- 基础
  - awvs11功能介绍
  - awvs10功能介绍
  - awvs扫描漏洞
  - docker版本awvs
- Acunetix Manual Pen Testing Tools
- 性能测试
  - sqlmap/burp/awvs 扫描能力对比
  - 爬虫能力对比
- awvs配置优化
- 翻译

Referer:

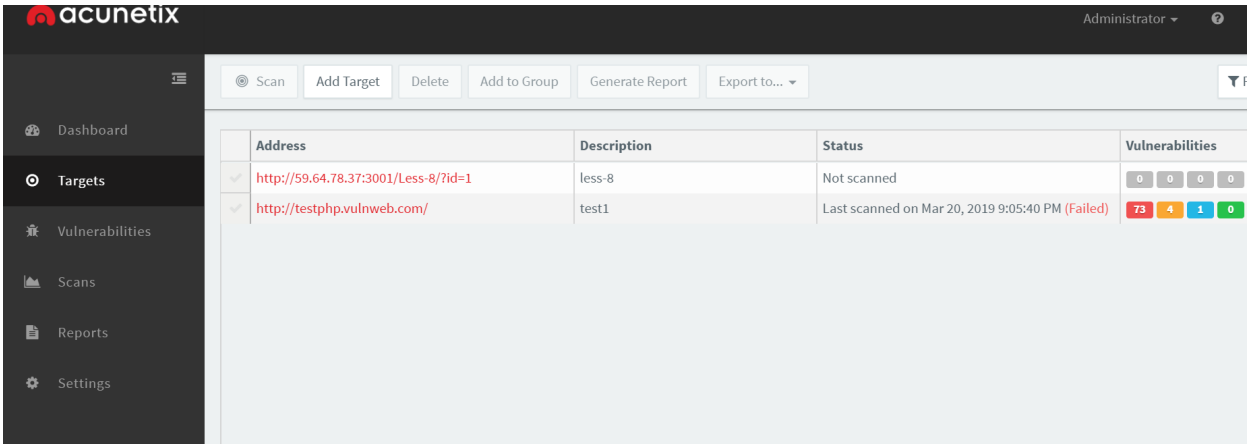
- Acunetix Support – Help and Documentation https://www.acunetix.com/support/
- awvs v12 Product Manual https://www.acunetix.com/resources/wvsmanual.pdf
- AWVS详细基本用法 https://zhuanlan.zhihu.com/p/30319661

基础

Acunetix Web Vulnerability Scanner是Acunetix 公司开发的一块自动化测试工具，扫描器架构可以分为: `Acunetix Web Interface`, `Web Scanner(Crawling,Scanning)`, `AcuSensor Technology Agent`, `AcuMonitor Technology`, `Reporter`几个部分

awvs11功能介绍

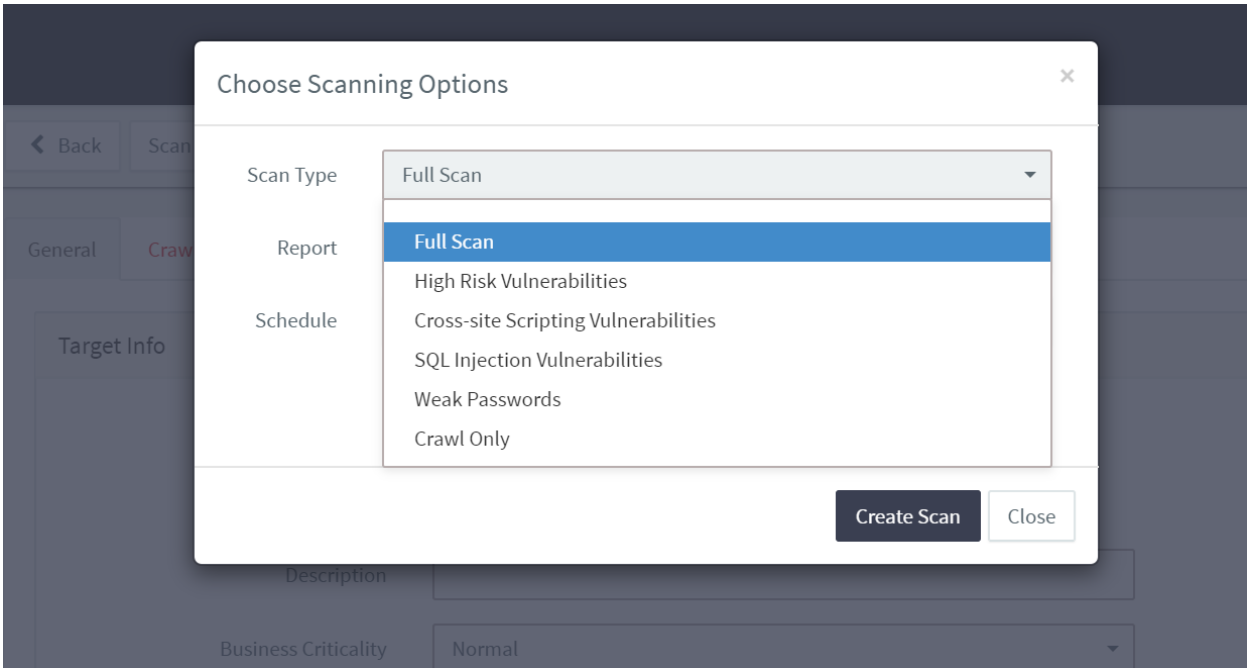
1. web界面: https://localhost:3443/ 账号密码: 2461805286@qq.com



相较于awvs10的客户端界面，Web界面界面功能精简了很多， 主界面主要设置了dashboard,Targets,Vulnerailities, Scans, Reports, Settings.

