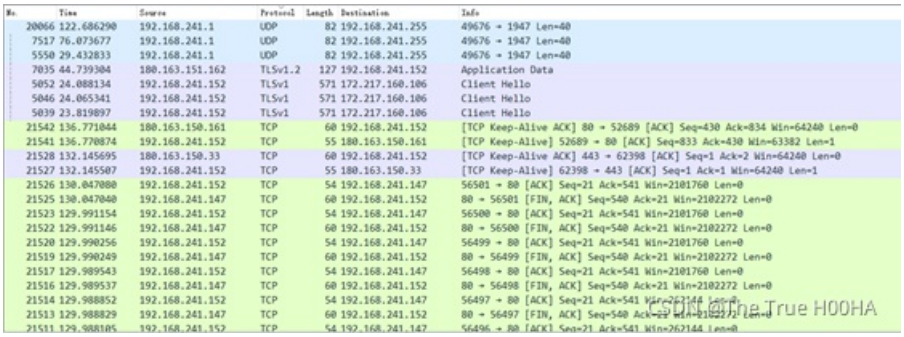
陇剑杯Writeup（部分）

原创

The True H00HA 于 2021-09-15 16:40:23 发布 1533 收藏
文章标签： web安全 安全架构 安全 系统安全

本文链接：https://blog.csdn.net/s1mplelife/article/details/120310801

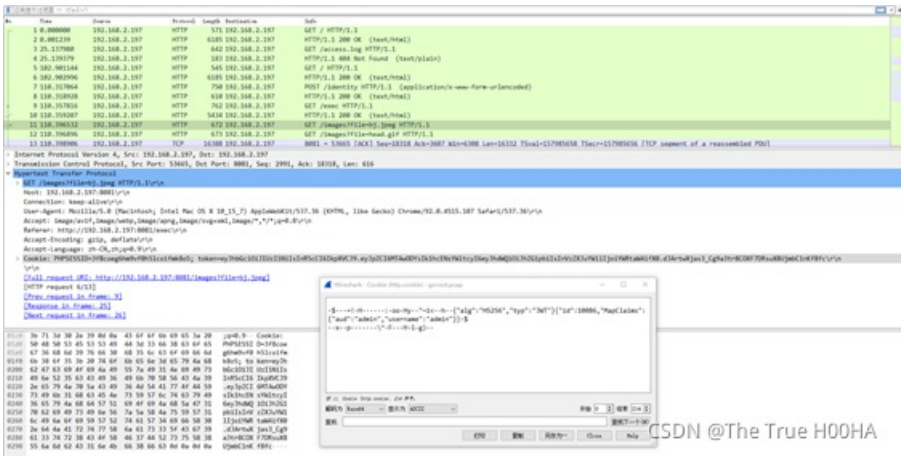
