THM-Nessus(基础)-学习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/rpnessusredux

H2 简介

注意：本文中安装的是免费版的Nessus。

Nessus 是一款 C/S 架构的漏洞扫描系统，作为一款漏洞扫描软件，不仅功能全面，而且还可以实时更新漏洞库，据统计有超过 75,000 个机构在使用它。

Nessus 使用类似于 Nmap 的技术来查找和报告漏洞，然后将这些漏洞呈现在一个GUI 中供我们查看，Nessus 与其他扫描软件不同，因为它在扫描时不做假设，例如，假设 Web 应用程序在端口 80 上运行。

Nessus有付费版和免费版，免费版的功能相对于付费版受到一定限制。

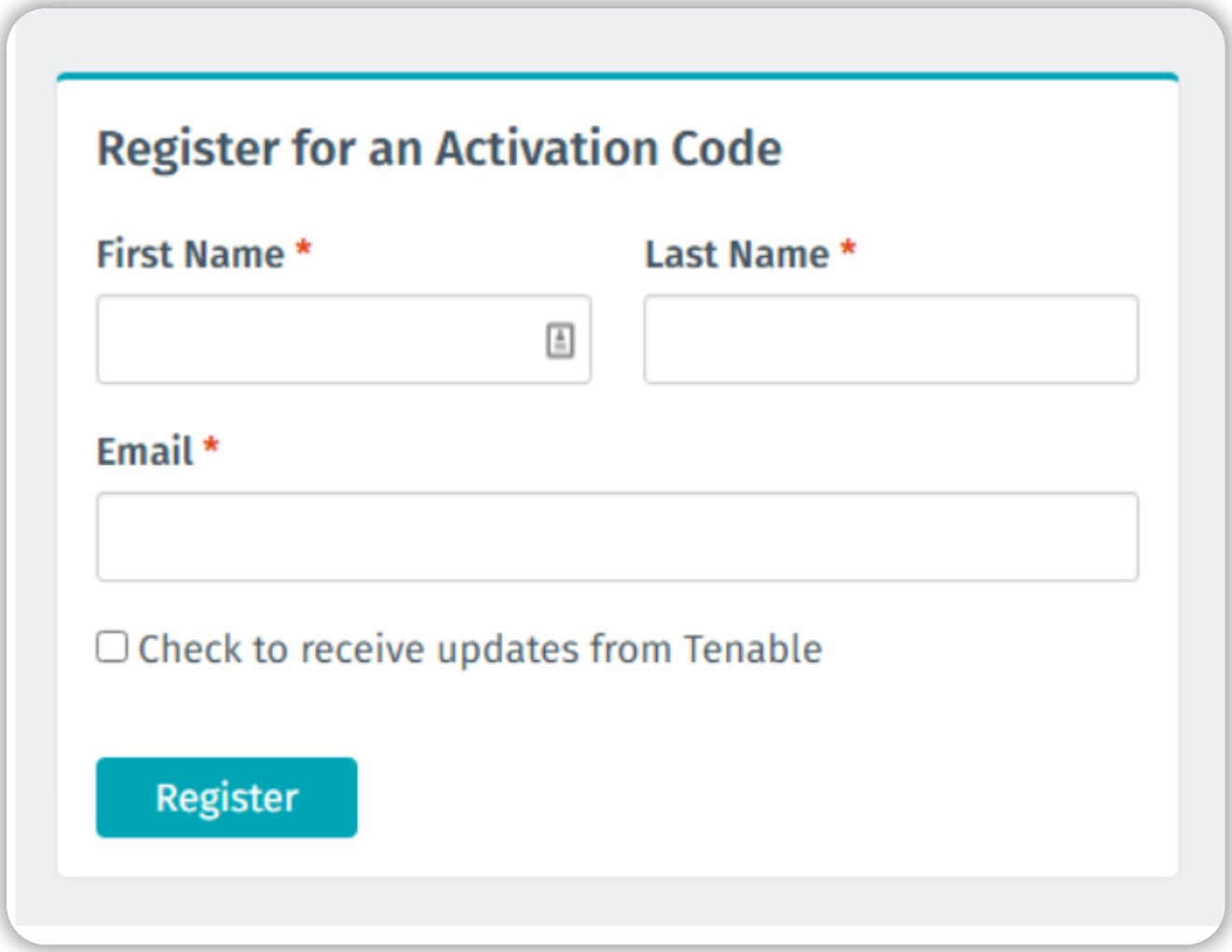
H2 Nessus安装

官方安装指南： https://docs.tenable.com/nessus/Content/GettingStarted.htm

在Kali虚拟机上安装Nessus

步骤一：

访问网址 https://www.tenable.com/products/nessus/nessus-essentials 注册一个账户（输入用户名称+电子邮箱即可），获取激活码



步骤二：

下载对应版本的Nessus（这里选择Linux-Debian-amd64平台，此平台对于比较新的Kali版本都适用），保存到/Downloads/文件夹（或者其他文件夹）

步骤三：

在终端中，我们将导航到包含刚才所下载文件的文件夹并运行以下命令：

```
#sudo dpkg -i package_file.deb
sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb     #请记住用你下载的文件的名称替换
package_file.deb
```

记录信息备用：

> - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
> - Then go to https://hekeats:8834/ to configure your scanner

步骤四：

现在我们将用以下命令启动 Nessus 服务:

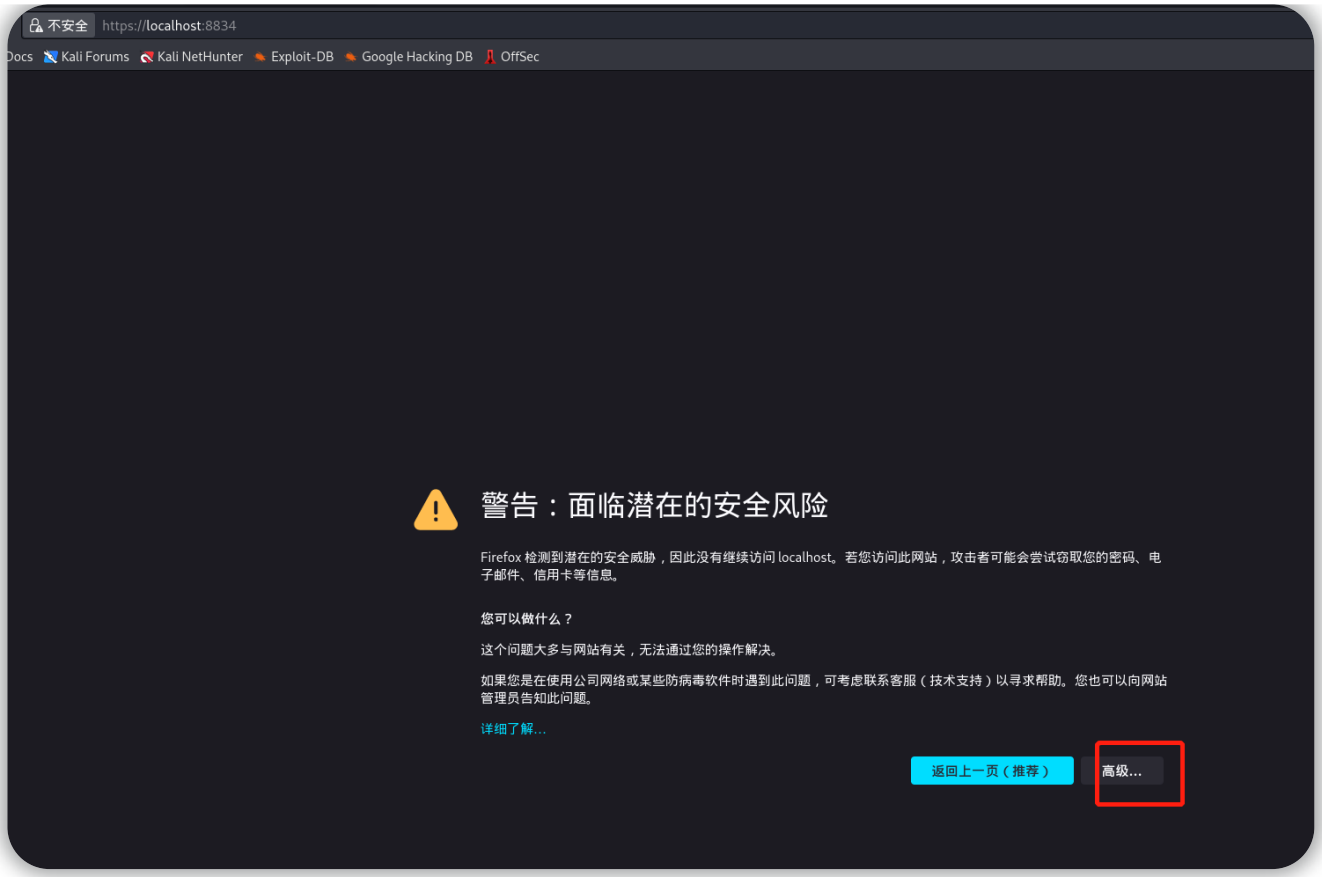
```
sudo /bin/systemctl start nessusd.service
```

步骤五：

打开网站访问本地8834端口：

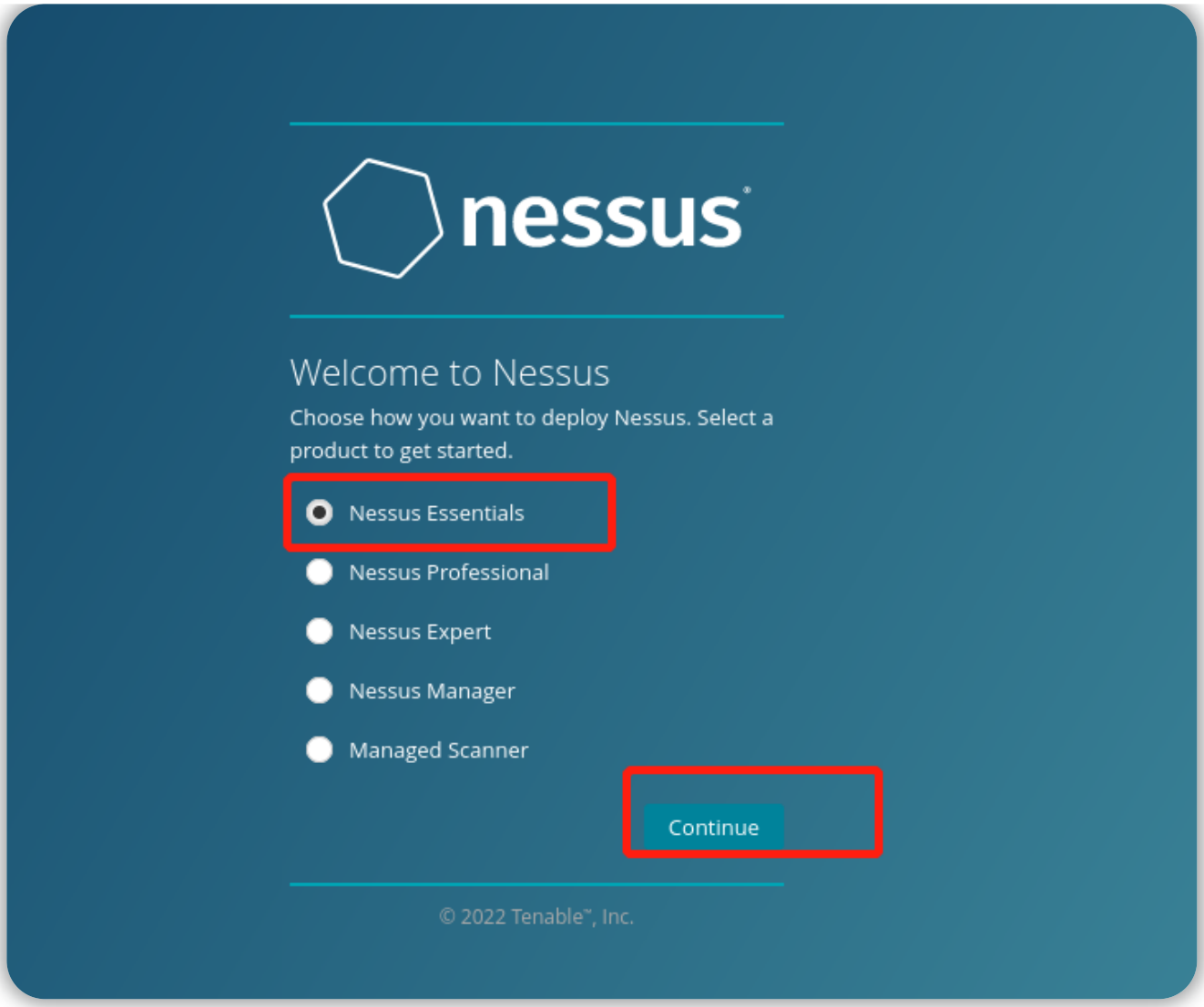
```
#在浏览器url中输入
https://localhost:8834/    #也可以使用自己的kali账户名：https://hekeats:8834/
```

