

PROFESSION INNOVATION FIGHTING PRICIPLE

COURSE NAME

AWVS使用

讲师：贾良超



课程任务及目标



课程目标

本节课程中我们主要学习使用AWVS工具的使用。



任务目标

通过本节课的学习，学会使用AWVS工具扫描网站，并灵活使用不同的扫描模块以应对不同的情况。



提交作业

根据本节课学习的内容，在平台上使用AWVS扫描目标网站，并且将扫描结果导出上交。



A. AWVS功能介绍

B. 使用AWVS扫描网站

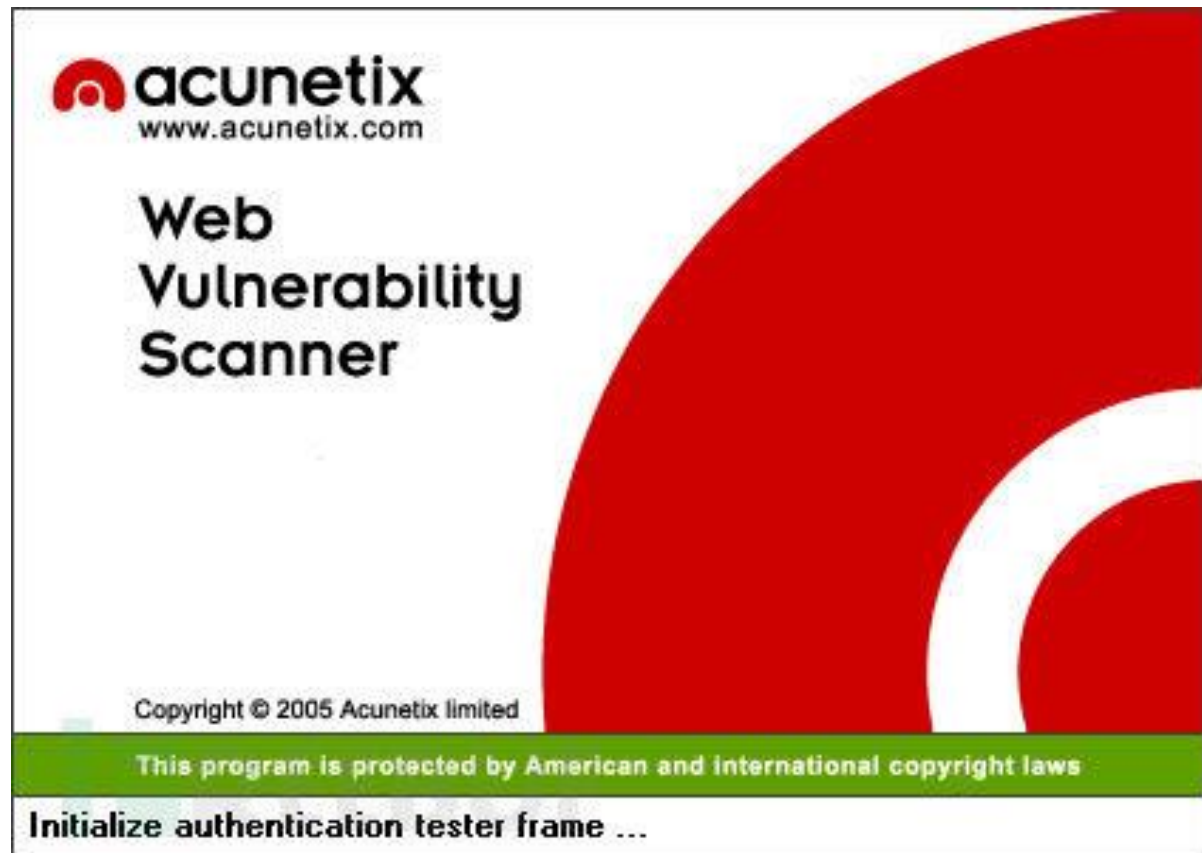
[1]
ANY

AWVS功能介绍

AWVS界面

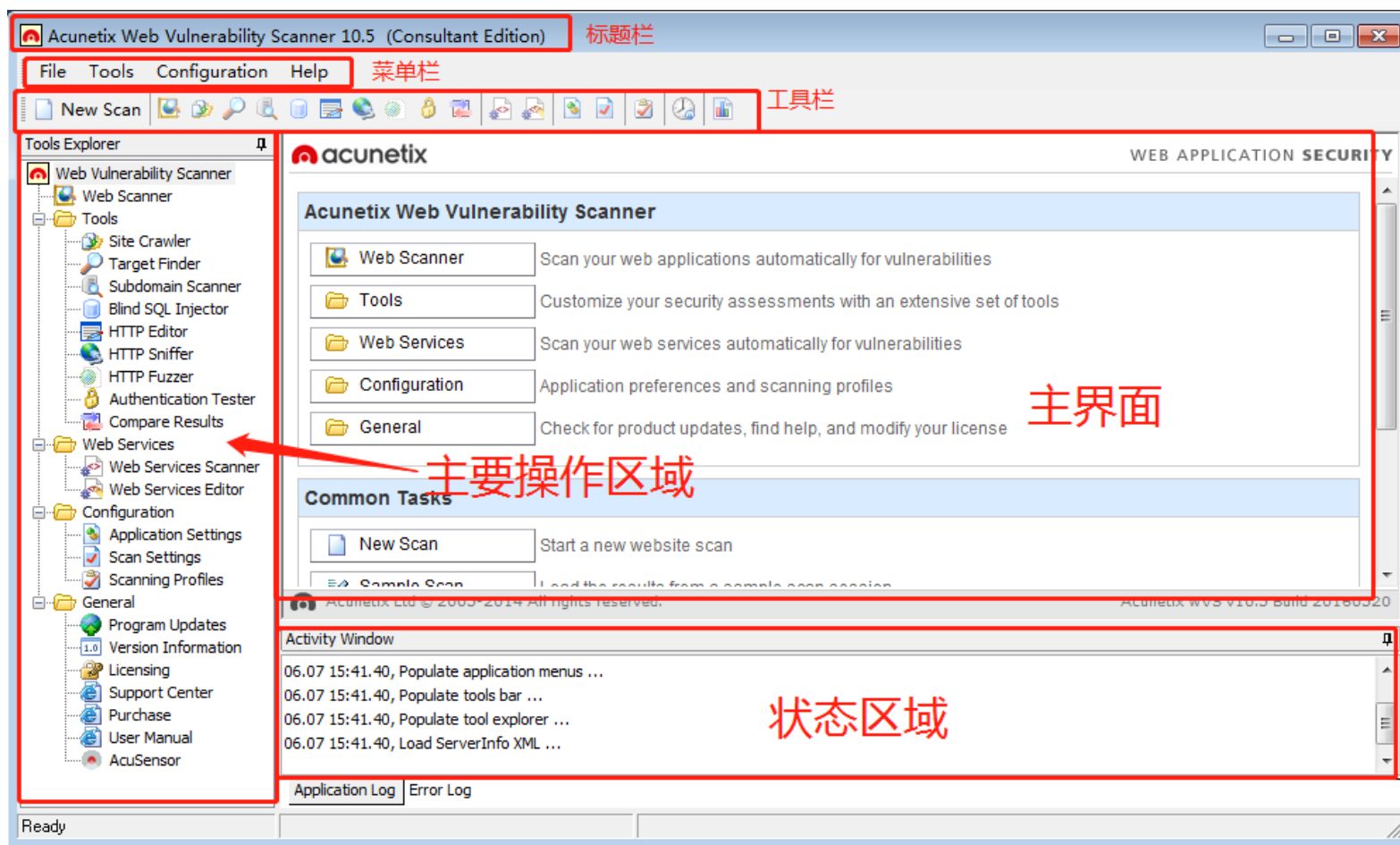
经过上一章的学习，我相信同学们对于awvs已经有了一定的了解，那么这节课我们就来学习一下awvs这款软件。

