XSS (Cross-Site Scripting)

Gridinsoft Help Center

What it is

XSS is a web bug where attackers make a site run their script in your browser. That script can read what you see, steal session cookies, change forms, or redirect you to fake pages. It shows up in a few flavors (reflected, stored, DOM-based), but the idea is the same: untrusted input becomes active code. More info: https://gridinsoft.com/xss

Why it matters

If a script runs in your session, it can act as you - grab logins, send messages, or change account settings without your click.

How it works - quick tour

- Inject: attacker slips script into a link, comment, profile, or search box.
- Render: the site doesn’t sanitize it and sends it to browsers.
- Execute: your browser runs the code as if it came from the site.
- Abuse: the script steals cookies/tokens, rewrites the page, or sends data out.

Red flags

- A link with odd parameters like <script>, onerror=, or data that looks like code.
- Pages that suddenly auto-fill or show pop-ups that don’t match the site’s style.
- You click a site link and get instantly redirected through strange domains.
- Your password manager won’t autofill on a page that looks normal.

Do it right

- Don’t click weird tracking-looking links from DMs or comments; open the site from your bookmarks.
- Log out and back in if a page looks tampered; clear site data for that domain.
- Turn on a password manager and MFA - they limit damage if a session is stolen.
- Keep your browser and extensions updated; remove extensions you don’t need.
- If you run a site: validate/escape user input and use Content Security Policy (CSP).