

XCTF simple js

原创

YenKoc



于 2019-12-03 23:56:50 发布



161



收藏

分类专栏: [XCTF](#)

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/YenKoc/article/details/103378366>

版权



[XCTF 专栏收录该内容](#)

26 篇文章 2 订阅

订阅专栏

simple_js  205 最佳Writeup由Venom • IceM提供

难度系数:  1.0

题目来源: [root-me](#)

题目描述: 小宁发现了一个网页, 但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx})

题目场景:  <http://111.198.29.45:36270>

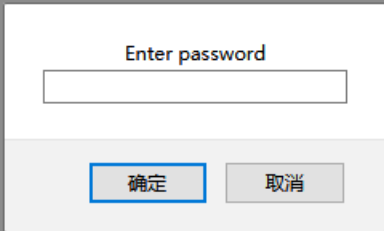
 [删除场景](#)

倒计时: 03:57:47 [延时](#)

题目附件: 暂无

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

思路分析:
进入靶场,



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

随便输入, 肯定是错误的, f12看下源码, 结合题目说js, 把js代码单独拿出来看看。

```

function dechiffre(pass_enc){
    var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
    var tab = pass_enc.split(',');
        var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
            k = j + (1) + (n=0);
            n = tab2.length;
            for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-1];p += String.fromCharCode((o = tab2[i]
));
                if(i == 5)break;}
            for(i = (o=0); i < (k = j = n); i++ ){
                o = tab[i-1];
                if(i > 5 && i < k-1)
                    p += String.fromCharCode((o = tab2[i]));
            }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x
2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));

    h = window.prompt('Enter password');
    alert( dechiffre(h) );
}

```

wdnmd, 这个东西看的人脑壳痛, 一大堆变量, 没用到的, 这里简化一下代码。

```

function dechiffre(){
var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
var tab2=pass.split(",");
var i,n=tab2.length;
for(i=0;i<n;i++)
{
    p+=String.fromCharCode(tab2[i]);
}
return p;
}

```

这里就是将ASCII码转换成字符串，同时我们发现

```
(dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));
```

这里已经有一个常量给我们了，说不定就是答案，但是参数是和pass还是有差距的，没事，用python操作一下

```
test.py × bad.py ×
1 data="\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"
2 print(data)
```

```
D:\Anaconda\python.exe D:/SourceLeakHacker/
55,56,54,79,115,69,114,116,107,49,50
```

Cyberpeace{786OsErtk12}

将这串换成pass变量里的值，执行js代码，得出flag，记得规范flag格式

总结：看了看大佬的wp，发现实际上chr函数是可以接收10进制和16进制的，所以不需要变，也可以得出答案的



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)