Acunetix Web Vulnerability Scanner（简称AWVS）是一款知名的网络漏洞扫描工具，它通过网络爬虫测试你的网站安全，检测流行安全漏洞。目前最新版是V10.5版本。awvs有收费和免费两种版本，一般个人用户使用免费版本就可以了。



awvs界面

awvs的界面主要分为六个部分，分别是：标题栏、菜单栏、工具栏、主要操作区域、主界面、状态区域。



主要操作区域简介

Web Vulnerability Scanner (网站漏洞扫描)	
webscan	整站扫描
Tools (工具)	
Site Crawler	网站爬行
Target Finder	可用指定网段, 开放指定端口的服务器
Subdomain Scanner	子域名扫描
Blind SQL Injection	SQL盲注手工测试
HTTP Editor	HTTP信息查看编辑
HTTP Sniffer	HTTP监听嗅探
HTTP Fuzzer	HTTP模糊测试
Authentication Tester	HTTP认证测试
Compaer Results	对比两次Acunetix扫描结果
Web Services (web服务)	
Web Services Scanner	网站服务扫描
Web Services Editor	网站服务手动分析
Configuration (配置)	
Application Settings	应用程序设置
Scan Settings	扫描设置
Scanning Profiles	配置所用扫描脚本
General (一般)	
Program Updates	程序升级
Version Information	版本信息
Licensing	许可证信息
Support Center	支持中心
Purchase	购买正版
User Manual	用户手册
Acunetix	Acunetix传感器功能介绍



A. AWVS功能介绍

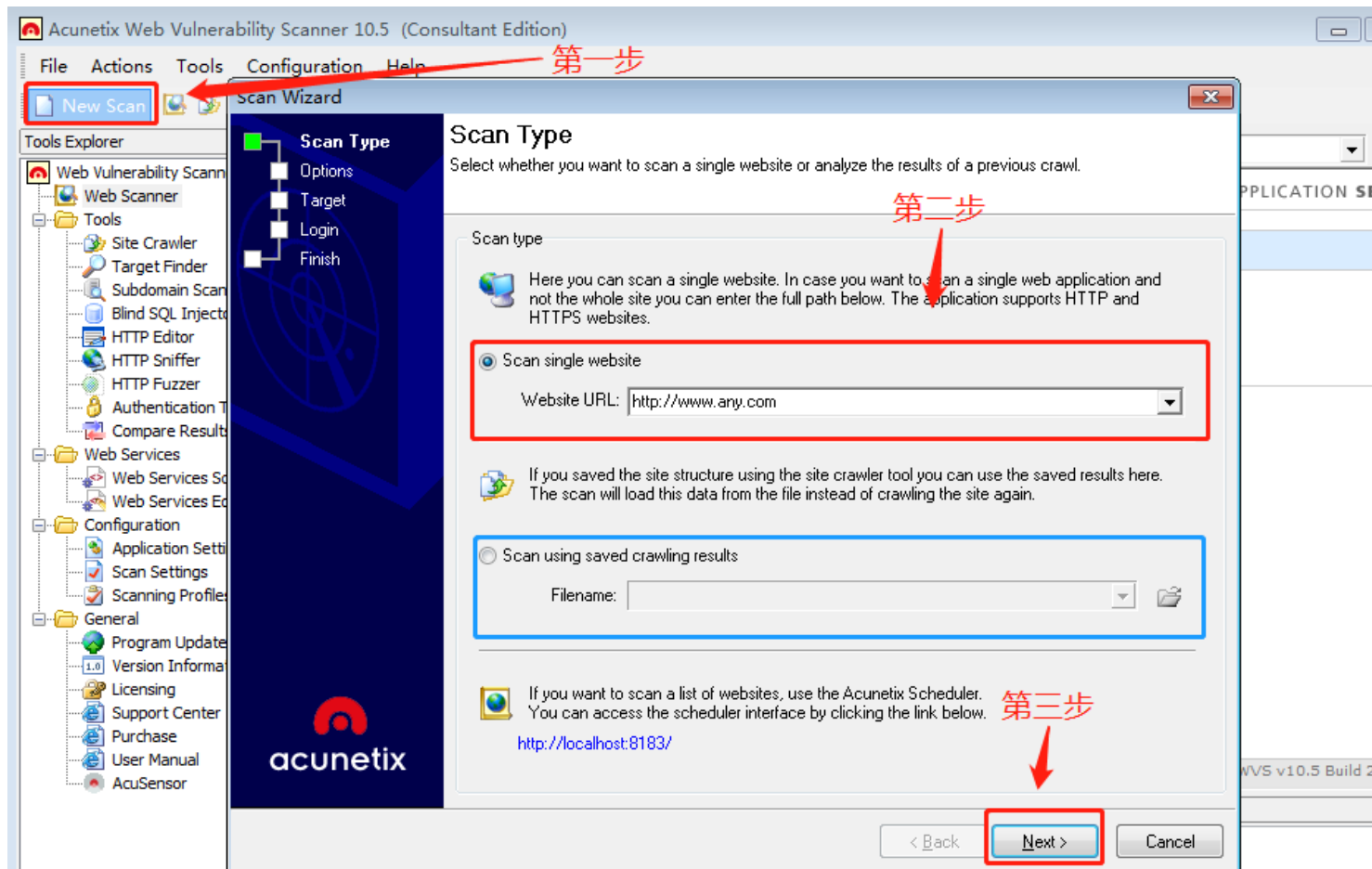
B. 使用AWVS扫描网站

[2]
ANY

使用awvs扫描网站

创建扫描项目

在之前的章节中讲了awvs的操作界面，这节课通过具体的实验，来实际操作awvs。



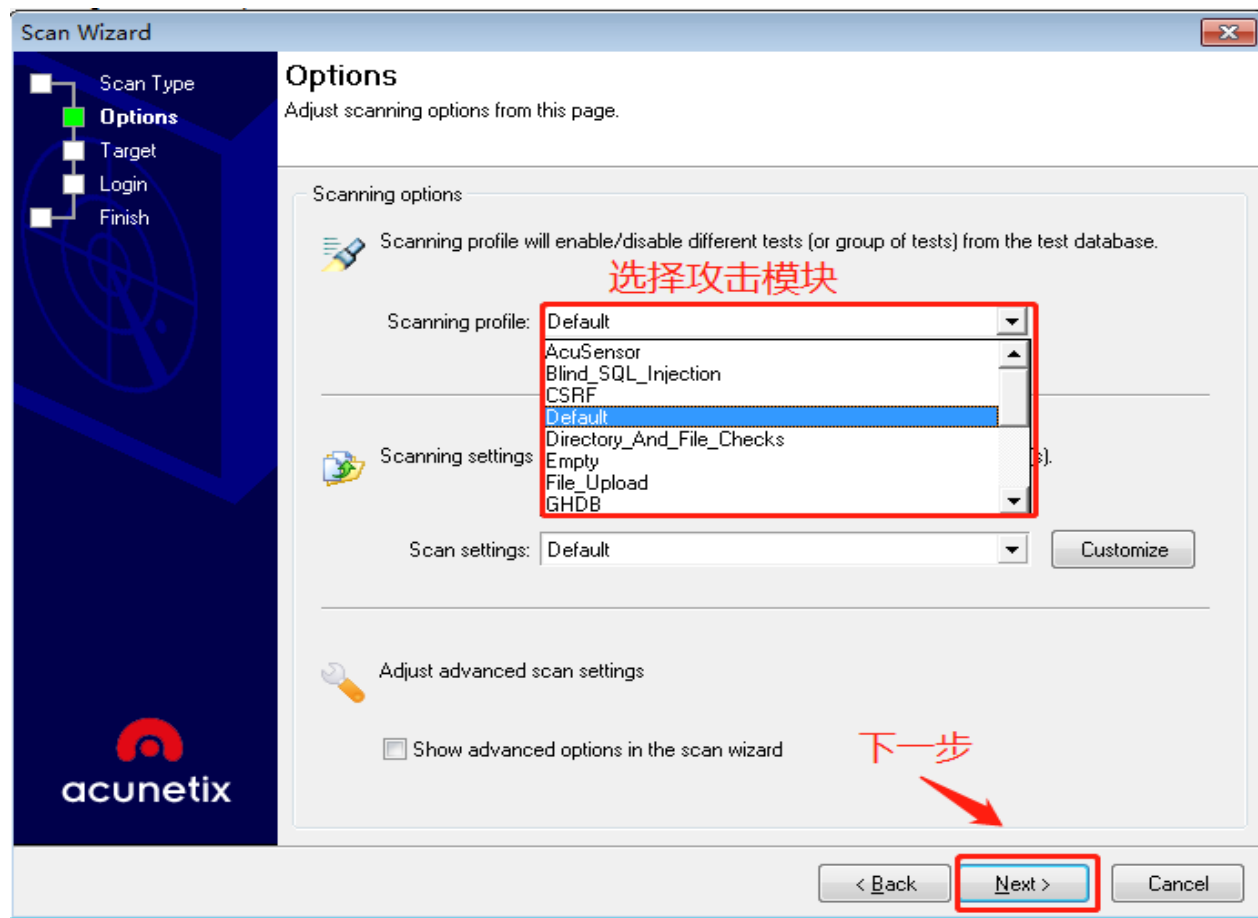
第一步Scan Type:

如图，首先选择图中的第一个红框 New Scan，然后在弹出的窗口中选择图中的第二个红框，在输入框里边输入将要检测的目标网站的URL，然后点击下边的Next即可。蓝框是我们额外讲的，这个的内容就是说如果我们之前曾经使用爬虫爬过目标网站，我们就可以使用蓝框来加载保存的文件继续爬行，不过这个实验因为我们是第一次爬行这个网站，所以并不需要使用这个。

创建扫描项目

第二步：

如图，这个界面是让我们选择攻击模块的，可以根据不同的攻击要求，选择不同的攻击模块，这里我们选择Default（默认），使用默认模块即可。



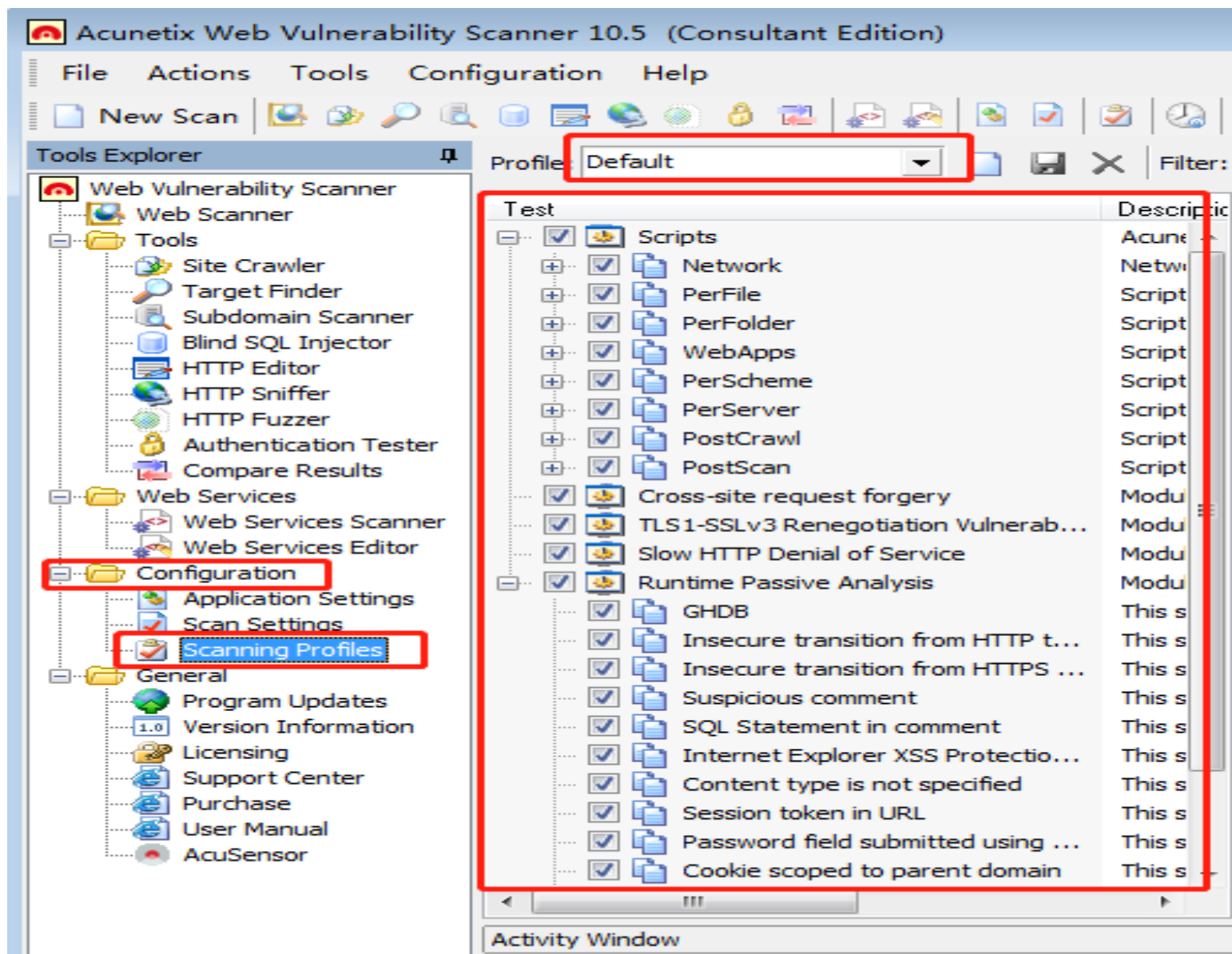
创建扫描项目

awvs一共有提供16种攻击模块，如下表：

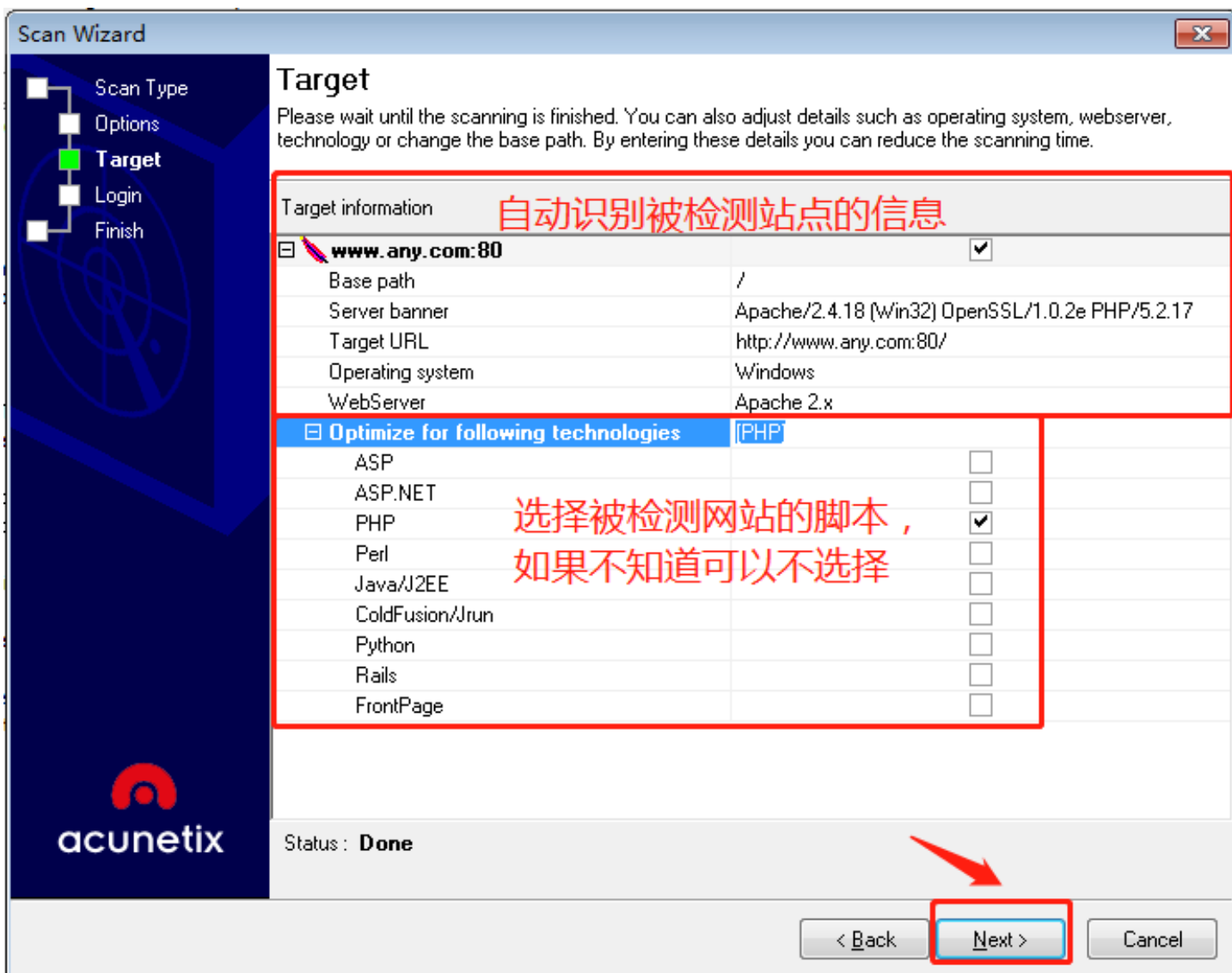
Defalut	默认，全部检测
AcuSensor	Acunetix传感器机制，可提升漏洞审查能力，需要在网站上安装文件，目前针对ASP.NET/PHP
Blind SQL Injertion	SQL盲注检测
CSRF	检测跨站请求伪造
Directory And File Checks	目录与文件检测
Empty	不使用任何检测
GHDB	利用Google hacking数据库检测
High Risk Alerts	高风险警告
Network Scripts	网络脚本检测
Parameter Manipulations	参数操作
Sql Injection	SQL注入检测
Text Search	文本搜索
Weak Passwords	检测弱口令
Web Applications	web应用检测
XSS	跨站请求伪造
File Upload	检测文件上传漏洞