1、签到



http协议网络攻击

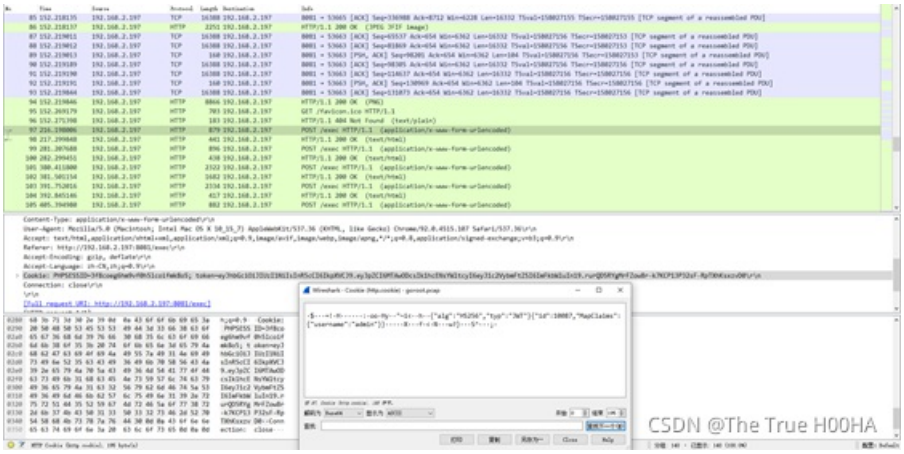
2 JWT

2.1



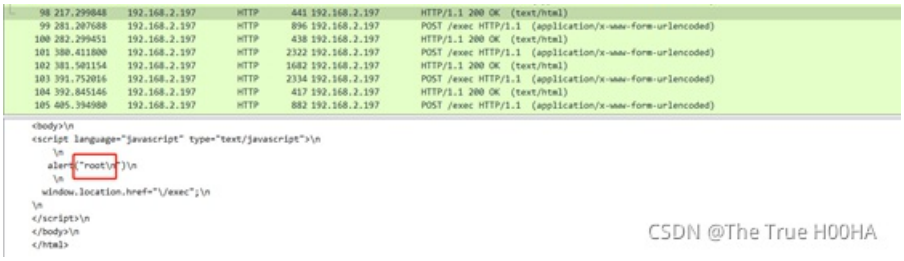
该网站使用了_ **JWT**_认证方式。

2.2



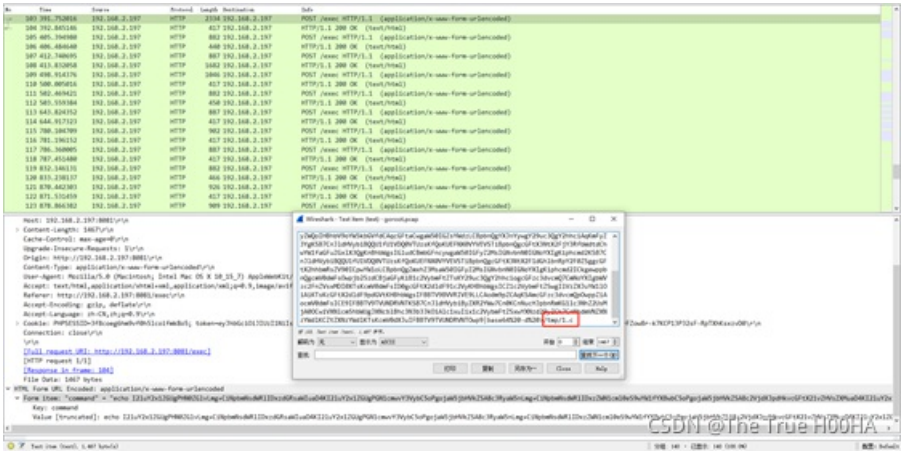
黑客绕过验证使用的jwt中，id和username是_**10087#admin** _。

