攻防世界web进阶区blgdel详解

原创

無名之涟 于 2020-08-19 20:30:18 发布

分类专栏： CTF

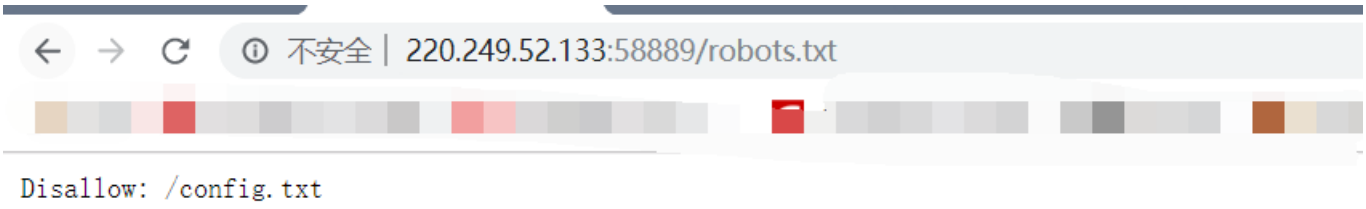
本文链接：https://blog.csdn.net/hxhxhxhxx/article/details/108109579

攻防世界web进阶区blgdel详解

题目

详解

我们发现他有个robots.txt文件




```
Disallow: /config.txt
```


我注册了好几次，也没登录成功，挺离谱


```
<?php

class master
{
        private $path;
        private $name;

        function __construct()
        {

        }

        function stream_open($path)
        {
                if(!preg_match('/(.*)\/(.*)$/s',$path,$array,0,9))
                        return 1;
                $a=$array[1];
                parse_str($array[2],$array);

                if(isset($array['path']))
                {
                        $this->path=$array['path'];
                }
                else
                        return 1;
                if(isset($array['name']))
                {
                        $this->name=$array['name'];
                }
                else
                        return 1;

                if($a==='upload')
```


直接访问，发现是源码

```php
<?php

class master
{
 private $path;
 private $name;

 function __construct()
 {

 }

 function stream_open($path)
```

```
{
 if(!preg_match('/(.*)\/(.*)$/s',$path,$array,0,9))
  return 1;
 $a=$array[1];
 parse_str($array[2],$array);

 if(isset($array['path']))
 {
  $this->path=$array['path'];
 }
 else
  return 1;
 if(isset($array['name']))
 {
  $this->name=$array['name'];
 }
 else
  return 1;

 if($a==='upload')
 {
  return $this->upload($this->path,$this->name);
 }
 elseif($a==='search')
 {
  return $this->search($this->path,$this->name);
 }
 else
  return 1;
}
function upload($path,$name)
{
 if(!preg_match('/^uploads\/[a-z]{10}\/$/is',$path)||empty($_FILES[$name]['tmp_name']))
  return 1;

 $filename=$_FILES[$name]['name'];
 echo $filename;

 $file=file_get_contents($_FILES[$name]['tmp_name']);

 $file=str_replace('<','!',$file);
 $file=str_replace(urldecode('%03'),'!',$file);
 $file=str_replace('"','!',$file);
 $file=str_replace("'","!",$file);
 $file=str_replace('.','!',$file);
 if(preg_match('/file:|http|pre|etc/is',$file))
 {
  echo 'illegalbbbbbb!';
  return 1;
 }

 file_put_contents($path.$filename,$file);
 file_put_contents($path.'user.jpg',$file);


 echo 'upload success!';
 return 1;
}
function search($path,$name)
```

```
{
 if(!is_dir($path))
 {
  echo 'illegal!';
  return 1;
 }
 $files=scandir($path);
 echo '</br>';
 foreach($files as $k=>$v)
 {
  if(str_ireplace($name,'',$v)!==$v)
  {
   echo $v.'</br>';
  }
 }

 return 1;
}

function stream_eof()
{
 return true;
}
function stream_read()
{
 return '';
}
function stream_stat()
{
 return '';
}

}

stream_wrapper_unregister('php');
stream_wrapper_unregister('phar');
stream_wrapper_unregister('zip');
stream_wrapper_register('master','master');

?>
```

