Form-Based Authentication - What it is, how it works, and best practices to secure logins

Gridinsoft Help Center

What it is

Form-based authentication is the login box you see on most websites. A page asks for your username and password, then the app checks them and signs you in if they match.

How it works - quick tour

- You enter credentials in a web form and submit.

- The server verifies them and, if valid, creates a session (usually via a cookie).

- Your browser sends that session cookie with each request so the site knows you’re logged in.

Benefits

- Familiar and easy to implement

- Works across browsers and devices

- Can be upgraded with stronger protections

Common pitfalls

- Plain HTTP or weak TLS settings

- Storing passwords without proper hashing

- Session cookies not marked Secure and HttpOnly

- No protection against brute force or phishing

Best practices

- HTTPS everywhere - no exceptions

- MFA for important accounts

- Hash passwords with bcrypt/Argon2 and use per-user salts

- Rate limit and lock out brute-force attempts

- CSRF and XSS protections to keep sessions safe

- Set cookies: Secure, HttpOnly, and SameSite

- Offer passwordless or passkeys where possible