Ako testovať dvojfaktorovú autentifikáciu (2FA) (nielen v bankovníctve)

**1. Overenie toku autentifikácie:**

* Je 2FA aktivovaná po zadaní správnych prihlasovacích údajov?
* Dostane používateľ výzvu na zadanie kódu (napr. SMS, e-mail, mobilná appka)?

**2. Správnosť a jedinečnosť kódu:**

* Kód je jedinečný pre každé prihlásenie?
* Platí len obmedzený čas (napr. 5 minút)?
* Čo sa stane po jeho uplynutí?

**3. Chybové stavy a pokusy o zneužitie:**

* Zadanie nesprávneho kódu – koľko pokusov je povolených?
* Ošetrenie opakovaných neúspešných pokusov – je účet zablokovaný?
* Zobrazujú sa zrozumiteľné a nie príliš konkrétne chybové hlásenia?

**4. Viacero spôsobov overenia:**

* Funguje aj alternatívna metóda (napr. mobilná appka pri nedostupnosti SMS)?
* Je možné zmeniť preferovaný spôsob 2FA?
* Otestovať obnovu/stratu zariadenia: čo ak používateľ stratí telefón?

**5. Scenáre pre rôzne zariadenia a siete:**

* Funguje overenie rovnako cez desktop, mobil, rôzne OS a prehliadače?
* Čo sa stane, ak používateľ prepne sieť (napr. Wi-Fi → mobilné dáta) počas overovania?

**6. Používateľská skúsenosť:**

* Je proces zrozumiteľný aj pre menej technických používateľov?
* Nie je 2FA zbytočne zdržujúce pri častom prihlasovaní?

**7. Bezpečnosť a logovanie:**

* Sú pokusy o 2FA zaznamenané v logoch?
* Zobrazí sa používateľovi upozornenie pri prihlásení z nového zariadenia?

Ak testujete bezpečnostné prvky ako 2FA, nezabúdajte: nejde len o to, či **funguje**, ale či je **odolné voči zneužitiu**, **dostatočne rýchle** a zároveň **zrozumiteľné pre koncového používateľa**.

**#AkoTestovať #Bezpečnosť #2FA #Fintech #Testovanie #QA #SecurityTesting #Bankovníctvo #TesterskýTip #SoftvérovéTestovanie #TestovanieAplikácií**