2018.3 强网杯 部分writeup

转载

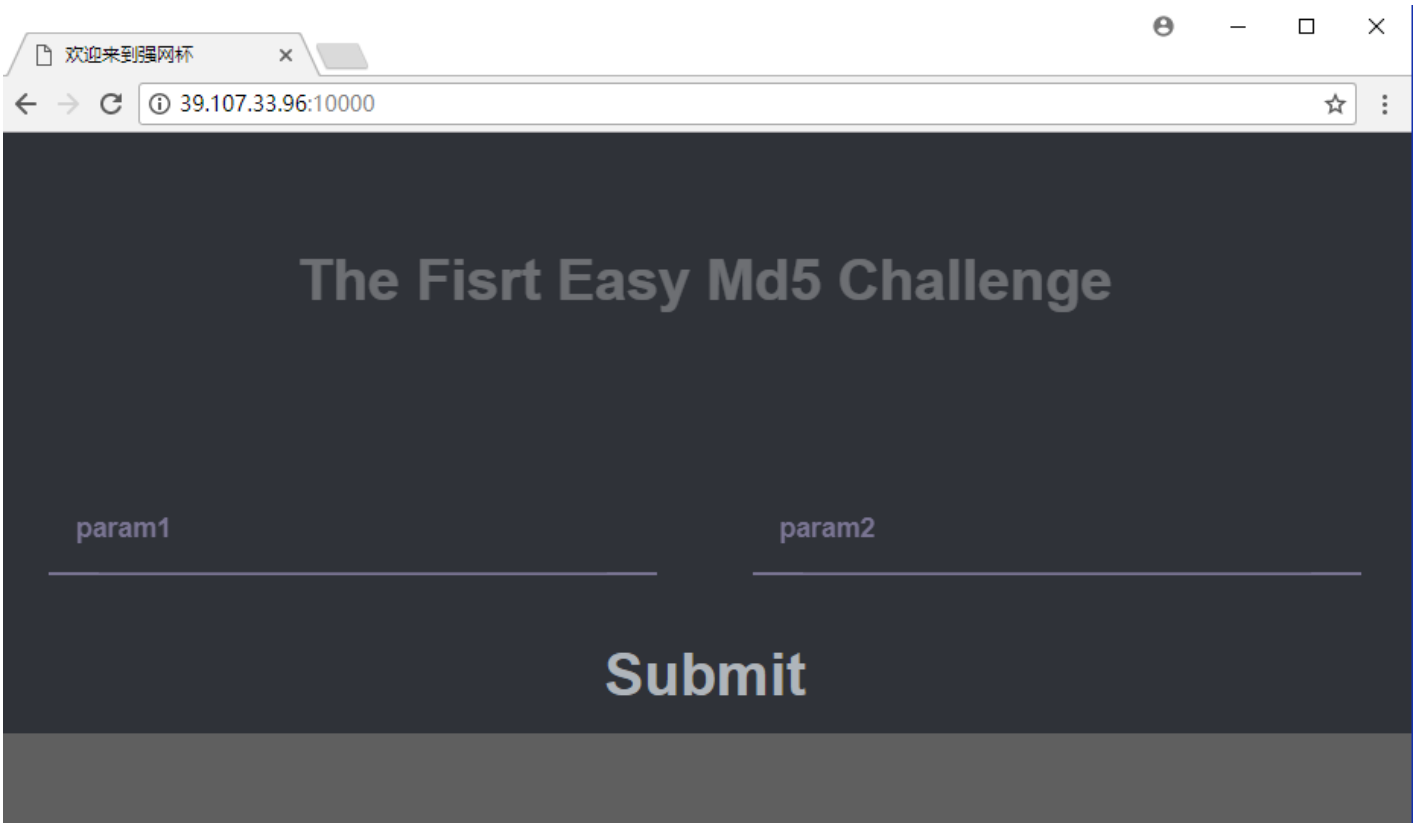
weixin_30765475 于 2018-03-28 10:32:00 发布 69 收藏
文章标签： php
原文链接：http://www.cnblogs.com/P201521410043/p/8662354.html