xctf环境无法登录，此题先更到这里
我们可以先代码审计，环境好了再写
在结合我们刚开始找的源代码，就是上传文件的操作。

parse_str() 函数把查询字符串解析到变量中。
代码审计，

定义了一个类master，其中有几个方法，我们逐个分析。

stream_open()
对path的传参和name的传参从字符串到变量，做了一个方法对应。

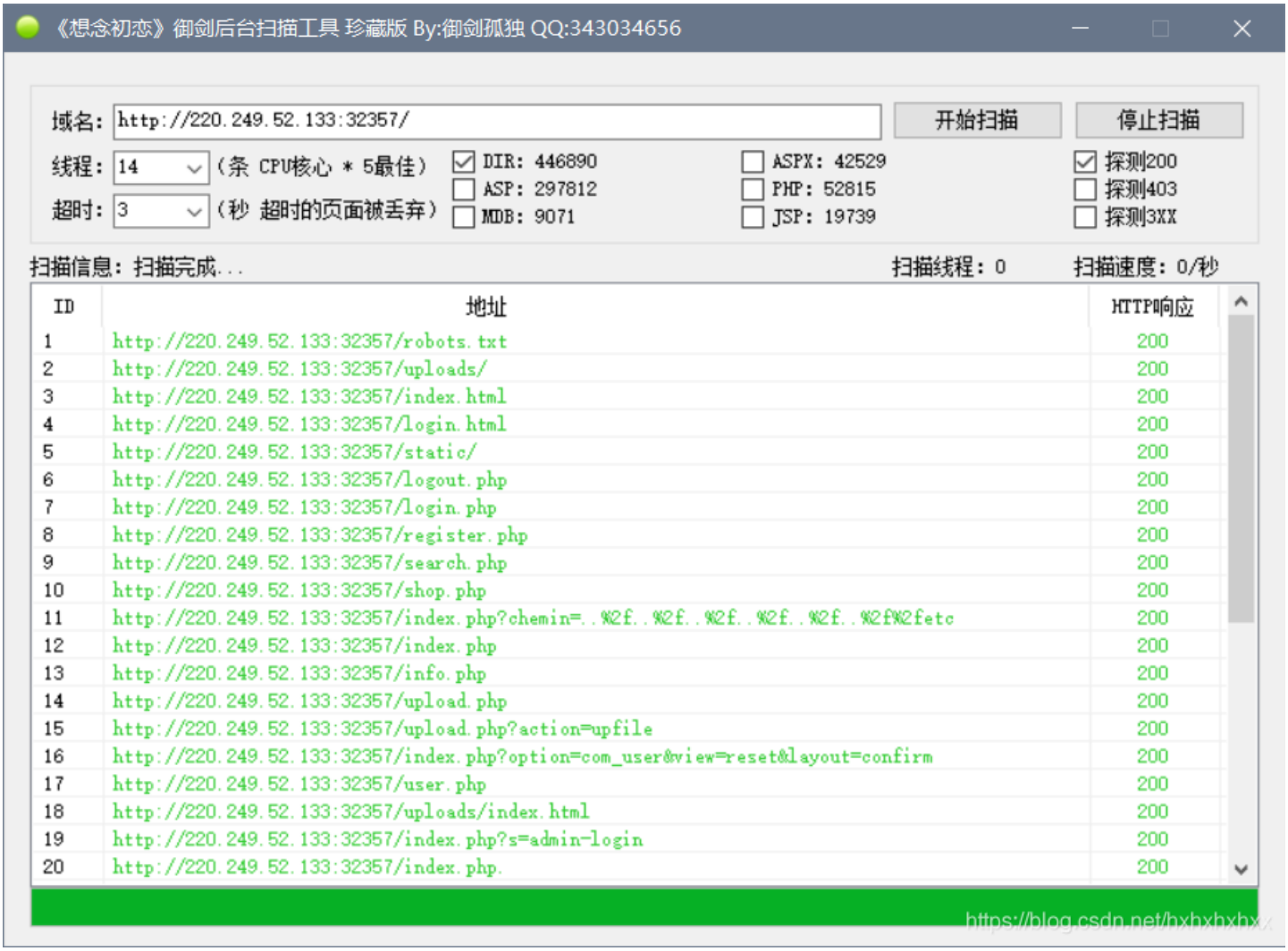
upload()
过滤了文件内容。

发现<"'. 文件内容都被替换成了!.

/file:|http|pre|etc/is也被过滤了。

search()
判断了是否存在path路径，对当前目录进行遍历，存在和path路径，对当前目录进行遍历，存在和name相同的文件或者目录替换为空 并列出当前目录。

但是我们可以上传.htaccess文件，但是平常遇到的文件内容都会触发过滤，所以得想想绕过文件内容检测。



御剑有了消息


```
CREATE DATABASE `sshop` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
USE `sshop`;
CREATE TABLE `sshop`.`users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NULL DEFAULT NULL,
  `mail` varchar(255) NULL DEFAULT NULL,
  `password` varchar(255) NULL DEFAULT NULL,
  `point` varchar(255) NULL DEFAULT NULL,
  `shopcar` varchar(255) NULL DEFAULT NULL,
  PRIMARY KEY (`id`)
) DEFAULT CHARSET=utf8 COLLATE=utf8_general_ci;
```


有一个sql.txt

sshop 商品列表 登录 注册

商品名称	商品价格	操作
a	3	加入购物车
b	3	加入购物车
c	3	加入购物车
d	3	加入购物车
e	3	加入购物车
f	3	加入购物车
g	3	加入购物车
h	3	加入购物车
i	3	加入购物车
j	3	加入购物车