- Targets 功能主要是对人物的增删改查操作。
- Vulnerabilities 主要是对漏洞进行展示
- Scans: 扫描细节展示，提供扫描信息展示界面，漏洞信息，网站结构，网站扫描结束时间和开始时间

2. 扫描设置Profile

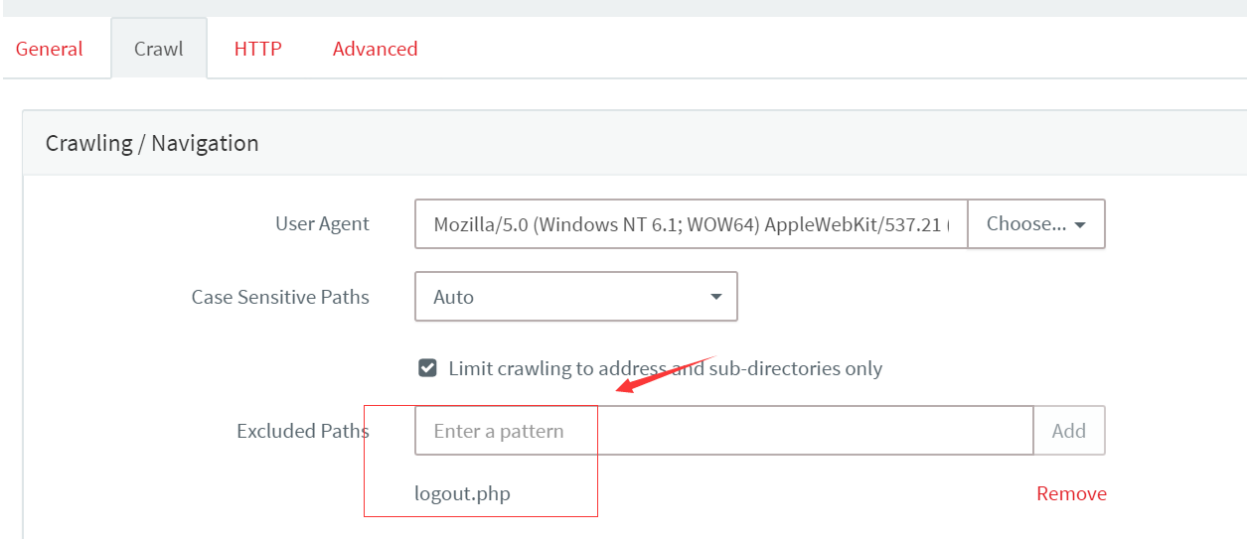


- Full Scan: 完全扫描
- High Risk Vul: 高危漏洞扫描: 扫描66种高危漏洞，包括常见Web安全漏洞，常见中间件的漏洞
- Cross Site Scripting: xss扫描
- SQL Injection: SQL注入扫描
- Weak passwords 弱口令扫描
- Crawl Only: 爬虫

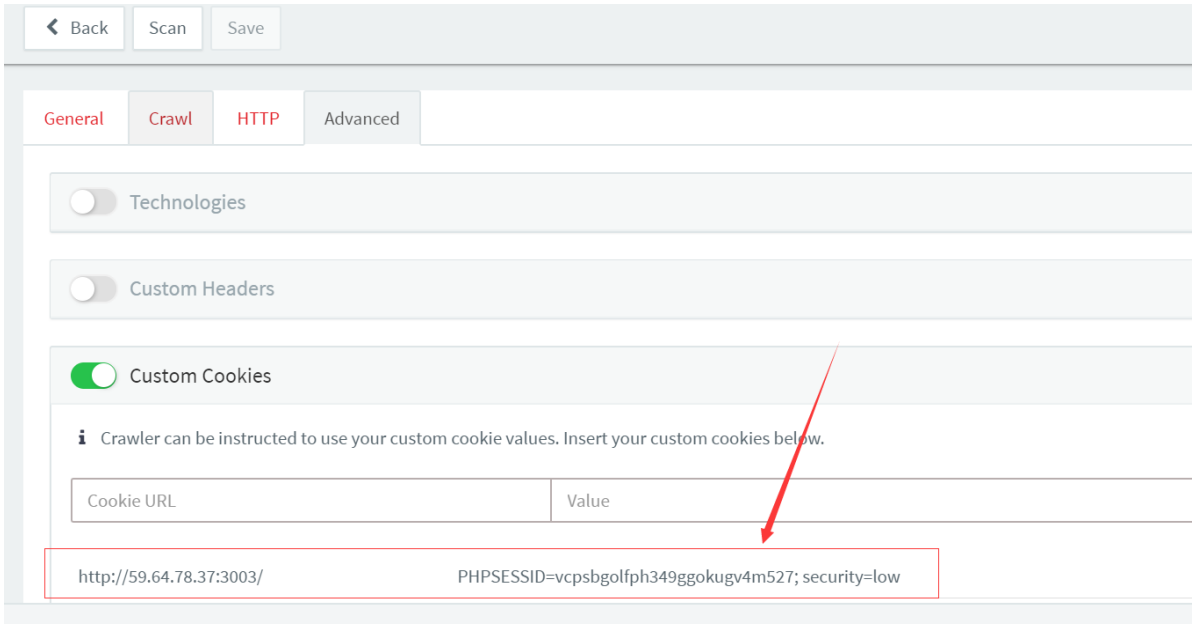
3. 扫描类型

1. 带Cookie扫描

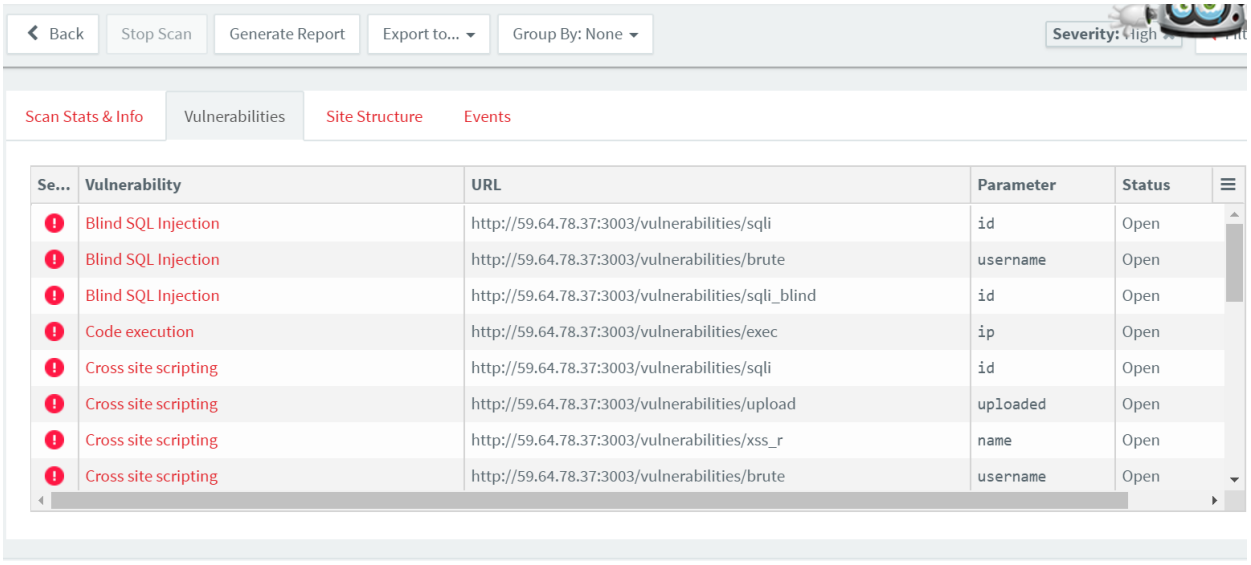
测试目标DVWA sqli 盲注， - 因为爬虫可能会爬取到logout.php因为去除该爬取目录:



