Acunetix Web Vulnerability Scanner

Contents

1. *Installation*
    1.1 Introduction to Acunetix WVS Files/Directories
2. *File*
    2.1 Web Site Scan
    2.2 Web Site Crawl
    2.3 Web Service Scan
    2.4 Report
    2.5 Load Scan Results
    2.6 Save Scan Results
3. *Actions*
    3.1 Import from Firefox Extension
    3.2 Export to AVDL
    3.3 Export to XML
    3.4 Export to Imperva WAF
    3.5 Edit with HTTP Editor
    3.6 Export to HTTP Fuzzer
    3.7 Export to Blind SQL Injector
    3.8 Retest alert(s)
4. *Tools*
    4.1 Web Scanner
    4.2 Site Crawler
    4.3 Target Finder
    4.4 Subdomain Scanner
    4.5 Blind SQL Injector
    4.6 HTTP Editor
    4.7 HTTP Sniffer
    4.8 HTTP Fuzzer
    4.9 Authentication Tester
    4.10Compare Results
    4.11Web Services Scanner
    4.12Web Services Editor
    4.13Vulnerability Editor
    4.14Scheduler
    4.15Reporter
5. *Configuration*
    5.1 Application Settings
    5.2 Scan Settings
    5.3 Scanning Profiles
6. *Appendix*

Installation

测试环境:

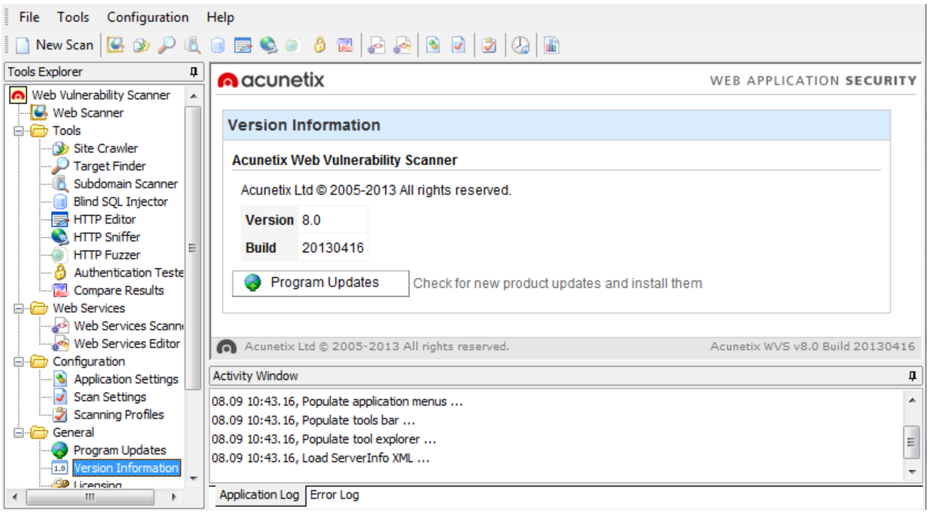
- 系统名称:　　　Microsoft Windows 7 Ultimate (x86)
- 系统版本:　　　6.1.7601 Service Pack 1 Build 7601
- Acunetix 版本:　8.0

最低系统配置要求:

- 操作系统: Microsoft Windows XP 或较新版本
- CPU:32 位或 64 位
- 系统内存:最小 2GB RAM
- 存储空间:200M 可用磁盘空间
- IE7 或较新版本:Acunetix 会调用 IE 浏览器的部分组件
- 可选:Microsoft SQL Server 用作报告数据库，默认使用 Access(不需安装 Microsft Access)

安装:

1. 下载最新版 Acunetix Web Vulnerability Scanner
2. 双击 webvulnscan8.exe 进行安装
3. 证书认证
4. 选择安装文件夹
5. 使用使用 Acunetix FireFox 插件(可用于扫描当前浏览的页面)或桌面快捷方式



Version Information

Acunetix Web Vulnerability Scanner

Acunetix Ltd © 2005-2013 All rights reserved.

Version	8.0
Build	20130416

Check for new product updates and install them

Acunetix Ltd © 2005-2013 All rights reserved.　Acunetix WVS v8.0 Build 20130416

```
08.09 10:43.16, Populate application menus ...
08.09 10:43.16, Populate tools bar ...
08.09 10:43.16, Populate tool explorer ...
08.09 10:43.16, Load ServerInfo XML ...
```

Introduction to WVS Files/Directories

Acunetix WVS 安装完成后，有效目录如下:

- C:\Program Files\Acunetix\Web Vulnerability Scanner 8
- C:\ProgramData\Acunetix WVS 8
- C:\Users\someone\Documents\Acunetix WVS 8
- C:\Users\Public\Documents\Acunetix WVS 8

C:\Program Files\Acunetix\Web Vulnerability Scanner 8	
AcuSensor	传感器机制(一般为空)
BlindSQL	盲注(一般为空)
Bugreports	Bug 记录(一般为空)
Fuzzer	模糊测试(一般为空)
HttpEditor	HTTP 编辑器(一般为空)
Logs	日志
Saves	保存结果(一般为空)
unins000.dat	卸载程序
libeay32.dll	OpenSSL 共享库
SciLexer.dll	Scintilla
DelZip190.dll	Zip/Unzip
ssleay32.dll	OpenSSL 共享库
pcre.dll	Perl 语言相关库
reporter_console.exe	命令行下产生报告程序
Activation.exe	wvs 激活程序
wvs.exe	Wvs 主程序
Reporter.exe	报告程序
lsr.exe	登录会话记录程序
WVSScheduler.exe	计划任务程序
unins000.exe	卸载程序
UnInstall.exe	卸载程序
ve.exe	漏洞信息编辑器
wvs_console.exe	Wvs 控制台程序
license.rtf	声明
ffacuscan.xpi	火狐插件

C:\ProgramData\Acunetix WVS 8	
CSA.dll	http://www.acunetix.com/websitesecurity/javascript/
Data	**WVS 扫描器的核心配置(建议熟悉每一个文件)**
Reports	报告样板

C:\Users\someone\Documents\Acunetix WVS 8	
AcuSensor	传感器机制配置文件
BlindSQL	
Bugreports	存放 wvs.exe 的 bug
Compare	
Fuzzer	
HttpEditor	
Logs	对应 Wvs.exe 的 logging 功能
Saves	
wvss.ini	
FalsePositives.xml	
ui.xml	

C:\Users\Public\Documents\Acunetix WVS 8	
LoginSequences	存放 wvs login Sequences 配置
Saves	存放 Scheduler 结果
SchedulerLogs	SchedulerLogs 日志
Settings	
FalsePositives	误报配置

File

1. Web Site Scan	完成一次网站扫描(爬行和漏洞审计)
2. Web Site Crawl	网站爬行
3. Web Service Scan	网站服务扫描，例如 WSDL
4. Report	生成报告
5. Load Scan Results	加载 Acunetix 的保存结果
6. Save Scan Results	保存 Acunetix 的扫描结果

1. WebSite Scan

菜单: File >> New >> Web Site Scan

网站扫描开始前，需要设定下面选项:

1. Scan type
2. Options
3. Target
4. Login
5. Finsh

1. Scan type

- Scan single website

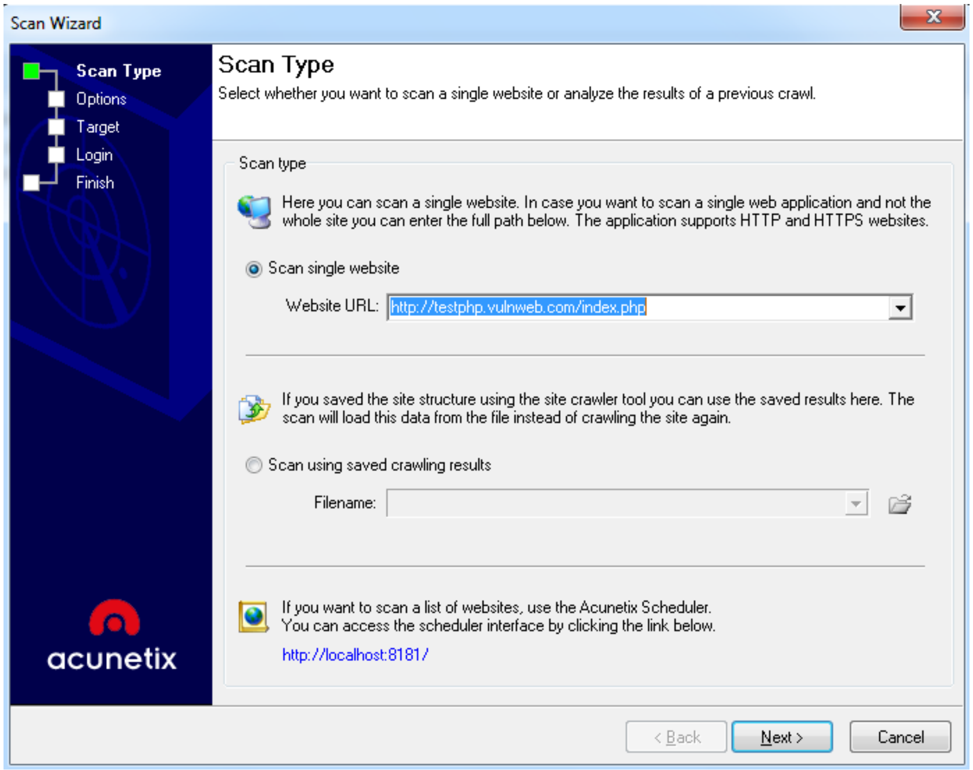
  在 Website URL 处填入需要扫描的网站网址，如果你想要扫描一个单独的应用程序，而不是整个网站，可以在填写网址的地方写入完整路径。wvs 支持 HTTP/HTTPS 网站扫描。

- Scan using saved crawling results

  导入 WVS 内置 site crawler tool 的爬行结果，然后进行漏洞扫描。

- Access the scheduler interface

  如果需要扫描的网站构成了一个列表，那么可以使用 Acunetix 的 Scheduler 功能完成任务，访问 http://localhost:8181，扫描后的文件存放在 C:\Users\Public\Documents\Acunetix WVS 8\Saves.



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://testphp.vulnweb.com/index.php

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:

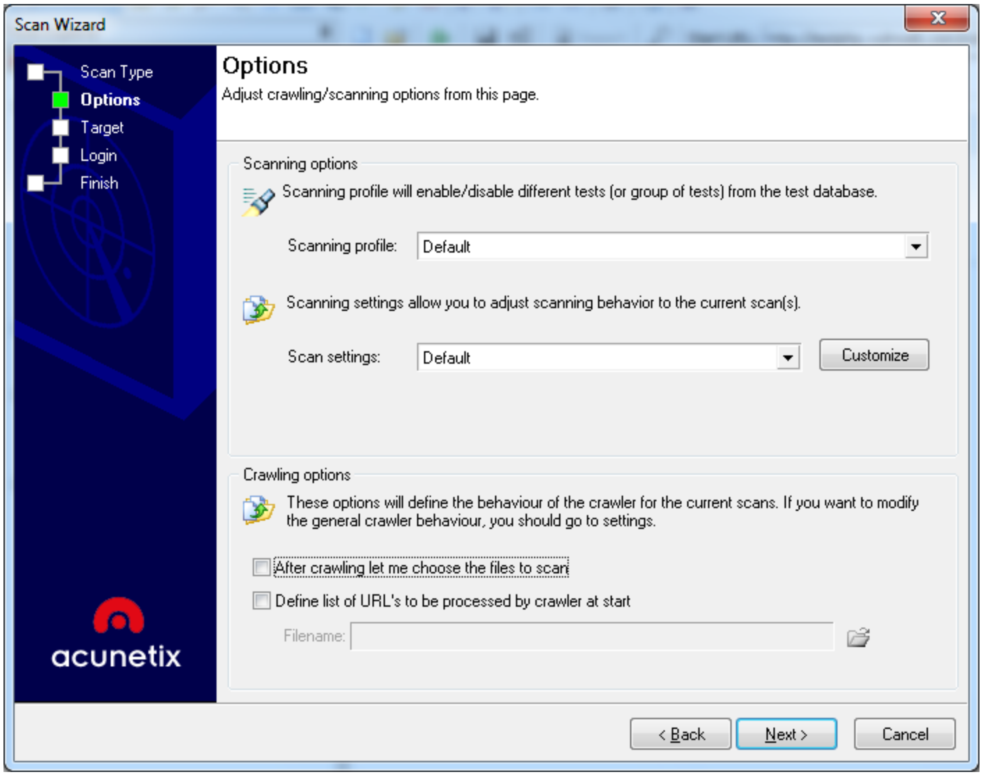
If you want to scan a list of websites, use the Acunetix Scheduler. You can access the scheduler interface by clicking the link below.

http://localhost:8181/

2. Options

Options 部分的设定主要分为两部分:

- **Scanning options**
- **Crawling options**



Options

Adjust crawling/scanning options from this page.

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

Crawling options

These options will define the behaviour of the crawler for the current scans. If you want to modify the general crawler behaviour, you should go to settings.

