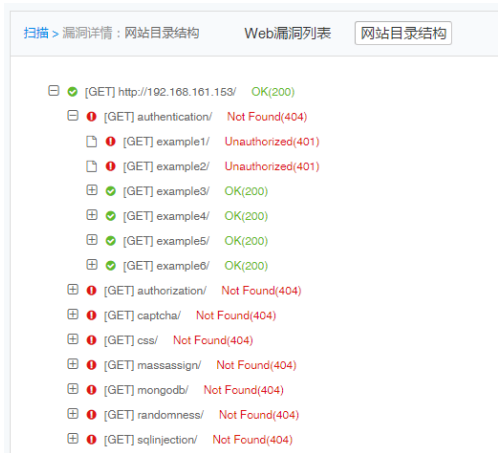
图30 开始扫描



6.3 验证配置

查看扫描结果，目录树显示不只提交的链接扫描，任务在提交链接的基础上，爬行出其他链接进行扫描。

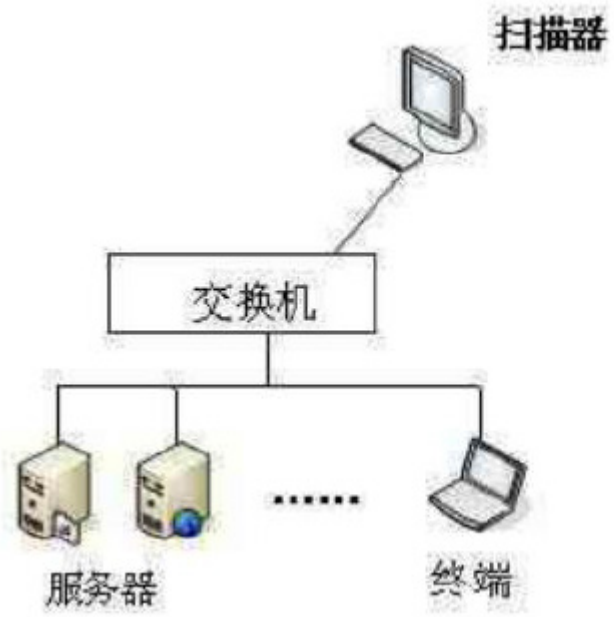
图31 验证配置



7 WEB 被动爬行扫描配置举例

7.1 组网需求

图32 配置组网图



对手动提交的 URL 进行扫描，只扫描提交的 URL，不扫描其余 URL。

7.2 配置步骤

通讯配置，设置扫描器与产品提供内置端浏览器通信地址，使用当前访问的扫描器 IP 地址。

配置路径：【其它】>【系统配置】>【通讯配置】。

图33 通讯配置

通过【扫描】>【新增任务】创建一个 WEB 扫描任务。

图34 新建任务

基本参数，配置任务名称，扫描类型选择 WEB 扫描，执行计划选择“暂不执行”，其他参数默认。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】。