第一次跟大佬打ctf 啥都不会 腆着脸抄了一个writeup

web签到题

原题链接：http://39.107.33.96:10000/

emmmm……



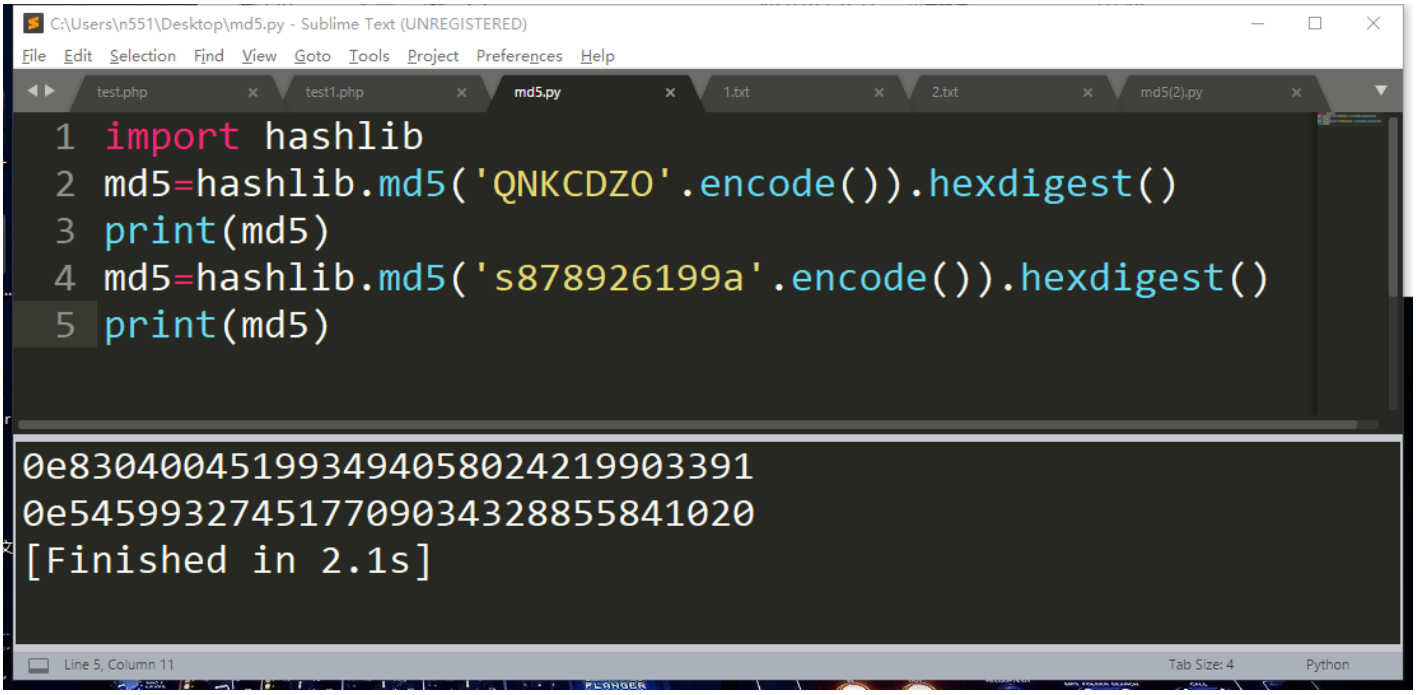
拿到此题，第一反应是MD5碰撞（生日攻击？）

查看网页源码

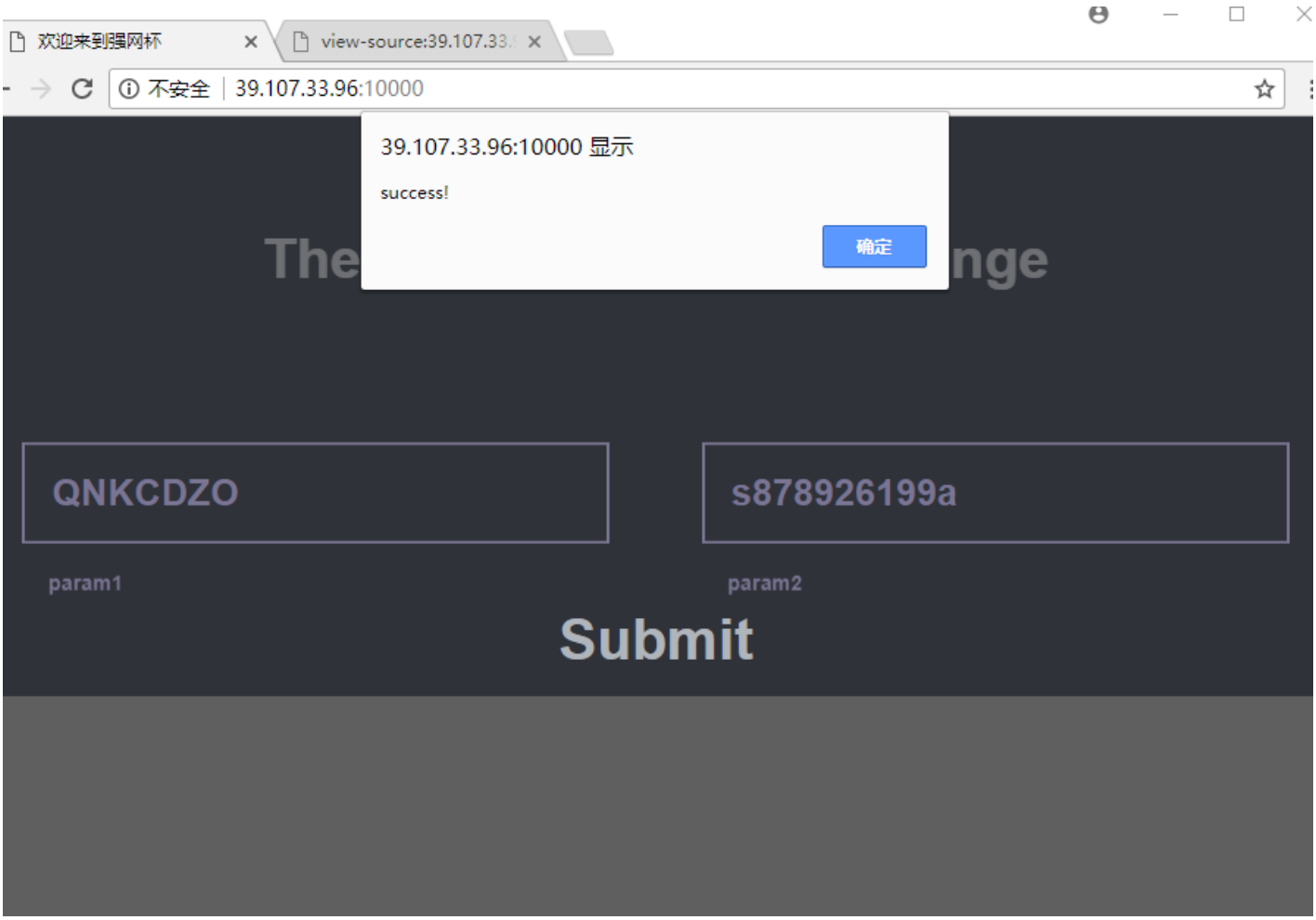
```
<!DOCTYPE html>
<html lang="zh" class="no-js">
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>欢迎来到强网杯</title>
        <link rel="stylesheet" type="text/css" href="css/normalize.css" />
        <link rel="stylesheet" type="text/css" href="fonts/font-awesome-4.2.0/css/font-awesome.min.css" />
        <link rel="stylesheet" type="text/css" href="css/demo.css" />
        <link rel="stylesheet" type="text/css" href="css/component.css" />
        <script src="js/jquery.min.js"></script>
    </head>
    <body>
        <div class="container">
                    <section class="content bgcolor-4">
                <h2>The Fisrt Easy Md5 Challenge</h2>
                <!--
                    if($_POST['param1']!=$_POST['param2'] && md5($_POST['param1'])==md5($_POST['param2'])){
                        die("success!");
                    }
                -->
                <span class="input input--madoka">
                    <input class="input__field input__field--madoka" type="text" id="input-31" name='param1'/>
                    <label class="input__label input__label--madoka" for="input-31">
                        <svg class="graphic graphic--madoka" width="100%" height="100%" viewBox="0 0 404 77"
preserveAspectRatio="none">
                            <path d="m0,0l404,0l0,77l-404,0l0,-77z"/>
                        </svg>
                        <span class="input__label-content input__label-content--madoka">param1</span>
                    </label>
                </span>
                <span class="input input--madoka">
                    <input class="input__field input__field--madoka" type="text" id="input-32" name='param2'/>
                    <label class="input__label input__label--madoka" for="input-32">
                        <svg class="graphic graphic--madoka" width="100%" height="100%" viewBox="0 0 404 77"
preserveAspectRatio="none">
```