你可能会收到安全风险警报提示，单击“高级...”-> 接受风险并继续：

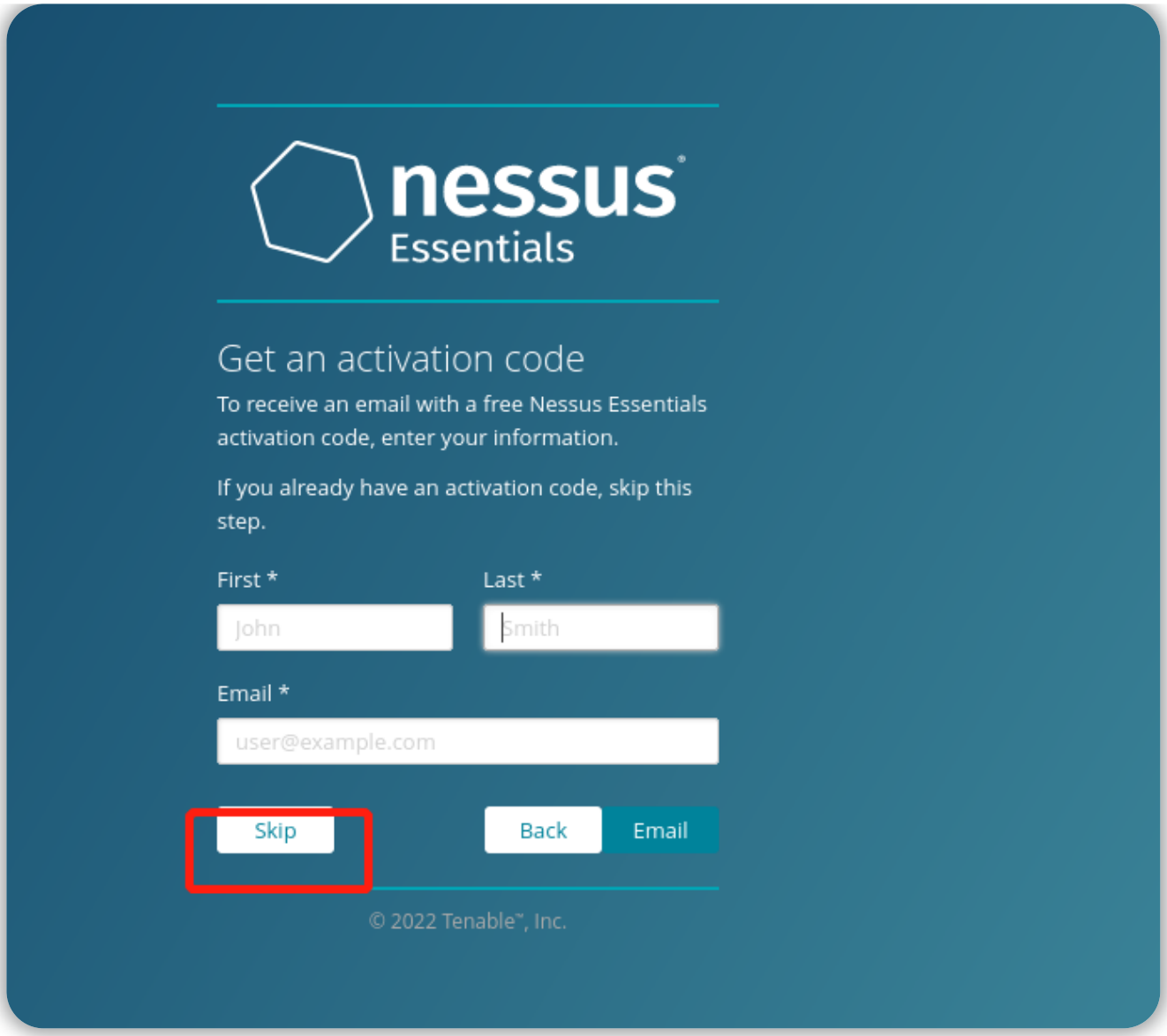


步骤六：

接下来，我们将设置扫描器，选择Nessus Essentials选项：



接下来选择skip，因为我们之前已经注册了账户，并在自己的邮箱里面收到了激活码：

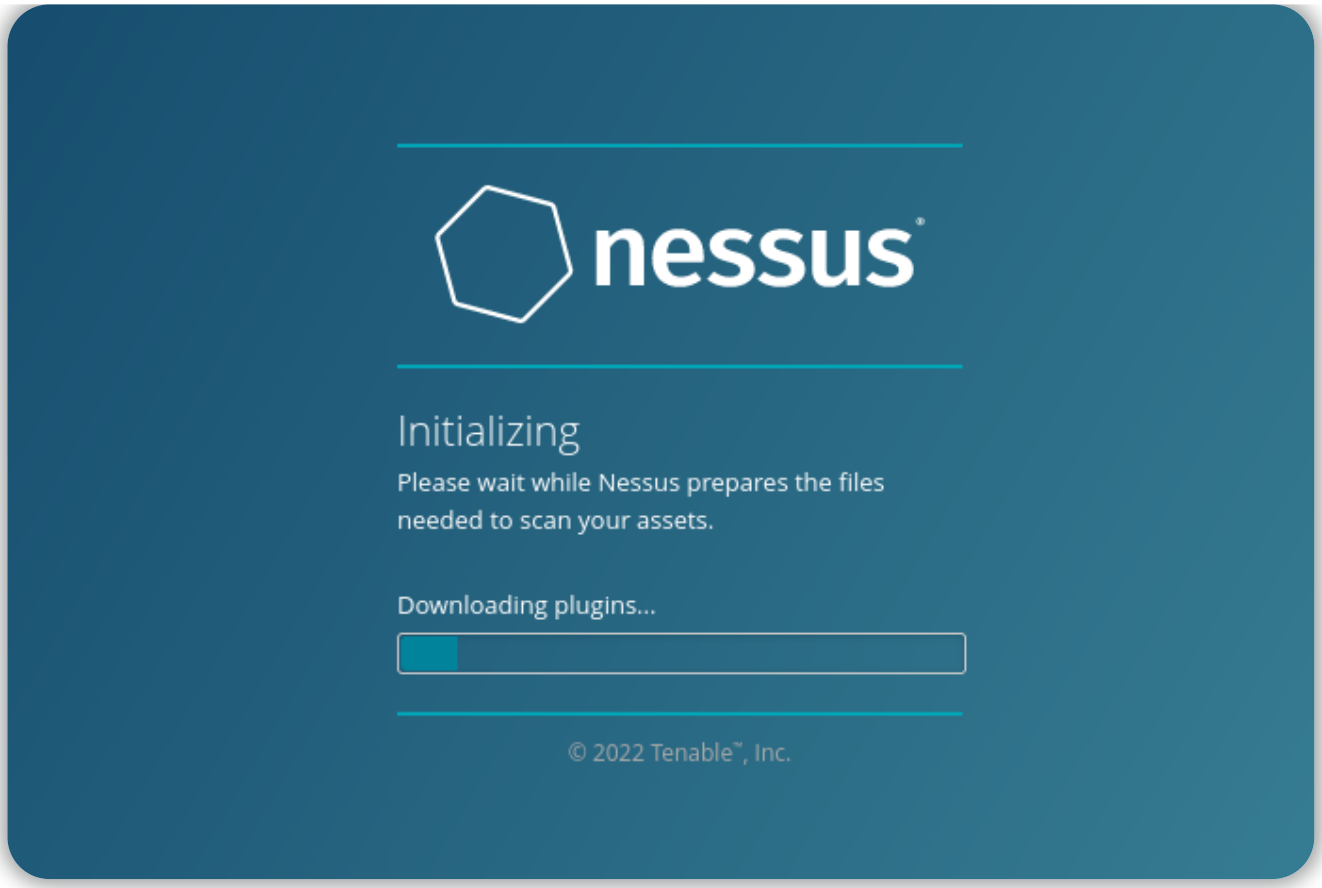


填入之前在邮箱中收到的激活码即可：

创建Nessus使用时进行登陆的账户和密码：

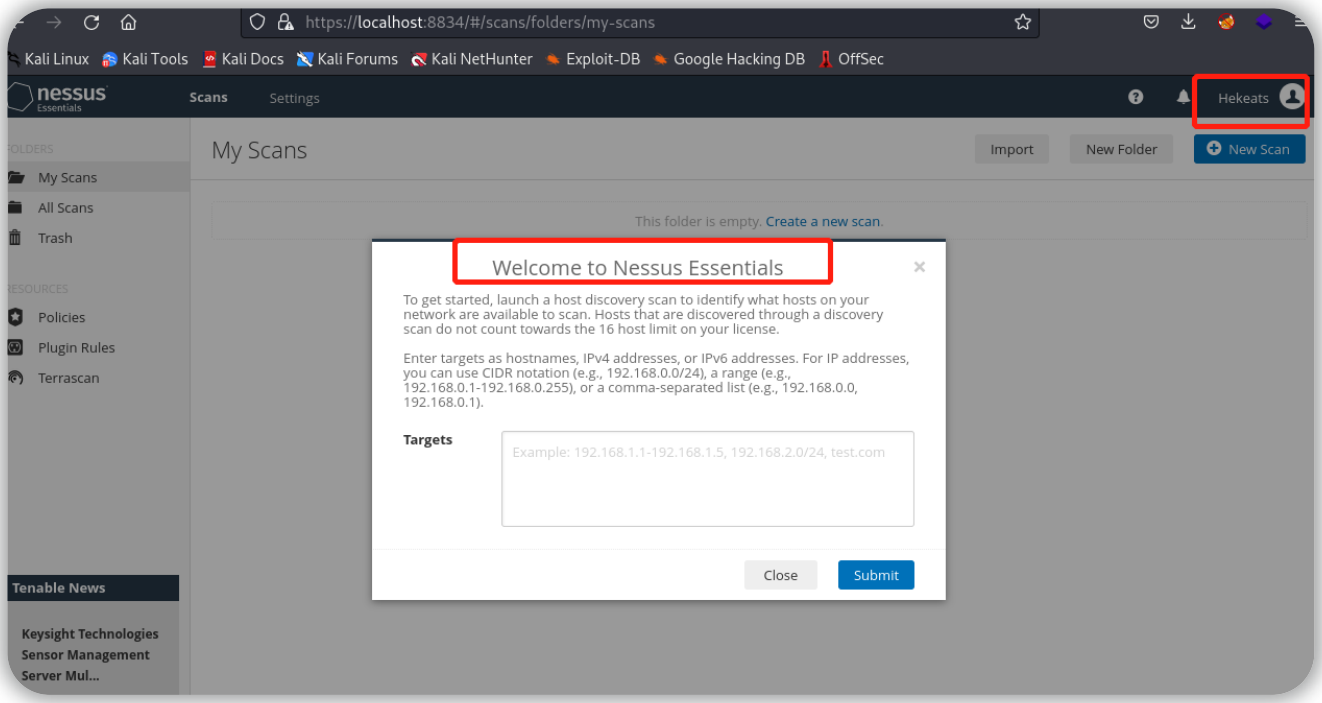
步骤八：

Nessus 现在将安装运行所需的插件（如果进度条看起来没有移动，这意味着 VM 上没有足够的空间来安装）。



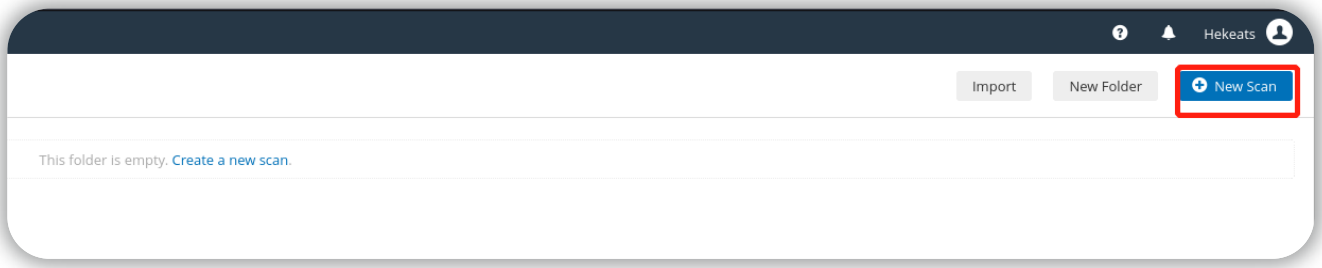
步骤九：

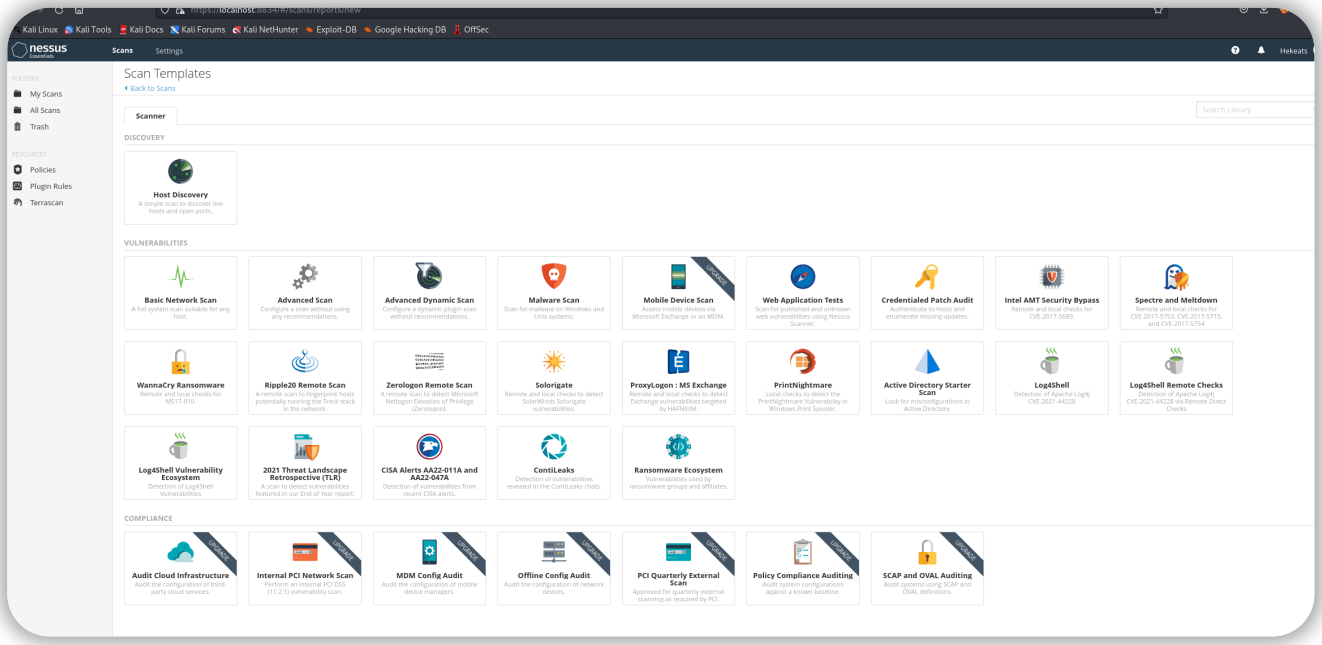
使用之前设置的账户密码--登陆即可。