第二天我们的环境终于正常了，我们先注册账号

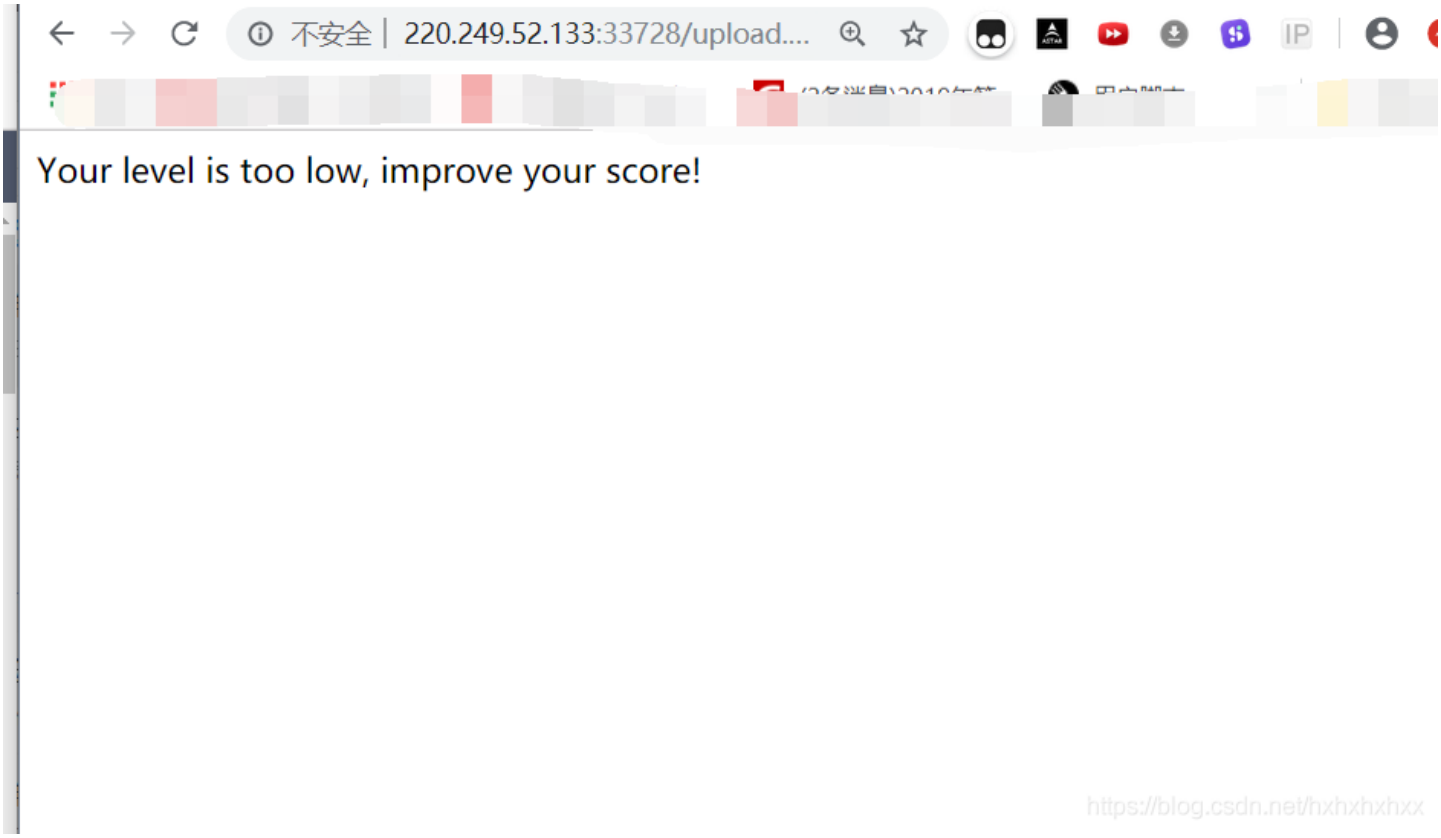
商品列表 个人中心 ！秒杀活动！ 购物车 修改密码 注销

上传一个头像?
搜索之前头像?

