

# UNIS XScan-G 系列漏洞扫描系统

## 典型配置举例

# 目 录

|                             |    |
|-----------------------------|----|
| 1 简介.....                   | 1  |
| 2 配置前提 .....                | 1  |
| 3 主机扫描配置举例.....             | 1  |
| 3.1 组网需求 .....              | 1  |
| 3.2 配置步骤 .....              | 2  |
| 3.3 验证配置 .....              | 4  |
| 4 主机弱口令扫描配置举例.....          | 5  |
| 4.1 组网需求 .....              | 5  |
| 4.2 配置步骤 .....              | 6  |
| 4.3 验证配置 .....              | 8  |
| 5 WEB cookie 录制扫描配置举例 ..... | 8  |
| 5.1 组网需求 .....              | 8  |
| 5.2 配置步骤 .....              | 9  |
| 5.3 验证配置 .....              | 11 |
| 6 WEB 手动爬行扫描配置举例 .....      | 12 |
| 6.1 组网需求 .....              | 12 |
| 6.2 配置步骤 .....              | 13 |
| 6.3 验证配置 .....              | 15 |
| 7 WEB 被动爬行扫描配置举例 .....      | 16 |
| 7.1 组网需求 .....              | 16 |
| 7.2 配置步骤 .....              | 16 |
| 7.3 验证配置 .....              | 19 |
| 8 数据库扫描配置举例 .....           | 20 |
| 8.1 组网需求 .....              | 20 |
| 8.2 配置步骤 .....              | 20 |
| 8.3 验证配置 .....              | 23 |

# 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

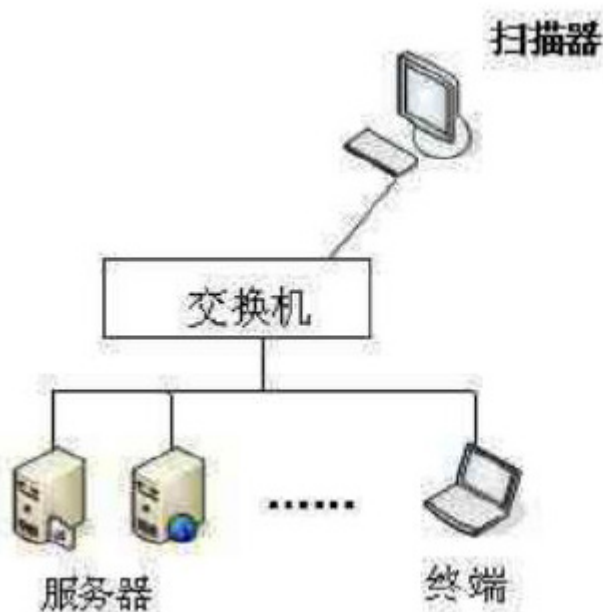
本文档不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

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

扫描

保存返回

基本配置

基本参数

主机扫描

主机扫描参数

主机通知参数

扫描 > 任务编辑

扫描目标: 192.168.101.158

从模板导入  
从资产导入  
模板下载

认证设置:

| 目标             | 协议 | 端口 | 用户名 | 密码 | 操作 |
|----------------|----|----|-----|----|----|
| 导入认证 手动添加 认证下载 |    |    |     |    |    |

策略模板: 完全扫描

参数模板: 默认参数

注意: 重新选择参数模板将重置所有已设置好的参数

点击【手动添加】，弹出新增认证界面窗口。

图5 新增认证

新增认证

目标:

协议:

端口:

端口范围为: 1-65535

用户名:

密码:

确定

取消

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

新增认证

\*

目标:

192.168.161.158

▼

\*

协议:

smb

▼

\*

端口:

445

端口范围为: 1-65535

\*

用户名:

administrator

密码:

\*\*\*\*\*

确定

取消

点击确定，完成新增认证配置

图7 完成配置

扫描

✓ 保存 返回

基本配置

基本参数

主机扫描

主机扫描参数

主机通知参数

扫描 > 任务编辑

扫描目标:

192.168.161.158

从模板导入

从资产导入

模板下载

认证设置:

| 目标              | 协议  | 端口  | 用户名           | 密码    | 操作 |
|-----------------|-----|-----|---------------|-------|----|
| 192.168.161.158 | smb | 445 | administrator | ***** | 删除 |

导入认证

手动添加

认证下载

策略模板:

完全扫描

参数模板:

