#XCTF整理#NaNNaNNaNNaN-Batman

原创

vircorns 于 2019-10-28 17:31:43 发布 1959 收藏 8

分类专栏： # 题解

本文链接：https://blog.csdn.net/weixin_43476037/article/details/102783724

- 做题地址

知识点

- html乱码处理
- 基础js代码
  - eval函数，这是执行函数；这里执行了_变量中的内容也就是''中的内容，但是，要注意的是，它并没有执行`$()`函数，仅仅执行了字符串而已（从而导致乱码），因而页面html页面没有任何显示，只显示了input标签的内容，但是我们想让源代码正常显示出来，不进行执行，那么，我们就用到了`alert`弹窗，将乱码的`$()`函数源码完整显示出来

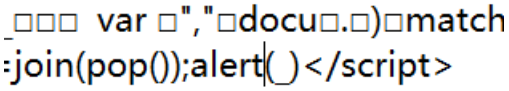
wp

- 下载附件以后用文本打开，发现是js乱码：

<script>_='function $(){ e=□getEle□Byld("c").value;□length==16□^be0f23□233ac□e98aa$□c7be9□){ t□fl□s_a□i□e}□n□a□_h0l□n□r□g{□e□_0□i□it
\'□_□n□s=[t,n,r,i];for(o=0;o<13;++o){ □[0]);□.splice(0,1)}}} \'<input id="c"><↟ onclick=$()>Ok</↟>\');delete _□□□ var □","□docu□.□)□match
(/□"]; □/)!=null□=[" □write(□s[o%4]↟button□if(e.□ment';for(Y in $='□□↟□ □□□□□□ □')with(_.split($[Y]))_=join(pop());eval(_)</script>

- 修改后缀，用html打开，发现有提交框，但是源代码仍然是乱码

- 将eval函数改为alert



- 弹窗看到源代码

- 即：

```
function $(){
var e=document.getElementById("c").value;
if(e.length==16)//构造长度为16
   if(e.match(/^be0f23/)!=null)//开头匹配到be0f23
      if(e.match(/233ac/)!=null)//e中有233ac
         if(e.match(/e98aa$/)!=null)//结尾匹配到e98aa
             if(e.match(/c7be9/)!=null){//e中有c7be9
             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 _
```

- 给的数正好可构造：e=be0f233ac7be98aa
- 把alert改回eval，在提交框中输入，即可得到flag：flag{it’s_a_h0le_in_0ne}