



JAVASCRIPT-OBFUSCATION

김두형

Plutoo

2018.7.9



Index



1. 문제분석

2. 풀이

3. QnA

"HAHAHAHAHAHAHA"

-DU HYEOUNG KIM

평화

산과강





CHARCODE?

- 키보드에서 유니코드를 나타내는 문자

```
function getKey(event)
{
    event = event || window.event;
    var keyCode = event.which || event.keyCode;
    alert(keyCode);
}
function getChar(event)
{
    event = event || window.event;
    var keyCode = event.which || event.keyCode;
    var typedChar = String.fromCharCode(keyCode);
    alert(typedChar);
}
```

Example

event.keyCode

문자가 아닌 다른 key event 반환

ASCII코드에 기반

event.charcode

문자 키의 유니코드 값을 반환



18

keydown.event.keyCode: 56

keydown.event.which: 56

keypress.event.keyCode: 56

keypress.event.which: 56

keyup.event.keyCode: 56

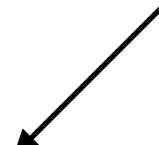
keyup.event.which: 56

0		10		20	Caps Lock	30		40	Arrow Down
1		11		21		31		41	
2		12		22		32		42	
3		13	Enter	23		33	Page Up	43	
4		14		24		34	Page Down	44	
5		15		25		35	End	45	Insert
6		16	Shift	26		36	Home	46	Delete
7		17	Ctrl	27	Esc	37	Arrow Left	47	
8	Backspace	18	Alt	28		38	Arrow Up	48	0
9	Tab	19	Pause/Break	29		39	Arrow Right	49	1
50	2	60		70	f	80	p	90	z
51	3	61	=+	71	g	81	q	91	Windows
52	4	62		72	h	82	r	92	
53	5	63		73	i	83	s	93	Right Click
54	6	64		74	j	84	t	94	
55	7	65	a	75	k	85	u	95	
56	8	66	b	76	l	86	v	96	0 (Num Lock)
57	9	67	c	77	m	87	w	97	1 (Num Lock)



```
<!--
Obfuscation
.Niveau : Facile
.By Hel0ck
.The mission :
    Retrouver le password contenu dans la var pass.
    You need my help ? IRC : irc.root-me.org #root-me
-->
<script type="text/javascript">
    var pass = unescape("unescape%28%22String.fromCharCode%2528104%252C68%252C117%252C102%252C106%252C100%252C107%252C105%252C49%252C53%252C54%2529%22%29");
</script>
</head>
```

Fromchar



%2528104%252C68%252C117%252C102%252C106%252C100%252C107%252C105%252C49%252C53%252C54%2529%22%29	charCodeAt()	37, 50, 53, 50, 56, 49, 48, 52, 37, 50, 53, 50, 67, 54, 56, 37, 50, 53, 50, 67, 49, 49, 55, 37, 50, 53, 50, 67, 49, 48, 50, 37,
---	--------------	---

이게 플레인 텍스트였어

codestring eval(pass)

비밀번호~

✓ Javascript - Obfuscation 2 32%



```
> unescape("unescape%28%22String.fromCharCode%2528104%252C68%252C117%252C102%252C106%252C100%252C107%252C105%252C49%252C53%252C54%2529%22%29")
< "unescape("String.fromCharCode%28104%2C68%2C117%2C102%2C106%2C100%2C107%2C105%2C49%2C53%2C54%29")"
> unescape("String.fromCharCode%28104%2C68%2C117%2C102%2C106%2C100%2C107%2C105%2C49%2C53%2C54%29")
< "String.fromCharCode(104,68,117,102,106,100,107,105,49,53,54)"
> String.fromCharCode(104,68,117,102,106,100,107,105,49,53,54)
< [REDACTED]
```



JAVASCRIPT-OBFUSCATION 3





함수처리

```

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 pass
  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-1)
      p += String.fromCharCode((o = tab2[i]));
  }
  p += String.fromCharCode(tab2[17]);
  pass = p; return pass;
}

```

```

String["fromCharCode"] ← 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('Entrez le mot de passe / Enter password');
alert( dechiffre(h) );

```

password가 필요하다. 나는

\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



70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65



70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65	FAUX PASSWORD HAHA
fromCharCode()	

개념부터 인성이;;



\\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



decoder을 사용하세요~



Decoded results:

```
dechiffre("55,56,54,79,115,69,114,116,107,49,50"))
```

개념글자 치환된분이군



55,56,54,79,115,69,114,116,107,49,50

fromCharCode()

빈칸넣음~



Javascript - Obfuscation 3

18%

"QnA"

–PT0