Account Enumeration

Theresa Henze - 2026-08-28 - Miscellaneous

What is Account Enumeration?

Account enumeration is a type of security issue where someone can figure out whether a specific username or email address is registered on a website or app — even if they don't know the password.

A simple way to think about it

Imagine you try to log in to a site and enter an email address. If the site responds with:

- "Email not found" → you now know that account doesn't exist
- "Incorrect password" → you now know the account *does* exist

That difference in responses lets someone "probe" the system and build a list of valid accounts. That's account enumeration.

Why it's a problem

On its own, it might not seem serious—but it creates a foundation for more harmful attacks:

- **Targeted hacking attempts**: Attackers can focus only on real accounts instead of guessing blindly
- **Password attacks**: Once valid accounts are known, they can try common or leaked passwords
- **Privacy risks**: Someone could check if a person is registered on a specific platform (e.g., a dating site or medical service)
- **Phishing**: Knowing an email is valid makes scam messages more convincing

How it usually happens

Account enumeration often occurs through small clues in how a system behaves:

- **Different error messages** during login ("user not found" vs "wrong password")
- **Password reset forms** that confirm whether an email exists
- **Signup pages** that say "this email is already registered"
- **Timing differences** (responses take longer when an account exists)

Attackers often automate this process, trying thousands or millions of possible emails or usernames very quickly.

TLDR

Account enumeration is like checking which names are on a guest list before trying to sneak into a party. It doesn't break in by itself — but it makes breaking in much easier.