新时代计算机人才培养系列教材

“互联网+”新形态一体化教材

渗透测试

主编◎林　斌　项尚清　蔡开立

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

新时代计算机人才培养系列教材

“互联网+”新形态一体化教材

渗透测试

主编◎林　斌　项尚清　蔡开立

扫一扫
学习资源库

上海交通大學出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书深入介绍了渗透测试的完整流程，包括渗透测试概论、前期交流、信息收集、漏洞扫描与验证、渗透攻击，以及报告提交与安全加固。书中不仅涵盖丰富的理论知识，还提供了实战案例，帮助读者将所学应用于实际场景。通过学习本书，读者将掌握如何模拟黑客攻击，发现潜在的安全风险，并采取有效措施加固防御。本书将相关法律法规融入课程讲解内容，在每一个渗透测试环节都强调树立正确的网络安全观。本书可作为信息安全等相关专业的教材，也可供信息安全从业人员参考阅读。

图书在版编目（CIP）数据

渗透测试 / 林斌，项尚清，蔡开立主编. -- 上海 : 上海交通大学出版社，2024.7 -- ISBN 978-7-313-28077-0

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 2024M1C618 号

渗透测试

SHENTOU CESHI

主　　编：林　斌　项尚清　蔡开立　　**地　　址**：上海市番禺路 951 号

出版发行：上海交通大学出版社　　**电　　话**：021-6407 1208

邮政编码：200030

印　　制：北京荣玉印刷有限公司　　**经　　销**：全国新华书店

开　　本：889mm × 1194mm　1/16　　**印　　张**：10.5

字　　数：268 千字

版　　次：2024 年 7 月第 1 版　　**印　　次**：2024 年 7 月第 1 次印刷

书　　号：ISBN 978-7-313-28077-0

定　　价：45.00 元

前言

在数字化转型的时代背景下，信息安全已成为企业乃至国家安全的重要保障。我国政府将信息安全与政治安全、经济安全、文化安全等放在同等重要的位置，强调信息安全是国家安全的重要组成部分。渗透测试作为信息安全领域中的重要一环，对于发现并解决潜在的信息安全风险起着至关重要的作用。

编写本书是为了满足社会对高素质信息安全人才的需求，旨在帮助学生掌握全面的渗透测试知识和技能。全书注重理论与实践相结合，通过丰富的案例和实战演练帮助学生加深理解、增强记忆，同时注重将课程思政融入其中，引导学生树立正确的网络安全观，培养良好的职业道德素养。本书还融入了党的二十大关于网络强国、数字中国建设的内容，引导学生认识到在信息安全领域肩负的时代使命，坚定“四个自信”，为新时代的信息安全贡献力量。

本书内容主要包括渗透测试概论、前期交流、信息收集、漏洞扫描与验证、渗透攻击、报告提交与安全加固等模块，涵盖了渗透测试的完整流程。通过学习本书，学生能够了解黑客攻击的手段和方法，发现潜在的信息安全风险，并采取有效措施加固系统防御。

本书适用于信息安全相关专业的学生以及从事信息安全工作的人员。

渗透测试作为一种重要的网络安全评估手段，对于保障信息系统的安全稳定运行具有重要意义，希望本书能够为你的信息安全学习之旅助力！

目录

项目三

信息收集 …… 25

项目四

漏洞扫描与验证 …… 45

项目五

渗透攻击 …… 81

项目六

报告提交 …… 101

项目七

安全加固 …… 111

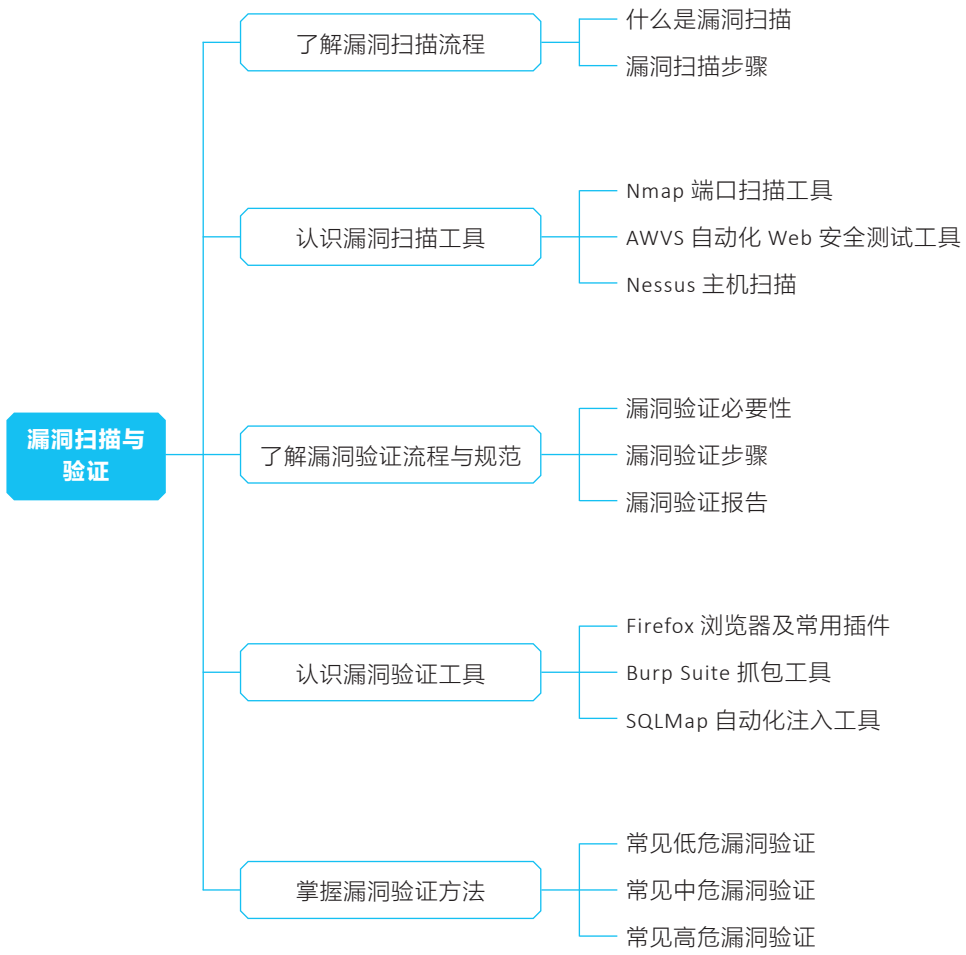
项目四
漏洞扫描与验证

项目导读

进行前期交流和信息收集后，接下来要对客户授权目标进行漏洞扫描和验证。使用工具进行漏洞扫描能够快速发现当前网站存在的漏洞，但存在一定的误报率，因此需要对已发现的漏洞进行验证，可以使用手动方式或其他方式。

本项目主要围绕漏洞扫描的原理及工具使用、漏洞验证流程、漏洞验证方法进行讲解。通过本项目的讲解，读者应对漏洞扫描与验证有整体的认识，能够自主完成对 Web 网站应用的漏洞扫描与验证。

课程导航



学习目标

知识目标

（1）了解漏洞验证的流程及规范、漏洞的风险评级方式。

（2）熟悉漏洞验证的原理。

（3）掌握漏洞手动验证的方法及相关工具的使用。

能力目标

能够使用相关方法和工具验证漏洞。

素质目标

激发对漏洞验证知识的兴趣，了解漏洞的危害，掌握漏洞验证的相关知识，提升网络素养。

任务一 了解漏洞扫描流程

一、什么是漏洞扫描

漏洞扫描是基于现有的漏洞数据库，通过集成化工具及其他手段对客户指定的测试目标进行以发现漏洞为目的的安全性检测，为后续渗透测试的开展提供依据。

二、漏洞扫描步骤

基于与客户进行前期交流和信息收集的结果，对客户的网络目标地址进行 TCP/UDP 端口扫描，确定其所开放的服务的数量和类型。通过端口扫描，可以基本确定一个系统的基本信息，并根据这些信息进行有关网站和主机系统的漏洞扫描。

任务二 认识漏洞扫描工具

一、Nmap 端口扫描工具

Nmap 是安全渗透领域最强大的开源端口扫描器，用来扫描网上计算机开放的网络连接端，确定哪些服务运行在哪些连接端，并且推断计算机运行的操作系统，以及用以评估网络系统安全程度。该工具支持跨平台运行。

Kali 操作系统默认已安装好 Nmap 软件，本书不再介绍该软件的安装步骤。

1. Nmap 常见的扫描类型和扫描选项

Nmap 常见扫描类型如表 4-1 所示。Nmap 常见扫描选项如表 4-2 所示。

表 4-1 Nmap 常见扫描类型

类型	名称	功能描述
-sS	TCP SYN 扫描	与目标主机建立 TCP 连接，该方式属于半开放扫描，具有隐蔽性
-sT	TCP 扫描	与目标主机建立 TCP 连接，该方式会留下痕迹
-sP	Ping 扫描	通过 ICMP 报文发送进行主机扫描
-sA	ACK 扫描	检测目标主机端口开放状态
-sW	TCP 窗口扫描	检测 RST 包的 TCP 窗口值，由此判断端口是否开放
-sM	Maimon 扫描	探测报文是 FIN/ACK，无论端口开放还是关闭，都响应 RST 报文

续表

类型	名称	功能描述
-sU	UDP 扫描	通过建立 UDP 连接，检测对方的 UDP 端口开放状态
-sN/sF/sX	TPC Null/FIN/Xmas 扫描	使用 TCP Null/FIN/Xmas 秘密扫描方式协助探测对方 TCP 端口状态
-sL	列表扫描	扫描列出 IP 地址的主机
-sI	闲置扫描	通过闲置的主机帮助扫描（前提是要找到“僵尸”主机）
-sY/sZ	SCTP INIT/COOKIE-ECHO 扫描	扫描使用 SCTP 协议的端口的开放状况
-sO	IP 协议扫描	扫描使用 IP 协议的主机

表 4-2　Nmap 常见扫描选项

选项	名称	功能描述
-A	综合扫描	启动多种扫描选项，如版本扫描和脚本扫描等
-T（0 ～ 5）	多任务扫描	可以开启多个线程扫描，提高速度
-sV	服务版本扫描	探测服务软件的版本
-S	源 IP 地址	探测伪造的源 IP 地址
-g	源端口号	指定特定的端口发送数据包
-p	端口范围	扫描指定的端口范围
--script	脚本扫描	使用指定的脚本进行扫描

2. Nmap 常用扫描方式

1）基本扫描

（1）这是 Nmap 的默认扫描方式。

```
nmap 192.168.1.102
```

扫描结果如图 4-1 所示。

实训视频

Nmap 实训

```
┌──(root💀kali)-[~]
└─# nmap 192.168.1.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-04 17:38 CST
Nmap scan report for 192.168.1.102
Host is up (0.0013s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 28:11:A8:85:7D:CA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```

图 4-1　Nmap 基本扫描结果

（2）扫描多个目标地址，可以利用增加空格的方式，将多个地址隔开。

```
nmap 192.168.1.102 192.168.1.103
```

（3）扫描一个连续的网段，可以利用”-”符号连接。

```
nmap 192.168.1.100-150
```

（4）扫描某文件中列出的所有目标地址。如某文件名为 ip.txt，内容如图 4-2 所示。

图 4-2 ip.txt 内容

可以通过 -iL 参数，引入该文件并扫描。

```
nmap -iL /home/carl/ip.txt
```

结果如图 4-3 所示。

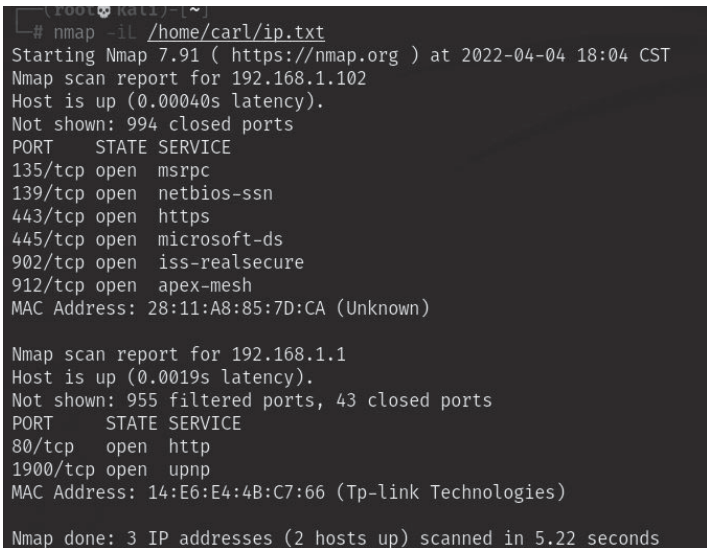


图 4-3 引入文件扫描结果

2）目标主机 C 段扫描

```
nmap -sn 192.168.1.0/24
```

该方法可以扫描指定主机段内所有存活的主机，结果如图 4-4 所示。

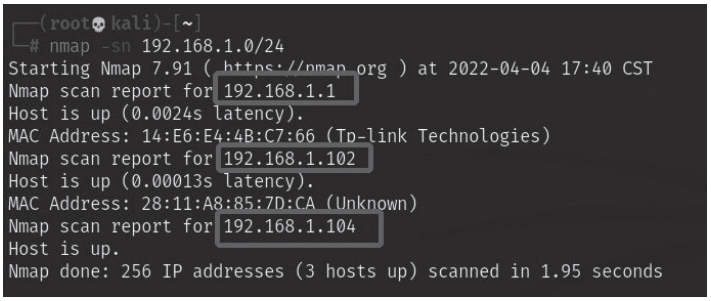


图 4-4 主机 C 段扫描结果

3）端口扫描

```
nmap -sS -p 1-20000 192.168.1.102
```

该方法能够扫描指定主机开放的端口，其中 -p 指定要扫描端口号的范围，端口扫描结果如图 4-5 所示。