图35 配置基本参数

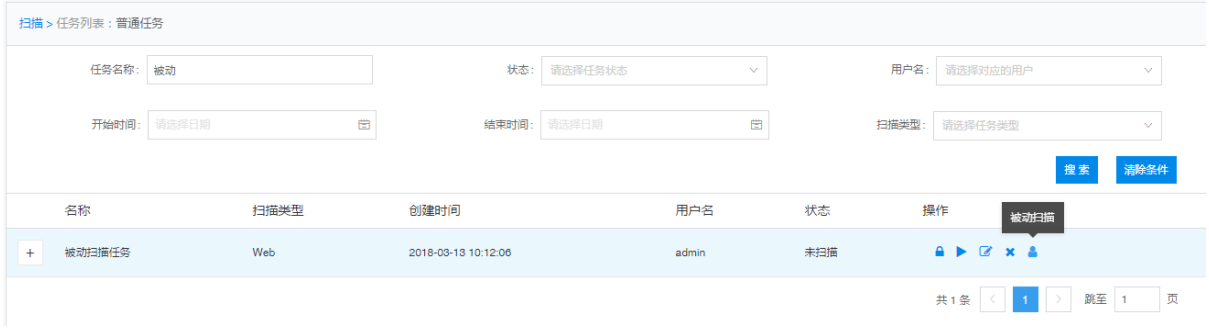
WEB 扫描，输入扫描目标，点击【添加】；扫描类型选择“被动扫描”。

配置路径：【扫描】>【新增任务】>【基本配置】>【WEB 扫描】。

图36 Web 扫描

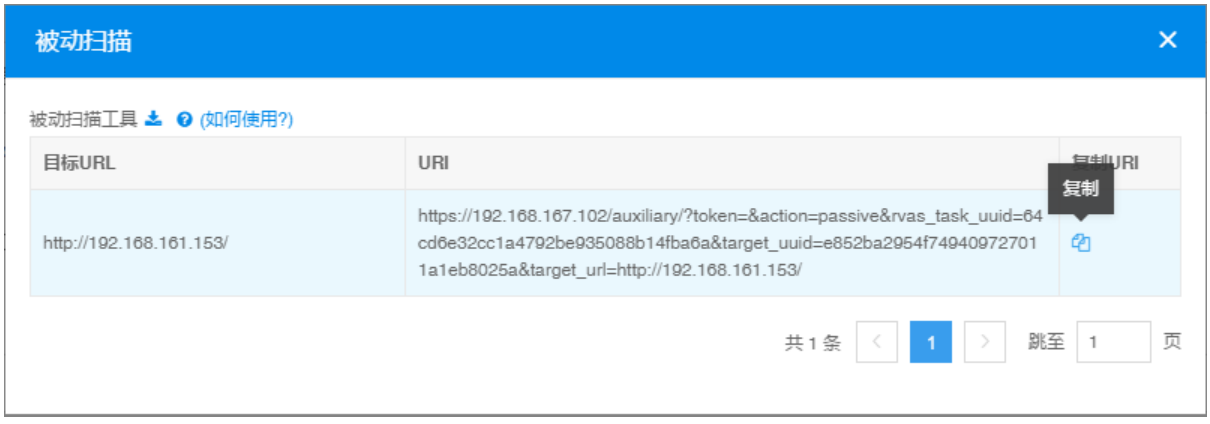
点击右上角【保存】按钮，查看扫描任务列表，点击该扫描任务右侧的【被动爬行】按钮，弹出被动爬行窗口。