☐ After crawling let me choose the files to scan

☐ Define list of URL's to be processed by crawler at start

Filename:

2.1 - Scanning options

2.1.1 - Scanning profile

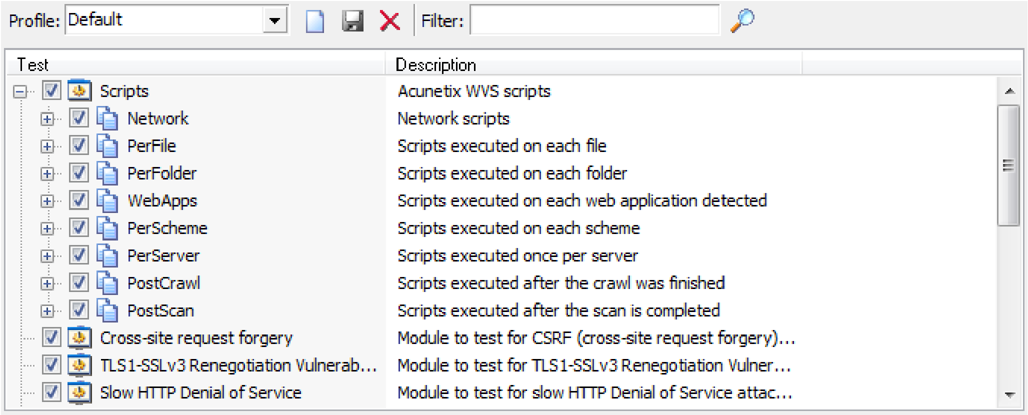
可设定扫描重点，配置文件位于 C:\ProgramData\Acunetix WVS 8\Data\Profiles

默认 15 种配置如下(建议深入挖掘 wvs 的检测机制):

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，目前主要针对 ASP.NET/PHP.
Blind SQL Injection	盲注扫描
CSRF	检测跨域访问
Default	默认配置(均检测)
Directory And File Checks	目录与文件检测
Empty	不使用任何检测

File Upload	文件上传检测
GHDB	利用 Google hacking 数据库检测
High Risk Alerts	高风险警告
Network Scripts	网络脚本
Parameter Manipulation	参数操作
Text Search	文本搜索
Weak Passwords	弱密码
Web Applications	Web 应用程序
Xss	跨站检测

如果需要做调整，请查看菜单 Configuration >> Scanning Profiles



Profile: Default Filter:

Test	Description
☑ Scripts	Acunetix WVS scripts
☑ Network	Network scripts
☑ PerFile	Scripts executed on each file
☑ PerFolder	Scripts executed on each folder
☑ WebApps	Scripts executed on each web application detected
☑ PerScheme	Scripts executed on each scheme
☑ PerServer	Scripts executed once per server
☑ PostCrawl	Scripts executed after the crawl was finished
☑ PostScan	Scripts executed after the scan is completed
☑ Cross-site request forgery	Module to test for CSRF (cross-site request forgery)...
☑ TLS1-SSLv3 Renegotiation Vulnerab...	Module to test for TLS1-SSLv3 Renegotiation Vulner...
☑ Slow HTTP Denial of Service	Module to test for slow HTTP Denial of Service attac...

2.1.2 - Scan settings

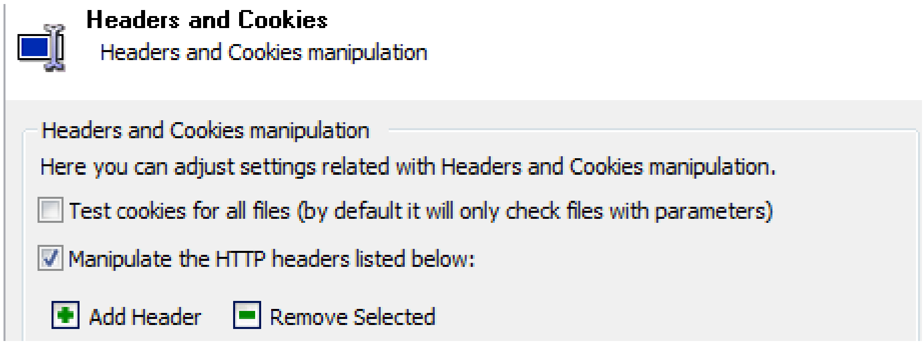
可定制扫描器扫描选项，例如:

- Headers and Cookies
- Parameter Exclusions
- GHDB

Headers and Cookies

Test cookies for all files (by default it will only check files with parameters)
访问所有文件，都使用 cookie 测试(默认情况下，只有带参数的文件才使用 cookie 进行检测)

Manipulate the HTTP headers listed below
操控列表中的 cookie，可按照自己的要求定制



Headers and Cookies

Headers and Cookies manipulation

Headers and Cookies manipulation

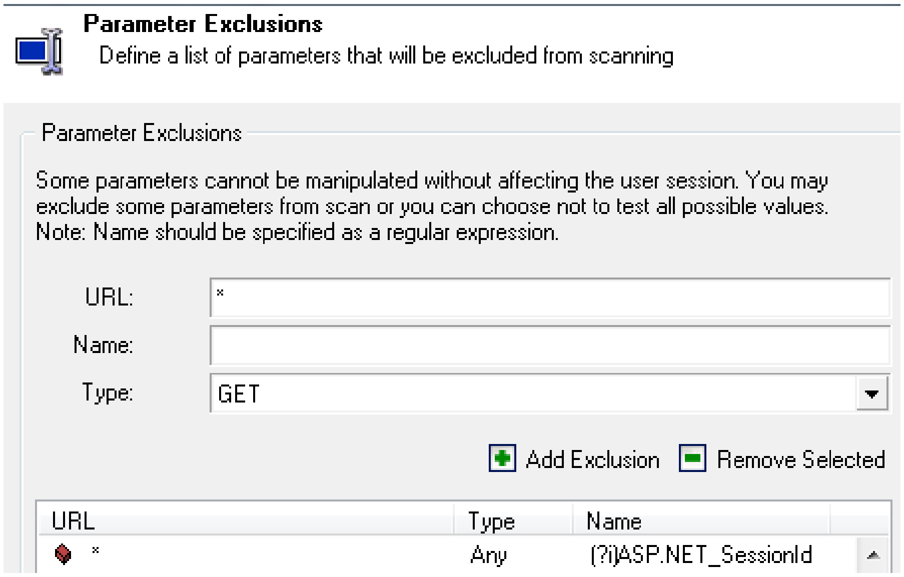
Here you can adjust settings related with Headers and Cookies manipulation.

□ Test cookies for all files (by default it will only check files with parameters)

☑ Manipulate the HTTP headers listed below:

Parameter Exclusion

有些参数我们无法操纵，但它不会影响会话，应此可进行排除，避免做不必要的扫描测试.



Parameter Exclusions

Define a list of parameters that will be excluded from scanning

Parameter Exclusions

Some parameters cannot be manipulated without affecting the user session. You may exclude some parameters from scan or you can choose not to test all possible values. Note: Name should be specified as a regular expression.

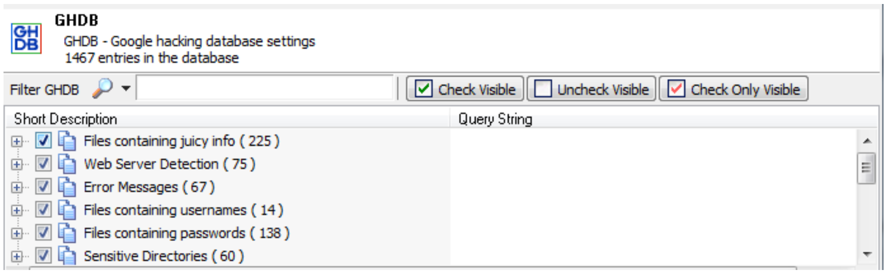
URL: *

Name:

Type: GET

URL	Type	Name
*	Any	(?i)ASP.NET_SessionId

GHDB



GHDB

GHDB - Google hacking database settings

1467 entries in the database

Short Description	Query String
☑ Files containing juicy info (225)	
☑ Web Server Detection (75)	
☑ Error Messages (67)	
☑ Files containing usernames (14)	
☑ Files containing passwords (138)	
☑ Sensitive Directories (60)	

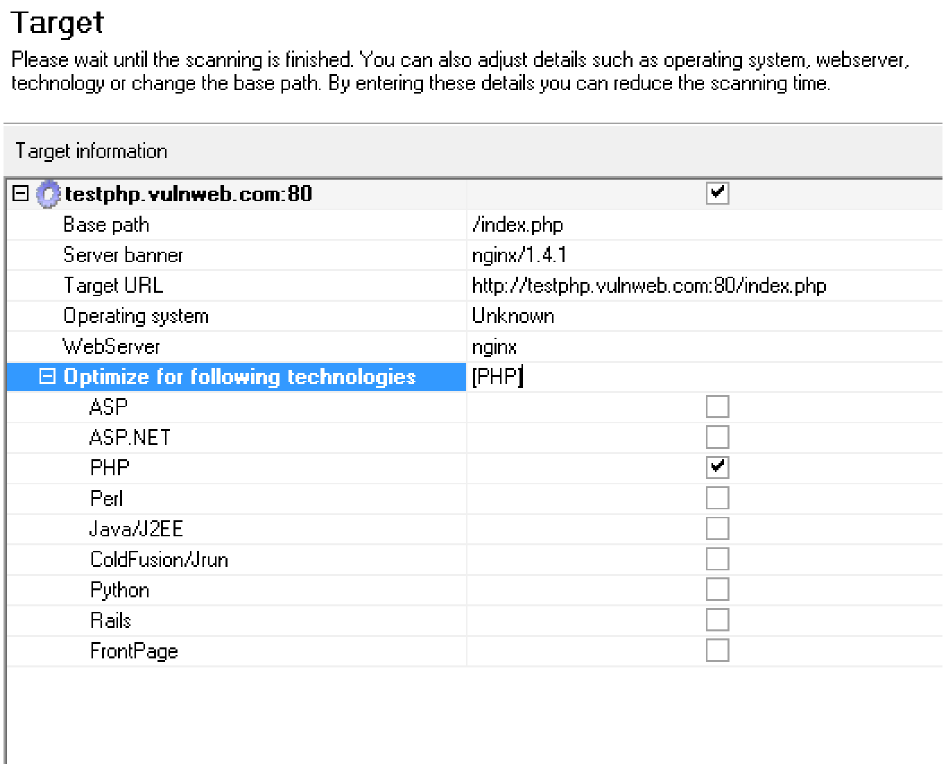
2.2 - Crawling options

- After crawling let me choose the files to scan
  爬行完成后，如何操作(可用于选择想要扫描的文件).

- Define list of URL’s to be processed by crawler at start。
  定义爬行起点

3. Target

有些时候 WVS 无法判定服务器所用脚本语言，可手动指定.



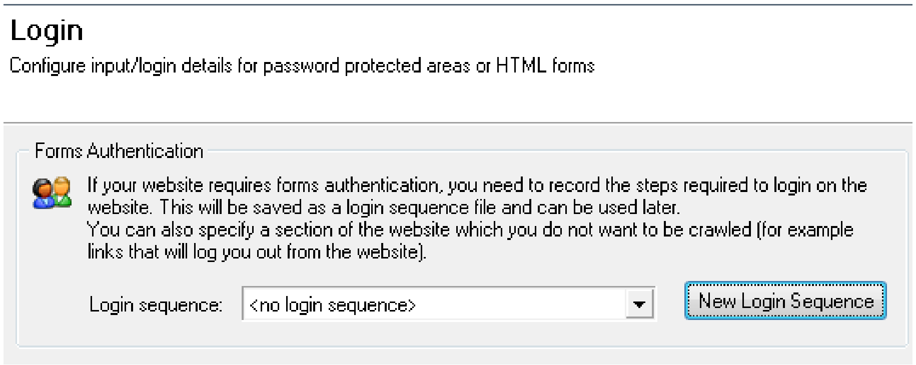
Target

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

⊟ testphp.vulnweb.com:80	☑
Base path	/index.php
Server banner	nginx/1.4.1
Target URL	http://testphp.vulnweb.com:80/index.php
Operating system	Unknown
WebServer	nginx
⊟ Optimize for following technologies	[PHP]
ASP	□
ASP.NET	□
PHP	☑
Perl	□
Java/J2EE	□
ColdFusion/Jrun	□
Python	□
Rails	□
FrontPage	□

4. Login



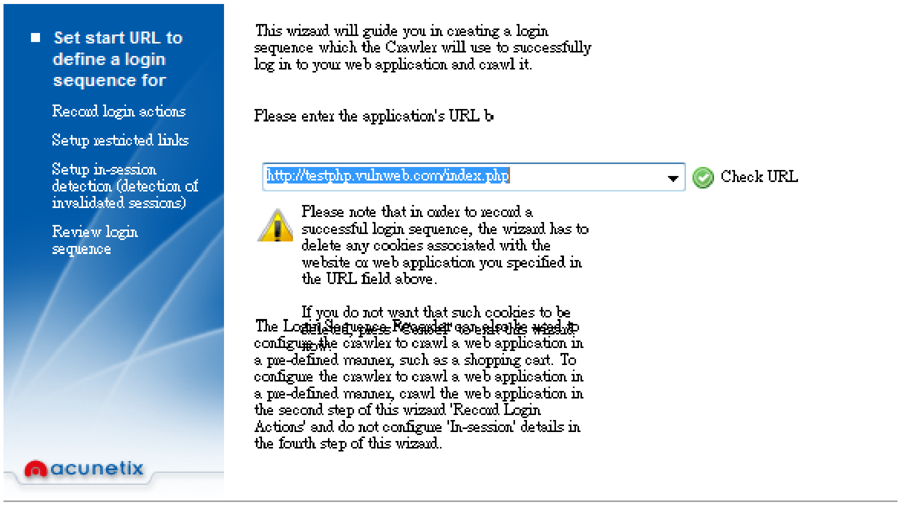
Login

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

Forms Authentication

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: <no login sequence>



Set start URL to define a login sequence for
Record login actions
Setup restricted links
Setup in-session detection (detection of invalidated sessions)
Review login sequence
acunetix

This wizard will guide you in creating a login sequence which the Crawler will use to successfully log in to your web application and crawl it.

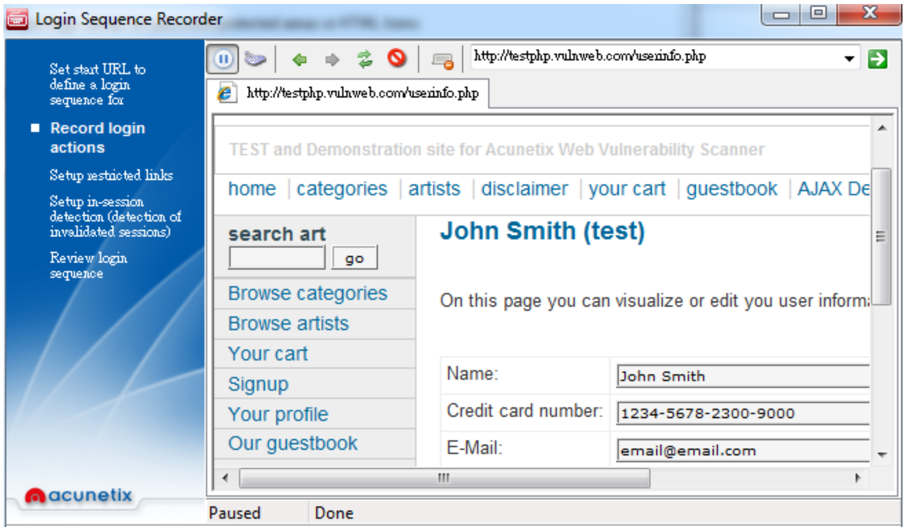
Please enter the application's URL b

http://testphp.vulnweb.com/index.php

Please note that in order to record a successful login sequence, the wizard has to delete any cookies associated with the website or web application you specified in the URL field above.

