# \*\*\*项目/学习 **2021年12月工作周报**

**时间：2021年12月1日~2021年12月7日**

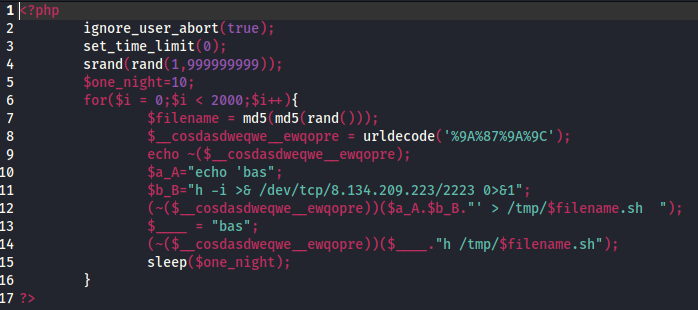
## **1.上周安排** **（1）看一些ctf上java反序列化的题目** **（2）继续做buuctf，选择性地做php代码审计的题目和pop链。** **（3）学一下非关系型数据库注入**

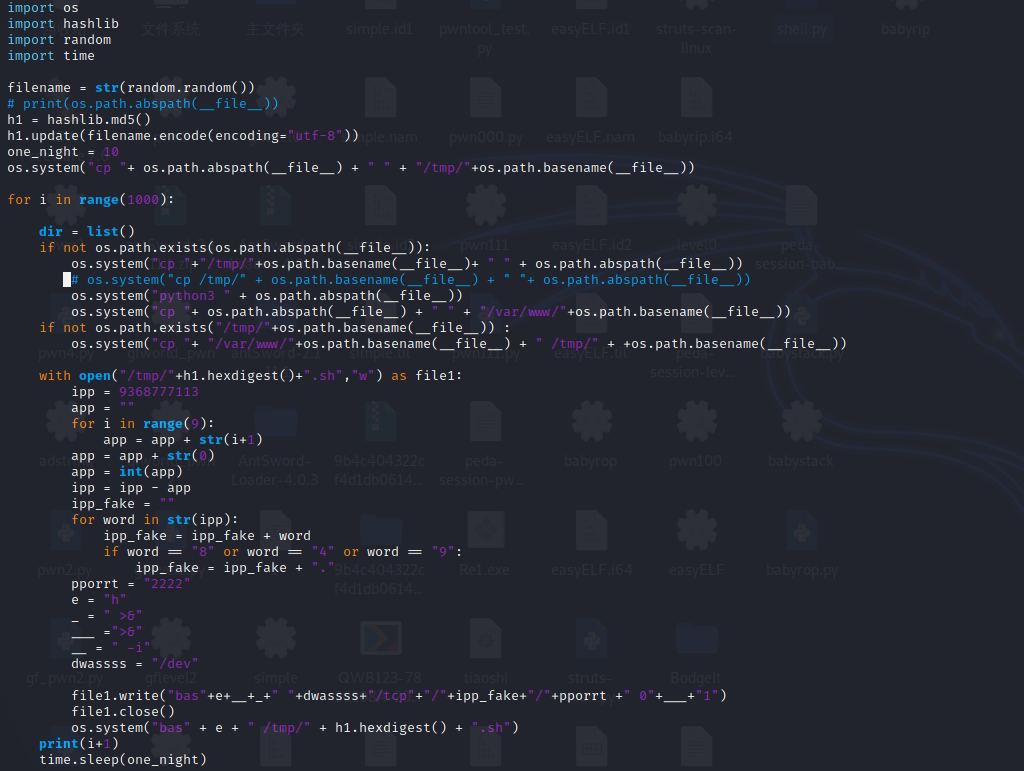
## 2. 本周做了什么事情

简要描述工作内容；

（1）看了一些java的反序列化题目感觉知道了熟悉了java的套路之后还是代码审计的问题，要继续加强java代码的审计能力，java目前接触的非常少

1. 主要是玩了一些木马，先是写了一个php+bash的反弹shell，通过取反和变量函数还有一点混淆的方式来达到免杀的效果。然后是用python写了个偷偷往别的路径备份，删掉又恢复的bash反弹shell，感觉没有意义但很好玩就是了。然后分析了一下metasploit生成的windows的反弹shell，在免杀上有点鸡肋，在经过多次编码之后，火绒不报木马病毒，改报代码混淆器，在ubx加壳之后又报木马病毒，再进行一次反虚拟机之后又报回代码混淆器，无语。。。虽然免杀上比较鸡肋，但是shell中集成的功能还是非常丰富的，提供了大量的小白式操作，一键获取windows系统权限，一键迁移shell到别的进程，还可以通过自带的persistence来设置开机自启动，甚至通过metsvc模块可以在已经获取shell的设备上面开启一个服务来提供后门功能，一键监听键盘，一键使用摄像头拍摄，禁用鼠标键盘等等。。。。尝试通过社工林俊材获得他电脑的系统权限，成功控制了半分钟。(当时他点开木马的时候没在监听！！注意到的时候输出了一下文件信息和进程信息，刚准备迁移进程，shell就断开咯)。









（3）了解了一下tomcat服务器的架构，以及它在处理web请求时候的步骤，过程。

(4) 刷了三道ctf题目，比较有收获的是一个php关于操作zip的原生类的反序列化利用，和一个脚本fastcoll，能根据你给的字符串，然后生成两串md5一样的字符串，前缀都是你给的字符串，后面的不一样。能用来过md5强碰撞。还能控制payload。

## 3. 工作结果

## 4. 结论

暂无

## 5. 下周工作安排

（1）写java server page，理解javaweb的原理。

（2）B105那边的设备快到了，要花时间做实验。

（3）偶尔刷刷题