2.3



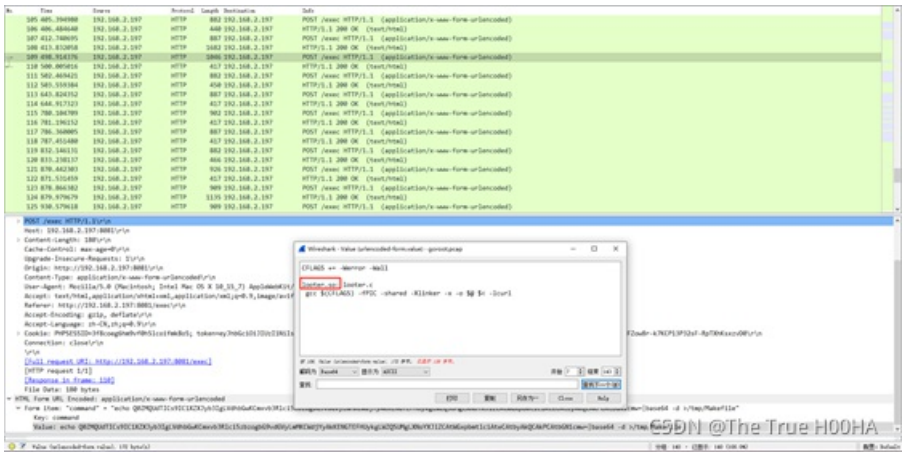
黑客获取webshell之后，权限是_ **root**_？

2.4



黑客上传的恶意文件文件名是/tem/1.c___。

2.5



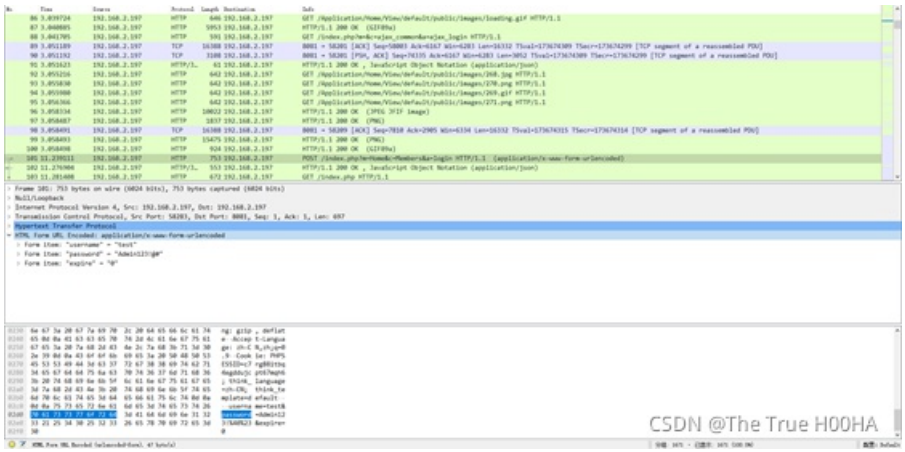
黑客在服务器上编译的恶意so文件，文件名是looter.so___。

2.6

黑客在服务器上修改了一个配置文件，文件的绝对路径为/etc/pam.d/common-auth_____。

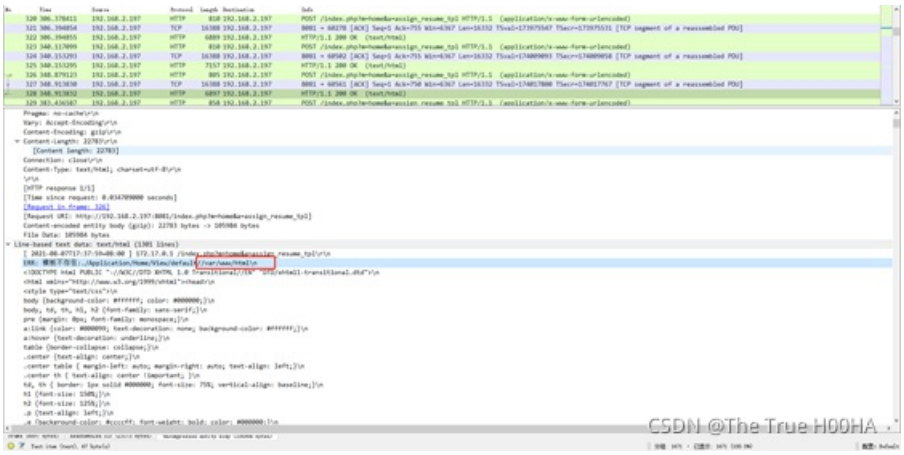
