

XSS injection

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. 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 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](#).

Walk Through

Step 1 : Go to the feedback page

42

HOME SURVEY MEMBERS

FEEDBACK

Name *

Message *

SIGN GUESTBOOK

Name : wil

Comment : This is the best site EVER

f t i

© BornToSec

Step 2 : Enter the XSS injection (the website is broken so typing script work)

42

HOME SURVEY MEMBERS

FEEDBACK

Name *

Message *

[SIGN GUESTBOOK](#)

Name : wit

Comment : This is the best site EVER

f t i

© BornToSec

Step 3 : we got the flag !

Fil d'actualité | LinkedIn × BornToSec - Web Section × +

← → ↻ 192.168.56.101/?page=feedback ☆

HOME SURVEY MEMBERS


FEEDBACK

Name *

Message *

SIGN GUESTBOOK

THE FLAG IS : 0FBB54BBF7D099713CA4BE297E1BC7DA0173D8B3C21C1811B916A3A86652724E



Name : alert("hello world")
Comment : coucou

Name : wit
Comment : This is the best site EVER

How to fix :

- Modern framework take care of injection in a built in way
- You can escape problematic char in php for example you can use the `htmlspecialchars()` function