

# Web渗透之Web利器合集——web漏洞扫描器-AWVS的安装和使用

原创

[Mr.Wanderer](#) 于 2020-07-19 22:51:08 发布 975 收藏 11

分类专栏: [Web渗透](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/Mr\\_Wanderer/article/details/107452077](https://blog.csdn.net/Mr_Wanderer/article/details/107452077)

版权



[Web渗透](#) 专栏收录该内容

17 篇文章 4 订阅

订阅专栏

## 文章目录

### 漏洞扫描器

#### 安装linux Awvs

1. 下载
2. 分配权限
3. 安装配置
4. 激活配置
5. 开启和关闭服务
6. 修改密码

#### 扫描示例

1. 添加目标
2. 开始扫描
3. 生成报告
4. 报告书下载

如果有帮到您请点个赞~

## 漏洞扫描器

漏洞扫描:

漏洞扫描是指基于漏洞数据库, 通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测, 发现可利用漏洞的一种安全检测(渗透攻击)行为。

Web漏洞扫描器:

针对于Web应用程序所开发的漏洞扫描器, 例如SQL注入、XSS跨站脚本攻击等常见漏洞, 进行主动式扫描探测是否存在漏洞。通过扫描器能够快速的发现漏洞, 来提升我们的效率, 以及漏洞覆盖面。

Web扫描器也是在为我们做信息收集、为接下来的渗透测试做准备。

# 安装linux Awvs

## 1. 下载

<https://pan.baidu.com/s/14teZDsBWV8z1A0V38IYtNQ>

提取码: in2j

移动两个文件到kali linux

## 2. 分配权限

把这两个压缩包的内容提取出来。

分配权限:

```
chmod 777 acunetix_trial.sh
```

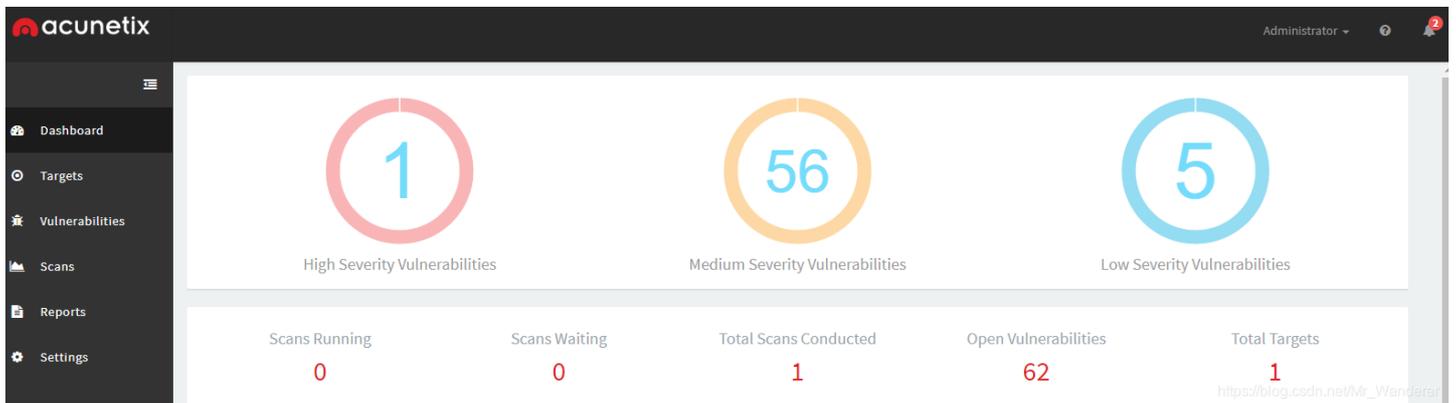
## 3. 安装配置

```
./acunetix_trial.sh
```



访问: [https://\[kali的ip\]:13443](https://[kali的ip]:13443)

