




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](#)

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/mochu7777777/article/details/104723710>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

NaNNaNNaNNaN-Batman 👍 16 最佳Writeup由darkless提供

难度系数: ★★ 2.0

题目来源: tinyctf-2014

题目描述: 暂无

题目场景: 暂无

题目附件: 附件1

<https://blog.csdn.net/mochu777777>

下载附件

The screenshot shows a Windows file explorer window with the following table of contents:

名称	修改日期	类型	大小
71ba6074725e4d4eaac06686e2ba629a	2019/8/22 16:57	文件夹	
71ba6074725e4d4eaac06686e2ba62...	2019/8/22 16:38	好压 ZIP 压缩文件	1 KB
web100	2014/9/24 23:15	文件	1 KB

Below the file explorer, a Sublime Text editor window is open, displaying the following JavaScript code:

```

1 <script>_='function $(){<0x02>e=<0x04>getEle<0x0f>ById("c").value;<0x0e>length==16
<0x05>^be0f23<0x01>233ac<0x01>e98aa$<0x01>c7be9<0x07>){<0x02>t<0x08>fl<0x03>s_a
<0x03>i<0x03>e}<0x06>n<0x08>a<0x03>_h01<0x03>n<0x06>r<0x08>g{<0x03>e<0x03>_0<0x06>i
<0x08>it\<0x03>_<0x03>n<0x06>s=[t,n,r,i];for(<0x02>o=0;o<13;++o){
<0x0b>[0]);<0x0b>.splice(0,1)}}} \<input id="c"><0x0c>
onclick=$()<0x0c>\<0x0c>);delete _<0x01><0x07><0x05><0x02>var <0x03>","<0x04>docu
<0x0f>.<0x05>><0x0e>match(/<0x06>"];<0x02><0x07>/)!<0x08>=["
<0x04>write(<0x0b>s[o%4]<0x0c>button<0x0e>if(e.<0x0f>ment';for(Y in
$='<0x0f><0x0e><0x0c><0x0b>
<0x08><0x07><0x06><0x05><0x04><0x03><0x02><0x01>')with(._split($[Y]))_<0x0c>
pop();eval(_</script>
  
```

The code is a JavaScript payload designed to exploit a vulnerability in a web application. It uses a function named '\$' to interact with the document object model (DOM) and execute various operations, including reading the value of an input field, calculating its length, and performing a series of conditional checks and actions based on the results. The code is encoded using hexadecimal characters to avoid detection by security tools.

<https://blog.csdn.net/mochu777777>

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

```
Elements Console Sources Network Performance Memory Application Security Audits HackBar
<html>
  <head>
    <script>
      _=function $(e=$(getEleById("c").value;length==16*be0f230233ac0e98a50c7be90){0t0f10s_a0i0e)0n0a0_010n0r0g(0e0_00i0it'\0_0n0s=[t,n,r,i];for(0=0;0<13;++0){ 0[0];0.splice(0,1)}}) \<input id="c"><
      onclick=$(0k<>');delete _0000var 0,"docu0.0)0match(/0");0/)!+null10=[" 0write(0s[004]button0if(e.0ment';for(Y in $="000 0000000')with(_split($[Y]))=_join(pop());eval(_
    </script>
  </head>
  <body>
    <input id="c">
    <button onclick="$()">Ok</button> == $0
  </body>
</html>
```

<https://blog.csdn.net/mochu777777>

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。



<https://blog.csdn.net/mochu7777777>

```
<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=["f1","s_a","i","e"];
                        var n=["a","_h01","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>
```

<https://blog.csdn.net/mochu7777777>

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。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)