默认参数

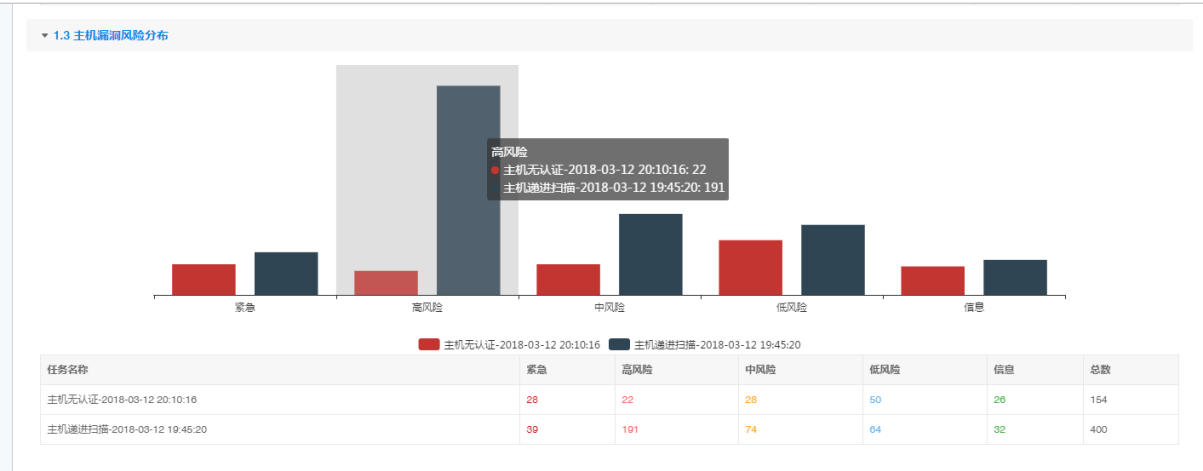
注意: 重新选择参数模板将重置所有已设置好的参数

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。

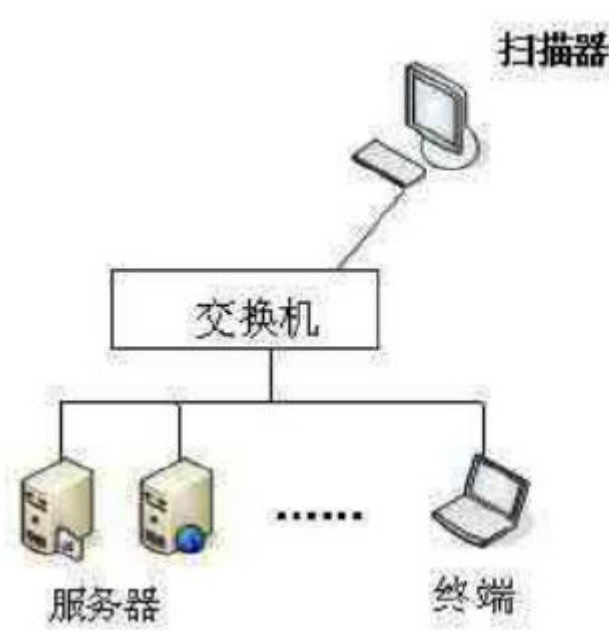
图8 验证配置



## 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

模板 > 字典模板

字典名称: test1  
描述信息: test  
字典类型: 用户字典

字典名称不为空且不超过30个字符  
描述信息不为空且不超过200个字符

Administrator  
administrator  
Guest  
guest  
admin  
system

字典内容长度不超过65535个字符

通过【扫描】>【新增任务】创建一个主机扫描任务。

图11 新增任务

扫描 > 任务编辑

任务名称: 任务名称  
任务分组: 未分组  
扫描类型: 主机扫描 Web扫描 数据库扫描  
优先级: 高 中 低  
执行计划: 立即执行  
是否开启: 自动添加到资产  
是否开启: 发送结果到邮箱 上传结果到FTP  
报表类型: html报表  
报表模板: 技术工程师

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

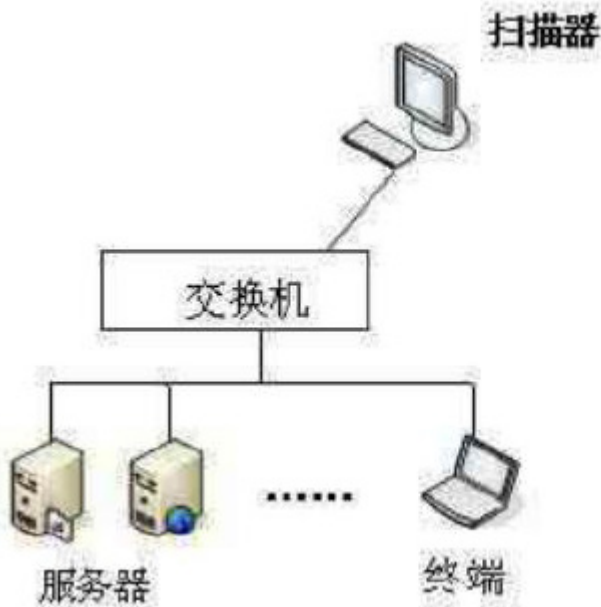
扫描

| 扫描 > 任务详情: 账户 |               |           |    |
|---------------|---------------|-----------|----|
| 主机目标          |               | 主机漏洞      | 服务 |
|               |               |           | 账户 |
| 服务            | 用户名           | 密码        | 次数 |
| + SMB/445     | admin         | #test-123 | 1  |
| + SMB/445     | Administrator | @test123  | 1  |
| + SMB/445     | Guest         | 未知        | 1  |

## 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

扫描 > 任务编辑

基本配置

任务名称:  不能为空 / 长度不超过30个字符 / 不能输入重复任务名称(不能包含 / : \* ? " < > |)

任务分组:  未分组

扫描类型: ☒ 主机扫描 ☐ Web扫描 ☐ 数据库扫描

优先级: ☐ 高 ☒ 中 ☐ 低

执行计划:  立即执行 \*任务的执行计划,可选择任务的执行时间与周期等

是否开启: ☐ 自动添加到资产

是否开启: ☐ 发送结果到邮箱 ☐ 上传结果到FTP

接收报告邮箱:

