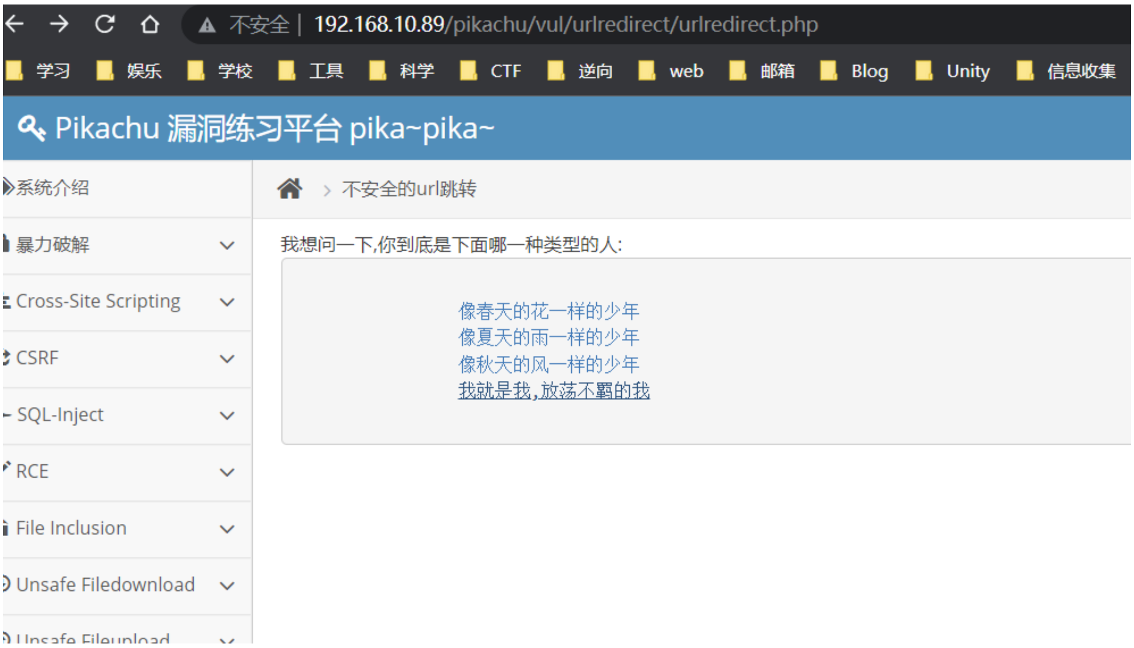
使用pikachu靶场实现url跳转漏洞

- 打开pikachu靶场的URL重定向关卡

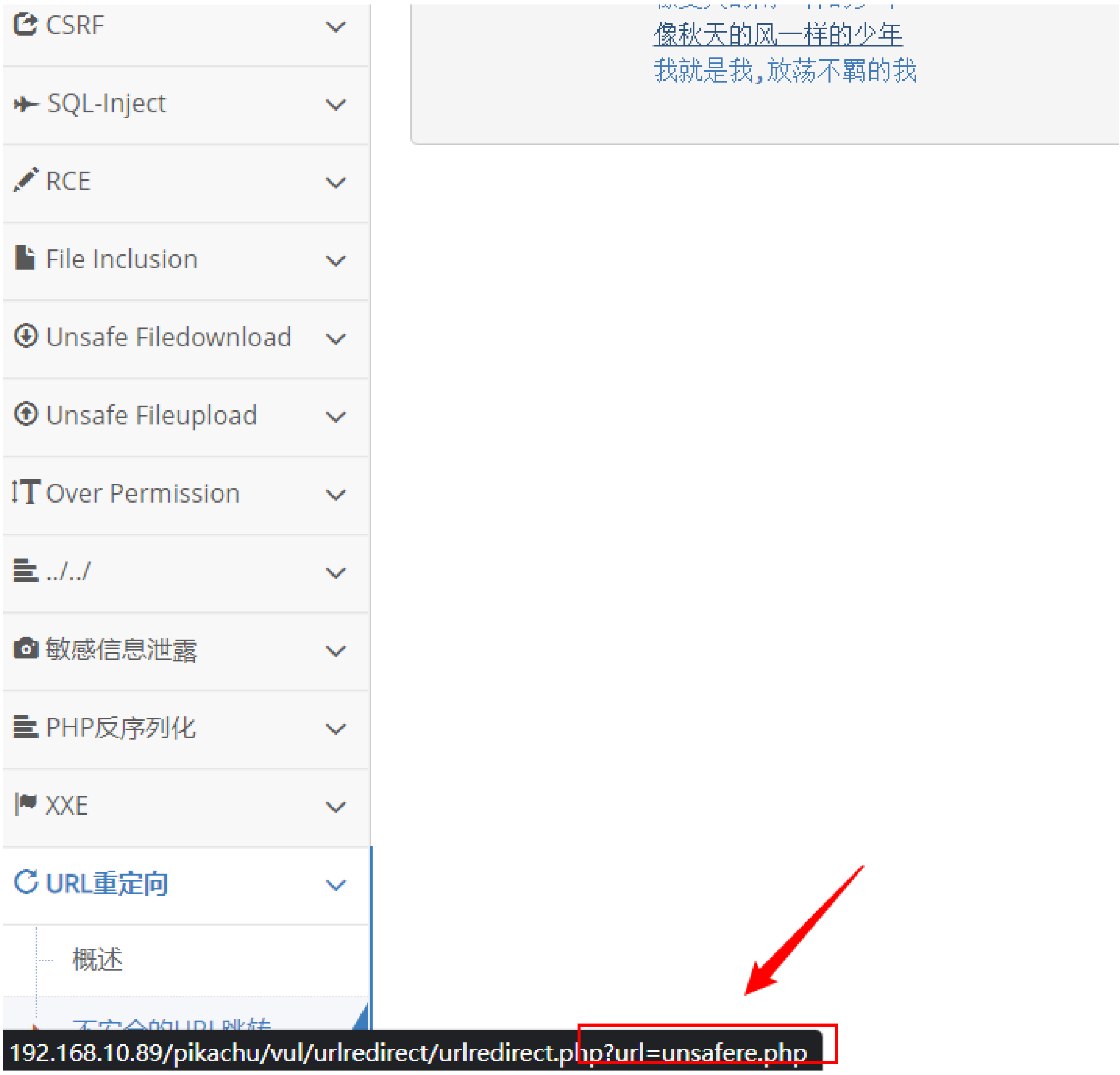


不安全 | 192.168.10.89/pikachu/vul/urlredirect/urlredirect.php

我想问一下,你到底是下面哪一种类型的人:

像春天的花一样的少年
像夏天的雨一样的少年
像秋天的风一样的少年
我就是我,放荡不羁的我

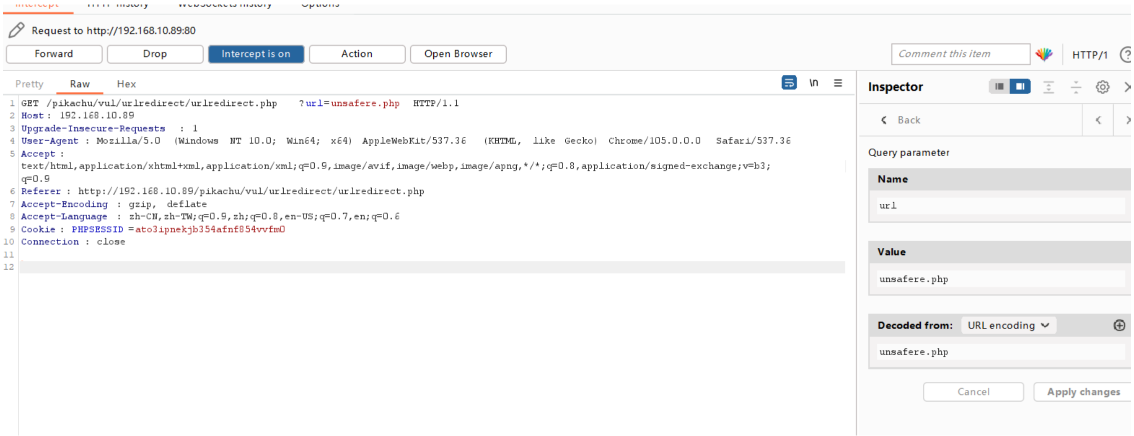
- 可以看到有链接存在跳转



像秋天的风一样的少年
我就是我,放荡不羁的我

192.168.10.89/pikachu/vul/urlredirect/urlredirect.php?url=unsafere.php

- 打开Omega代理并使用burp进行抓包



Request to http://192.168.10.89:80

```
GET /pikachu/vul/urlredirect/urlredirect.php    ?url=unsafere.php   HTTP/1.1
Host : 192.168.10.89
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64) AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/105.0.0.0   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer : http://192.168.10.89/pikachu/vul/urlredirect/urlredirect.php
Accept-Encoding  : gzip,  deflate
Accept-Language  : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie : PHPSESSID =ato3ipnekjb354afnf854vvfm0
Connection : close
```