应该能看到页面



## 4. 激活配置

把文件patch\_aws复制到/home/acunetix/.acunetix\_trial/v\_190325161/scanner/下

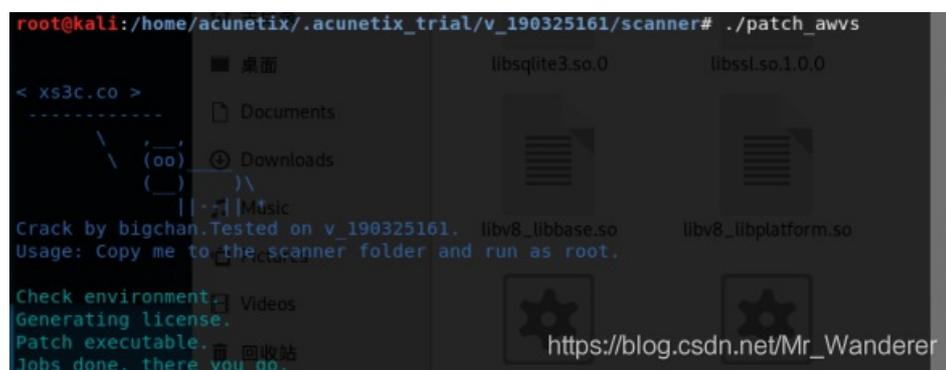
```
cp patch_aws /home/acunetix/.acunetix_trial/v_190325161/scanner/
```

提权脚本:

```
chmod 777 patch_aws
```

运行脚本:

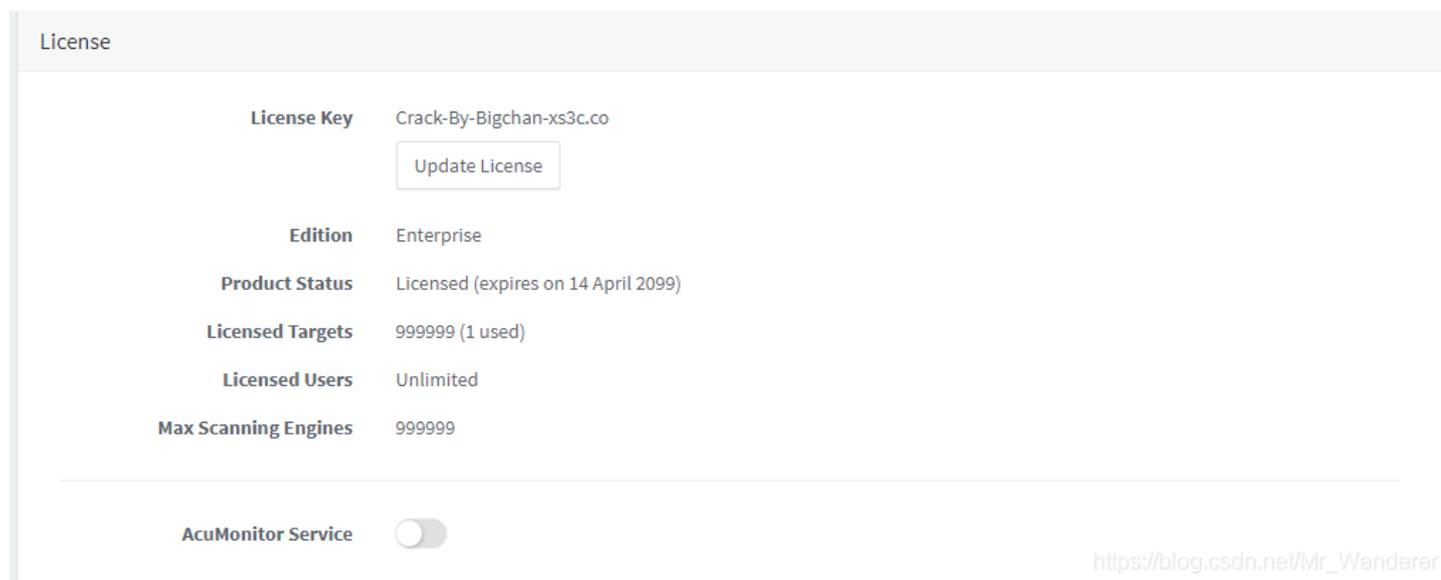
```
./patch_aws
```



```
root@kali:~/home/acunetix/.acunetix_trial/v_190325161/scanner# ./patch_aws
< xs3c.co >
-----
Crack by bigchan. Tested on v_190325161.
Usage: Copy me to the scanner folder and run as root.

Check environment.
Generating license.
Patch executable.
Jobs done, there you go.
```

