

Loophole recurrence: if(isset(\$_FILES['uploadfile'])) { checktoken(); if(!isset(\$_SERVER["HTTP_REFERER"])) { die('error'); if(stripos(\$_GET['dir'],'..')===false) {}else {die('error file');} if(is_uploaded_file(\$_FILES['uploadfile']['tmp_name'])){ \$filaname=\$alldir.\$_FILES["uploadfile"]["name"]; if(@move_uploaded_file(\$_FILES['uploadfile']['tmp_name'],\$filaname)) { adminmsg(\$refererurl,'上传成功',0); }else { adminmsg(\$refererurl,'上传失败,无法写入文件,请确认目录权限',1); } exit(); ■ 后台管理中心 × + ← → C O 8 192.168.9.69/ucms/ucms/index.php?do=sadmin_file 器公 ta +> ≡ □ 火狐官方站点 🍅 新手上路 ■ 移动设备上的书签 站点设置 # 后台管理 > 文件管理 根目录 最近修改 返回 文件管理 /ucms/ 创建时间 修改时间 (h) 12.php 21 B 2022-07-04 11:36:18 2022-07-04 11:36:32 编辑 重命名 删除 e cache 2022-07-04 18:03:50 打开文件夹 重命名 2022-07-01 15:41:12 inc inc 2022-07-01 15:41:12 2022-07-01 16:32:37 打开文件夹 重命名 ndex.php 2021-05-20 00:00:00 编辑 重命名 删除 install 2022-07-01 15:41:12 打开文件夹 重命名 2022-07-01 15:41:12 phpinfo.php 2022-07-04 11:19:16 2022-07-04 11:21:11 编辑 重命名 删除 e template 2022-07-01 15:41:12 2022-07-01 15:41:12 打开文件夹 重命名 ucms 2022-07-01 15:41:12 2022-07-01 15:41:13 打开文件夹 重命名 uploadfile 2022-07-01 15:41:13 2022-07-04 18:01:14 打开文件夹 重命名 ⊕ •◆◆.htm 3.51 KB 编辑 重命名 删除

新建文件夹:

提交

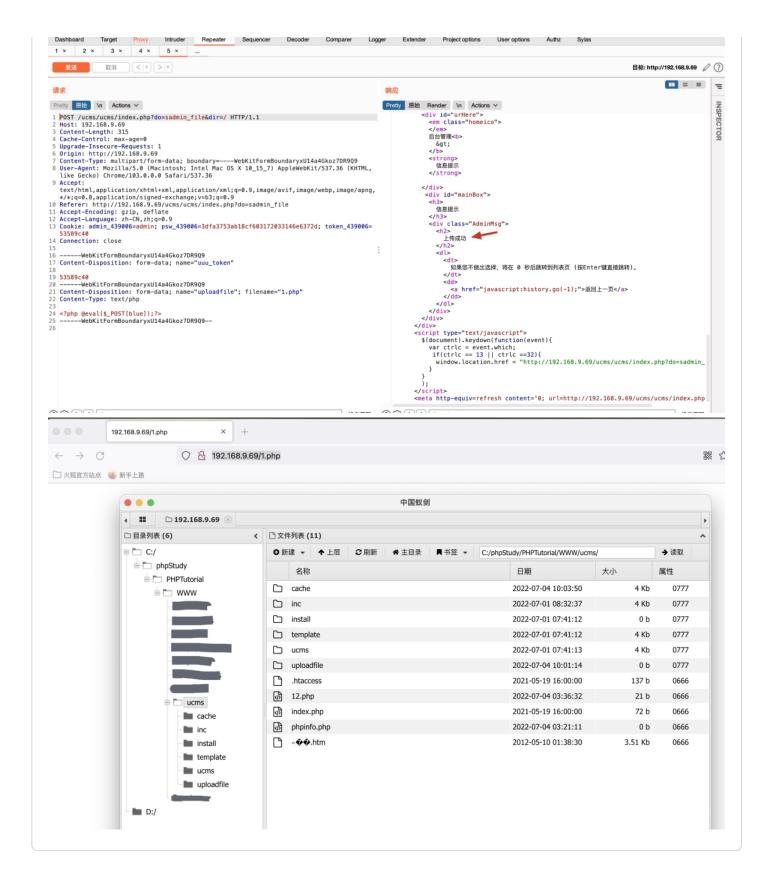
新建文件:

2022-07-01 15:41:12

提**交** 上传文件: 浏览... 1.php

2012-05-10 09:38:30

总数:10



Assignees

No one assigned

Labels

None yet

| None yet |
|---|
| Milestone No milestone |
| Development No branches or pull requests |

1 participant