If you do not want that such cookies to be deleted, press 'Cancel' to close the wizard now.

The Login Sequence Recorder can also be used to configure the crawler to crawl a web application in a pre-defined manner, such as a shopping cart. To configure the crawler to crawl a web application in a pre-defined manner, crawl the web application in the second step of this wizard 'Record Login Actions' and do not configure 'In-session' details in the fourth step of this wizard.

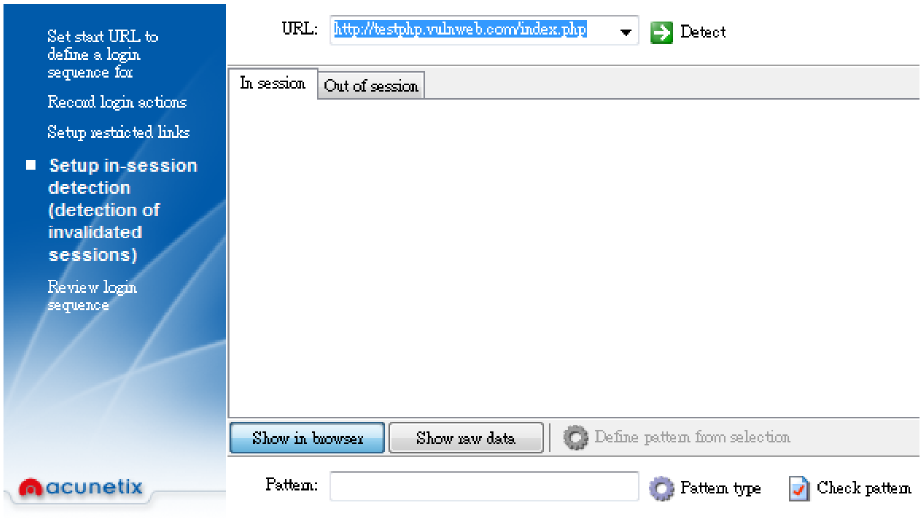


Login Sequence Recorder
Set start URL to define a login sequence for
Record login actions
Setup restricted links
Setup in-session detection (detection of invalidated sessions)
Review login sequence
acunetix
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/userinfo.php
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX De
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
Paused
Done

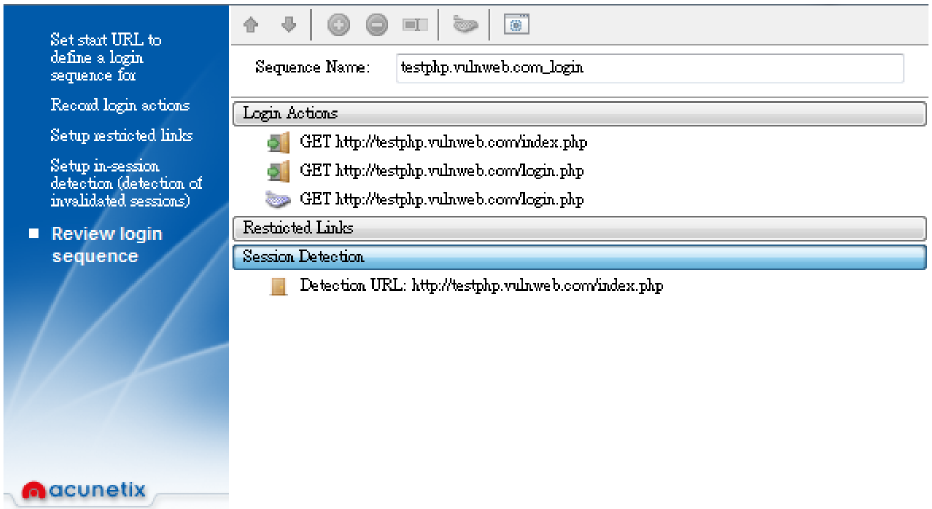
John Smith (test)

On this page you can visualize or edit you user inform

Name:	John Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com



URL: http://testphp.vulnweb.com/index.php



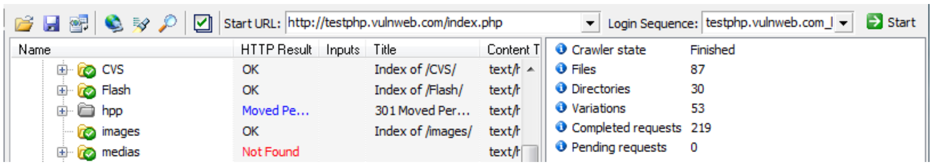
Sequence Name: testphp.vulnweb.com_login

GET http://testphp.vulnweb.com/index.php
GET http://testphp.vulnweb.com/login.php
GET http://testphp.vulnweb.com/login.php

Detection URL: http://testphp.vulnweb.com/index.php

了解以上规则，即可开始一次 Web Site Scan 扫描.

2. Web Site Crawl



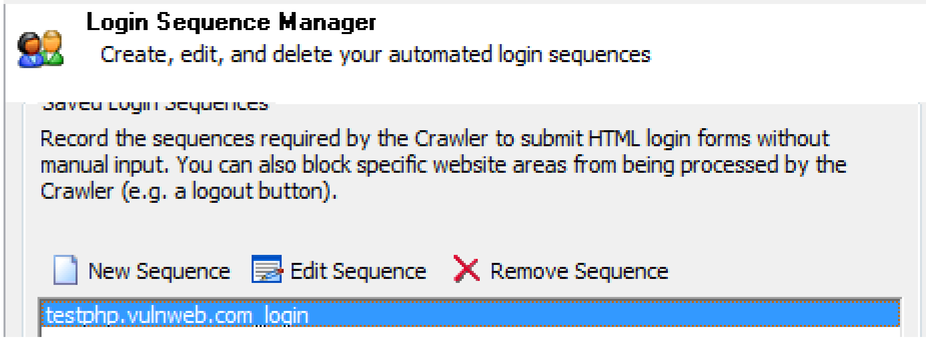
Start URL: http://testphp.vulnweb.com/index.php

Login Sequence: testphp.vulnweb.com_l

Name	HTTP Result	Inputs	Title	Content T
CVS	OK		Index of /CVS/	text/h
Flash	OK		Index of /Flash/	text/h
hpp	Moved Pe...		301 Moved Per...	text/h
images	OK		Index of /images/	text/h
medias	Not Found			text/h

Crawler state	Finished
Files	87
Directories	30
Variations	53
Completed requests	219
Pending requests	0

网站爬行，只需设定网站及是否进行启动会话.
会话设置，请访问 Configuration >> Application Settings >> Login Sequence Manager



Login Sequence Manager

Create, edit, and delete your automated login sequences

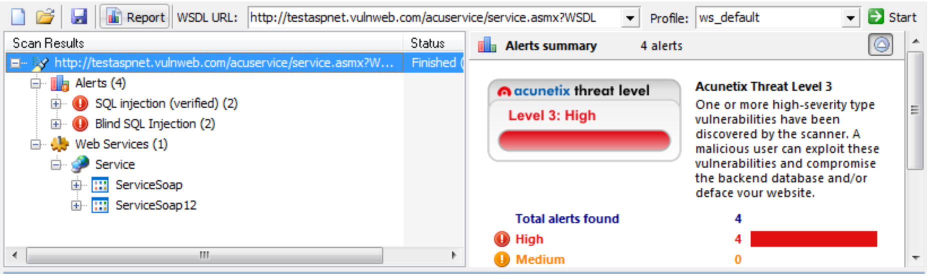
Saved Login Sequences

Record the sequences required by the Crawler to submit HTML login forms without manual input. You can also block specific website areas from being processed by the Crawler (e.g. a logout button).

testphp.vulnweb.com_login

此处的会话文件位于 C:\Users\Public\Documents\Acunetix WVS 8\LoginSequences

3. Web Service Scan



WSDL URL: http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL

Profile: ws_default

```
Scan Results                                                          Status
http://testaspnet.vulnweb.com/acuservice/service.asmx?W...            Finished (
  Alerts (4)
    SQL injection (verified) (2)
    Blind SQL Injection (2)
  Web Services (1)
    Service
      ServiceSoap
      ServiceSoap12
```

Alerts summary 4 alerts

acunetix threat level

Level 3: High

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Total alerts found	4
High	4
Medium	0

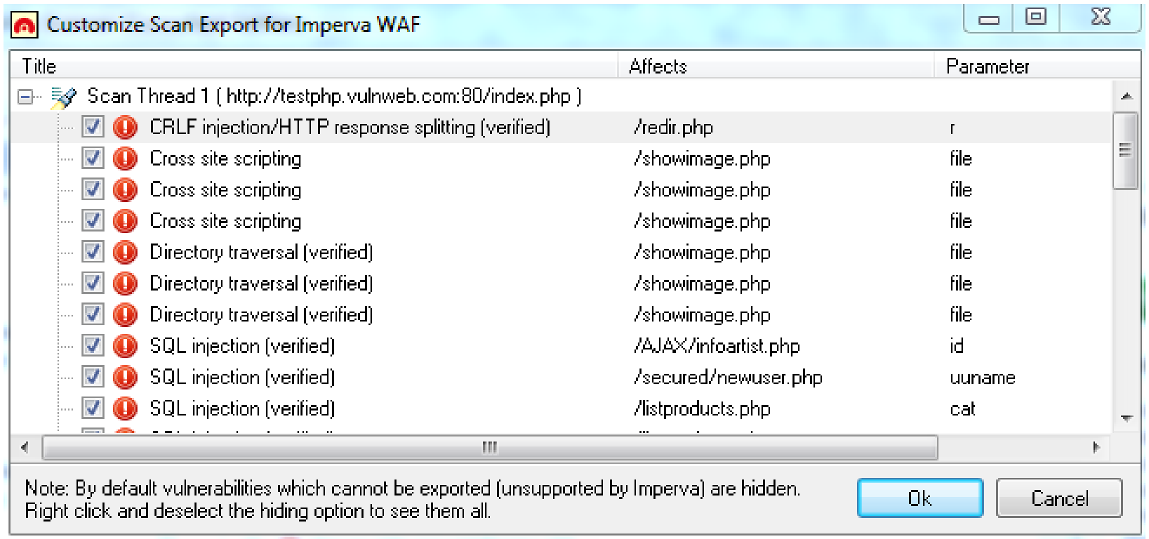
Web Service Scan 可用于对审计 WSDL 接口

关于 Report，Load Scan Results，Savw Scan Results 的介绍，请参阅后面的内容.

Actions

Import from FireFox Extension	从火狐插件导入 xml 文件
Export to AVDL	导出 AVDL 格式文件
Export to XML	导出 XML 格式文件
Export for Imperva WAF	导出以便 Imperva WAF 使用
Generate Report	生成扫描报告
Import Scan Results to Database	将扫描结果放入数据库
Stop active scan	停止正在进行的扫描
Save scan results	保存扫描结果
Retest alert(s)	重置预警信息

Export for Impera WAF



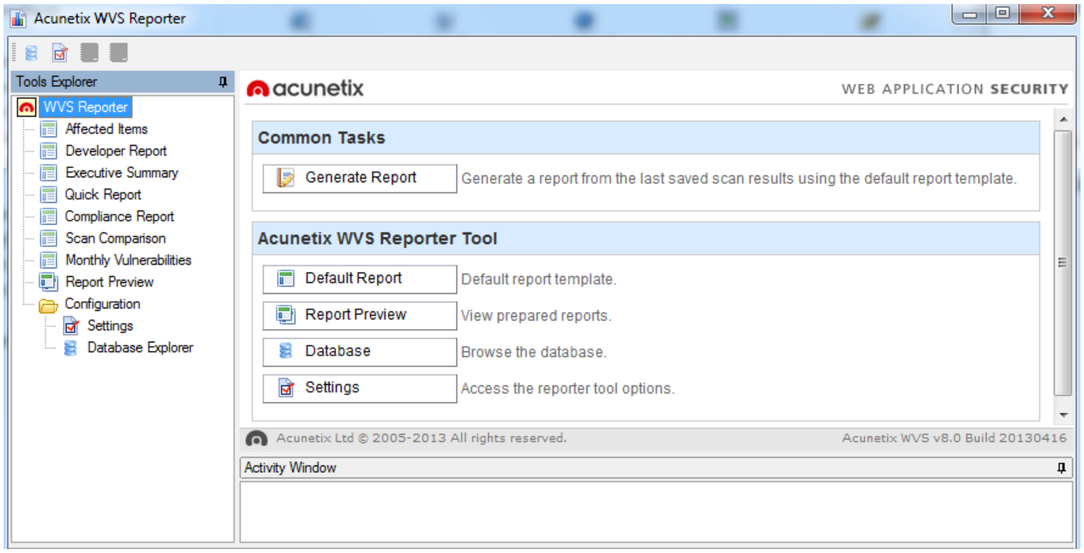
Customize Scan Export for Imperva WAF

Scan Thread 1 (http://testphp.vulnweb.com:80/index.php)

Title	Affects	Parameter
☑ CRLF injection/HTTP response splitting (verified)	/redir.php	r
☑ Cross site scripting	/showimage.php	file
☑ Cross site scripting	/showimage.php	file
☑ Cross site scripting	/showimage.php	file
☑ Directory traversal (verified)	/showimage.php	file
☑ Directory traversal (verified)	/showimage.php	file
☑ Directory traversal (verified)	/showimage.php	file
☑ SQL injection (verified)	/AJAX/infoartist.php	id
☑ SQL injection (verified)	/secured/newuser.php	uuname
☑ SQL injection (verified)	/listproducts.php	cat

Note: By default vulnerabilities which cannot be exported (unsupported by Imperva) are hidden.
Right click and deselect the hiding option to see them all.

