攻防世界XCTF： NaNNaNNaNNaN-Batman

原创

末 初 于 2020-03-07 22:14:28 发布 758 收藏

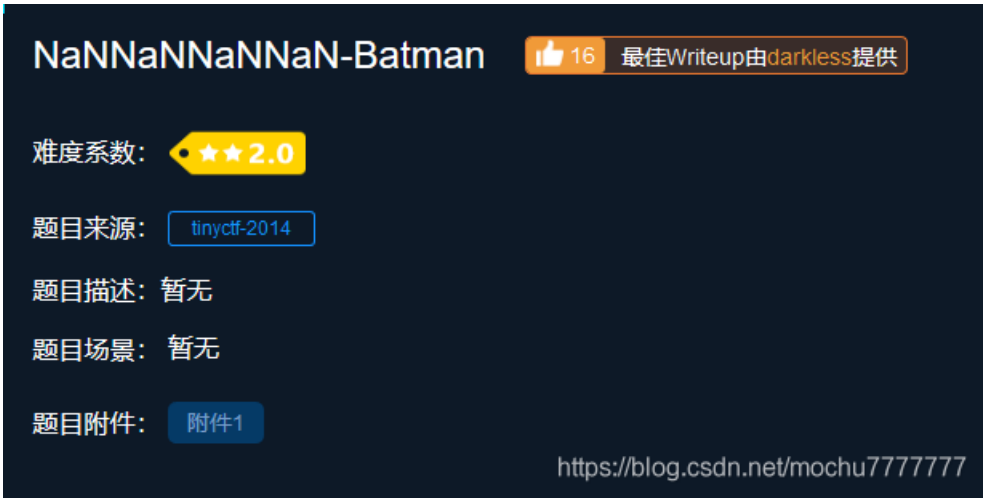
分类专栏： CTF_WEB_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/104723710

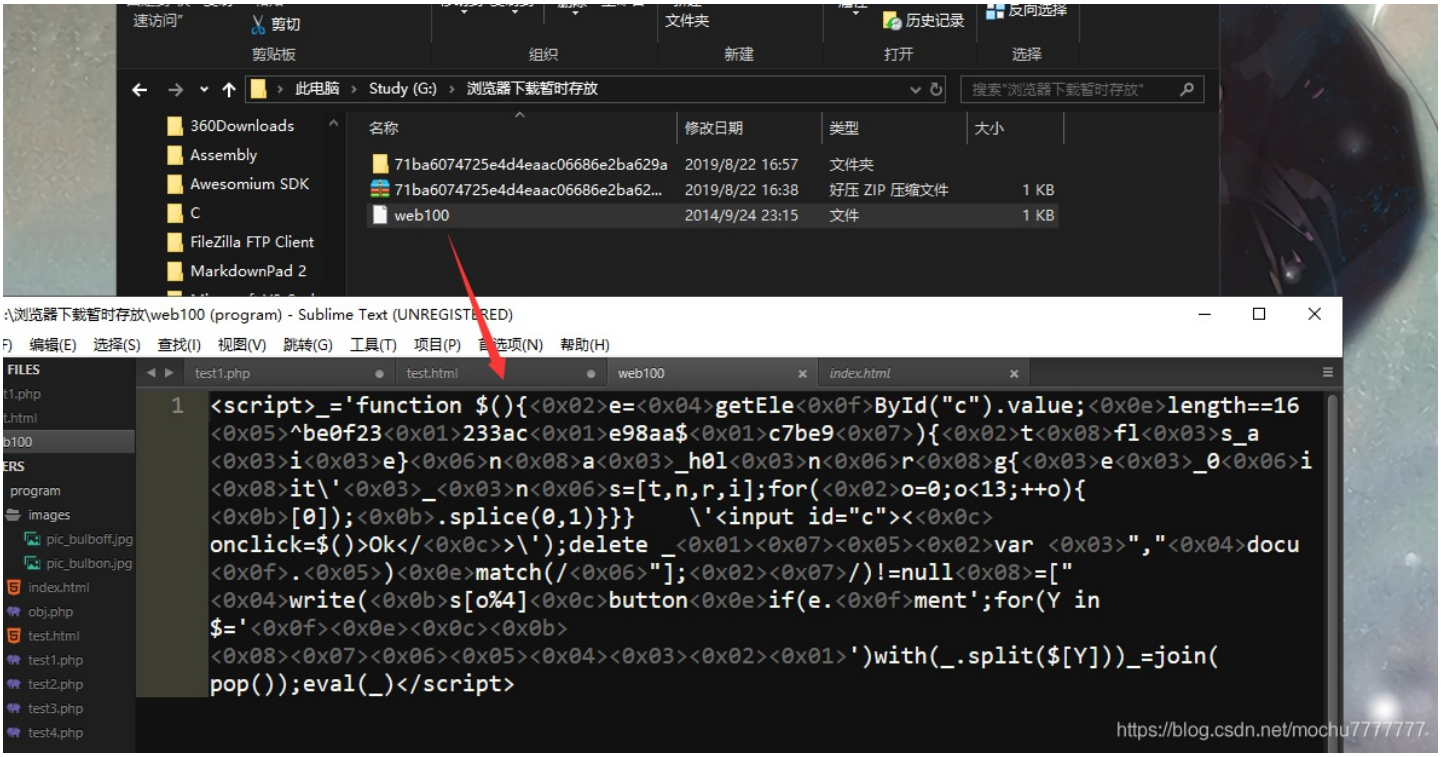
CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

