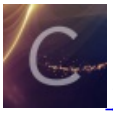
CTF练习平台 JavaScript ”点击一万次“ writeup

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



进入题目，查看源代码

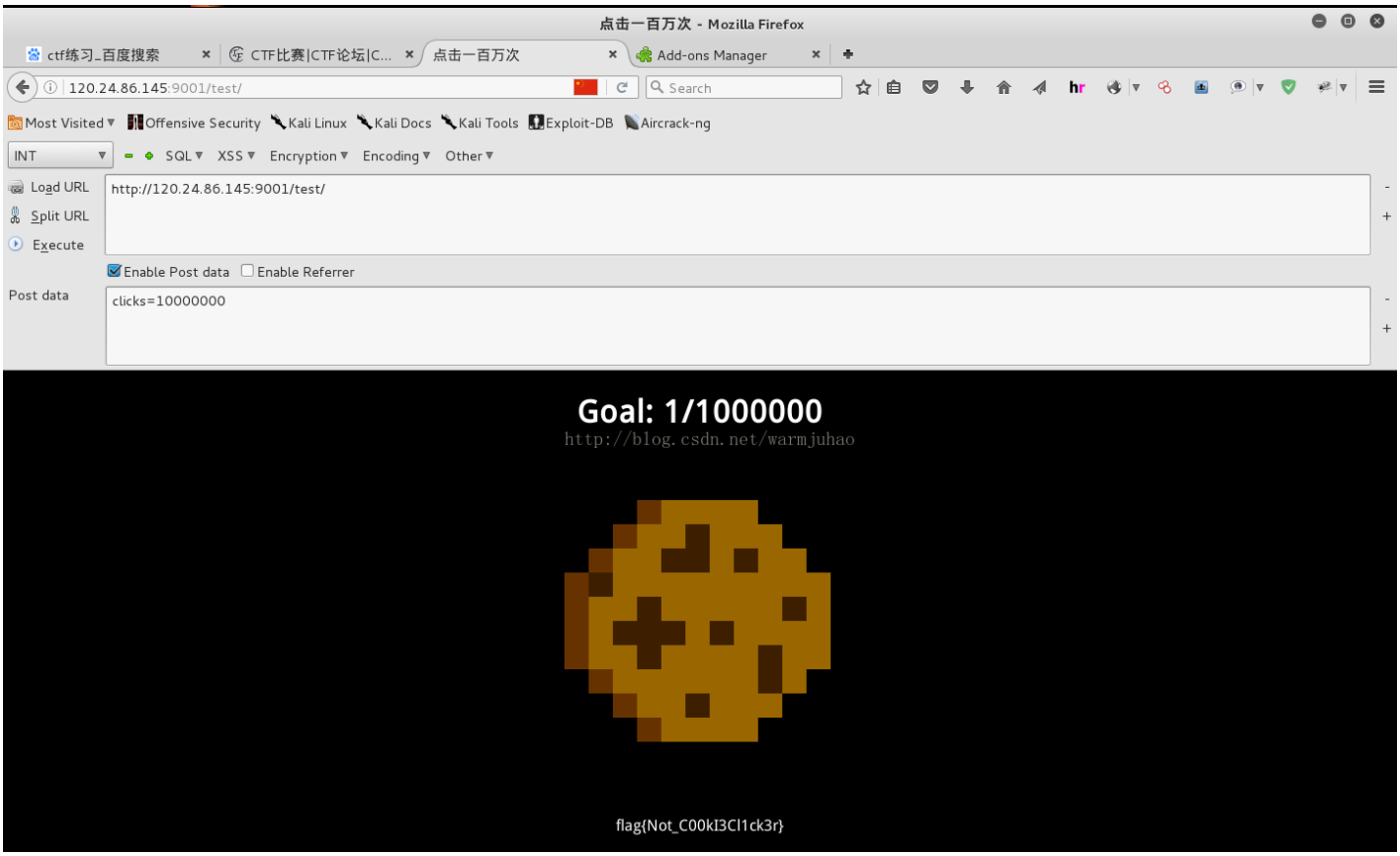
```
      margin: 0 auto;
    }
    #flag{
        color: white;
      text-align: center;
      display: block;
    }
  </style>
  <head>
    <meta charset="utf-8"
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <script src="jquery-3.2.1.min.js"></script>
    <title>点击一百万次</title>
  </head>
  <body>
    <h1 id="goal">Goal: <span id="clickcount">0</span>/1000000</h1>
    <img id="cookie" src="cookie.png">
    <span id="flag"></span>
  </body>
  <script>
    var clicks=0
    $(function() {
      $("#cookie")
        .mousedown(function() {
          $(this).width('350px').height('350px');
        })
        .mouseup(function() {
          $(this).width('375px').height('375px');
          clicks++;
          $("#clickcount").text(clicks);
          if(clicks >= 1000000){
            var form = $('<form action="" method="post">' +
                         '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
                         '</form>');
                         $('body').append(form);
                         form.submit();
          }
        });
    });
  </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hackbar来post


点击一百万次 - 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/
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://120.24.86.145:9001/test/
Enable Post data
Enable Referrer
Post data
clicks=10000000
Goal: 1/1000000
http://blog.csdn.net/warmjuhao
flag{Not_C00kI3Cl1ck3r}

得到flag！