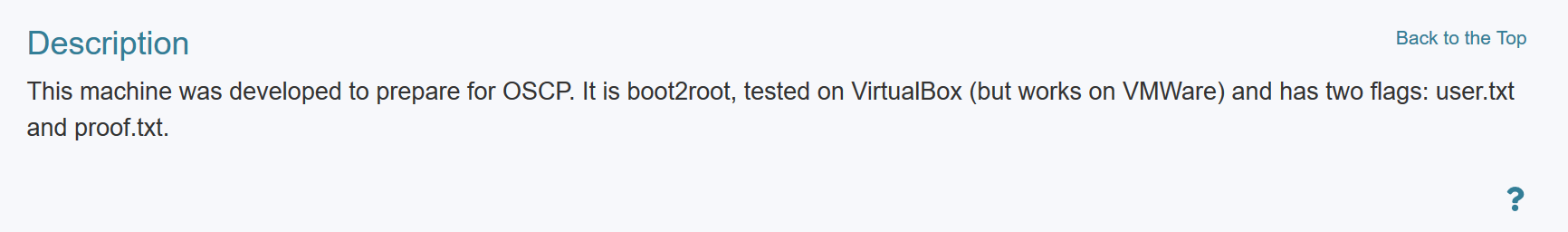
# 0x00:靶机下载

靶机下载: <https://www.vulnhub.com/entry/photographer-1,519/>

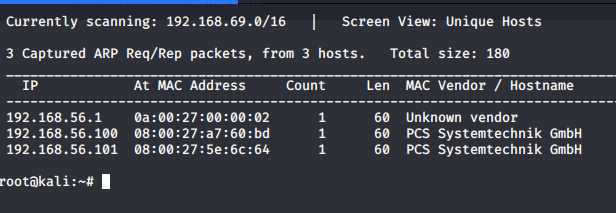
这个靶机是给想考OSCP准备的，在virtualbox下运行，有2个flag



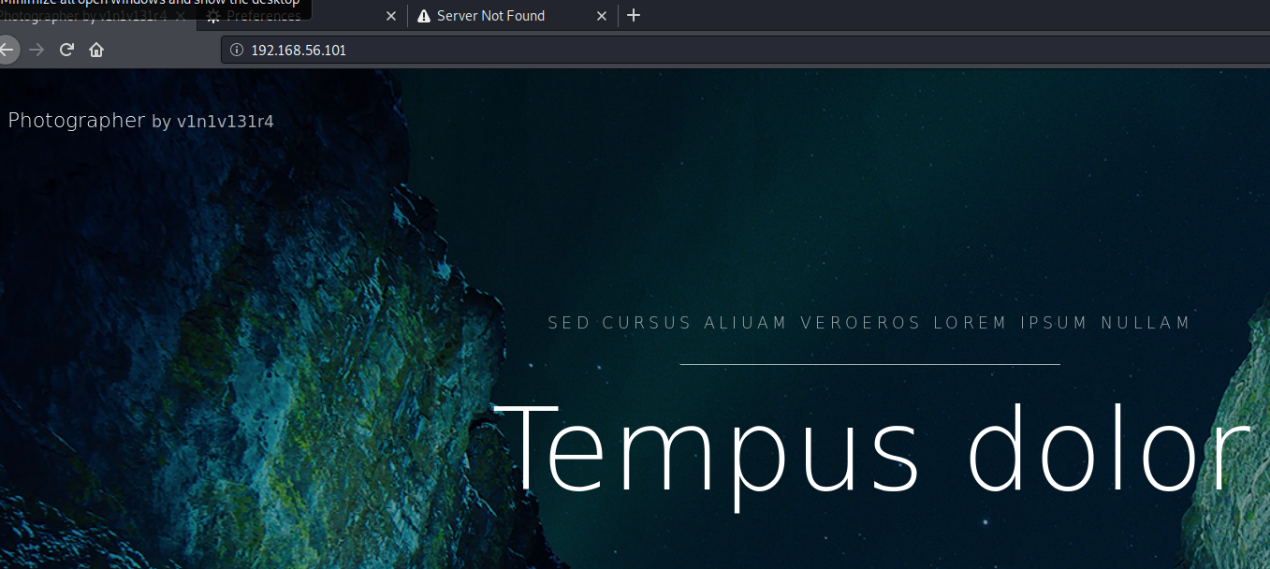
# 0x01:探测靶机

先用Netdiscover探测一波，由于我的kali出了点问题重新分配IP以后变成了这样。。。。明明只开了一个靶机结果变成了2个PCS

命令:netdiscover -r 192.168.56.0/16

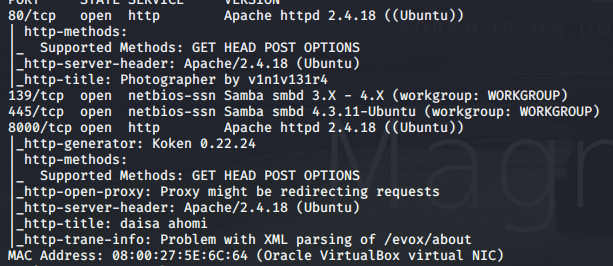


轮流访问了一波以后可以确定靶机IP为192.168.56.101



开始用Nmap探测波端口,这次开了80，139，445和8000端口

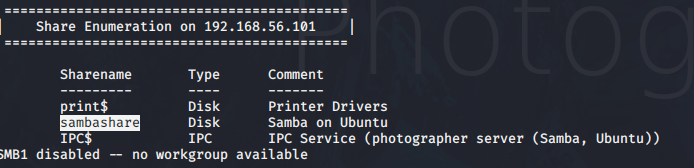