```
┌──(root💀kali)-[~]
└─# nmap -sS -p 1-20000 192.168.1.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-04 17:42 CST
Nmap scan report for 192.168.1.102
Host is up (0.00058s latency).
Not shown: 19992 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5040/tcp open  unknown
7250/tcp open  unknown
MAC Address: 28:11:A8:85:7D:CA (Unknown)
```

图 4-5　端口扫描结果

除此之外，Nmap 软件指可以通过设置 -p 参数和“,”的方式指定端口。

例如，扫描目标主机的 21、22、80、443、445 端口是否开放。

```
nmap 192.168.1.102 -p 21，22，80，443，445
```

4）系统扫描

```
nmap -O 192.168.1.102
```

该方法能够通过指纹识别技术识别目标主机使用的操作系统版本，结果如图 4-6 所示。

```
┌──(root💀kali)-[~]
└─# nmap -O 192.168.1.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-04 17:44 CST
Nmap scan report for 192.168.1.102
Host is up (0.00039s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 28:11:A8:85:7D:CA (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/4%OT=135%CT=1%CU=32820%PV=Y%DS=1%DC=D%G=Y%M=2811A8%T
OS:M=624ABDFD%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=106%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=40%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=Z)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.77 seconds
```

图 4-6　系统扫描结果

5）服务版本扫描

```
nmap -sV 192.168.1.102
```

该方法能够探测目标主机使用的应用软件和操作系统，结果如图 4-7 所示。

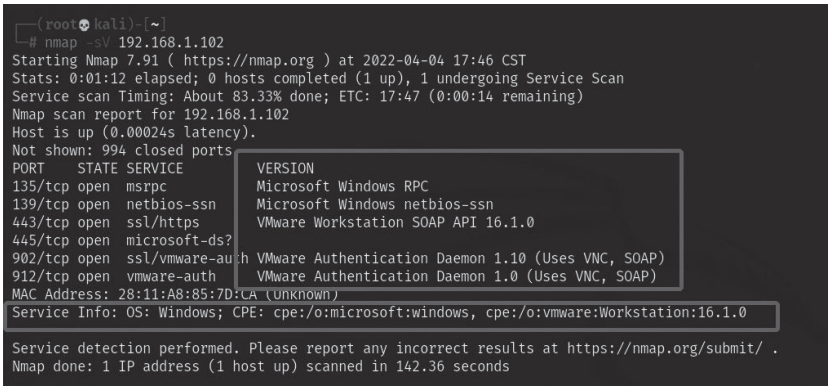


图 4-7　服务版本扫描结果

6）综合扫描

```
nmap -A 192.168.1.102
```

该方法会启动许多扫描选项，如版本扫描和脚本扫描，结果如图 4-8 所示。

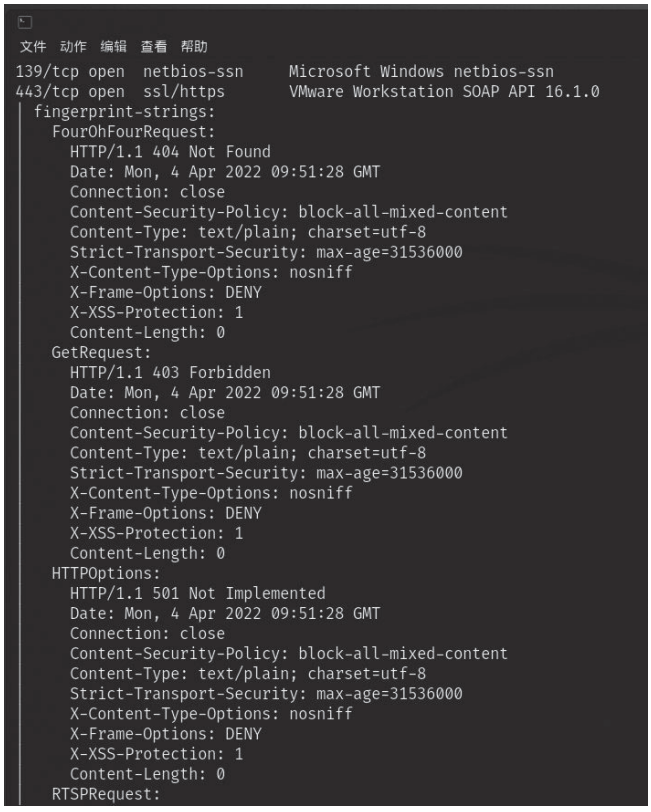


图 4-8　综合扫描结果

7）脚本扫描

利用 Nmap 内置的脚本进行扫描，格式为：