创建扫描项目

如果想要调整或修改攻击模块，根据路径Configuration >> Scanning Profiles修改，如图：



创建扫描项目



第三步:

如图, awvs会自动识别被检测站点的信息, 在这个页面显示出来, 还可以选择目标网站的脚本语言, 如果不知道, 可以不选择, 直接点击下一步即可。

其中target information中的内容是:

- base path: 扫描目标的根路径
- server banner: 服务的banner
- target URL: 目标url
- operating system: 目标操作系统
- webserver: 目标的web服务器

创建扫描项目

第四步：

如图，根据需求，可以录入或者填写登录信息，如果没有的话，直接按照默认设置，然后点击“Next”

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 required to login 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:

Automatic Forms Authentication

☒ Try to auto-login into the site

Website's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified.

Please enter your credentials below.

Username:

Password:

< Back Next > Cancel

创建扫描项目

如果网站需要登录，则需要提供登录信息，否则有些需要登录才能操作的页面就无法探测到。

1) Use pre-recorded login sequence选项，第一个红圈：

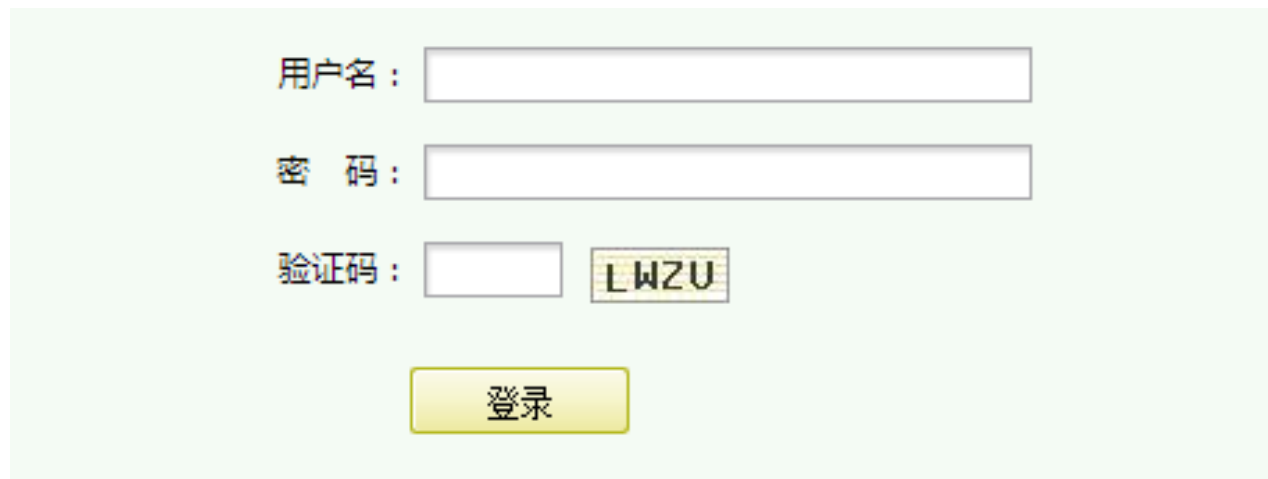
黄色圈内：可直接打开AWVS的内置浏览器，录制登录被测网站的脚本

蓝色圈内：可导入已经录制好的登录脚本

2) Try to auto-login into the site选项，第二个红圈：

可直接输入登录网站所需的账户名和密码，然后AWVS用自动探测技术进行识别，不需要手工录入登录过程。

这里因为我们将要访问的网站是不需要直接登录就能访问的网站，所以这里就不在细说。



用户名：

密 码：

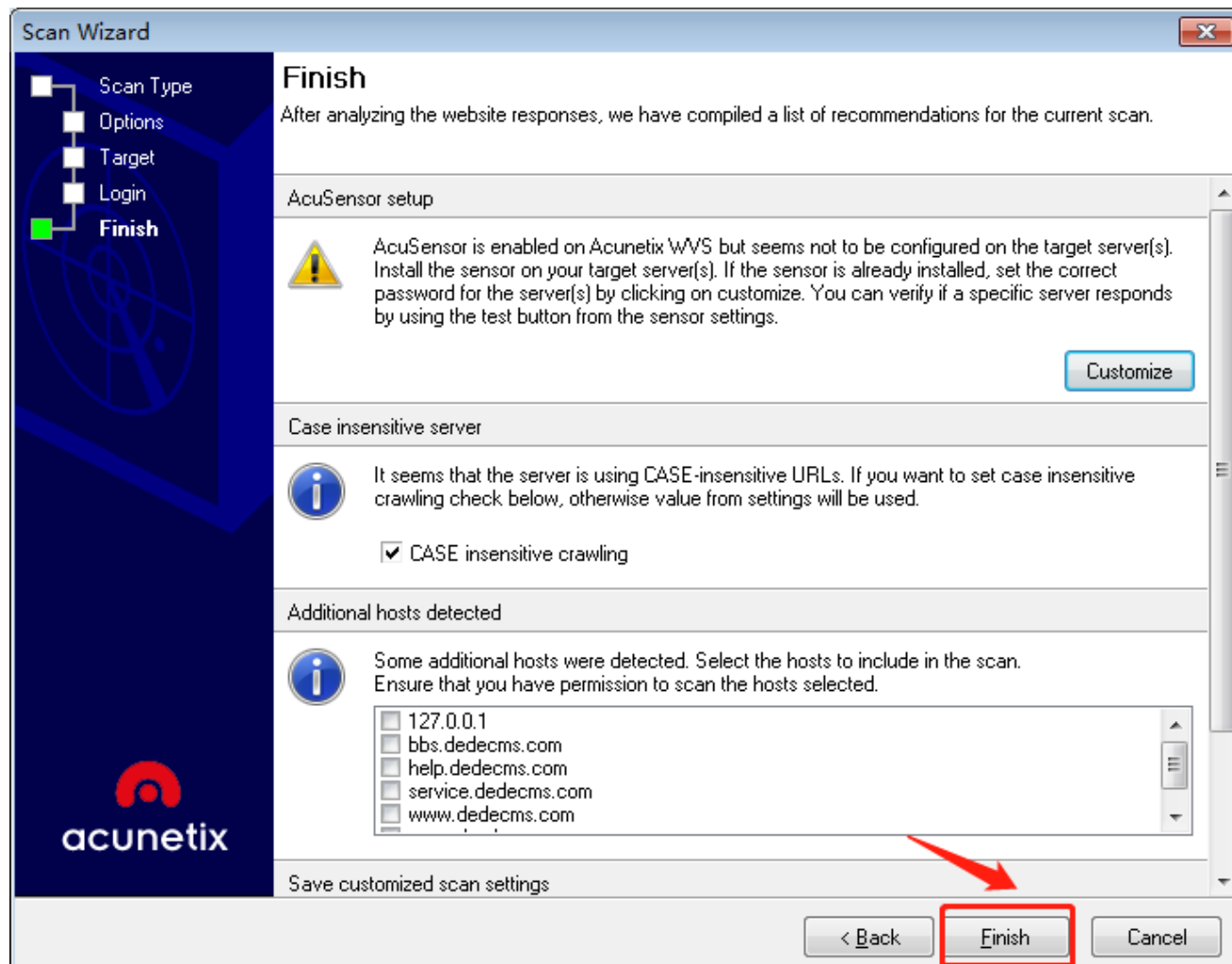
验证码： LWZU

登录

创建扫描项目

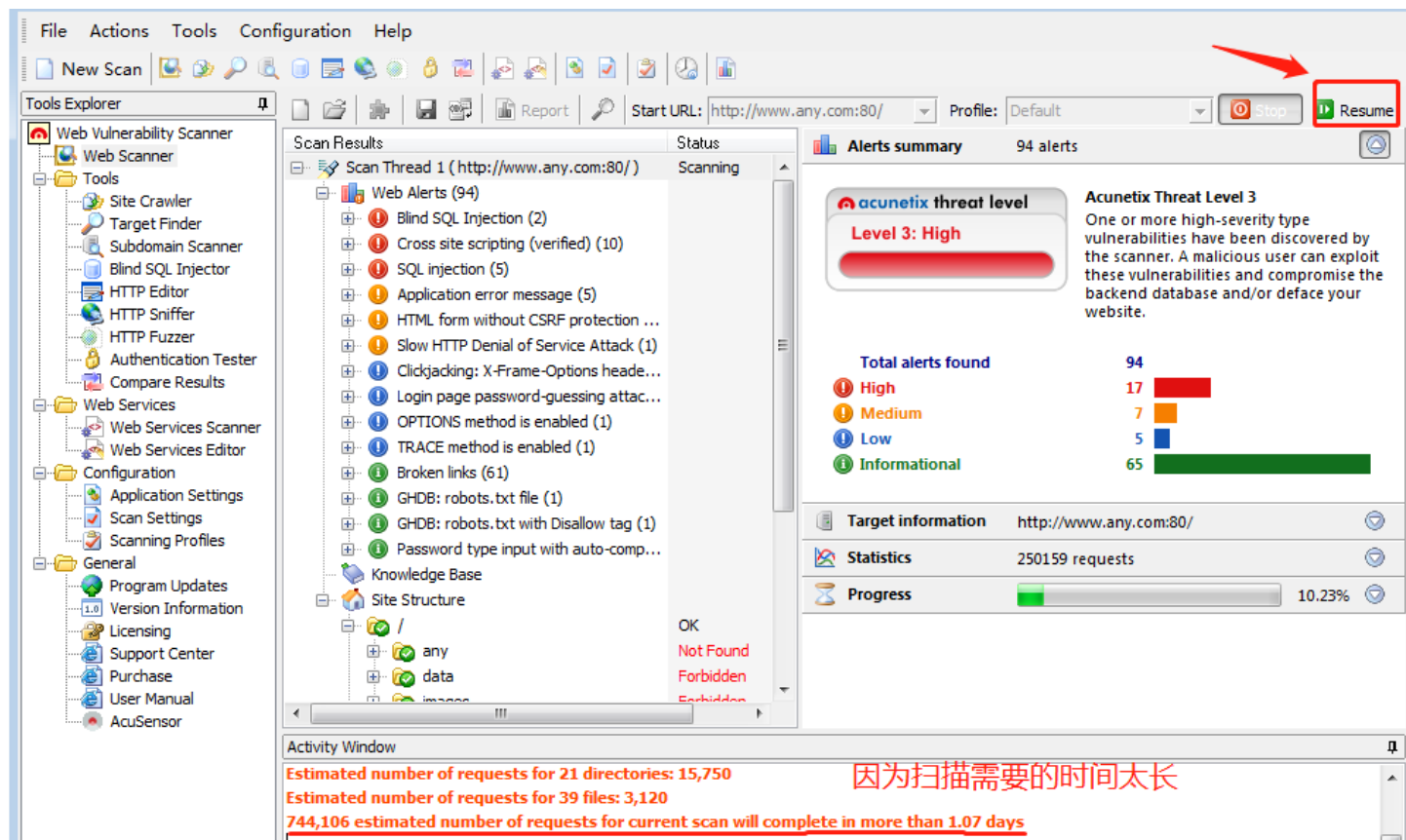
第五步：

如图，直接点击Finish即可。之后awvs会对目标网站进行扫描，然后需要耐心等待扫描完成。



查看扫描结果

如图，既是在上一节中创建的扫描项目“www.any.com”的扫描结果。因为目标网站太大，所以要完全扫描完成需要较长的时间，所以这次就先在扫到10%的时候暂停，使用已经扫描得到的结果检测网站的漏洞。暂停按钮在界面的右上方的Pause（暂停），图片上是已经点击暂停之后的界面，所以显示的是Resume（继续）。



查看扫描结果

在成功暂停之后，观察下图，可以看到，一共分为了三个板块，左边红框框起来的是已经发现的漏洞详情，右侧上方红框框起来的是发现的高中低危漏洞以及无关紧要的信息。通过颜色也可以看出来，高危漏洞是红色的，中危漏洞是黄色的，低危漏洞是蓝色的，而绿色的是危害很小的信息。右侧下方中划红线的是扫描进度，可以看出来我们这次扫描只进行了10.23%就结束了。

The screenshot displays the Acunetix Web Vulnerability Scanner interface. The left sidebar contains a 'Tools Explorer' with various tools like Site Crawler, Target Finder, and Subdomain Scanner. The main area is divided into three sections:

- Scan Results (Left):** A list of detected vulnerabilities under 'Web Alerts (94)'. A red box highlights the following items:
 - Blind SQL Injection (2)
 - Cross site scripting (verified) (10)
 - SQL injection (5)
 - Application error message (5)
 - HTML form without CSRF protection ...
 - Slow HTTP Denial of Service Attack (1)
 - Clickjacking: X-Frame-Options heade...
 - Login page password-guessing attac...
 - OPTIONS method is enabled (1)
 - TRACE method is enabled (1)
 - Broken links (61)
 - GHDB: robots.txt file (1)
 - GHDB: robots.txt with Disallow tag (1)
 - Password type input with auto-comp...
- Alerts summary (Right):** A summary of 94 alerts. A red box highlights the 'Acunetix threat level' section, which shows 'Level 3: High'. Below this, a table shows the distribution of alerts by severity:

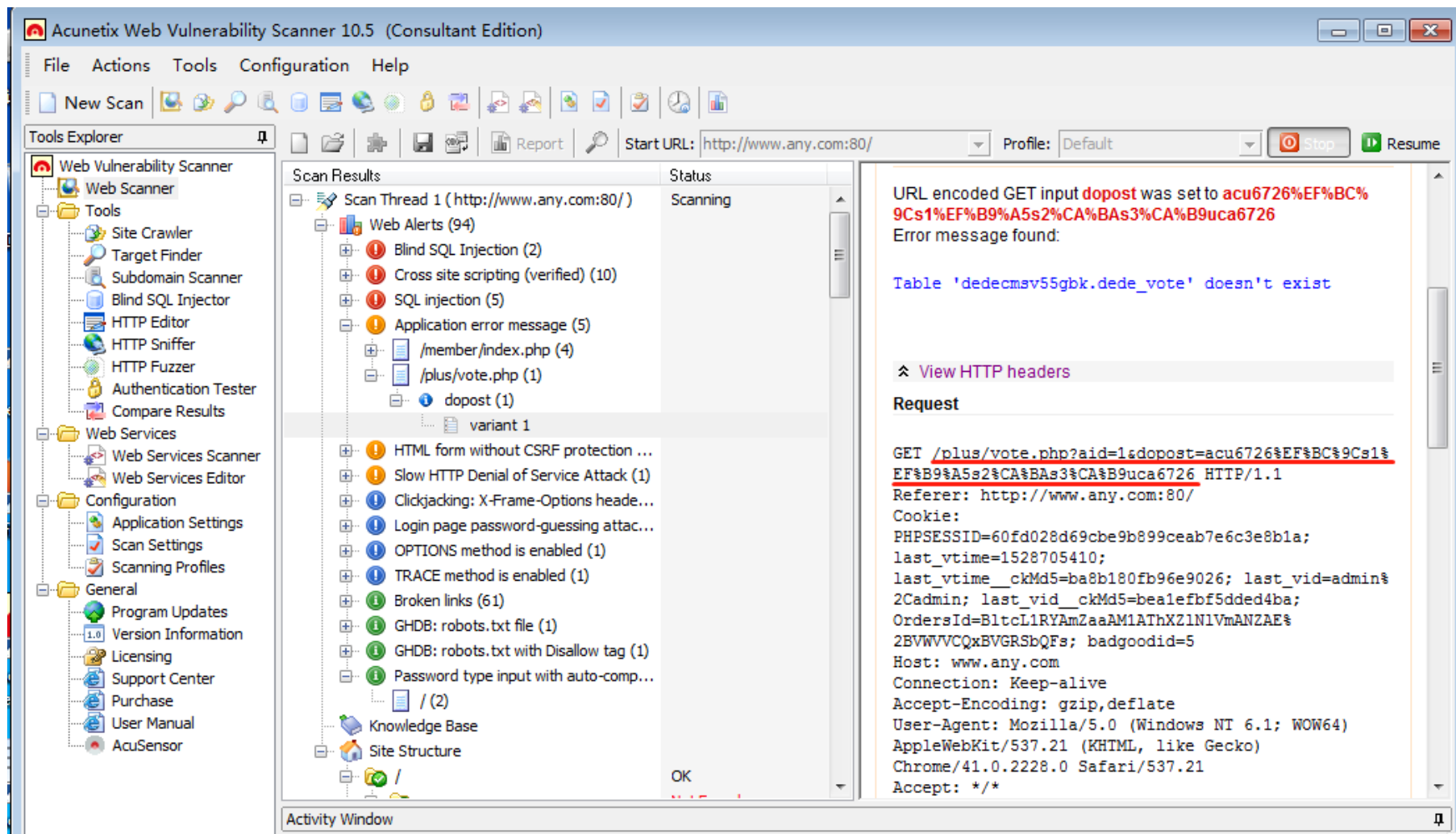
Severity	Count
High	17
Medium	7
Low	5
Informational	65
- Progress (Bottom Right):** A progress bar indicating the scan is at 10.23% completion. A red line is drawn under the progress bar.

Red annotations on the image include:

- '已经发现的漏洞' (Already discovered vulnerabilities) pointing to the 'Total alerts found' section.
- '检测进度' (Detection progress) pointing to the progress bar.
- '发现的漏洞详情' (Details of discovered vulnerabilities) pointing to the 'Scan Results' list.

The bottom status bar shows estimated request counts: 15,750 for 21 directories, 3,120 for 39 files, and a total of 744,106 estimated requests for the current scan, which will complete in more than 1.07 days.