这里面要求POST上去的参数 param1 != param2 && md5(‘param1’) == md5(‘param2’)

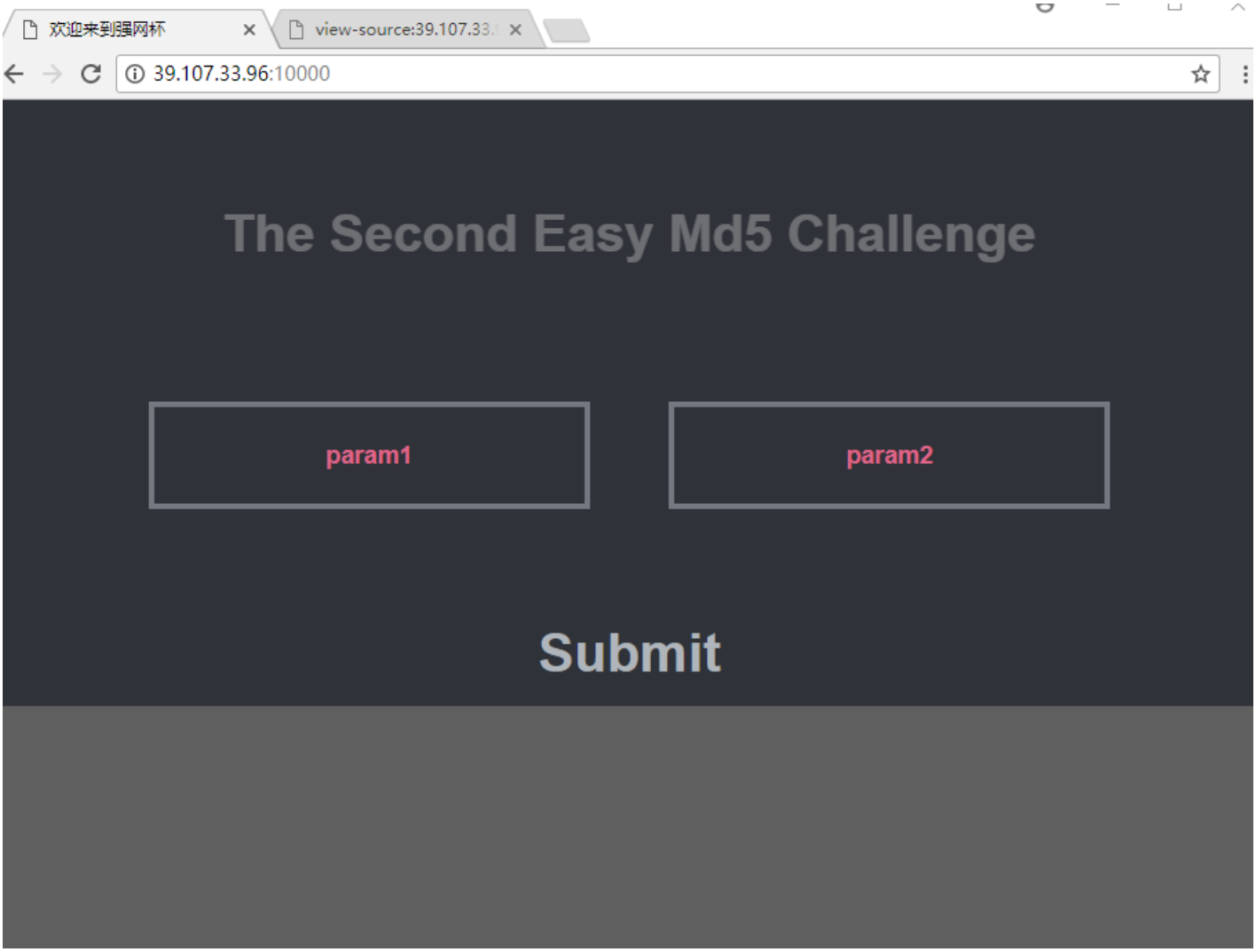
这道题运用了php的一个哈希比较缺陷，就是php在处理0e开头md5哈希字符串时，会将他看成 0 ，PHP在处理哈希字符串时，会利用"!="或"=="来对哈希值进行比较，它把每一个以"0E"开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以"0E"开头的，那么PHP将会认为他们相同，都是0。