3 webshell

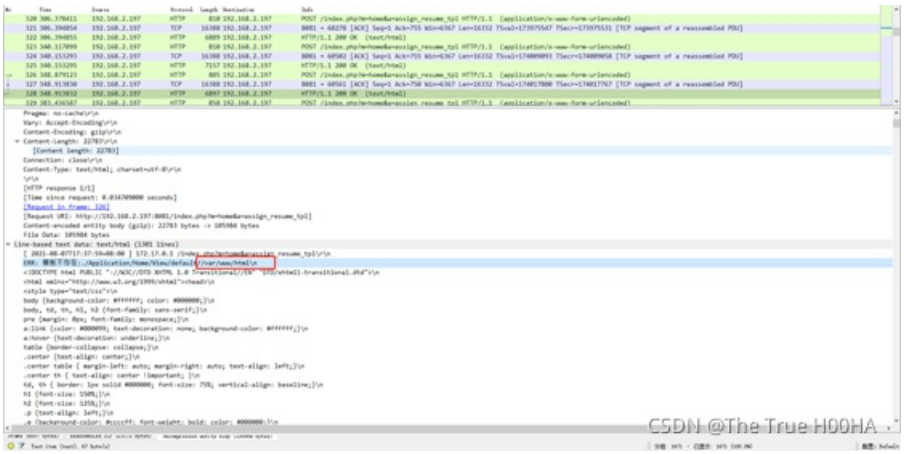
3.1



黑客登录系统使用的密码是__***Admin123!@#***_。

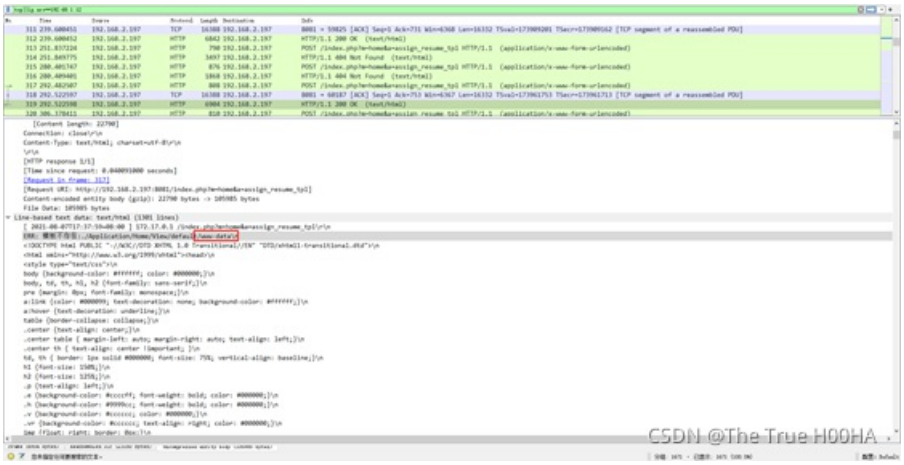
3.2





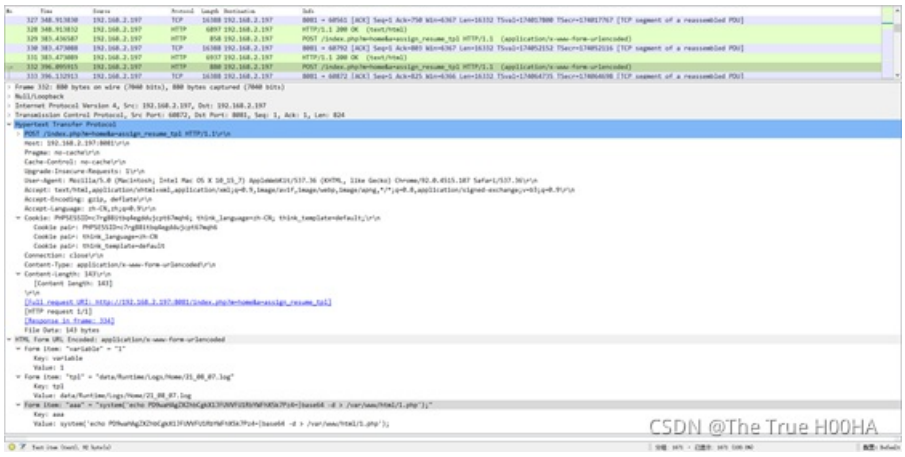
黑客修改了一个日志文件，文件的绝对路径为/var/www/html/data/Runtime/Logs/Home/21_08_07.log_____。