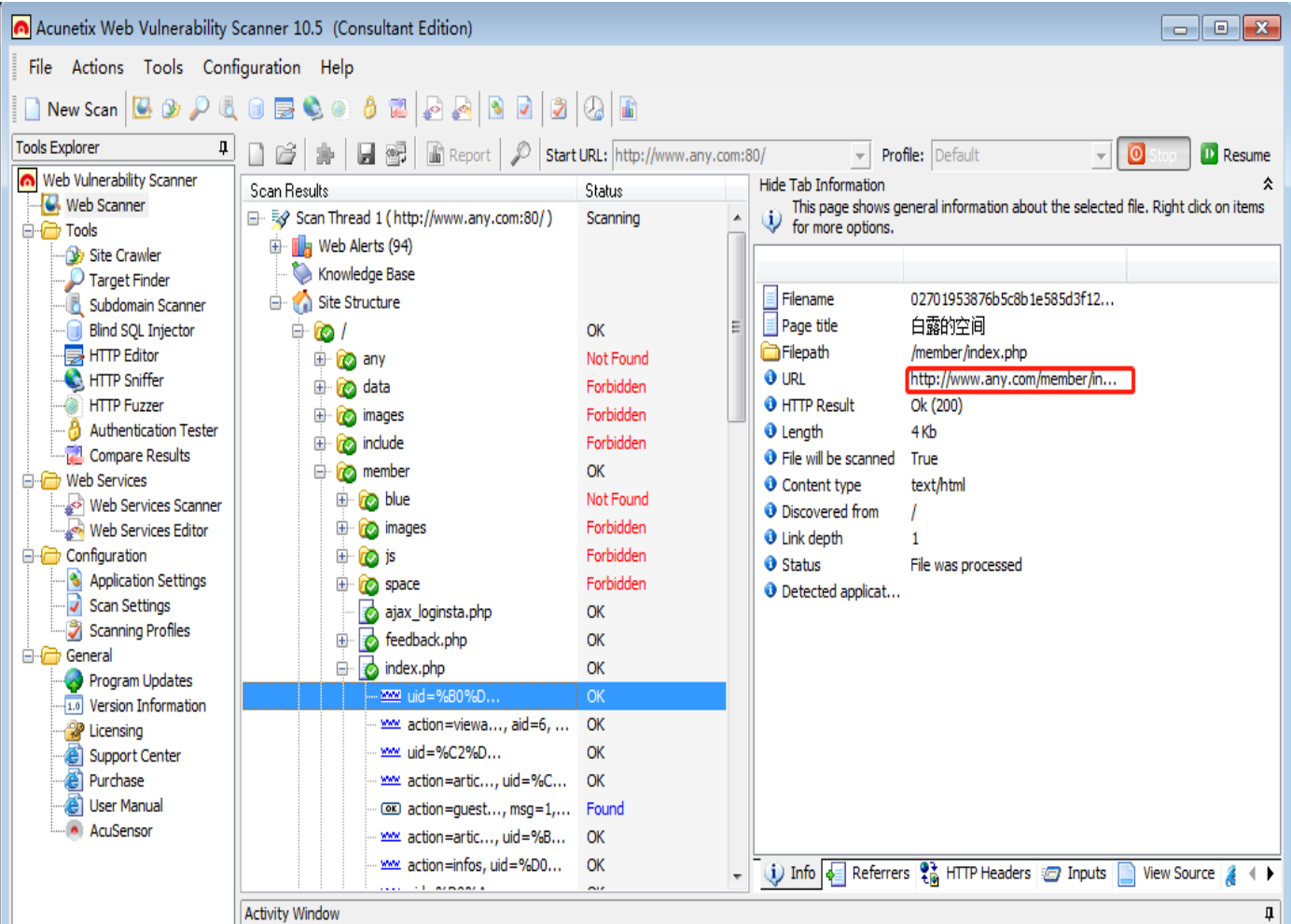
如图，我们随便点开一个漏洞，然后将划红线的写入浏览器的url中



如图。从图中可以看到，在错误信息中，该系统使用的数据库与数据表的名字泄露了，而这些本来应该是非常机密的信息。



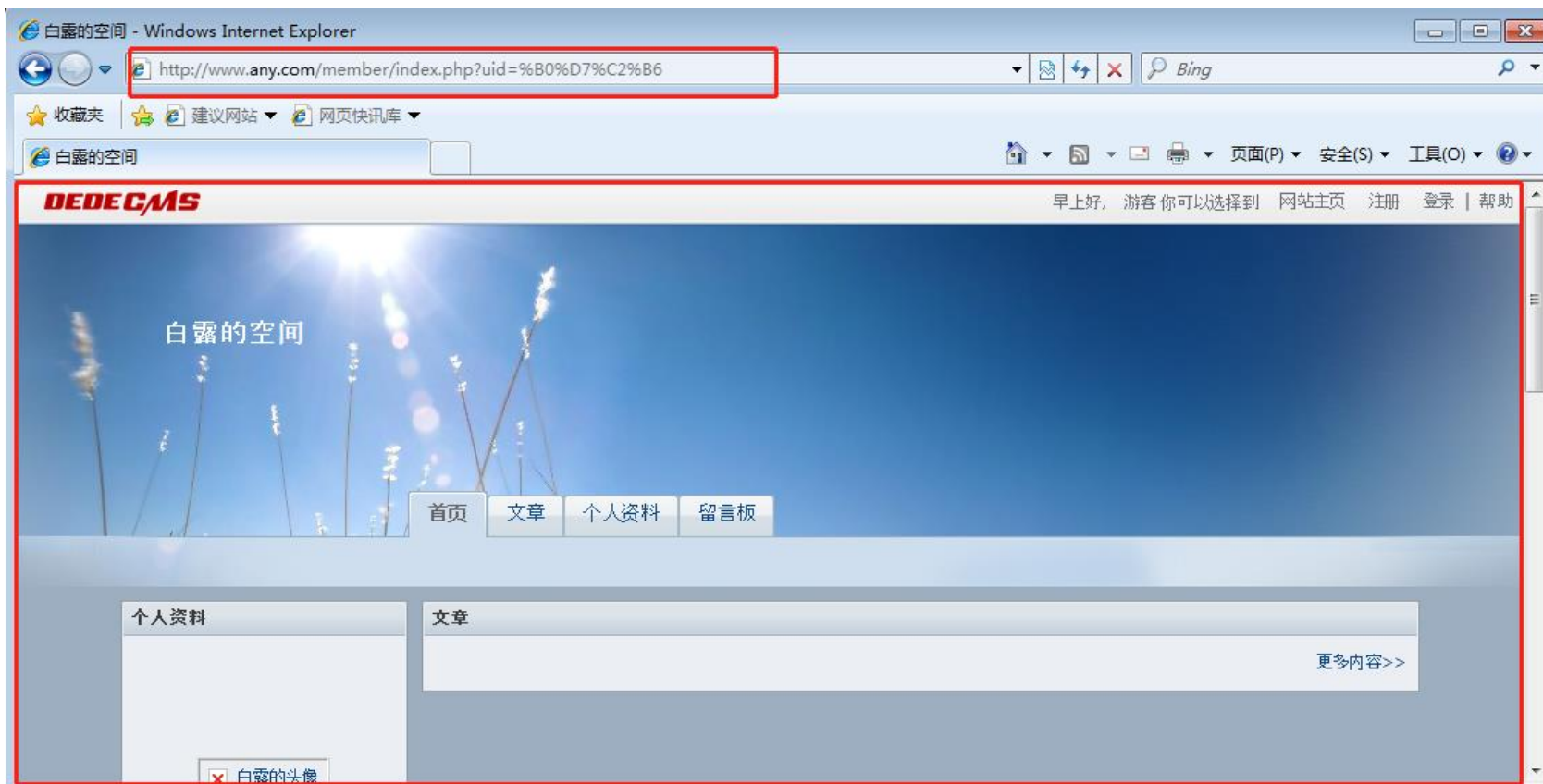
贴讲地址栏。



查看扫描出的网站结构

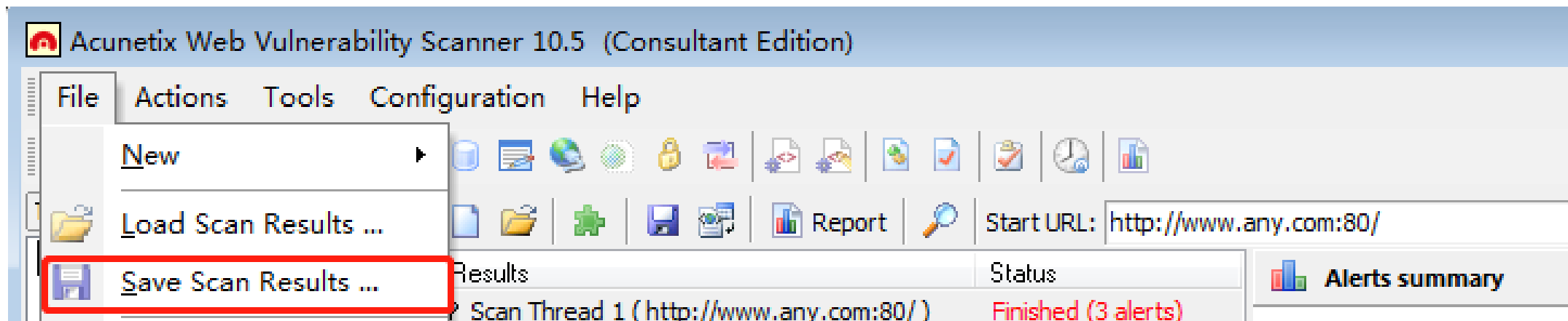
从图中可以看到，通过在地址栏输入URL之后，就可以直接进入用户“白露”的空间，并不需要进行登录的操作。

