

# Forum:[Hack Forums](#)

Thread: [\[TUT\]XSS - cross site scripting\[TUT\]](#)

SQLfang - November 4, 2011, 9:00 pm

So today im going to teach you a vulnerability called XSS or cross site scripting.  
Ill only be teaching persistent XSS today.

what is XSS?

XSS is a common vulnerability in things like search bars  
comment boxes and even guest books! The biggest thing that causes  
XSS vulnerability is....yes u guessed LAZY ASSES! People that did not bother  
to filter out things like ">","/,</ or poor php coding in search boxes and such

What can you do with XSS

You can deface, hijack cookies, and even redirect to a defacement!

the types of XSS

There are two types of XSS persistent and non persistent.

You will quickly learn that non persistent is a huge pain in the ass!

The payoff for non persistent can sometimes be good but involves getting a slave  
to click on something and when ive done it they usually dont click but when they do, you can  
use a cookie editor and change your cookie to theirs and log in as admin or  
as that user.

testing for XSS

To test for xss you have to add some Javascript into a search box.

So find a site with some type of search box and get ready to type.

Quote:<script>alert("XSS");</script>

Alright now we have found that this site is vulnerable because  
a javascript box popped up saying XSS

Defacing with persistent XSS

Ok, so weve found this site to be vulnerable and now we want to deface so we enter this code

Quote:<script>>window.location="http://www.yourdefacepage.com/index.html"; </script>

Well now youve deface a webpage and taught those LAZY programmers a lesson!

-SQLfang