Inspector

Query parameter

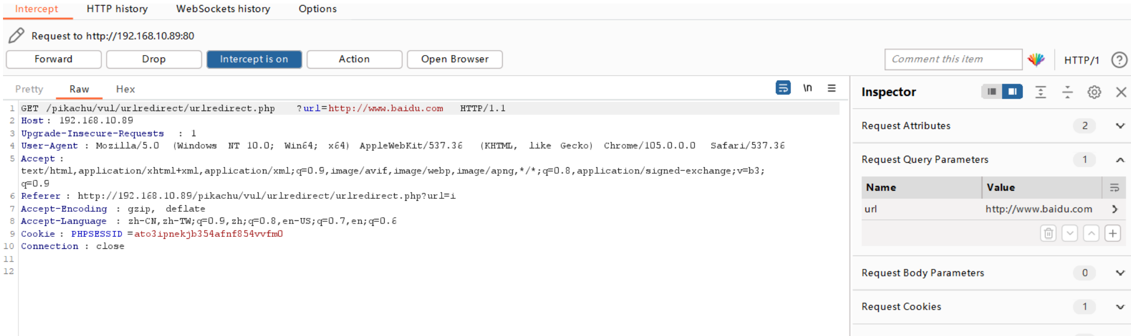
Name: url

Value: unsafere.php

Decoded from: URL encoding

unsafere.php

- 将url改为http://www.baidu.com后放包



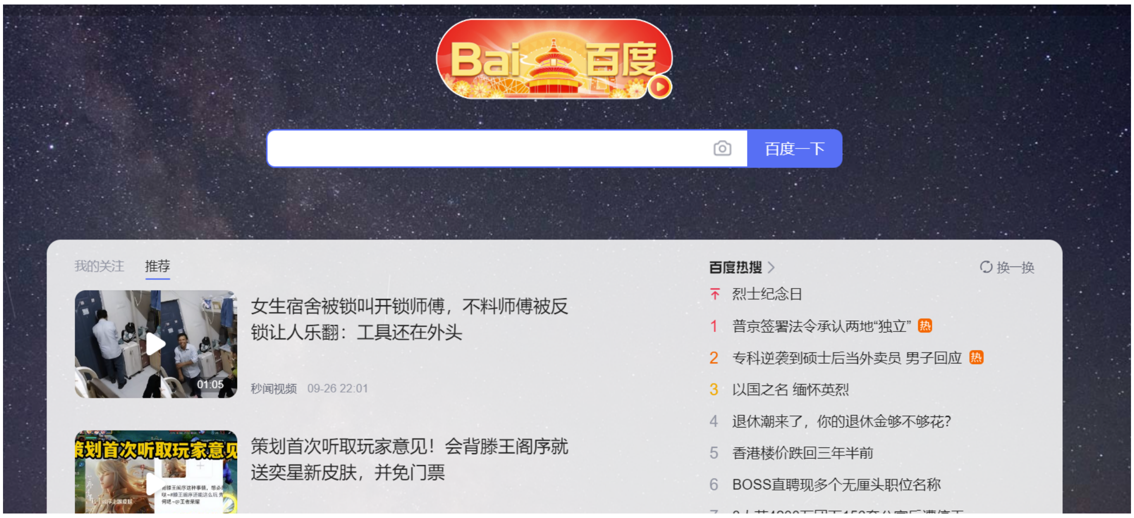
Request to http://192.168.10.89:80

```
GET /pikachu/vul/urlredirect/urlredirect.php    ?url=http://www.baidu.com    HTTP/1.1
Host : 192.168.10.89
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64) AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/105.0.0.0   Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer : http://192.168.10.89/pikachu/vul/urlredirect/urlredirect.php?url=i
Accept-Encoding  : gzip,  deflate
Accept-Language  : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie : PHPSESSID =ato3ipnekjb354afnf854vvfm0
Connection : close
```

Inspector

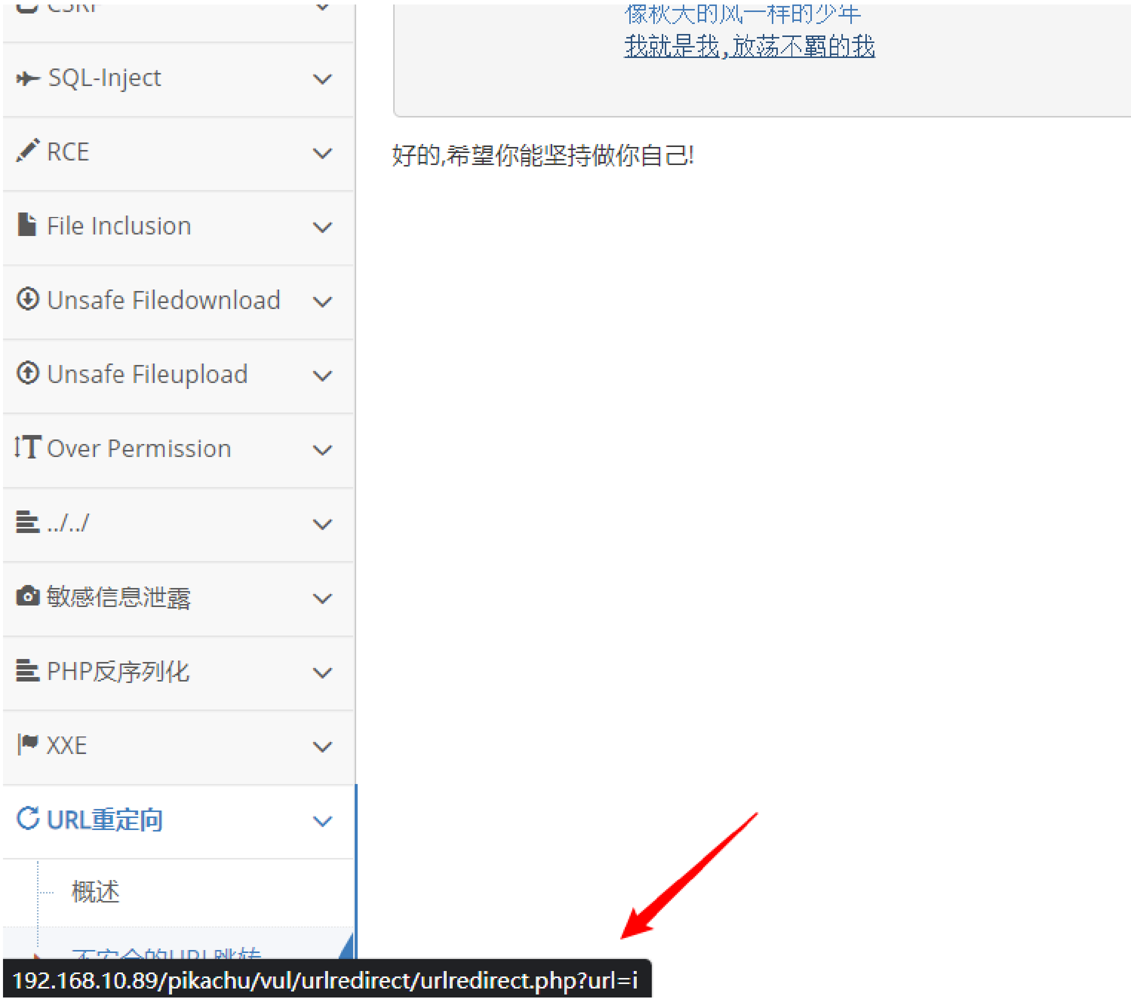
Name	Value
url	http://www.baidu.com

- 可以看到跳转到了http://www.baidu.com



Bai 百度
百度一下
我的关注
推荐
女生宿舍被锁叫开锁师傅，不料师傅被反锁让人乐翻：工具还在外头
01:05
秒闻视频 09-26 22:01
策划首次听取玩家意见！会背滕王阁序就送突星新皮肤，并免门票
百度热搜
换一换
烈士纪念日
1 普京签署法令承认两地“独立”
2 专科逆袭到硕士后当外卖员 男子回应
3 以国之名 缅怀英烈
4 退休潮来了，你的退休金够不够花?
5 香港楼价跌回三年半前
6 BOSS直聘现多个无厘头职位名称