Generate Report



Common Tasks

Generate Report — Generate a report from the last saved scan results using the default report template.

Acunetix WVS Reporter Tool

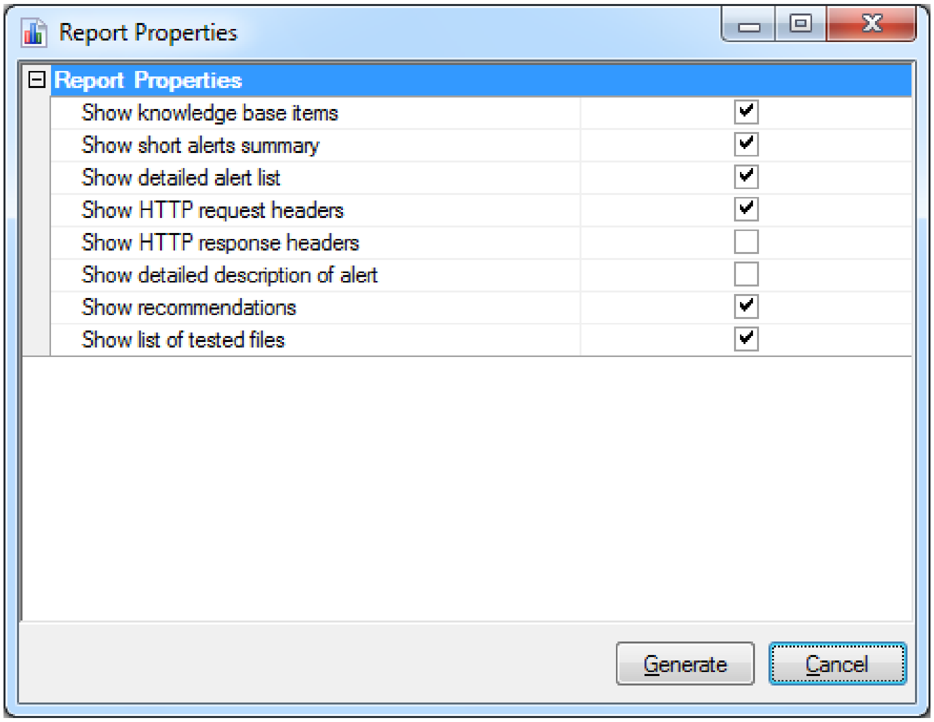
Default Report — Default report template.

Report Preview — View prepared reports.

Database — Browse the database.

Settings — Access the reporter tool options.

Acunetix Ltd © 2005-2013 All rights reserved. Acunetix WVS v8.0 Build 20130416



Report Properties	
Show knowledge base items	☑
Show short alerts summary	☑
Show detailed alert list	☑
Show HTTP request headers	☑
Show HTTP response headers	□
Show detailed description of alert	□
Show recommendations	☑
Show list of tested files	☑

使用 Configuration Settings 可定制报告的某些信息，例如 logo 等.

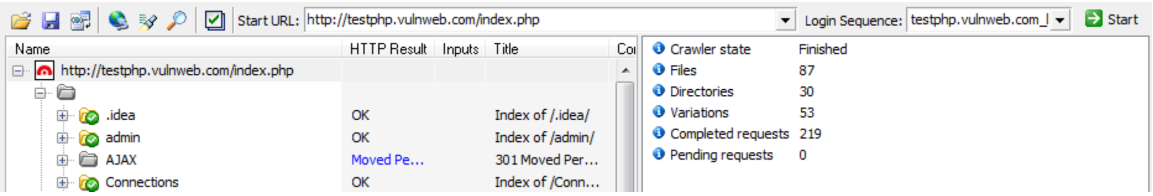
Tools

Web Scanner	Web 扫描器
Site Crawler	网站爬行
Target Finder	可扫描指定网段，开放指定端口的服务器
Subdomain Scanner	子域名扫描
Blind SQL Injector	盲注手工测试
HTTP Editor	HTTP 信息查看
HTTP Sniffer	HTTP 监听器
HTTP Fuzzer	HTTP 模糊测试
Authentication Tester	HTTP 验证测试
Compare Results	对比两次 Acunetix 扫描结果
Web Services Scanner	网站服务扫描，例如 WSDL
Web Services Editor	网站服务手动分析
Vulnerability Editor	编辑 wvs 提供的漏洞描述信息
Scheduler	任务计划，访问 http://localhost:8181/
Reporter	生成扫描报告

1. Web Scanner

详见 Web Site Scan 处介绍

2. Site Crawler



Start URL: http://testphp.vulnweb.com/index.php

Login Sequence: testphp.vulnweb.com_l

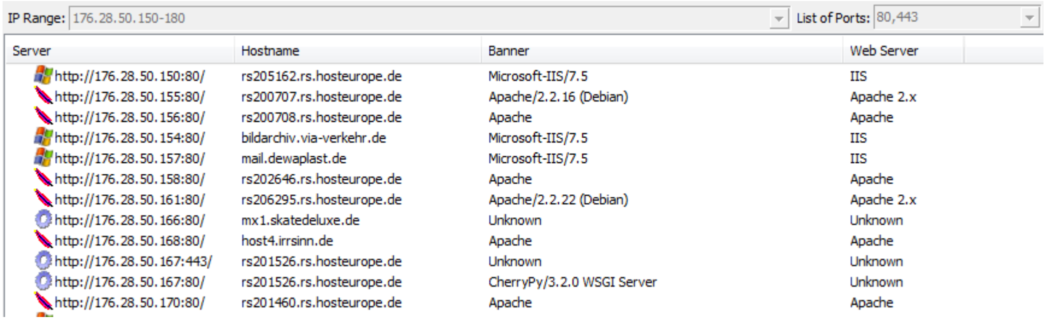
Name	HTTP Result	Inputs	Title	Co
http://testphp.vulnweb.com/index.php				
.idea	OK		Index of /.idea/	
admin	OK		Index of /admin/	
AJAX	Moved Pe...		301 Moved Per...	
Connections	OK		Index of /Conn...	

Crawler state	Finished
Files	87
Directories	30
Variations	53
Completed requests	219
Pending requests	0

指定爬行网址和登录会话(可选，默认有验证会提示)

3. Target Finder

可查询某网段，开放指定端口的服务器.

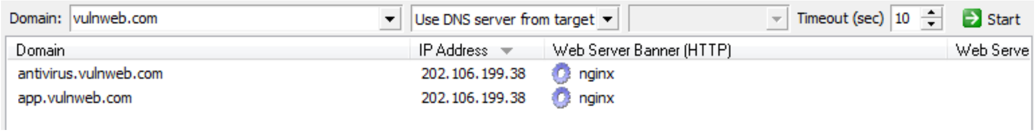


IP Range: 176.28.50.150-180 List of Ports: 80,443

Server	Hostname	Banner	Web Server
http://176.28.50.150:80/	rs205162.rs.hosteurope.de	Microsoft-IIS/7.5	IIS
http://176.28.50.155:80/	rs200707.rs.hosteurope.de	Apache/2.2.16 (Debian)	Apache 2.x
http://176.28.50.156:80/	rs200708.rs.hosteurope.de	Apache	Apache
http://176.28.50.154:80/	bildarchiv.via-verkehr.de	Microsoft-IIS/7.5	IIS
http://176.28.50.157:80/	mail.dewaplast.de	Microsoft-IIS/7.5	IIS
http://176.28.50.158:80/	rs202646.rs.hosteurope.de	Apache	Apache
http://176.28.50.161:80/	rs206295.rs.hosteurope.de	Apache/2.2.22 (Debian)	Apache 2.x
http://176.28.50.166:80/	mx1.skatedeluxe.de	Unknown	Unknown
http://176.28.50.168:80/	host4.irrsinn.de	Apache	Apache
http://176.28.50.167:443/	rs201526.rs.hosteurope.de	Unknown	Unknown
http://176.28.50.167:80/	rs201526.rs.hosteurope.de	CherryPy/3.2.0 WSGI Server	Unknown
http://176.28.50.170:80/	rs201460.rs.hosteurope.de	Apache	Apache

4. Subdomain Scanner

可设定 DNS 服务和 DNS 超时时间，如果存在区域传输，可进行深入挖掘.



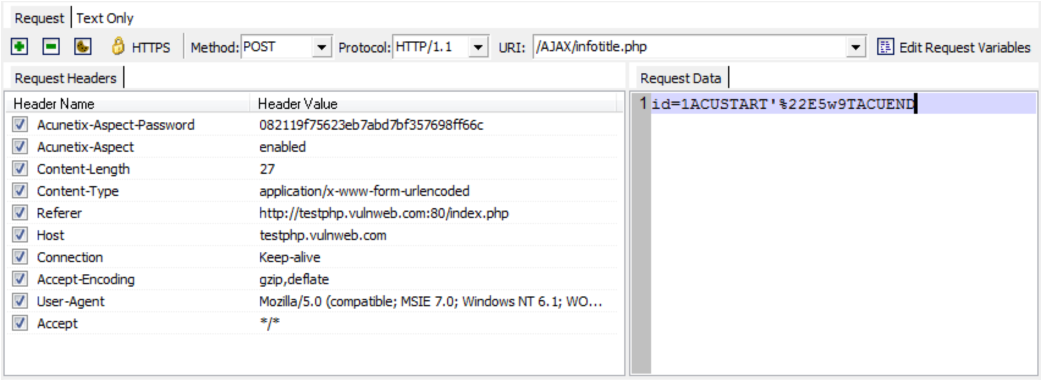
Domain: vulnweb.com Use DNS server from target Timeout (sec) 10 Start

Domain	IP Address	Web Server Banner (HTTP)	Web Serve
antivirus.vulnweb.com	202.106.199.38	nginx	
app.vulnweb.com	202.106.199.38	nginx	

5. Blind SQL Injector

建议去 youtube 查看对应的视频

6. HTTP Editor

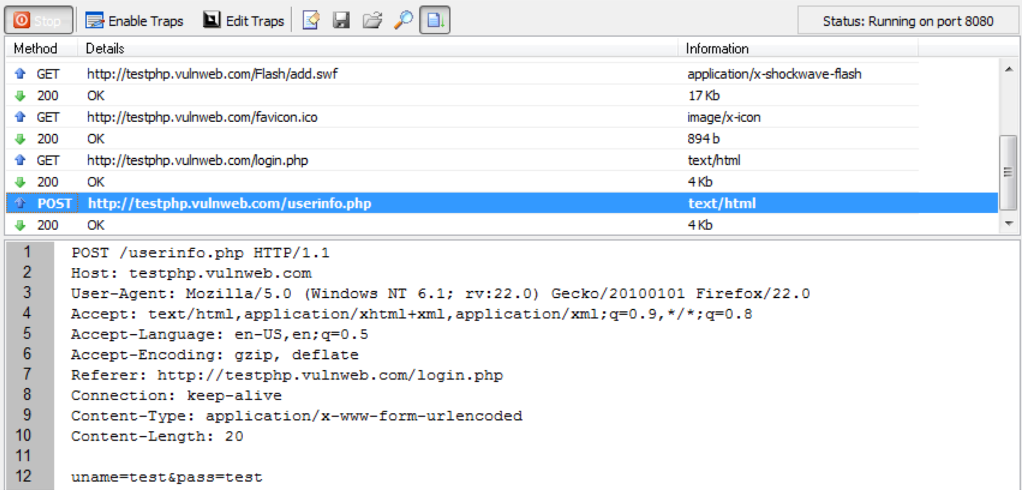


	Header Name	Header Value
☑	Acunetix-Aspect-Password	082119f75623eb7abd7bf357698ff66c
☑	Acunetix-Aspect	enabled
☑	Content-Length	27
☑	Content-Type	application/x-www-form-urlencoded
☑	Referer	http://testphp.vulnweb.com:80/index.php
☑	Host	testphp.vulnweb.com
☑	Connection	Keep-alive
☑	Accept-Encoding	gzip,deflate
☑	User-Agent	Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; WO...
☑	Accept	*/*

```
id=1ACUSTART'%22E5w9TACUEND
```

7. HTTP Sniffer

Acunetix WVS 提供的 HTTP/HTTPS 代理功能.



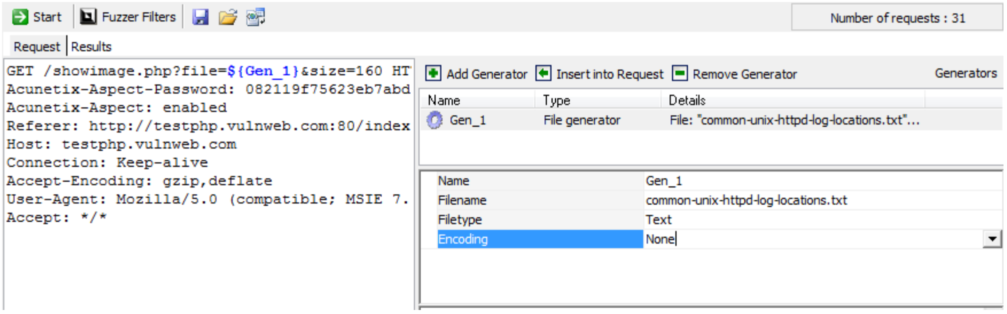
Method	Details	Information
GET	http://testphp.vulnweb.com/Flash/add.swf	application/x-shockwave-flash
200	OK	17 Kb
GET	http://testphp.vulnweb.com/favicon.ico	image/x-icon
200	OK	894 b
GET	http://testphp.vulnweb.com/login.php	text/html
200	OK	4 Kb
POST	http://testphp.vulnweb.com/userinfo.php	text/html
200	OK	4 Kb

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100101 Firefox/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

uname=test&pass=test
```

8. HTTP Fuzzer

某种程度上，类似 burp 的 Intruder 功能.