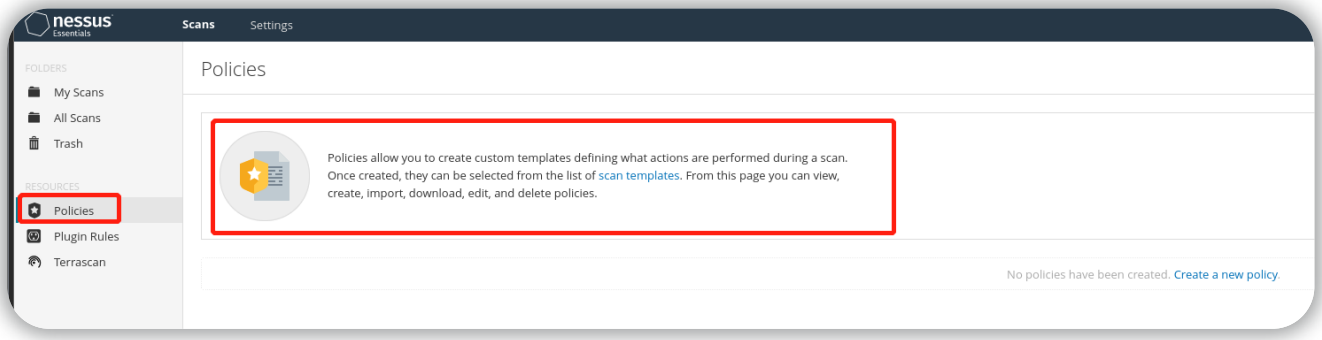
H2 Nessus导航和扫描

点击右上角的"New Scan"按钮，进入到Nessus的导航和扫描界面：

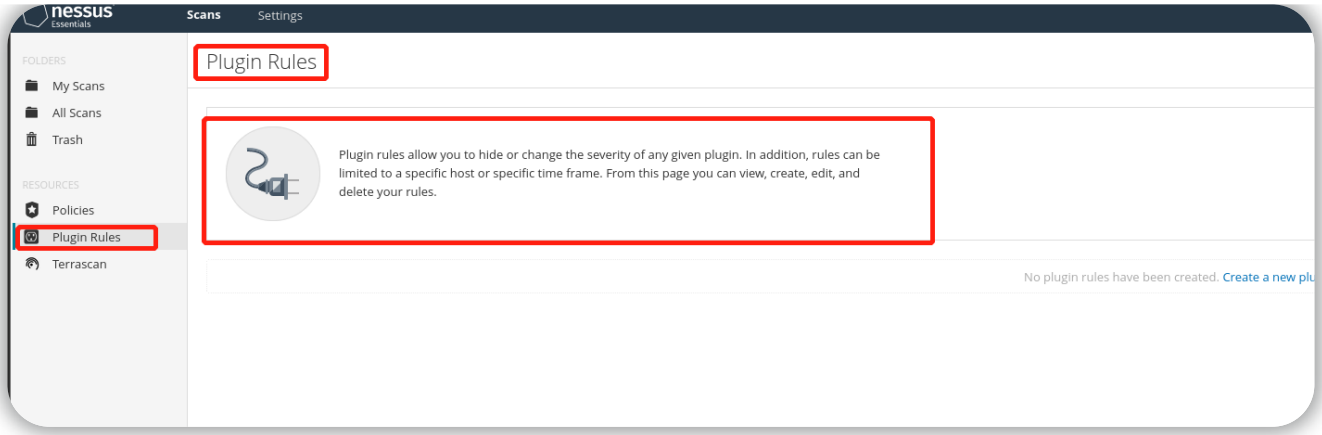




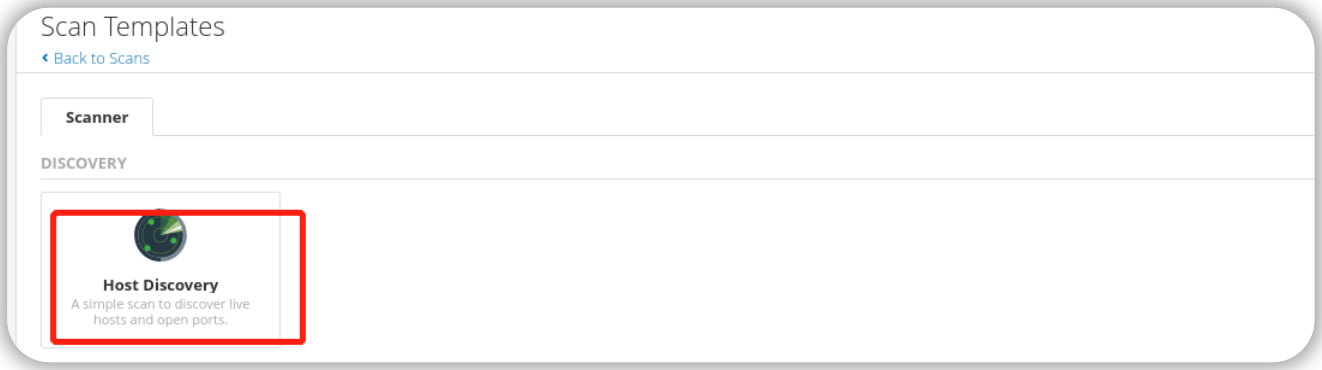
策略页面--允许你创建自定义模板来定义扫描过程中执行的操作。一旦创建好了自定义模版，你就可以从扫描（scan）模板列表中选择它们。从该页面，你可以查看、创建、导入、下载、编辑和删除策略。



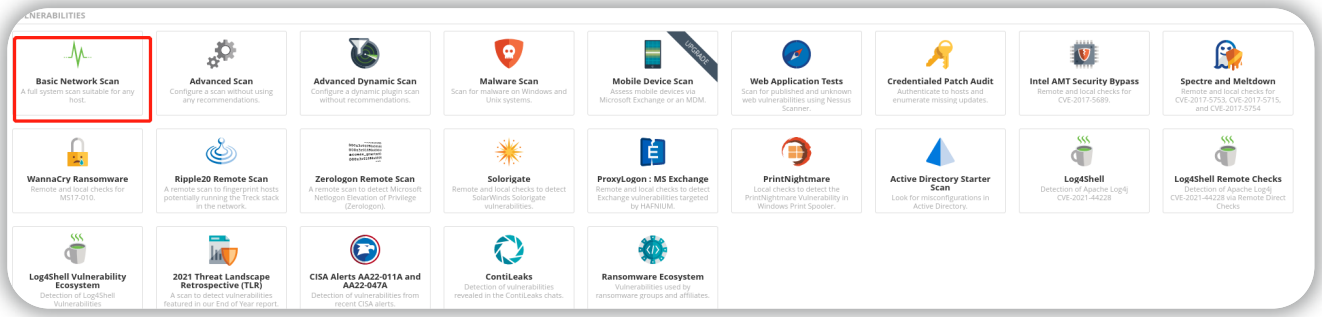
插件规则页面--插件规则允许你隐藏或更改任何给定插件的严重性，此外，规则可以限制在特定的主机或特定的时间范围内。你可以从这个页面查看创建、编辑和删除规则。



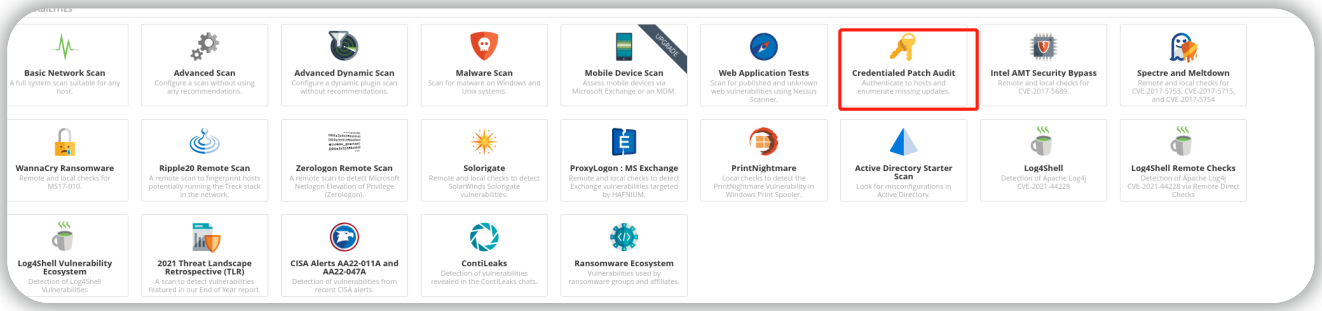
使用NewScan页面的Host Discovery功能，可以让我们简单地看到哪些主机是存活的。