- 还有一个链接也存在url跳转



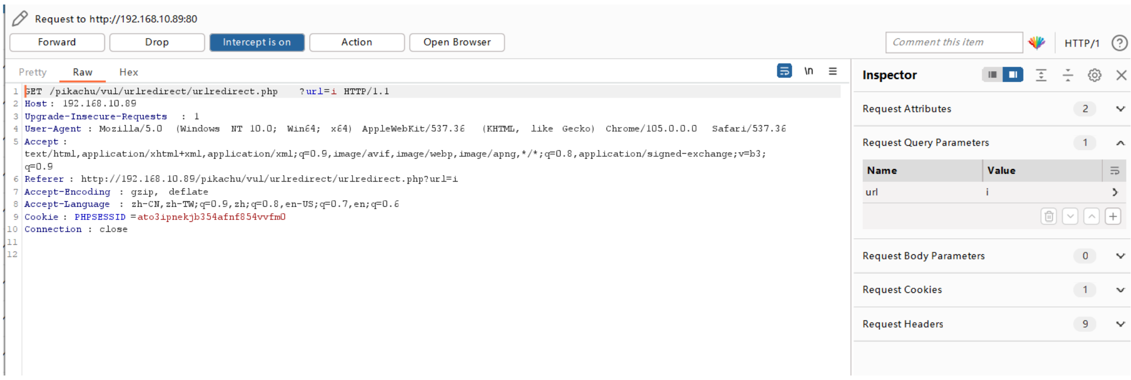
像秋天的风一样的少年

我就是我,放荡不羁的我

好的,希望你能坚持做你自己!

192.168.10.89/pikachu/vul/urlredirect/urlredirect.php?url=i

- 继续使用burp抓包



```
GET /pikachu/vul/urlredirect/urlredirect.php ?url=i HTTP/1.1
Host : 192.168.10.89
Upgrade-Insecure-Requests : 1
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer : http://192.168.10.89/pikachu/vul/urlredirect/urlredirect.php?url=i
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie : PHPSESSID =ato3ipnekjb354afnf854vvfm0
Connection : close
```

Request Attributes 2

Request Query Parameters 1

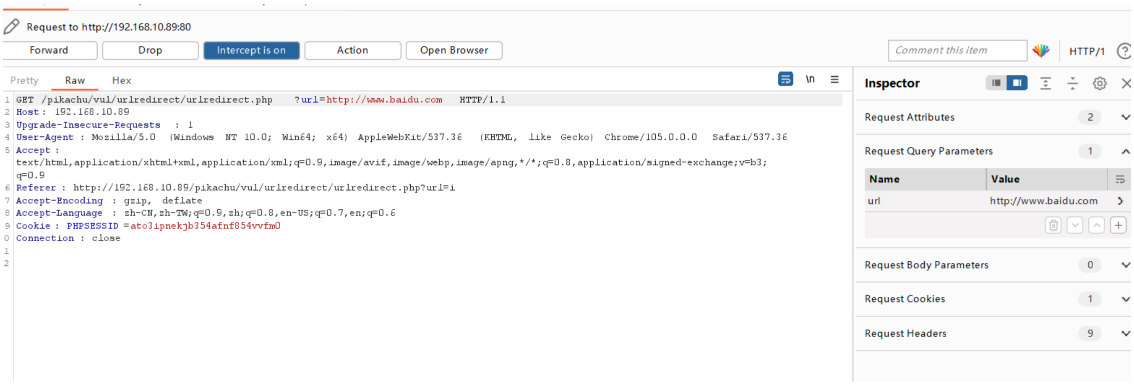
Name	Value
url	i

Request Body Parameters 0

Request Cookies 1

Request Headers 9

- 使用与上面相同的方法修改url即可实现跳转



```
GET /pikachu/vul/urlredirect/urlredirect.php ?url=http://www.baidu.com HTTP/1.1
Host : 192.168.10.89
Upgrade-Insecure-Requests : 1
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer : http://192.168.10.89/pikachu/vul/urlredirect/urlredirect.php?url=i
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie : PHPSESSID =ato3ipnekjb354afnf854vvfm0
Connection : close
```

