




# Bugku CTF flag.php WriteUp

原创

[evoA](#)  于 2018-03-18 14:24:48 发布  8403  收藏 1

文章标签: [CTF 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\\_40860784/article/details/79600372](https://blog.csdn.net/qq_40860784/article/details/79600372)

版权

#Bugku CTF flag.php WriteUp

原题链接 [flag.php](#)

进去后第一反应是SQL注入得到flag, 但是发现输入任何特殊字符点击Login都没有反应, 查看源代码未发现异样。回到Bugku CTF界面, 发现给了一个hint

提示给了一个hint, 用户名密码输入hint没有反应, 突然想到Get传参, 传入参数  
**120.24.86.145:8002/flagphp/?hint=1**

---

突然发现显示了源代码

```

<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
    <form method="POST" action="#">
        <p><input name="user" type="text" placeholder="Username"></p>
        <p><input name="password" type="password" placeholder="Password"></p>
        <p><input value="Login" type="button"/></p>
    </form>
</div>
</body>
</html>

<?php
}
$KEY='ISecer:www.isecer.com';
?>

```

代码逻辑是传入的cookie参数的值反序列化后等于KEY就输出Flag，一开始我以为\$KEY的值是最下面的ISecer:www.isecer.com，结果忙活了半天发现这里其实上面\$KEY的值还没有被定义，上面代码中\$KEY的值应该是NULL，而不是下面的值，所以应该是反序列化的值为NULL。

输出FLAG，但是我把代码复制下来在自己电脑里输出serialize(\$KEY)的值为 s:0:"";

于是构造cookie :ISser = s:0:"";

但是注意;(分号)在cookie中不会被正确的上传到服务器，构造URL编码

;的URL编码为%3B

于是在火狐的HackBar插件中传入Cookie ISser = s:0:""%3B

得到Flag

欢迎关注我的博客<http://evoa.me>