```
nmap --script= 脚本名 主机 ip 地址
```

下面介绍 Nmap 扫描中常用的脚本。

（1）default：使用 -sC 或 -A 选项扫描时默认的脚本，提供基本的脚本扫描能力。

（2）auth：负责处理鉴权证书（绕开鉴权）的脚本。

（3）brute：针对常见的应用提供暴力破解方式，如 HTTP、SNMP（简单网络管理协议）等。

（4）broadcast：在局域网内探查更多服务的开启状况，如 DHCP（动态主机配置协议）、DNS、SQL Server 等服务。

（5）vuln：负责检查目标主机是否有常见的漏洞。

（6）smb-brute.nse：负责对目标主机进行 smb 服务破解。

二、AWVS 自动化 Web 安全测试工具

Acunetix Web Vulnerability Scanner（简称 AWVS）是一款 Web 网络漏洞扫描工具。它通过网络爬虫测试网站的安全状况，检测流行的安全漏洞。官方网站上可免费下载的是试用 14 天的版本。

1. AWVS 功能特点

AWVS 包含以下多种创新功能。

（1）AcuSensor 技术。

（2）自动的客户端脚本分析器，允许对 AJAX（asynchronous JavaScript and XML，异步 JavaScript 和 XML）和 Web 2.0 应用程序进行安全性测试。

（3）先进且深入的 SQL 注入和跨站脚本测试。

（4）高级渗透测试工具，如 HTTP Editor 和 HTTP Fuzzer。

（5）可视化宏记录器帮助用户轻松测试 Web 表格和受密码保护的区域。

（6）支持含有 capthca 的页面，支持单个开始指令和 Two-factor（双因素）验证机制。

（7）丰富的报告功能，包括 VISA PCI 依从性报告。

（8）高速的多线程扫描器轻松检索成千上万个页面。

（9）智能爬行程序检测 Web 服务器类型和应用程序语言。

（10）Acunetix 检索并分析网站，包括 flash 内容、SOAP（简单对象访问协议）和 AJAX 端口，扫描 Web 服务器并对在服务器上运行的网络服务进行安全检查。

2. 安装流程

（1）以 acunetix_13.0 为例。下载 Windows 版本并双击打开 acunetix_13.0 安装包后，单击“Next”按钮。

（2）勾选“I accept the agreement”多选框后，单击“Next”按钮。

（3）在“Email”“Password”和“Confirm password”中填写邮箱和密码（见图 4-9，密码要求包含大小写字母、数字和特殊字符）后，单击“Next”按钮。记住填写的邮箱和密码，后续需要用该信息登录。

（4）在“Server Port”编辑框内输入需设置的端口号，默认填 3443，如无需修改则单击“Next”按钮，如图 4-10 所示。

（5）勾选“Create a desktop shortcut”多选框，单击“Next”按钮。

（6）安装前软件弹出警告窗口，安装 CA 证书，请单击“是”按钮，如图 4-11 所示。

（7）安装完毕，单击“Finish”按钮，如图 4-12 所示。

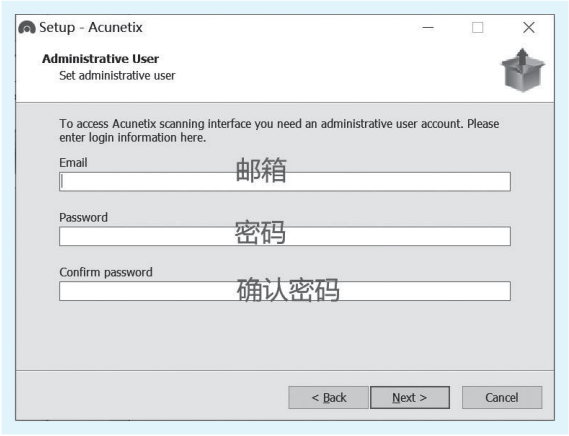


图 4-9　填写邮箱和密码

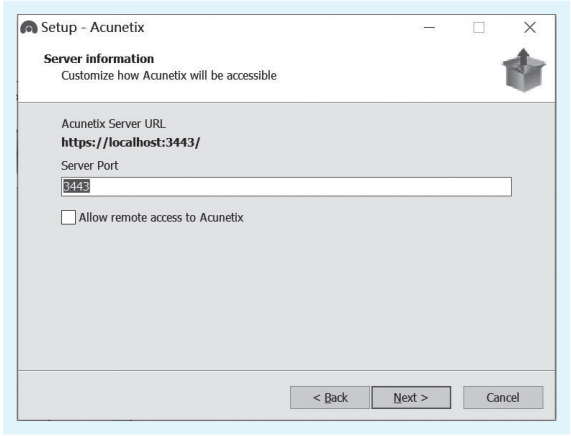


图 4-10　AWVS 监听端口设置

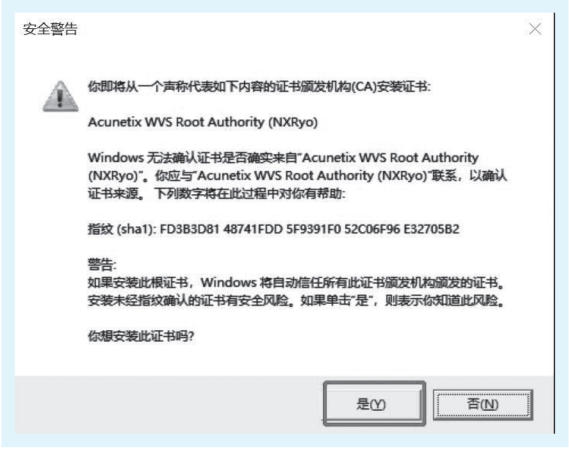


图 4-11　CA 证书安装

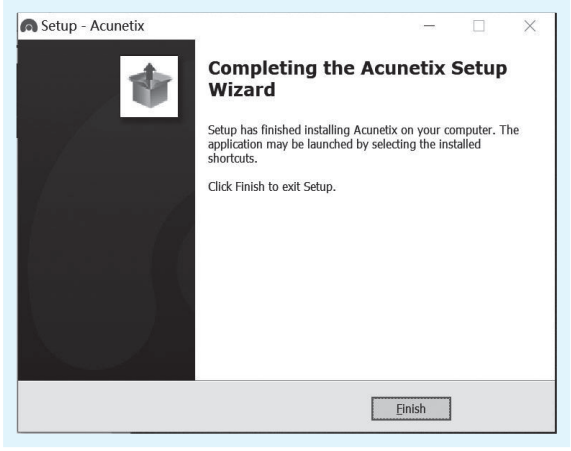


图 4-12　安装完成

（8）打开浏览器，在浏览器地址栏输入 https://localhost:3443/#/login 后，按 Enter 键，如图 4-13 所示。

（9）输入刚才填写的邮箱和密码后，单击“Login”按钮，进入 AWVS 操作界面，如图 4-14 所示。

图 4-13　AWVS 登录界面

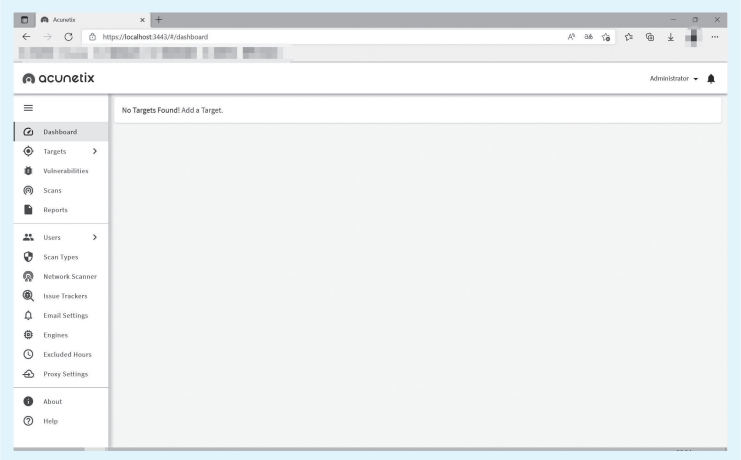


图 4-14　AWVS 操作界面

3. AWVS 菜单功能

1）主菜单

主菜单共有 5 个模块，分别为 Dashboard、Targets、Vulnerabilities、Scans 和 Reports。

（1）Dashboard：仪表盘，显示扫描过的网站的漏洞信息。

（2）Targets：目标网站，需要被扫描的网站。

（3）Vulnerabilities：漏洞，显示所有被扫描出来的网站漏洞。

（4）Scans：扫描目标站点，从 Targets 里面选择目标站点进行扫描。

（5）Reports：漏洞扫描完成后生成的报告。

2）设置菜单

设置菜单共有 8 个模块，分别为 Users、Scan Types、Network Scanner、Issue Trackers、Email Settings、Engines、Excluded Hours、Proxy Settings。

（1）Users：添加网站的使用者，新增用户身份验证、用户登录会话和锁定设置。

（2）Scan Types：可根据需要勾选完全扫描、高风险漏洞、跨站点脚本漏洞、SQL 注入漏洞、弱密码、仅爬网、恶意软件扫描等选项。

（3）Network Scanner：网络扫描仪，配置网络信息，包括地址、用户名、密码、端口、协议。

（4）Issue Trackers ：问题跟踪器，可配置问题跟踪平台，如 github、gitlab、JIRA（项目与事务跟踪工具）等。

（5）Email Settings：配置邮件发送信息。

（6）Engines：引擎安装、删除、禁用设置。

（7）Excluded Hours：扫描时间设置，可设置在空闲时间扫描。

（8）Proxy Settings：设置代理服务器信息。

实训视频

AWVS 工具实训

4. 扫描过程

（1）单击左侧菜单栏“Targets”→“Add Target”，右侧出现 Address（扫描地址）和 Description（备注）输入框，Address 处填写“ testphp.vulnweb.com”，Description 处填写“testphp”，填写完毕后单击“Save”按钮，如图 4-15 所示。

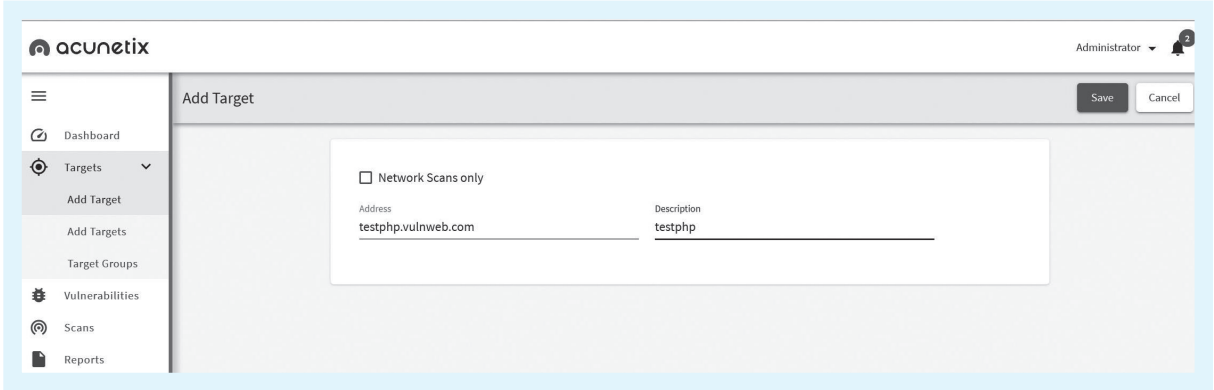


图 4-15　创建扫描

（2）单击“Save”按钮后，进行扫描相关设置，如图 4-16 所示。

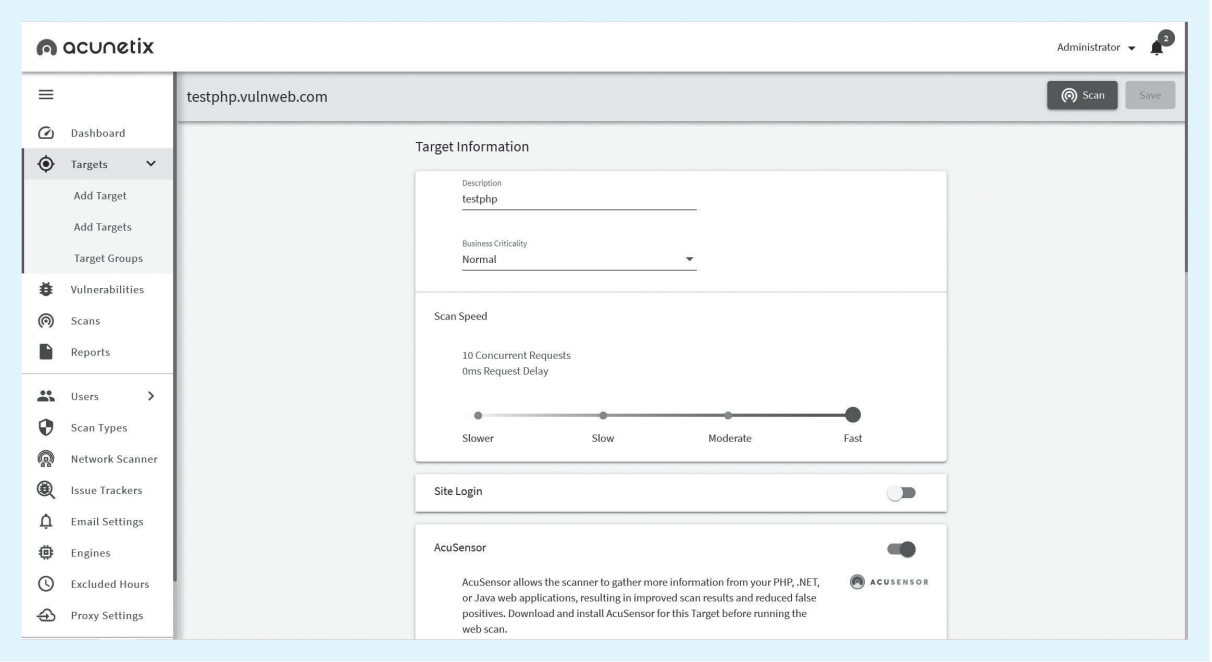


图 4-16　扫描设置

下面对此页面出现的模块进行说明。

① Business Criticality：设置扫描级别，有 Low（低）、Normal（正常）、High（高）、Critical（严格）四个级别，默认情况是 Normal。

② Scan Speed：设置扫描速度，有 Slower（非常慢）、Slow（慢）、Moderate（缓慢）、Fast（快）四个级别，默认情况是 Fast。

③ Site Login：设置登录账户和密码，通常在扫描网站应用时会遇到登录表单，通过设置该项，AWVS 在扫描过程中遇到登录表单时，会尝试使用设置的账户和密码登录。

④ HTTP：HTTP 协议相关设置。

⑤ Advanced：高级选项设置，可以设置 Cookies 等。

如果无须修改，请单击“Scan”按钮。

（3）进入扫描类型及报告输出设置界面，如图 4-17 所示。

下面对该界面进行说明。

① Scan Type：设置扫描类型，一般选择 Full Scan（全面扫描）。

② Report：设置报告输出类型。

③ Schedule：设置定时扫描，一般选择 Instant（立即）。

（4）选择好后单击“Create Scan”按钮，此时会跳转至“Scan”界面，如图 4-18 所示。

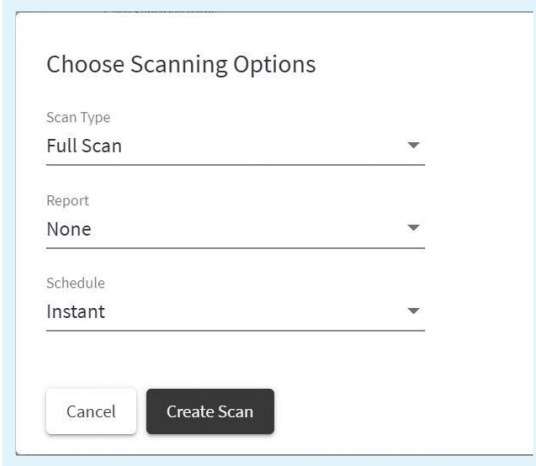


图 4-17　扫描类型及报告输出设置

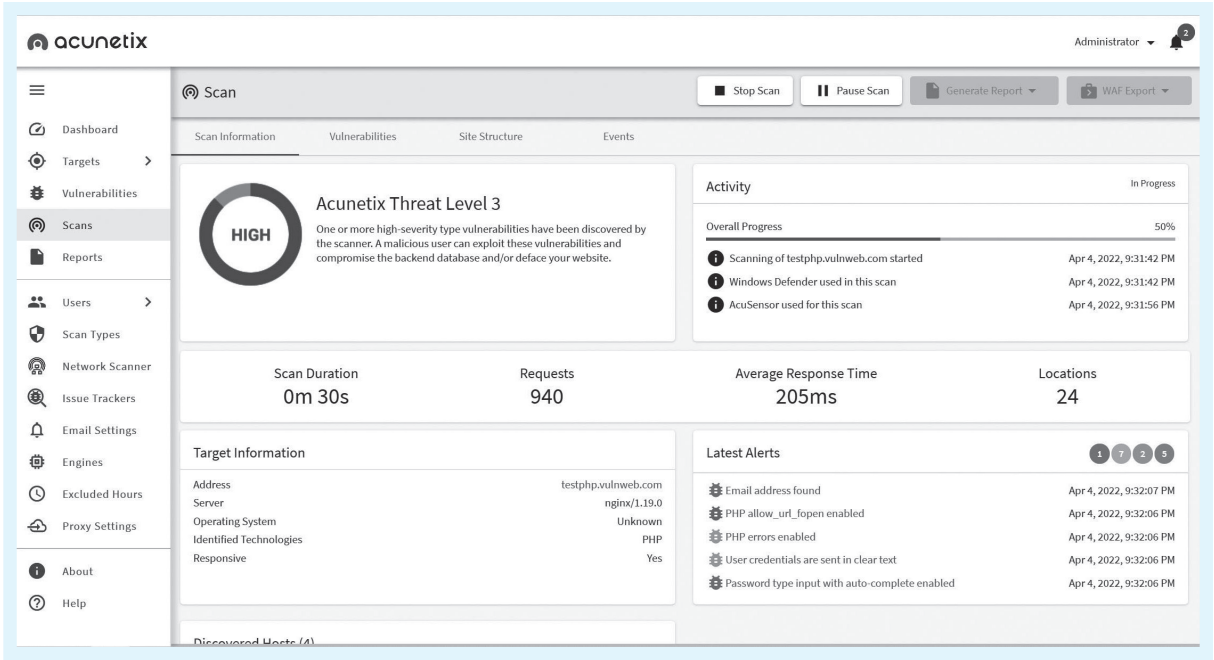


图 4-18　正在进行网站漏洞扫描

此时 AWVS 正在对指定的网站应用进行扫描，其中 Latest Alerts 模块展示已扫描出的漏洞情况，红色代表高危（High）漏洞，黄色代表中危（Medium）漏洞，蓝色代表低危（Low）漏洞，绿色代表可能存在（information）漏洞。

单击 Latest Alerts 模块下任意一条高危漏洞链接，会打开该网站某接口对应漏洞的相关信息，并显示触发该漏洞的方式，如图 4-19 所示。

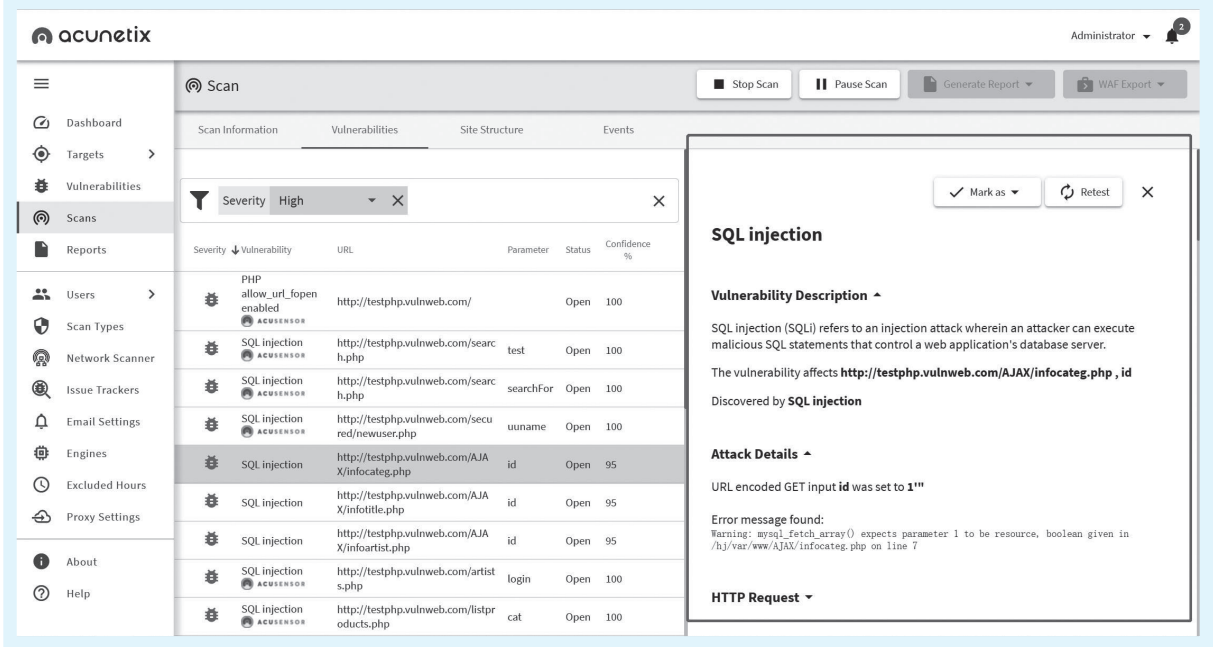


图 4-19　扫描报告浏览

5. 输出扫描报告

（1）打开扫描结果页面，单击“Generate Report”按钮，如图 4-20 所示。

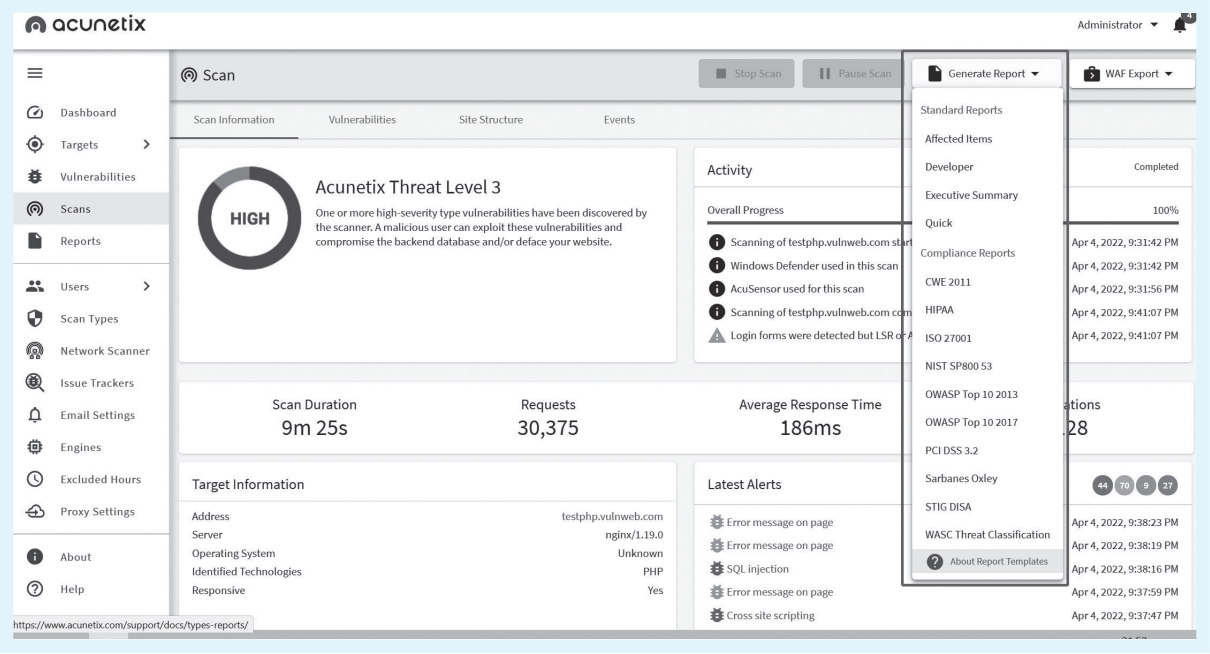


图 4-20　选择报告输出模板

（2）选择输出的报告格式（见图 4-21）后，即可跳转至报告下载页面，这里以单击“OWASP TOP 10 2017“选项为例。

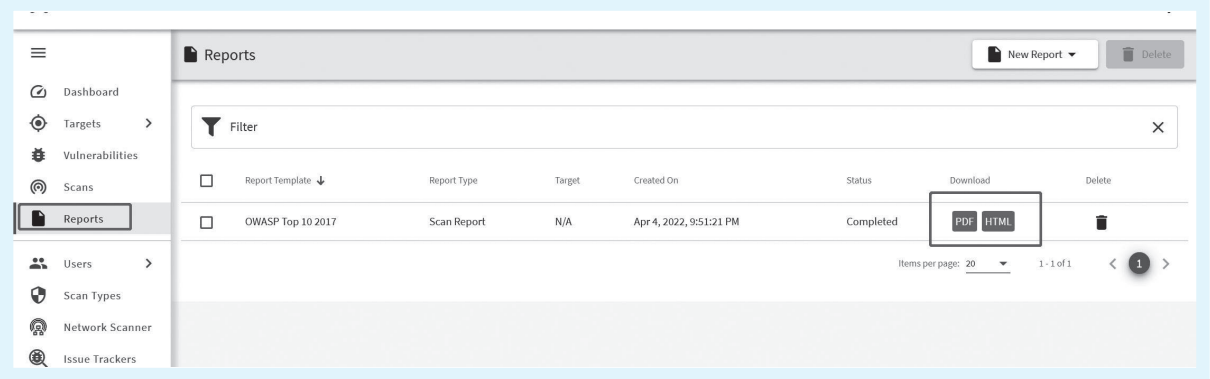


图 4-21　选择报告输出格式

（3）单击“PDF”或“HTML”按钮即可下载对应格式的报告。这里单击“PDF”按钮后立即下载报告，报告如图 4-22 所示。

图 4-22　报告样式

三、Nessus 主机扫描

Nessus 是一款功能强大又容易操作的远程安全扫描器，不仅免费而且更新极快。Nessus 具有检测漏洞多而准确、速度快的特点。

Nessus 能够对目标主机系统进行具有攻击性的安全漏洞扫描。其目的是帮助系统管理者寻找系统主机的弱点，让系统管理者对主机进行更正或防护，以免被入侵者攻击。

实训视频

Nessus 工具实训

1. 软件运行流程

（1）由于 Nessus 免费版只能使用 16 次扫描，因此本课程使用 docker 容器运行 Nessus（docker 安装流程请自行查阅）。

通过 docker 命令运行 Nessus 镜像：