Request Attributes 2

Request Query Parameters 1

Name	Value
url	http://www.baidu.com

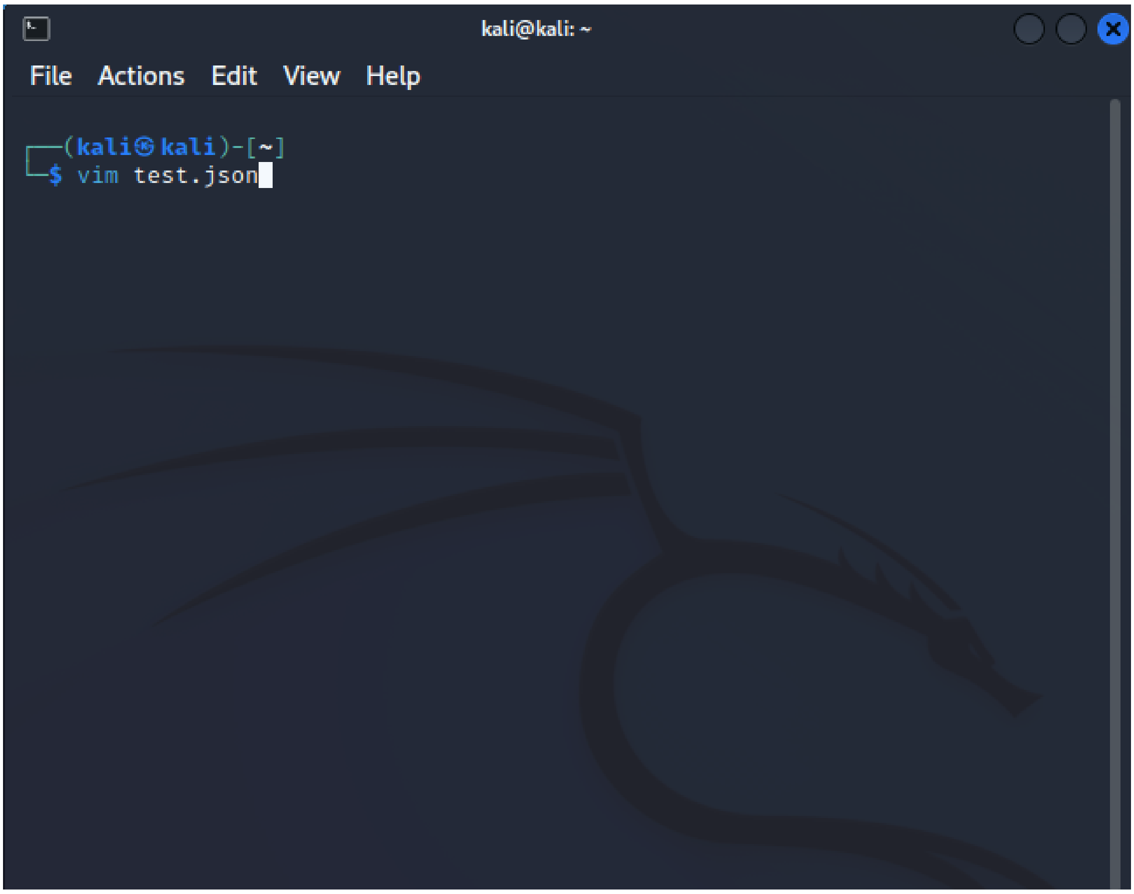
Request Body Parameters 0

Request Cookies 1

Request Headers 9

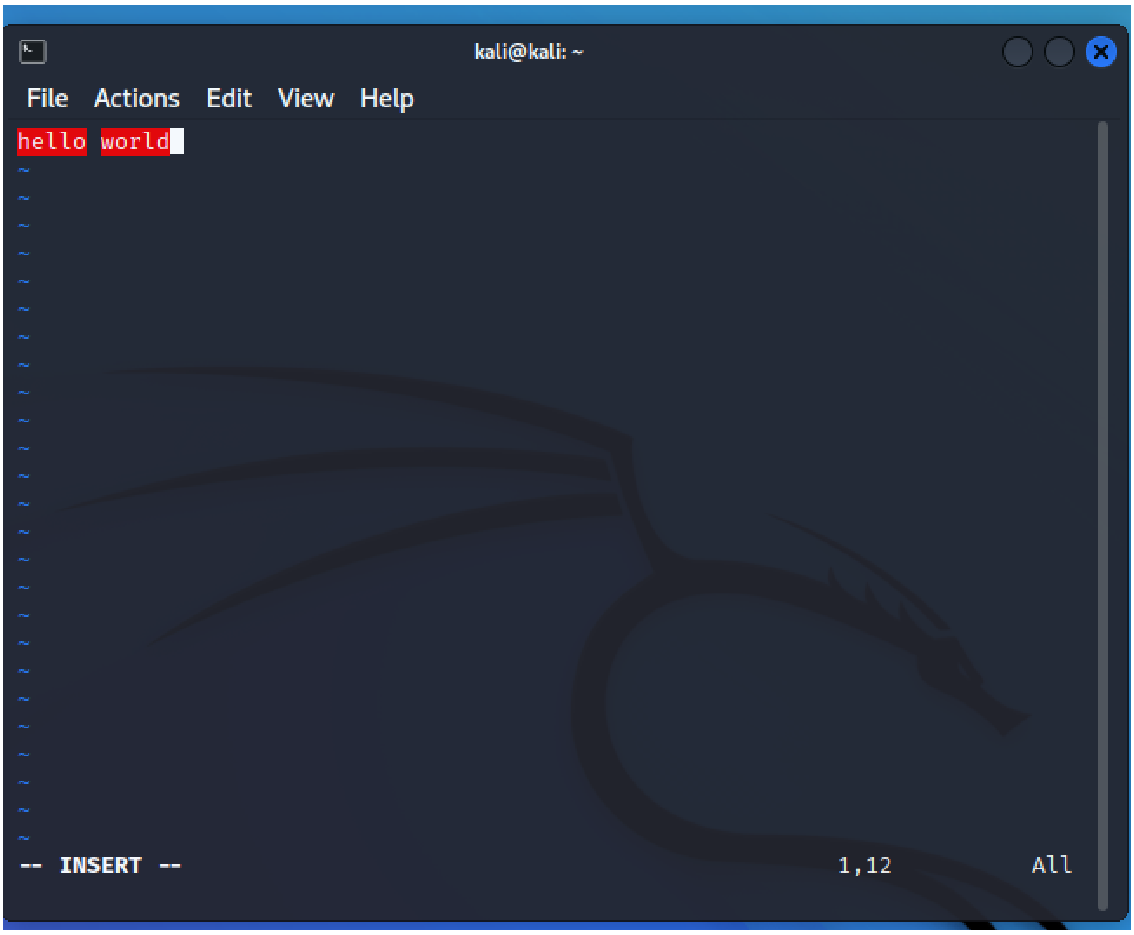
用vim创建一个test.json文件，内容为hello world