报告类型:  html报告

报告模板:  技术工程师

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

扫描 > 任务编辑

基本配置

任务名称:  cookie复制扫描 不能为空 / 长度不超过30个字符 / 不能输入重复任务名称(不能包含 / : \* ? " < > |)

任务分组:  未分组

扫描类型: ☐ 主机扫描 ☒ Web扫描 ☐ 数据库扫描

优先级: ☐ 高 ☒ 中 ☐ 低

执行计划:  立即执行 \*任务的执行计划,可选择任务的执行时间与周期等

是否开启: ☐ 自动添加到资产

是否开启: ☐ 发送结果到邮箱 ☐ 上传结果到FTP

接收报告邮箱:

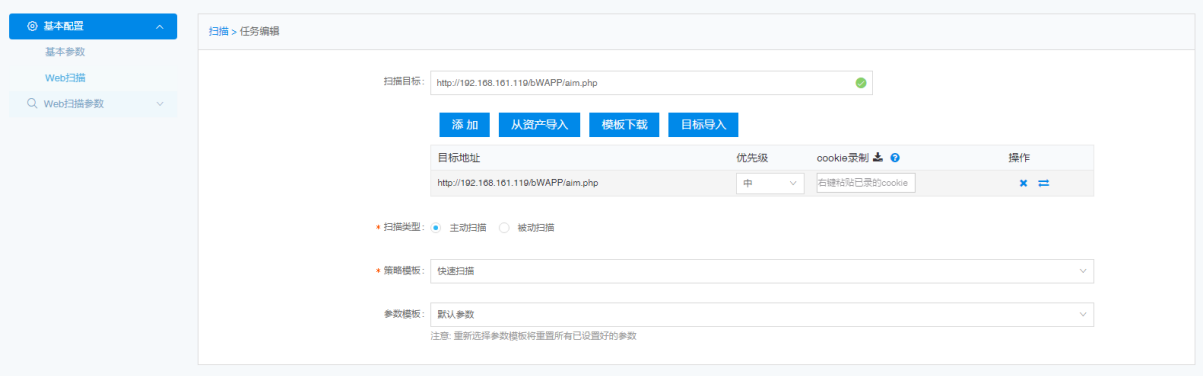
