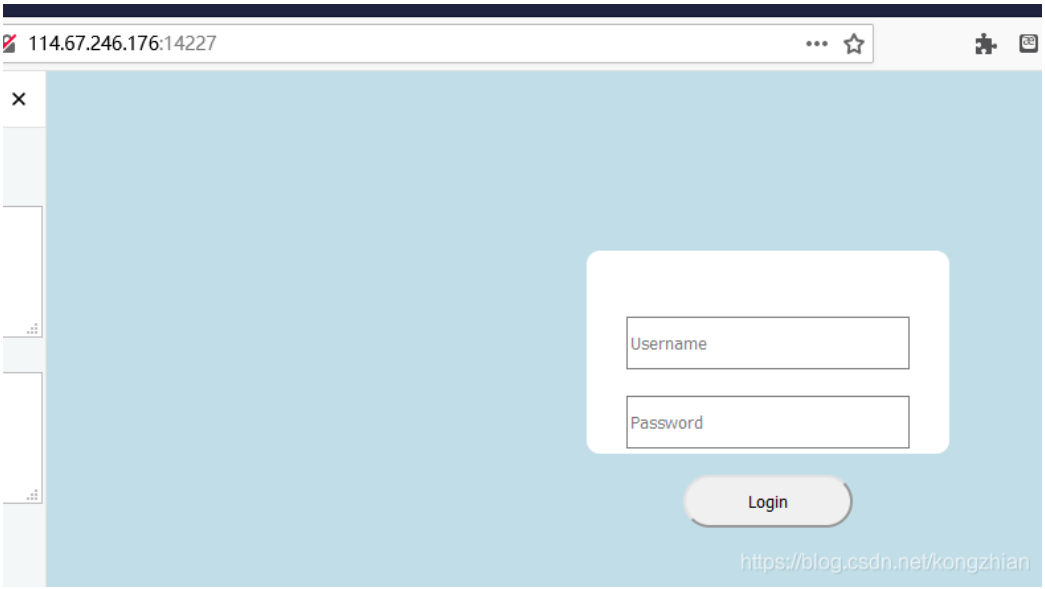
【bugku_writeup】web35 点了login咋没反应

原创

kzaaa 于 2021-01-06 16:43:42 发布 655 收藏
分类专栏： ctf_bugku_writeup

本文链接：https://blog.csdn.net/kongzhian/article/details/112279612



随便输入一个账号密码，点击login没有反应

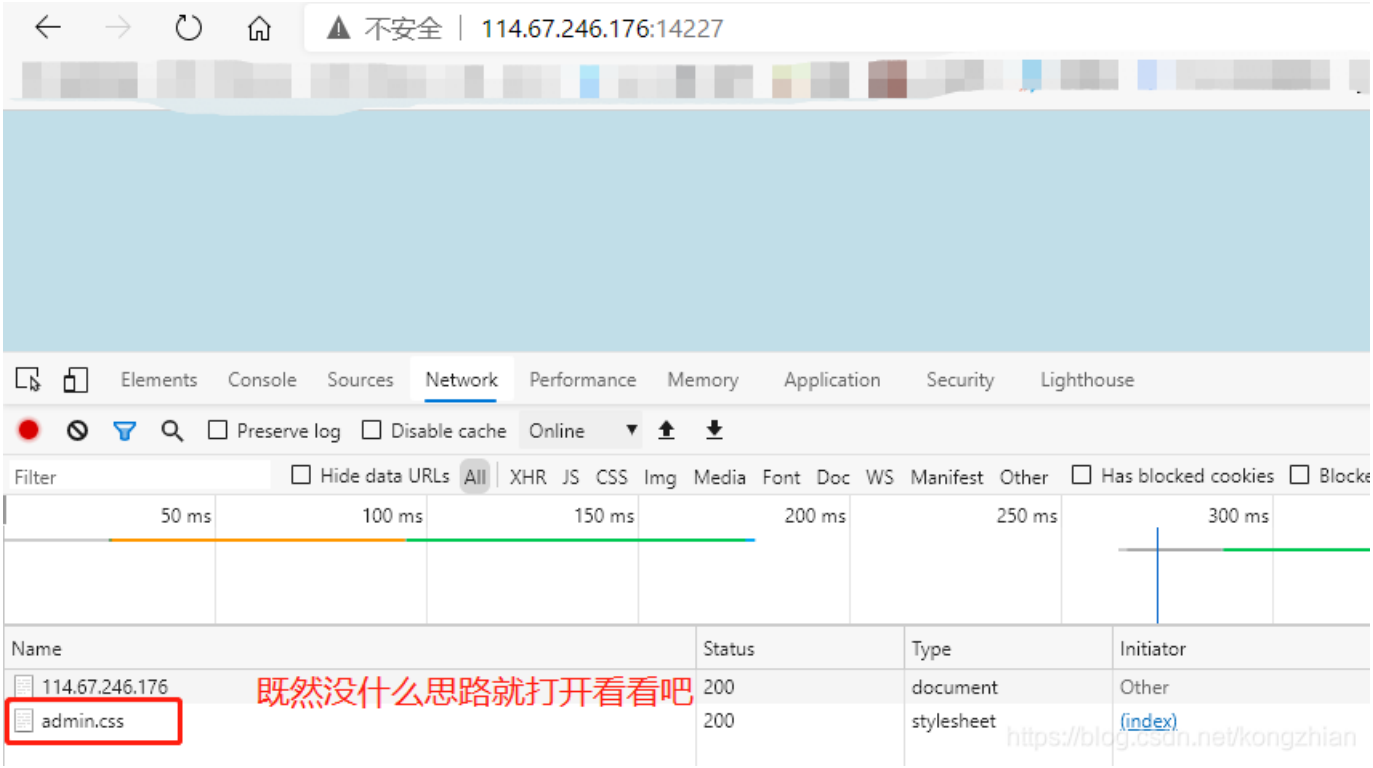
当时想一下，是不是后台设置了button不能点击，所以post提交不了，所以想构造一个post？还是想太多了，并没有什么作用，而且这是不切实际的

