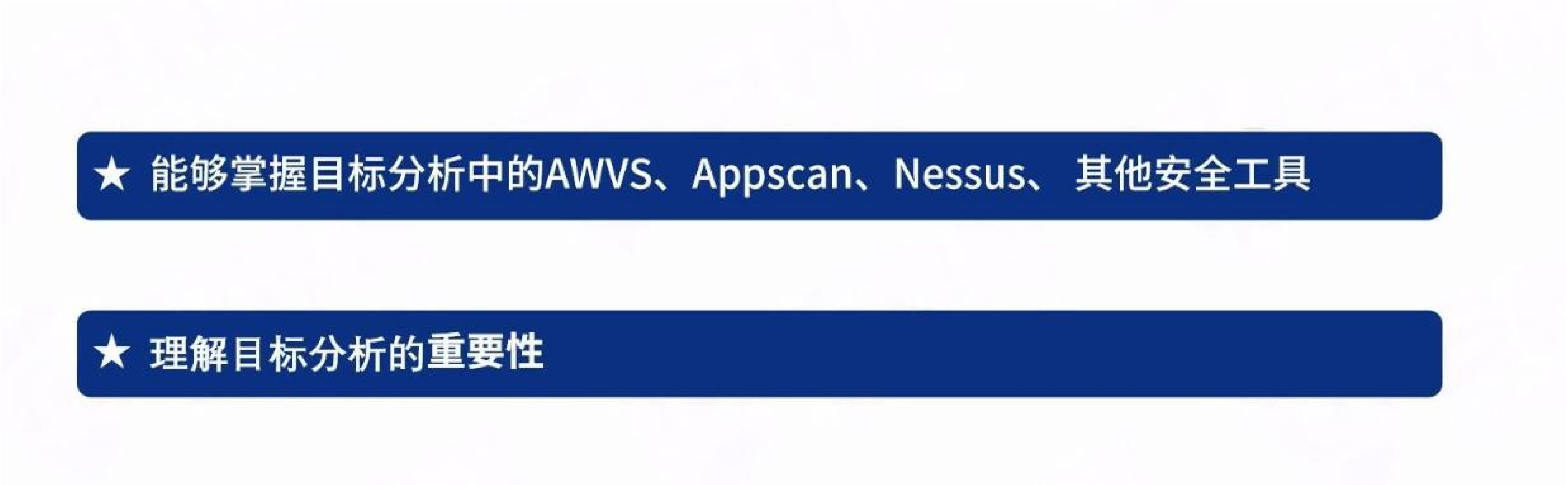
渗透测试工程师技术实战课

渗透工具篇渗透工具篇2 第1-3课

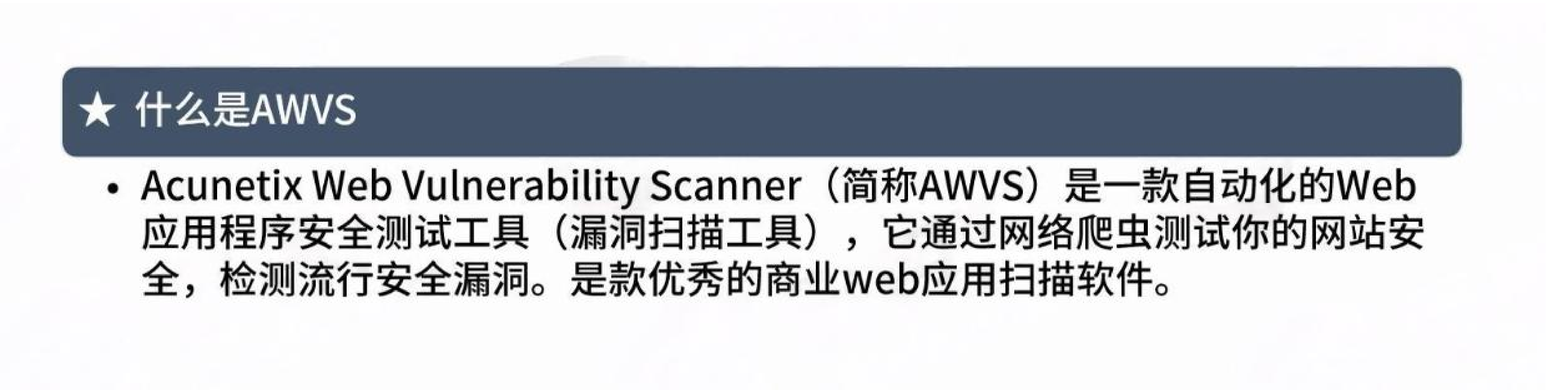
教学目标



★ 能够掌握目标分析中的AWVS、Appscan、Nessus、 其他安全工具

★ 理解目标分析的重要性