命令:nmap -A -sS -sV -v -p- 192.168.56.101



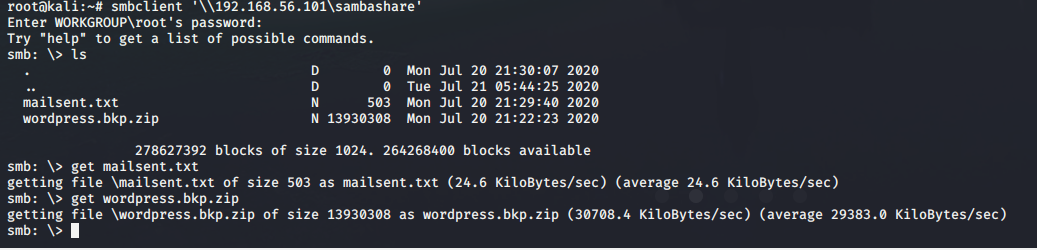
# 0x02:挖掘samba服务信息

由于这次开了139和445端口尝试用enum4linux探测了一波哦吼发现个sambashare

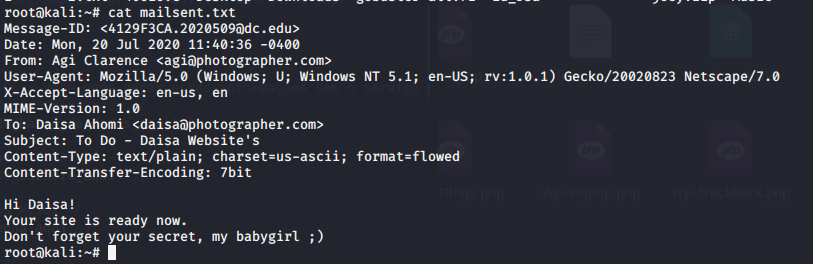
命令: enum4linux 192.168.56.101



然后使用波smbclient连接以下，密码为空，ls一波以后发现有2个文件用get下载到本地



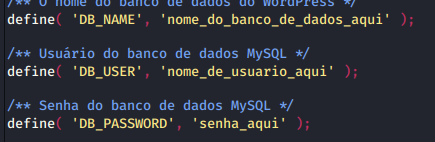
这里先打开mailsent.txt,提取波关键词 Daisa Ahomi(用户名) [daisa@photographer.com](mailto:daisa@photographer.com)(用户名) Agi Clarence [agi@photographer.com](mailto:agi@photographer.com)(用户名) secret可能是babygirl