- 输入vim test.json



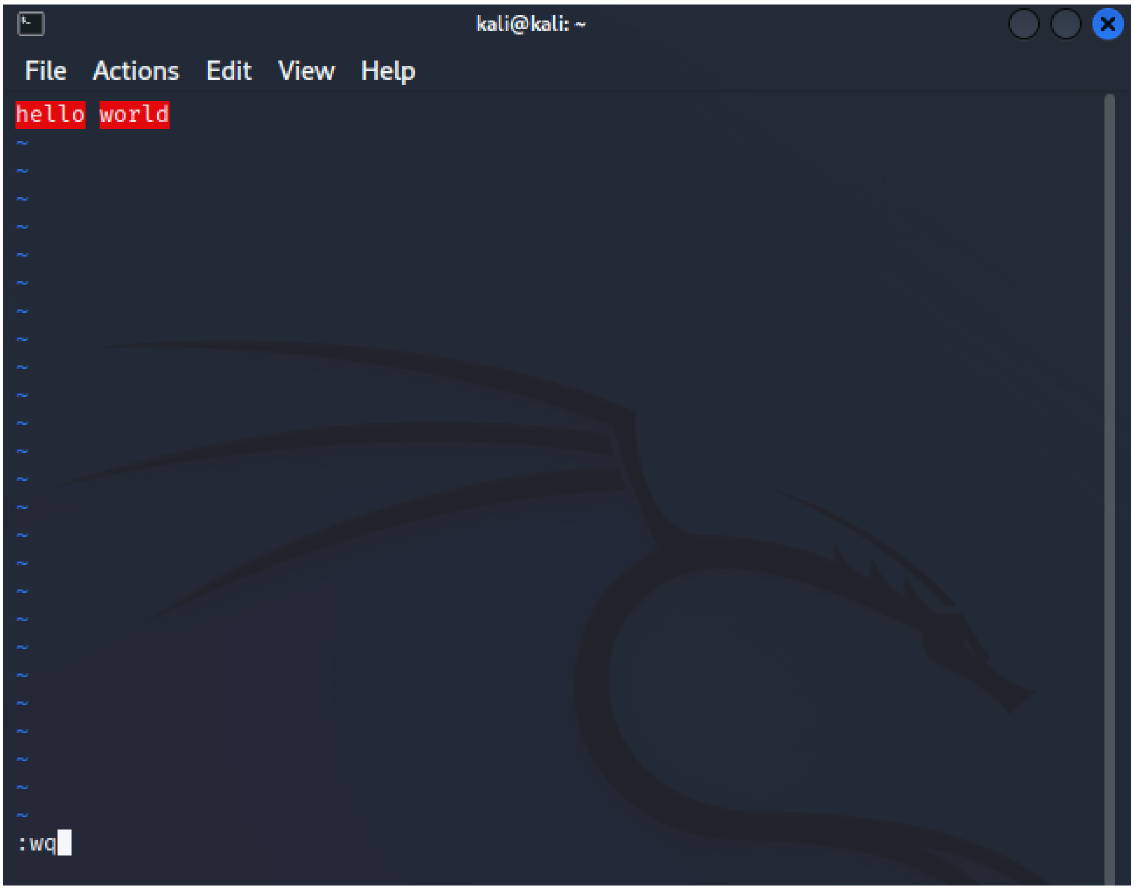
```
┌──(kali㉿kali)-[~]
└─$ vim test.json
```

- 在进入的界面中按i键并输入内容



```
hello world
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
-- INSERT --                                      1,12          All
```