通过这个例子同学们应该已经明白了awvs的强大之处。



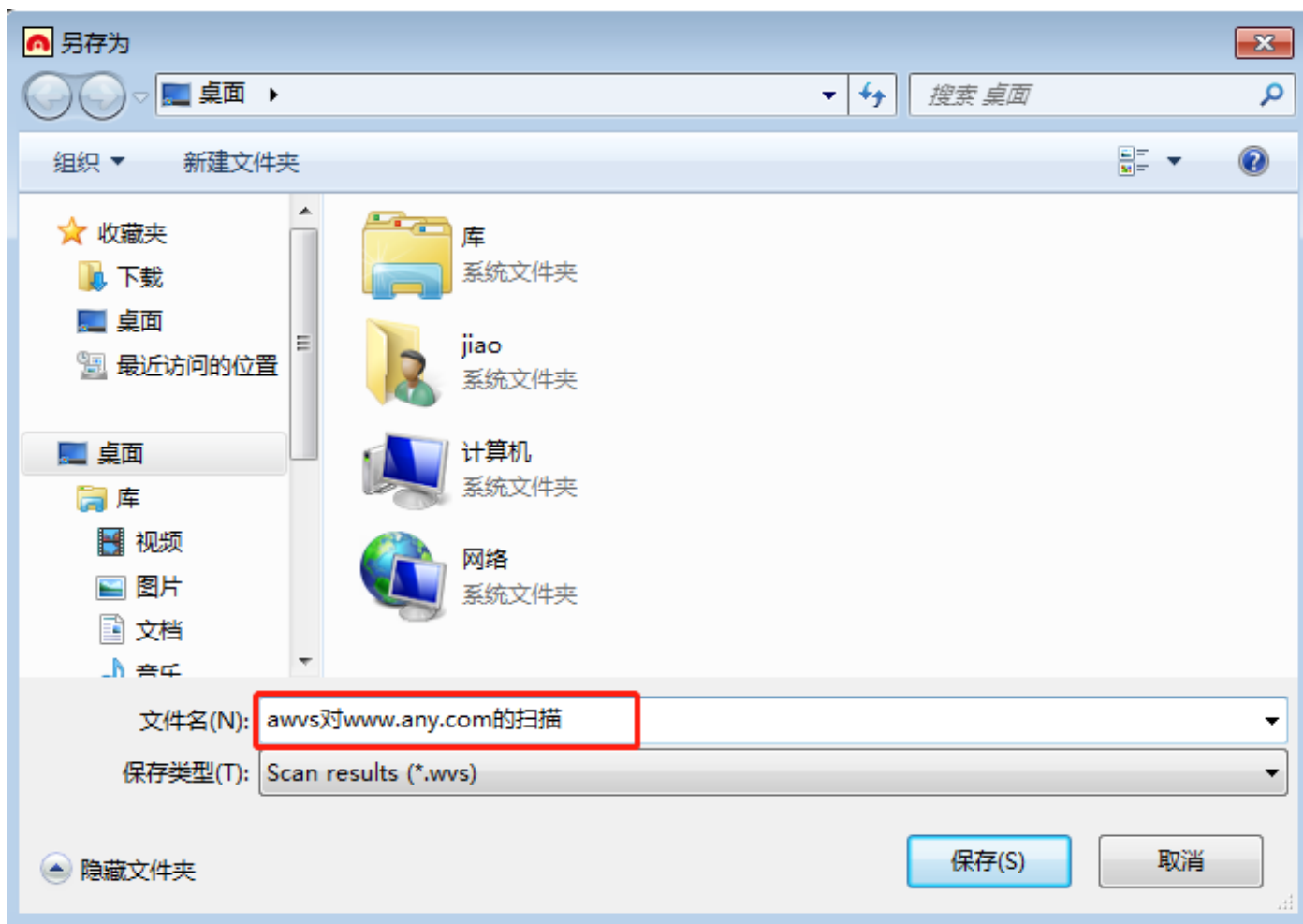
保存扫描结果

在扫描完成后（必须是扫描全部完成后，才可以保存扫描结果。因为目标网站实在太大，扫描用时过长，同学们可以选择新建对www.any.com/2.php进行扫描，很快就可以扫描完成，然后就可以针对这次扫描保存扫描结果，在本节课的图片中我使用的还是www.any.com这个网站）。选择，File→Save Scan Results，如图：



