Cross-Site Scripting (XSS)

El Cross-Site Scripting (XSS) és una vulnerabilitat web molt comuna. Afecta moltes aplicacions i pot tenir conseqüències greus. Veurem què és, com funciona i com prevenir-lo.

Què és el XSS?

Infiltració de codi

El XSS permet que codi maliciós s'infiltri en pàgines web legítimes. Aprofita la manca de control en l'entrada d'usuaris.

Modificació de contingut

Aquest codi pot alterar la pàgina web o accedir a informació sensible. Actua en nom de l'usuari afectat.

Abast ampli

Afecta a tot tipus d'aplicacions web, des de blogs fins a xarxes socials. La seva prevalença el fa especialment perillós.

Com funciona el XSS?

1

Entrada d'usuari

Un usuari introdueix dades en un formulari web, com un comentari en un blog.

2

Falta de filtratge

La web no valida ni filtra adequadament aquesta entrada, permetent la inserció de codi.

3

Execució del codi

Quan altres usuaris visiten la pàgina, el codi maliciós s'executa en els seus navegadors.

Tipus de XSS

XSS reflectit

El codi maliciós es troba en la resposta immediata d'una sol·licitud. Sovint en enllaços manipulats.

XSS emmagatzemat

El codi s'emmagatzema en la base de dades del lloc. S'executa cada vegada que es carrega la pàgina.

XSS basat en DOM

Afecta directament el navegador. El codi es manipula des del client, no des del servidor.

Exemple pràctic de XSS reflectit

1

URL maliciosa

Un atacant crea un enllaç amb codi JavaScript incrustat a la URL

2

Clic de l'usuari

L'usuari fa clic a l'enllaç, enviant la sol·licitud al servidor web.

3

Execució del codi

El servidor retorna la pàgina amb el codi maliciós, que s'executa al navegador.

Impacte dels atacs XSS

Suplantació d'identitat

L'atacant pot actuar en nom de l'usuari, accedint a comptes personals.

Robatori de dades

Pot capturar contrasenyes, números de targeta de crèdit i altra informació sensible.

Desfiguració web

Pot alterar l'aparença i funcionalitat de la pàgina web afectada.

Detecció i prevenció de XSS

Mètode	Descripció
Eines d'anàlisi	Utilitzar Burp Suite o similars per escanejar vulnerabilitats.
Filtrar entrades	Validar i netejar totes les dades introduïdes pels usuaris.
Codificar sortides	Assegurar que les dades es mostren com a text, no com a codi.
Polítiques de seguretat	Implementar Content Security Policy (CSP) per limitar l'execució de scripts.