# 漏洞扫描：AWVS使用方法

原创

Zeker62 于 2021-08-02 21:25:19 发布 11425 收藏 3

分类专栏： 网络安全学习 文章标签： docker awvs 漏洞





## 安装AWVS：

推荐一个大佬的AWVS的安装博客
https://www.sqlsec.com/2020/04/awvs.html
我使用的是docker版本的，其他的我觉得太麻烦了。

## Linux上使用AWVS

将Docker的3443端口映射到物理机的 13443端口

```
docker run -it -d -p 13443:3443 secfa/docker-awvs
```

> awvs13 username: admin@admin.com
> awvs13 password: Admin123

根据博客所述，我将AWVS安装在kali虚拟机上

```
┌──(root💀kali)-[/home/kali/下载]
└─# docker pull secfa/docker-awvs
Using default tag: latest
latest: Pulling from secfa/docker-awvs
345e3491a907: Pull complete
57671312ef6f: Pull complete
5e9250ddb7d0: Pull complete
353bccaea3bd: Pull complete
Digest: sha256:162b167b80aedcc3aadf412bc4a4dbb73764f045d3b353362b891d44ea2124a3
Status: Downloaded newer image for secfa/docker-awvs:latest
docker.io/secfa/docker-awvs:latest

┌──(root💀kali)-[/home/kali/下载]
└─# docker run -it -d -p 13443:3443 secfa/docker-awvs
122c219d5ed73270dfded13c8859fe20ea4aedaa6304362e5bb05c9d79434b75
```



但是我并不想在kali上运行，因为kali实在是有些慢。

## 在Windows上使用awvs

找到kali的IP地址是：192.168.43.238

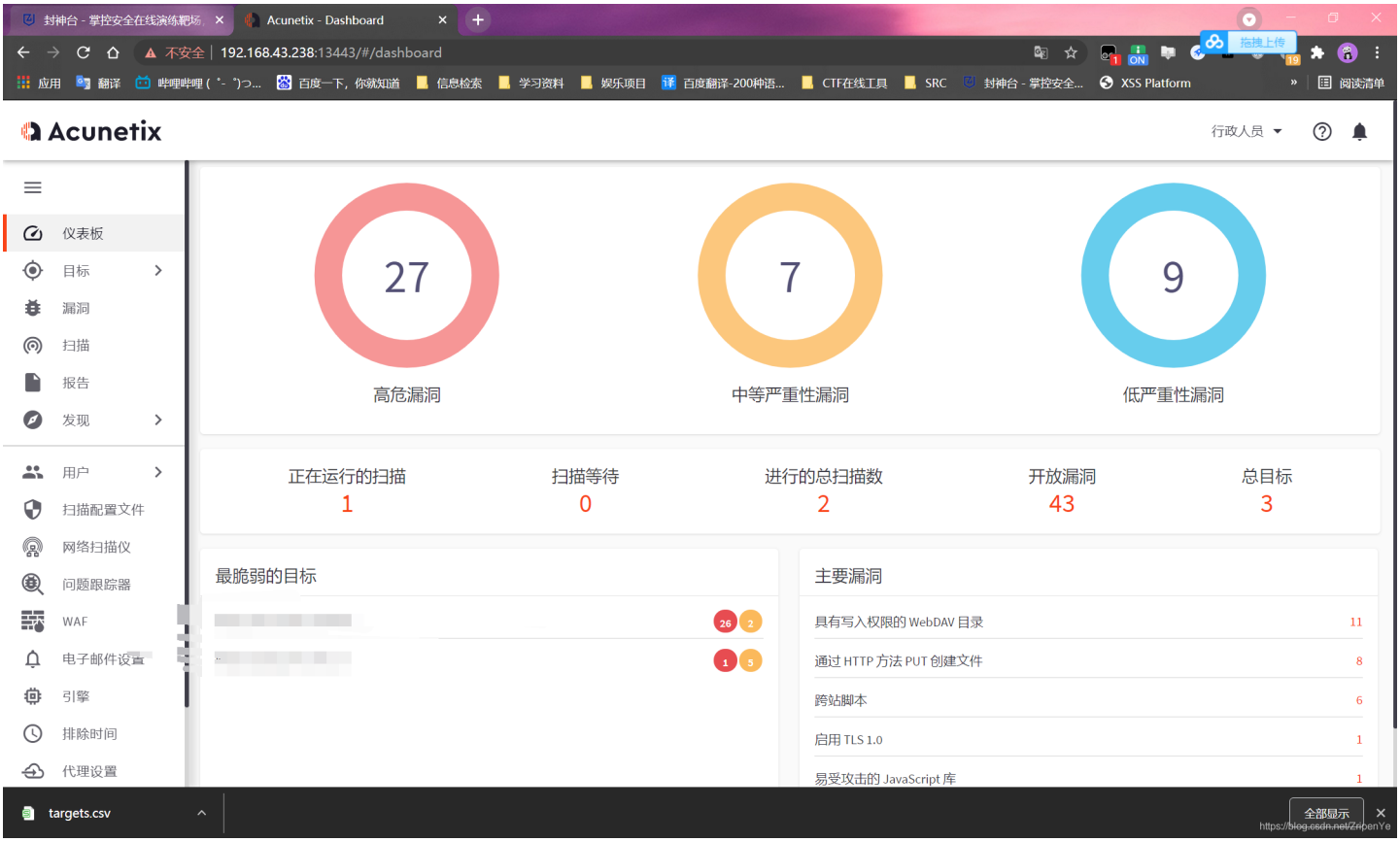
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.238  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::20c:29ff:feeb:3409  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:eb:34:09  txqueuelen 1000  (Ethernet)
        RX packets 383771  bytes 573228665 (546.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 113475  bytes 8500888 (8.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