```
docker run --rm -itd -p 8834:8834 registry.cn-hangzhou.aliyuncs.com/steinven/nessus:v0.1
```

运行结果如图 4-23 所示。

```
[root@VM-12-8-centos ~]# docker run --rm  -itd -p 12580:8834 registry.cn-hangzhou.aliyuncs.com/steinven/n
essus:v0.1
Unable to find image 'registry.cn-hangzhou.aliyuncs.com/steinven/nessus:v0.1' locally
v0.1: Pulling from steinven/nessus
6aa38bd67045: Pull complete
981ae4862c05: Pull complete
5bad8949dcb1: Pull complete
ca9461589e70: Pull complete
0ba6fd783ba6: Pull complete
14b6802748e8: Pull complete
8dbada7de82a: Pull complete
b83219675e8a: Pull complete
Digest: sha256:dd19e9b6e636b9618e43791228b4aa17aae048f8236c1b807ab6c7c6b9731464
Status: Downloaded newer image for registry.cn-hangzhou.aliyuncs.com/steinven/nessus:v0.1
1fc30c5ef5f8d3f29c81d6d59ecc95da625087bdcea34a1ca3d79a8604b0635d
[root@VM-12-8-centos ~]#
```

图 4-23　运行 Nessus

注意　该镜像有两个版本，分别是 v0.1 和 v0.2。其中 v0.1 大小约为 8G，无需等待初始化即可使用；v0.2 大小约为 2G，需要手动激活，建议网速较好的用户使用 v0.1 版本。

（2）当容器完全启动后，打开浏览器，在地址栏输入网址，如图 4-24 所示。

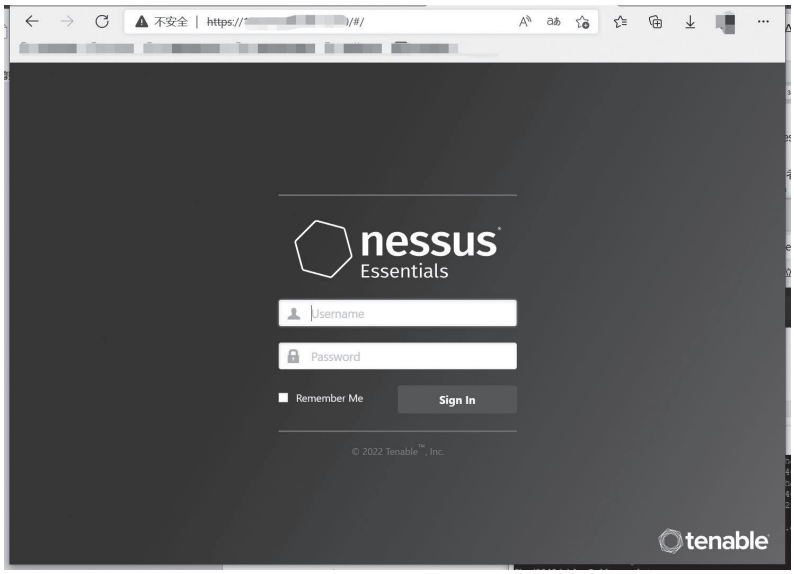


图 4-24　Nessus 登录界面

在该界面，通常只需要对 BASIC 下的 General，以及 DISCOVERY、ASSESSMENT、ADVANCED 进行设置。

（3）在 Username 和 Password 输入框内分别输入“admin”和“admin”后，单击“Sign In”（登录）按钮，进入操作界面，如图 4-25 所示。

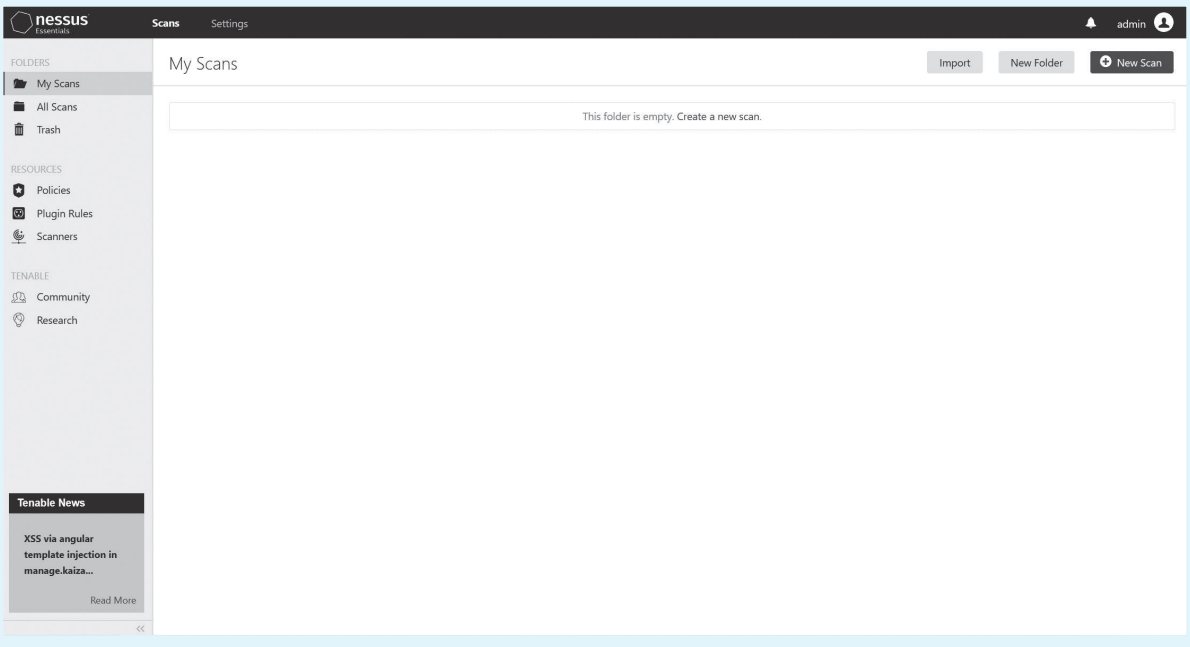


图 4-25　Nessus 操作界面

2. 进行基本网络扫描

以扫描主机 10.0.12.8 为例。

（1）单击“My Scans”→“New Scan”按钮，如图 4-26 所示。

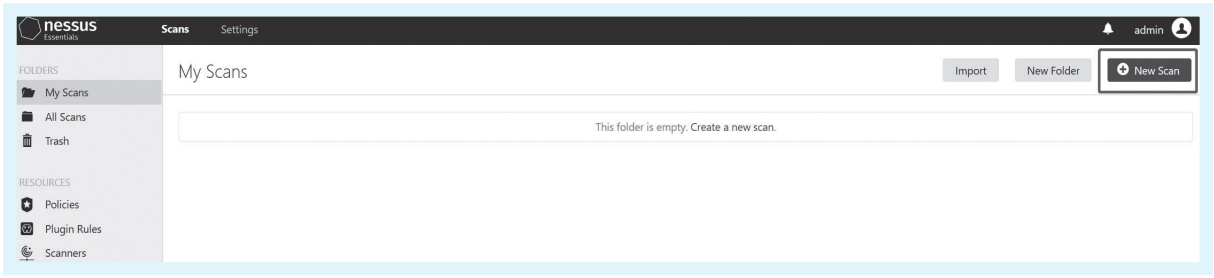


图 4-26　扫描入口

（2）单击“Basic Network Scan”（基本网络扫描）按钮，如图 4-27 所示。

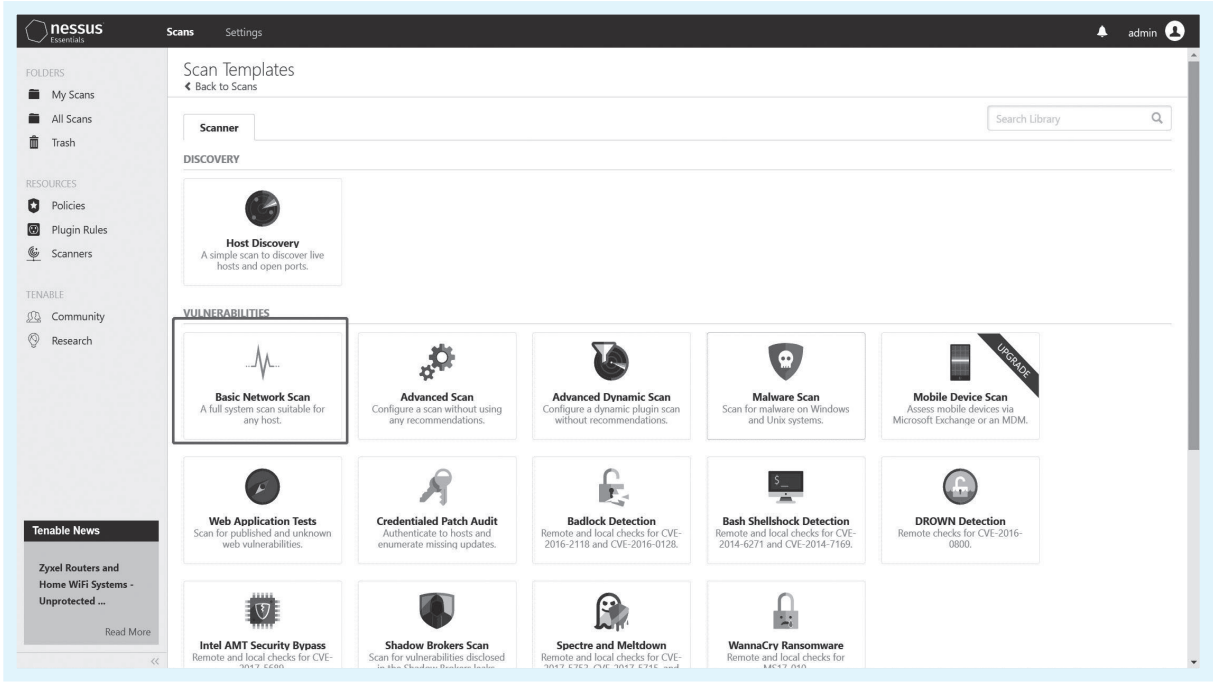


图 4-27　选择“基本网络扫描”

注意　带有 UPGRADE 标签的扫描选项，需要将 Nessus 升级为专业版（收费）才能使用。

需要命名扫描任务并填写备注等信息。

（3）进入扫描设置界面，如图 4-28 所示。

下面对该界面的模块进行说明。

① General：进行项目说明，其中 Targets 填写的是需要扫描的 IP、IP 段或域名。

② Schedule：设置扫描开始时间，默认为立即扫描。

③ Notifications：设置通知邮箱，当扫描结束后，可通过邮件方式告知用户扫描完成。默认

不发送。

④ DISCOVERY：主机发现，可以设置端口扫描类型，默认设置为常见端口扫描。

⑤ ASSESSMENT：进行 Web 应用漏洞扫描，可以设置 Web 应用漏洞扫描级别。

⑥ REPORT：报告输出设置，可以设置报告输出的信息。

⑦ ADVANCED：设置 Nessus 扫描的速度，主要是通过设置线程数来调整扫描速度。

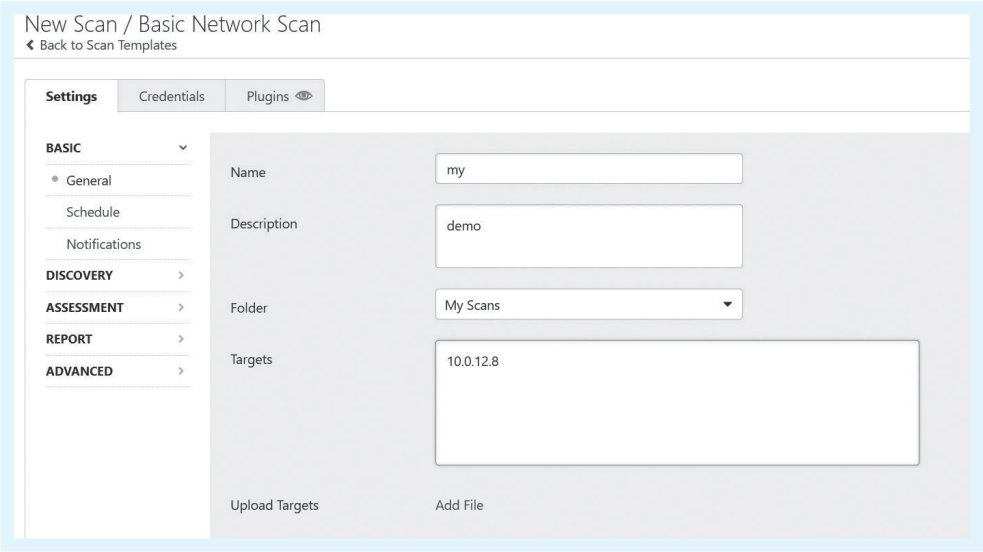


图 4-28　主机扫描设置界面

（4）设置完毕后，单击“Launch”按钮立即扫描，如图 4-29 所示。

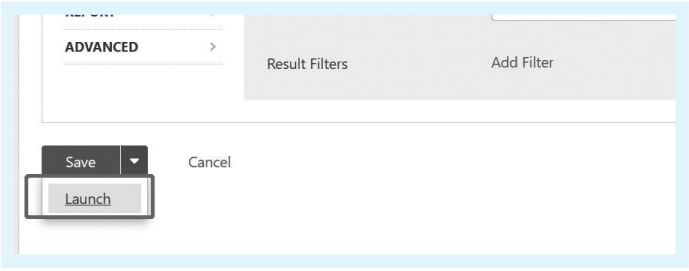


图 4-29　立即扫描

（5）这时可以回到“My Scans”界面查看扫描记录，当扫描结束时，会出现“√”的图标，如图 4-30 所示。

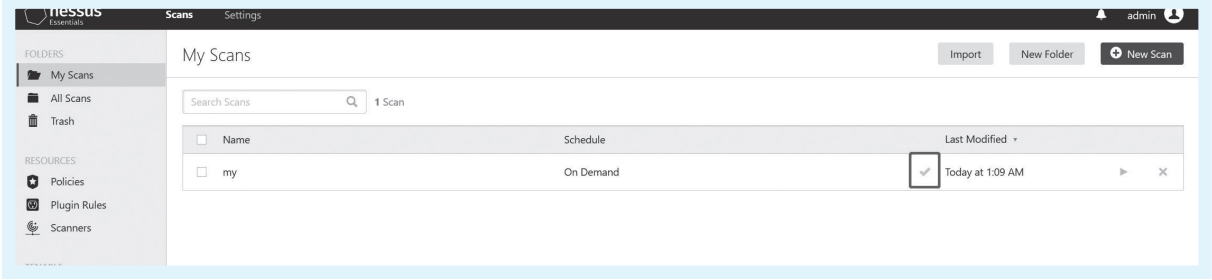


图 4-30　查看扫描情况

（6）查看扫描结果，如图 4-31 所示。

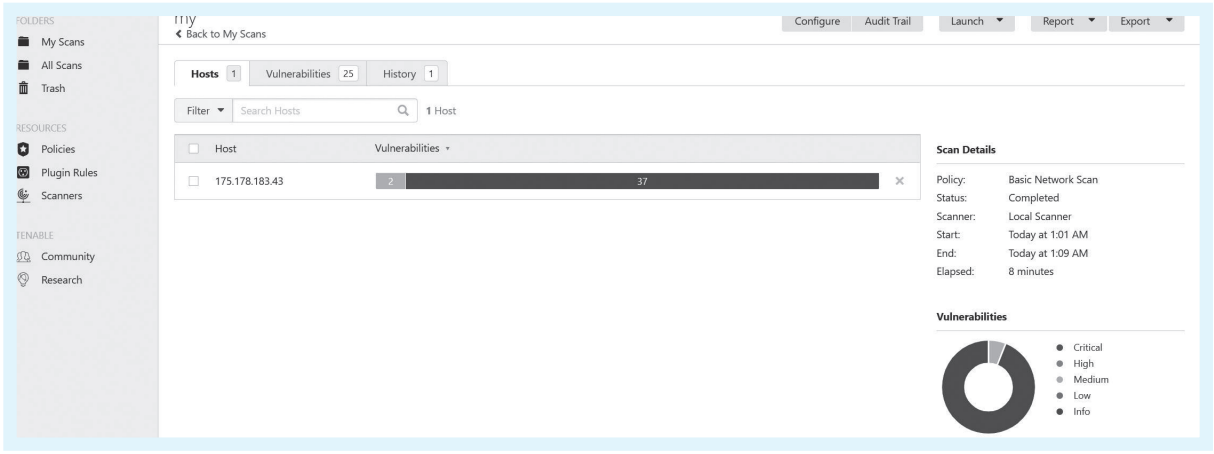


图 4-31　查看扫描结果

（7）单击“Vulnerabilities”（漏洞）选项，查看漏洞情况，如图 4-32 所示。

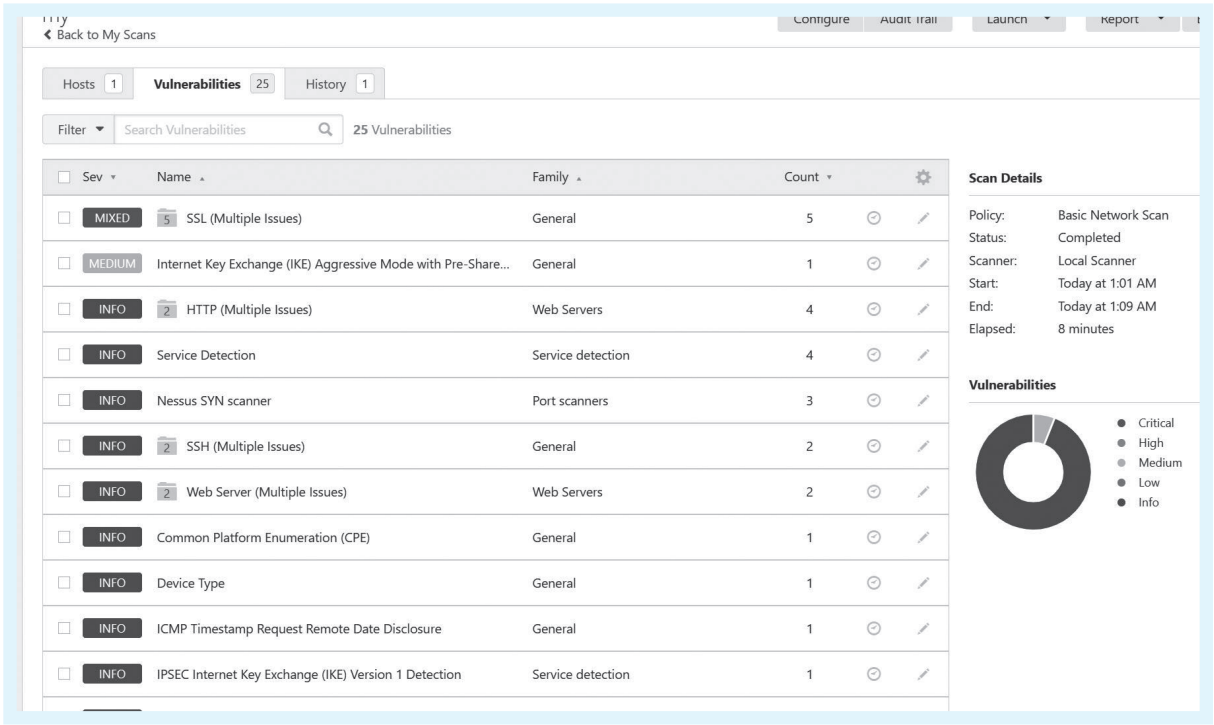


图 4-32　查看漏洞情况

Nessus 会将同一类型的漏洞进行归类，并给出漏洞的描述、解决方案、案例、端口号和主机名，如图 4-33 所示。

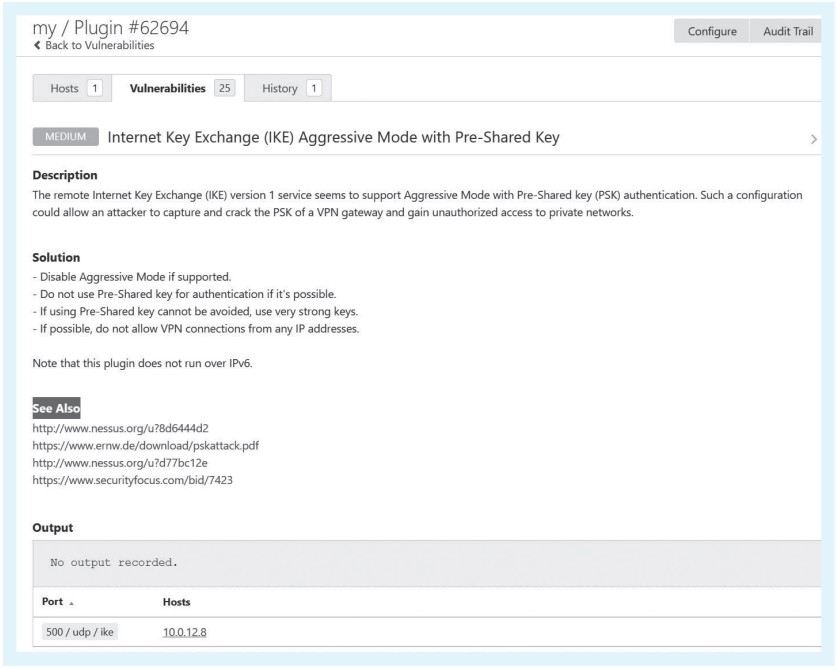


图 4-33　漏洞说明

3. 报告输出

（1）在该页面的菜单栏处单击“Report”→“HTML”按钮，如图 4-34 所示。

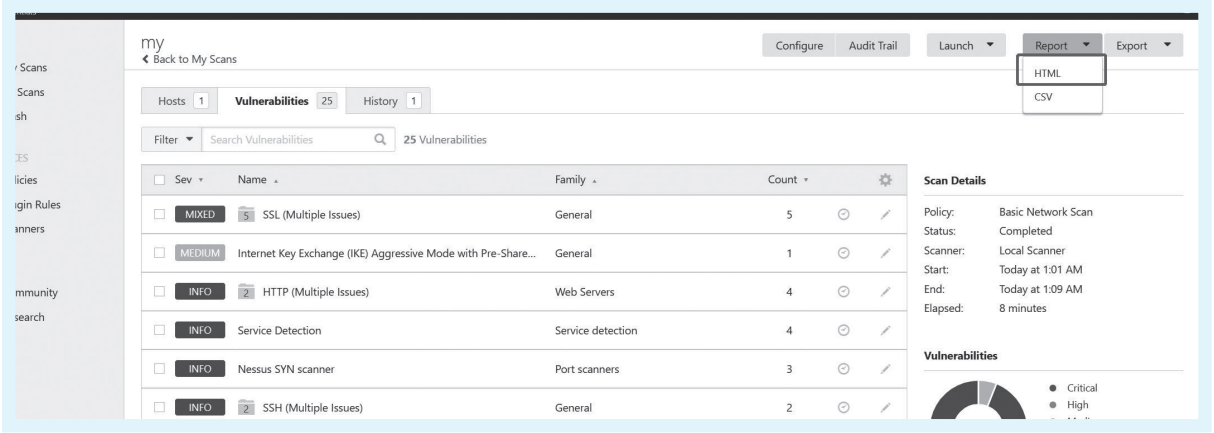


图 4-34　报告导出界面

（2）选择报告模板。报告输出分为 Custom（自定义）和 Executive Summary（默认版本），这里选择“Executive Summary”，单击“Generate Report”按钮，立即下载报告，如图 4-35 所示。

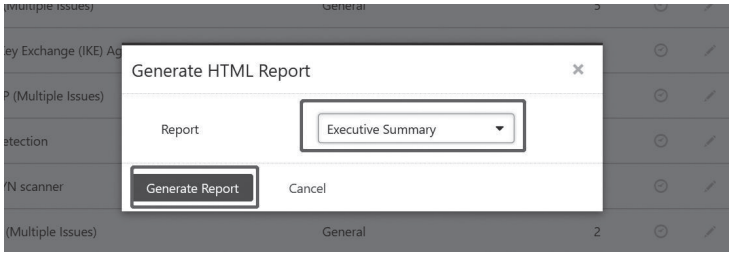


图 4-35　报告导出设置

（3）打开刚下载的 HTML 报告，如图 4-36 所示。

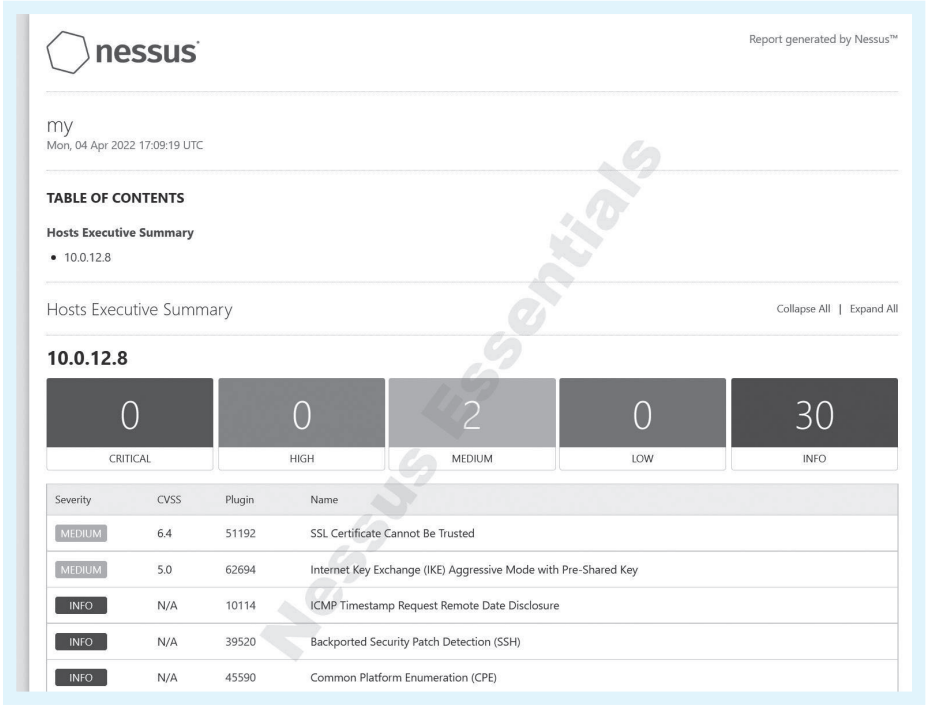


图 4-36　查阅报告

任务三　了解漏洞验证流程与规范

一、漏洞验证必要性

以漏洞扫描报告为基础，由于漏洞扫描器存在一定的误报率，需要根据报告中描述的漏洞进一步进行验证，提高漏洞扫描报告准确率，为下一步渗透测试做好准备。

二、漏洞验证步骤

根据漏洞扫描报告内容进行漏洞验证的步骤如下。

（1）仔细阅读漏洞扫描报告，将报告显示的漏洞按风险等级进行分类。

（2）对报告中的漏洞进行手动或使用工具复验，并记录下复验结果。

（3）输出漏洞验证报告。

三、漏洞验证报告

漏洞验证报告是在漏洞扫描报告的基础上进行内容增添，增添的内容为漏洞验证的结果。漏洞验证报告包含 3 部分。

（1）漏洞信息：主要包含漏洞名称、漏洞风险等级、漏洞相关描述、漏洞危害。

（2）漏洞验证结果：引发漏洞的位置、漏洞证明步骤与结果。

（3）补救方案：漏洞解决方式或临时补救措施。

任务四 认识漏洞验证工具

一、Firefox 浏览器及常用插件

Firefox 是由 Mozilla 基金会开发的自由及开放源代码的网页浏览器。后续有关的渗透攻击，都采用该浏览器进行相对应的操作。

通常会在 Firefox 上安装插件，辅助进行漏洞验证或渗透攻击。

1. FoxyProxy Standard

FoxyProxy 是一个高级的代理管理工具，它完全替代了 Firefox 有限的代理功能，可自定义配置代理并快速完成代理切换。该插件界面如图 4-37 所示。

图 4-37 FoxyProxy 插件界面

2. Max Hacker