另一边解压好wordpress.bkp.zip以后是套wordpress的CMS直接找wp-config-sampe.php找到数据库用户密码

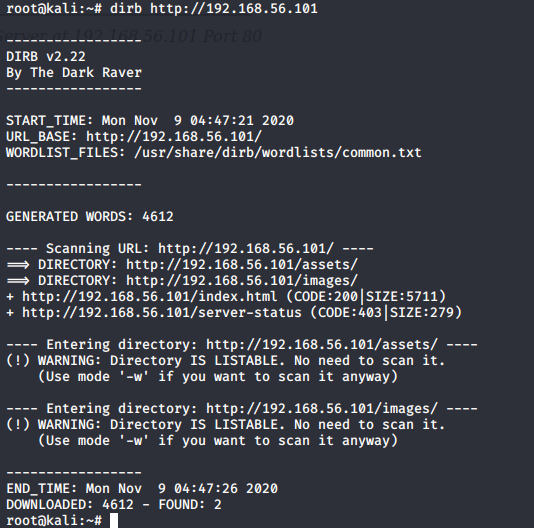
Nome\_de\_usuario\_auqi

Senha\_auqi

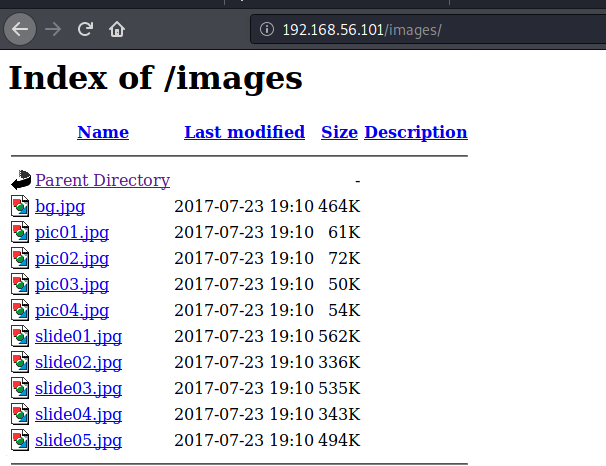


# 0x03:挖掘8000端口漏洞

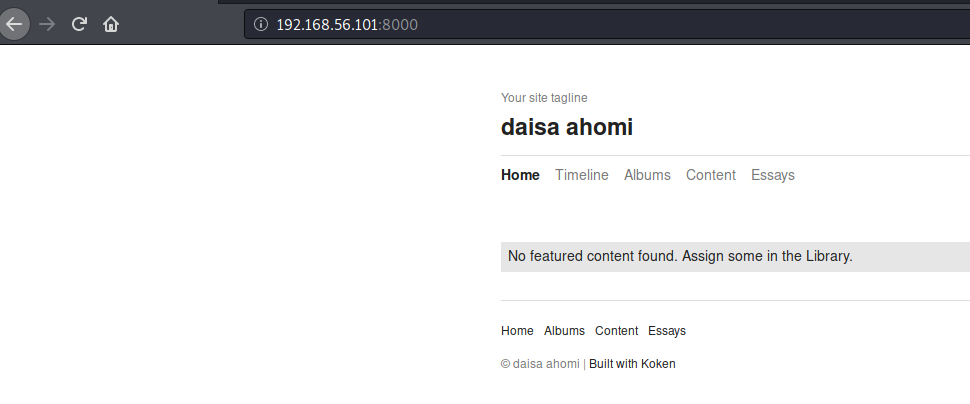
这里首先对80端口进行目录挖掘，然而只扫出/assets/和/images/目录



