

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](#)

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/m0_62094846/article/details/121398583

版权

The screenshot shows the CSDN article page for 'simple_js'. At the top, it has a title 'simple_js' with a like count of 969 and a note '最佳Writeup由Venom • IceM提供'. There are buttons for 'WP' and '建议'. Below the title, the difficulty coefficient is '3.0' (3 stars). The source is 'root-me'. The description says: '小宁发现了一个网页, 但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxxx})'. The scenario is 'http://111.200.241.244:61419' with a '删除场景' button. A timer shows '03:49:57' with a '延时' button. The attachments section is empty. The bottom right corner has 'CSDN @m0_62094846'.

The screenshot shows a web browser window with the address bar displaying '111.200.241.244:61419'. The browser tabs include '导入书签...', '火狐官方网站', '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...', and 'BUUCTF MISC部分题...'. The main content area is a grey background with a white dialog box in the center. The dialog box has the title '111.200.241.244:61419' and the text 'Enter password'. Below the text is a password input field. At the bottom of the dialog box, there is a checkbox labeled '允许来自 111.200.241.244:61419 的此类通知, 将您带往该网站标签页' and two buttons: '确定' and '取消'. At the bottom left of the browser window, there is a status bar that says '正在传输来自 111.200.241.244 的数据...'. The bottom right corner has 'CSDN @m0_62094846'.

密码输不对, 包也抓不到, 就看看源代码

```
1
2 <html>
3 <head>
4   <title>JS</title>
5   <script type="text/javascript">
6     function dechiffre(pass_enc){
7       var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
8       var tab = pass_enc.split(',');
9       var tab2 = pass.split(',');var i, j, k, l=0, m, n, o, p = "";i = 0;j = tab.length;
10      k = j + (1) + (n=0);
11      n = tab2.length;
12      for(i = (o=0); i < (k = j = n); i++){o = tab[i-1];p += String.fromCharCode((o = tab2[i]));
13        if(i == 5)break;}
14      for(i = (o=0); i < (k = j = n); i++){
15        o = tab[i-1];
16        if(i > 5 && i < k-1)
17          p += String.fromCharCode((o = tab2[i]));
18      }
19      p += String.fromCharCode(tab2[17]);
20      pass = p;return pass;
21    }
22    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"));
23
24    h = window.prompt('Enter password');
25    alert( dechiffre(h) );
26
27 </script>
28 </head>
29
30 </html>
31
```

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 + (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\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。

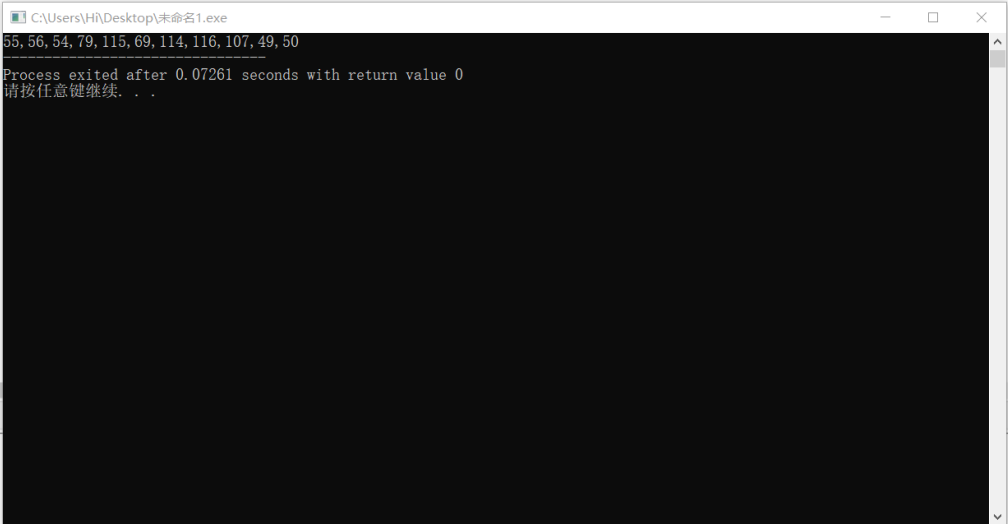
注意： 该方法是 String 的静态方法，字符串中的每个字符都由单独的 Unicode 数字编码指定。使用语法：String.fromCharCode()

CSDN@m0_62094846

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。

```
1 #include <stdio.h>
2 int main(){
3     printf("\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\x31");
4 }
```



```
C:\Users\Hi\Desktop\未命名1.exe
55,56,54,79,115,69,114,116,107,49,50
Process exited after 0.07261 seconds with return value 0
请按任意键继续...
```

编译日志 调试 搜索结果 关闭
编译结果...
- 错误: 0
- 警告: 0
- 输出文件名: C:\Users\Hi\Desktop\未命名1.exe
- 输出大小: 148.66796875 KiB
- 编译时间: 1.94s

CSDN@m0_62094846

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

源代码 (显示异常):

点击运行

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>菜鸟教程(runoob.com)</title>
</head>
<body>

<p id="demo">单击按钮显示一个UNICODE编码的字符</p>
<button onclick="myFunction()">点我</button>
<script>
function myFunction(){
    var n=String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50);
    document.getElementById("demo").innerHTML=n;
}
</script>

</body>
</html>
```

运行结果

786OsErtk12

点我

CSDN @m0_62094846

不知道提交密码的那一页有什么用，没用到