这是一款可快速使用 SQL 注入、XSS 和 Bypass 等 payload 进行测试的渗透工具，并且可以进行多种编码和解码。该插件界面如图 4-38 所示。

图 4-38 Max Hecker 界面

3. Wappalyzer

这是一款能够分析目标网站所采用的平台构架、网站环境、服务器配置环境、JavaScript 框架、编程语言等参数的插件。该插件界面如图 4-39 所示。

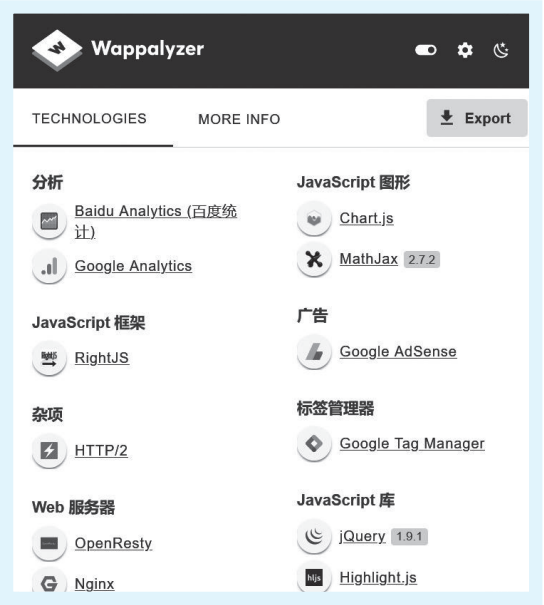


图 4-39　Wappalyzer 界面

二、Burp Suite 抓包工具

Burp Suite 是用于攻击 Web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以加快攻击应用程序的进程。Burp Suite 界面如图 4-40 所示。

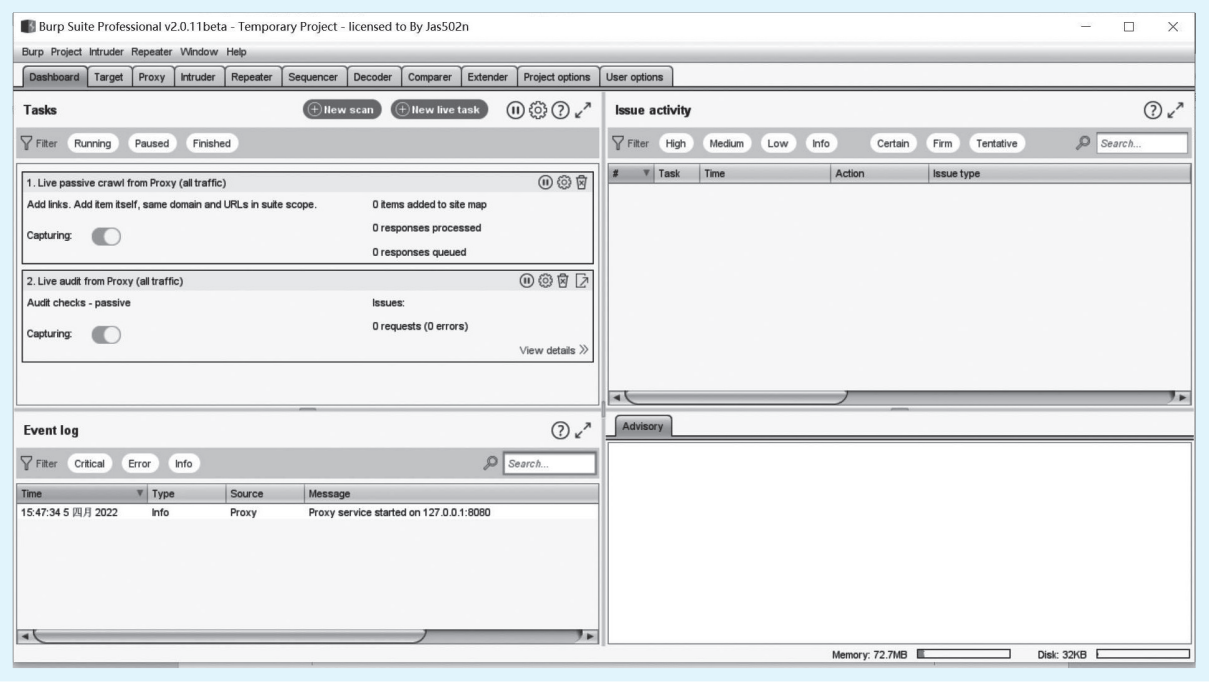


图 4-40　Burp Sutie 界面

注意 Burp Suite 工具是基于 Java 语言开发的，因此在安装 Burp Suite 前，需要先安装好 JDK 8.0 以上版本，并添加到环境变量。

1. Burp Suite 常用功能

（1）Target（目标）：显示目标目录结构。

（2）Proxy（代理）：拦截 HTTP(S) 的代理服务器，作为在浏览器和目标应用程序之间的“中间人”，允许拦截、查看、修改两个方向上的原始数据流。

（3）Intruder（入侵）：一个定制的高度可配置的工具，对 Web 应用程序进行自动化攻击，如枚举标识符，收集有用的数据，以及使用 fuzzing 技术探测常规漏洞。

（4）Repeater（中继器）：一个靠手动操作来触发单独的 HTTP 请求并分析应用程序响应的工具。

2. 利用 Burp Suite 工具抓包

实训视频

Burp Suite 代理工具实训

1）配置监听端口

（1）在工具栏处单击“Proxy”→“Options”选项，在“Proxy Listeners”模块下单击“Add”按钮，弹出窗口后往“Bind to port”输入框处填写监听端口，如 8899，填写完毕后单击“OK”按钮，如图 4-41 所示。

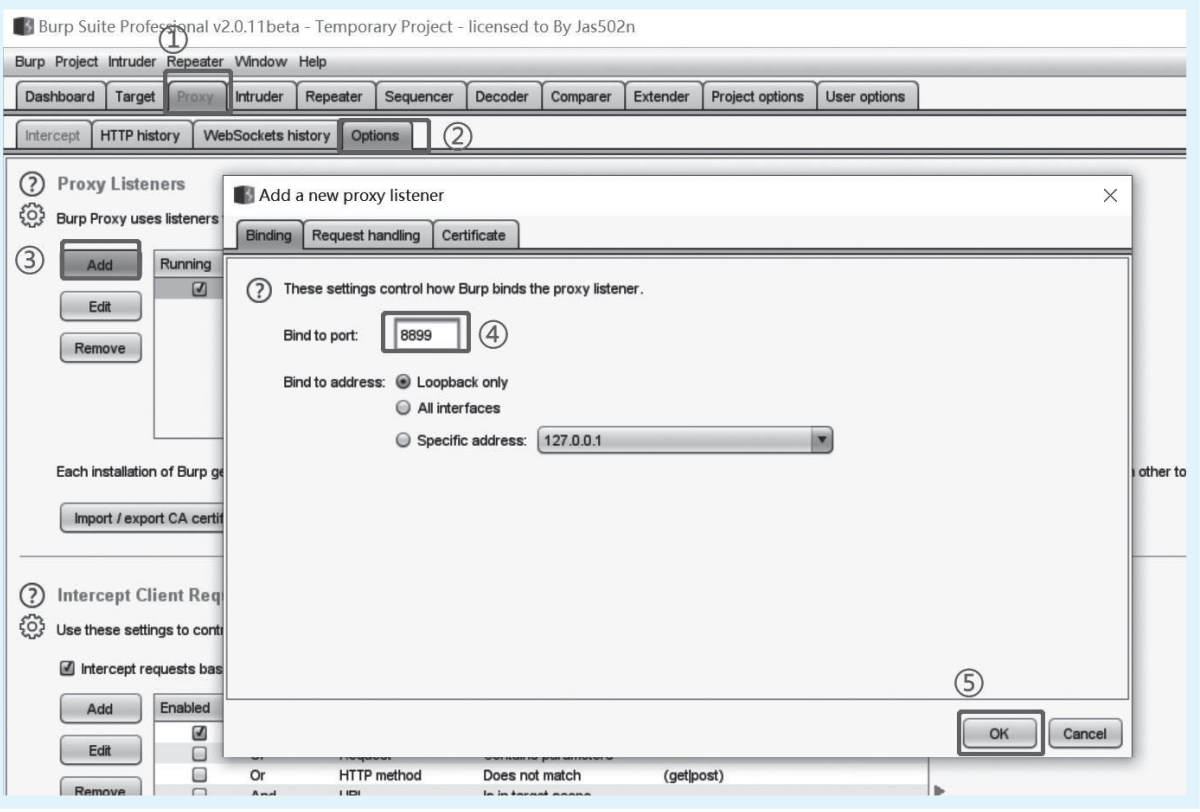


图 4-41 Burp Suite 配置监听端口

（2）添加完毕后，需要在“Running”处把刚添加的监听地址选项勾上，如图 4-42 所示。

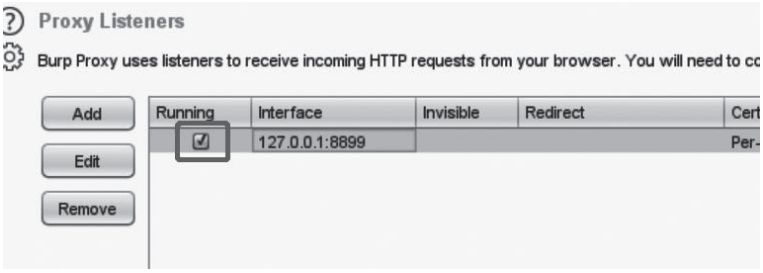


图 4-42　启动监听端口

2）下载 CA 证书

由于未给 Firefox 浏览器安装 Burp Suite 的 CA 证书，无法抓取 HTTPS 请求，因此需要先下载 CA 证书。打开浏览器，在地址栏处输入 http://127.0.0.1:8899 后按 Enter 键，跳转到 Burp Suite 的 CA 证书下载网站，单击“CA Certificate”按钮即可下载 CA 证书，如图 4-43 所示。

图 4-43　CA 证书下载界面

3）将 CA 证书导入 Firefox 浏览器

（1）打开 Firefox 浏览器，单击“设置”→“隐私与安全”，找到“安全”模块，单击“查看证书”按钮，如图 4-44 所示。

图 4-44　浏览器证书查看

（2）单击“证书颁发机构”选项卡后，单击“导入”按钮，选择刚下载的 CA 证书文件，勾选“信任由此证书颁发机构来标识网站”和“信任由此证书颁发机构来标识电子邮件用户”多选框，单击“确定”按钮，如图 4-45 所示。

图 4-45　导入 CA 证书

（3）添加完毕后，即可在“证书颁发机构”选项卡内查看对应 CA 证书，如图 4-46 所示。

图 4-46　查看证书导入状况

4）在 FoxyProxy 插件中添加代理信息

打开 FoxyProxy 插件，单击“添加”按钮，在代理类型下拉框单击“HTTP”选项，在代理 IP 地址编辑框填写“127.0.0.1”，在端口编辑框填写“8899”，单击“保存”按钮，如图 4-47 所示。

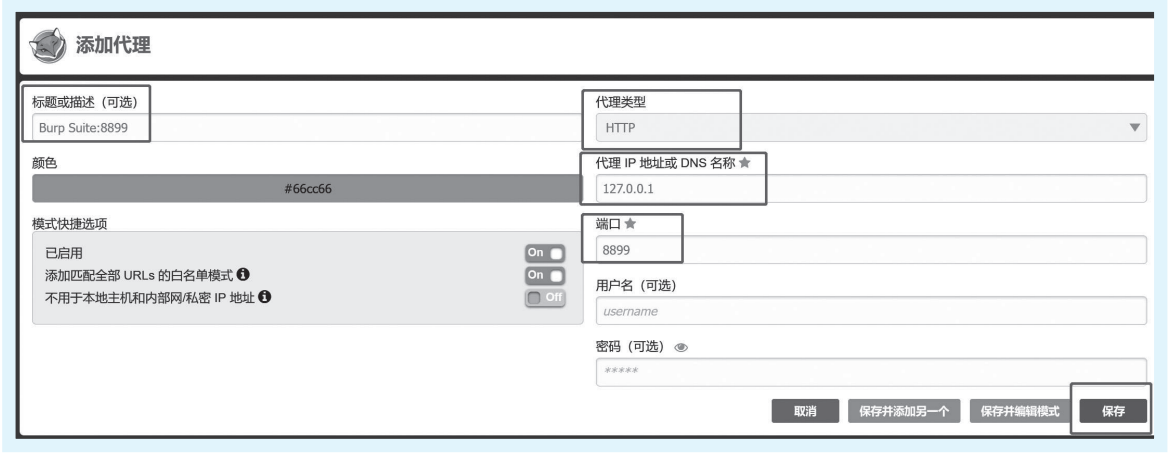


图 4-47　使用 FoxyProxy 设置代理服务器

5）抓取“百度”网址请求包

（1）在 Burp Suite 软件的“Proxy”→“Intercept”模块处，单击“Intercept is off”按钮，将其改为“Intercept is on”，如图 4-48 所示。

（2）在 Firefox 浏览器下单击 FoxyProxy 插件按钮，在显示的代理名称下单击“Burp Suite: 8899”选项，如图 4-49 所示。

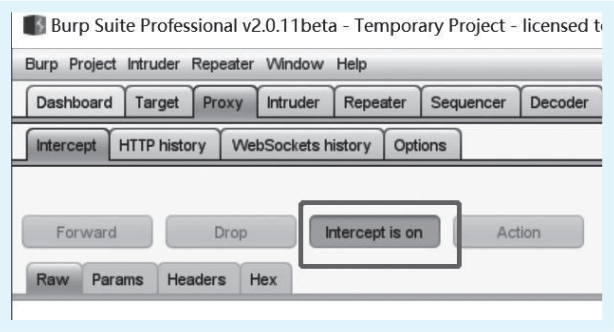


图 4-48　开启请求拦截

图 4-49　开启请求转发代理服务器

（3）在 Firefox 地址栏输入“baidu.com”后按 Enter 键，Burp Suite 将自动抓取请求包，如图 4-50 所示。

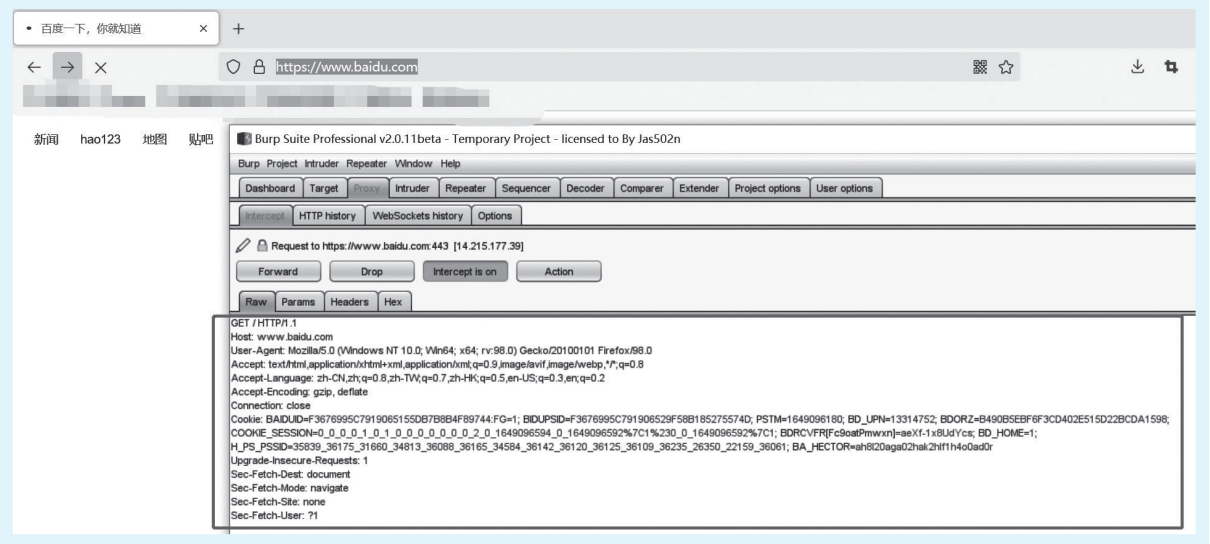


图 4-50　查看拦截请求包

三、SQLMap 自动化注入工具

SQLMap 是一个开源渗透测试工具，它可以自动检测和利用 SQL 注入漏洞并接管数据库服务器。它具有强大的检测引擎，还有众多功能，包括数据库指纹识别、从数据库中获取数据、访问底层文件系统，以及通过带外连接，可在操作系统上执行命令。

1. SQLMap 特点

SQLMap 由 Python 写成，具有如下特点。

（1）支持市场多种数据库，如 MySQL、Oracle、SQL Server 等。

（2）操作过程全程使用命令，通过命令形式，自动执行数据渗透工作。

（3）支持字符串型注入、数值型注入、布尔型盲注、时间型盲注、报错注入、联合查询注入以及堆叠查询注入等渗透注入方式。

（4）当渗透成功后，能够获取数据库名、数据表名，并根据渗透人员要求获取表中相关数据。

（5）支持执行任意数据库命令并回显输出。

Kali 操作系统已集成 SQLMap 软件，无需额外安装。该软件界面如图 4-51 所示。

图 4-51　SQLMap 界面

2.SQLMap 常用选项

SQLMap 常用选项如表 4-3 所示。

表 4-3　SQLMap 常用选项

选项	功能	选项描述
-u	网址	设置 SQL 扫描的地址
-p	参数	设置 SQL 扫描指定地址的参数，如不设置，默认为地址栏上所有参数
--batch	使用默认配置扫描	使用所有默认配置，从不询问用户输入
--data	POST 参数设置	设置 SQL 扫描地址 POST 参数

续表

选项	功能	选项描述
--cookie	cookie 设置	设置请求头的 Cookie 字段
-r	读取请求头文件	发送请求时使用该文件的请求头
--current-db	获取数据库名称	获取当前数据库的名称
--tables	获取数据表名称	获取当前数据表的名称
--columns	获取数据表字段名	获取当前数据表所有的字段名
--dump	获取表中数据	输出指定数据表中的数据，保存为 csv 格式
-D	设置数据库名	设置 SQL 扫描时的指定数据库
-T	设置数据表名	设置 SQL 扫描时的指定数据表
-C	设置字段名	设置 SQL 扫描时指定数据表中的字段名
--level	探测等级	设置 SQLMap 的探测等级，一共是 1 ～ 5 级，默认值为 1
--risk	探测风险	设置 SQLMap 的探测风险，一共是 1 ～ 3 级，默认值为 1

3. 扫描 testphp 网站

实训视频

SQLMap 工具实训

1）寻找注入点

SQL 一般在可输入点进行注入，因此可以任意找一处输入点，如图 4-52 所示。

2）抓包分析

抓包，分析出该请求包是 POST 请求、请求网址，以及参数为 searchFor，如图 4-53 所示。

图 4-52　获取注入元素

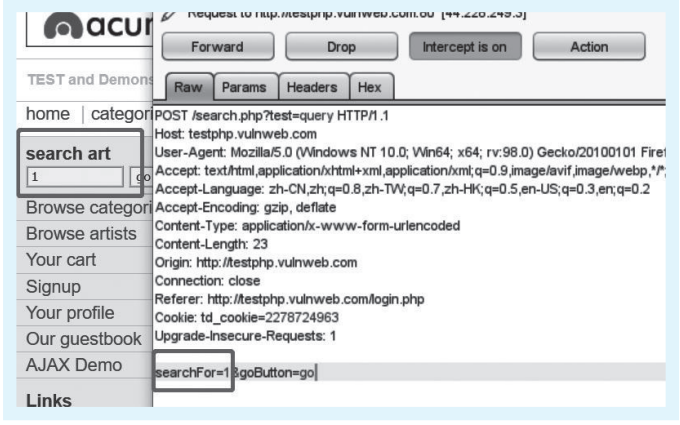


图 4-53　获取请求参数

3）执行 SQLMap 脚本进行扫描

（1）对该注入点进行 SQL 自动化注入，执行命令：

