UXSS - what it is, why it’s dangerous, and simple steps to stay safe

Gridinsoft Help Center

What it is

UXSS (Universal Cross-Site Scripting) is a browser bug that lets bad code run inside your browser, not just on one weak website. When this happens, the code can ignore the normal rule that keeps one site from peeking at another. Result: many tabs - even trusted ones like email or banking - can be affected.

Why it matters

If attackers run code in your browser, they can read pages you open, steal your login cookies, change forms, or send you to fake logins. One flaw can put several accounts at risk at the same time.

How it works

- Break the wall: a bug in the browser or an extension skips the "sites stay separate" rule.
- Run code: a script executes in your tab.
- Cross over: it reads or edits other pages you have open.
- Steal: it grabs tokens/cookies or changes what you submit.

Red flags

- Trusted pages show weird pop-ups or fill in forms by themselves.
- You get redirected or logged out/in without clicking.
- Your password manager won’t autofill on a page that looks normal.
- A new/updated extension asks for extra, broad permissions.

Do it right

- Update now: keep your browser and OS on auto-update.
- Limit extensions: install only what you need; remove unknown ones; review permissions.
- Separate profiles: don’t mix risky browsing with banking/email in the same profile.
- Harden logins: turn on MFA; use a password manager.
- If it feels off: close tabs, disable recent extensions, clear site data, restart the browser - try another browser until fixed.