图37 被动爬行



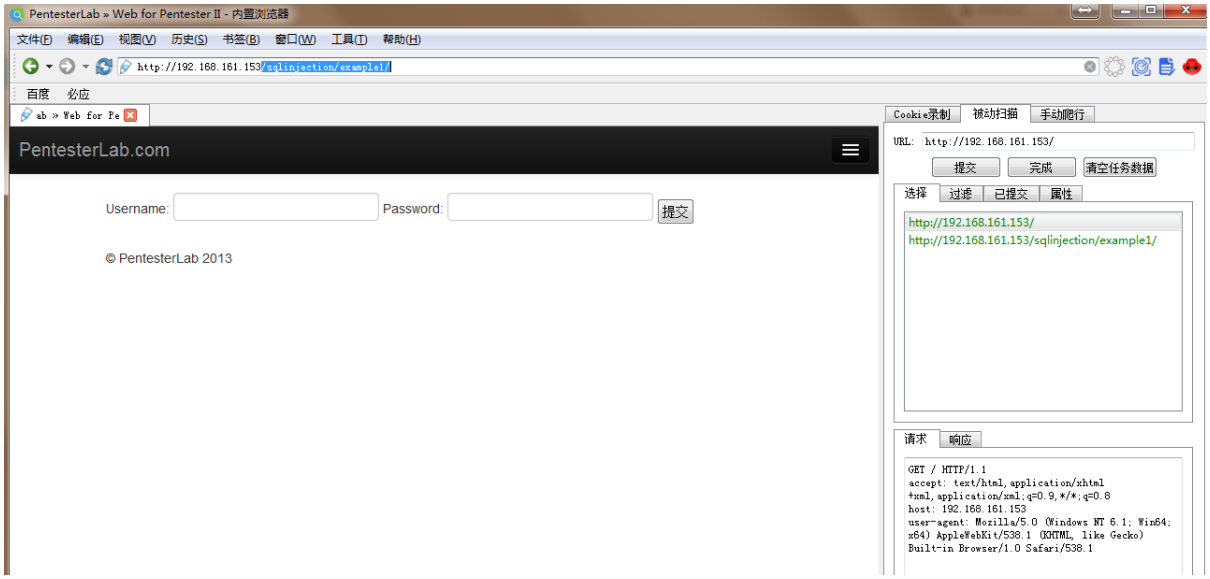
点击【复制】按钮，复制 URI 内容到剪贴板（一次只限一条）。

图38 复制信息



将复制好的 URI 内容粘贴到内置浏览器的地址栏，并回车；通过内置浏览器，用户手动点击要检测页面的 URL，既可以多次点击【提交】按钮进行提交 URL，也可以最后一次性提交 URL，点击【完成】按钮，扫描器将对所有提交的 URL 进行漏洞检测。

图39 漏洞扫描



7.3 验证配置

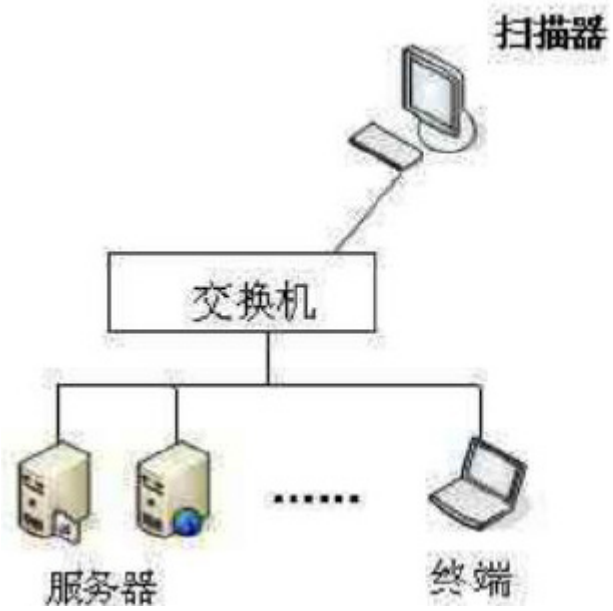
查看扫描结果，目录树只显示了提交的链接，扫描任务不进行其他爬行，只对提交的链接进行扫描。