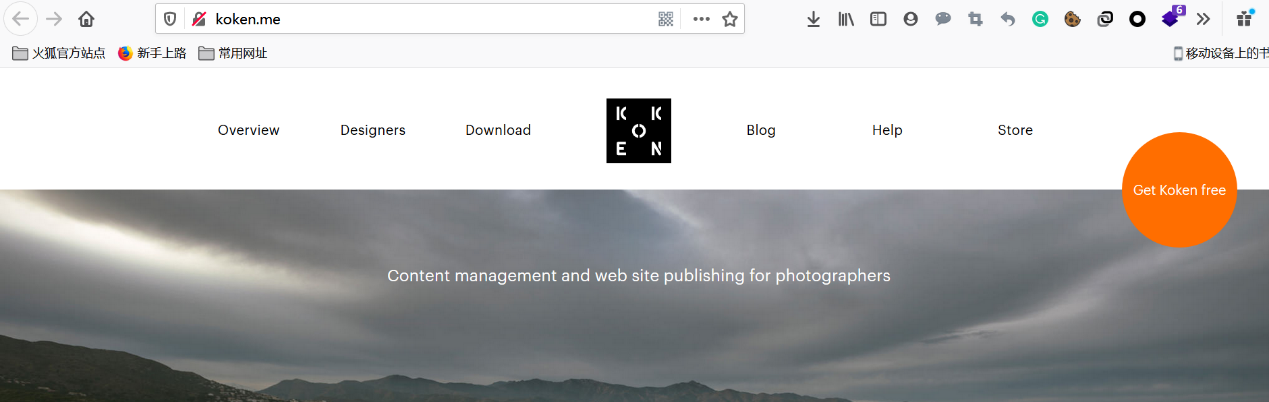
跟进以下/images=图片， /assets=CSS+js代码卒，更换字典也找不出东西



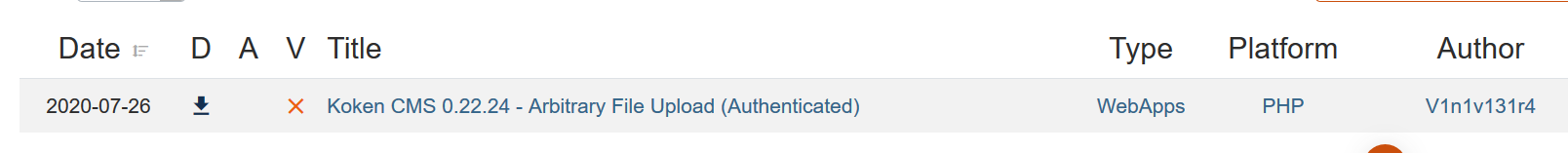
不过在8000端口倒是发现了点东西，下面是!daisa ahomi跟之前mail里面的内容符合然后旁边有个buit with koken