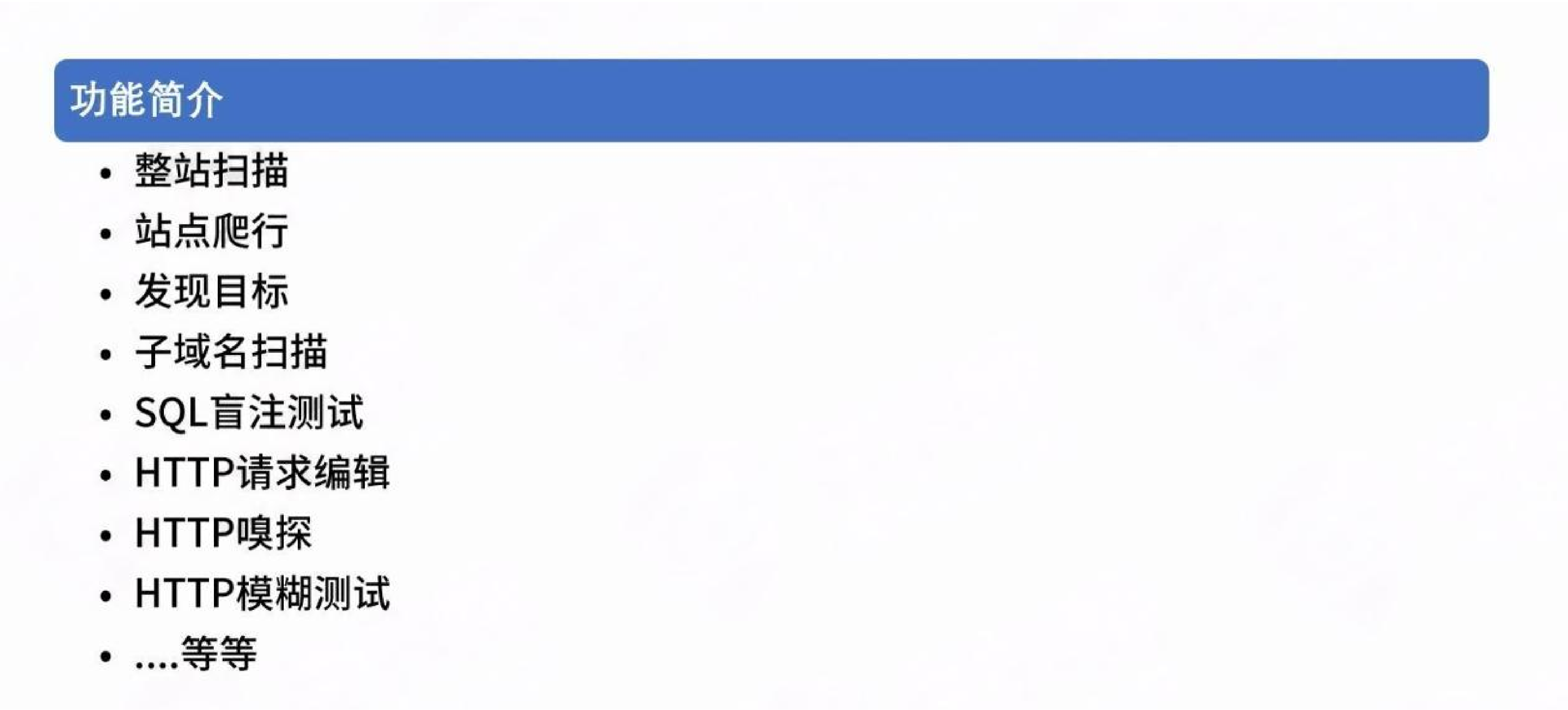
●AWVS



★ 什么是AWVS

- Acunetix Web Vulnerability Scanner（简称AWVS）是一款自动化的Web应用程序安全测试工具（漏洞扫描工具），它通过网络爬虫测试你的网站安全，检测流行安全漏洞。是款优秀的商业web应用扫描软件。