```
GET /showimage.php?file=${Gen_1}&size=160 HT
Acunetix-Aspect-Password: 082119f75623eb7abd
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/index
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 7.
Accept: */*
```

Name	Type	Details
Gen_1	File generator	File: "common-unix-httpd-log-locations.txt"...

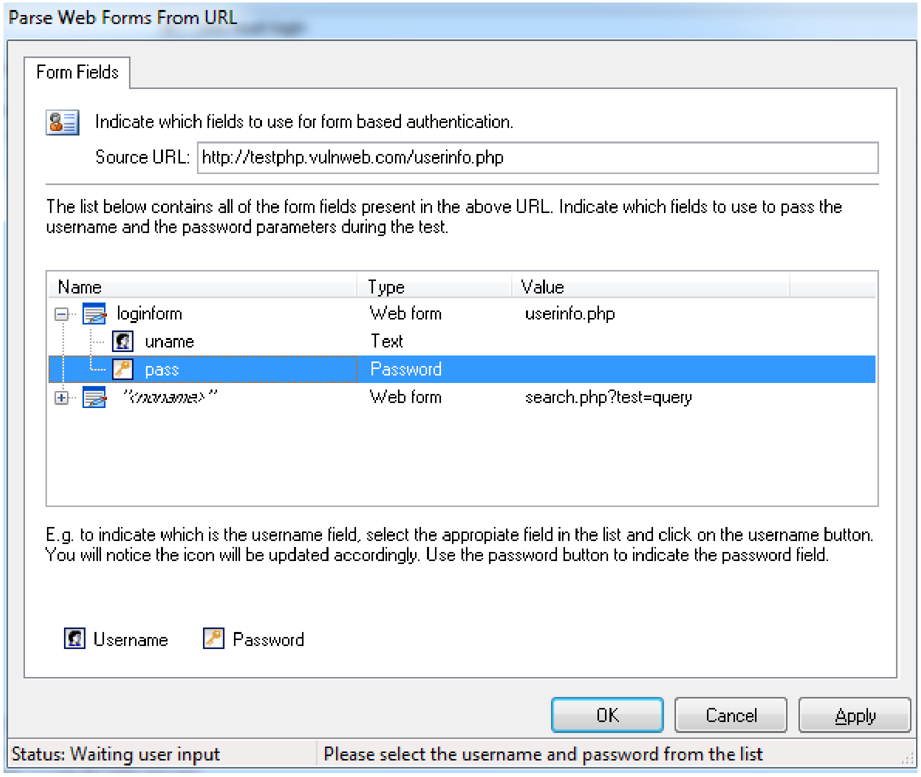
Name	Gen_1
Filename	common-unix-httpd-log-locations.txt
Filetype	Text
Encoding	None

9. Authentication Tester

Authentication method: 支持 HTTP/表单验证

Logon has failed if: 可设定验证错误返回的 HTTP Code

Username dictionary/Password dictionary path: 设定用户名/密码字典.



Indicate which fields to use for form based authentication.

Source URL: http://testphp.vulnweb.com/userinfo.php

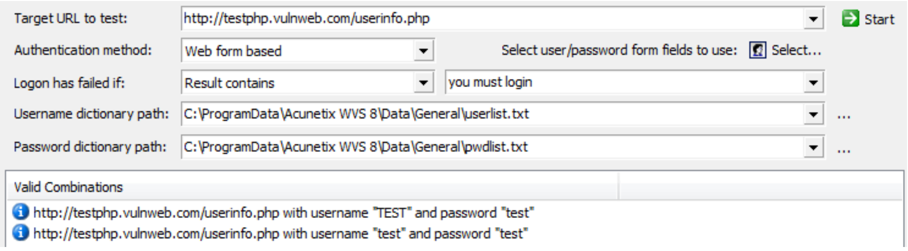
The list below contains all of the form fields present in the above URL. Indicate which fields to use to pass the username and the password parameters during the test.

Name	Type	Value
loginform	Web form	userinfo.php
uname	Text	
pass	Password	
"<noname>"	Web form	search.php?test=query

E.g. to indicate which is the username field, select the appropiate field in the list and click on the username button. You will notice the icon will be updated accordingly. Use the password button to indicate the password field.

Status: Waiting user input

Please select the username and password from the list



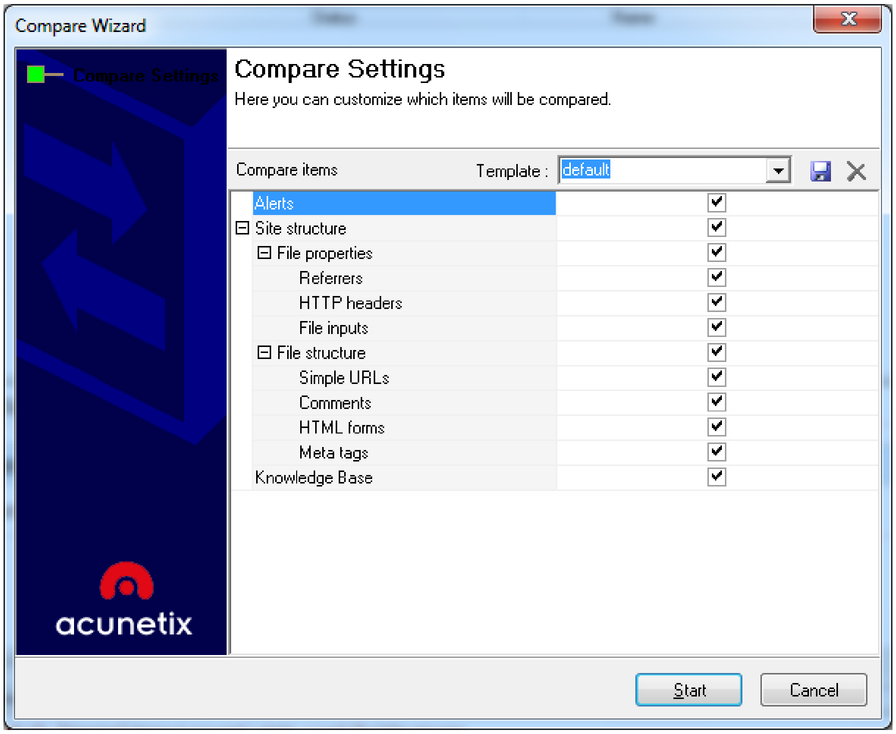
Target URL to test:	http://testphp.vulnweb.com/userinfo.php	Start
Authentication method:	Web form based	Select user/password form fields to use: Select...
Logon has failed if:	Result contains	you must login
Username dictionary path:	C:\ProgramData\Acunetix WVS 8\Data\General\userlist.txt	...
Password dictionary path:	C:\ProgramData\Acunetix WVS 8\Data\General\pwdlist.txt	...

Valid Combinations

- http://testphp.vulnweb.com/userinfo.php with username "TEST" and password "test"
- http://testphp.vulnweb.com/userinfo.php with username "test" and password "test"

10. Compare

两次扫描结果进行对比，可深入挖掘不同产生的原因.



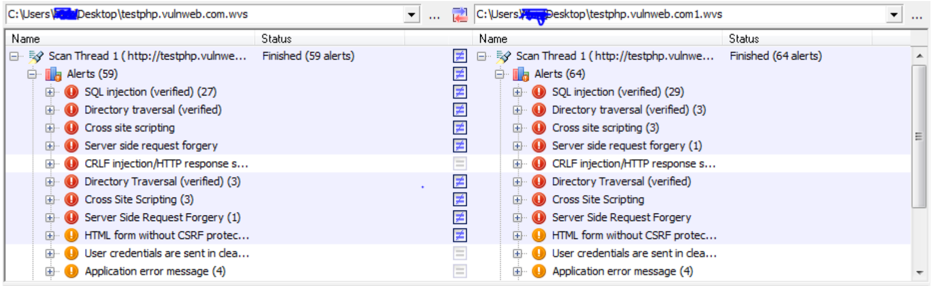
Compare Wizard

Compare Settings

Here you can customize which items will be compared.

Compare items — Template : default

Alerts	☑
⊟ Site structure	☑
⊟ File properties	☑
Referrers	☑
HTTP headers	☑
File inputs	☑
⊟ File structure	☑
Simple URLs	☑
Comments	☑
HTML forms	☑
Meta tags	☑
Knowledge Base	☑

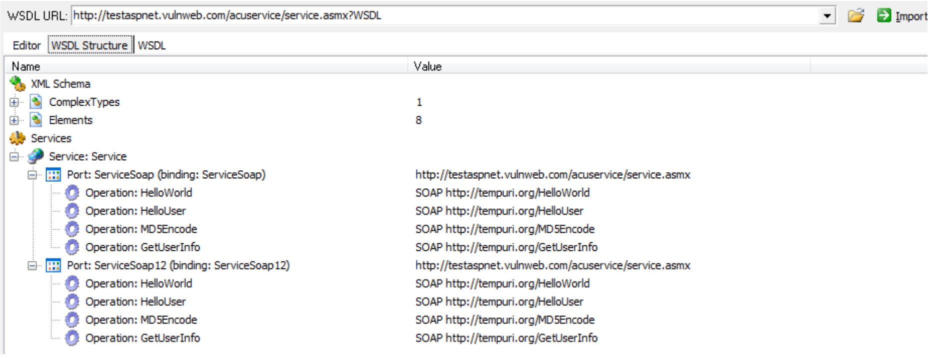


C:\Users\[redacted]Desktop\testphp.vulnweb.com.wvs

C:\Users\[redacted]Desktop\testphp.vulnweb.com1.wvs

Name	Status		Name	Status
Scan Thread 1 (http://testphp.vulnwe...	Finished (59 alerts)	≠	Scan Thread 1 (http://testphp.vulnwe...	Finished (64 alerts)
Alerts (59)		≠	Alerts (64)	
SQL injection (verified) (27)		≠	SQL injection (verified) (29)	
Directory traversal (verified)		≠	Directory traversal (verified) (3)	
Cross site scripting		≠	Cross site scripting (3)	
Server side request forgery		≠	Server side request forgery (1)	
CRLF injection/HTTP response s...		=	CRLF injection/HTTP response s...	
Directory Traversal (verified) (3)		≠	Directory Traversal (verified)	
Cross Site Scripting (3)		≠	Cross Site Scripting	
Server Side Request Forgery (1)		≠	Server Side Request Forgery	
HTML form without CSRF protec...		≠	HTML form without CSRF protec...	
User credentials are sent in clea...		=	User credentials are sent in clea...	
Application error message (4)		=	Application error message (4)	

11. Web Services



WSDL URL: http://testaspnet.vulnweb.com/acuservice/service.asmx?WSDL

Name	Value
XML Schema	
ComplexTypes	1
Elements	8
Services	
Service: Service	
Port: ServiceSoap (binding: ServiceSoap)	http://testaspnet.vulnweb.com/acuservice/service.asmx
Operation: HelloWorld	SOAP http://tempuri.org/HelloWorld
Operation: HelloUser	SOAP http://tempuri.org/HelloUser
Operation: MD5Encode	SOAP http://tempuri.org/MD5Encode
Operation: GetUserInfo	SOAP http://tempuri.org/GetUserInfo
Port: ServiceSoap12 (binding: ServiceSoap12)	http://testaspnet.vulnweb.com/acuservice/service.asmx
Operation: HelloWorld	SOAP http://tempuri.org/HelloWorld
Operation: HelloUser	SOAP http://tempuri.org/HelloUser
Operation: MD5Encode	SOAP http://tempuri.org/MD5Encode
Operation: GetUserInfo	SOAP http://tempuri.org/GetUserInfo

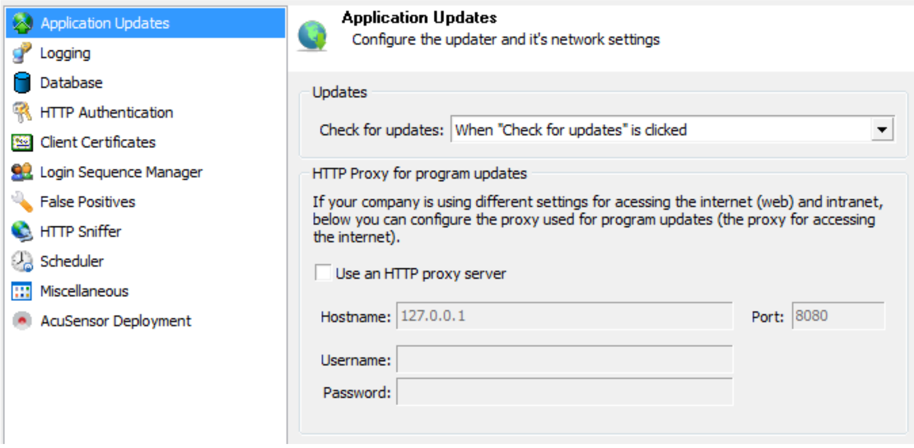
Configuration

Application Settings	应用程序设置
Scan Settings	扫描设置
Scanning Profiles	配置所用扫描脚本

Application Settings

程序更新

用于设定程序更新时所用代理服务.
Wvs 代理扫描设定，请使用 Configuration >> Scan Settings >> LAN Settings
升级后的文件位于 C:\ProgramData\Acunetix WVS 8\Data\Update



Application Updates
Configure the updater and it's network settings

Updates

Check for updates: When "Check for updates" is clicked

HTTP Proxy for program updates

If your company is using different settings for acessing the internet (web) and intranet, below you can configure the proxy used for program updates (the proxy for accessing the internet).

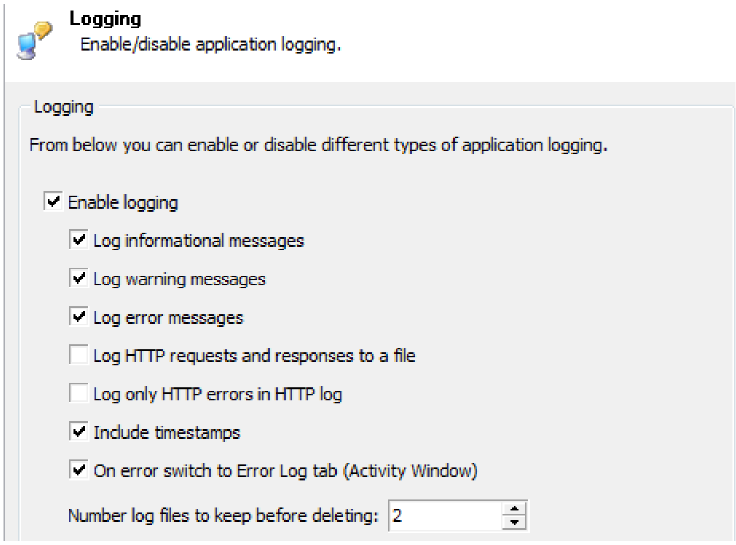
□ Use an HTTP proxy server

Hostname: 127.0.0.1 Port: 8080

Username:

Password:

日志记录



Logging
Enable/disable application logging.

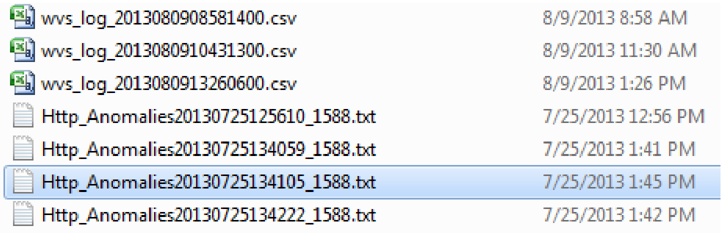
Logging

From below you can enable or disable different types of application logging.

☑ Enable logging
☑ Log informational messages
☑ Log warning messages
☑ Log error messages
□ Log HTTP requests and responses to a file
□ Log only HTTP errors in HTTP log
☑ Include timestamps
☑ On error switch to Error Log tab (Activity Window)

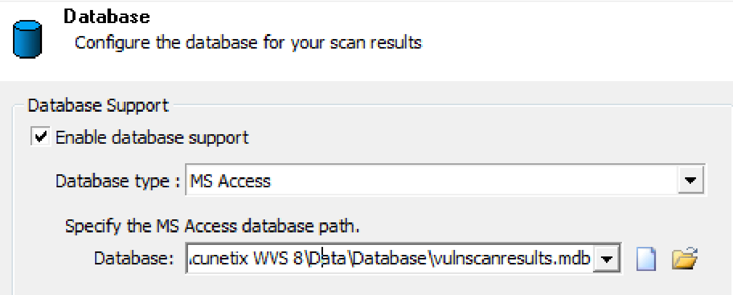
Number log files to keep before deleting: 2

Acunetix WVS 的记录功能，记录信息请查阅文件夹 C:\Users\Max\Documents\Acunetix WVS 8\Logs



wvs_log_2013080908581400.csv	8/9/2013 8:58 AM
wvs_log_2013080910431300.csv	8/9/2013 11:30 AM
wvs_log_2013080913260600.csv	8/9/2013 1:26 PM
Http_Anomalies20130725125610_1588.txt	7/25/2013 12:56 PM
Http_Anomalies20130725134059_1588.txt	7/25/2013 1:41 PM
Http_Anomalies20130725134105_1588.txt	7/25/2013 1:45 PM
Http_Anomalies20130725134222_1588.txt	7/25/2013 1:42 PM

数据库



Database
Configure the database for your scan results

Database Support

☑ Enable database support

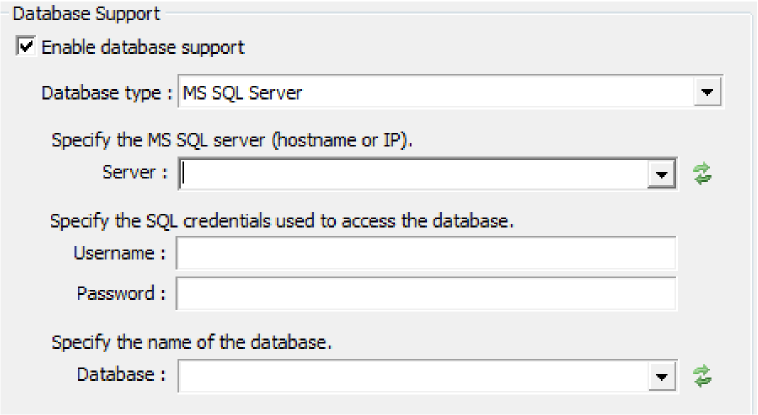
Database type : MS Access

Specify the MS Access database path.

Database: cunetix WVS 8\Data\Database\vulnscanresults.mdb

扫描结果默认保存在 Access 数据库，位置 C:\ProgramData\Acunetix WVS 8\Data\Database\vulnscanresults.mdb.

如果有需要，可以安装 MSSQL 数据库，保存扫描结果.



Database Support

☑ Enable database support

Database type : MS SQL Server

Specify the MS SQL server (hostname or IP).

Server :

Specify the SQL credentials used to access the database.

Username :

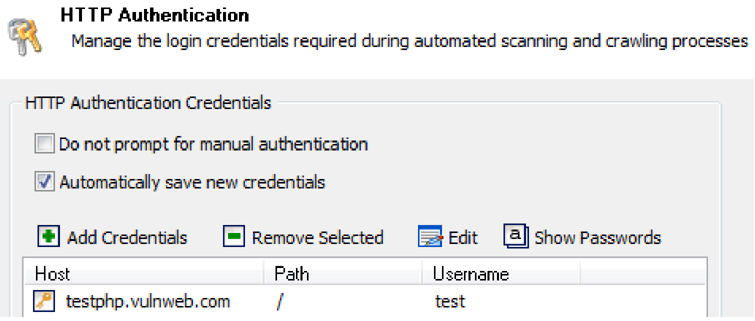
Password :

Specify the name of the database.

Database :

HTTP 验证

此处可设置验证所用的证书.



HTTP Authentication

Manage the login credentials required during automated scanning and crawling processes

HTTP Authentication Credentials

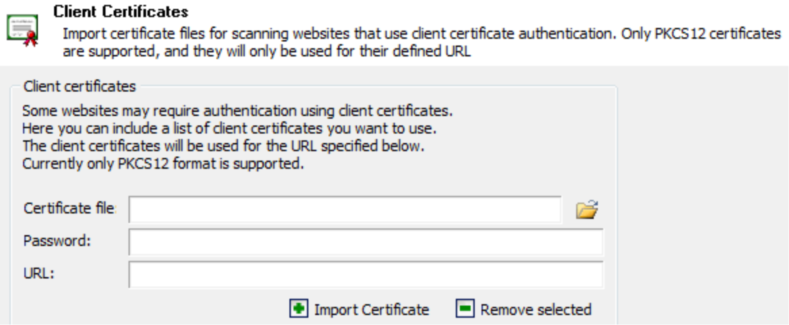
□ Do not prompt for manual authentication

☑ Automatically save new credentials

Host	Path	Username
testphp.vulnweb.com	/	test

客户端证书

有些网站需要证书验证，才能访问某些资源，此处可指定访问所需证书.



Client Certificates

Import certificate files for scanning websites that use client certificate authentication. Only PKCS12 certificates are supported, and they will only be used for their defined URL

Client certificates

Some websites may require authentication using client certificates.
Here you can include a list of client certificates you want to use.
The client certificates will be used for the URL specified below.
Currently only PKCS12 format is supported.

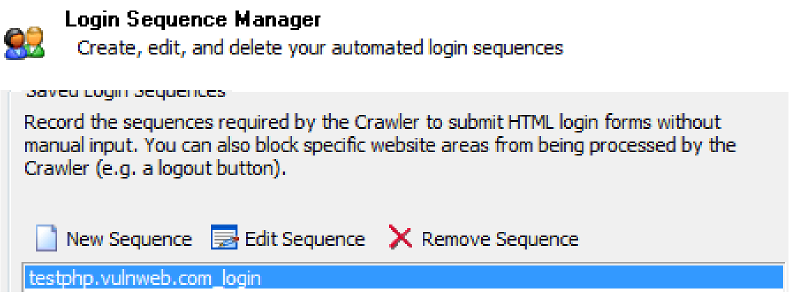
Certificate file

Password:

URL:

登陆会话管理

注意与前面的 HTTP Authentication 做区分，它们是两个不同的概念.
LoginSequenceManager 的功能是记录爬行过程中需要发送登录表单的过程，无需手动输入。
HTTP Authentication 则是完成 HTTP 请求验证，例如:需要验证才能访问的文件或文件夹。


Login Sequence Manager
Create, edit, and delete your automated login sequences

Saved Login Sequences

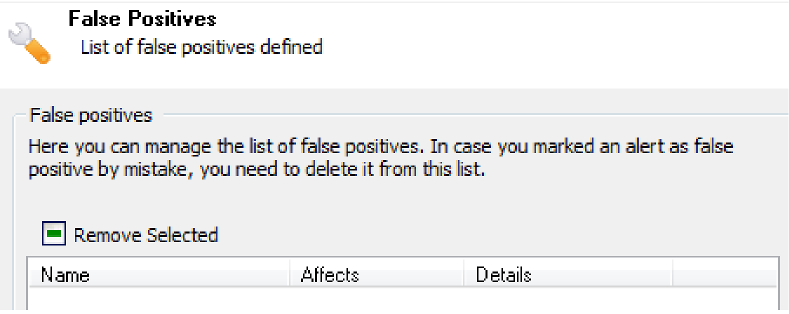
Record the sequences required by the Crawler to submit HTML login forms without manual input. You can also block specific website areas from being processed by the Crawler (e.g. a logout button).

New Sequence | Edit Sequence | Remove Sequence

testphp.vulnweb.com_login

False Positives

处理误报


False Positives
List of false positives defined

False positives

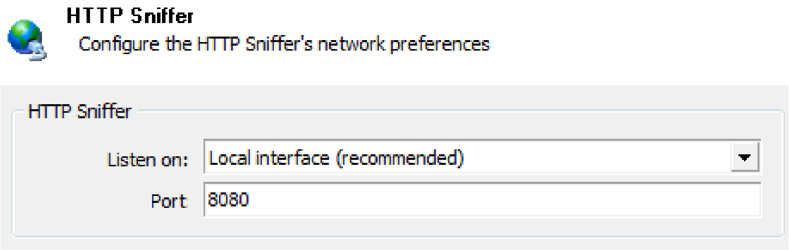
Here you can manage the list of false positives. In case you marked an alert as false positive by mistake, you need to delete it from this list.

Remove Selected

Name	Affects	Details

HTTP Sniffer

Acunetix HTTP 代理设置，默认监听 8080 端口(此功能默认不开启)

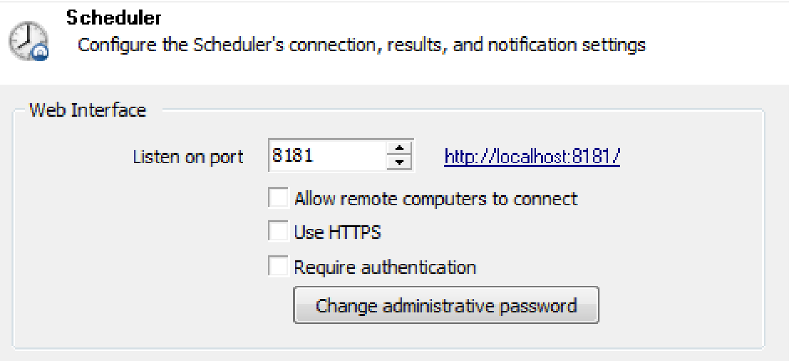

HTTP Sniffer
Configure the HTTP Sniffer's network preferences

HTTP Sniffer

Listen on: Local interface (recommended)

Port 8080

Scheduler



Scheduler

Configure the Scheduler's connection, results, and notification settings

Web Interface

Listen on port 8181 http://localhost:8181/

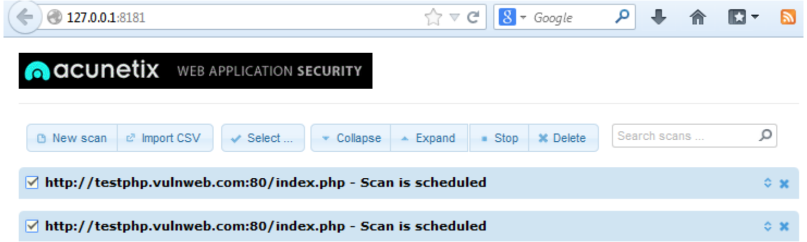
□ Allow remote computers to connect

□ Use HTTPS

□ Require authentication

Acunetix 的计划任务，主要特性如下:

1. 可用于大量扫描，扫描结果保存在 C:\Users\Public\Documents\Acunetix WVS 8\Saves\。
2. 扫描结束，可以使用邮件通知。
3. 可设定计划时间，什么时候允许扫描，什么时候不允许.



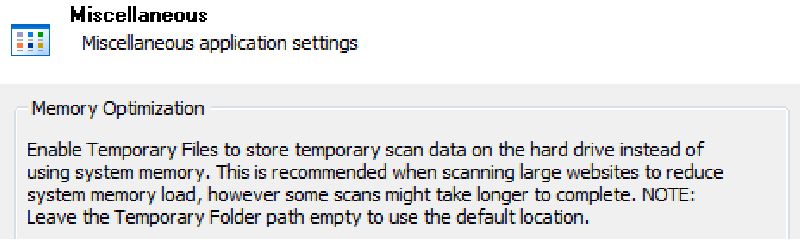
☑ http://testphp.vulnweb.com:80/index.php - Scan is scheduled

☑ http://testphp.vulnweb.com:80/index.php - Scan is scheduled

Miscellaneous

使用临时文件夹，减小内存开销，默认爬行时，最大内存是 1024M

Wvs 密码保护，设定一个密码，只有通过验证才能使用 wvs.



Miscellaneous

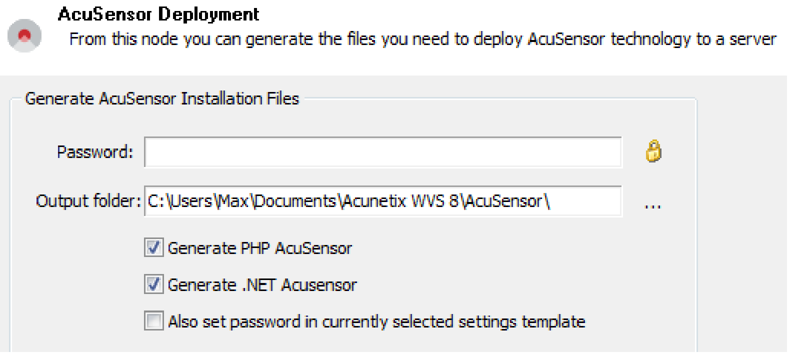
Miscellaneous application settings

Memory Optimization

Enable Temporary Files to store temporary scan data on the hard drive instead of using system memory. This is recommended when scanning large websites to reduce system memory load, however some scans might take longer to complete. NOTE: Leave the Temporary Folder path empty to use the default location.

AcuSensor Deployment

Acunetix 传感器功能，用于提升漏洞审查能力.具体用法请查阅 wvs 手册.



AcuSensor Deployment

From this node you can generate the files you need to deploy AcuSensor technology to a server

Generate AcuSensor Installation Files

Password:

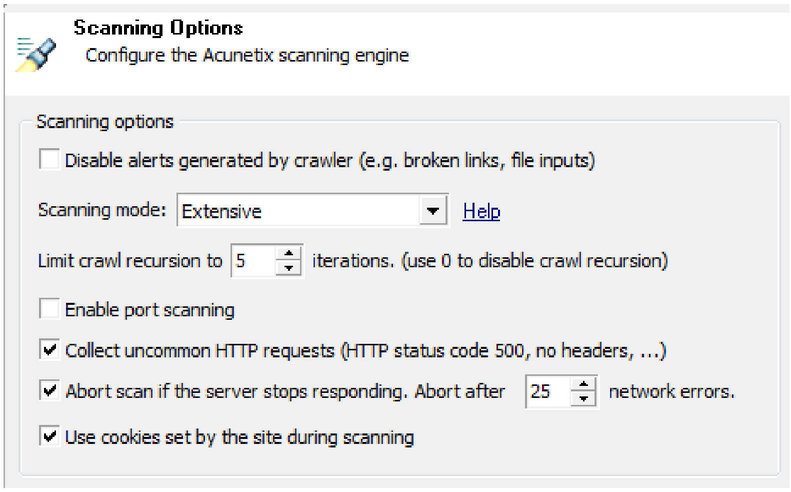
Output folder: C:\Users\Max\Documents\Acunetix WVS 8\AcuSensor\ ...

☑ Generate PHP AcuSensor

☑ Generate .NET Acusensor

□ Also set password in currently selected settings template

Scan Settings



Scanning Options

Configure the Acunetix scanning engine

Scanning options

□ Disable alerts generated by crawler (e.g. broken links, file inputs)

Scanning mode: Extensive Help

Limit crawl recursion to 5 iterations. (use 0 to disable crawl recursion)

□ Enable port scanning

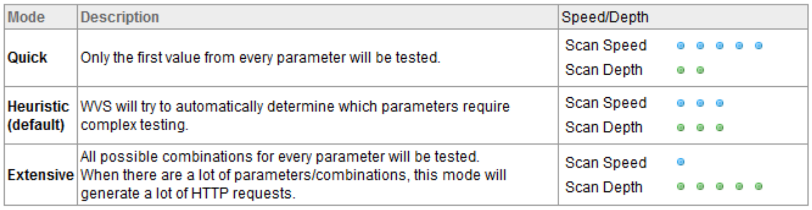
☑ Collect uncommon HTTP requests (HTTP status code 500, no headers, ...)

☑ Abort scan if the server stops responding. Abort after 25 network errors.

☑ Use cookies set by the site during scanning

是否关闭 crawler 警告(坏链接，文件输入等)

扫描模式:Quick|Heuristic(default)|Extensive



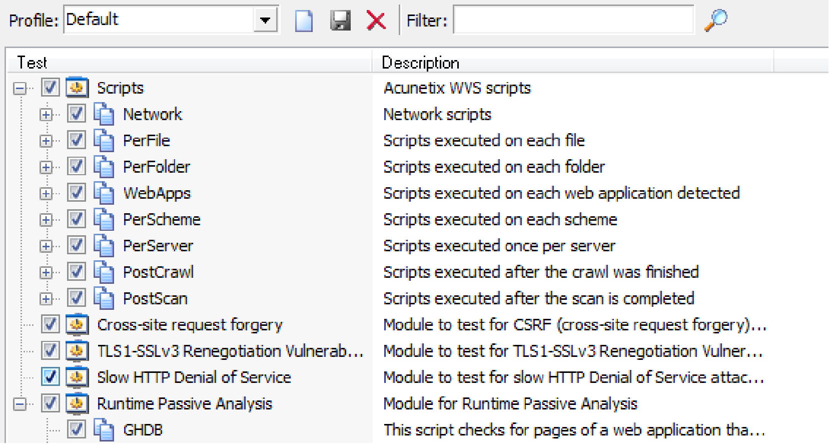
Mode	Description	Speed/Depth
Quick	Only the first value from every parameter will be tested.	Scan Speed ● ● ● ● ● Scan Depth ● ●
Heuristic (default)	WVS will try to automatically determine which parameters require complex testing.	Scan Speed ● ● ● Scan Depth ● ● ●
Extensive	All possible combinations for every parameter will be tested. When there are a lot of parameters/combinations, this mode will generate a lot of HTTP requests.	Scan Speed ● Scan Depth ● ● ● ● ●

爬行深度，默认是 5。

是否开启端口扫描功能.
是否收集不常规的 HTTP 请求.
服务器不响应的时候是否忽略扫描，可设定多少次错误以后开始忽略.
在扫描过程中，是否使用网站设定的 cookie
添加其他网站服务器文件路径(默认只扫描同域名下的网站文件)

注意: 其他功能在此略过(请按照自己的需求定制).

Scanning Profiles



Profile: Default Filter:

Test	Description
☑ Scripts	Acunetix WVS scripts
☑ Network	Network scripts
☑ PerFile	Scripts executed on each file
☑ PerFolder	Scripts executed on each folder
☑ WebApps	Scripts executed on each web application detected
☑ PerScheme	Scripts executed on each scheme
☑ PerServer	Scripts executed once per server
☑ PostCrawl	Scripts executed after the crawl was finished
☑ PostScan	Scripts executed after the scan is completed
☑ Cross-site request forgery	Module to test for CSRF (cross-site request forgery)...
☑ TLS1-SSLv3 Renegotiation Vulnerab...	Module to test for TLS1-SSLv3 Renegotiation Vulner...
☑ Slow HTTP Denial of Service	Module to test for slow HTTP Denial of Service attac...
☑ Runtime Passive Analysis	Module for Runtime Passive Analysis
☑ GHDB	This script checks for pages of a web application tha...

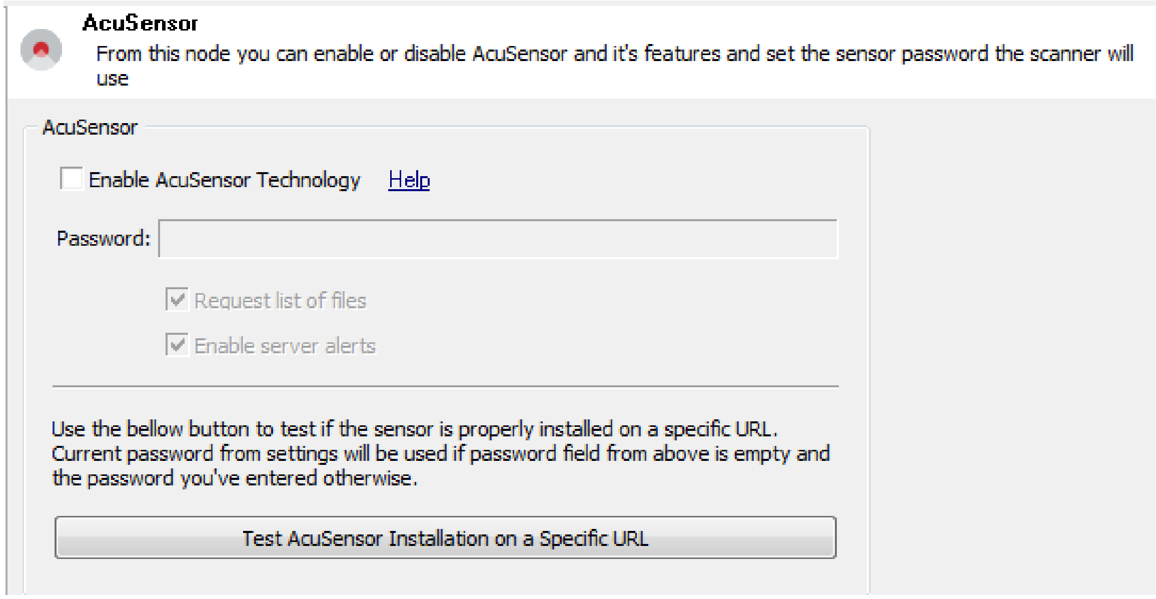
Scanning profile 可设定扫描重点，Acunetix WVS 默认提供 15 中配置，可参照前面提到的内容.
按照扫描重点，亦可配置按需配置.
配置文件位于 C:\ProgramData\Acunetix WVS 8\Data\Profiles
配置文件依赖扫描所需的脚本 C:\ProgramData\Acunetix WVS 8\Data\Scripts\

Appendix A

案例一:

```
GET /redir.php?r=ACUSTART%0d%0aACUEND HTTP/1.1
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect: enabled
Referer: http://testphp.vulnweb.com:80/index.php
Host: testphp.vulnweb.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/5.0)
Accept: */*
```

Acunetix WVS 默认启用 AcuSensor，因此多数请求中都含有红色标识信息。IDS/FireWall 设定某些规则，很容易据它于千里之外。实际检测时，请将其关闭。(关于 AcuSensor 机制，请阅读 WVS 用户手册)



AcuSensor

From this node you can enable or disable AcuSensor and it's features and set the sensor password the scanner will use

AcuSensor

□ Enable AcuSensor Technology Help

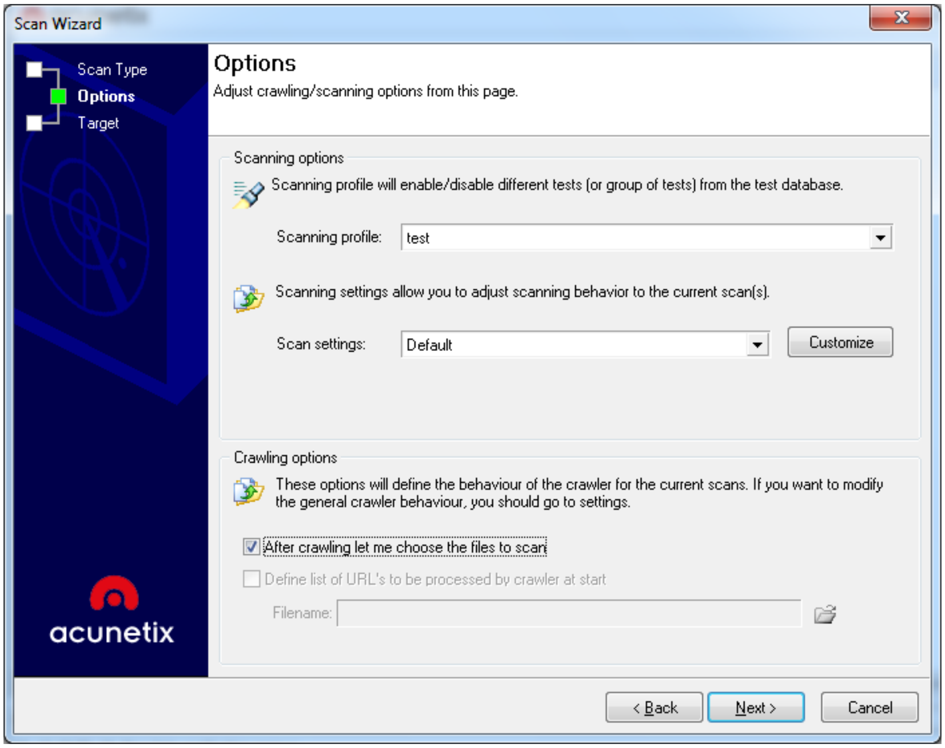
Password:

☑ Request list of files

☑ Enable server alerts

Use the bellow button to test if the sensor is properly installed on a specific URL. Current password from settings will be used if password field from above is empty and the password you've entered otherwise.

案例二:



Options

Adjust crawling/scanning options from this page.

Scanning options

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

Scanning profile: test

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

Scan settings: Default

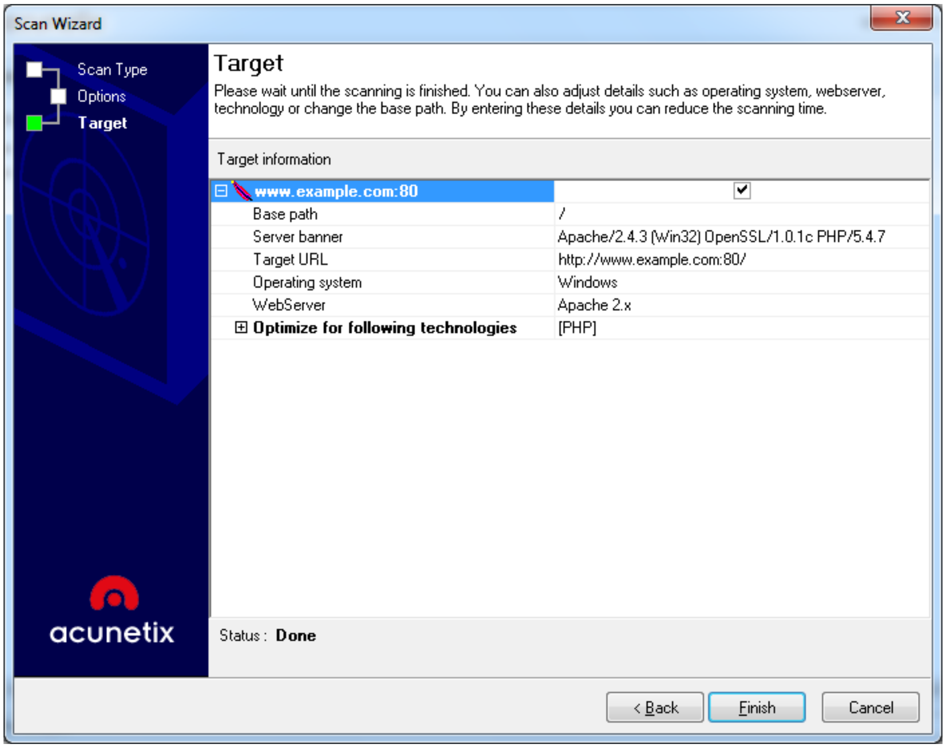
Crawling options

These options will define the behaviour of the crawler for the current scans. If you want to modify the general crawler behaviour, you should go to settings.

☑ After crawling let me choose the files to scan

□ Define list of URL's to be processed by crawler at start

Filename:



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

⊟ www.example.com:80	☑
Base path	/
Server banner	Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
Target URL	http://www.example.com:80/
Operating system	Windows
WebServer	Apache 2.x
⊞ **Optimize for following technologies**	[PHP]

Status : **Done**

上图 Options 到 Target 的设置，会完成两次 HTTP/HTTPS 请求，如下所示:

第一次 HTTP 请求:

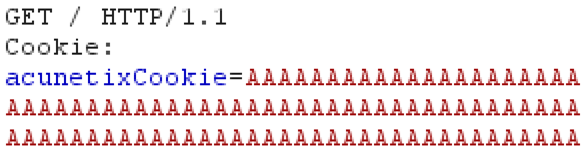
```
 GET / HTTP/1.1
 Pragma: no-cache
 Host: www.example.com
 Connection: Close
 Accept-Encoding: gzip,deflate
 User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0)
 Accept: */*
```

第二次 HTTP 请求:

```
 GET /acunetix-wvs-test-for-some-inexistent-file HTTP/1.1
 Pragma: no-cache
 Host: www.example.com
 Connection: Close
 Accept-Encoding: gzip,deflate
 User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0)
 Accept: */*
```

Acunetix WVS 在获取服务器版本/脚本语言类型的时候，发送含有特征字符串的请求。此字符串可用于设定 IDS/Firewall 规则。

类似的情况还有:

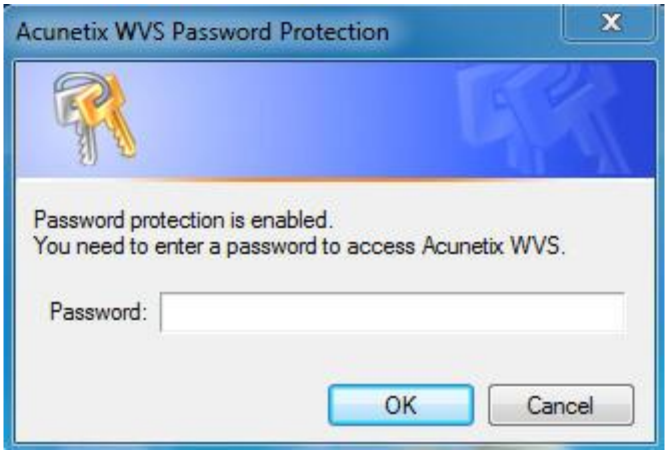