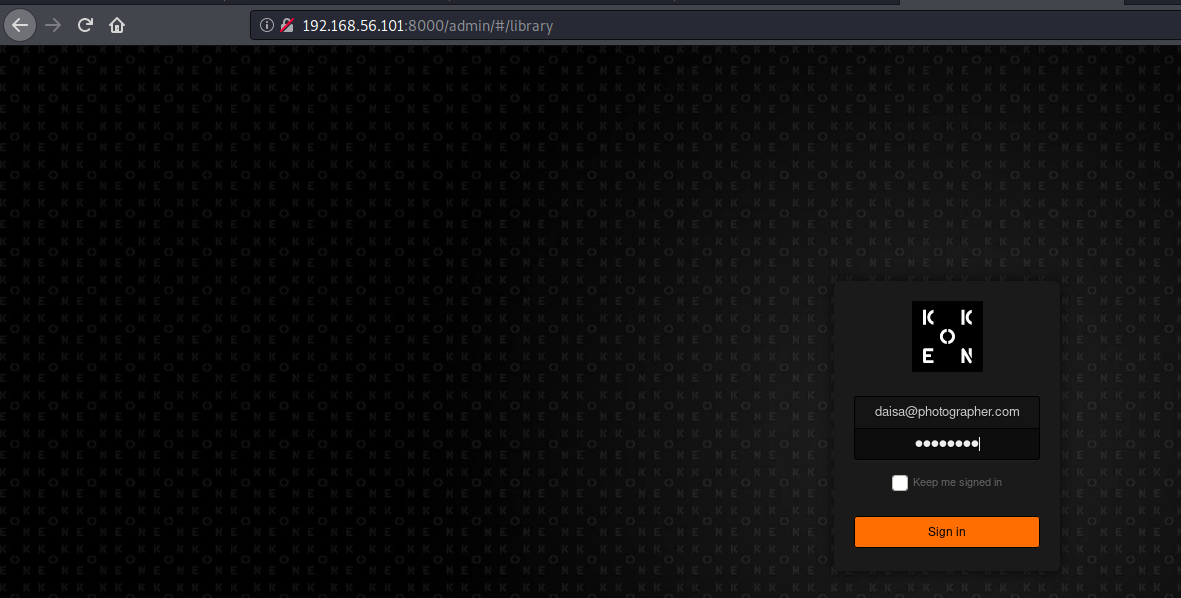
用必应查了一下是一个类似于个人博客的CMS来着



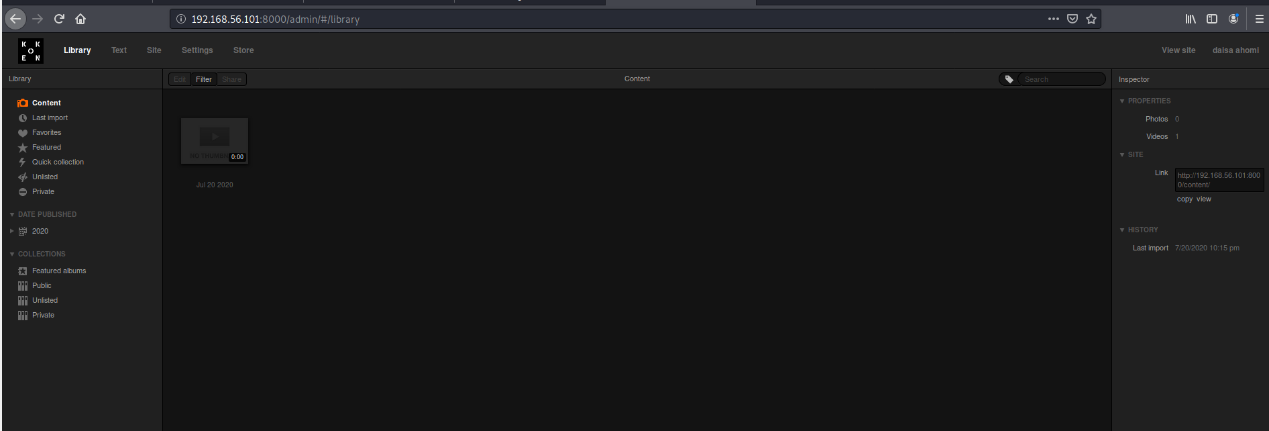
同时在exploitdb找到有关漏洞信息，只不过需要先登录后台。。。



后台就是直接/admin,密码的话结果这是daisa的站而且账号是邮箱的话可以确定用户名是daisa@photographer.com 密码尝试了一波以后是babygirl



