

# XCTF攻防世界 Web高手进阶区 NaNNaNNaNNaN-Batman writeup

原创

[Senimo](#) 于 2020-03-30 14:30:22 发布 590 收藏 2

分类专栏: [各CTF平台 Writeup](#) 文章标签: [web](#) [XCTF攻防世界](#) [Web高手进阶区](#) [writeup](#) [NNaNNaN-Batman](#)

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/weixin\\_44037296/article/details/105197856](https://blog.csdn.net/weixin_44037296/article/details/105197856)

版权



[各CTF平台 Writeup 专栏收录该内容](#)

16 篇文章 6 订阅

订阅专栏

## XCTF攻防世界 Web高手进阶区 NaNNaNNaNNaN-Batman writeup

**NaNNaNNaNNaN-Batman**

难度系数: 2.0

题目来源: [tinyctf-2014](#)

题目描述: 暂无

题目附件: [附件1](#)

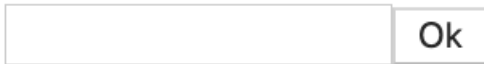
下载附件，解压得到：`web100` 文件：



因为没有文件后缀名，放入到Hex Fiend中查看：

```
0 3C736372 6970743E 5F3D2766 756E6374 696F6E20 2428297B <script>_='function $(){
24 02653D04 67657445 6C650F42 79496428 22632229 2E76616C e= getEle ById("c").val
48 75653B0E 6C656E67 74683D3D 3136055E 62653066 32330132 ue; length==16 ^be0f23 2
72 33336163 01653938 61612401 63376265 39072978 02740866 33ac e98aa$ c7be9 ){ t f
96 6C03735F 61036903 657D066E 0861035F 68306C03 6E067208 l s_a i e} n a _h0l n r
120 677B0365 035F3006 69086974 5C27035F 036E0673 3D5B742C g{ e _0 i it\' _ n s=[t,
144 6E2C722C 695D3866 6F722802 6F3D303B 6F3C3133 3B2B286F n,r,i];for( o=0;o<13;+o
168 297B090B 5B305D29 3B0B2E73 706C6963 6528302C 31297D7D ){ [0]]; .splice(0,1)}}
192 7D095C27 3C696E70 75742069 643D2263 223E3C0C 206F6E63 } \'<input id="c">< onc
216 6C696368 3D242829 3E4F6B3C 2F0C3E5C 27293864 656C6574 lick=$( )>Ok</ >\');delet
240 65205F01 07050276 61722003 222C2204 646F6375 0F2E0529 e _ var ", " docu . )
264 0E6D06174 6368282F 06225D38 02072F29 213D6E75 6C6C083D match(/ "; /)!=null =
288 5B220904 77726974 65280B73 5B6F2534 5D0C6275 74746F6E [" write( s[o%4] button
312 0E696628 652E0F6D 656E7427 3B666F72 28592069 6E20243D if(e. ment';for(Y in $=
336 270F0E0C 0B090807 06050403 02012729 77697468 285F2E73 ' )with( _s
360 706C6974 28245859 5D29295F 3D6A6F69 6E28706F 70282929 plit($[Y]))_=_join(pop())
384 3B657661 6C285F29 3C2F7363 72697074 3E https://blog.x ;eval( _)</script>1037296
```

可以看到其中有 `<script>` 标签，填上后缀名 `.html`，使用浏览器打开：



得到一个输入框，查看网页源码：

```
// 经整理后的源码：
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","_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>');
```

方法一：

满足给出的正则表达式，`^` 为开始，`$` 为结束，即构造：

```
be0f(23)233ac(c)7b(e9)e98aa  
be0f233ac7be98aa
```

去掉拼接完 () 中的字符串，将其长度控制在 16 位，输入字符串，得到 flag：

flag{it's\_a\_h0le\_in\_0ne}

方法二：

因为输入的字符串由 JavaScript 判断，所以直接在控制台执行结果的代码即可：

```
var t=["f1","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)  
}
```



在浏览器控制台执行如上代码，得到 flag：

flag{it's\_a\_h0le\_in\_0ne}