

BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

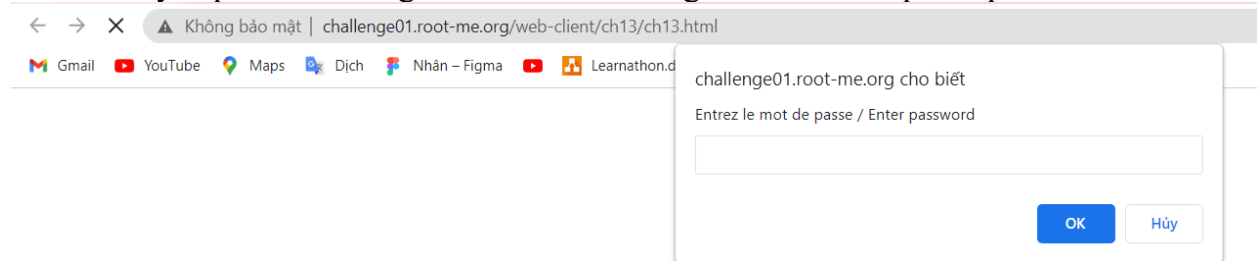
Giảng viên hướng dẫn: *Đỗ Hoàng Hiến*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

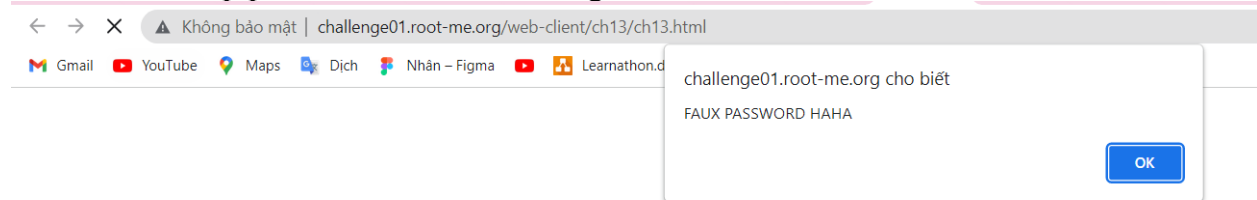
Challenge 8: Javascript - Obfuscation 3 (level medium)

Link challenge <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Obfuscation-3>

- ✓ Truy cập vào challenge thì xuất hiện thông báo bắt ta nhập vào password



- ✓ Thử nhập pass là 1 thì hiện ra thông báo là FAUX PASSWORD HAHA



- ✓ Sử dụng **ctr + u** để xem mã nguồn

```
← → ↺ Không bảo mật | view-source:challenge01.root-me.org/web-client/ch13/ch13.html
Gmail YouTube Maps Dịch Nhân - Figma Learnathon.drawio...

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

- ✓ Ta thấy password ta nhập vào sẽ lưu vào biến h. Sau đó hàm dechiffre được gọi với đối số là h (pass vừa nhập vào) và xuất ra thông báo.
- ✓ Phân tích function dechiffre, biến pass lưu dãy số ở dạng decimal của chuỗi “FAUX PASSWORD HAHA”. Biến tab lưu giá trị của chuỗi password ta nhập vào được tách bởi dấu “,”. Biến tab2 sẽ tách biến pass ra bởi dấu “,” để lấy từng số decimal, n sẽ lưu độ dài của tab2 (n = 18).
- ✓ Ở vòng for đầu tiên biến p sẽ được chuyển sang dạng ký tự từ biến tab2, lúc này 6 số ở dạng decimal của tab2 sẽ được chuyển sang dạng char và lưu vào biến p. Do đó, p sẽ là “FAUX P”.
- ✓ Ở vòng for tiếp theo, tiếp tục chuyển sang dạng char và nối vào biến p, ở vòng for này sẽ chuyển từ số thứ 7 của tab2 đến số thứ 16. Do đó, p sẽ là “FAUX PASSWORD HAH”.
- ✓ Cuối cùng p sẽ được nối thêm ký tự cuối cùng được chuyển từ tab2 sang, vậy p sẽ là “FAUX PASSWORD HAHA”. Sau đó pass gán bằng p và return pass. Ta nhận thấy rằng chương trình luôn return về “FAUX PASSWORD HAHA”.
- ✓ Ta chú ý thấy rằng, có 1 đoạn code khá đáng nghi nó gọi hàm dechiffre, trong khi hàm này luôn trả về “FAUX PASSWORD HAHA”. Có thể ở đây chứa password

- ✓ Thử decode đoạn mã hex trong này ra. Ta nhận được một dãy số decimal, tiếp tục chuyển đổi sang kiểu char ta thu được dãy 7860sErtk12

```
Elements Console Recorder Sources Network Performance Memory Application Security Lighthouse EditThisCookie
top Filter
DevTools failed to load source map: Could not load content for chrome-extension://amfojhdiedpnljjbhjnhokbnohfdhfb/js/effector.es.js.map: System error: ne
DevTools failed to load source map: Could not load content for chrome-extension://fheoggkfdfchfphceiefdbepaooicaho/sourceMap/chrome/scripts/iframe_form_de
DevTools failed to load source map: Could not load content for chrome-extension://fheoggkfdfchfphceiefdbepaooicaho/sourceMap/chrome/scripts/content_scroll
> \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
✖ Uncaught SyntaxError: Invalid or unexpected token
> "\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'
> String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50)
< '7860sErtk12'
```

✓ Thử submit và ta đã vượt qua thử thách 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](#) (Virologie)
-  [Spiffy: Automated JavaScript deobfuscation](#) (Virologie)
-  [Automatic detection for JavaScript obfuscation attacks](#) (Virologie)
-  [DEFCON a different approach to JavaScript obfuscation](#) (Virologie)

Validation

Well done but you've already won the 30 Points

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

Flag:786OsErtk12