图40 验证配置

8 数据库扫描配置举例

8.1 组网需求

图41 配置组网图

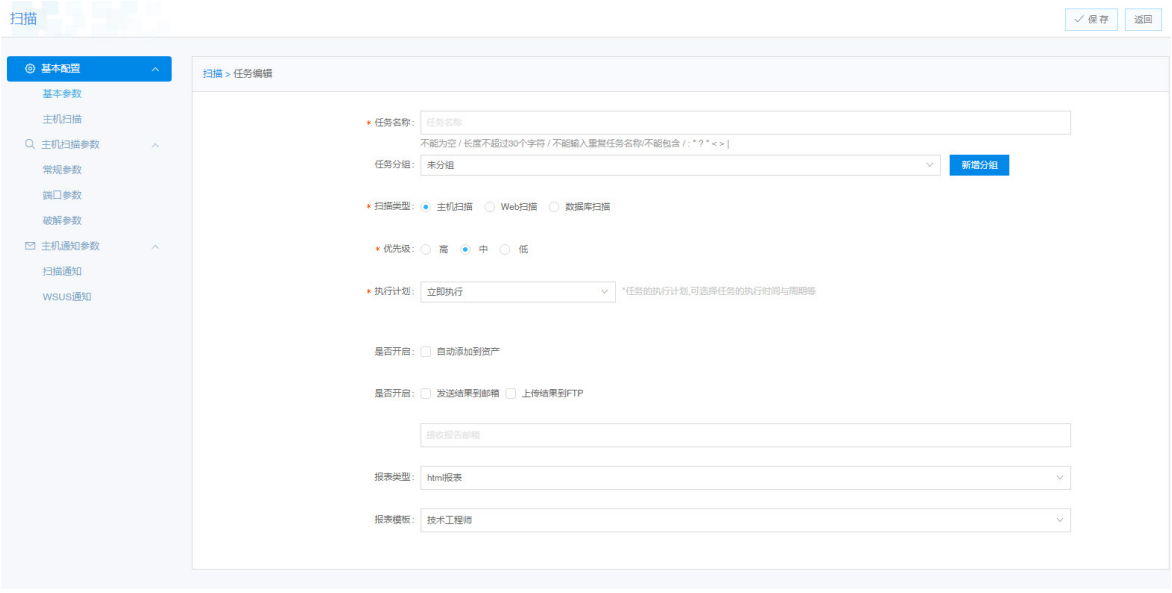


配置认证的数据库扫描结果更加具体详细，扫描的漏洞更全面。

8.2 配置步骤

通过【扫描】>【新增任务】创建一个数据库扫描任务。

图42 新建任务



基本参数，配置任务名称，扫描类型选择“数据库扫描”，其他参数默认。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】。

图43 配置基本参数

数据库扫描，输入扫描目标，显示认证设置配置功能。

配置路径：【扫描】>【新增任务】>【基本配置】>【数据库扫描】。

图44 数据库扫描

点击【手动添加】，弹出新增认证界面窗口。

图45 手动添加

配置扫描认证参数，选择目标、协议、端口、用户名、密码。

图46 配置扫描认证参数

点击【测试连接】，提示“连接成功”。

图47 测试连接

点击【确定】，完成新增认证配置。

图48 完成配置

点击右上角【保存】按钮，即完成数据库递进扫描任务创建。

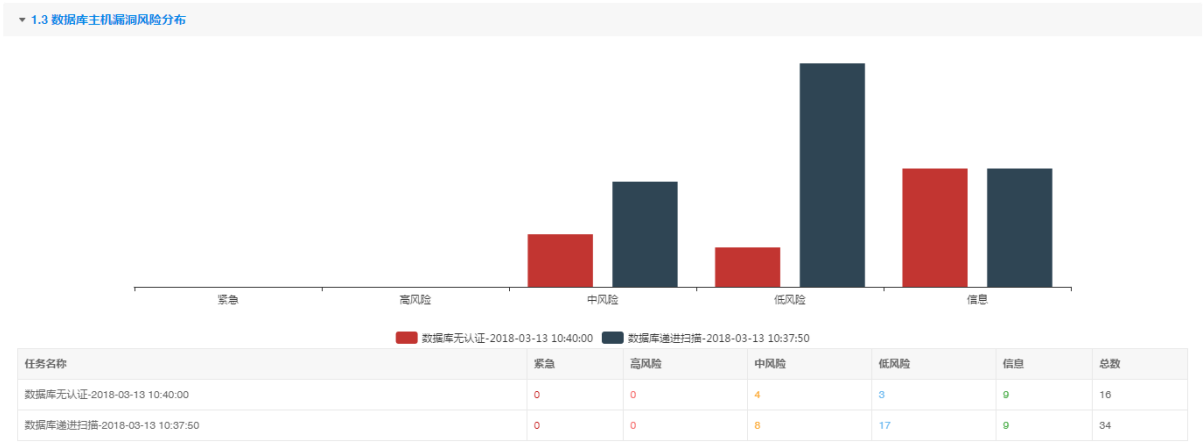
8.3 验证配置

(1) 新建数据库扫描任务，未配置认证参数，其他参数与数据库递进扫描任务一致。

(2) 扫描结束，2 个任务扫描结果，进行对比分析。

(3) 正常情况下扫描出来的数据库递进扫描任务结果比未配置认证参数的扫描任务多。

图49 验证配置



任务名称	紧急	高风险	中风险	低风险	信息	总数
数据库无认证-2018-03-13 10:40:00	0	0	4	3	9	16
数据库递进扫描-2018-03-13 10:37:50	0	0	8	17	9	34