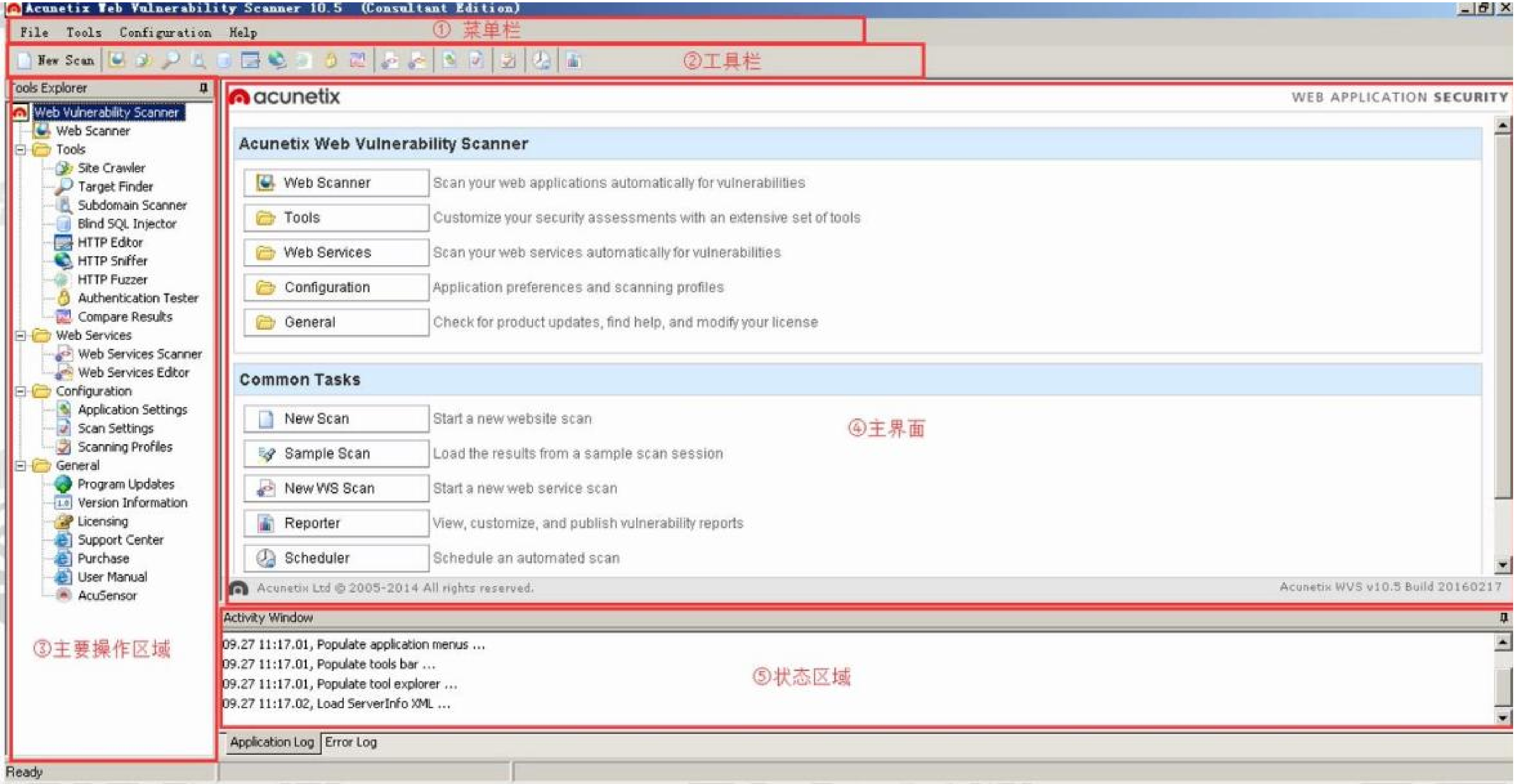
●AWVS



功能简介

- 整站扫描
- 站点爬行
- 发现目标
- 子域名扫描
- SQL盲注测试
- HTTP请求编辑
- HTTP嗅探
- HTTP模糊测试
- ....等等

●AWVS界面



Acunetix Web Vulnerability Scanner 10.5 (Consultant Edition)

Acunetix Web Vulnerability Scanner

Web Scanner	Scan your web applications automatically for vulnerabilities
Tools	Customize your security assessments with an extensive set of tools
Web Services	Scan your web services automatically for vulnerabilities
Configuration	Application preferences and scanning profiles
General	Check for product updates, find help, and modify your license