报告类型:  html报告

报告模板:  技术工程师

WEB扫描，输入扫描目标，点击添加。

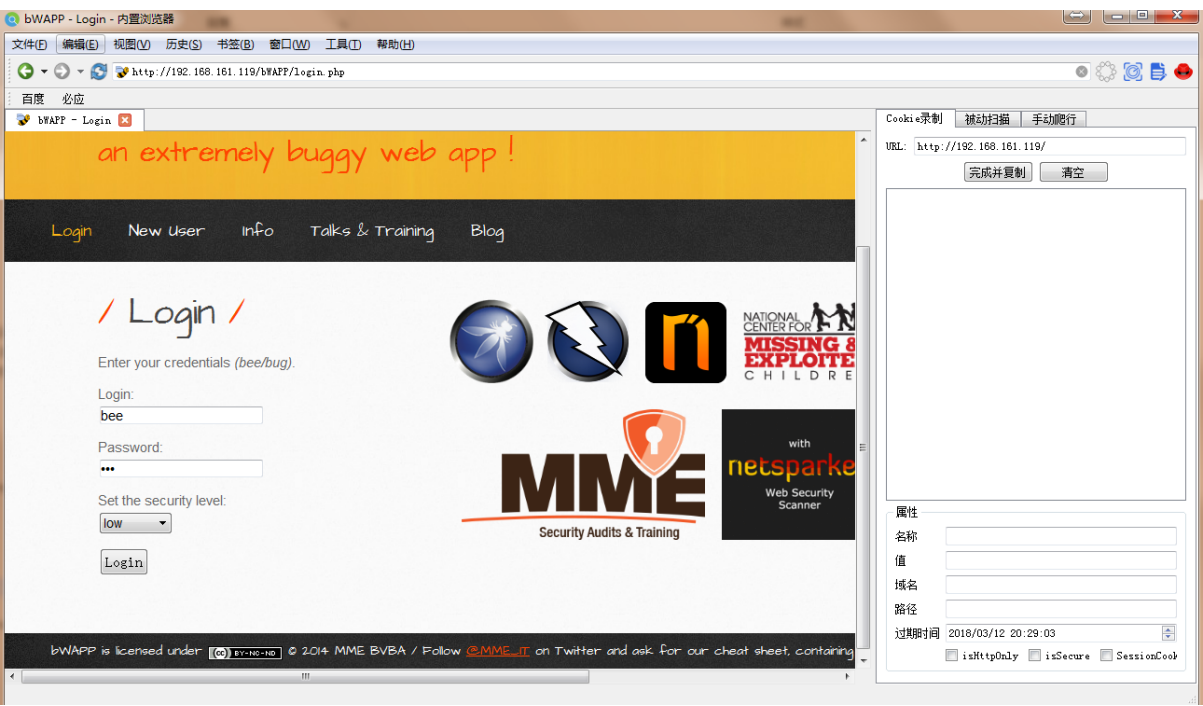
配置路径：【扫描】>【新增任务】>【基本配置】>【WEB扫描】。

图19 Web 扫描



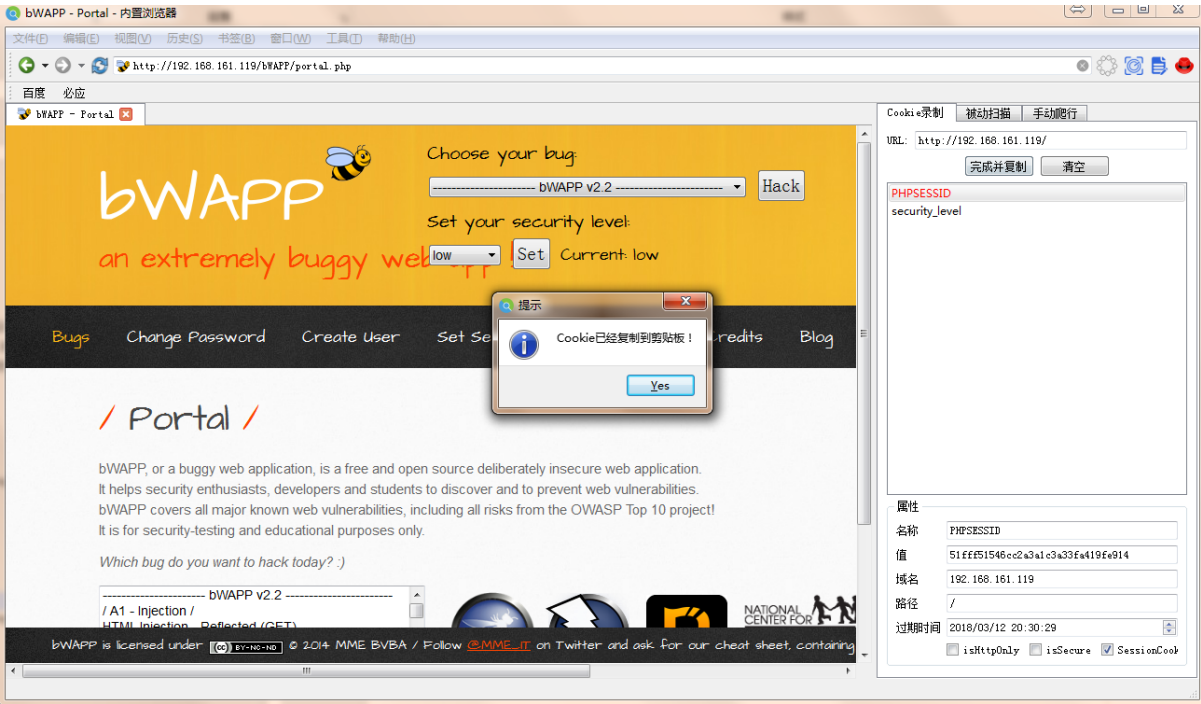
打开内置浏览器，在地址栏输入要录制 cookie 的目标 URL，回车并在网页上输入正确用户名密码登录。

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



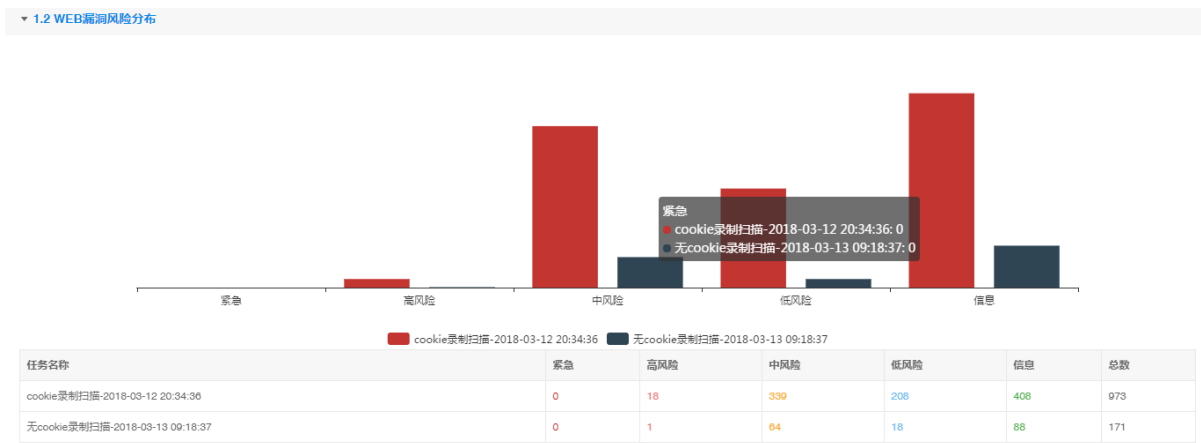
点击右上角【保存】按钮，即完成扫描任务创建，注意：扫描过程不要关闭内置浏览器，关闭会影响扫描结果