打开我们喜欢的浏览器

输入：https://192.168.43.238:13443/

输入账号密码（都在第一个链接的大佬博客里）

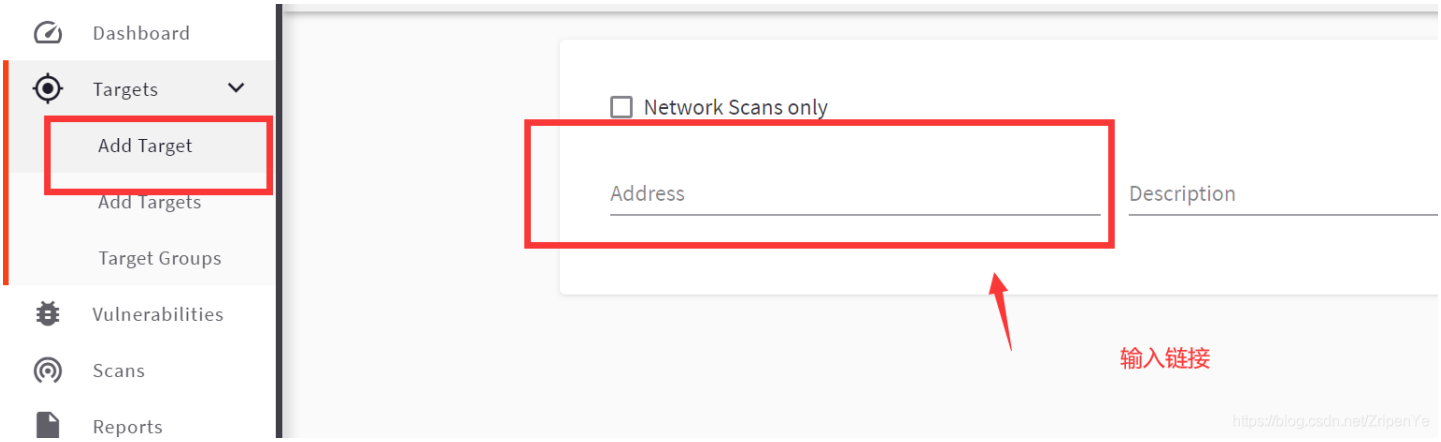