```
GET / HTTP/1.1
Cookie:
acunetixCookie=AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Appendix B

Bypass Acunetix Password Protection

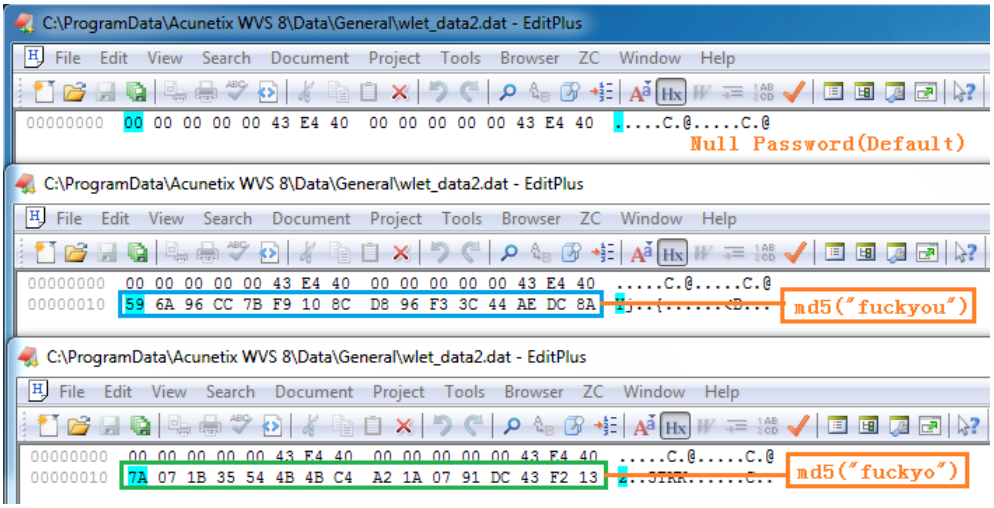
Set a password to prevent unauthorized use of Acunetix WVS.
[Menu]: Configuration >> Application Settings >> Miscellaneous >> Password Protection.
The default password is null.
If you set a password, it needs authentication to use it.



Acunetix WVS Password Protection

Password protection is enabled.
You need to enter a password to access Acunetix WVS.

Password:



C:\ProgramData\Acunetix WVS 8\Data\General\wlet_data2.dat - EditPlus

```
00000000  00 00 00 00 00 43 E4 40  00 00 00 00 00 43 E4 40  .....C.@.....C.@
```

Null Password(Default)

C:\ProgramData\Acunetix WVS 8\Data\General\wlet_data2.dat - EditPlus

```
00000000  00 00 00 00 00 43 E4 40  00 00 00 00 00 43 E4 40  .....C.@.....C.@
00000010  59 6A 96 CC 7B F9 10 8C  D8 96 F3 3C 44 AE DC 8A  Yj..{......<D...
```

md5("fuckyou")

C:\ProgramData\Acunetix WVS 8\Data\General\wlet_data2.dat - EditPlus

```
00000000  00 00 00 00 00 43 E4 40  00 00 00 00 00 43 E4 40  .....C.@.....C.@
00000010  7A 07 1B 35 54 4B 4B C4  A2 1A 07 91 DC 43 F2 13  z..5TKK......C..
```

md5("fuckyo")

Appendix C

简单介绍一下 Directory_And_File_Checks.profile 所用的 payload，希望看完这些 payload 大家有些新的想法，如下所示:

```
..
../security.7z
../security.bak
../security.bz2
../security.cfg
../security.csv
../security.dump
../security.gz
../security.ini
../security.old
../security.ost
../security.pst
../security.sh
../security.sln
../security.sql
../security.sql.bz2
../security.sql.gz
../security.tar
../security.tar.bz2
../security.tar.gz
../security.zip
```

```
.adm
.admin
.bash_history
.bashrc
.bzr
.bzr/README
.cvsignore
.DS_Store
.git
.git/config
.gitignore
.hg
.hg/requires
.history
.htaccess
.htpasswd
.idea
.idea/workspace.xml
.listing
.passwd
.ssh
.subversion
.svn
.svn/entries
.user.ini
/WS_FTP.LOG
```

_mmServerScripts/MMHTTPDB.asp
_mmServerScripts/MMHTTPDB.php

a6JiF.html
access.log
acunetix_invalid_filename.aspx
admin.htm
admin.html
admin.php
ajax.php
apc.php
aspxspy.aspx
auth_user_file.txt

bigdump.php

c99.php
c99shell.php
c-h.v2.php
CHANGELOG.txt
citydesk.xml
cleanup.log
clients.mdb
clients.sqlite
cmdasp.asp
common.inc
config.inc
config.php
config/database.yml
configuration.php
connect.inc
customers.csv
customers.log
customers.mdb
customers.sql
customers.sql.gz
customers.sqlite
customers.txt
customers.xls

data.mdb
data.sqlite
database.csv
database.inc
database.log
database.mdb
database.php
database.sql
database.sqlite
database_credentials.inc
databases.yml
db.csv
db.inc
db.log
db.mdb
db.sql
db.sqlite
db1.mdb
db1.sqlite
dbaccess.log
debug.inc
debug.log
debug.php
dra.php

environment.rb
error.log
errors.log

global.asa.bak
global.asa.old
global.asa.orig
global.asa.temp
global.asa.tmp
global.asax.bak
global.asax.old
global.asax.orig
global.asax.temp
global.asax.tmp

head.php
htaccess.bak
htaccess.txt

i.php
id_dsa.ppk
img/xampp.ico
index.php
info.php
info.txt
install.log
install.txt

localhost.sql
log.htm
log.html
log.mdb
log.sqlite
log.txt
logs.htm
logs.html
logs.mdb
logs.sqlite
lol.php

members.csv
members.log
members.mdb
members.sql
members.sql.gz
members.sqlite
members.txt
members.xls
mfHhm.mdb
mt-check.cgi

navi.php
nst.php
nstview.php

orders.csv
orders.log
orders.sql
orders.sql.gz
orders.txt
orders.xls
output-build.txt

password.sqlite
passwords.mdb
passwords.sqlite
personal.mdb
personal.sqlite
php.ini
php.php
php-backdoor.php
phpinfo.php
phpinfo.php5
phpliteadmin.php
phpThumb.php
pi.php
pi.php5
private.key
private.mdb
private.sqlite
propel.ini
publication_list.xml

r.php
r57.php
r57eng.php
r57shell.php
r58.php
README.txt
register.php
rst.php

sales.csv
sales.log
sales.sql
sales.sql.gz

sales.txt
sales.xls
schema.sql
schema.yml
security.7z
security.bak
security.bz2
security.cfg
security.csv
security.dump
security.gz
security.ini
security.old
security.ost
security.php
security.pst
security.sh
security.sln
security.sql
security.sql.bz2
security.sql.gz
security.tar
security.tar.bz2
security.tar.gz
security.zip
server.log
service.asmx
settings.php
shell.php
simple-backdoor.php
sql.inc
sqlnet.log
system.log

tar.bz2
tar.gz
temp.php
test.asp
test.aspx
test.chm
test.htm

```
test.html
test.jsp
test.mdb
test.php
test.sqlite
test.txt
Trace.axd


uploadify.php
user.txt
users.csv
users.db
users.ini
users.log
users.mdb
users.sql
users.sql.gz
users.sqlite
users.txt
users.xls


validator.php

web.config
web.config.bak
web.config.bakup
web.config.old
web.config.temp
web.config.tmp
webadmin.php
webstats.html
wwwstats.htm

xhtnU.mdb
xmlrpc_server.php

zehir.php
zIVnUwyoNN.jsp
```

```
0
21%
23%
24%
40%
1
2
3
4
5
6
7
8
9
10
2008
2009
2010
2011
2012
2013
'
-
%21%21
%21%21%21
%21install
%21test
%2b
%3f
%7eadmin
%7eftp
%7eguest
%7elog
%7elogs
%7enobody
%7eroot
%7ewww
/971617%40
?=967155%40
?925570%40
```

```
?id=1'"1000
_
__MACOSX
__SQL
_adm
_admin
_errors
_files
_include
_install
_layouts
_logs
_mmServerScripts
_old
_pages
_private
_source
_SQL
_sqladm
_src
_test
_tests
_www
1'"1000
1'"3000
905783%40
a
access
access_log
accesslog
access-log
accounts
ad
addons
admin
admin_
admin_files
admin_login
admin_logon
admin0
admin1
```

adminconsole
admin-console
adminfiles
administration
administrative
administrator
administrivia
adminpanel
admins
ads
ainstall
apps
archives
aspnet
atom
audio
auth
b
bac
backup
backups
bak
banner
banners
base
beta
billing
bin
blogs
browse
bugs
build
c
cache
cache_html
cerberusweb
CHANGELOG
chat
ckeditor
class
classes

```
client
clients
cmd
CMS
common
compat
conf
config
console
content
contents
controller
core
cp
csv
customer
customers
CVS
CVS/Root
d
dat
data
database
db
db2
dbase
de
Default
demo
dev
devel
developer
developers
devels
dl
doc
documents
down
download
downloads
dump
```

```
e
E7Amz
edit
editor
en
english
err
error
error_log
errorlog
error-log
errors
etc
example
examples
Exchange
export
f
fck
FCKeditor
feed
file
fileadmin
filemanager
files
fileserver
flash
folder
fonts
forgot
forms
fP8OP
fpadmin
fr
ftp
g
global
globals
graphics
group
h
```

help
horde
htdocs
html
i
icon
icons
id_dsa
id_rsa
iisadmin
iishelp
image
images
img
img/
import
inc
include
includes
incomming
index
index/1'"1000
index/1'"3000
index_files
info
ini
install
install_
INSTALL_admin
installer
internal
intranet
invoker
j
jdbc
jmx-console
js
json
k
l
languages

```
latest
lib
libs
list
log
logfile
logfiles
login
logs
lostpassword
m
main
management
manager
manual
manuals
media
member
memberlist
members
menu
messages
mime
misc
modules
mp3
msql
mssql
mt
music
mysql
n
New%20Folder
New%20folder%20(2)
o
oauth
odbc
old
old_files
oldfiles
oracle
```

orders
p
package
page
pass
passwd
password
passwords
personal
pgadmin
photo
php
phpldapadmin
phpmyadmin
phpmyadmin0
phpmyadmin1
phpPgAdmin
phpsysinfo
phpThumb
pics
pictures
plugins
plupload
pma
portal
private
profile
projects
prv
q
r
README
recaptcha
release
report
reseller
reset
resources
restricted
root
rss

s
sample
samples
save
script
scripts
search
secret
secrets
secure
secured
security
servlet
session
sessions
settings
setup
share
shell
signup
site
site_admin
siteadmin
smarty
snapshot
soap
space
spool
sql
sqladm
src
staff
static
statistics
stats
storage
svn
swf
swfupload
sysadmin
sysadmins

sysbackup
system
t
tag
tags
tar
TEMP
templates
test
test_
test0
test1
testing
tests
testweb
text-base
themes
thread
threads
thumb
thumbnail
TMP
TODO
tools
tst
tsweb
types
updates
upgrade
upload
uploader
uploadify
uploads
uri
url
user
user_uploads
useradmin
usercp
UserFile
UserFiles

users
utf8
v
v1
version
view
w
warez
web
webaccess
webadmin
webmin
WebService
wizards
wp
wp-admin
wp-content
wp-includes
WS_FTP
www
xls
xml
xmlrpc
z
zip
zipfiles
zips

更多关于扫描器的知识，欢迎大家一起探讨.