```
sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --data "searchFor=1" –batch
```

扫描过程如图 4-54 所示。

图 4-54　使用 SQLMap 脚本扫描

（2）当脚本执行完毕后，可以得知该点存在 SQL 注入漏洞，如图 4-55 所示。

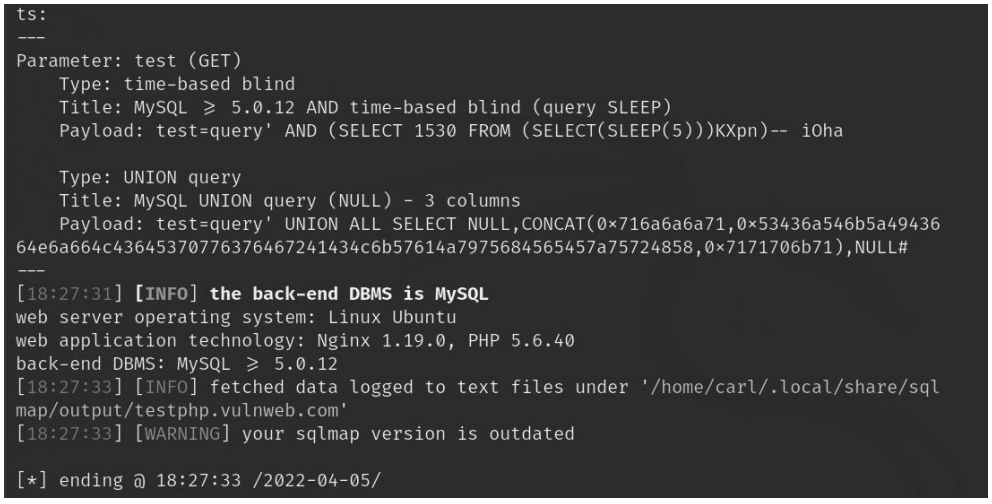


图 4-55　SQLMap 扫描结果

4）获取数据库名

通过此注入点获取数据库名，执行脚本命令：