提交上去


欢迎来到强网杯
view-source:39.107.33.
不安全 | 39.107.33.96:10000
39.107.33.96:10000 显示
success!
确定
QNKCDZO
s878926199a
param1
param2
Submit

然后到了第二个页面



看一下源码

```
        <script src="js/jquery.min.js"></script>
    </head>
    <body>
        <div class="container">
                    <section class="content bgcolor-4">
                <h2>The Second Easy Md5 Challenge</h2>
                <!--
                    if($_POST['param1']!==$_POST['param2'] && md5($_POST['param1'])===md5($_POST['param2'])){
                            die("success!");
                        }
                -->
                <span class="input input--kuro">
                    <input class="input__field input__field--kuro" type="text" id="input-7"  name="param1"/>
                    <label class="input__label input__label--kuro" for="input-7">
                        <span class="input__label-content input__label-content--kuro">param1</span>
                    </label>
                </span>
```

$a == $b	Equal	**TRUE** if *$a* is equal to *$b* after type juggling.
$a === $b	Identical	**TRUE** if *$a* is equal to *$b*, and they are of the same type.
$a != $b	Not equal	**TRUE** if *$a* is not equal to *$b* after type juggling.
$a <> $b	Not equal	**TRUE** if *$a* is not equal to *$b* after type juggling.
$a !== $b	Not identical	**TRUE** if *$a* is not equal to *$b*, or they are not of the same type.
$a < $b	Less than	**TRUE** if *$a* is strictly less than *$b*.
$a > $b	Greater than	**TRUE** if *$a* is strictly greater than *$b*.
$a <= $b	Less than or equal to	**TRUE** if *$a* is less than or equal to *$b*.
$a >= $b	Greater than or equal to	**TRUE** if *$a* is greater than or equal to *$b*.

共3张图,当前是第2张

定义和用法

md5() 函数计算字符串的 MD5 散列。

md5() 函数使用 RSA 数据安全，包括 MD5 报文摘要算法。

来自 RFC 1321 的解释 - MD5 报文摘要算法：*MD5 报文摘要算法将任意长度的信息作为输入值，并将其换算成一个 128 位长度的"指纹信息"或"报文摘要"值来代表这个输入值，并以换算后的值作为结果。MD5 算法主要是为数字签名应用程序而设计的；在这个数字签名应用程序中，较大的文件将在加密（这里的加密过程是通过在一个密码系统下[如：RSA]的公开密钥下设置私有密钥而完成的）之前以一种安全的方式进行压缩。*

如需计算文件的 MD5 散列，请使用 md5_file() 函数。

语法

```
md5(string,raw)
```

参数	描述
string	必需。规定要计算的字符串。
raw	可选。规定十六进制或二进制输出格式： • TRUE - 原始 16 字符二进制格式 • FALSE - 默认。32 字符十六进制数

此时比较符已经变成了 === 这样的类型

php中，MD5函数所传入的参数必须是字符串类型，那么假设我们传入的不是一个字符串呢？

我们构造一个数组试试

```php
<?php
$a=array("a");
$b=array();
var_dump(md5($a)==md5($b));
var_dump($a==$b);
if ($a!==$b&& md5($a)===md5($b))
 {
    die("success!");# code...
    }
?>
```

Warning: md5() expects parameter 1 to be string, array given in **E:\AppServ\www\test1.php** on line **4**

