

# simple-js

这几个adworld三星题难度完全就是没有，，不用公式搜索都能做

[上一题](#)[下一题](#)[随机一题](#)

**simple\_js**

GFSJ0480

积分 3

金币 3

487 最佳Writeup由 huang8huang 提供

[收藏](#)[反馈](#)

难度: 3    方向: Web    题解数: 131    解出人数: 37731

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://61.147.171.105:63820

100%

倒计时: 3时29分21秒

[延时](#)[删除场景](#)

题目已回答正确 ✓

首先登陆是一个js框，猜测有没有xss注入？

测试了一下是没有的，进行源代码的查看，顺便目录爆破

```
<html>
<head>
  <title>JS</title>
  <script type="text/javascript">
    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;
    }
  </script>

```

```
        return pass;
    }

    String["fromCharCode"]
(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"));

    h = window.prompt('Enter password');
    alert(dechiffre(h));
</script>
</head>
</html>
```

可以发现这个函数的目的就是拼接字符串的，无论怎么写都是输出这个

正确答案就是把String["fromCharCode"]的转译成ascii就行了，有点easy