# Apache ssrf CVE-2021-40438

使用vulhub 靶场

先安装docker

然后git clone <https://github.com/vulhub/vulhub.git> 下载vulhub

进到vulhub目录下启动环境

到vulhub/httpd/CVE-2021-40438下启动环境

docker-compose build

docker-compose up -d

使用docker-compose的时候出了问题 总是提示不支持，就换成 docker compose 把-去掉

Docker pull很慢的话

就在docker desktop里 的Docker Engine 的配置里把https://yxzrazem.mirror.aliyuncs.com加到"registry-mirrors"的数组里

手机屏幕截图

描述已自动生成

然后重启 重新pull

然后访问 8080

<http://localhost:8080/>

图形用户界面, 文本, 应用程序, 网站

描述已自动生成

如果burpsuite点了send repeater没反应

那就在这个页面

图形用户界面, 文本, 应用程序

描述已自动生成

点击send 才有反应

unix:与|之间传入内容长度大概超过4092的字符串，就能构造出uds\_path为null的结果，让Apache不再发送请求给unix套接字。

SSRF漏洞的本质是Apache在解析反代服务URL的时候，由于对unix:位置要求不严格，导致用户的输入可以控制反代的逻辑，最终导致反代URL被控制，造成SSRF漏洞。

没复现出来 里面一些东西没理解 后面再重新复现

不太懂他这个利用点