3.3



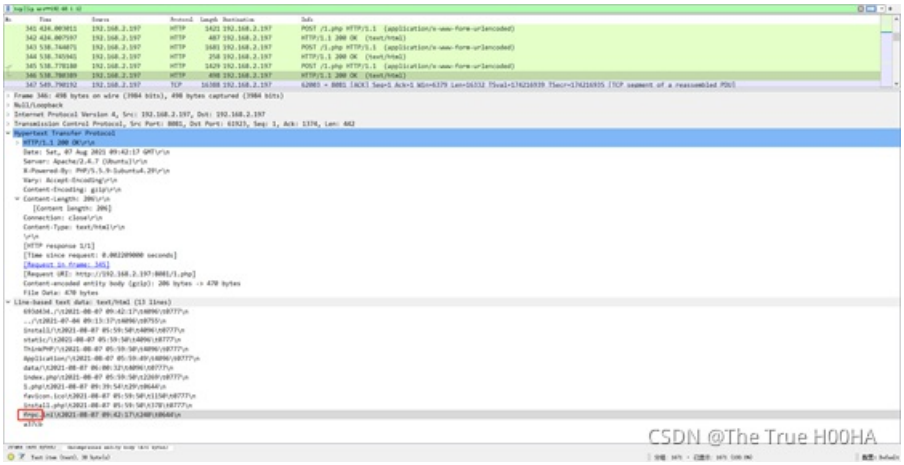
黑客获取webshell之后，权限是_ **www-data**_？

3.4



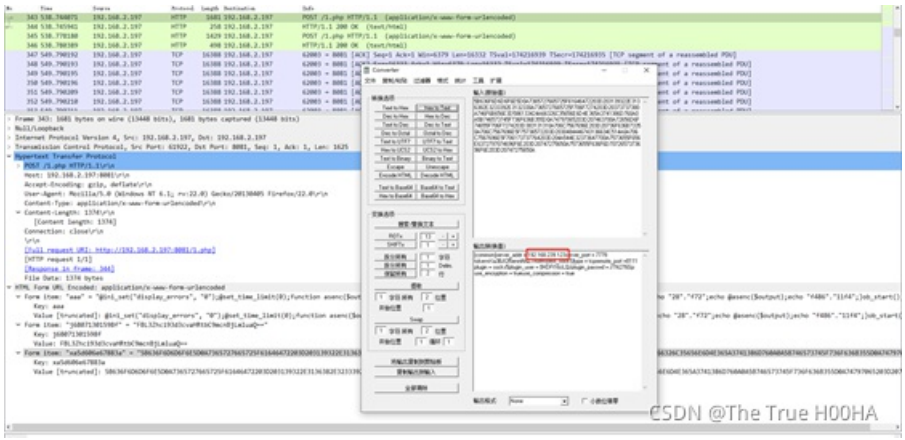
黑客写入的webshell文件名是1.php_____。

3.5



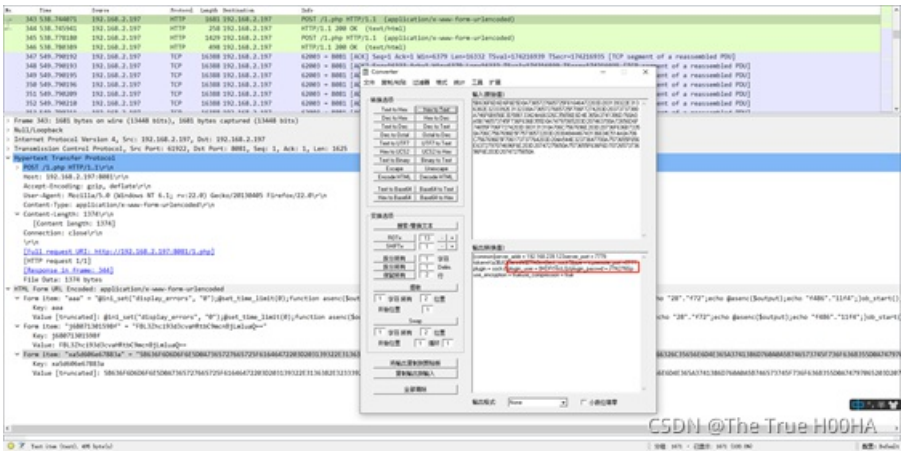
黑客上传的代理工具客户端名字是__**frpc**___。

3.6



黑客代理工具的回连服务端IP是__**192.168.239.123**___。

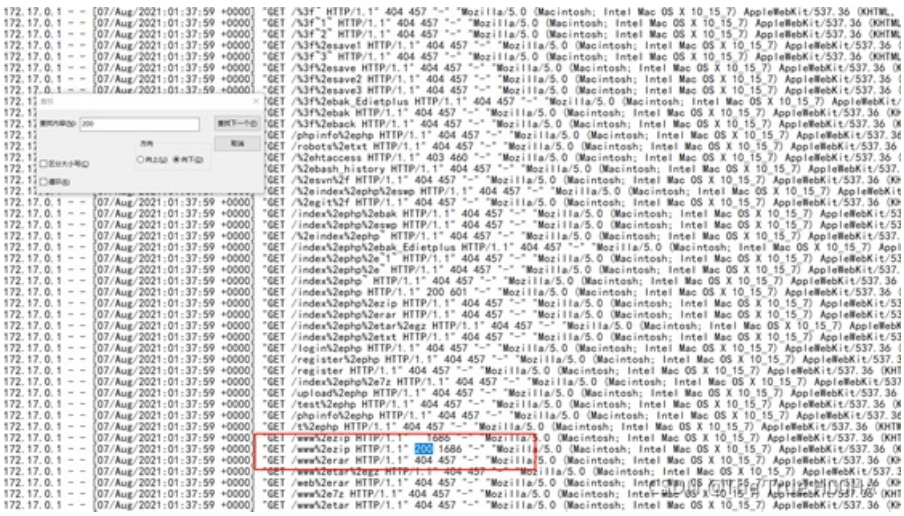
3.7



黑客的socks5的连接账号、密码是_ **0HDFt16cLQJ#JTN276Gp**_。

4 日志分析

4.1

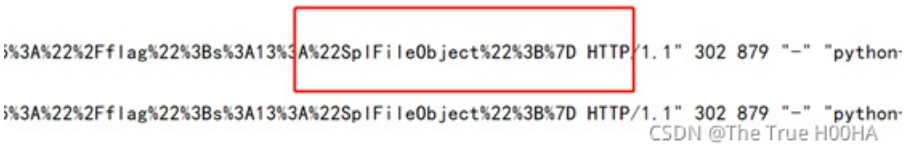