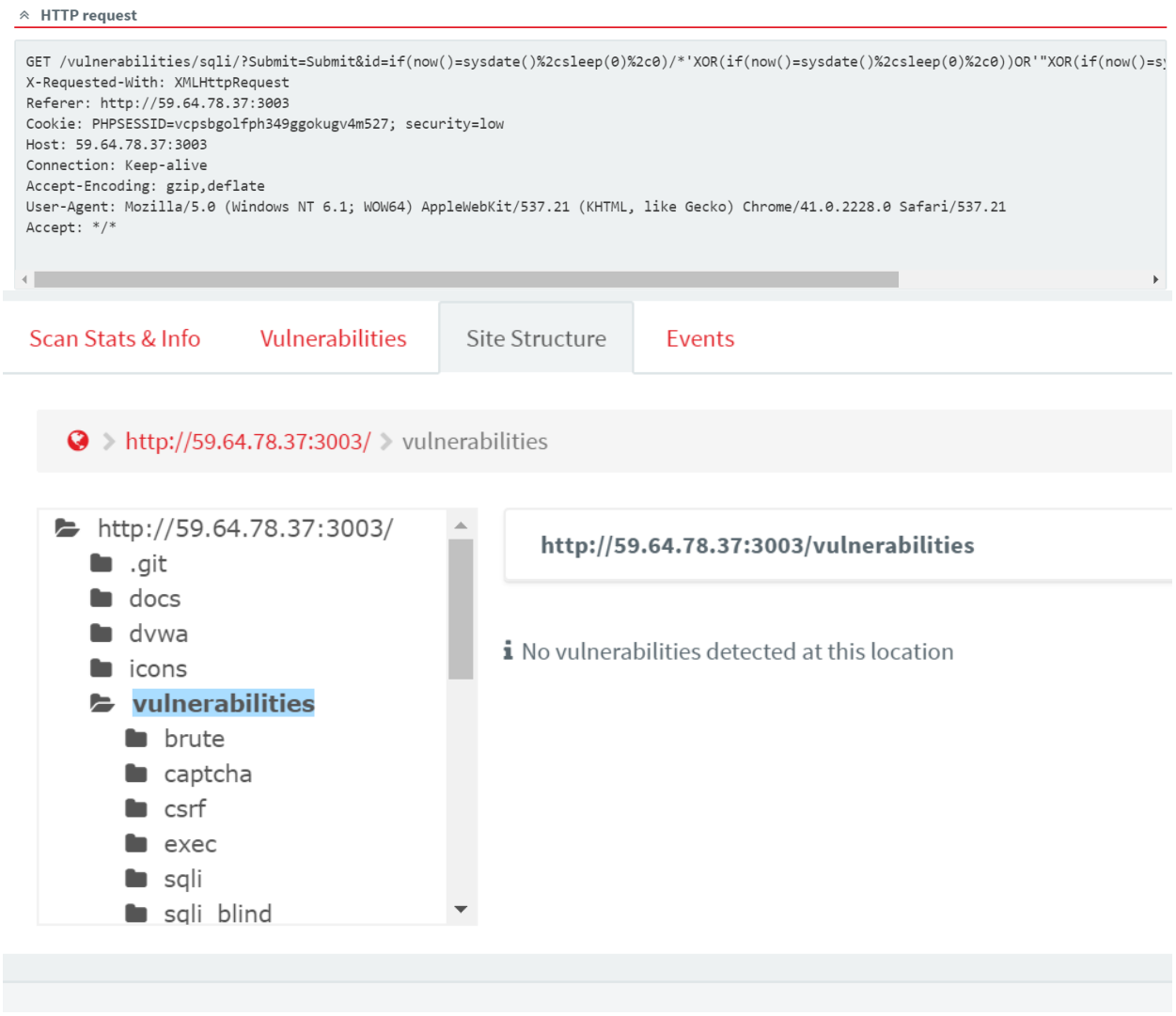
- 加上自定义的Cookie



扫描结果:

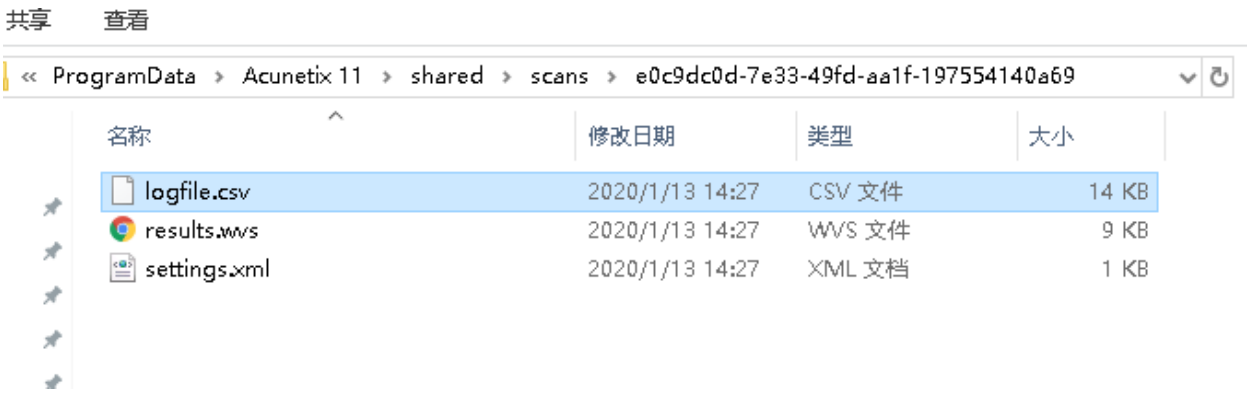


Se...	Vulnerability	URL	Parameter	Status
!	Blind SQL Injection	http://59.64.78.37:3003/vulnerabilities/sqli	id	Open
!	Blind SQL Injection	http://59.64.78.37:3003/vulnerabilities/brute	username	Open
!	Blind SQL Injection	http://59.64.78.37:3003/vulnerabilities/sqli_blind	id	Open
!	Code execution	http://59.64.78.37:3003/vulnerabilities/exec	ip	Open
!	Cross site scripting	http://59.64.78.37:3003/vulnerabilities/sqli	id	Open
!	Cross site scripting	http://59.64.78.37:3003/vulnerabilities/upload	uploaded	Open
!	Cross site scripting	http://59.64.78.37:3003/vulnerabilities/xss_r	name	Open
!	Cross site scripting	http://59.64.78.37:3003/vulnerabilities/brute	username	Open



4. debug调试模式

Targets -> Advanced -> Debug scans for this target (打勾), 之后扫完便会产出三个文件(logfile.csv, results.wvs, settings.xml)，放在 C:\ProgramData\Acunetix 11\shared\scans\ 底下，并以zip储存。



awvs10功能介绍

1. alerts 四种模式

```
High(红色)
Medium(橙色)
Low(蓝色)
Informational(绿色)
```

2. 扫描配置

新建一个扫描包括五个准备: 1) SCAN TYPE 2)options 3)target 4)login 5)finish

1. SCAN TYPE

- ①：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。
- ②：Scan using saved crawling results：导入WVS内置 site crawler的爬行到的结果，然后对爬行的结果进行漏洞扫描。
- ③：Access the scheduler interface：如果被扫描的网站构成了一个列表形式(也就是要扫描多个网站的时候)，那么可以使用Acunetix的Scheduler功能完成任务，访问 http://localhost:8183，扫描后的文件存放在“C:/Users/Public/Documents/Acunetix WVS 10/Saves”.

2. OPTIONS

Scanning options：侧重扫描的漏洞类型设置,包含16种侧重检测类型，如下

进入高级之后分别是:

①：在爬行结果之后选择我们需要扫描哪些文件 ②：自定义从哪里开始扫描，导入txt文件，例如扫描http://www.baidu.com，不想从根路径开始扫，而从二级目录http://www.baidu.com/test/，将其保存到txt文件中之后将从test二级目录开始扫描 ③：爬行的时候使用外部测试工具，蜘蛛爬行的过程中将运行您设置的命令，以及超时时间设置 ④：设置包含一个火狐扩展插件Selenium IDE生成的HTML文件，蜘蛛爬行的过程中将会根据它来进行爬行。

3. Target: 包含目标的一些信息

4)Login: 填写用户名密码，尝试自动登录.在某些情况下，可以自动识别网站的验证。

awvs扫描漏洞

漏洞类型可以参考:

- Acunetix Web Vulnerabilities Index https://www.acunetix.com/vulnerabilities/web/

awvs对漏洞类型分了45种: `Abuse Of Functionality,Arbitrary File Creation,Authentication Bypass,Bruteforce Possible,Buffer Overflow,CSRF,Code Execution,Configuration,Crlf Injection,Default Credentials,Denial Of Service,Dev Files,Directory Listing,Directory Traversal,Error Handling,File Inclusion,Http Parameter Pollution,Http Response Splitting,Information Disclosure,Insecure Admin Access,Internal Ip Disclosure,Known Vulnerabilities,Ldap Injection,Malware,Missing Update,Needless Service,Network Alert,Privilege`

`Escalation,RCE,Remote Code Execution,SSRF,Sensitive Data Not Over Ssl,Session Fixation,Source Code Disclosure,Sql Injection,Test Files,Unauthenticated File Upload,Url Redirection,W3 Total Cache,Weak Credentials,Weak Crypto,XFS,XSS,XXE,Xpath Injection`

docker版本awvs

- https://github.com/fengziHK/awvs_190703137

```
git clone https://github.com/fengziHK/awvs_190703137.git
wget https://s3.amazonaws.com/a280ccaaf904330a389db759e6275285/acunetix_trial.sh
docker build -t awvs_2019_07 ./
docker run -d -p 51443:13443 --name wvs07 awvs_2019_07
docker exec -it -u root wvs07 /bin/bash
//运行patch
./patch_awvs

账号密码:
admin@test.com
Test123...
```

