安装环境

一、安装docker

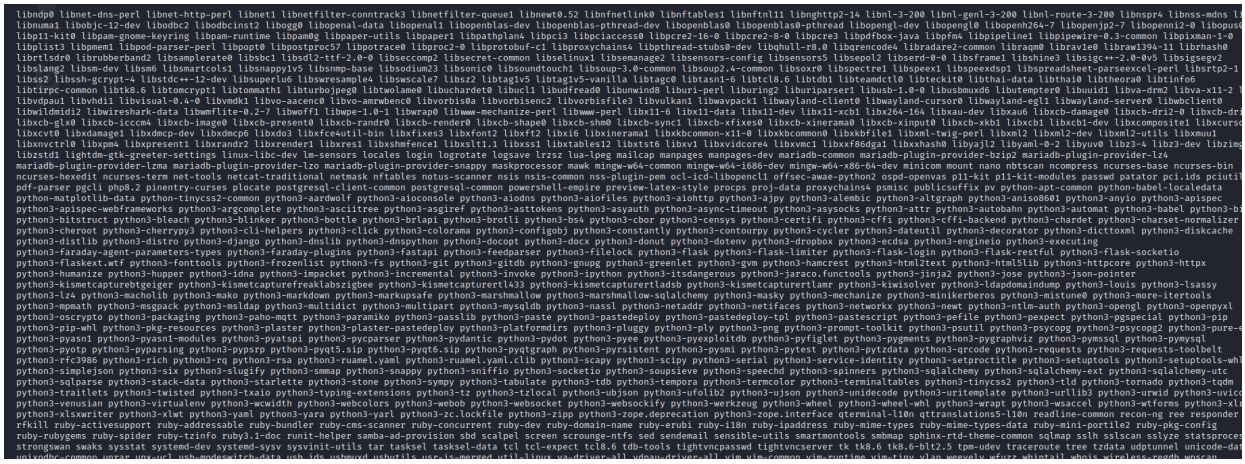
为方便渗透，本实验在kali虚拟机中进行。因此为布置靶场，决定在kali环境下安装。

1. 更新apt源满足下载要求

```
vim /etc/apt/sources.list

#中科大
deb http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib
deb-src http://mirrors.ustc.edu.cn/kali kali-rolling main non-free contrib

#进行系统或工具的更新
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
```



正在更新软件

```
获取:1034 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-t2info all 2.0.6-1 [66.7 kB]
获取:1035 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-i18n all 1.14.5-1 [41.4 kB]
获取:1036 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-activesupport all 2:6.1.7.3+dfsg-3 [202 kB]
获取:1037 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-addressable all 2.8.5-1 [53.0 kB]
获取:1038 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-cms-scanner all 0.13.9-0kali2 [34.2 kB]
获取:1039 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-dev amd64 1:3.1+nmu1 [4,828 B]
获取:1040 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-domain-name all 0.6.20240107-1 [47.9 kB]
获取:1041 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-erubi all 1.12.0-1 [10.6 kB]
获取:1042 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-ipaddress all 0.8.3-4 [28.6 kB]
获取:1043 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-mime-types-data all 3.2024.0206-1 [139 kB]
获取:1044 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-mime-types all 3.5.2-1 [26.2 kB]
获取:1045 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-mini-portile2 all 2.8.5-1 [20.8 kB]
获取:1046 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-pkg-config all 1.5.6-1 [8,456 B]
获取:1047 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby-spider all 0.5.0-6 [11.0 kB]
获取:1048 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 ruby3.1-doc all 3.1.2-8.3 [2,450 kB]
获取:1049 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 runit-helper all 2.16.2 [6,568 B]
获取:1050 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 samba-ad-provision all 2:4.20.1+dfsg-4 [497 kB]
获取:1051 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sbd amd64 1.37-1kali5 [46.2 kB]
获取:1052 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 scalpel amd64 1.60+git20240110.6960eb2-1 [33.3 kB]
获取:1053 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 screen amd64 4.9.1-1 [594 kB]
获取:1054 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 scrounge-ntfs amd64 0.9-11 [17.4 kB]
获取:1055 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sendemail all 1.56-5.2 [31.4 kB]
获取:1056 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 smartmontools amd64 7.4-2 [642 kB]
获取:1057 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 smbmap all 1.9.2-1 [29.4 kB]
获取:1058 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sslh amd64 1.22c-1+b2 [81.1 kB]
获取:1059 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sslscan amd64 2.1.3-0kali1 [1,519 kB]
获取:1060 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sslyze all 5.2.0-0kali2 [420 kB]
获取:1061 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 statsprocessor amd64 0.11+git20160316-4 [11.7 kB]
获取:1062 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 strongswan all 5.9.13-2 [84.5 kB]
获取:1063 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 swaks all 20240103.0-1 [118 kB]
获取:1064 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 sysstat amd64 12.7.5-2 [623 kB]
获取:1065 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 systemd-dev all 255.5-1 [60.5 kB]
获取:1066 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 tdb-tools amd64 1.4.10-1 [26.9 kB]
获取:1067 http://mirrors.ustc.edu.cn/kali kali-rolling/main amd64 tk amd64 8.6.14 [4,076 B]
```

2. 安装docker并检验

```
sudo apt-get install docker.io
docker run --rm hello-world
```

```
┌──(root㉿kali)-[/home/malanbo/Desktop]
└─# docker run --rm hello-world
Unable to find image 'hello-world:latest' locally

latest: Pulling from library/hello-world
2db29710123e: Pull complete
Digest: sha256:2498fce14358aa50ead0cc6c19990fc6ff866ce72aeb5546e1d59caac3d0d60f
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

利用书上的docker源码，成功挂载

- 4.1 暴力破解漏洞
  - 4.1.2 暴力破解漏洞攻击
- 4.2 SQL注入漏洞基础
  - 4.2.4 Union注入攻击
  - 4.2.6 Boolean注入攻击
  - 4.2.8 报错注入攻击
- 4.3 SQL注入漏洞进阶
  - 4.3.1 时间注入攻击
  - 4.3.3 堆叠查询注入攻击
  - 4.3.5 二次注入攻击
  - 4.3.7 宽字节注入攻击
  - 4.3.9 Cookie注入攻击
  - 4.3.11 Base64注入攻击
  - 4.3.13 XFF注入攻击
- 4.4 XSS漏洞基础
  - 4.4.3 反射型XSS漏洞攻击
  - 4.4.5 存储型XSS漏洞攻击
  - 4.4.7 DOM型XSS漏洞攻击
- 4.6 CSRF漏洞
  - 4.6.3 CSRF漏洞攻击
  - 4.6.5 XSS+CSRF漏洞攻击
- 4.7 SSRF漏洞
  - 4.7.3 SSRF漏洞攻击
  - 4.7.5 SSRF漏洞绕过技术
- 4.8 文件上传漏洞