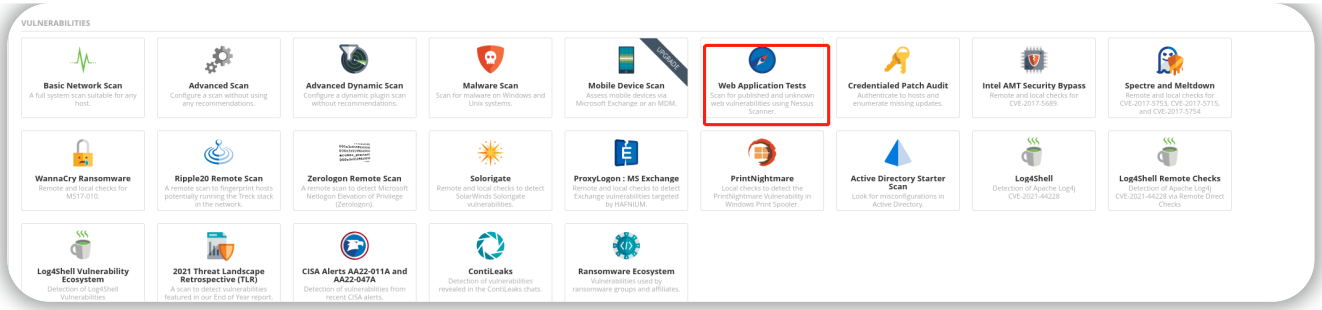
NewScan页面的 Basic Network Scan是最有用的扫描类型之一，被认为“适用于任何主机”：



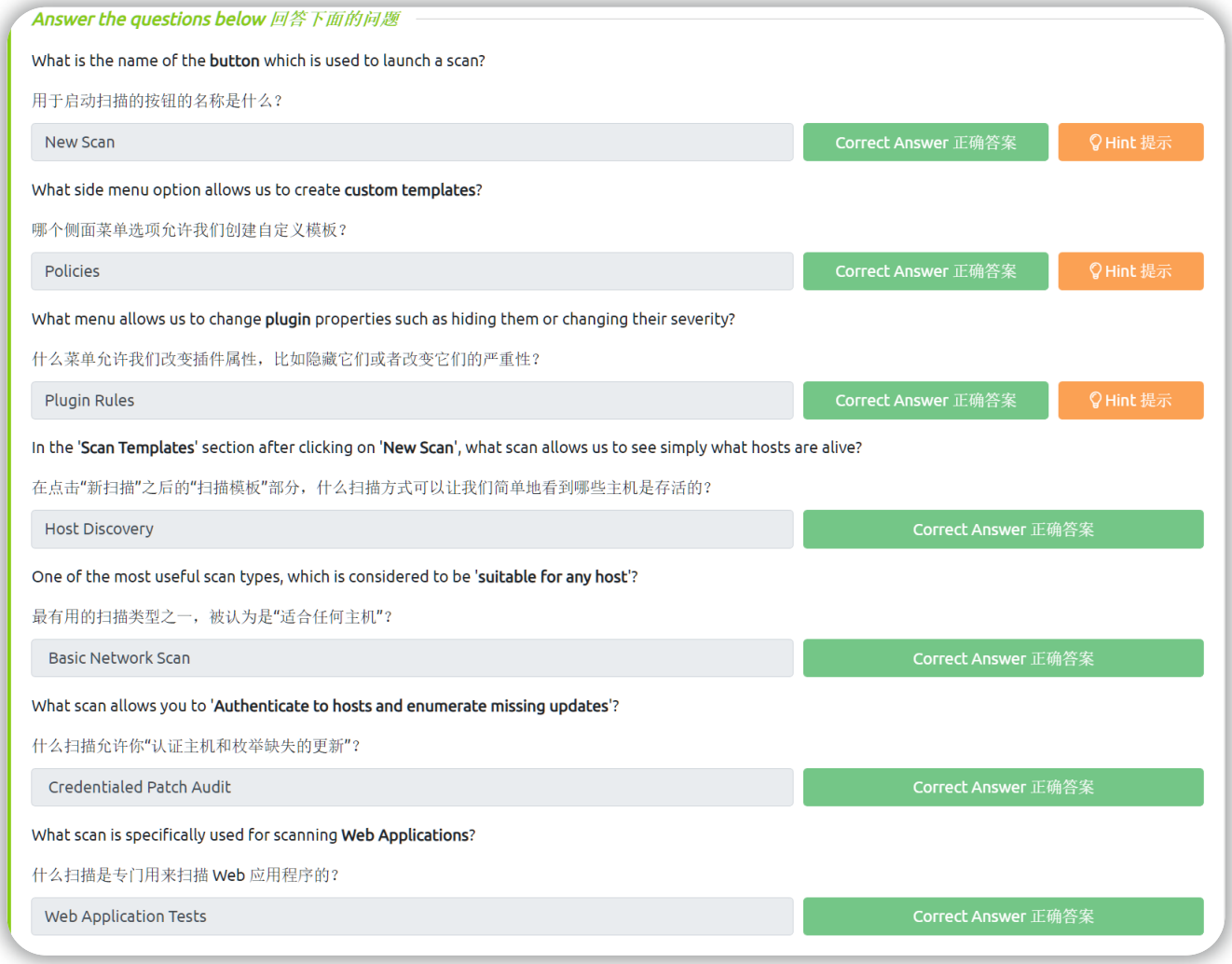
NewScan页面的 Credentialed Patch Audit扫描允许你“向主机验证并枚举缺失的更新”



