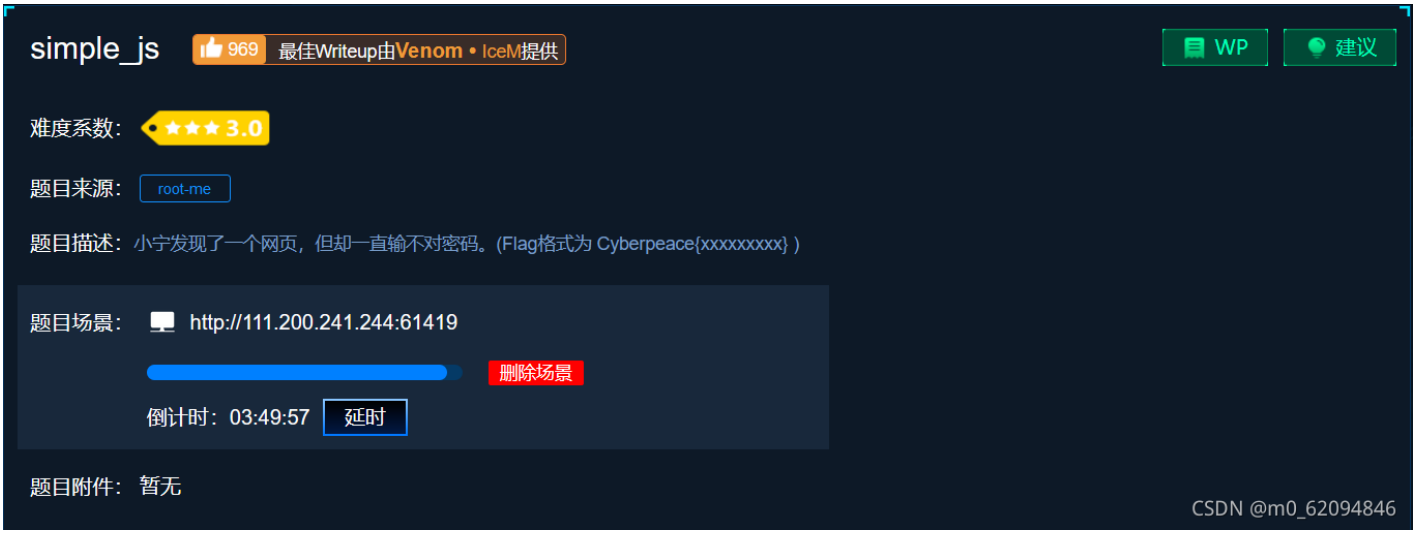
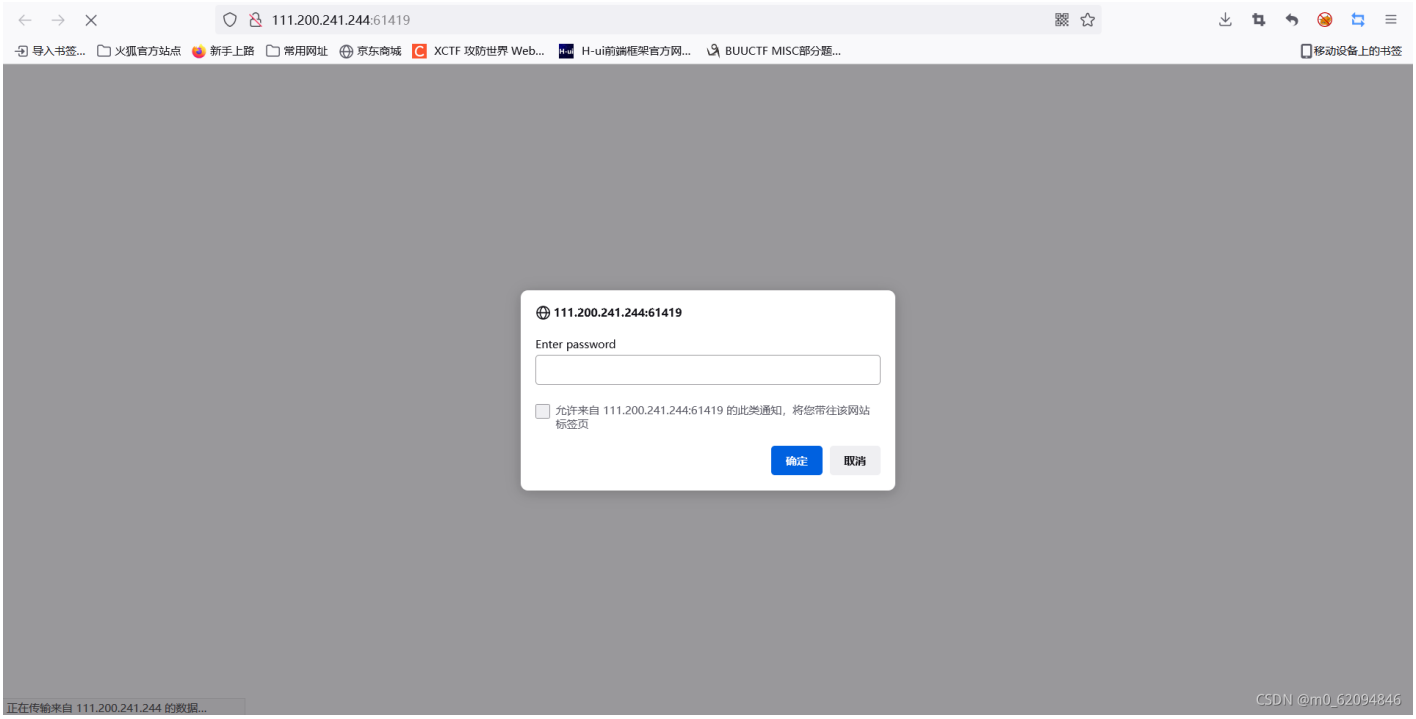
攻防世界-simple_js