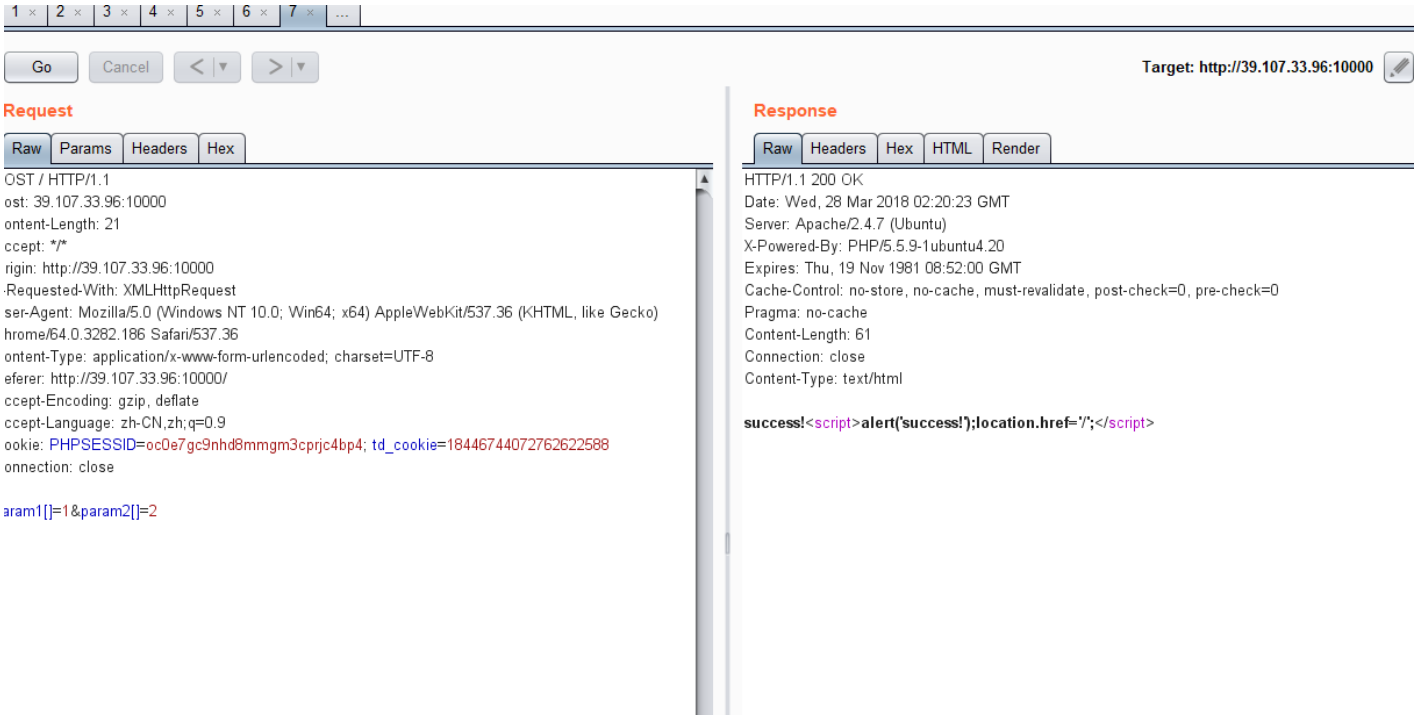
Warning: md5() expects parameter 1 to be string, array given in **E:\AppServ\www\test1.php** on line **4**
bool(true) bool(false)
Warning: md5() expects parameter 1 to be string, array given in **E:\AppServ\www\test1.php** on line **6**

Warning: md5() expects parameter 1 to be string, array given in **E:\AppServ\www\test1.php** on line **6**
success!

可以看出 发现报错了

这里边我们构造了一个数组，传入到md5()这个函数里边，报错提示md5()第一个参数必须为str类型。虽然说if条件不符合，但是程序依然会继续运行。

抓包试一下，把参数改为数组


1 × 2 × 3 × 4 × 5 × 6 × 7 × ...
Go
Cancel
Target: http://39.107.33.96:10000
Request
Raw Params Headers Hex
OST / HTTP/1.1
ost: 39.107.33.96:10000
ontent-Length: 21
ccept: */*
rigin: http://39.107.33.96:10000
·Requested-With: XMLHttpRequest
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
hrome/64.0.3282.186 Safari/537.36
ontent-Type: application/x-www-form-urlencoded; charset=UTF-8
eferer: http://39.107.33.96:10000/
ccept-Encoding: gzip, deflate
ccept-Language: zh-CN,zh;q=0.9
ookie: PHPSESSID=oc0e7gc9nhd8mmgm3cprjc4bp4; td_cookie=18446744072762622588
onnection: close
aram1[]=1&param2[]=2
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Wed, 28 Mar 2018 02:20:23 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.20
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 61
Connection: close
Content-Type: text/html
success!<script>alert('success!');location.href='/';</script>