NewScan页面的Web Application Tests扫描--专门用来扫描 Web 应用程序



答题卡

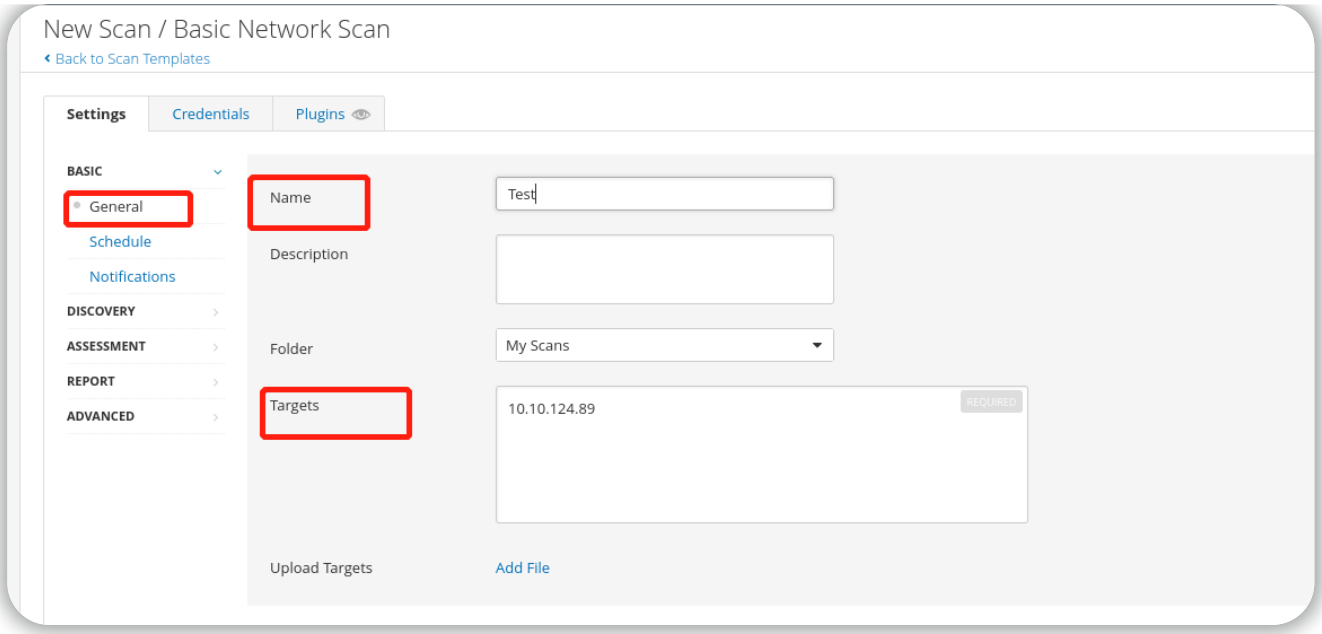


H2 运行网络扫描！

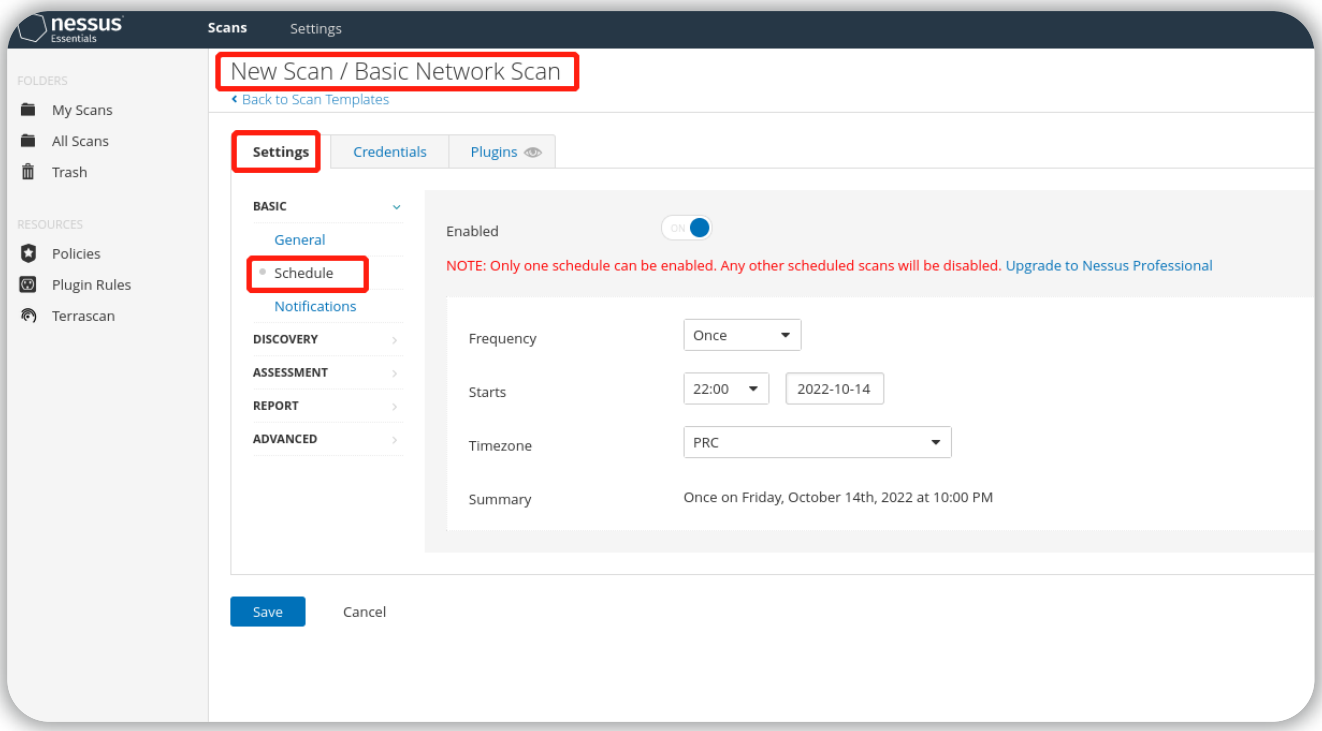
启用靶机并通过Openvpn将kali连接到TryHackMe的靶场内网环境。

本小节将使用Basic Network Scan扫描，开始扫描前先进行选项设置。

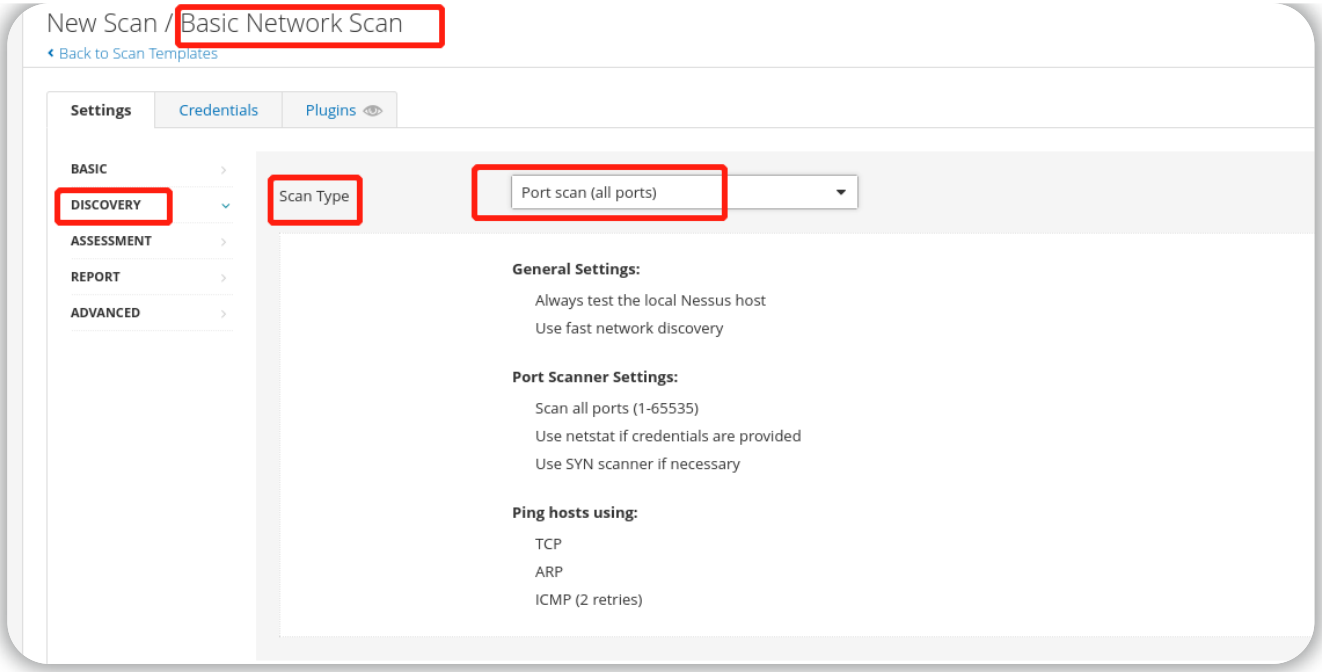
在以下界面设置本次扫描的名称和扫描的目标（New Scan button > Basic Network Scan > Settings > BASIC >General）：



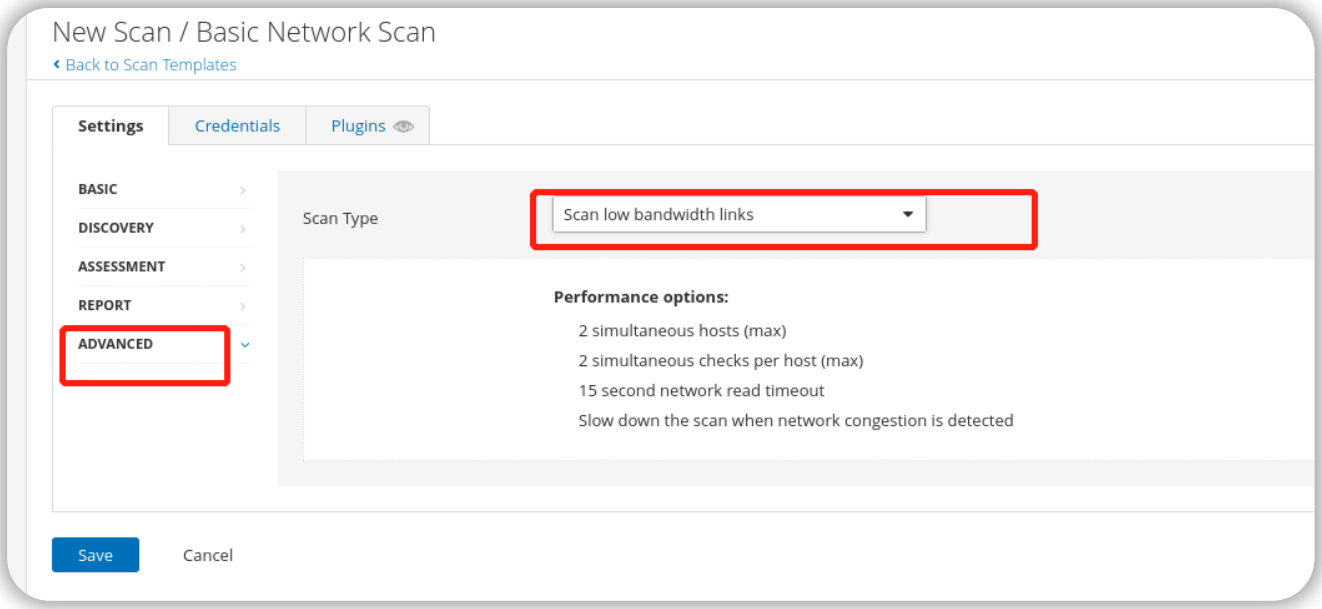
可以设置Schedule选项来设定扫描运行的时间（也可以不设置），选择New Scan button > Basic Network Scan > Settings > BASIC > Schedule：



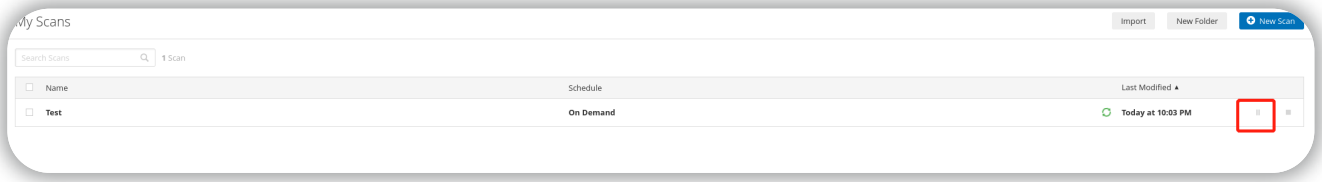
在DISCOVERY里面的扫描类型（Scan Type）中可以选择要扫描的端口，可以设置为全端口扫描、通用端口扫描、自定义端口扫描。