开启成功

## 扫描漏洞

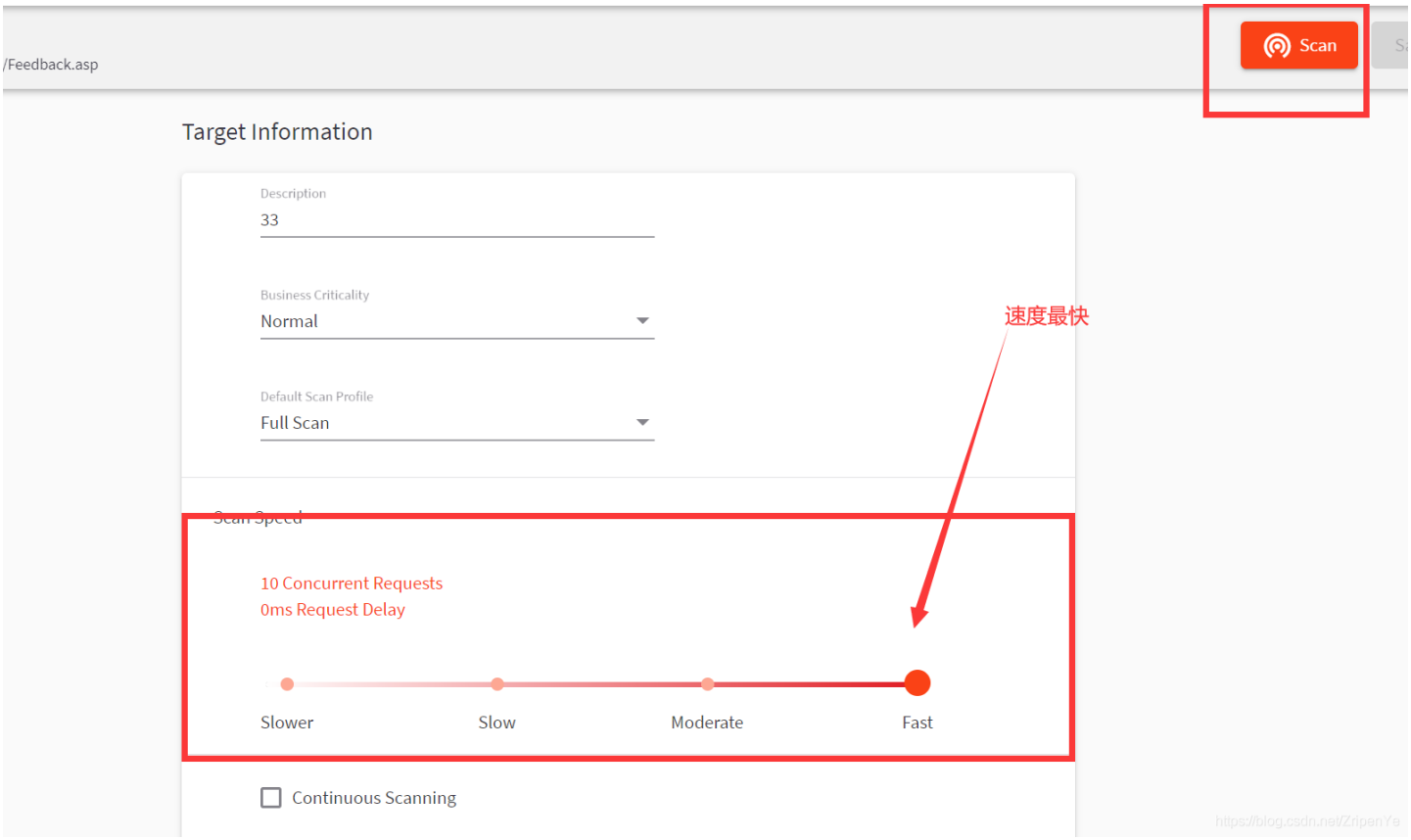
以封神台靶场为例：

http://59.63.200.79:8004/Feedback.asp

