

# 攻防世界--filemanager

原创

Uzero 于 2022-01-05 18:03:45 发布 617 收藏

文章标签: [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/qq\\_46263951/article/details/122328643](https://blog.csdn.net/qq_46263951/article/details/122328643)

版权  
看到这里猜测是个文件上传漏洞, 测试几次发现好像只能上传图片, rename只能更改文件名, 但无法更改后缀。

## Control

[Delete file](#)

[Rename file](#)

## Content

选择文件 未选择任何文件

upload file

CSDN @Uzero.

随手扫了一下发现源码泄漏,

2KB - /www.tar.gz

审阅rename代码

```
<?php
/**
 * Created by PhpStorm.
 * User: phithon
 * Date: 15/10/14
 * Time: 下午9:39
 */

require_once "common.inc.php";

if (isset($req['oldname']) && isset($req['newname'])) {
    $result = $db->query("select * from `file` where `filename`='{ $req['oldname'] }'");
    if ($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`='{ $result['filename'] }' where
if (!$re) {
    print_r($db->error);
    exit;
}
$oldname = UPLOAD_DIR . $result["filename"] . $result["extension"];
$newname = 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>";
}
}
?>
<!DOCTYPE html>
<html>
<head>
    <title>file manage</title>
    <base href="/">
    <meta charset="utf-8" />
</head>
<h3>Rename</h3>
<body>
<form method="post">
    <p>
        <span>old filename(exclude extension): </span>
        <input type="text" name="oldname">
    </p>
    <p>
        <span>new filename(exclude extension): </span>
        <input type="text" name="newname">
    </p>
    <p>
        <input type="submit" value="rename">
    </p>
</form>
</body>
</html>

```

- `filename=$req[oldname]`是从数据库查询输入的oldname是否在于filename字段，然后进行update修改
- `oldname={$result[filename]}`将之前从数据库中查询出的filename更新到oldname当中，再次入库造成二次注入
- `extension`为后缀名
- 可以通过sql注入，影响其`extension`为空，再修改文件时加上.php后缀
- 绕过`file_exists()`只需要再次上传一个与数据库当中filename的值相同的文件名即可

具体操作：

先上传一个空文件，命名

```
' ,extension='.jpg
```

## Control

[Delete file](#)

[Rename file](#)

## Content

选择文件 ' ,extension='.jpg

upload file

CSDN @Uzero.

更改文件名为即将上传的木马文件名

## Rename

old filename(exclude extension):

new filename(exclude extension):

CSDN @Uzero.

此时使extension后缀名为空值

```
update `file` set `filename`='test.jpg', `oldname`='',extension='' where `fid`=${$result['fid']}
```

上传木马文件

## Control

[Delete file](#)

[Rename file](#)

## Content

test.jpg

CSDN @Uzero.

rename

## Rename

old filename(exclude extension):

new filename(exclude extension):

CSDN @Uzero.