在**ADVANCED**选项下设置扫描类型为Scan low bandwidth links，使用较低的带宽连接进行扫描：

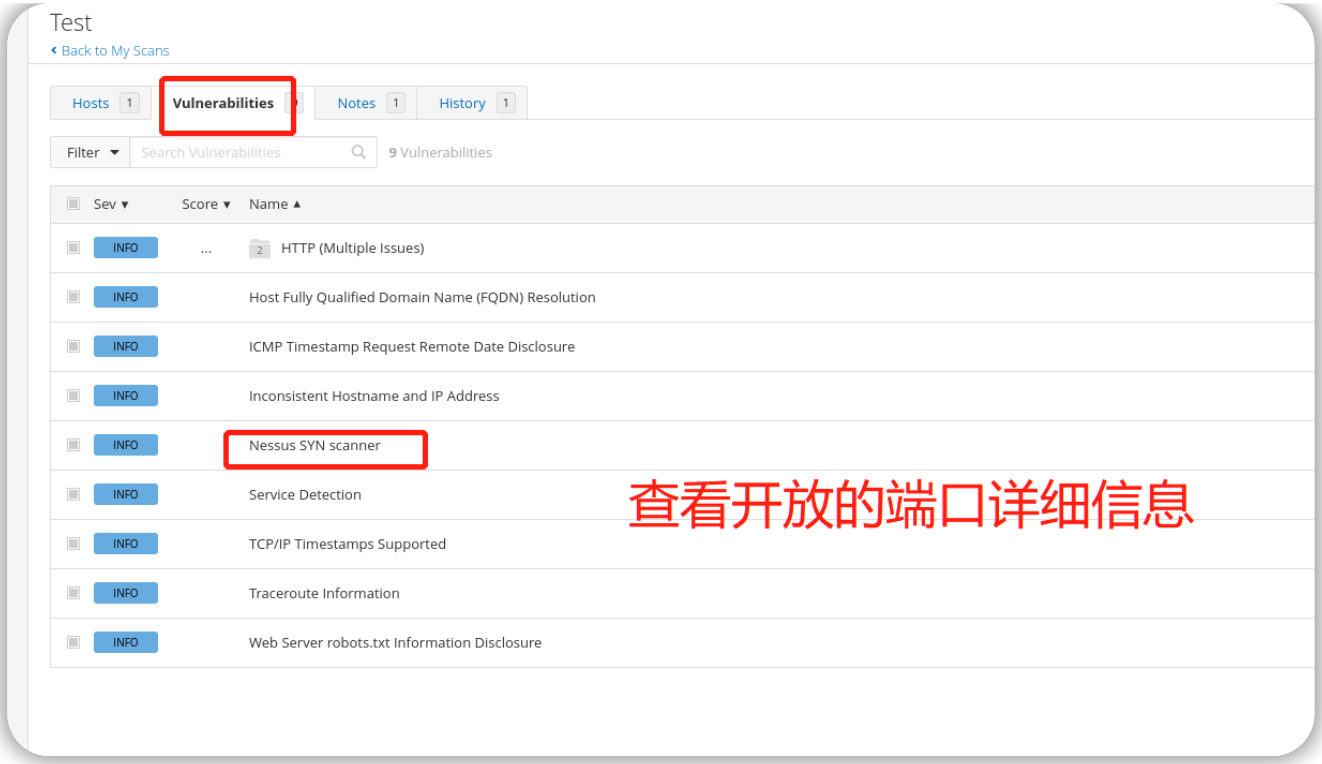


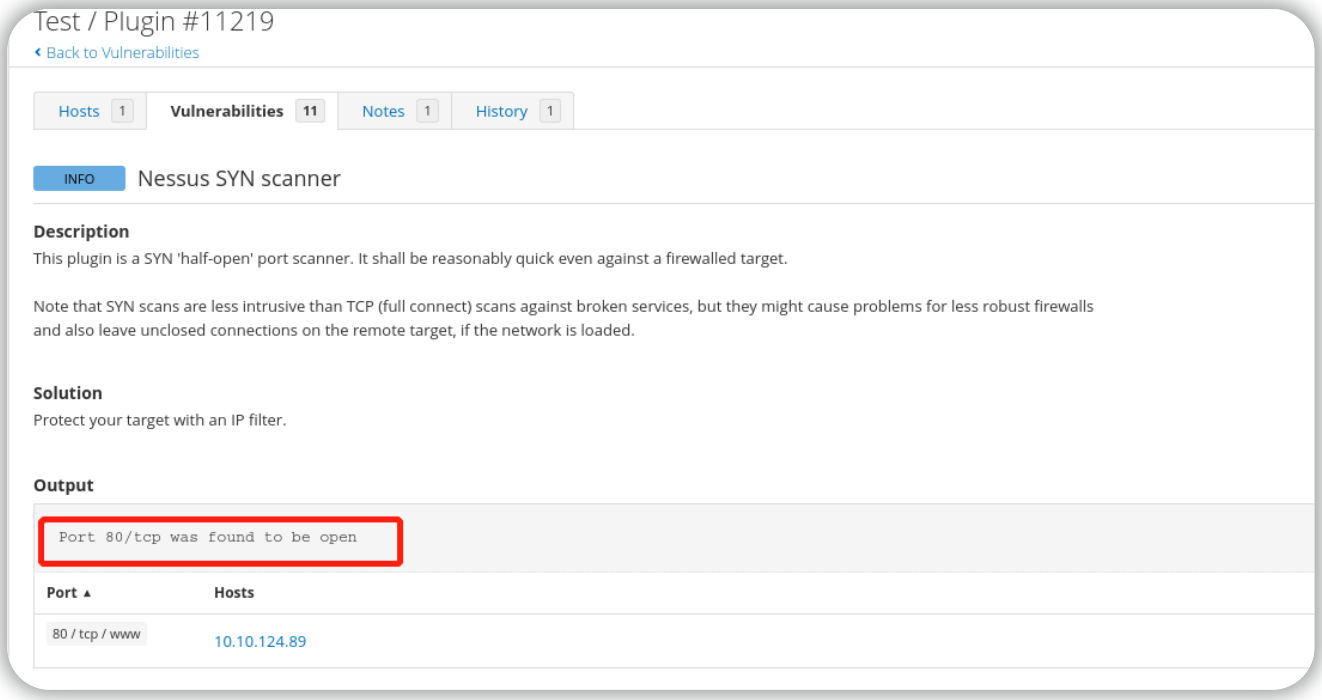
设置完成之后，保存配置并开始扫描：



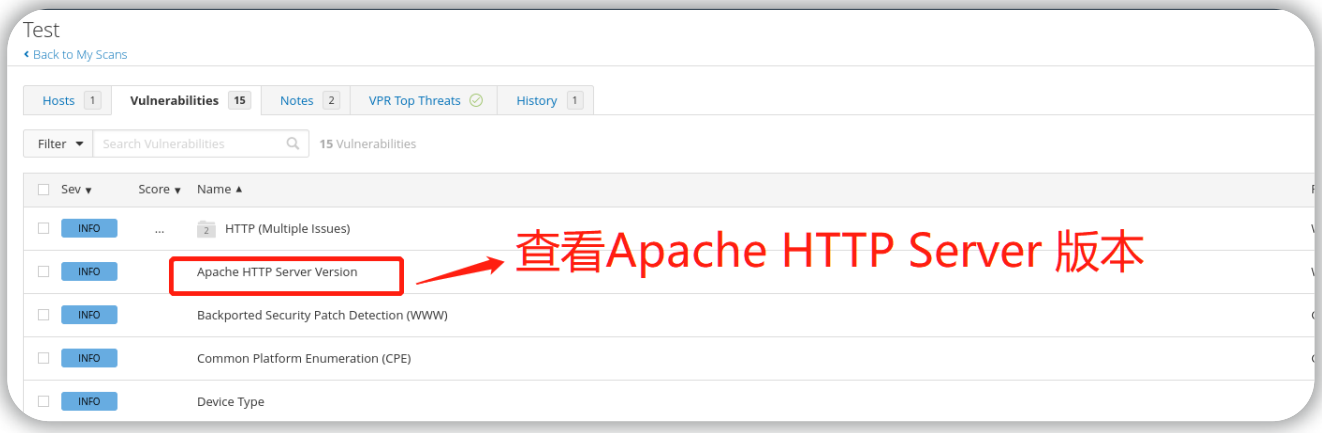
等待扫描完成（可能需要1-5分钟），查看扫描结果即可。

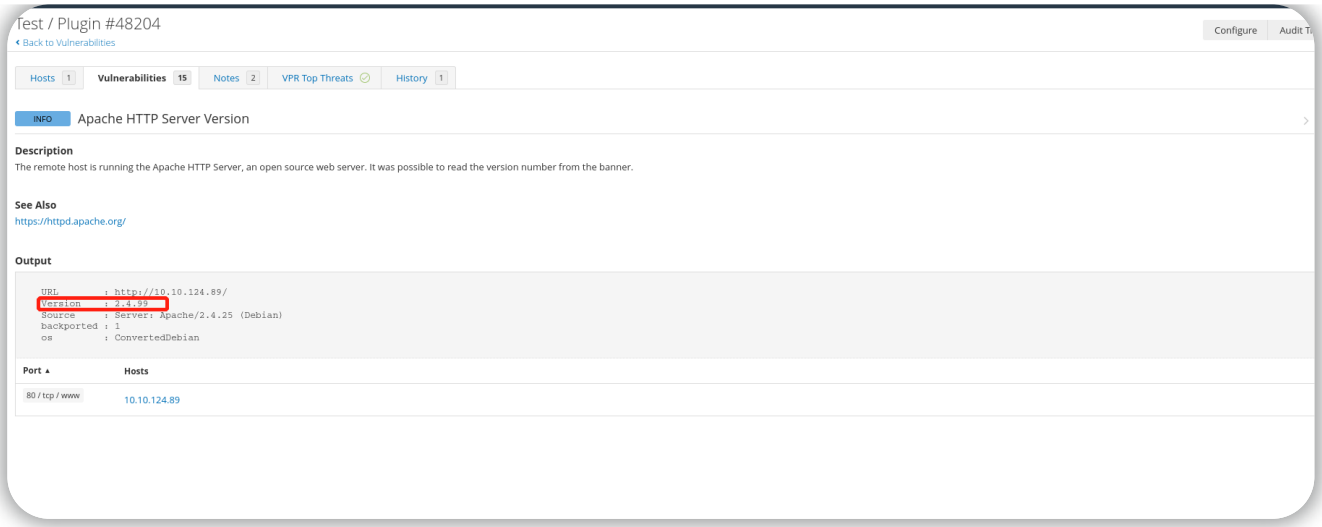
查看开放的端口详细信息：



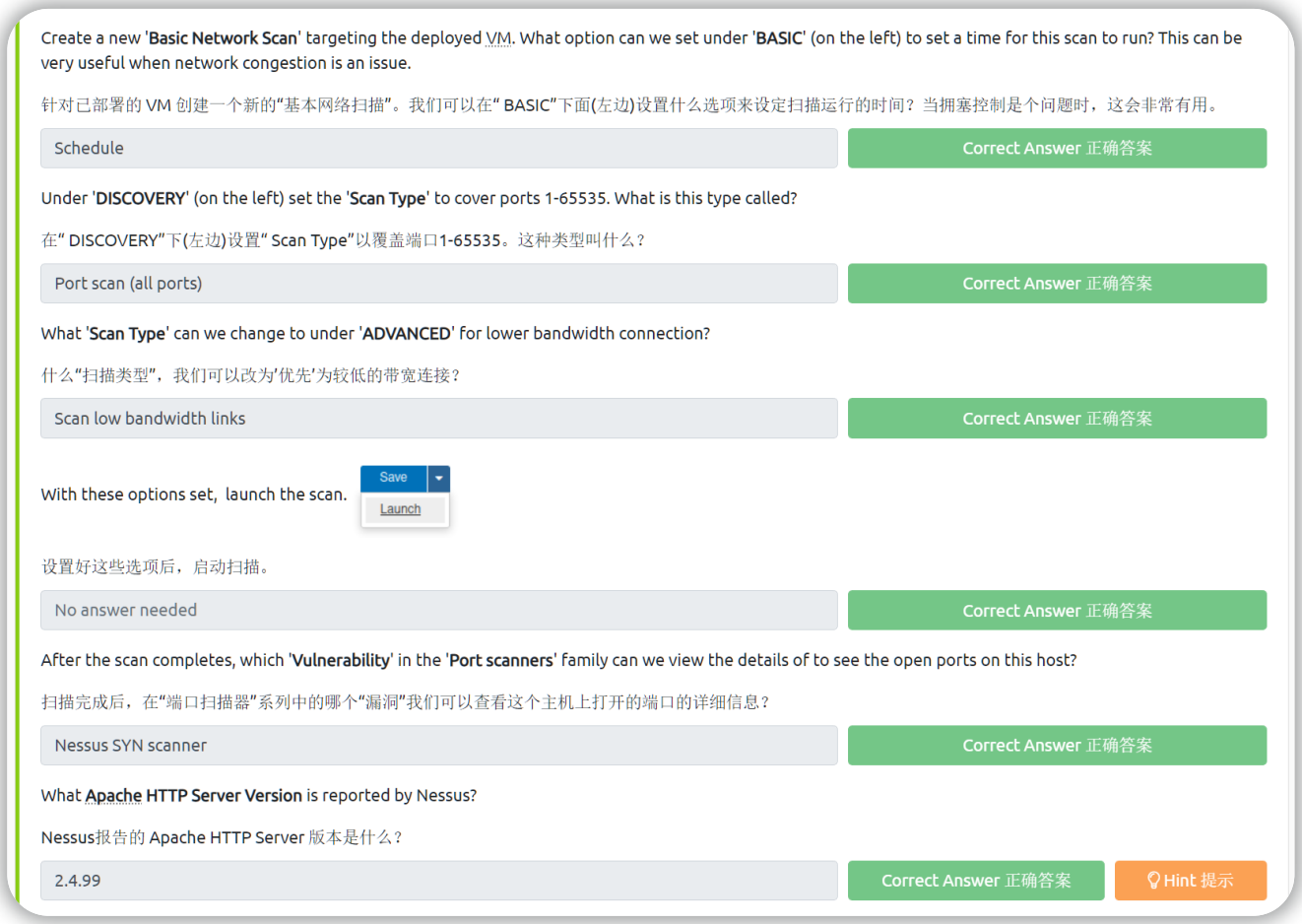


查看Apache HTTP Server 版本：





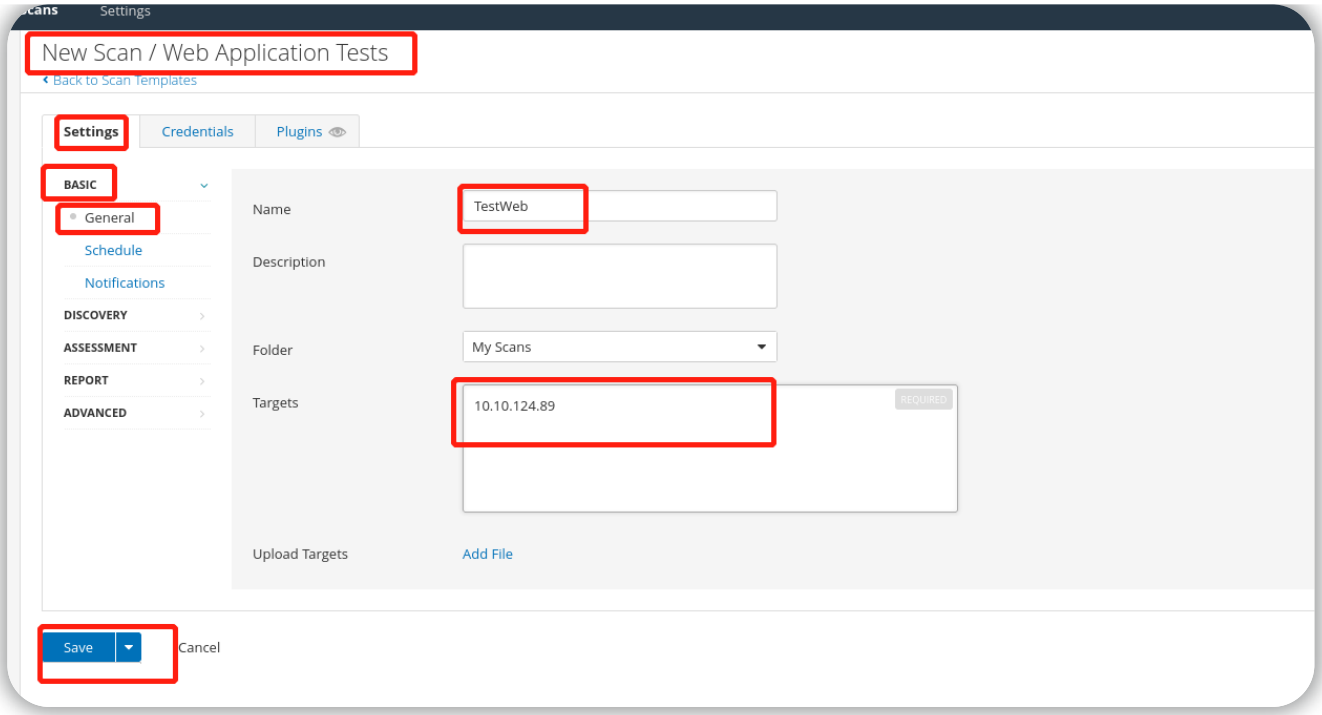
答题卡



H2 运行 **Web** 应用程序扫描！

现在进行web应用程序扫描，运行此扫描将需要一些时间来完成，请耐心等待！！