admin

邮箱地址：121007777@qq.com

剩余积分：0.0



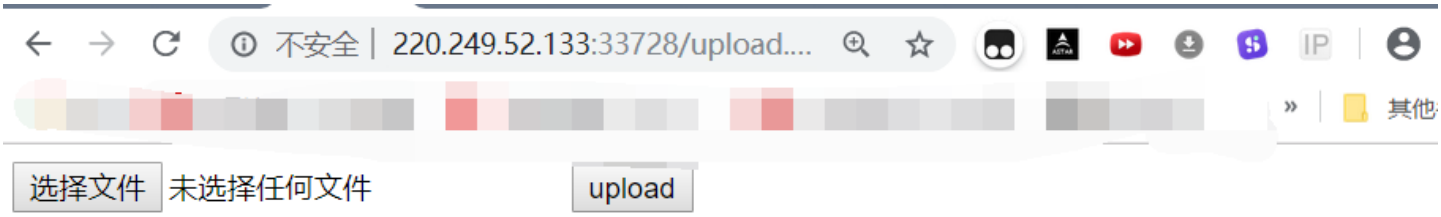
我们登录之后，发现，我们的等级，并不能够让我们上传，
我们当推荐人，多注册几个

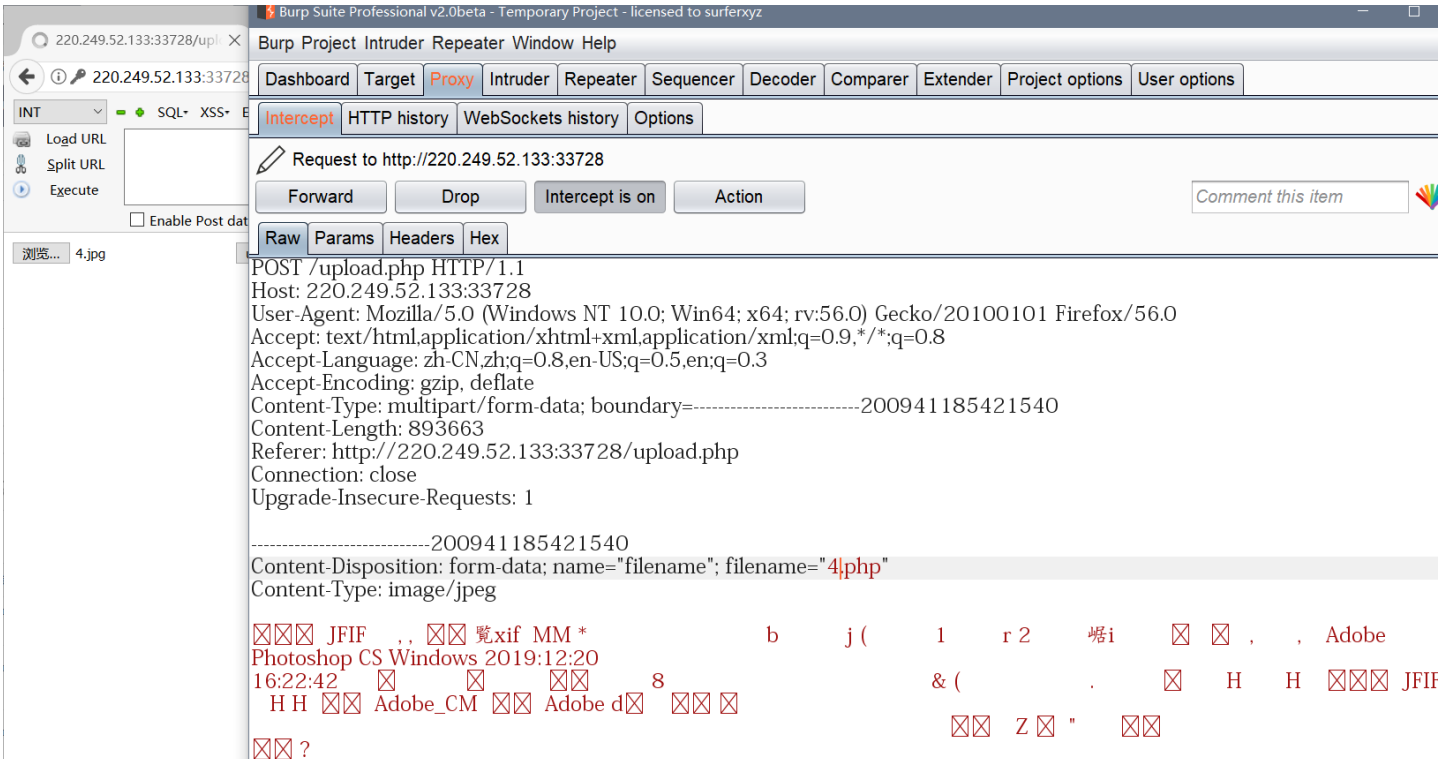
admin