原创

m0_62094846 于 2021-11-18 14:10:44 发布 65 收藏
文章标签： 安全 mysql 数据库

本文链接：https://blog.csdn.net/m0_62094846/article/details/121398583





密码输不对，包也抓不到，就看看源代码

view-source:http://111.200.241.244:61419/

导入书签... 火狐官方站点 新手上路 常用网址 京东商城 XCTF 攻防世界 Web... H-ui前端框架官方网... BUUCTF MISC部分题... 移动设备上的书签

```
<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 + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-l)
                                        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\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>
```


看着就是javascript代码，要代码审计

```
<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 + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-l)
                                        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\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>
```


第一部分是函数部分，先看第二部分

JavaScript String 参考手册

← 上一节　　下一节 →

String 对象

String 对象用于处理文本（字符串）。

JavaScript fromCharCode() 方法

JavaScript String 对象

实例

将 Unicode 编码转为一个字符:

```
var n = String.fromCharCode(65);
```

n 输出结果:

```
A
```

尝试一下 »

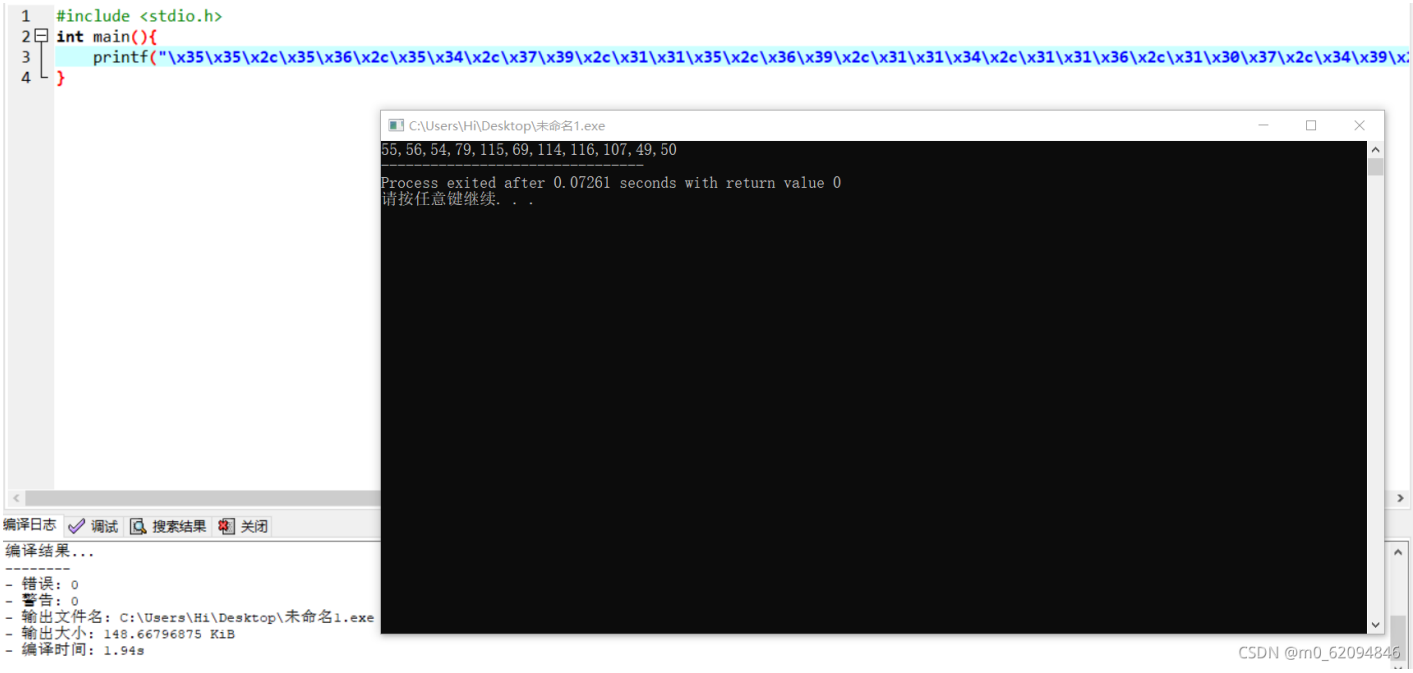
定义和用法

fromCharCode() 可接受一个指定的 Unicode 值，然后返回一个字符串。

注意：该方法是 String 的静态方法，字符串中的每个字符都由单独的 Unicode 数字编码指定。使用语法： String.fromCharCode()。

String["fromCharCode"]应该就是说把Unicode转换成字符串并返回

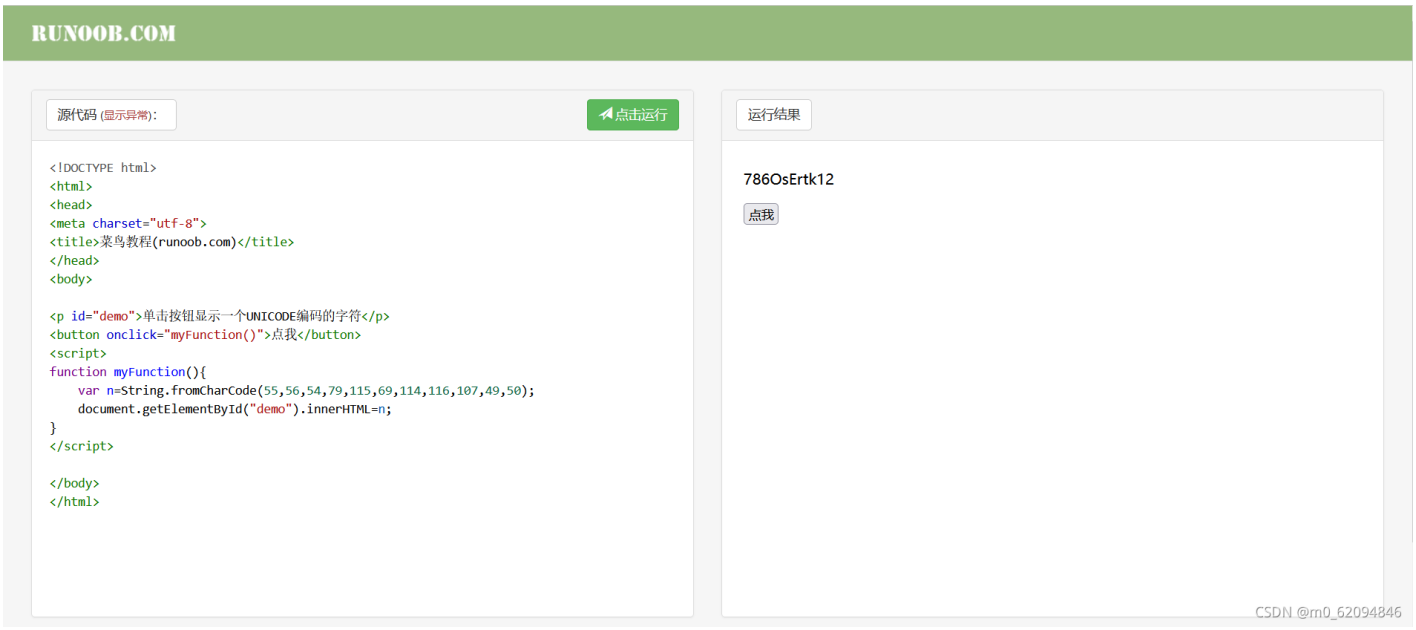
函数部分有点难懂，先看看 \x35\x35\x2c 这部分的内容，在网上查看，知道这就是 C/C++ 里普通的转义字符。直接用cout 或者 printf 就能显示出来。也可以查ASCII表，每个\x后面的两位 是一个十六进制数。



得到转化后的代码，要看看有什么用

用其他编码转换器转换不了，直接用菜鸟教程的编译器解码

完成了fromCharCode的那一步



不知道提交密码的那一页有什么用，没用到