

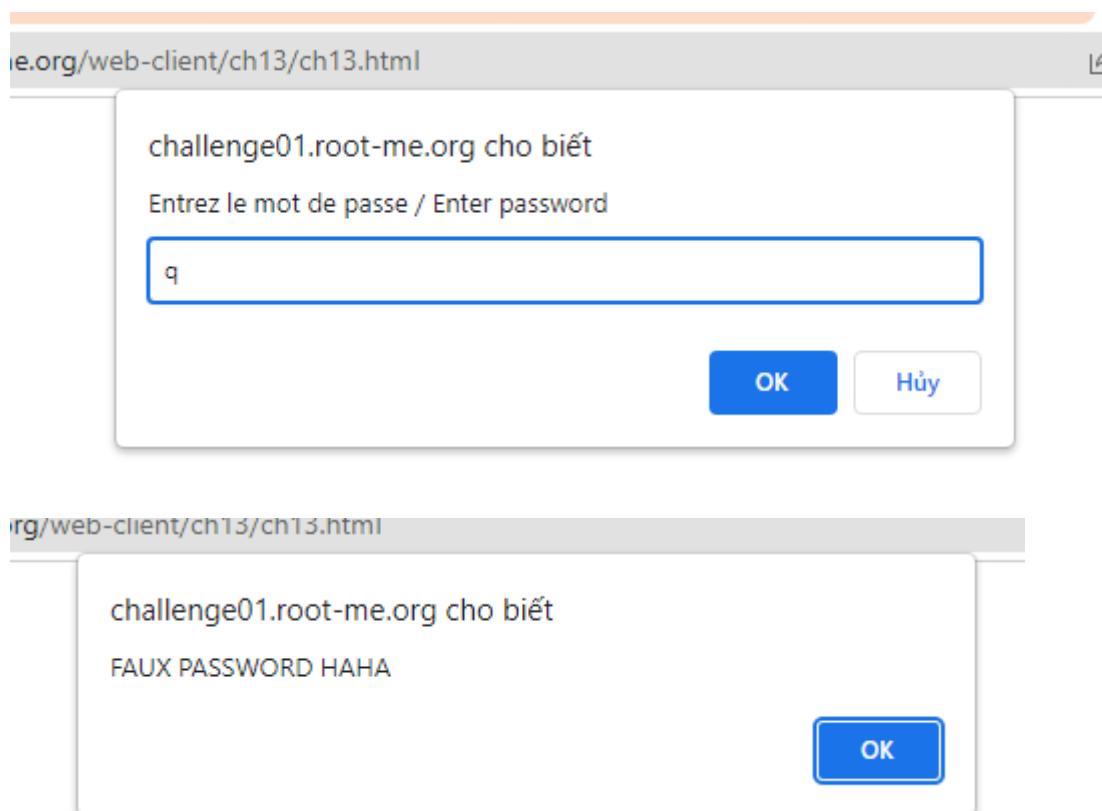
Write up challenge Javascript - Obfuscation 3

Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một form yêu cầu nhập password. Nhập thử thì thông báo **FAUX PASSWORD HAHA** hiện lên.



Tiến hành inspect, ta thấy có một hàm **dechiffre** thực hiện các phép tính toán dài dòng. Xem sơ hàm thì có thể thấy có vẻ đầu vào không ảnh hưởng đến kết quả trả về của hàm cho lắm!

```

<html>
<head>
  <title>Obfuscation 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\x
39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));
    h = window.prompt('Entrez le mot de passe / Enter password');
    alert( dechiffre(h) );
  </script>

```

Thử xem xét các manh mối khác. Có một chuỗi Hex liên tiếp và ta thấy có một hàm trong javascript được gọi ý đó là String.fromCharCode()

```

String["fromCharCode"]
(dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x
39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));

```

Tiến hành convert chuỗi Hex đó:

```

> (" \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")
< '55,56,54,79,115,69,114,116,107,49,50'

```

Sử dụng hàm String.fromCharCode() với kết quả convert thu được, ta nhận được một chuỗi suy đoán đó là flag.

```

> String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50);
< '7860sErtk12'

```

Thử submit challenge. Thành công !

Javascript - Obfuscation 3

30 Points 

Useful or Useless that is the question...

Author

Hel0ck, 4 February 2011





Level ?



Statement

[Start the challenge](#)

4 related ressource(s)

-  Automatic simplification of obfuscated JavaScript code
-  Spiffy: Automated JavaScript deobfuscation (Virologie)
-  Automatic detection for JavaScript obfuscation attacks
-  DEFCON a different approach to JavaScript obfuscation

Validation

Well done, you won 30 Points

Don't forget to give your opinion on the challenge by voting :-)

 twittez le !

Flag: 786OsErtk12