### 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 录制的扫描任务多。

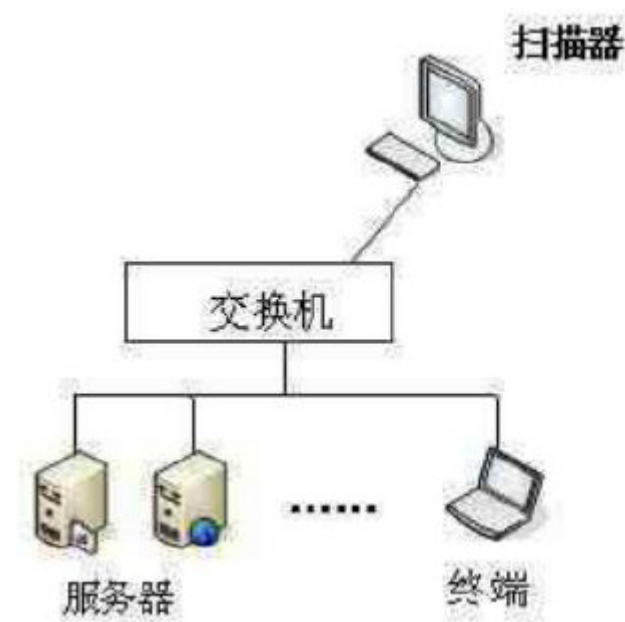
图23 验证配置



## 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

基本配置

基本参数

Web扫描

Web扫描参数

扫描 > 任务编辑

任务名称: 手动扫描任务

不能为空 / 长度不超过30个字符 / 不能输入重复任务名称/不能包含 / : \* ? " < > |

任务分组: 未分组

新增分组

扫描类型: ☐ 主机扫描 ☒ Web扫描 ☐ 数据库扫描

优先级: ☐ 高 ☒ 中 ☐ 低

执行计划: 暂不执行

\*任务的执行计划,可选择任务的执行时间与周期等

是否开启: ☐ 自动添加到资产

是否开启: ☐ 发送结果到邮箱 ☐ 上传结果到FTP

接收报告邮箱

报表类型: html报表

报表模板: 技术工程师

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

扫描

基本配置

基本参数

Web扫描

Web扫描参数

扫描 > 任务编辑

扫描目标: http://192.168.101.153/

添加

从资产导入

模板下载

目标导入

| 目标地址                    | 优先级 | cookie限制      | 操作                        |
|-------------------------|-----|---------------|---------------------------|
| http://192.168.101.153/ | 中   | 右键粘贴已选的cookie | <div>✕</div> <div>≡</div> |

扫描类型: ☒ 主动扫描 ☐ 被动扫描

策略模板: 快速扫描

参数模板: 默认参数

注意: 重新选择参数模板将重置所有已设置好的参数

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

扫描 > 任务列表 : 普通任务

任务名称: 手动

状态: 请选择任务状态

用户名: 请选择对应的用户

开始时间: 请选择日期

结束时间: 请选择日期

扫描类型: 请选择任务类型

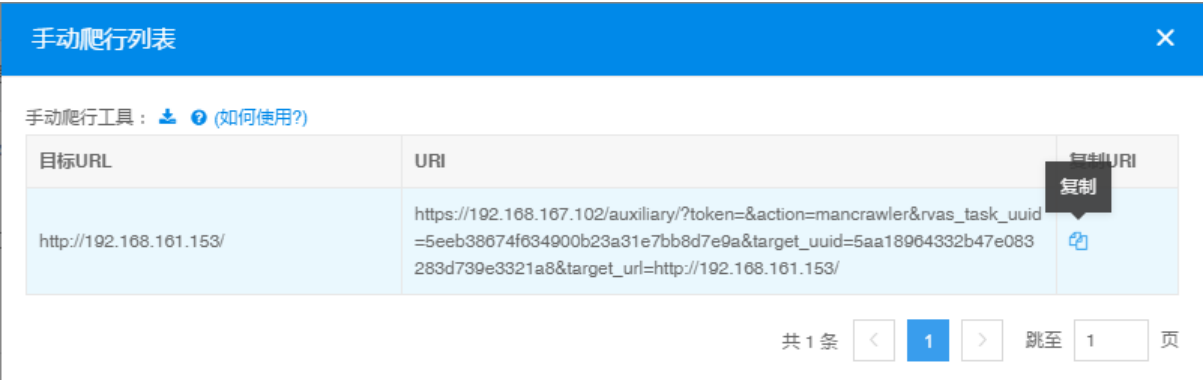
搜索

清除条件

| 名称       | 扫描类型 | 创建时间                | 用户名   | 状态  | 操作              |
|----------|------|---------------------|-------|-----|-----------------|
| + 手动扫描任务 | Web  | 2018-03-13 10:21:21 | admin | 未扫描 | <div>手动爬行</div> |