网络存在源码泄漏，源码文件名是__www.zip___。

4.2

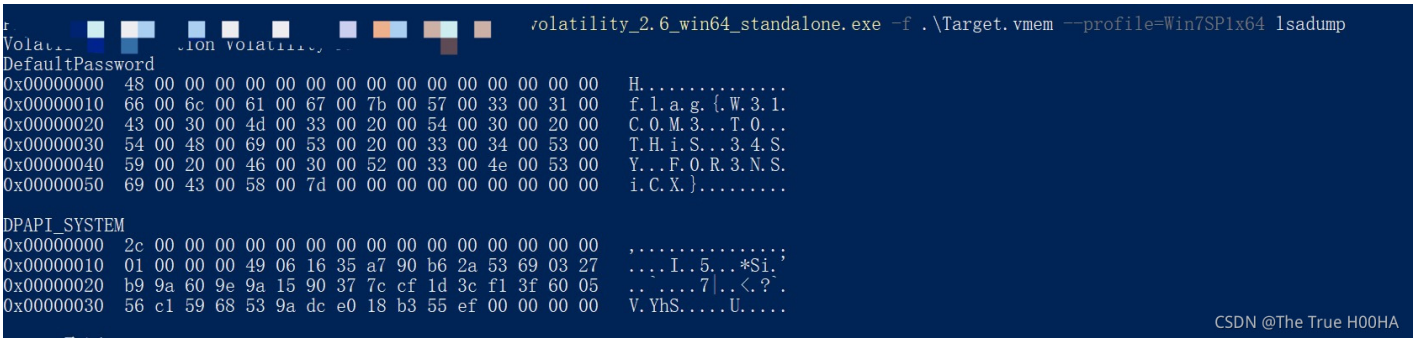
分析攻击流量，黑客往/tmp目录写入一个文件，文件名为__***sess_car***_。

4.3



分析攻击流量，黑客往/tmp目录写入一个文件，文件名为__SplFileObject__。

6.1



虚拟机的密码是flag{W31C0M3 T0 THiS 34SY FOR3NSiCX} _____。

6.2

vol镜像 die逆向文件

exe导出后是个自动解压的，获得文件夹

华为备份加密使用工具

https://github.com/RealityNet/kobackupdec

python .\kobackupdec.py -vvv W31C0M3_T0_THiS_34SY_F0R3NSiCX “C:\Users\Snowywar\Desktop\HUAWEI P40_2021-aa-bb xx.yy.zz” ./HUAWEI