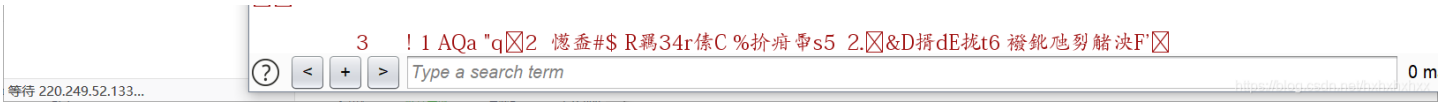
邮箱地址：121007777@qq.com

剩余积分：110.0

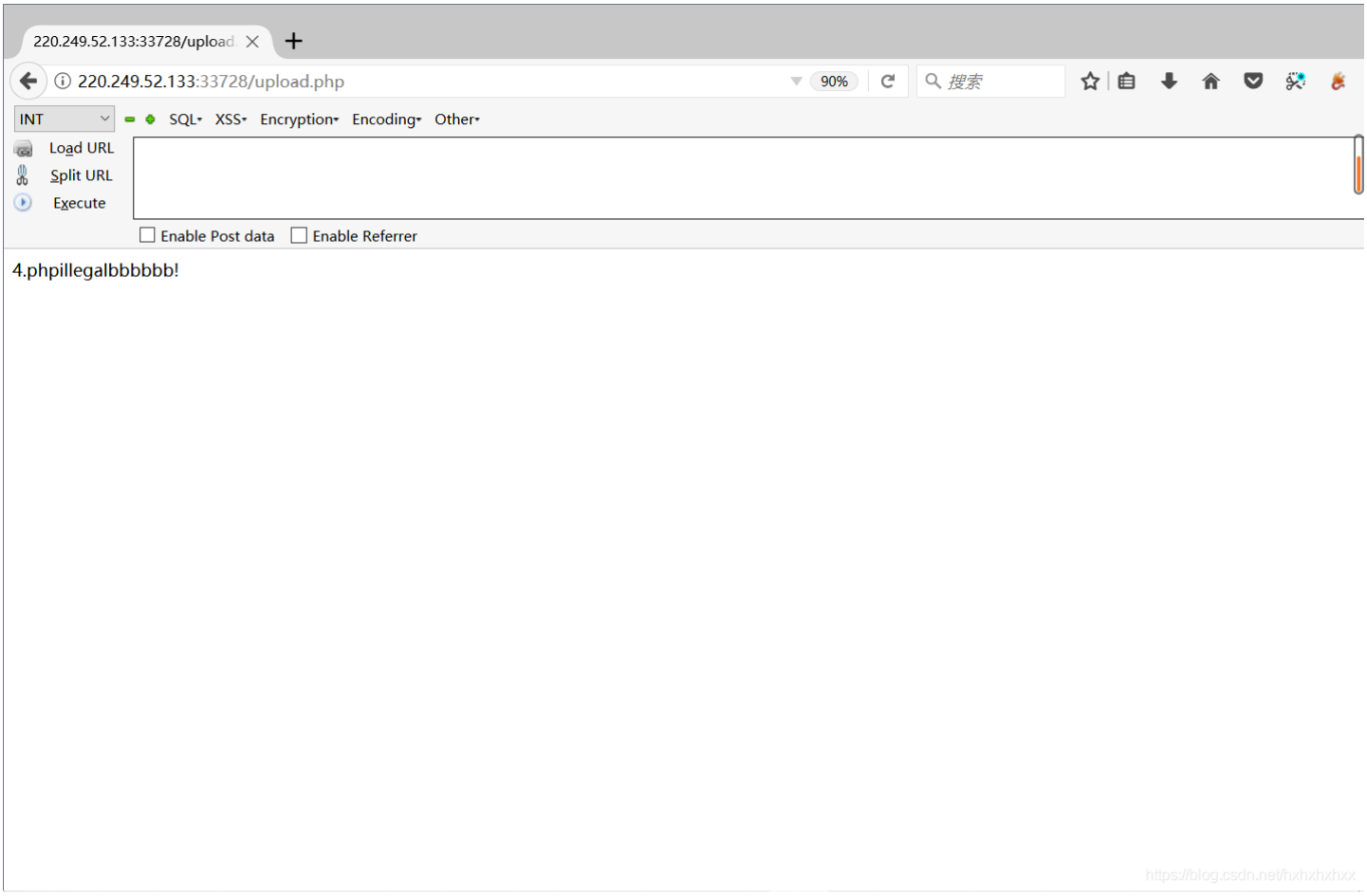
我们有了积分以后，可以上传了

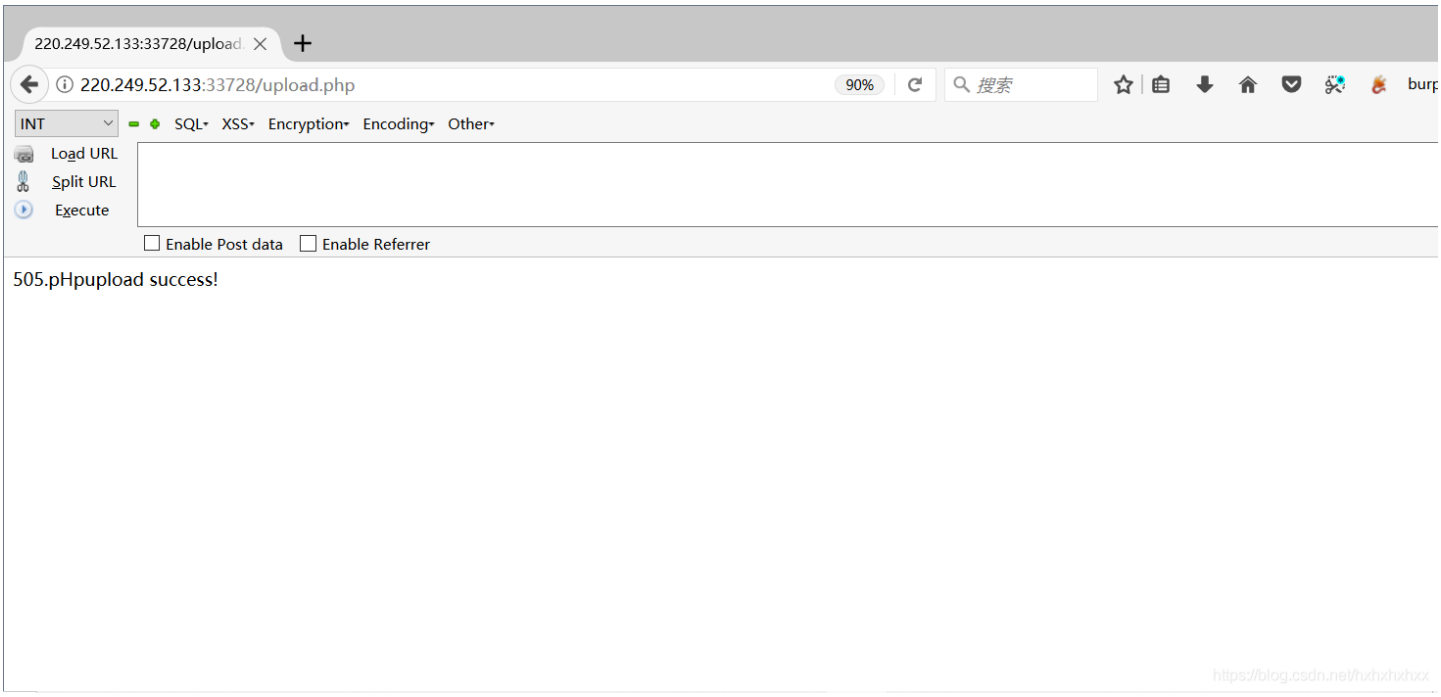