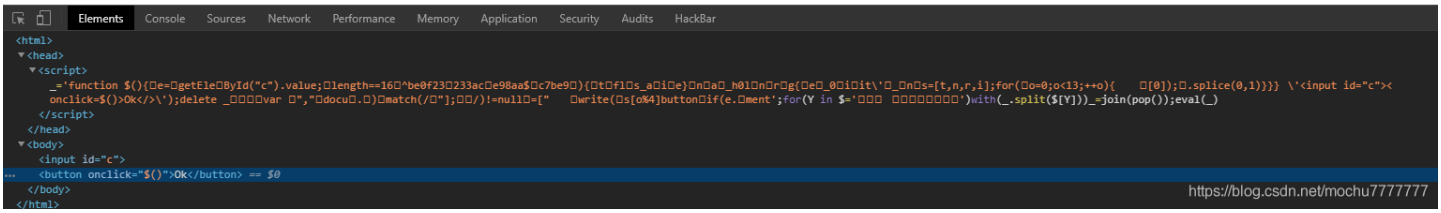


下载附件



乱码，但是根据内容大概可判别为网页文件，javascript脚本。修改后缀名为.html用浏览器打开

Ok



还是看不懂，然后把内容部分执行函数eval修改为alert，弹窗显示正常。


```
<script type="text/javascript">
    function $(){
            var e=document.getElementById("c").value;
            if(e.length==16)
             if(e.match(/^be0f23/)!=null)
                if(e.match(/233ac/)!=null)
                  if(e.match(/e98aa$/)!=null)
                    if(e.match(/c7be9/)!=null){
                     var t=["fl","s_a","i","e}"];
                     var n=["a","_h0l","n"];
                     var r=["g{","e","_0"];
                     var i=["it'","_","n"];
                     var s=[t,n,r,i];
                     for(var o=0;o<13;++o){
                         document.write(s[o%4][0]);s[o%4].splice(0,1)
                     }
                  }
        }document.write('<input id="c"><button onclick=$()>Ok</button>');delete _
</script>
```


两种方法得到flag

第一种方法：

匹配正则，根据内容可知以 ^ 开头 $ 结尾的，拼接就可以了，注意长度==16，删除一些重复的刚刚好。

提交内容：be0f233ac7be98aa\

第二种方法：

因为源码在我们手上，直接把限制条件全部删除，直接运行，即可得到flag。