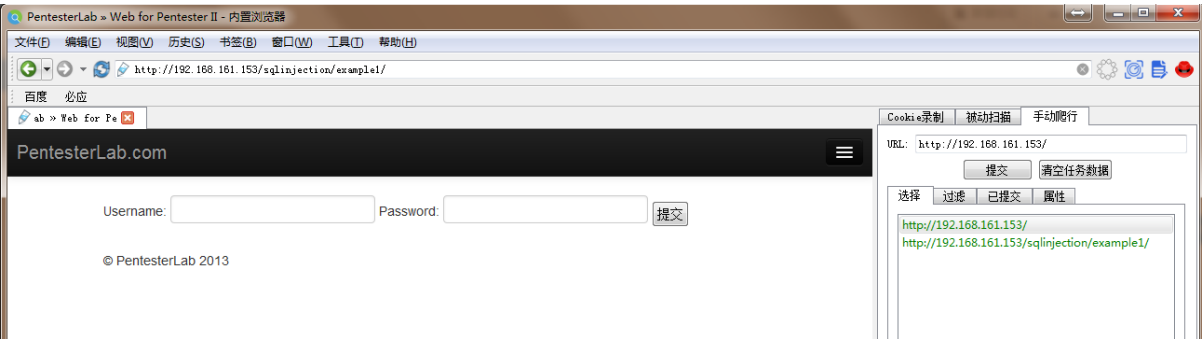
共 1 条 < 1 > 跳至 1 页

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。

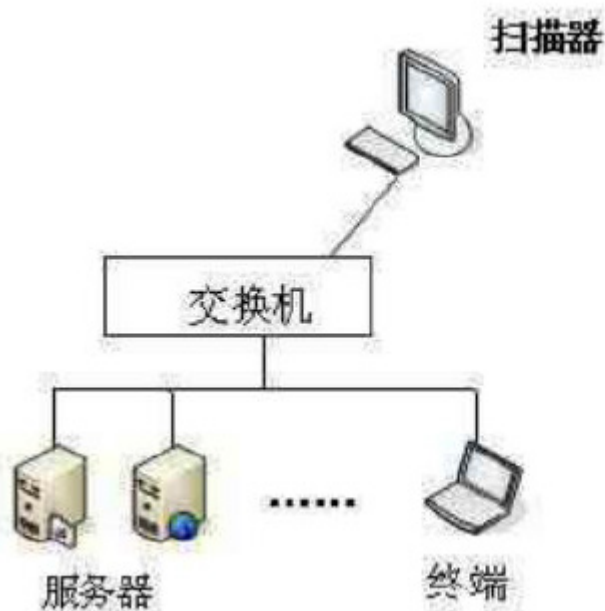
图31 验证配置



## 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



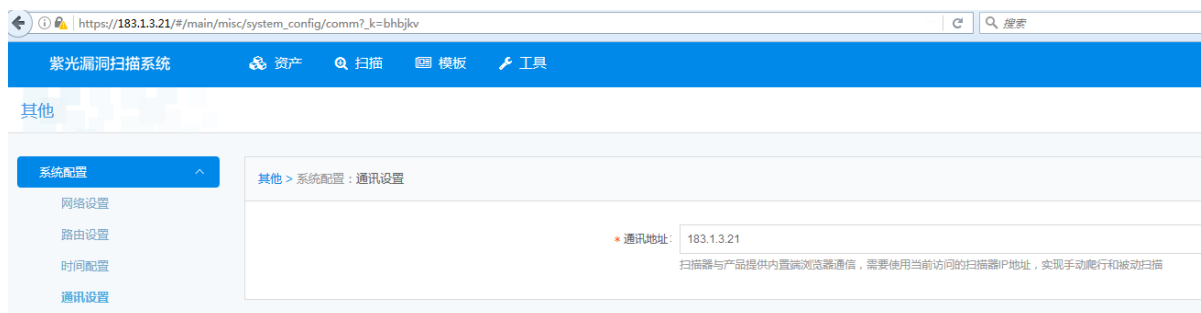
对手动提交的 URL 进行扫描，只扫描提交的 URL，不扫描其余 URL。

### 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

扫描

基本配置

基本参数

主机扫描

主机扫描参数

常规参数

端口参数

破解参数

主机通知参数

扫描通知

WSUS通知

扫描 > 任务编辑

任务名称:  不能为空 / 长度不超过30个字符 / 不能输入重复任务名称/不能包含 / : \* ? " < > |

任务分组: 未分组 新增分组

扫描类型: ☒ 主机扫描 ☐ Web扫描 ☐ 数据库扫描

优先级: ☐ 高 ☒ 中 ☐ 低

执行计划: 立即执行 \*任务的执行计划,可选择任务的执行时间与周期等

是否开启: ☐ 自动添加到资产

是否开启: ☐ 发送结果到邮箱 ☐ 上传结果到FTP

接收报告邮箱:

报表类型: html报表

报表模板: 技术工程师

保存 返回

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

基本配置

基本参数

Web扫描

Web扫描参数

扫描 > 任务编辑

任务名称: 被动扫描任务 不能为空 / 长度不超过30个字符 / 不能输入重复任务名称/不能包含 / : \* ? " < > |

任务分组: 未分组 新增分组

扫描类型: ☐ 主机扫描 ☒ Web扫描 ☐ 数据库扫描

优先级: ☐ 高 ☒ 中 ☐ 低

执行计划: 暂不执行 \*任务的执行计划,可选择任务的执行时间与周期等

是否开启: ☐ 自动添加到资产

是否开启: ☐ 发送结果到邮箱 ☐ 上传结果到FTP

接收报告邮箱:

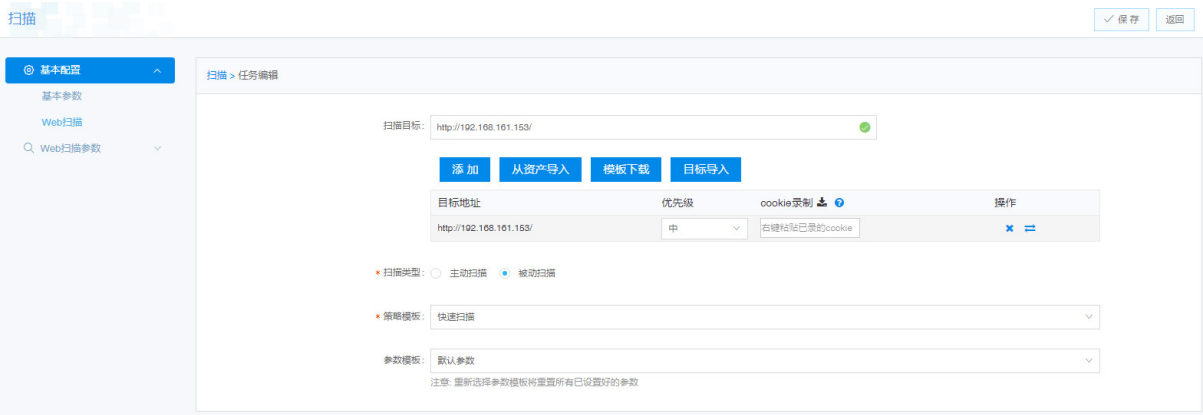
报表类型: html报表

报表模板: 技术工程师

保存 返回

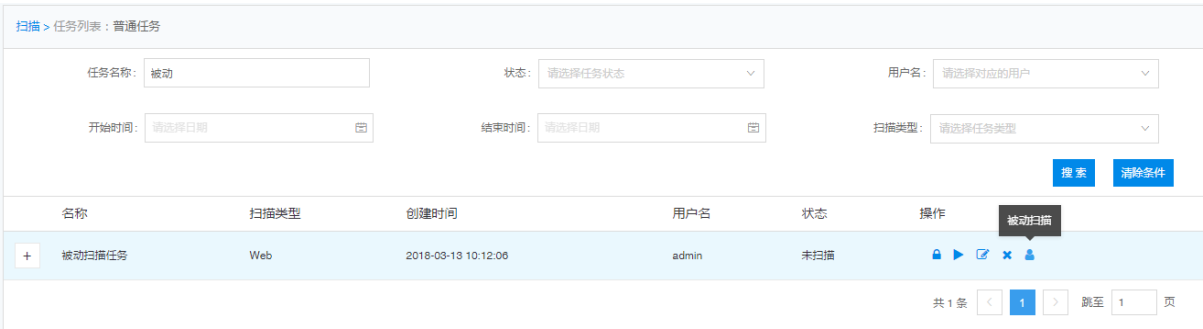
WEB 扫描，输入扫描目标，点击【添加】；扫描类型选择“被动扫描”。  
配置路径：【扫描】>【新增任务】>【基本配置】>【WEB 扫描】。

图36 Web 扫描



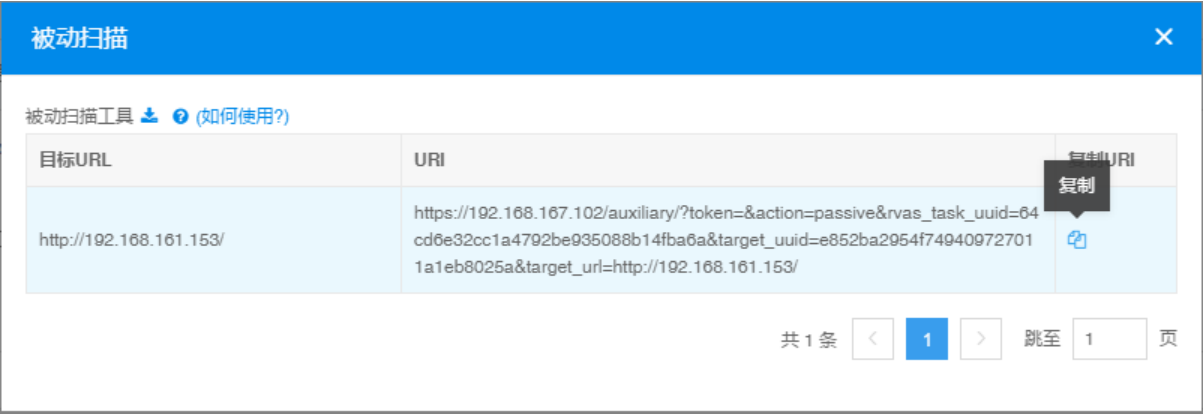
点击右上角【保存】按钮，查看扫描任务列表，点击该扫描任务右侧的【被动爬行】按钮，弹出被动爬行窗口。