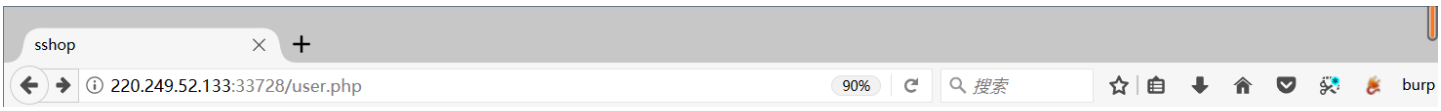
我们将图片上传并修改后缀，发现不行



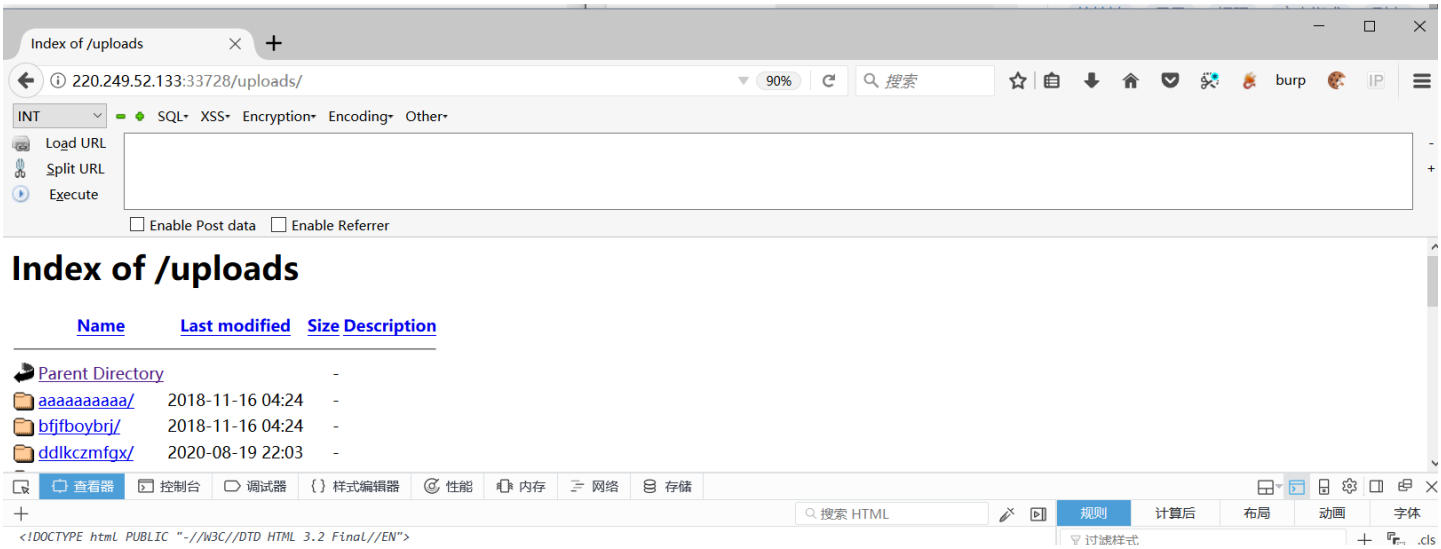


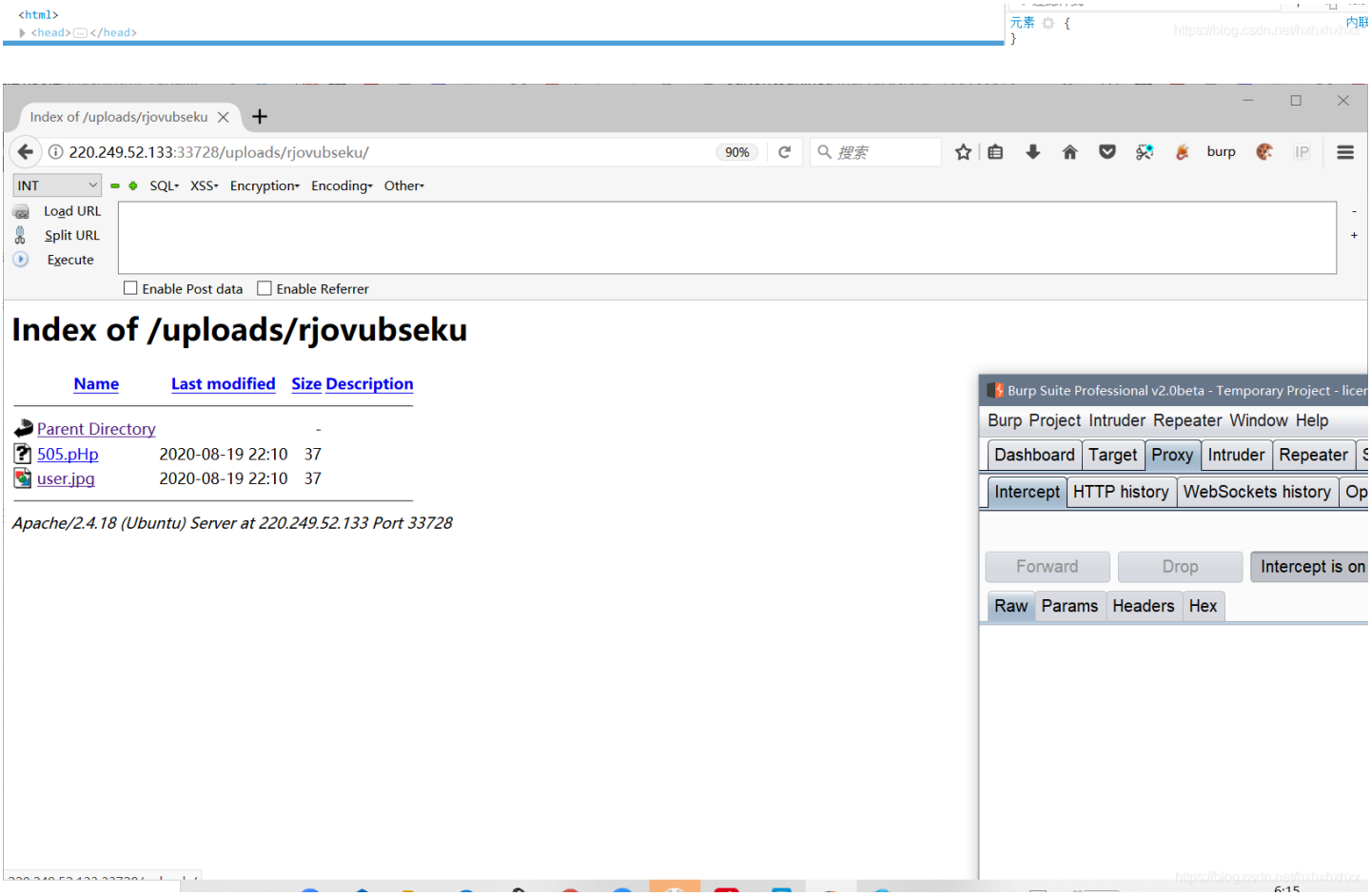
正常一句话是随便上传的！

大马不行= =



我们根据这个网页，虽然打不开，但是它可以进行目录遍历！