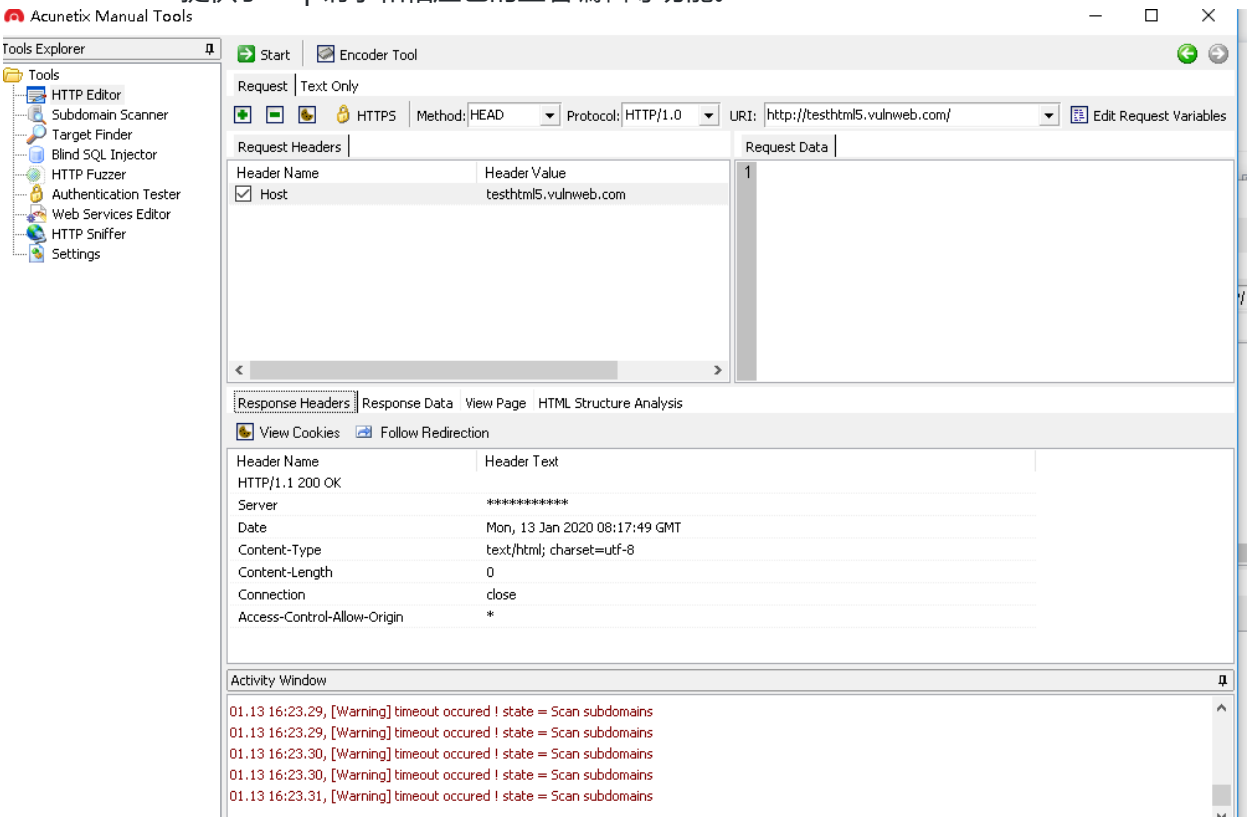
Acunetix Manual Pen Testing Tools

- https://www.acunetix.com/vulnerability-scanner/free-manual-pen-testing-tools/

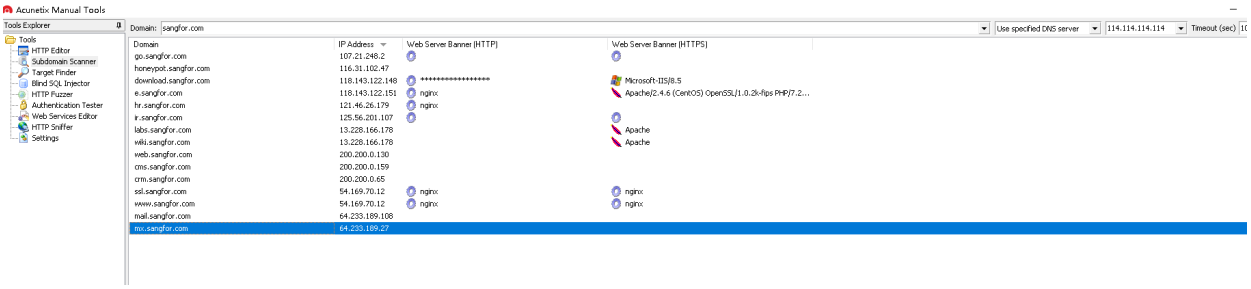
awvs11把一些常见的信息收集小工具独立出来了。这些工具虽然功能不是很强大，但很实用。这些工具包括:

- HTTP Editor
- Subdomain Scanner
- Target Finder
- Blind SQL Injector
- HTTP Fuzzer
- Authentication Tester
- Web Services Editor
- HTTP Sniffer

HTTP Editor 提供了http请求和相应包的查看编辑等功能。



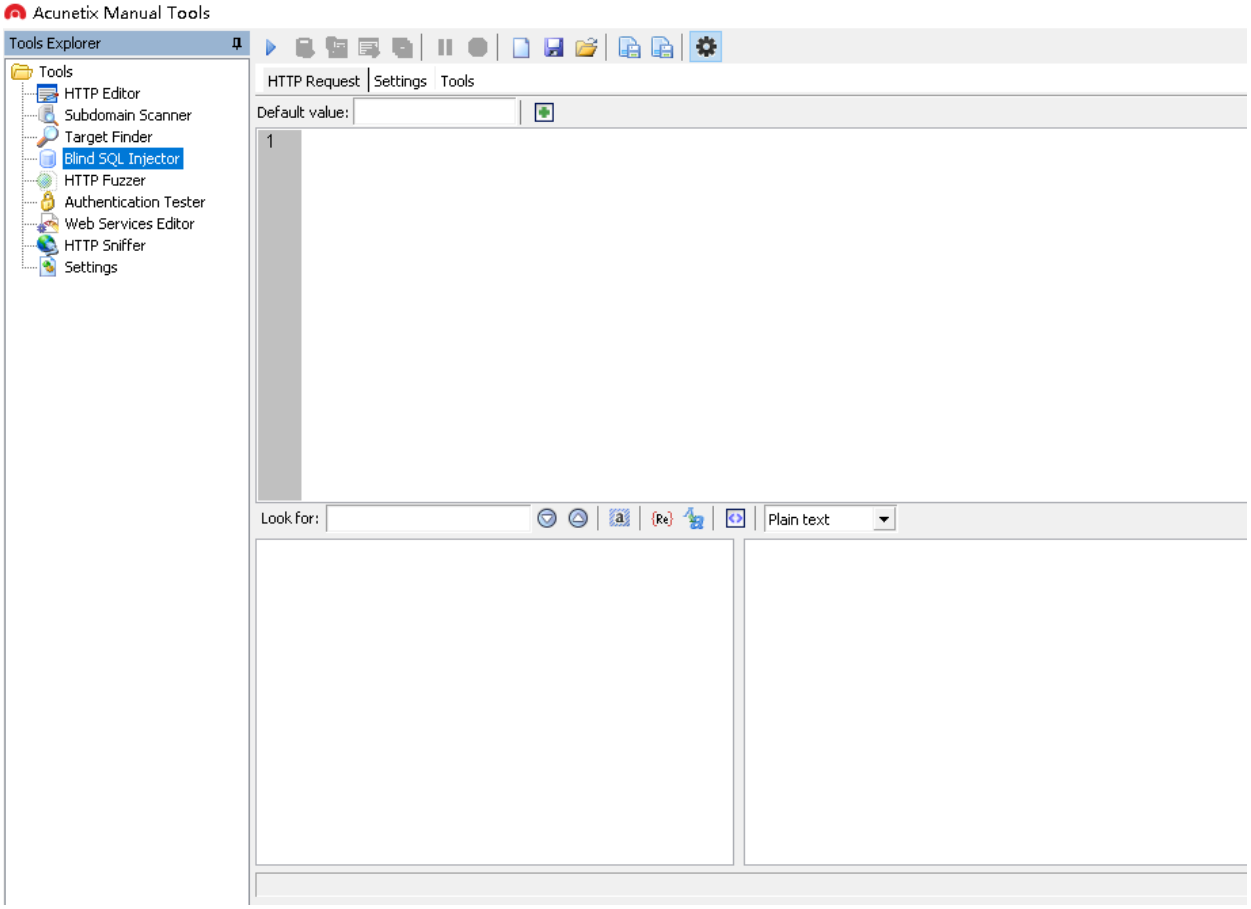
subdomain scanner 该功能提供了简单的子域名爆破的功能，可能是内置字典比较小，爆破出来的子域名不是很多。会探测http,https页面的banner, 耗时3min.



