

Forum:[Hack Forums](#)

Thread: [How can I execute XSS by bypassing filters for "=", "<script" and "javascript" ?](#)

mr.cracker - August 2, 2015, 11:03 am

I want to execute XSS.

but WAF filters ==>

Code:

Code <script, javascript, =

my search terms are => p1=sachin&p2=dravid

output :

Code:

Code <input type="text" value="sachin"/>

<input type="text" value="dravid"/>if I give <script, javascript,= it suddenly redirect to Default Error page!

Below code doesn't give any error,

Code:

Code <<!--mm-->script>alert(1);</script>But in browser it doesn't execute as a <script> tag.

i can use any other charcters except <script, javascript, = .

I can inject HTML tagslike,

Code:

Code "><marquee><H1>HACKED<H1><marquee>[b]<!--[/b]But I wanna execute XSS.

Without above filtered terms how can I bypass the WAF ?

Yoshikage Kira - August 2, 2015, 11:05 am

try this:

"><body onload=alert(1)><marquee><!--

edit:

if it censors =, not sure if there is a solution lol..

mr.cracker - August 2, 2015, 8:25 pm

(Aug 2, 2015 11:05 AM)Gr?ed Wrote: [\[CITE\]](#) try this:

"><body onload=alert(1)><marquee><!--

edit:

if it censors =, not sure if there is a solution lol..

It filters "=", <script, javascript" .

All other characters are allowed!

Then too can't we bypass it !?