保存扫描结果

输入文件名称后，选择保存即可。如图



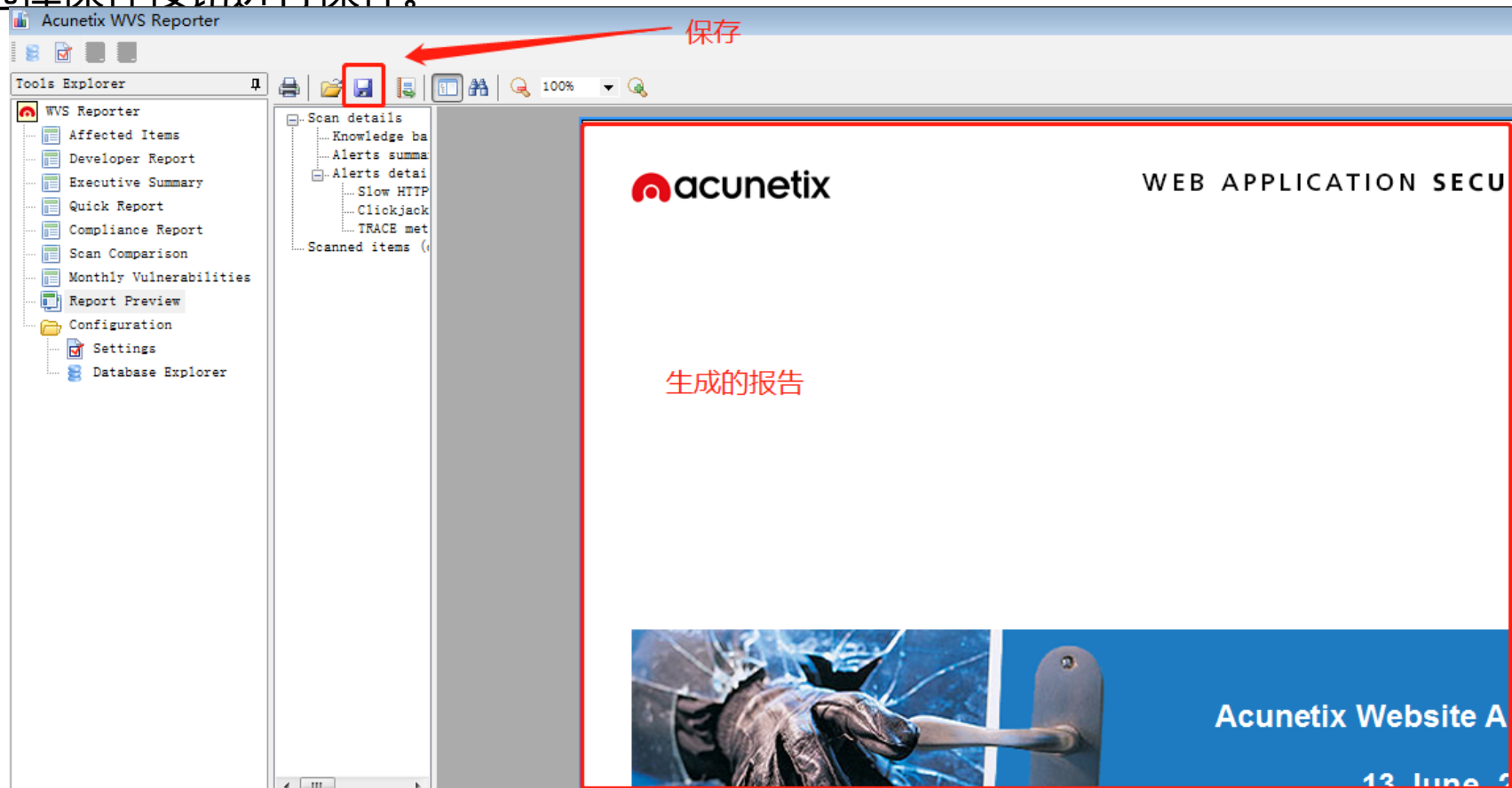
导出扫描报告

在扫描完成后，找到工具栏里的report，如图



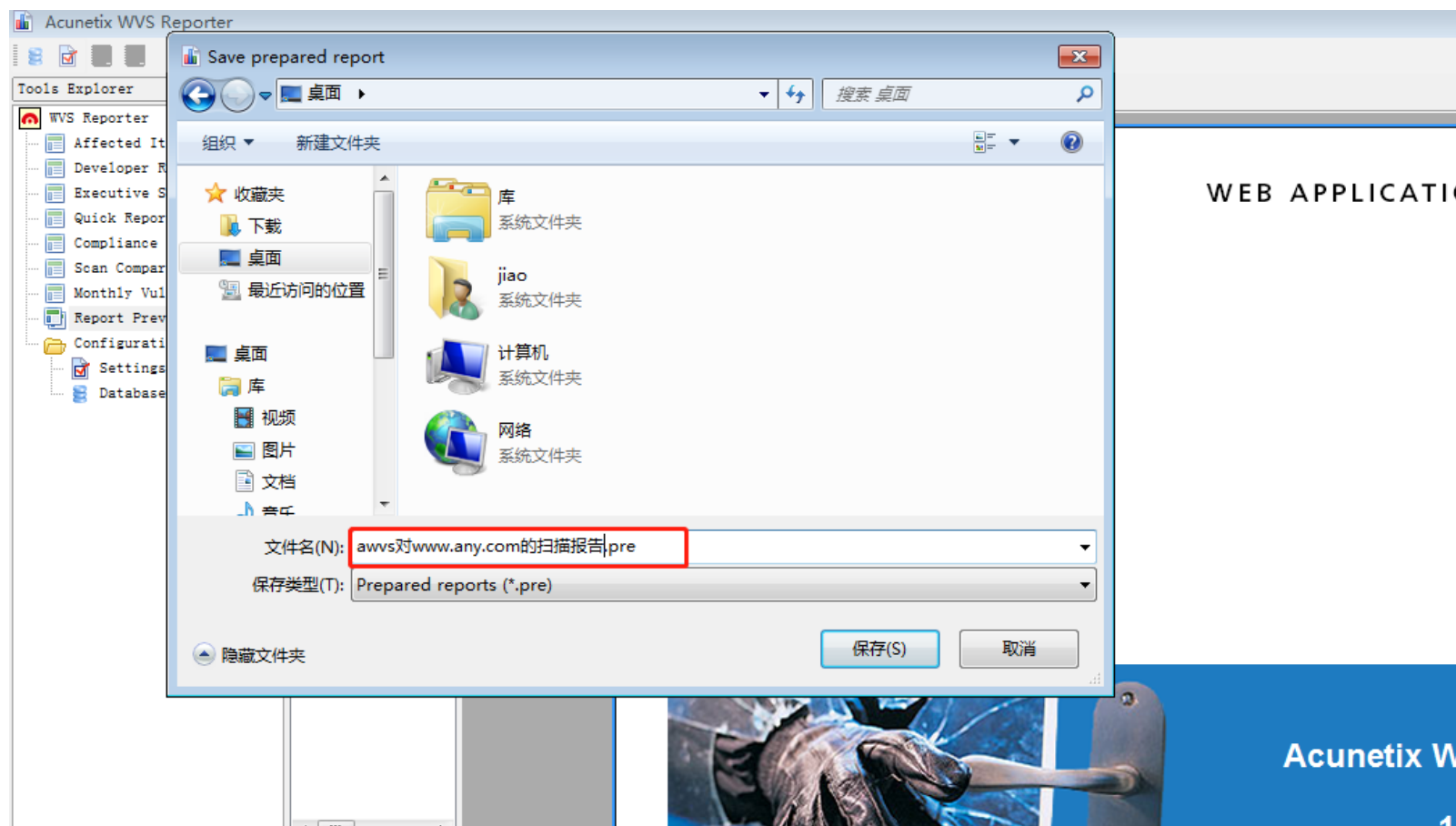
导出扫描报告

然后就会出现扫描报告的预览图，如图，其中红色框起来的位置就是扫描报告的预览图，选择保存按钮进行保存。



导出扫描报告

输入文件名称后，选择保存即可。如图



Thanks!

变革创新，服务无限