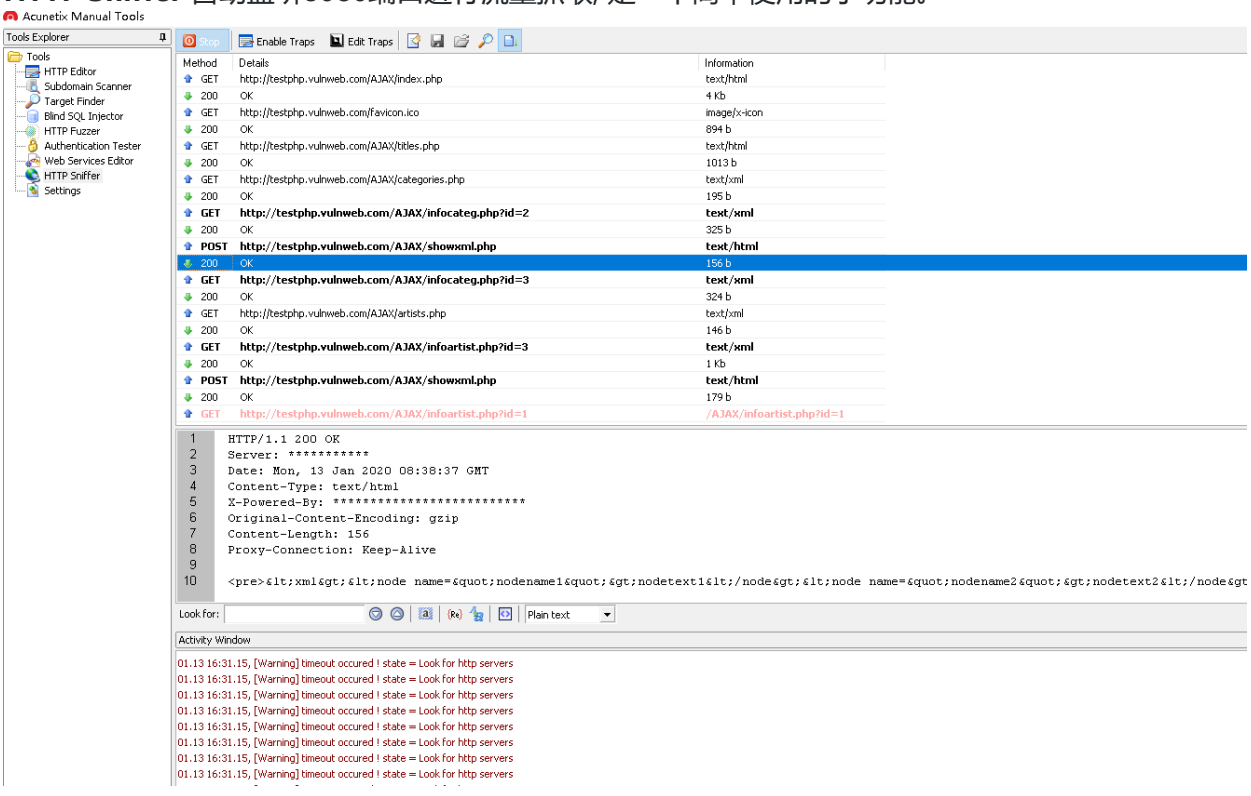
Target Finder 主机探测+常见开放端口， 好像是单线程，速度比较慢。

```
example.com Scan a host by DNS hostname
192.168.0.1 Scan a host by IP address
192.168.0.1-30  Scan all hosts between two IP addresses
192.168.0.0/24  Scan all hosts in a subnet (CIDR format)
```

Blind SQL Injector

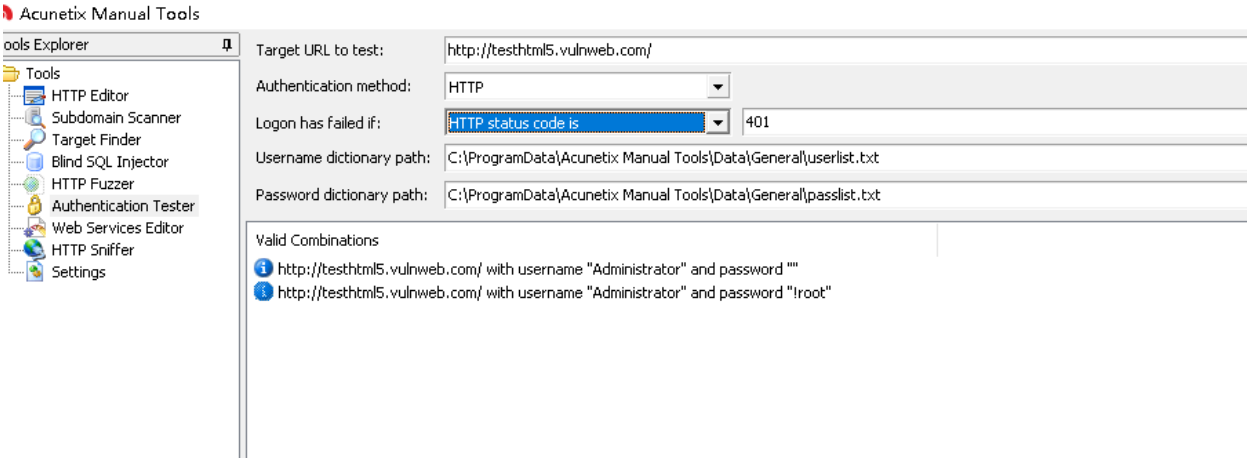


HTTP Sniffer 自动监听8080端口进行流量抓取, 是一个简单使用的小功能。



缺点: 只能监听http的站点，无法监听https的站。

Authentication Tester 字典爆破



性能测试

sqlmap/burp/awvs 扫描能力对比

- 靶机: awvs
- sqlmap扫描模式: `sqlmap.py -l data.req --batch -smart`
- awvs的扫描模式: 高危漏洞扫描

