

# CTF练习平台 JavaScript ”点击一万次“ writeup

原创

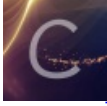
warmjuhao 于 2017-11-29 20:01:08 发布 7210 收藏

分类专栏: [Linux](#) 文章标签: [CTF](#) [writeup](#) [javascript](#)

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/warmjuhao/article/details/78669230>

版权



[Linux 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

进入题目, 查看源代码

```
14     margin: 0 auto;
15   }
16   #flag{
17     color: white;
18     text-align: center;
19     display: block;
20   }
21 </style>
22 <head>
23   <meta charset="utf-8"
24   <meta name="viewport" content="width=device-width, initial-scale=1"
25   <script src="jquery-3.2.1.min.js"></script>
26   <title>点击一万次</title>
27 </head>
28 <body>
29   <h1 id="goal">Goal: <span id="clickcount">0</span>/1000000</h1>
30   </span>
32 </body>
33 <script>
34   var clicks=0
35   $(function() {
36     $("#cookie")
37       .mousedown(function() {
38         $(this).width('350px').height('350px');
39       })
40       .mouseup(function() {
41         $(this).width('375px').height('375px');
42         clicks++;
43         $("#clickcount").text(clicks);
44         if(clicks >= 1000000){
45           var form = $('<form action="" method="post">' +
46             '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
47             '</form>');
48           $('body').append(form);
49           form.submit();
50         }
51       });
52   });
53 </script>
```

可以看到

```
var form = $('<form action="" method="post">' +
  '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
  '</form>');
$('body').append(form);
form.submit();
```

当满足条件后, 会执行post clicks=1000000

所以我们直接用ackbar来post

Click 100,000 times - Mozilla Firefox

ctf练习\_百度搜索 × CTF比赛|CTF论坛|C... × 点击一百万次 × Add-ons Manager ×

120.24.86.145:9001/test/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

INT SQL XSS Encryption Encoding Other

Load URL http://120.24.86.145:9001/test/


Split URL

Execute

Enable Post data  Enable Referrer

Post data clicks=1000000

**Goal: 1/1000000**  
<http://blog.csdn.net/warmjuhao>



flag{Not\_C00kI3C1ck3r}

得到flag!