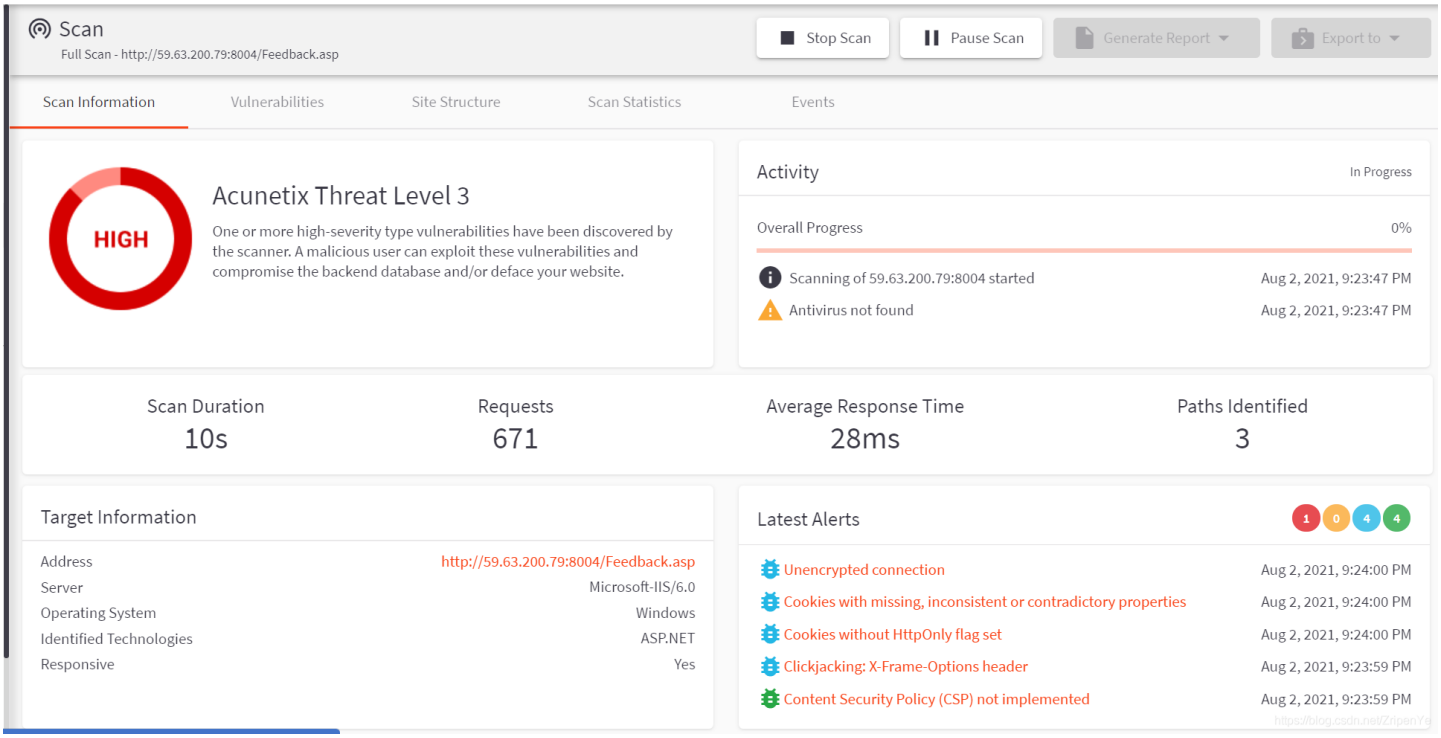



后面的描述相当于是备注，不是必须。


新手的话直接点最快吧，也是试试水
直接点扫描即可



等一下就有漏洞被扫描出来了




扫描出来的漏洞就可以用作一些渗透测试。