1-10关

扫描器	第一关	第二关	第三关	第四关	第五关	第六关	第七关	第八关	第九关	第十关
burpsuite	存在	存在	存在	存在	存在	存在	存在	存在	存在	不存在
sqlmap	存在	存在	存在	存在	存在	存在	存在	存在	存在	不存在
awvs	存在	存在	存在	存在	存在	存在	存在	存在	存在	存在

11-20关

扫描器	第十一关	第十二关	第十三关	第十四关	第十五关	第十六关	第十七关	第十八关	第十九关
burpsuite	存在	存在	存在	存在	存在	不存在	不存在	不存在	不存在

扫描器	第十一关	第十二关	第十三关	第十四关	第十五关	第十六关	第十七关	第十八关	第十九关
sqlmap	存在	存在	存在	存在	不存在	不存在	不存在	不存在	不存在
awvs	存在	存在	存在	存在	存在	存在	存在	不存在	不存在

数据分析:

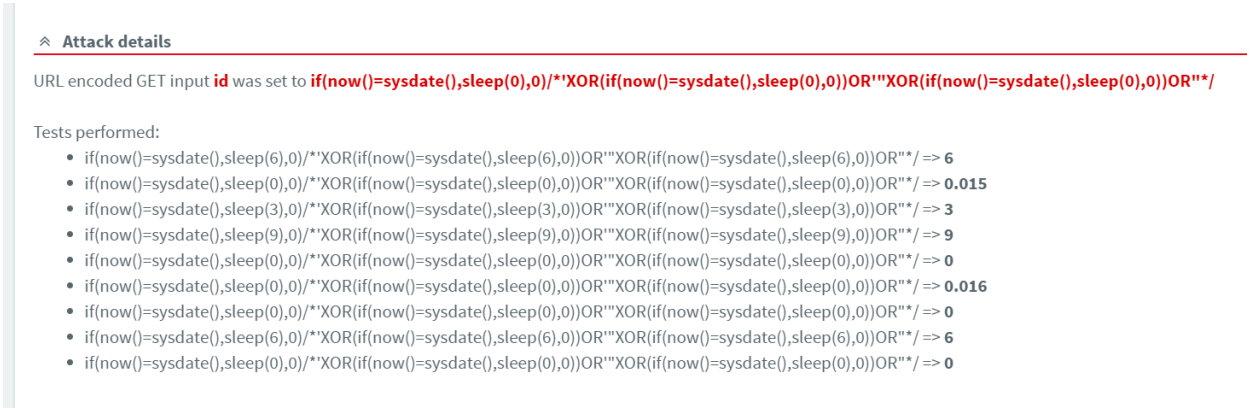
1. 在第十关，第十五关，第十六关，第十七关中，sqlmap和burpsuite都每没扫描出漏洞(十五关burpsuite可扫描出来)，但awvs可以扫描出来，证明出awvs的漏洞扫描能力在burpsuite和sqlmap之上的。

我们来看一下less-10 awvs的扫描payload:
`id=if(now()=sysdate()%2csleep(0)%2c0)/*'XOR(if(now()=sysdate()%2csleep(0)%2c0))OR'"XOR(if(now()=sysdate()%2csleep(0)%2c0))OR"*/`

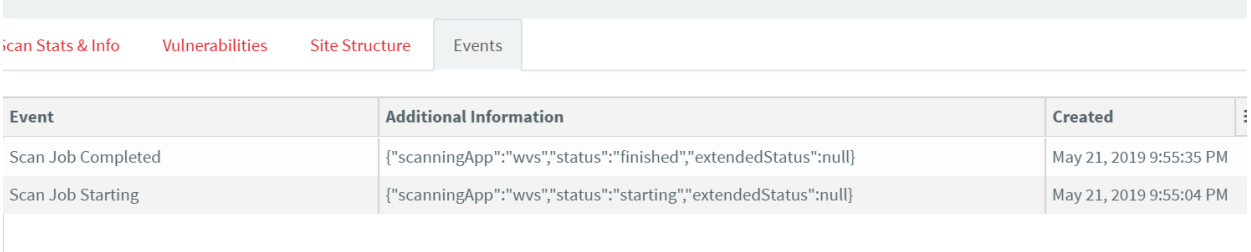
less-15的扫描payload:
`passwd=if(now()=sysdate()%2csleep(0)%2c0)/*'XOR(if(now()=sysdate()%2csleep(0)%2c0))OR'"XOR(if(now()=sysdate()%2csleep(0)%2c0))OR"*/&uname=rbqlhexw`

less-16的扫描payload: `passwd=(select(0)from(select(sleep(0)))v)/*'%2b(select(0)from(select(sleep(0)))v)%2b'"%2b(select(0)from(select(sleep(0)))v)%2b"*/&uname=eqmrwkbh`

less-17的扫描payload: `uname=1'"`



2. awvs扫描post注入也同样有效，会自动提取post参数进行扫描，设置成快速扫描后扫描速度也是非常地快:



爬虫能力对比

Acunetix的高级爬虫和JavaScript引擎称为DeepScan, Acunetix DeepScan全面支持现代单页应用程序（SPA，并且可以理解和测试完全基于JavaScript框架（例如React，Angular，Ember和Vue）的应用程序。 Acunetix还可以使用高级污点分析技术来检测难以找到的基于DOM的跨站点脚本.