```
sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --data "searchFor=1" --batch –dbs
```

获取的数据库名如图 4-56 所示。

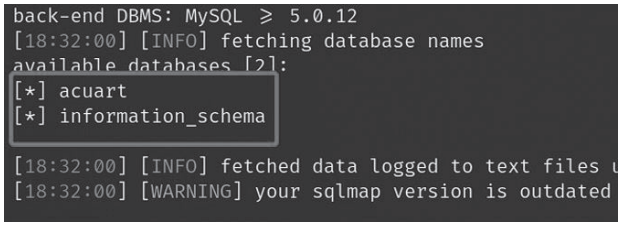


图 4-56　SQLMap 获取数据库名

5）获取数据表名

通过此注入点，获取 acuart 数据库下的所有数据表名，执行脚本命令：

```
sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --data "searchfor=1" --batch -D "acuart" –tables
```

获取的数据表名如图 4-57 所示。

6）获取 users 表中的字段名

通过此注入点，获取数据表 users 中的所有字段名，执行命令：

```
sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --data "searchfor=1" --batch -D "acuart" -T "users" –columns
```

获取的字段名如图 4-58 所示。

图 4-57　获取 acuart 数据库中的数据表名

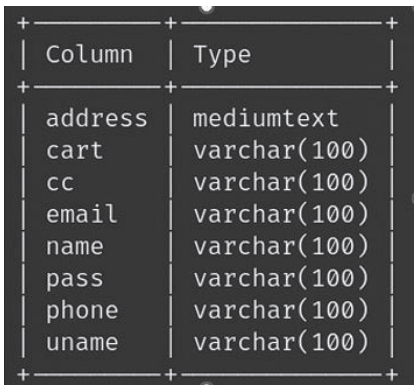


图 4-58　获取 users 表中的字段名

7）导出 users 表中所有的数据

将 users 表中的所有数据导出为 csv 文件，执行命令：