然后我们去可视化界面，查看他的执照



License	
License Key	Crack-By-Bigchan-xs3c.co
	<input type="button" value="Update License"/>
Edition	Enterprise
Product Status	Licensed (expires on 14 April 2099)
Licensed Targets	999999 (1 used)
Licensed Users	Unlimited
Max Scanning Engines	999999

AcuMonitor Service

已经激活，可以开始扫描网站啦。

## 5. 开启和关闭服务

默认为开启，如果要进行操作，先进入安装目录

开启服务:

```
service acunetix_trial start
```

关闭服务:

```
service acunetix_trial stop
```

## 6.修改密码

进入/home/acunetix/.acunetix\_trial目录下  
运行change\_credentials.sh文件

```
./change_credentials.sh
```

## 扫描示例

### 1.添加目标



此处为“掌控安全学院”打call，感谢老师们的教诲。  
然后我们可以设置很多参数。

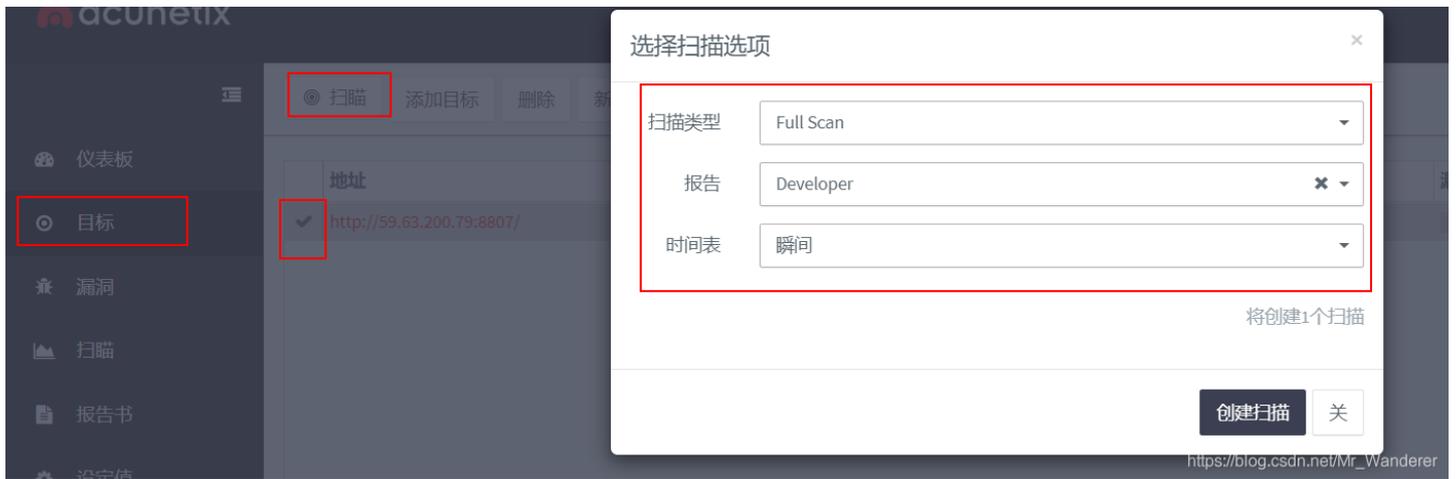


添加一个扫描引擎：高级->扫描引擎



之后保存

## 2.开始扫描



这里可以设置扫描类型、报告类型和时间参数。

**Acunetix威胁等级3**

**HIGH**

扫描程序发现了一个或多个高严重类型漏洞。恶意用户可以利用这些漏洞并破坏后端数据库和/或破坏您的网站。

总体进程 7%

开始扫描59.63.200.79 2020年7月19日晚上10:24:51

扫描时间	要求	平均响应时间	地点
1m 45s	1,162	799毫秒	55

**目标信息**

地址	59.63.200.79
服务器	nginx / 1.11.5
操作系统	未知
识别技术	的PHP
反应灵敏	是

**最新警报**

- Clickjacking: 缺少X-Frame-Options标头 2020年7月19日10:25:09 PM
- nginx整数溢出 2020年7月19日晚上10:25:20
- 内容安全政策 (CSP) 未实施 2020年7月19日晚上10:25:26
- 没有CSRF保护的HTML表单 2020年7月19日10:25:27 PM