发现了我们的马

尖括号，单引号都被过滤了，

测了好久不能绕过了，

那么我们上我们的user.ini或者.htaccess

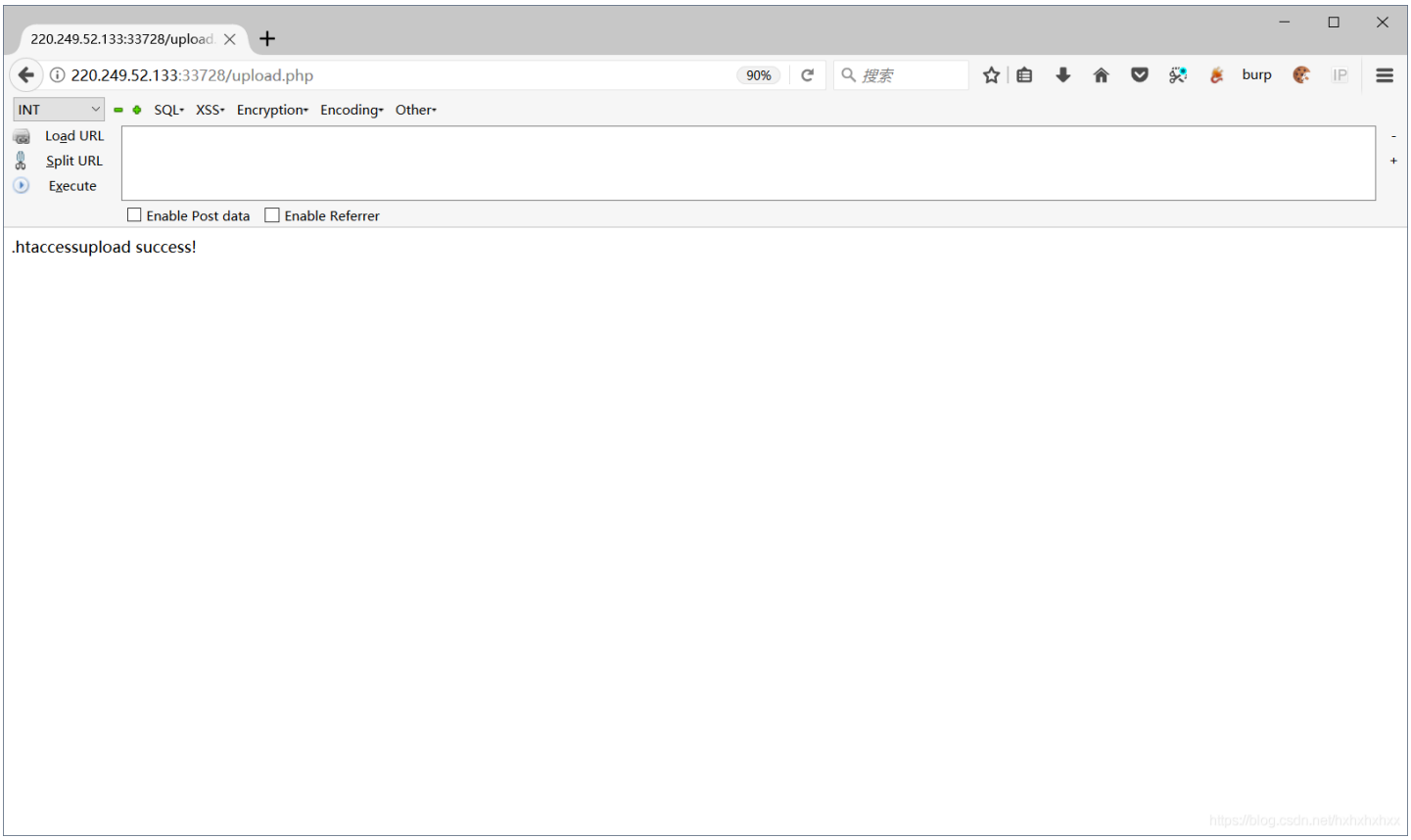
```
php_value auto_append_file master://search/path=%2fhome%2f&name=flag
```