```
sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --data "searchfor=1" --batch -D "acuart" -T "users" --dump
```

导出文件所在目录如图 4-59 所示。

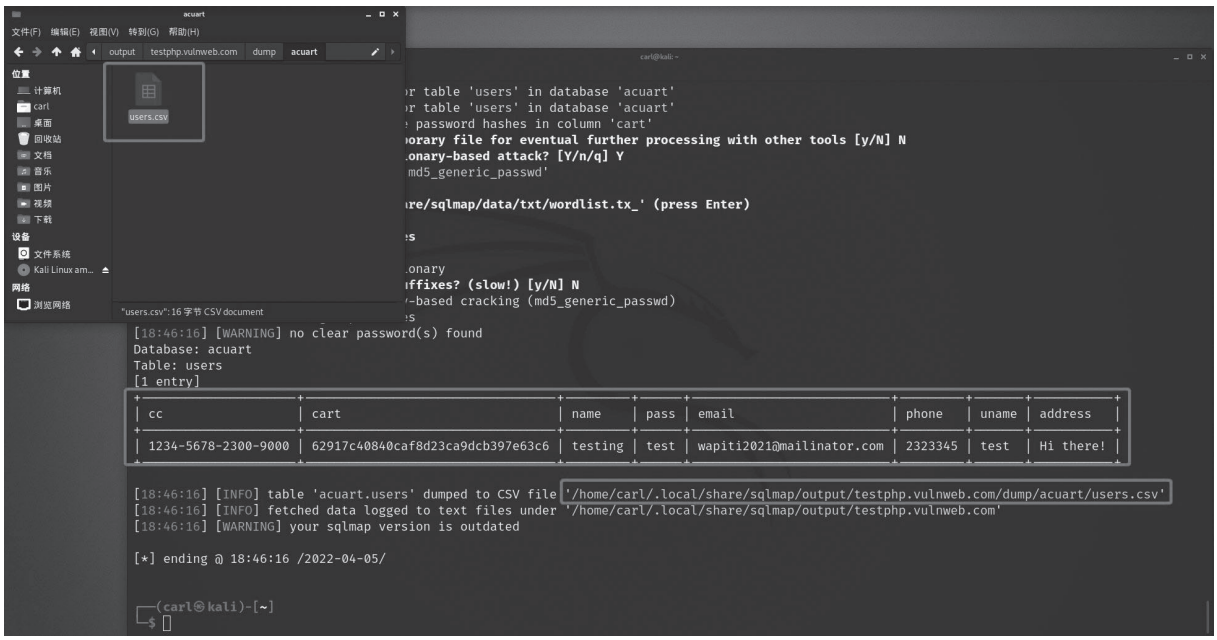


图 4-59　导出文件所在目录

任务五 掌握漏洞验证方法

本任务漏洞验证方法的使用以任务二的 AWVS 工具生成的报告为例进行介绍。

一、常见低危漏洞验证

1. X-Frame-Options 未配置

漏洞说明如图 4-60 所示。

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	

```
GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
```

图 4-60 存在 X-Frame-Options 漏洞

1）漏洞描述

点击劫持（ClickJacking）是一种视觉上的欺骗手段。攻击者将透明的 iframe 覆盖在网页上，然后诱使用户在网页上进行操作，此时用户将在不知情的情况下点击透明的 iframe 页面。调整 iframe 页面的位置，可以诱使用户恰好点击在 iframe 页面的一些功能性按钮上。

HTTP 响应头信息中的 X-Frame-Options 可以指示浏览器是否应该加载一个 iframe 页面。如果服务器响应头信息中没有 X-Frame-Options，则该网站存在 ClickJacking 攻击风险。网站可以通过设置 X-Frame-Options 阻止站点内的页面被其他页面嵌入，从而防止点击劫持。

2）验证方法

查看报告可知该漏洞的位置，验证该漏洞的方式为抓取响应包查看是否存在 X-Frame-Options 字段，若响应包不存在该字段，则证明该漏洞存在，如图 4-61 所示。

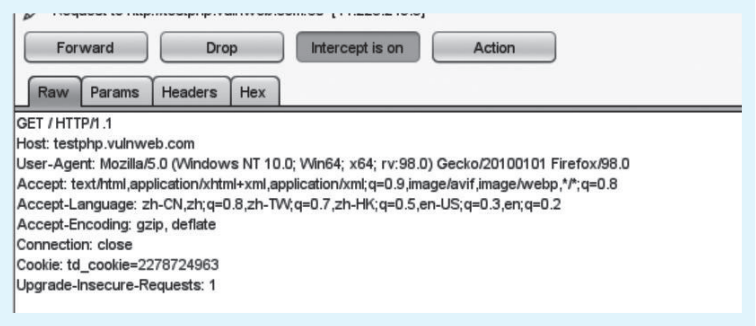


图 4-61　漏洞响应包详情

2. HttpOnly 未设置

漏洞说明如图 4-62 所示。

1）漏洞介绍

使用 HttpOnly 标志设置 Cookie 时，它会指示浏览器该 Cookie 只能由服务器访问，而不能由客户端脚本访问。若响应包没有设置 HttpOnly 属性，则客户端可以通过 JavaScript 脚本访问 Cookie。通过 XSS 攻击的方式窃取客户端的 Cookie，导致盗窃者利用此信息非法查看数据或执行属于被盗窃用户权限的操作。

2）验证方式

查看报告可知该漏洞的位置，验证该漏洞的方式为抓取响应包查看 Set-Cookie 字段里 HttpOnly 字段是否存在，若不存在，则证明该漏洞存在，如图 4-63 所示。

Web Server	
Alert group	Cookie(s) without HttpOnly flag set (verified)
Severity	Low
Description	This cookie does not have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HttpOnly flag for this cookie.
Alert variants	
Details	Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0

```
GET /logout.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-Queries: aspectalerts

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
```

图 4-62　存在 HttpOnly 漏洞

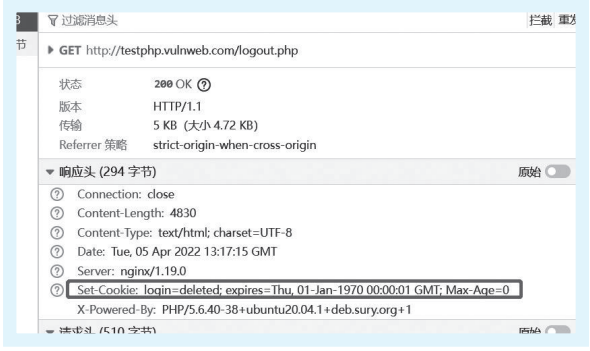


图 4-63　查看 Set-Cookie 字段

二、常见中危漏洞验证

1. htaccess 文件可读

漏洞说明如图 4-64 所示。

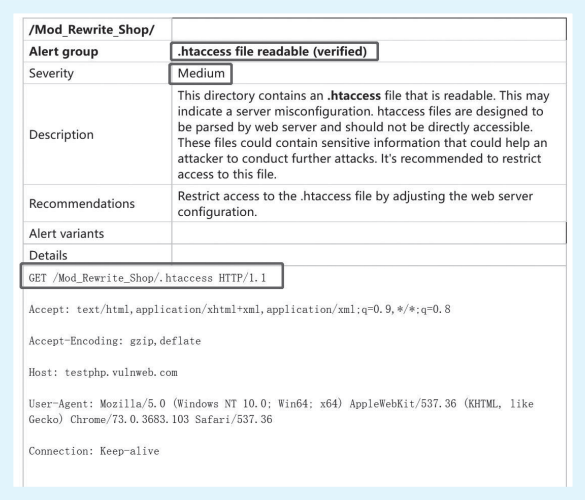
1）漏洞介绍

htaccess 文件是 Apache 服务器下的一个配置文件，主要负责相关目录下的网页配置，即在一个特定的文档目录中放置一个包含一个或多个指令的文件来对网页进行配置。

报告显示该目录包含一个可读的 htaccess 文件，这可能表示服务器配置错误。htaccess 文件由 Web 服务器解析，不应直接访问。文件可能包含敏感信息，可以帮助攻击者进行进一步的攻击。

2）验证方法

在浏览器中输入 htaccess 文件所在的位置，若能查看或下载，则代表该漏洞存在，如图 4-65 所示。



/Mod_Rewrite_Shop/	
Alert group	**.htaccess file readable (verified)**
Severity	Medium
Description	This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.
Recommendations	Restrict access to the .htaccess file by adjusting the web server configuration.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive
```

图 4-64　存在 htaccess 文件可读漏洞

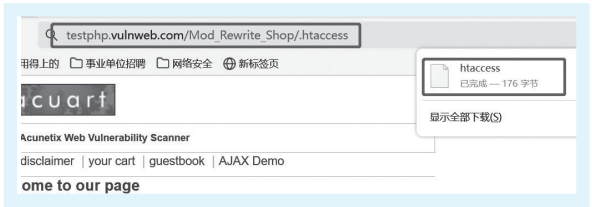
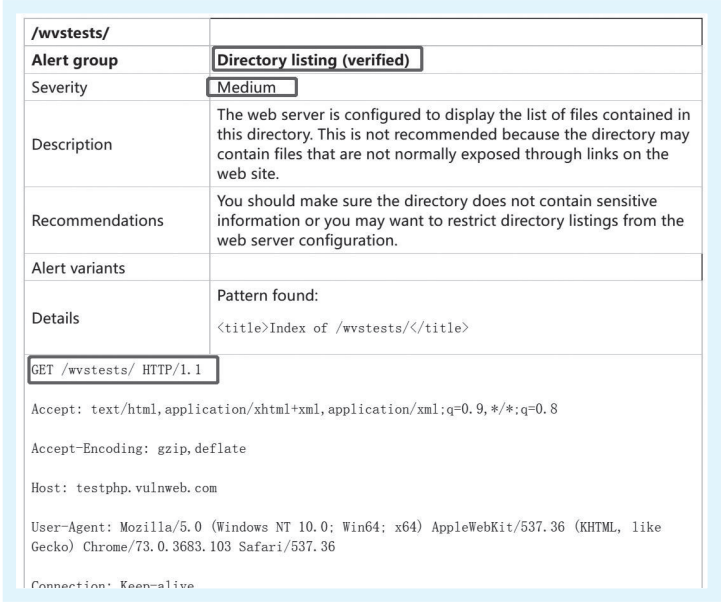


图 4-65　htaccess 文件可下载

2. 目录列表漏洞

漏洞说明如图 4-66 所示。



/wvstests/	
Alert group	**Directory listing (verified)**
Severity	Medium
Description	The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.
Recommendations	You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	Pattern found: <title>Index of /wvstests/</title>

```
GET /wvstests/ HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: testphp.vulnweb.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36

Connection: Keep-alive
```

图 4-66　存在目录列表漏洞

1）漏洞介绍

由于 Web 服务器的相关配置导致用户可以通过浏览器访问服务器的目录列表和网站开发人员隐藏的目录。

2）验证方式

根据报告提供的位置，在浏览器地址栏处填写链接，若能显示目录，则证明该漏洞存在，如图 4-67 所示。

图 4-67　目录列表漏洞证明

三、常见高危漏洞验证

1. SQL 注入

漏洞说明如图 4-68 所示。

/Mod_Rewrite_Shop/Details/color-printer/3/	
Alert group	**SQL injection (verified)**
Severity	High
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URI and/or header was set to **1\"**.

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1ACUSTART'"ACUEND HTTP/1.1
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
```

图 4-68　存在 SQL 注入漏洞

1）漏洞介绍

SQL 注入是指 Web 应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在 Web 应用程序中事先定义好的查询语句的结尾添加额外的 SQL 语句，在管理员不知情的情况下实现非法操作，以此来欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

2）验证方法

根据访问报告指向的网址，尝试使用报错注入方式访问网站，若出现报错语句，则证明该漏洞存在，如图 4-69 所示。

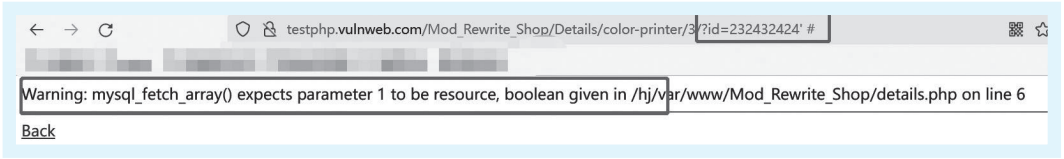


图 4-69　出现 SQL 报错

2. 跨站点脚本攻击

漏洞说明如图 4-70 所示。

/guestbook.php	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **name** was set to **anonymous user'" ()&%<acx><ScRiPt >07ut(9758)</ScRiPt>**

```
POST /guestbook.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
```

图 4-70　存在 XSS 漏洞

1）漏洞介绍

跨站点脚本（XSS）是指客户端代码注入攻击。其中攻击者可以将恶意脚本嵌入合法网站或 Web 应用程序中。当 Web 应用程序在其生成的输出中使用未经验证或未编码的用户输入时，就会发生 XSS 攻击。

2）漏洞验证

查看报告中指出的漏洞位置，往以下编辑框内写入

```
<img src="https://www.baidu.com/img/flexible/logo/pc/result.png" />
```

若能出现百度的图片，则证明该漏洞存在，如图 4-71、图 4-72 所示。

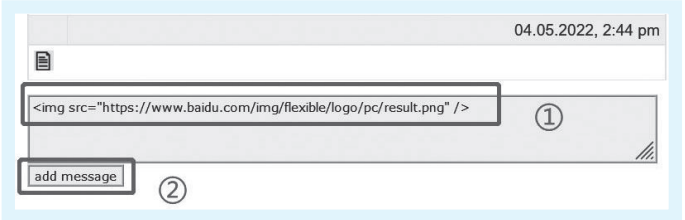


图 4-71　手动写入 img 标签

图 4-72　图片显示证明存在漏洞

思考与练习

（1）请使用 Wampmanager 或 PhpStudy 集成工具，搭建 Sqli-Labs 靶场网站，使用 SQLMap 工具或 AWVS 工具对 Sqli-Labs 第 1 关进行扫描，记录该关卡的漏洞类型。

（2）根据第（1）题的结论，使用 Firefox 浏览器和 Burp Suite 抓包工具，对 Sqli-Labs 第 1 关进行手动注入，获取 Sqli-Labs 靶场数据库的表名。

（3）使用 VMware 虚拟机工具，搭建 Kali 操作系统，使用 Nmap 工具对 Kali 操作系统进行扫描，记录本主机端口开放状态和操作系统类型。

拓展阅读

漏洞扫描与验证的社会意义和要点精髓