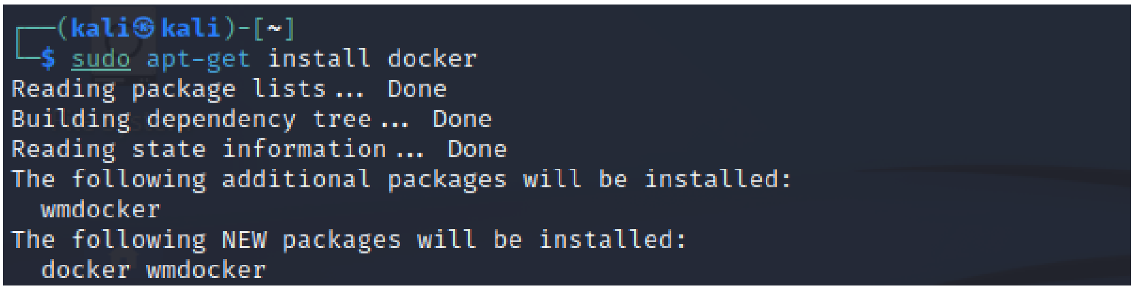
- 按下esc后按下shift+;后输入wq即可保存



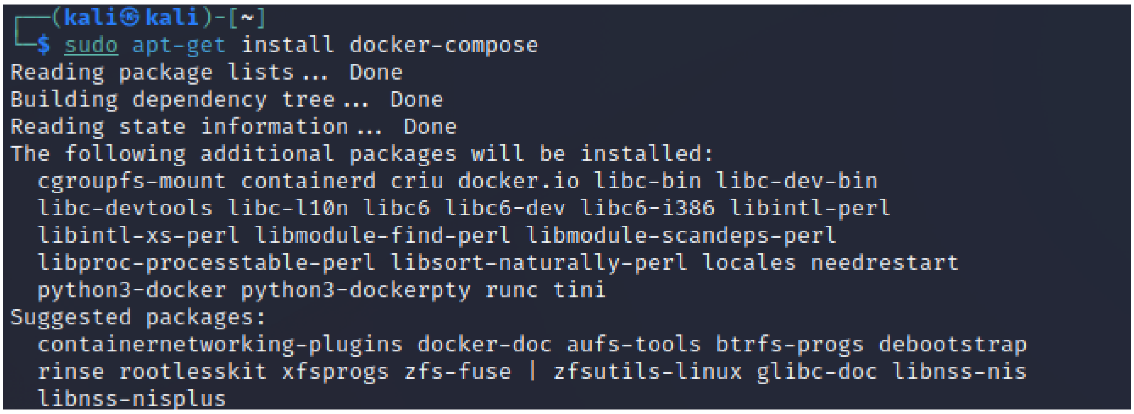
```
hello world
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

使用docker安装thinkphp靶场

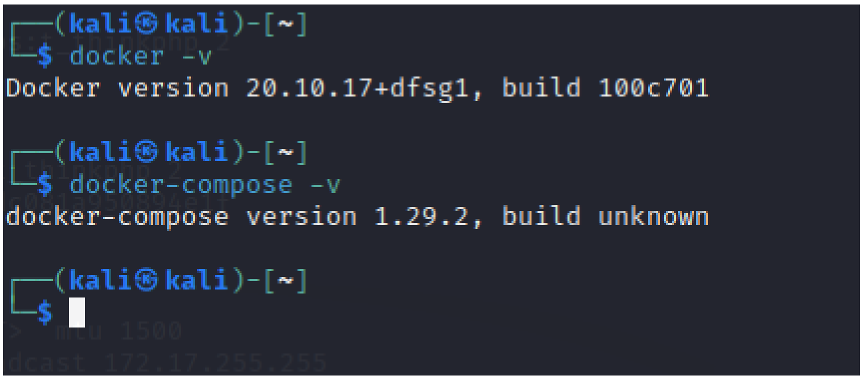
- 安装docker和docker-compose



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wmdocker
The following NEW packages will be installed:
  docker wmdocker
```

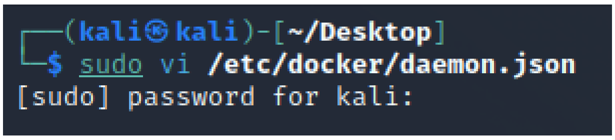


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install docker-compose
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cgroupfs-mount containerd criu docker.io libc-bin libc-dev-bin
  libc-devtools libc-l10n libc6 libc6-dev libc6-i386 libintl-perl
  libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl
  libproc-processtable-perl libsort-naturally-perl locales needrestart
  python3-docker python3-dockerpty runc tini
Suggested packages:
  containernetworking-plugins docker-doc aufs-tools btrfs-progs debootstrap
  rinse rootlesskit xfsprogs zfs-fuse | zfsutils-linux glibc-doc libnss-nis
  libnss-nisplus
```

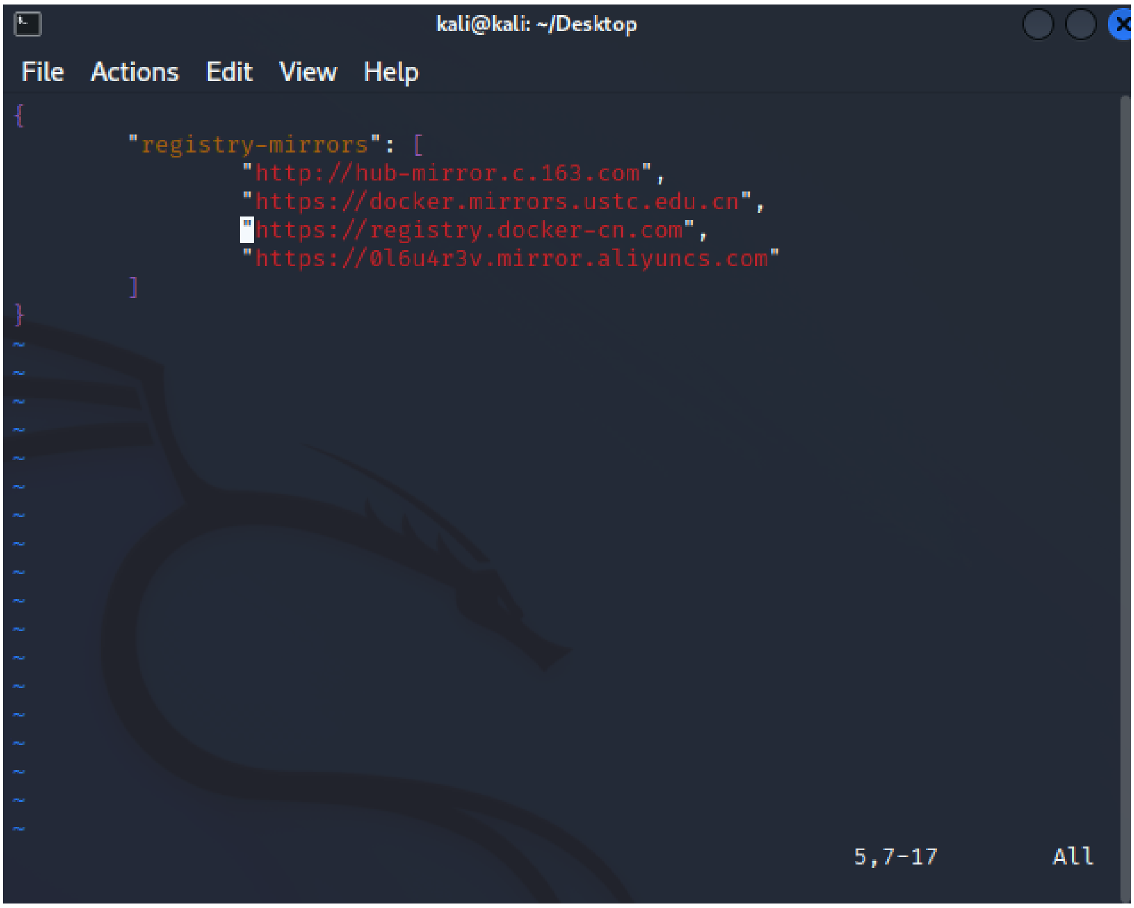


