

What are browser cookies, and how do attackers abuse them?

Short answer: Cookies are small pieces of data a website stores in your browser, and some of them are authentication cookies that keep you logged in. Stealing those is functionally equivalent to stealing an active session — the attacker can load them into their own browser and appear to be you.

Not all cookies matter equally

- **Preference cookies** — language, theme, layout. Low value.
- **Analytics cookies** — usage measurement. Low value.
- **Authentication / session cookies** — prove you're logged in. **High value.**

Attackers care almost exclusively about the third category.

Why cookie theft is effective

A stolen authentication cookie usually doesn't trigger a login event, a password prompt, or an MFA challenge. The session already exists; the attacker is simply presenting proof of it. From the application's perspective this looks like ordinary continued activity.

Browsers store cookies in known, predictable file locations on every operating system, so automated tools can locate them without knowing anything about the specific machine.

Why the browser is a focal point

The browser holds cookies, saved passwords, OAuth tokens, and history in one place, which makes it the single richest identity target on most endpoints. Cyber Crucible has seen this directly: from Q4 2023 onward, automated responses against Chrome, Edge, and Chromium activity climbed from zero into the thousands, with related CVEs later published by Google and Microsoft.

Protection

Browser credential storage is one of the protected identity locations. A process attempting to read it is assessed in context — an exploited browser is treated very differently from a healthy one, and in neither case does an overreaching request receive the real cookie.

Revision #3

Created 2026-07-20 19:24:25 UTC by Dennis Underwood

Updated 2026-07-21 19:32:39 UTC by Dennis Underwood