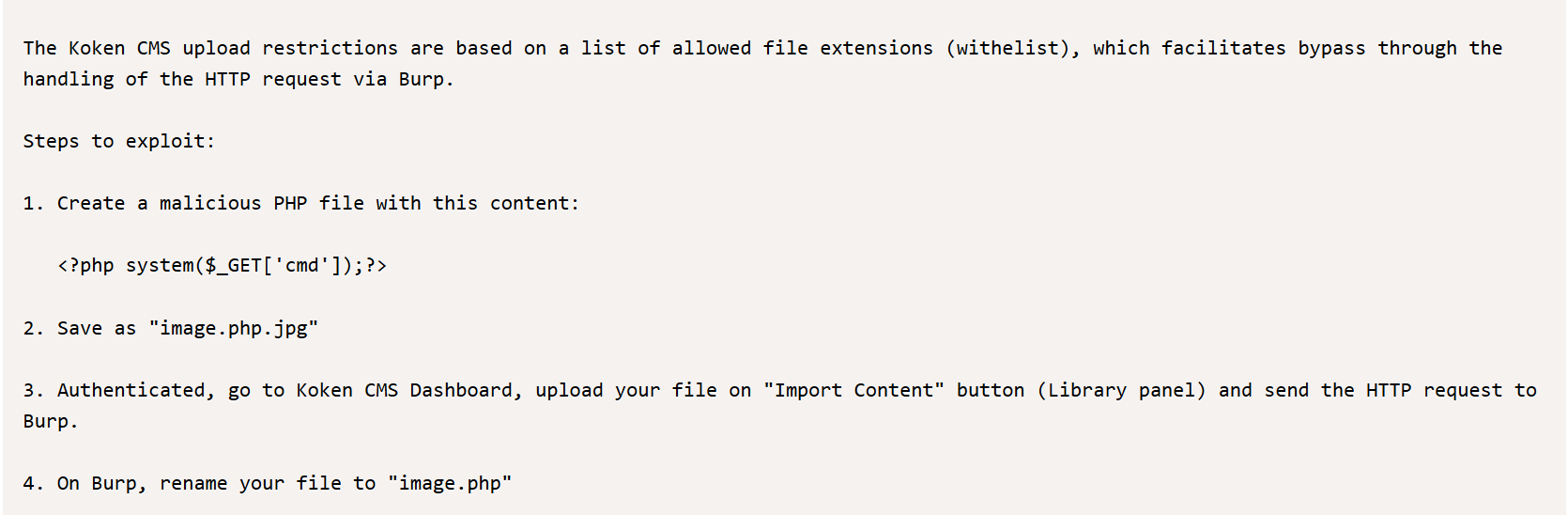
成功登录后台



# 0x04:上传反弹shell

这里看了exploitdb的说法，主要是通过白名单机制用burp抓包改东西来绕过

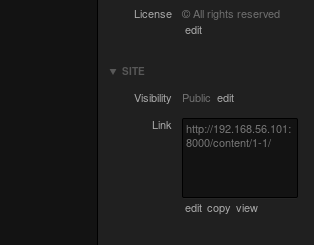
1. 首先建立一个php一句话保存为Image.php.jpg
2. 然后去到后台的Import content功能上传
3. 提前开启burp抓包改名为image.php
4. 最后通过下载来确定文件的位置



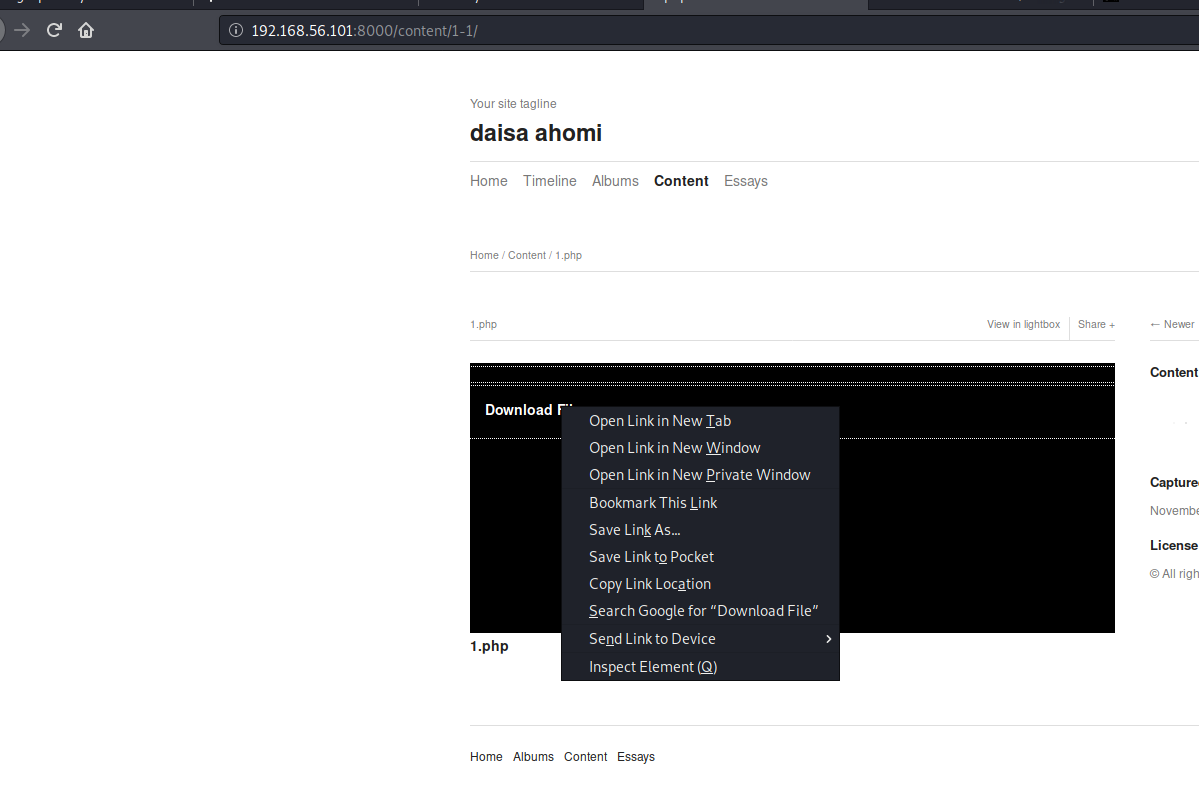
我觉得可以简化以下流程，直接把kali的反弹马改成1.php.jpg就行了然后用burp抓包删除后缀