flag{TH4NK Y0U FOR DECRYPTING MY DATA}

7 简单日志分析

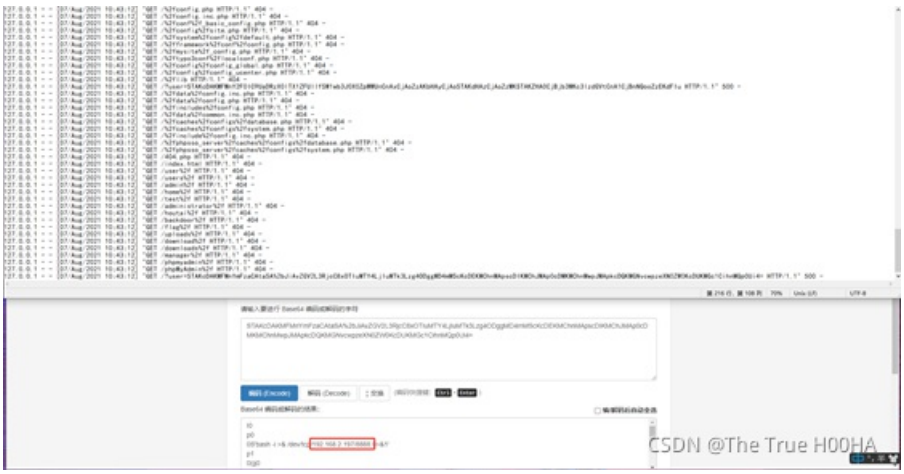
7.1

黑客攻击的参数是_ **user**_。

7.2

黑客查看的秘密文件的绝对路径是/Th4s_IS_VERY_Import_Fi1e_____。

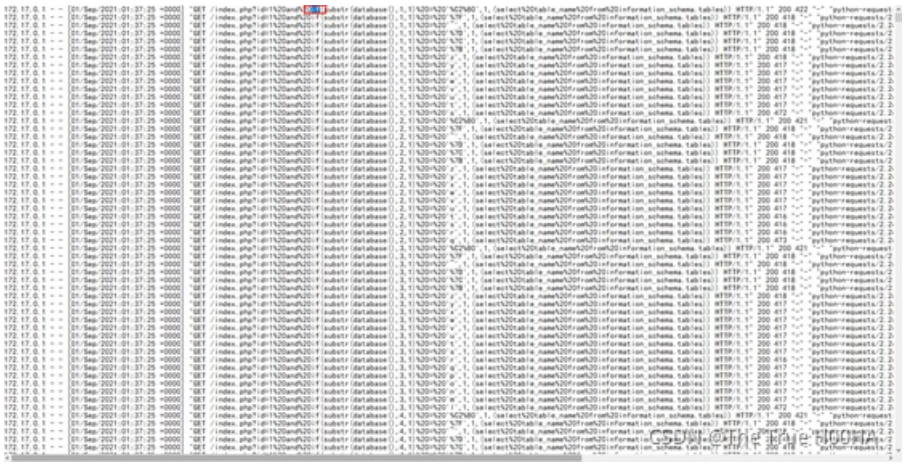
7.3



黑客反弹shell的ip和端口是__192.168.2.197：8888___。

8、SQL注入

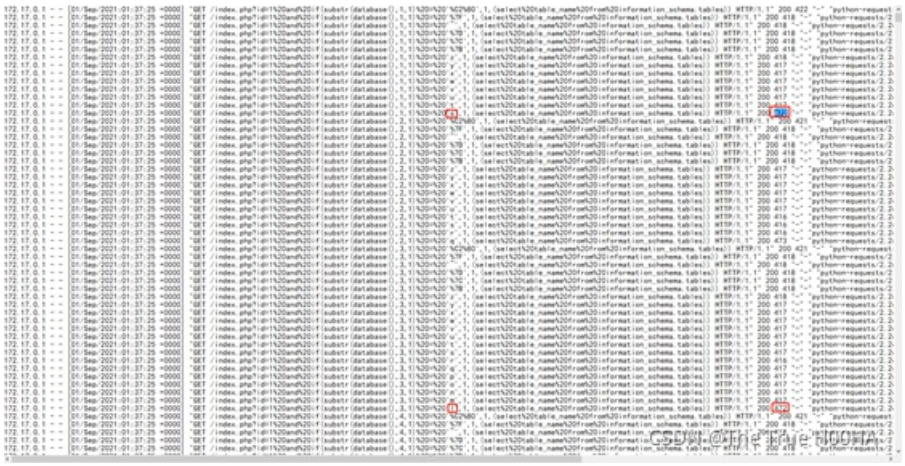
8.1



通过if确定未布尔盲注

黑客在注入过程中采用的注入手法叫__布尔盲注___。

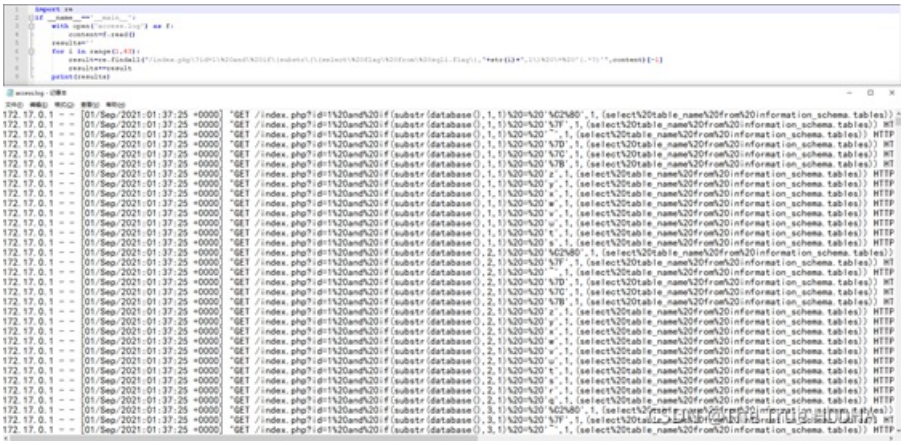
8.2



通过状态码判断盲注

黑客在注入过程中，最终获取flag的数据库名、表名和字段名是sqli#flag#flag_____。

8.3



通过python脚本获得flag再进行url编码

