What is an authentication bypass?

An authentication bypass is any flaw that lets an attacker gain authenticated access without valid credentials, by exploiting logic errors, weak password resets, token tampering, or forced browsing rather than guessing a password. Examples include skipping a verification step, manipulating a JWT, abusing a predictable reset token, or reaching a protected page directly. It maps to OWASP's Identification and Authentication Failures, and the fix is enforcing authentication and authorisation server-side on every request.

HOW IT WORKS

01 How it works and common patterns

Bypasses take many shapes:

- Logic flaws: a multi-step flow that trusts a client-set "verified" flag, or an account-creation step reachable out of order.
- Forced browsing: navigating straight to `/admin` because access is only hidden in the UI, not enforced server-side.
- Token tampering: manipulating a JWT (alg confusion, weak secret) to forge an authenticated session.
- Weak password reset: predictable or leaking reset tokens, or host-header poisoning of the reset link.
- Response/parameter tampering: changing a `role=user` value or a redirect after a partial login.

Examples shown for defensive context.

> ENFORCE SERVER-SIDE
>
> *Most bypasses come down to a check that exists in the UI or client but not on the server. Authentication and authorisation must be enforced server-side on every request, never assumed from a prior step or a hidden link.*

HOW TO DEFEND

- Enforce authentication and authorisation server-side on every request, not just by hiding links.
- Validate every step of multi-step flows server-side; never trust client-set state like a "verified" flag.
- Use vetted authentication libraries and strong, correctly verified tokens (see JWT attacks).
- Harden password reset: unpredictable, single-use, expiring tokens; ignore attacker-controlled host headers.
- Add MFA for sensitive access and test the full authentication flow, including out-of-order and direct-access attempts.

SOURCES

[1] OWASP: Authentication

[2] MITRE CWE-287: Improper Authentication

[3] OWASP Top 10

Test your application for authentication flaws and 30+ other classes.

securelayer7.net/learn/application-security/authentication-bypass

Open online