CTF学习记录 i春秋 《从0到1：CTFer成长之路》文件上传

原创

LovelyLucy 于 2021-10-21 11:05:57 发布 3349 收藏 1

文章标签： r语言 开发语言

本文链接：https://blog.csdn.net/mastergu2/article/details/120869454

21.10.19 第二次开始学习CTF 感觉很有收获 至少有让自己忙起来了的感觉 感觉有一些学习状态了 打算重新记录一下学习笔记！加油 我会坚持下去的！

题目代码

首先附上题目的代码段（不完整）

```
    show_source(__FILE__);
}else{
    $file = $_FILES['file'];

    if(!$file){
        exit("请勿上传空文件");
    }
    $name = $file['name'];

    $dir = 'upload/';
    $ext = strtolower(substr(strrchr($name, '.'), 1));
    $path = $dir.$name;

    function check_dir($dir){
        $handle = opendir($dir);
        while(($f = readdir($handle)) !== false){
            if(!in_array($f, array('.', '..'))){
                if(is_dir($dir.$f)){
                    check_dir($dir.$f.'/');
                 }else{
                    $ext = strtolower(substr(strrchr($f, '.'), 1));
                    if(!in_array($ext, array('jpg', 'gif', 'png'))){
                        unlink($dir.$f);
                    }
                }

            }
        }
    }

    if(!is_dir($dir)){
        mkdir($dir);
    }

    $temp_dir = $dir.md5(time(). rand(1000,9999));
    if(!is_dir($temp_dir)){
        mkdir($temp_dir);
    }
```

```
    if(in_array($ext, array('zip', 'jpg', 'gif', 'png'))){
        if($ext == 'zip'){
            $archive = new PclZip($file['tmp_name']);
            foreach($archive->listContent() as $value){
                $filename = $value["filename"];
                if(preg_match('/\.php$/', $filename)){
                     exit("压缩包内不允许含有php文件!");
                 }
            }
            if ($archive->extract(PCLZIP_OPT_PATH, $temp_dir, PCLZIP_OPT_REPLACE_NEWER) == 0) {
                check_dir($dir);
                   exit("解压失败");
            }

            check_dir($dir);
            exit('上传成功!');
        }else{
            move_uploaded_file($file['tmp_name'], $temp_dir.'/'.$file['name']);
            check_dir($dir);
            exit('上传成功!');
        }
    }else{
        exit('仅允许上传zip、jpg、gif、png文件!');
    }
}
```

前端如图所示：

时隔多年（1年），拿到文件上传的题目之后我其实是没有任何思路的。。。

在上网查阅了大神的wp之后大概了解了有一种思路：

上传一个一句话木马（此处为php），然后连接中国菜刀（我使用的是antsword），获得文件目录，从而得到flag。

其实这并不是这个题目的正确解法，不过还没试，谁知道呢。

于是尝试上传php文件，结果提示

> 仅允许上传zip、jpg、gif、png文件

想想也是，不会有什么服务器允许你直接上传php文件的，那么我们自然要绕过这个限制。

网上有一种思路就是00截断：

00作为结束符，如%00 0x00 都是作为结束符，在php5.3.4（不确定）版本之前，某些函数读取到以上00的时候会认为字符串已经结束，不会再读取后面的内容，此时就绕过了检查函数。

但是在这里上传之后会被删掉，我认为应该是那个检查函数没有这个漏洞，也有可能检查函数是从后往前检查，总之对它应该是不起作用

所以直接留下xxx.php文件这个方法不靠谱

pass！

然后我就不会了，经过大神wp可知，在这里的dir_check 只遍历检查了upload目录，所以如果说，文件不在这个目录就好了

这里其实有两种上传 一种是非zip 如jpg、png这种，另一种是zip 。

我一开始直接试的jpg 确实是可以用00截断上传 .php文件，但是因为md5的目录穿越好像总是有点问题，这里考虑原因可能是函数move_uploaded_file的问题，具体的原因因为我没有docker的关系没有试出来，总之上传一个…/…/shell.jpg0x00.php的文件是不行的。

也没办法 就只能用zip来上传了 其实这个不好分析 因为zip的文件结构有三个 一个是数据内容 一个是目录 一个是目录结束 archive->extract这个解压函数似乎获取的内容是目录的内容。所以这里是通过010editor编辑的 只要修改目录的文件名就好了。而那个遍历读取压缩文件名的函数似乎读取的是文件内容，所以这里随便弄一下就好具体可以参考一下这篇文章 我觉得说得比较详细

> https://blog.csdn.net/zy15667076526/article/details/114139749

虽然有很多不是特别清楚的地方。。。但是 就酱!