Common Tasks

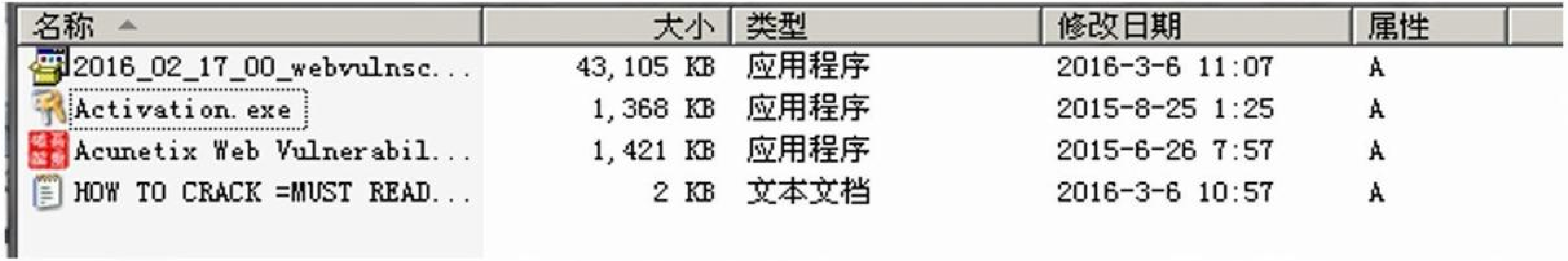
New Scan	Start a new website scan
Sample Scan	Load the results from a sample scan session
New WS Scan	Start a new web service scan
Reporter	View, customize, and publish vulnerability reports
Scheduler	Schedule an automated scan

Acunetix Ltd © 2005-2014 All rights reserved.

Acunetix WVS v10.5 Build 20160217

```
09.27 11:17.01, Populate application menus ...
09.27 11:17.01, Populate tools bar ...
09.27 11:17.01, Populate tool explorer ...
09.27 11:17.02, Load ServerInfo XML ...
```

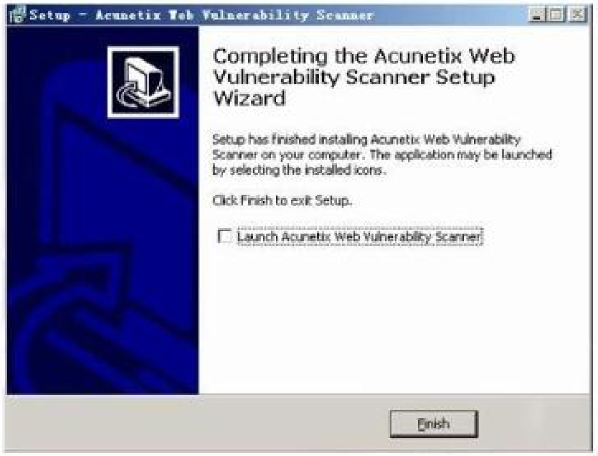
●AWVS安装过程



名称	大小	类型	修改日期	属性
2016_02_17_00_webvulnsc...	43,105 KB	应用程序	2016-3-6 11:07	A
Activation.exe	1,368 KB	应用程序	2015-8-25 1:25	A
Acunetix Web Vulnerabil...	1,421 KB	应用程序	2015-6-26 7:57	A
HOW TO CRACK =MUST READ...	2 KB	文本文档	2016-3-6 10:57	A

- 其中 2016_02_17_00_webvulnscan105.exe是AWVS v10.5的安装包，而 Acunetix_Web_Vulnerability_Scanner_10.x_Consultant_Edition_KeyGen_Hmily 是破解补丁

●AWVS安装破解



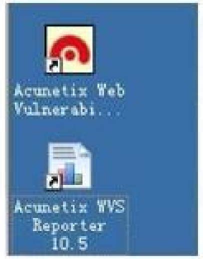
Setup - Acunetix Web Vulnerability Scanner

Completing the Acunetix Web Vulnerability Scanner Setup Wizard

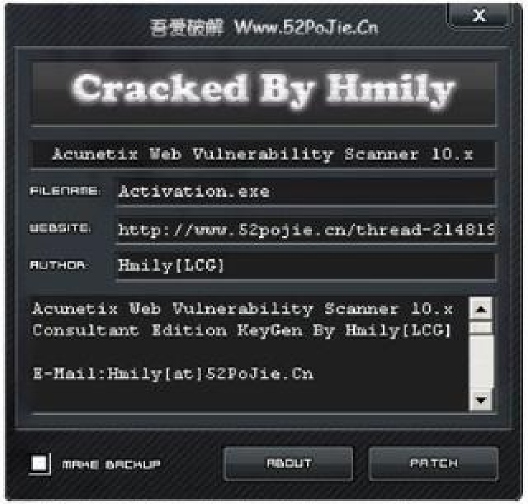
Setup has finished installing Acunetix Web Vulnerability Scanner on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

□ Launch Acunetix Web Vulnerability Scanner



- 安装到最后一步的时候将“Launch Acunetix Web Vulnerbility Scanner”前的勾去掉，安装完成之后将会在桌面生成两个图标



吾爱破解 Www.52PoJie.Cn

Cracked By Hmily

Acunetix Web Vulnerability Scanner 10.x

FILENAME: Activation.exe

WEBSITE: http://www.52pojie.cn/thread-21481

AUTHOR: Hmily[LCG]