还没拿到flag。。。。

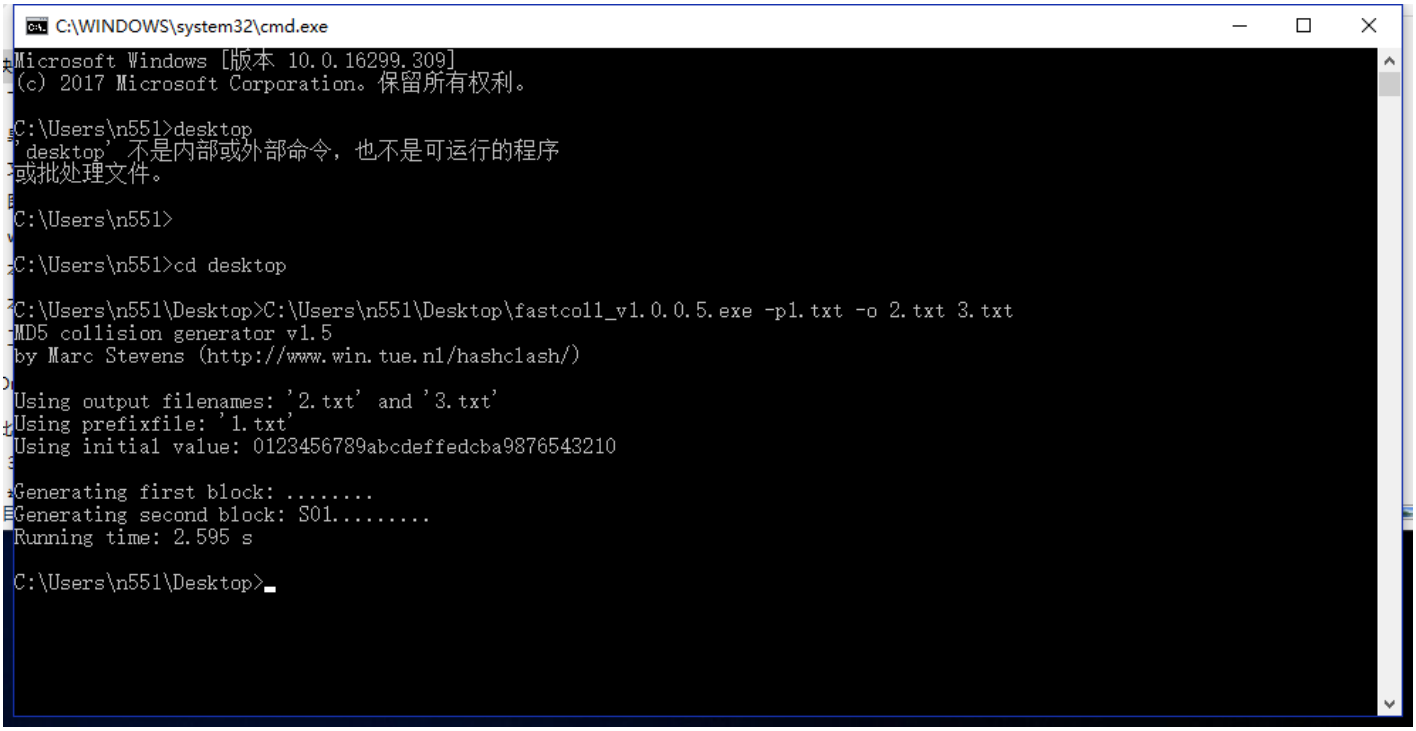

Md5 Revenge Now!
param1
param2
Submit

```
<h2>Md5 Revenge Now!</h2>
<!--
if((string)$_POST['param1']!==(string)$_POST['param2'] && md5($_POST['param1'])===md5($_POST['param2'])){
    die("success!");
}
-->
```

