What is XSS?

XSS uses the website as the attack vector to inject code into a different user's browser

Typically used to steal users cookies or session tokens, modify/redirect the page for phishing

Uses the <script> tag to execute your code on the website you are attacking

Types

Reflected XSS (Non-persistent)

Stored XSS (Persistent)

What is Reflected XSS?

If you can get persistence, all other users who visit that website will have your code executed.

Deadly with link shortening

Can be used to test which fields lack filtering