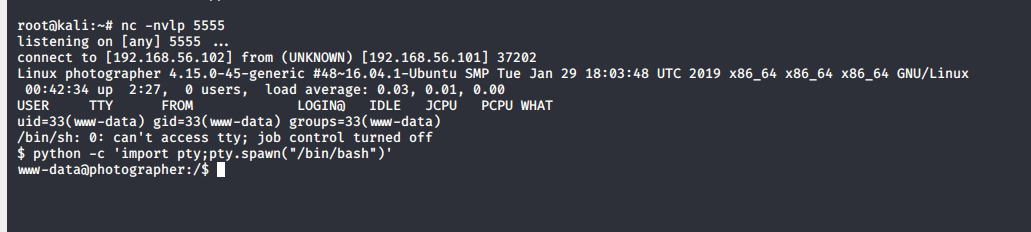
上传成功以后在右下角会有个link指向我们刚才上传的文件名字位置



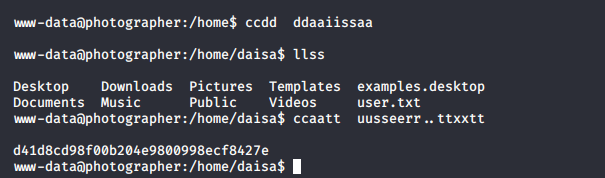
跟进以后有个下载文件功能右击点打开链接，记得提前开启netcat



成功反弹

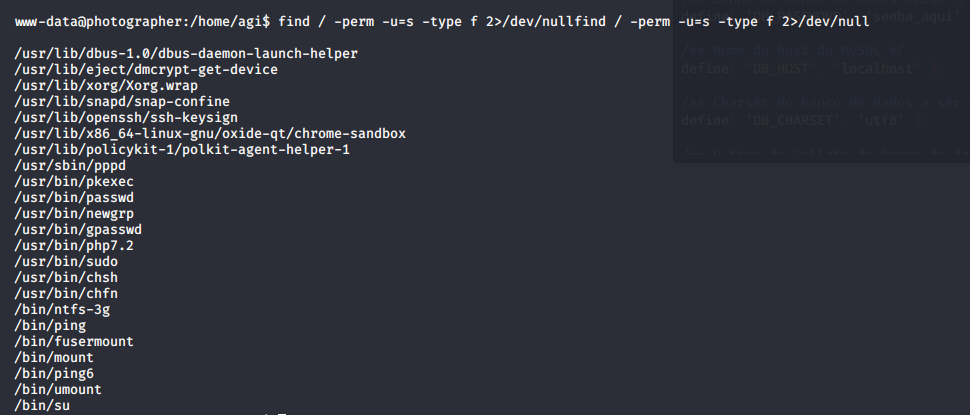


然后去到/home/daisa目录下得到user的flag注意这里是我的shell乱码了输入变成双倍输入



# 0x05:提权

Sudo -l日常失败，用find找到一波php7.2



这里原本想用me-and-my girlfriend的提权方法结果发现要我们输入密码，去gtfo bin找到波SUID的方法



提权成功