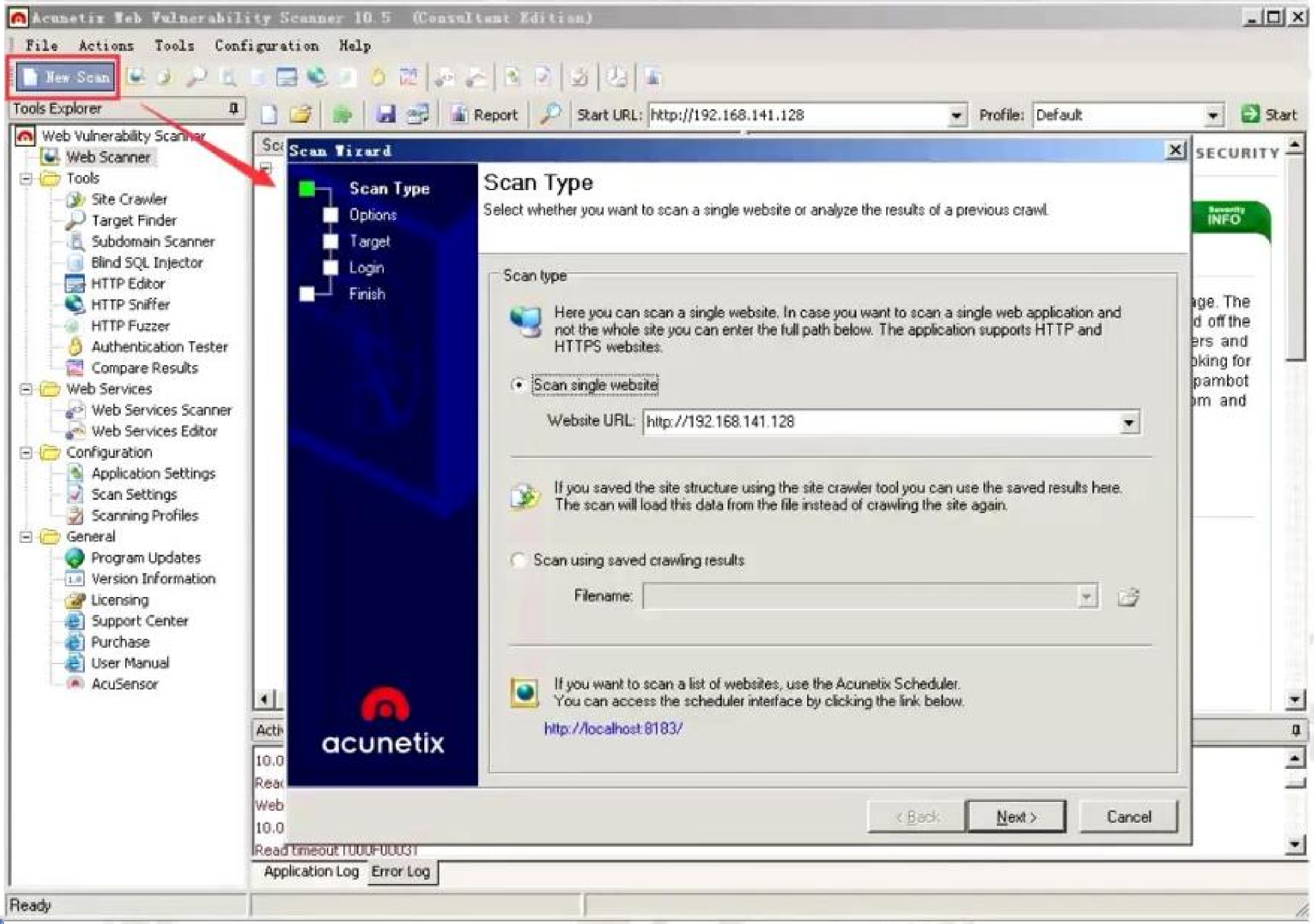
Acunetix Web Vulnerability Scanner 10.x Consultant Edition KeyGen By Hmily[LCG]

E-Mail:Hmily[at]52PoJie.Cn

□ MAKE BACKUP

- 之后我们将破解补丁移动到AWVS的安装目录，打开破解补丁。点击patch之后便可以完成破解，最后关闭破解补丁。

●AWVS—次新的扫描功能全面概述 Scan Type



Start URL: http://192.168.141.128

Profile: Default

Scan Type

Select whether you want to scan a single website or analyze the results of a previous crawl.

Scan type

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.

● Scan single website

Website URL: http://192.168.141.128

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.