选择New Scan button > Web Application Tests ，在目标文本字段中输入目标机的ip地址，保存设置并启动扫描，最后等待结果即可

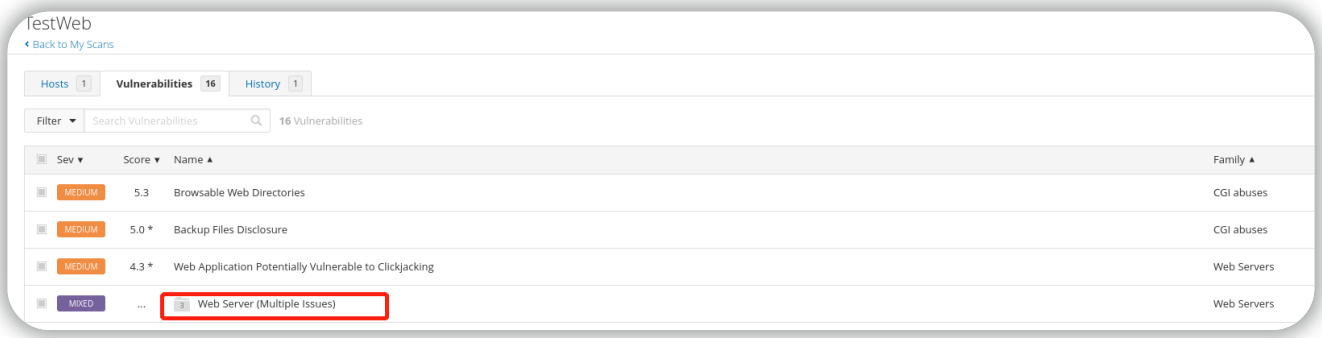


查看扫描结果并回答问题

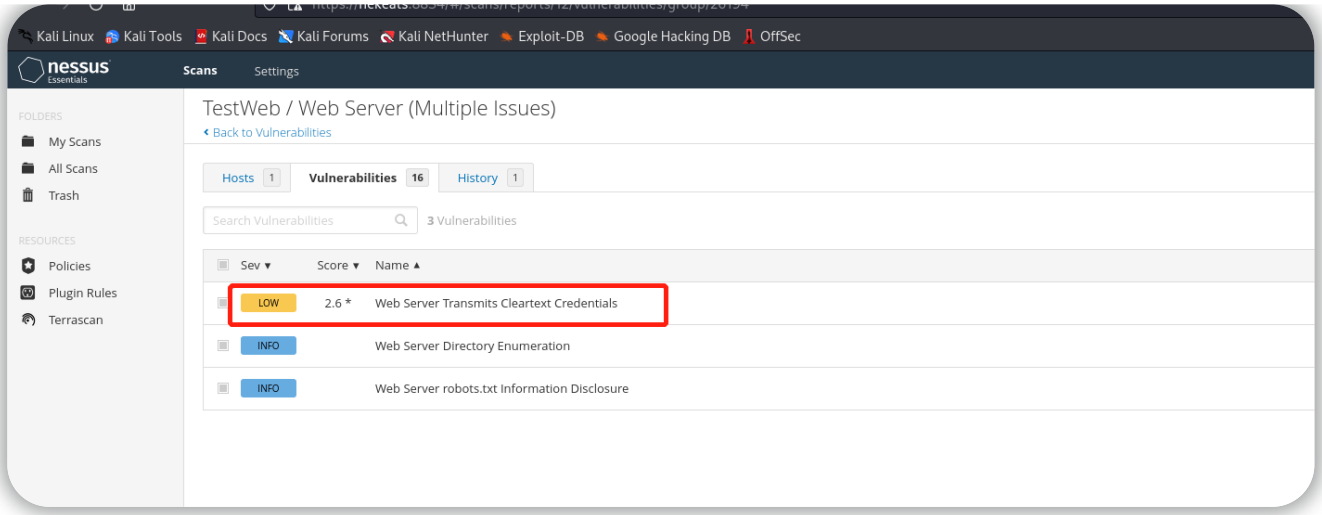
识别"HTTP 服务器类型和版本"的插件的ID 是什么?

扫描器发现了哪个身份验证页面以明文形式传输凭据?

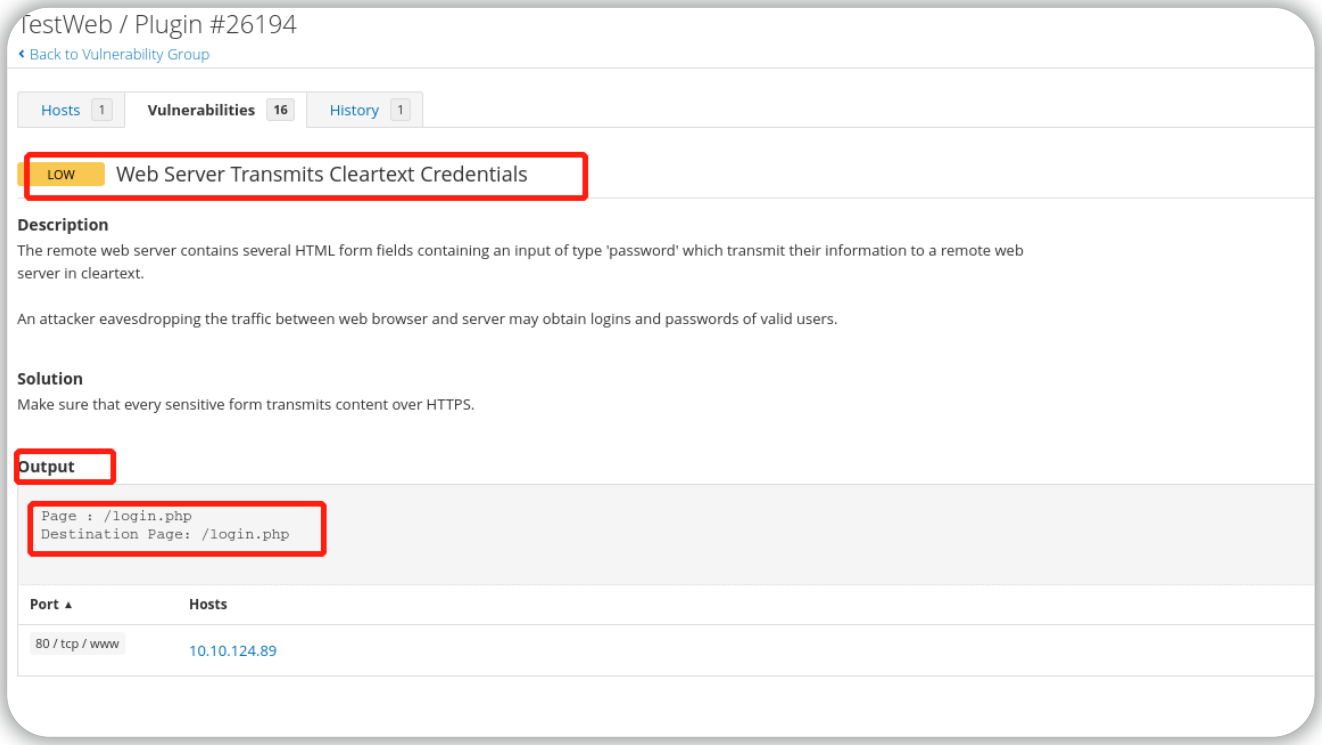
单击行项目"Web 服务器（多个问题）"



然后单击行项目"Web 服务器传输明文凭据"

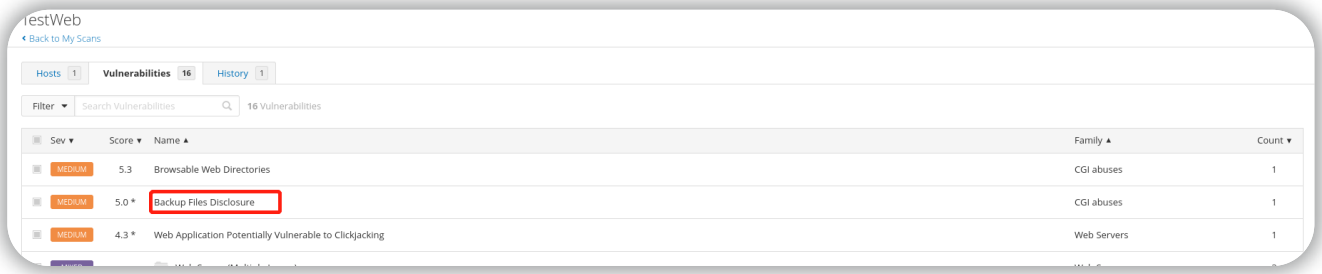


在输出部分下，你将看到传输明文凭据的页面。

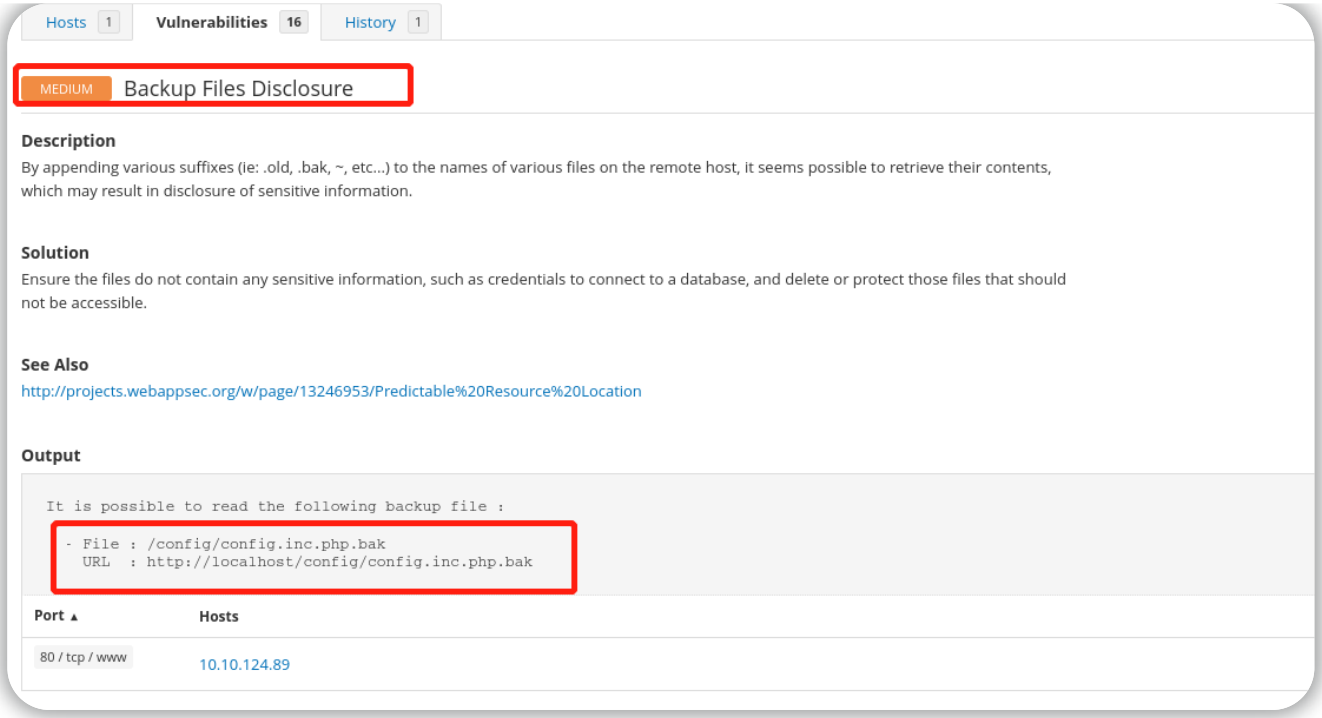


配置备份的文件扩展名是什么?