我们可以使用这个方法，

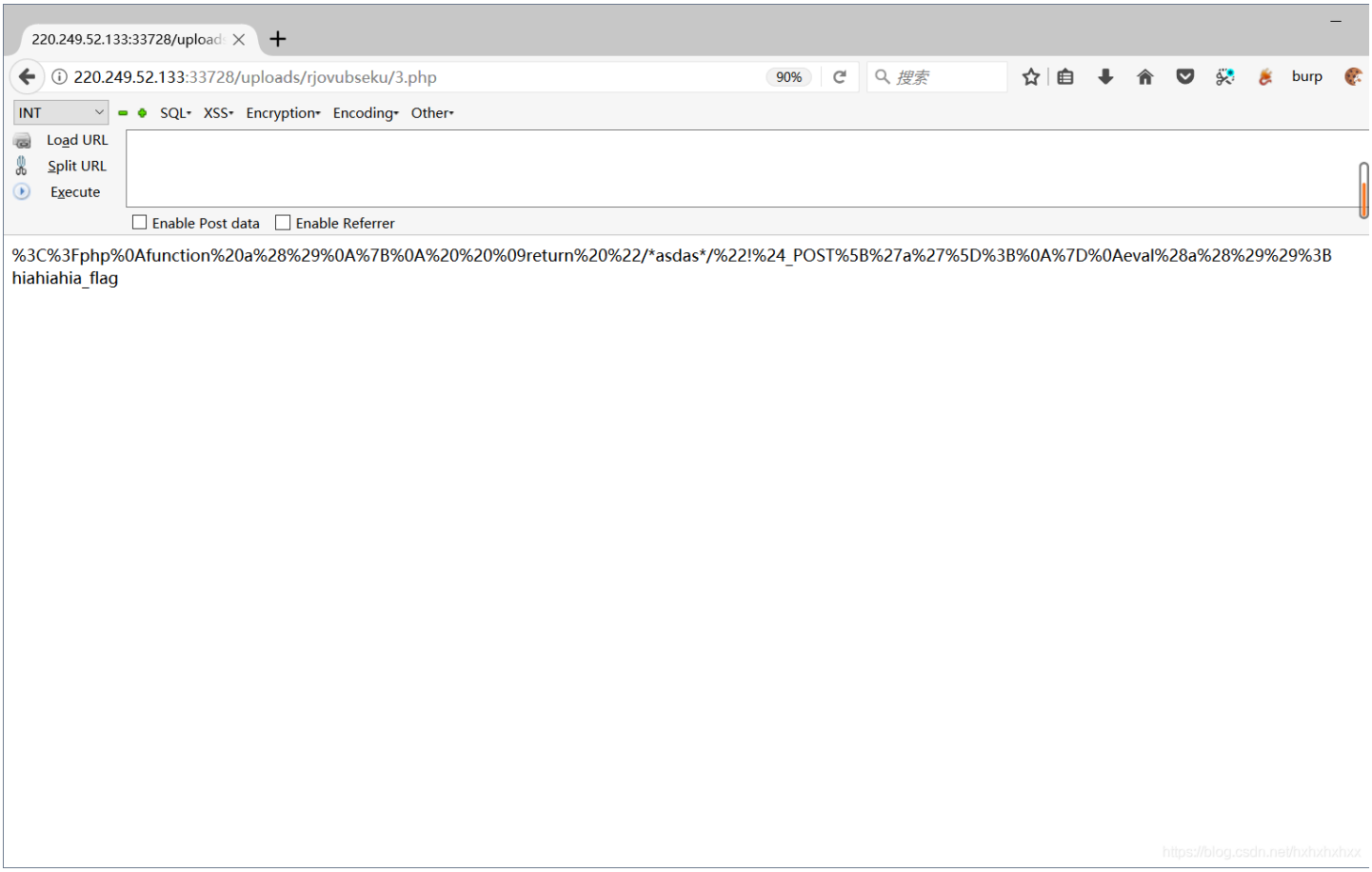
%2f 是 / 因为他里面有一次匹配规则，所以需要使用%2f绕过

这里的master search path name 都是在代码中他自己写的

这里只是调用它的功能



可以的，没有问题

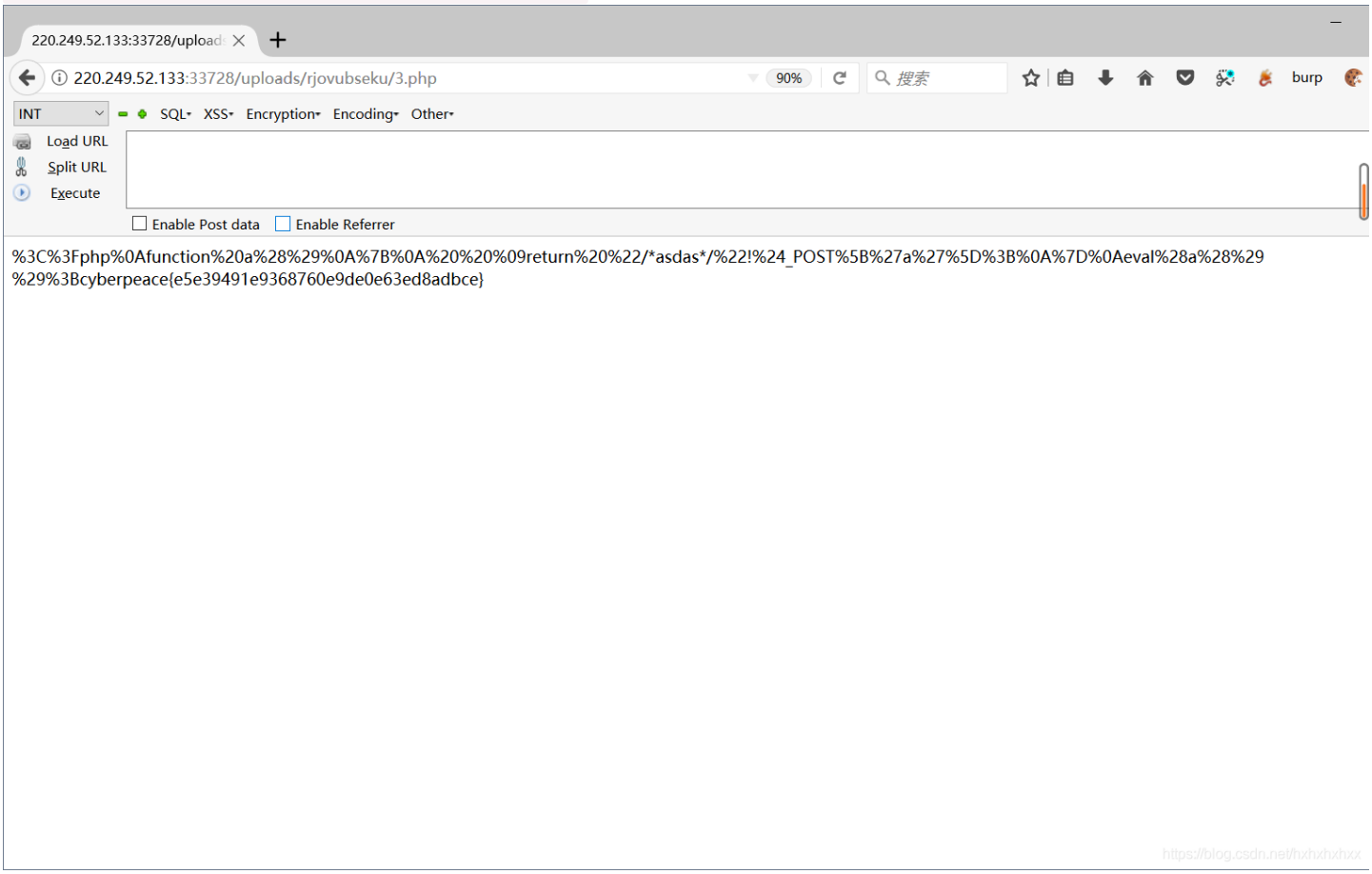


因为刚刚 505.pHp 影响了htaccess，我们这里重新上传一个 .php的正常结尾

发现文件，hiahiahia_flag

然后访问映射的文件发现存在再上传一个.htaccess，内容为

```
php_value auto_append_file /home/hiahiahia_flag
```



正则

```
if(!preg_match('/(.*)\/(.*)$/s',$path,$array,0,9))
        return 1;
```

\s是指空白，包括空格、换行、tab缩进等所有的空白
$是从后匹配字符串
/是为了匹配 /
() 是为了提取匹配的字符串。表达式中有几个()就有几个相应的匹配字符串。
. 表示 匹配除换行符 \n 之外的任何单字符，*表示零次或多次

所以.*在一起就表示任意字符出现零次或多次。没有?表示贪婪
模式。比如a.*b，它将会匹配最长的以a开始，以b结束的字符串。如果用它来搜索aabab的话，它会匹配整个字符串aabab。这被称为贪婪匹配。

php_value

见这里
https://www.dazhuanlan.com/2019/10/19/5daaf6b58f83b/