Account Enumeration

Theresa Henze - 2026-08-28 - Verschiedenes

Was ist Account Enumeration?

Account Enumeration ist ein Sicherheitsproblem, bei dem jemand herausfinden kann, ob ein bestimmter Benutzername oder eine E-Mail-Adresse auf einer Website oder in einer App registriert ist – selbst ohne das Passwort zu kennen.

Einfach erklärt

Stell dir vor, du versuchst dich auf einer Website anzumelden und gibst eine E-Mail-Adresse ein. Wenn die Seite unterschiedlich reagiert:

- „E-Mail nicht gefunden“ → du weißt, dass das Konto nicht existiert
- „Falsches Passwort“ → du weißt, dass das Konto existiert

Dieser Unterschied ermöglicht es, das System zu „testen“ und eine Liste gültiger Konten zu erstellen. Das nennt man Account Enumeration.

Warum ist das ein Problem?

Allein wirkt das vielleicht harmlos – aber es ist oft der erste Schritt für größere Angriffe:

- **Gezielte Angriffe**: Angreifer konzentrieren sich nur auf echte Konten
- **Passwort-Angriffe**: Bekannte Konten können mit häufigen oder geleakten Passwörtern getestet werden
- **Datenschutzrisiken**: Man kann prüfen, ob jemand bei bestimmten Diensten registriert ist (z. B. Dating- oder Gesundheitsplattformen)
- **Phishing**: Betrugsversuche werden glaubwürdiger, wenn die E-Mail-Adresse bestätigt ist

Wie passiert das typischerweise?

Account Enumeration entsteht oft durch kleine Hinweise im Verhalten eines Systems:

- **Unterschiedliche Fehlermeldungen** beim Login („Benutzer nicht gefunden“ vs. „Falsches Passwort“)
- **Passwort-zurücksetzen-Formulare**, die bestätigen, ob eine E-Mail existiert
- **Registrierungsseiten**, die sagen „Diese E-Mail ist bereits registriert“
- **Zeitunterschiede** bei Antworten (bestehende Konten brauchen länger zur Verarbeitung)

Angreifer automatisieren diesen Prozess häufig und testen sehr viele mögliche E-Mail-Adressen oder Benutzernamen in kurzer Zeit.

TLDR

Account Enumeration ist so, als würde man vor einer Party prüfen, welche Namen auf der Gästeliste stehen. Es ist kein Einbruch an sich – macht es aber deutlich einfacher.