图37 被动爬行



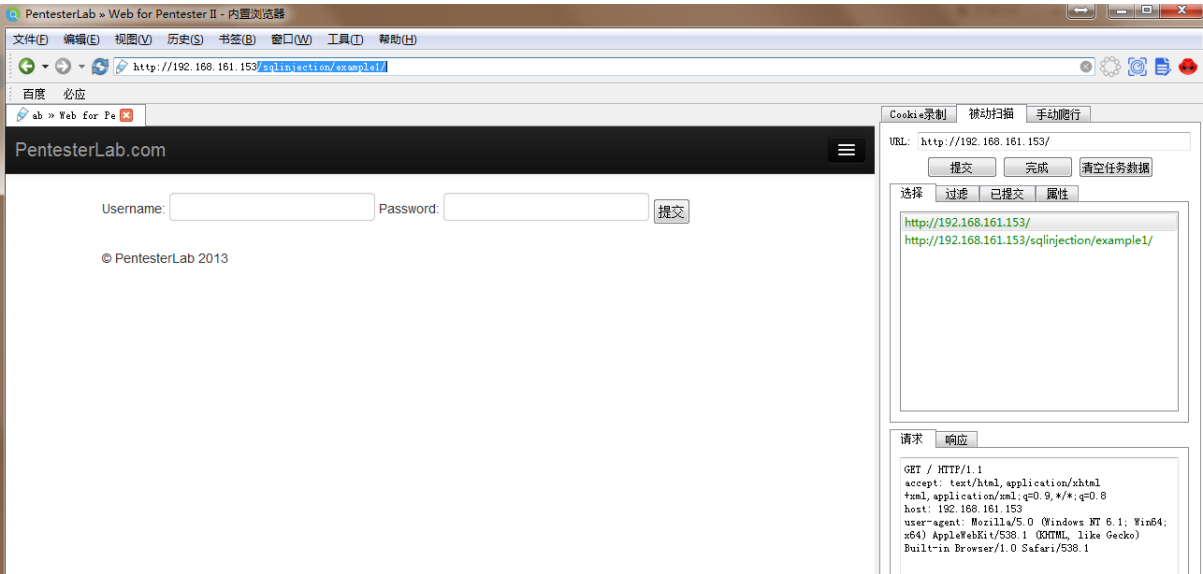
点击【复制】按钮，复制 URI 内容到剪贴板（一次只限一条）。

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。

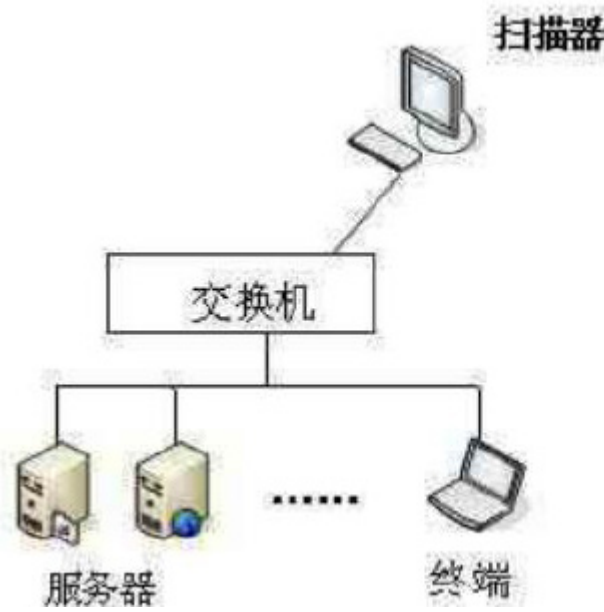
图40 验证配置



# 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

The screenshot shows the '扫描' (Scan) section of a software interface. On the left is a sidebar with navigation options: '基本参数' (Basic Parameters), '主机扫描' (Host Scan), '主机扫描参数' (Host Scan Parameters), '常规参数' (General Parameters), '端口参数' (Port Parameters), '破解参数' (Crack Parameters), '主机通知参数' (Host Notification Parameters), '扫描通知' (Scan Notification), and 'WSUS通知' (WSUS Notification). The main area is titled '扫描 > 任务编辑' (Scan > Task Edit). It contains several configuration fields: '任务名称' (Task Name) with a text input and a validation rule; '任务分组' (Task Group) with a dropdown menu and a '新建分组' (New Group) button; '扫描类型' (Scan Type) with radio buttons for '主机扫描' (selected), 'Web扫描' (Web Scan), and '数据库扫描' (Database Scan); '优先级' (Priority) with radio buttons for '高' (High), '中' (selected), and '低' (Low); '执行计划' (Execution Plan) with a dropdown set to '立即执行' (Execute Immediately) and a note; '是否开启' (Whether to Enable) with checkboxes for '自动添加到资产' (Automatically add to assets), '发送结果到邮箱' (Send results to email), and '上传结果到FTP' (Upload results to FTP); '接收器IP地址' (Receiver IP address) with a text input; '报表类型' (Report Type) with a dropdown set to 'html报表' (HTML Report); and '报表模板' (Report Template) with a dropdown set to '技术工程师' (Technical Engineer). At the top right of the main area are '保存' (Save) and '返回' (Return) buttons.

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

新增认证

目标:

协议:

端口:

端口范围为 : 1-65535

用户名:

密码:

确定

取消

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

新增认证

目标:

192.168.162.136

协议:

mysql

端口:

3306

端口范围为 : 1-65535

用户名:

root

密码:

\*\*\*\*\*

数据库名称:

配置路径:

数据库安装目录，如：/usr/local/mysql/

测试链接

确定

取消

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