flag{deddcd67-bcfd-487e-b940-1217e668c7db}

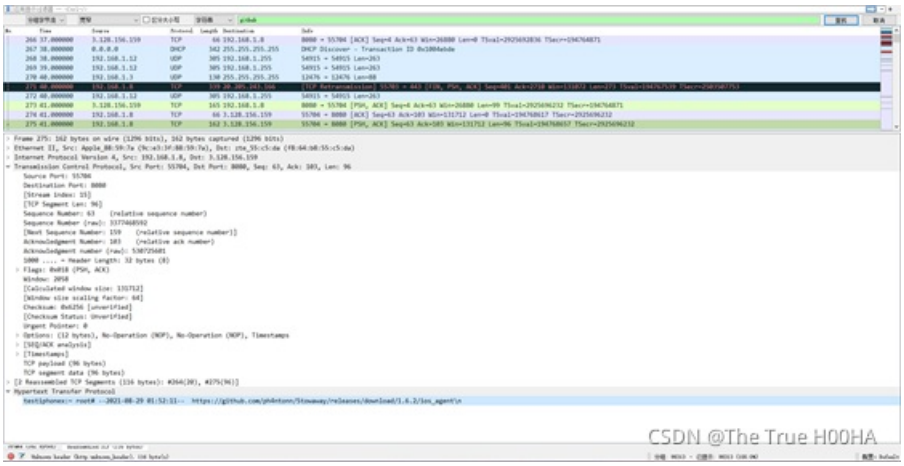
黑客最后获取到的flag字符串为__flag{deddcd67-bcfd-487e-b940-1217e668c7db}___。

10、IOS

10.1

黑客所控制的C&C服务器IP是__ 3.128.156.159___。

10.2



黑客利用的Github开源项目的名字是**_stowaway _**。

10.3

通讯加密密钥的明文是___ hack4sec_。

10.4

黑客通过SQL盲注拿到了一个敏感数据，内容是_746558f3-c841-456b-85d7-d6c0f2edabb2__。

10.5

黑客端口扫描的扫描器的扫描范围是_10-499_。（格式使用“开始端口-结束端口”，例如1-65535）

10.7

黑客访问/攻击了内网的几个服务器，IP地址为_172.28.0.2#192.168.1.12_。（多个IP之间按从小到大排序，使用#来分隔，例如127.0.0.1#192.168.0.1)

10.8

黑客写入了一个webshell，其密码为_fxxk___