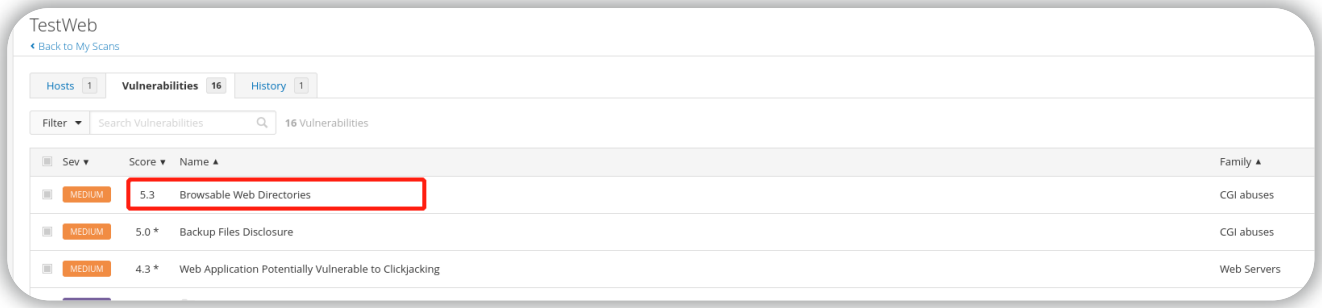
单击“Backup Files Disclosure”漏洞行项。

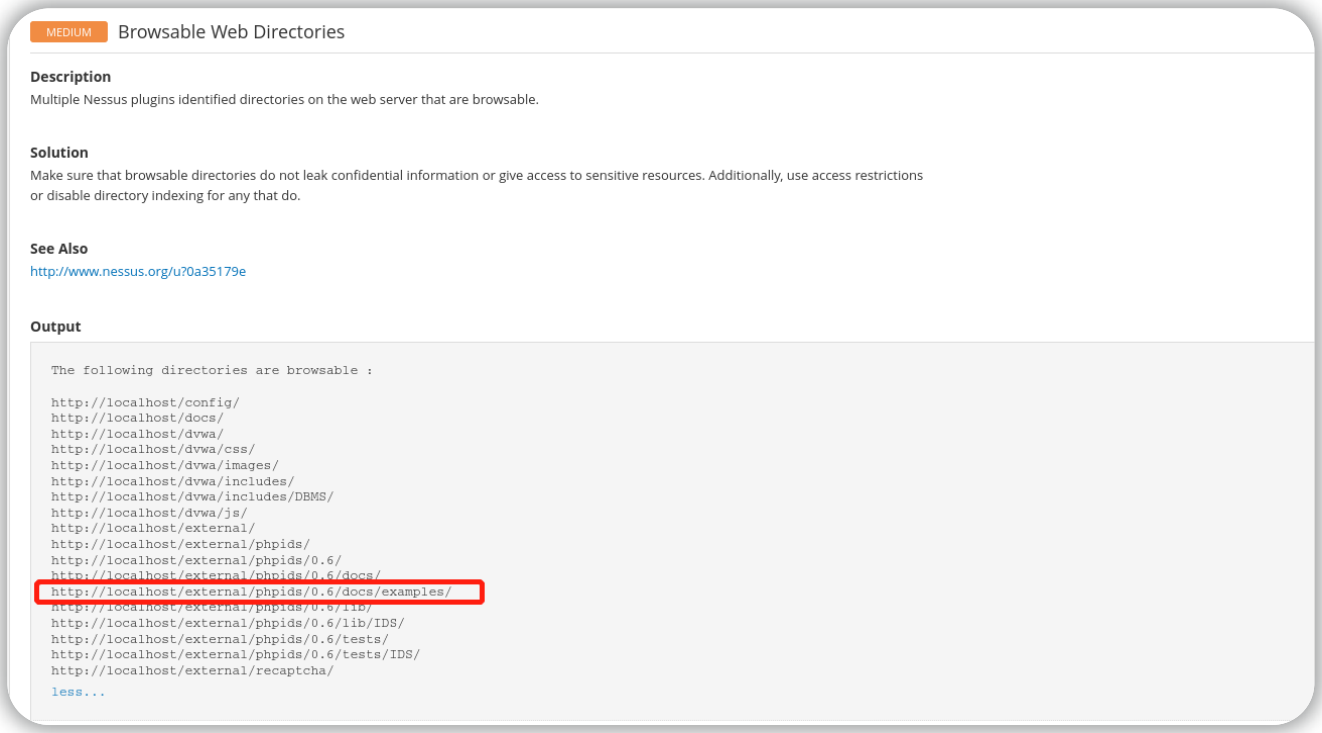


备份文件的扩展名可以在漏洞详细信息的“输出”部分找到：

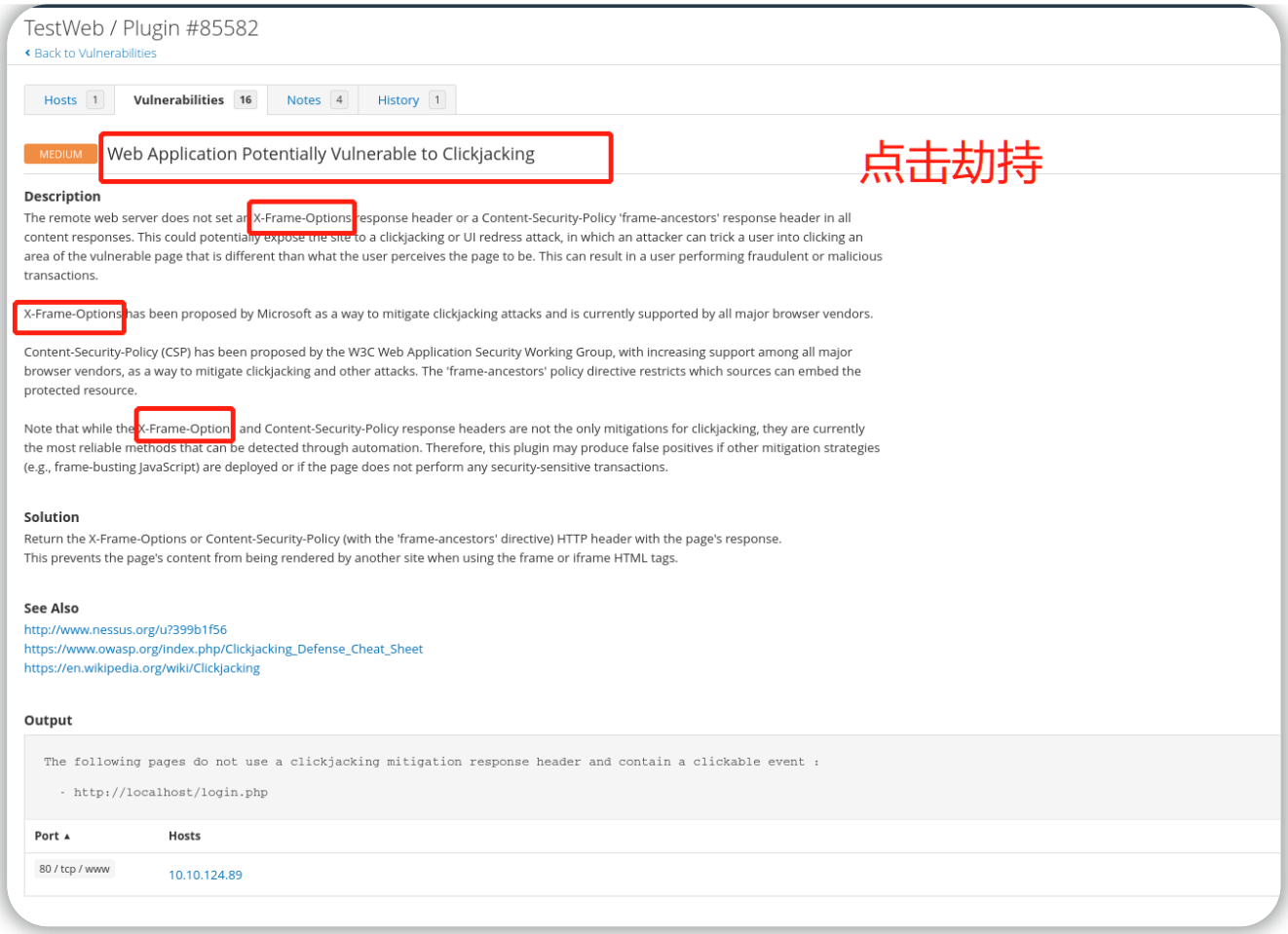


哪个目录包含示例文档？（在 php 目录中）

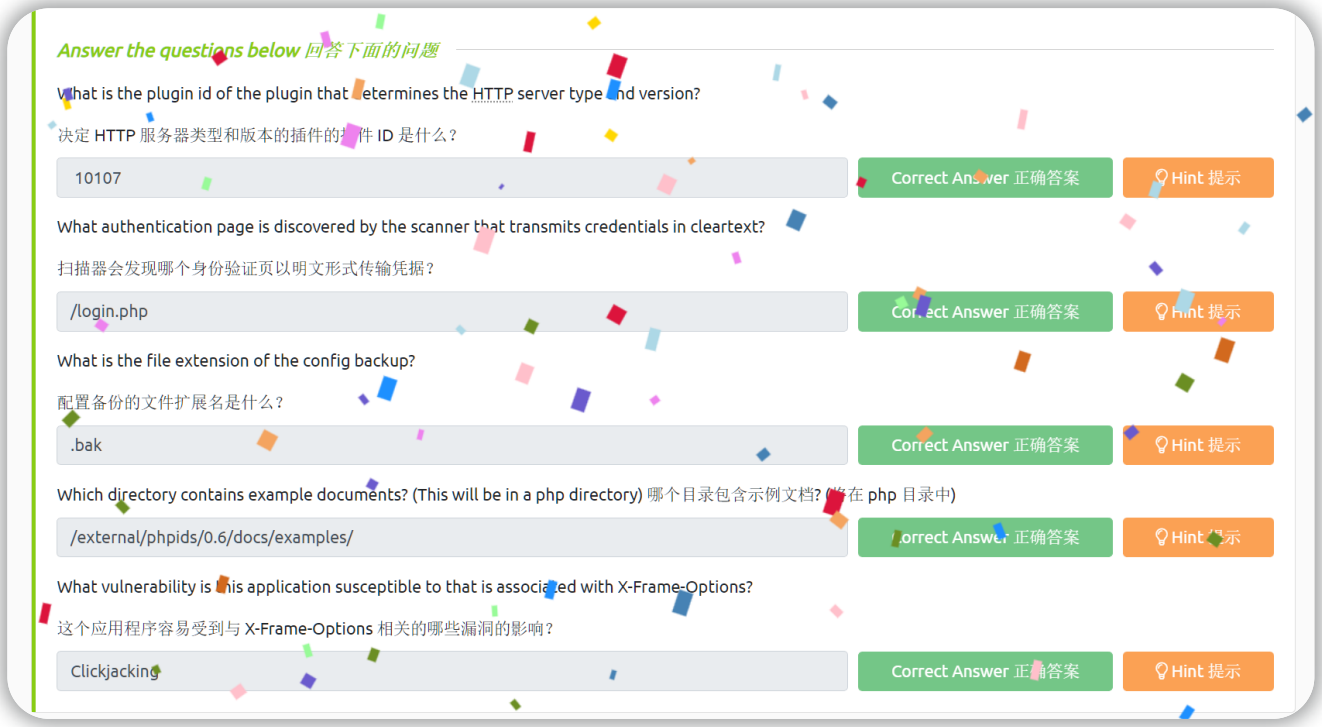




此web应用程序容易受到与 X-Frame-Options 相关联的哪些漏洞的影响?


TestWeb / Plugin #85582
Back to Vulnerabilities
Hosts 1
Vulnerabilities 16
Notes 4
History 1
MEDIUM
Web Application Potentially Vulnerable to Clickjacking
点击劫持
Description
The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.
Solution
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.
See Also
http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking
Output
The following pages do not use a clickjacking mitigation response header and contain a clickable event :
- http://localhost/login.php
Port
Hosts
80 / tcp / www
10.10.124.89

答题卡


Answer the questions below 回答下面的问题
What is the plugin id of the plugin that determines the HTTP server type and version?
决定 HTTP 服务器类型和版本的插件的插件 ID 是什么？
10107
Correct Answer 正确答案
Hint 提示
What authentication page is discovered by the scanner that transmits credentials in cleartext?
扫描器会发现哪个身份验证页以明文形式传输凭据？
/login.php
Correct Answer 正确答案
Hint 提示
What is the file extension of the config backup?
配置备份的文件扩展名是什么？
.bak
Correct Answer 正确答案
Hint 提示
Which directory contains example documents? (This will be in a php directory) 哪个目录包含示例文档？(将在 php 目录中)
/external/phpids/0.6/docs/examples/
Correct Answer 正确答案
Hint 提示
What vulnerability is this application susceptible to that is associated with X-Frame-Options?
这个应用程序容易受到与 X-Frame-Options 相关的哪些漏洞的影响？
Clickjacking
Correct Answer 正确答案
Hint 提示