```
┌──(kali㉿kali)-[~]
└─$ docker -v
Docker version 20.10.17+dfsg1, build 100c701

┌──(kali㉿kali)-[~]
└─$ docker-compose -v
docker-compose version 1.29.2, build unknown

┌──(kali㉿kali)-[~]
└─$ 
```

- 配置docker仓库镜像地址

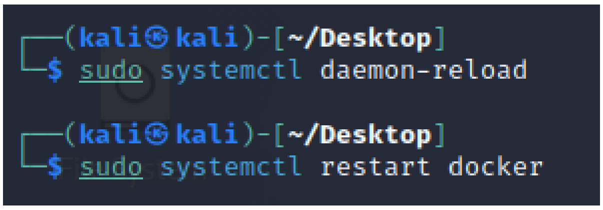


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo vi /etc/docker/daemon.json
[sudo] password for kali:
```

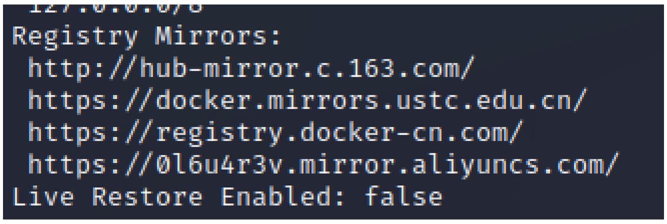


```
{
        "registry-mirrors": [
                "http://hub-mirror.c.163.com",
                "https://docker.mirrors.ustc.edu.cn",
                "https://registry.docker-cn.com",
                "https://0l6u4r3v.mirror.aliyuncs.com"
        ]
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                  5,7-17        All
```

- 重启服务

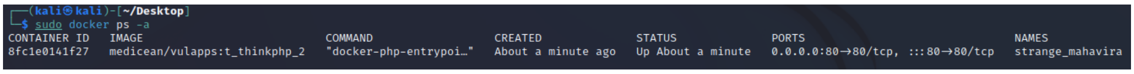


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl daemon-reload

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl restart docker
```



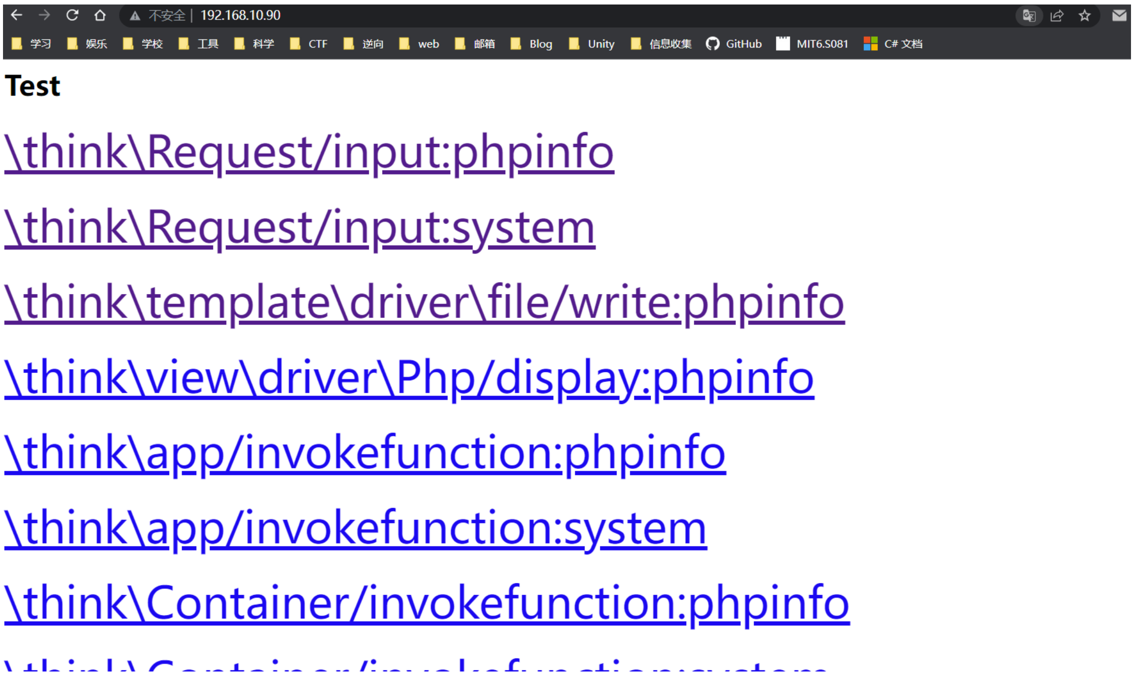
```
  127.0.0.0/8
Registry Mirrors:
 http://hub-mirror.c.163.com/
 https://docker.mirrors.ustc.edu.cn/
 https://registry.docker-cn.com/
 https://0l6u4r3v.mirror.aliyuncs.com/
Live Restore Enabled: false
```

- 拉取镜像并启动



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE                         COMMAND                  CREATED              STATUS              PORTS                               NAMES
8fc1e0141f27   medicean/vulapps:t_thinkphp_2   "docker-php-entrypoi…"   About a minute ago   Up About a minute   0.0.0.0:80→80/tcp, :::80→80/tcp   strange_mahavira
```

- 访问地址



Test

\think\Request/input:phpinfo

\think\Request/input:system

\think\template\driver\file/write:phpinfo

\think\view\driver\Php/display:phpinfo

\think\app/invokefunction:phpinfo

\think\app/invokefunction:system

\think\Container/invokefunction:phpinfo

\think\Container/invokefunction:system