它事先定义了string类型了，之前的方法无法绕过去了。

我们用到了fastcoll_v1.0.0.5 这个软件，用来生成两个有着相同MD5值的文件。

先在桌面上建立一个空的文本文件，取名1.txt



生成两个文件后，比较它们的md5值

发现一模一样

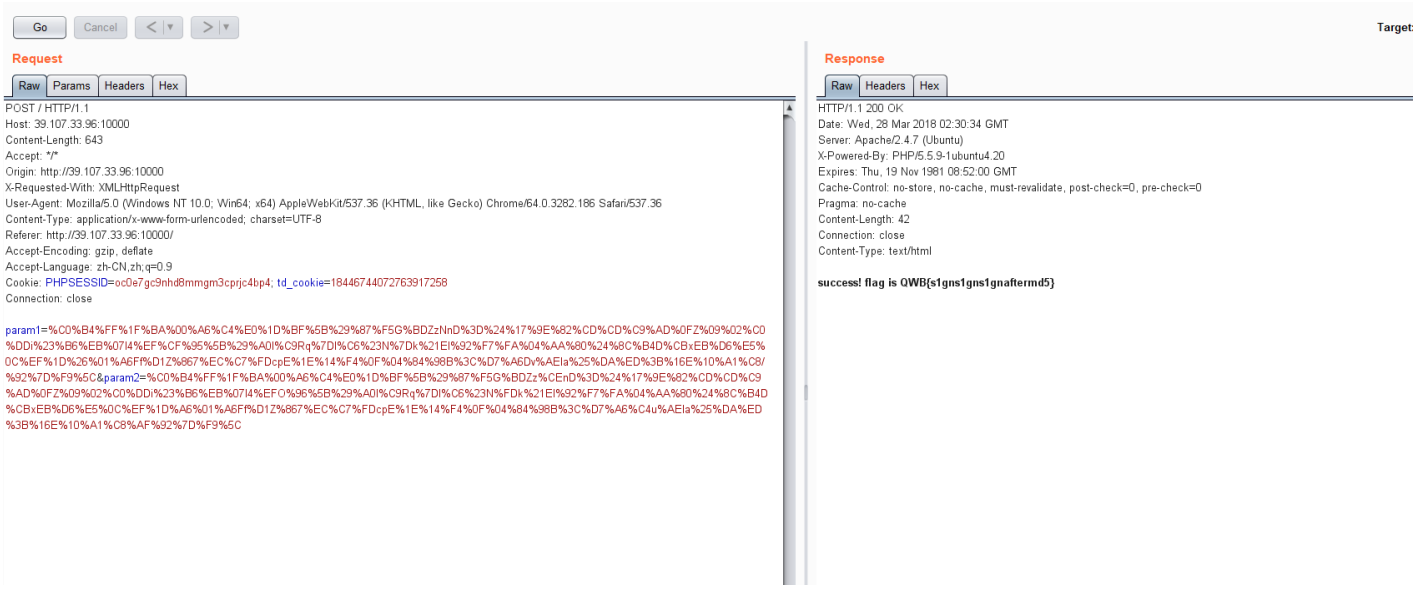
那我们怎么将文件传上去呢？ 这里将文件转为url编码

```python
import hashlib
import urllib.parse

print(urllib.parse.quote(open('2.txt','rb').read()))
print(urllib.parse.quote(open('3.txt','rb').read()))
```

```
%C0%B4%FF%1F%BA%00%A6%C4%E0%1D%BF%5B%29%87%F5G%BDZzNnD%3D%24%17%9E%82%CD%CD%C9%AD%0FZ%09%02%C0%DDi%23%B6%EB%0714%EF%CF%95%5B%29%A0I%C9Rq%7Dl%C6%23N%7Dk%21EI%92%F7%FA%04%AA%80%24%8C%B4D%CBxEB%D6%E5%0C%EF%1D%26%01%A6Ff%D1Z%867%EC%C7%FDcpE%1E%14%F4%0F%04%84%98B%3C%D7%A6Dv%AEIa%25%DA%ED%3B%16E%10%A1%C8/%92%7D%F9%5C
%C0%B4%FF%1F%BA%00%A6%C4%E0%1D%BF%5B%29%87%F5G%BDZz%CEnD%3D%24%17%9E%82%CD%CD%C9%AD%0FZ%09%02%C0%DDi%23%B6%EB%0714%EFO%96%5B%29%A0I%C9Rq%7Dl%C6%23N%FDk%21EI%92%F7%FA%04%AA%80%24%8C%B4D%CBxEB%D6%E5%0C%EF%1D%A6%01%A6Ff%D1Z%867%EC%C7%FDcpE%1E%14%F4%0F%04%84%98B%3C%D7%A6%C4u%AEIa%25%DA%ED%3B%16E%10%A1%C8%AF%92%7D%F9%5C
[Finished in 0.5s]
```

再用burpsuite抓一下包，修改一下参数



flag is QWB{s1gns1gns1gnaftermd5}

转载于:https://www.cnblogs.com/P201521410043/p/8662354.html