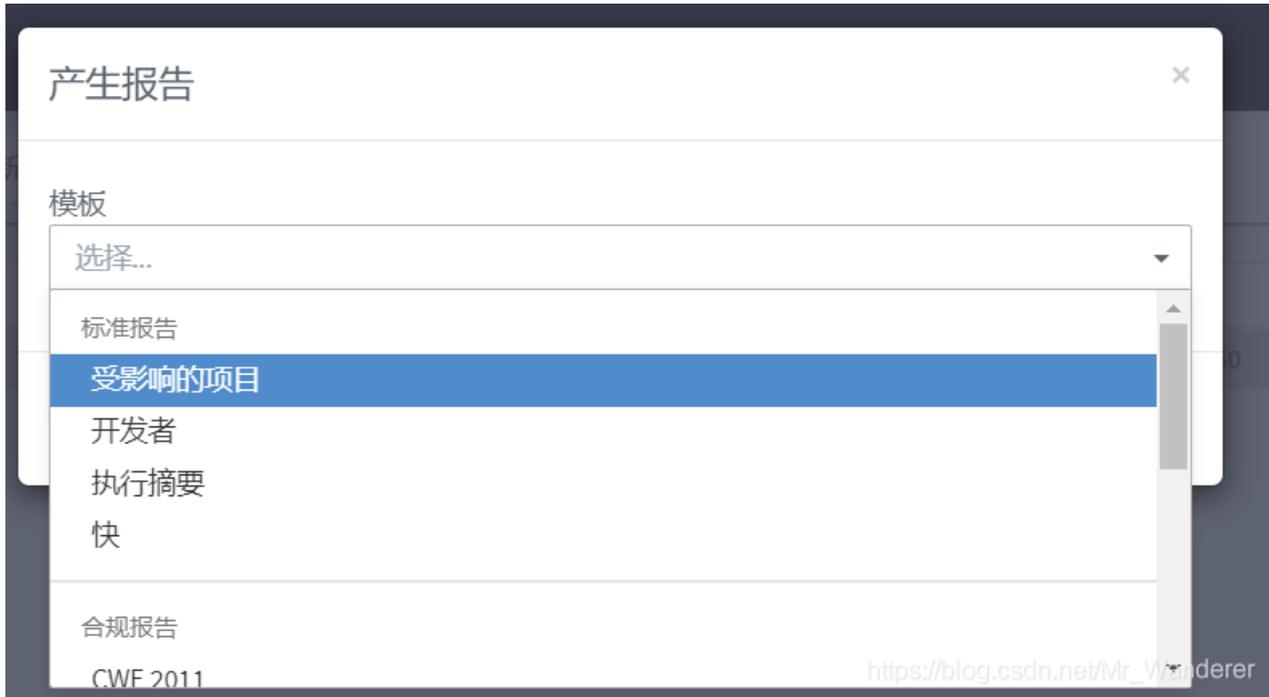
这里可以查看进度、目标信息和扫出来的安全问题。

Se...	Vulnerability	URL	Parameter	Status	Last Seen
!	nginx Integer Overflow	http://59.63.200.79:8807/		Open	Jul 19, 2020 10:25:20 PM
!	Application error message	http://59.63.200.79:8807/index.php	m	Open	Jul 19, 2020 10:30:23 PM
!	Backup files	http://59.63.200.79:8807/index.php.bak		Open	Jul 19, 2020 10:33:44 PM
!	Backup files	http://59.63.200.79:8807/index.php.bac		Open	Jul 19, 2020 10:33:44 PM
!	Backup files	http://59.63.200.79:8807/index.php_bak		Open	Jul 19, 2020 10:33:44 PM
!	Backup files	http://59.63.200.79:8807/index.php_		Open	Jul 19, 2020 10:33:44 PM
!	Backup files	http://59.63.200.79:8807/index.php.bak		Open	Jul 19, 2020 10:33:45 PM

点击漏洞，会显示其具体描述和对应的解决方案，会给我们一些相关的url。

### 3.生成报告

需等待扫描完成，或者主动停止扫描。



这里可以选择模板

## 4. 报告书下载



如果有帮到您请点个赞~