○ Scan using saved crawling results

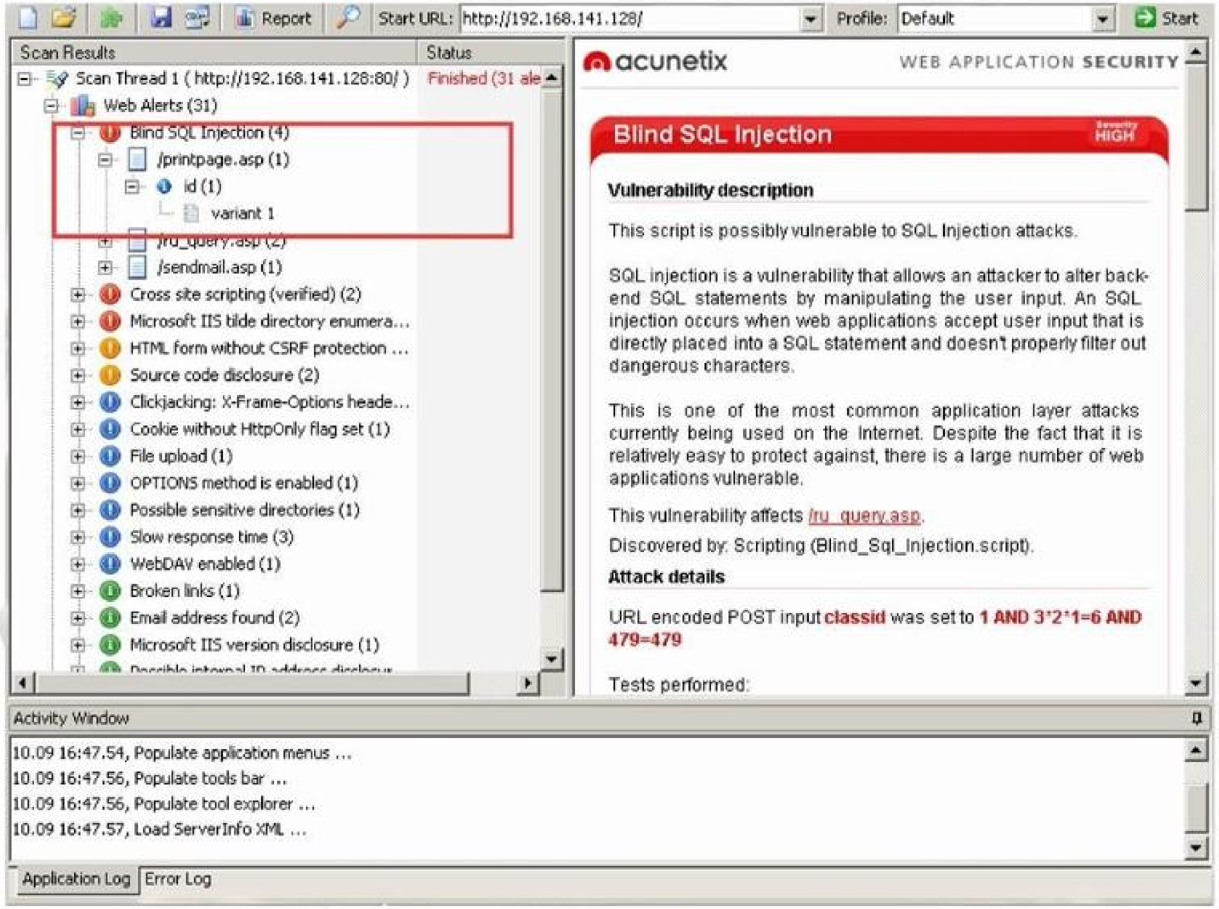
Filename:

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/

●AWVS一次新的扫描功能全面概述 报告分析

- 详情信息显示，需要点击左边的扫描结果才会展示详情信息。如下图就是左侧显示的SQL注入和参数，右边是SQL注入的详情



Scan Thread 1 (http://192.168.141.128:80/) — Finished (31 ale

- Web Alerts (31)
  - Blind SQL Injection (4)
    - /printpage.asp (1)
      - id (1)
        - variant 1
    - /ru_query.asp (2)
    - /sendmail.asp (1)
  - Cross site scripting (verified) (2)
  - Microsoft IIS tilde directory enumera…
  - HTML form without CSRF protection …
  - Source code disclosure (2)
  - Clickjacking: X-Frame-Options heade…
  - Cookie without HttpOnly flag set (1)
  - File upload (1)
  - OPTIONS method is enabled (1)
  - Possible sensitive directories (1)
  - Slow response time (3)
  - WebDAV enabled (1)
  - Broken links (1)
  - Email address found (2)
  - Microsoft IIS version disclosure (1)
  - Possible internal IP address disclosur

Blind SQL Injection

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects /ru_query.asp.

Discovered by: Scripting (Blind_Sql_Injection.script).