- 目标1: http://testphp.vulnweb.com/AJAX/index.php
- 该目标包含首页4个需要dom触发的ajax请求 titles.php,artists.php,categories.php,showxml.php, 以及4个二级页面需要dom触发的ajax请求:infocateg.php,infotitle.php,infoartist.php,showimage.php.

awvs结果

1. 扫描事件:6min
2. 扫描结果: 高危8,低危1

Scan of http://testphp.vulnweb.com/AJAX/index.php

Scan details

Scan information	
Start time	10/01/2020, 14:32:18
Start url	http://testphp.vulnweb.com/AJAX/index.php
Host	http://testphp.vulnweb.com/AJAX/index.php
Scan time	6 minutes, 51 seconds
Profile	High Risk Vulnerabilities

Threat level

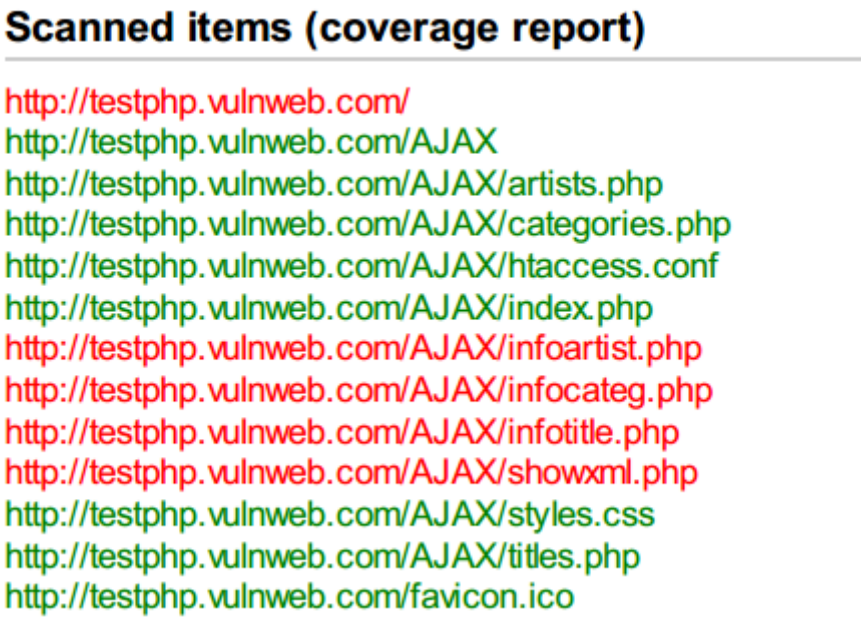
Acunetix Threat Level 3

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.

Alerts distribution

Total alerts found	9
High	8
Medium	1
Low	0
Informational	0

3. 爬虫爬取链接数量(漏洞链接数量): 除首页外8个



crawlergo结果:

- 命令: `./crawlergo -c /opt/google/chrome/chrome --event-trigger-mode sync --event-trigger-interval 1s --before-exit-delay 5s http://testphp.vulnweb.com/AJAX /index.php`

crawlergo爬虫爬取的链接数量:7个

```
Crawling GET http://testphp.vulnweb.com/AJAX/index.php
Crawling GET http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
Crawling GET http://testphp.vulnweb.com/AJAX/titles.php
Crawling GET http://testphp.vulnweb.com/AJAX/infocateg.php?id=1
Crawling POST http://testphp.vulnweb.com/AJAX/infotitle.php
Crawling GET http://testphp.vulnweb.com/AJAX/artists.php
Crawling GET http://testphp.vulnweb.com/AJAX/categories.php
Crawling POST http://testphp.vulnweb.com/AJAX/showxml.php
```

数据分析:

- 第一层需要dom触发的四个ajax请求比如titles.php,artists.php,categories.php,showxml.php四个链接都获取到了，但第二层需要dom触发的三个ajax请求比如infocateg.php,infotitle.php,infoartist.php使用crawergo就很难获取到了。
- 爬虫能力: awvs > crawlergo, 但crawlergo已经非常优秀了。 速度方面cralergo比awvs要快很多。

awvs配置优化

1. awvs默认开启AcuSensor, 如果没有配置代理端，建议关闭,这样会在请求中添加一些易被waf识别的字段.

```
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
```

2. 扫描端口非常慢，建议关闭端口扫描的功能

翻译

file

new

- Web Site Scan 新建一个扫描向导，包括爬虫和漏洞审计
- Web Site Crawl 新建一个网站爬虫
- Web service Scan 新建一个网站服务扫描,如WDSL
- Report 生成一个报告

Load Scan Result: 加载一个扫描结果,必须是.wvs文件

Save Scan Result: 保存一个扫描结果位.wvs文件，和导出报告不一样

Exit : 退出

Tools

Web Scanner

Site Crawler: 网站爬虫，和file->new->Web Site Crawl一样

Target-Finder: 主机网段扫描

SubDomain Scanner:子域名扫描

Bind SQL Injector:盲注手工测试

HTTP Editor: HTTP信息查看,还有Encoder Tool编码工具，很贴心哦

HTTP Sniffer: HTTP 嗅探

HTTP Fuzzer: HTTP fuzz

Authentication Tester: HTTP 验证测试,表单爆破

Compare Results:比较测试结果

Web Services Scanner: WSDL漏洞扫描

WEb Services Editor: 网站服务手动分析

Configuration

Application Settings

- Application Updates 更新,可设置代理服务器
- Logging 日志记录: 目录在用户->Dockment>Acunetix WVS 10>Logs 该目录下还有AcuSensor,BlindSQL,Bugreports,Fuzzer,HttpEditor,Logs,Saves,Storage
- 保存扫描结果: 包括设置保存数据库，保存目录
- 可设置验证所用的证书
- Client Certificates 指定客户端访问所需证书
- Login Sequence Manger:登录会话管理
- False Positives:处理误报
- HTTP Sniffer: 设置监听网卡和端口
- Scheduler: 设置计划任务
- Miscellaneous: 其他设置,可设置扫描是的内存，默认1024M,使用临时文件夹
- Acunetix 传感器功能,提高漏洞审计能力

Scan Setting

- 扫描选项: 是否关闭爬虫错误，扫描模式，是否扫描端口
- 爬虫选项
- HTTP选项
- Scanning Profiles: 设定扫描重点,默认15个扫描方式，默认位default,及扫描全部

help

Check for update:检查更新

Application Dicectories: 程序目录，包括数据目录,用户目录和扫描计划保存目录

Schelduler Web Interface: localhost:8183 扫描计划web平台

Update License: 更新证书