没有思路

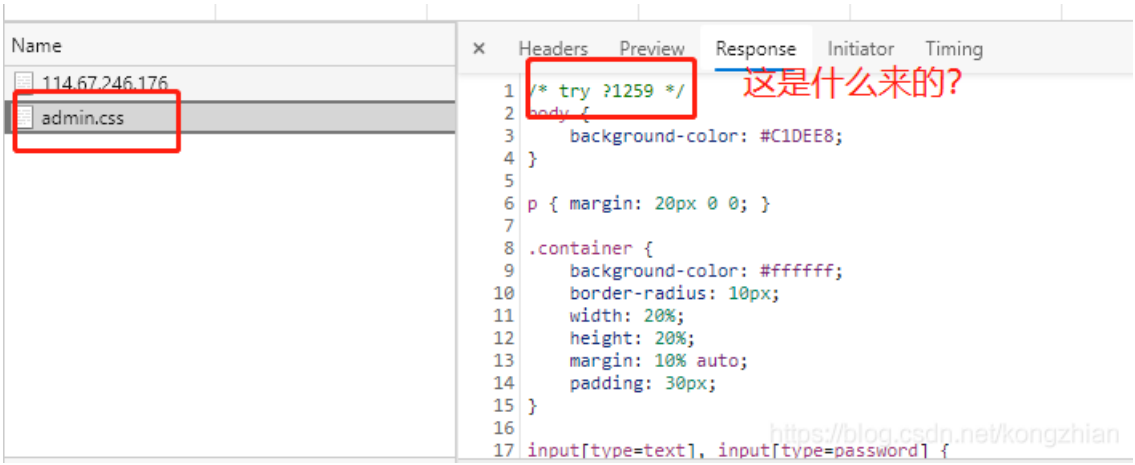
。。。

。。。

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
Preserve log Disable cache Online
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other Has blocked cookies
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
114.67.246.176
admin.css
Headers Preview Response Initiator Timing
这是什么来的?
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] {
https://blog.csdn.net/kongzhian

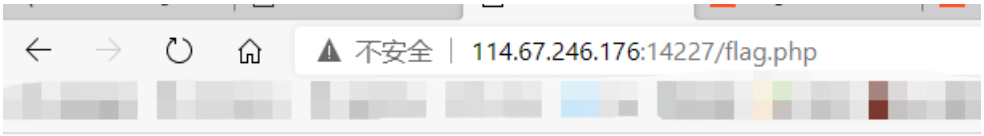
--------分割线----------


```
<?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

--------分割线----------



flag.php是存在的，并非404，只是没有内容

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

还原到默认code

```php
<?php
$KEY='ctf.bugku.com';
print(serialize("$KEY"))
?>
/*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";
```


在burpsuite上repeater一下