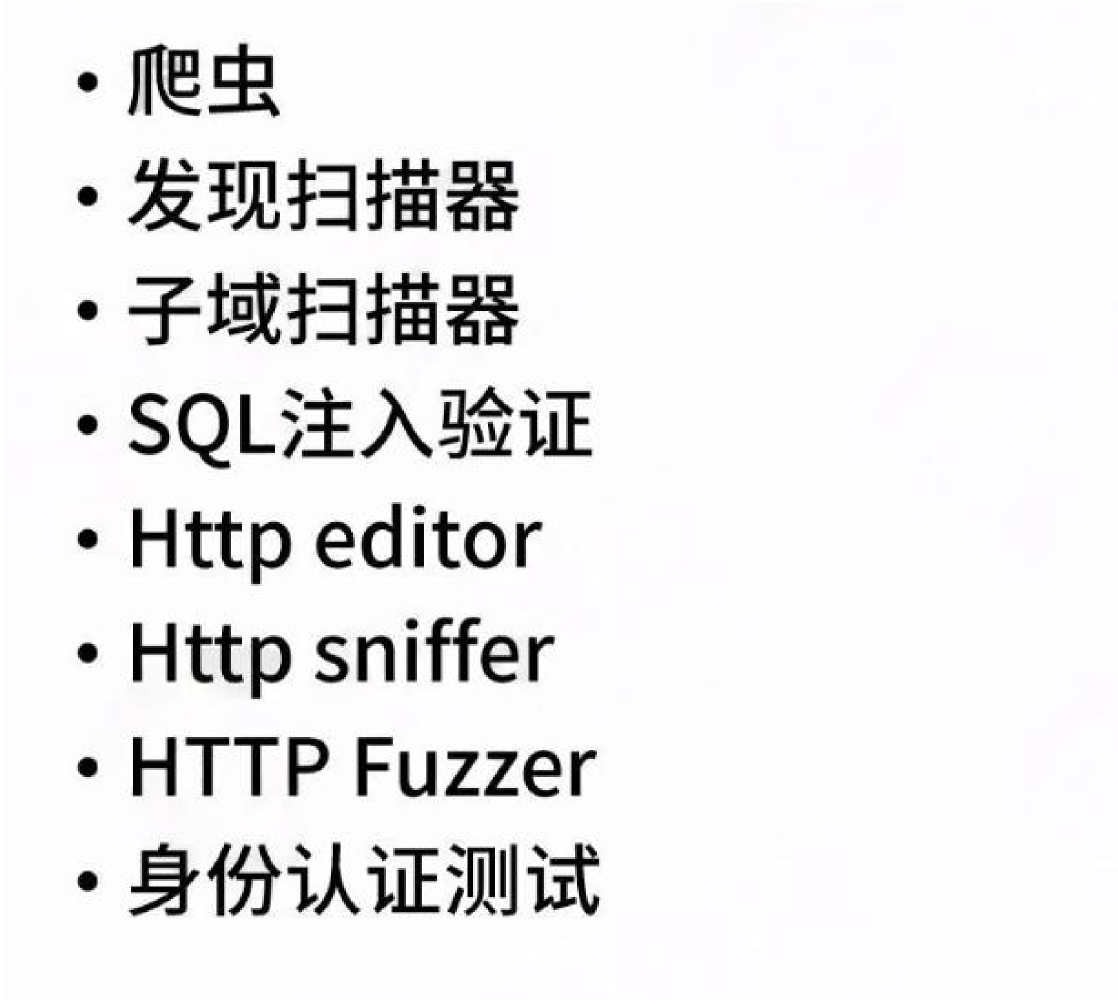
Attack details

URL encoded POST input **classid** was set to **1 AND 3*2*1=6 AND 479=479**

Tests performed:

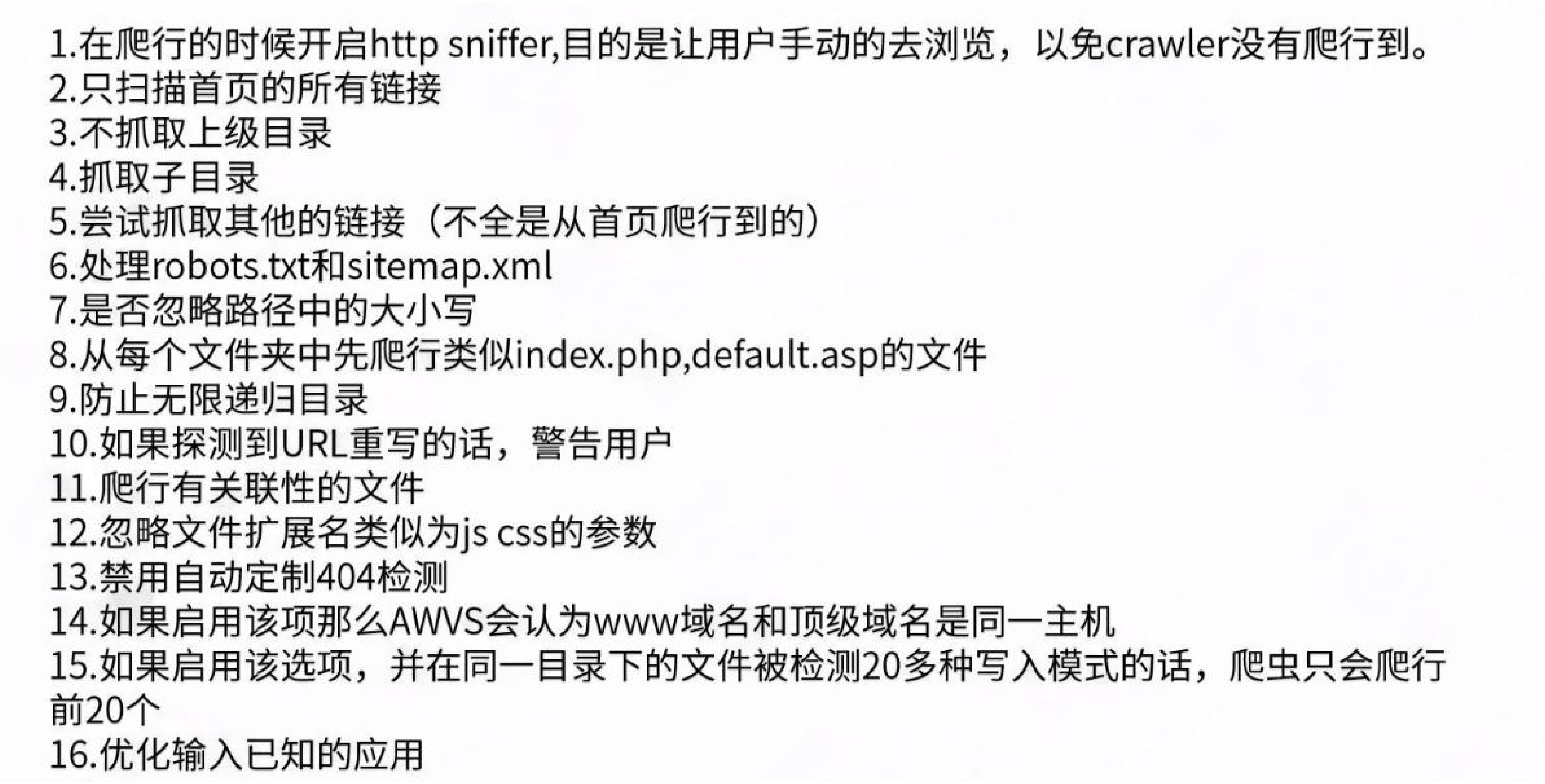
```
10.09 16:47.54, Populate application menus ...
10.09 16:47.56, Populate tools bar ...
10.09 16:47.56, Populate tool explorer ...
10.09 16:47.57, Load ServerInfo XML ...
```

●AWVS



- 爬虫
- 发现扫描器
- 子域扫描器
- SQL注入验证
- Http editor
- Http sniffer
- HTTP Fuzzer
- 身份认证测试

●AWVS 爬虫设置



1.在爬行的时候开启http sniffer,目的是让用户手动的去浏览，以免crawler没有爬行到。
2.只扫描首页的所有链接
3.不抓取上级目录
4.抓取子目录
5.尝试抓取其他的链接（不全是从首页爬行到的）
6.处理robots.txt和sitemap.xml
7.是否忽略路径中的大小写
8.从每个文件夹中先爬行类似index.php,default.asp的文件
9.防止无限递归目录
10.如果探测到URL重写的话，警告用户
11.爬行有关联性的文件
12.忽略文件扩展名类似为js css的参数
13.禁用自动定制404检测
14.如果启用该项那么AWVS会认为www域名和顶级域名是同一主机
15.如果启用该选项，并在同一目录下的文件被检测20多种写入模式的话，爬虫只会爬行前20个
16.优化输入已知的应用

●Nessus

- 家庭版
  - 免费、限制扫描16个IP地址
- 专业版
  - 收费、无限的并发连接
- 下载
  - https://www.tenable.com/downloads/nessus
- 安装
  - dpkg -i deb文件
  - 安装路径：/opt/nessus
- 启动服务
  - /etc/init.d/nessusd start

谢谢观赏