Ako testovať obmedzenie prístupu k citlivým údajom (napr. zostatky, výpisy, IBANy)

Predstav si, že si tester v banke a máš za úlohu overiť, že bežný zákazník nemá prístup k údajom iného klienta. V praxi to znamená, že ak sa prihlásim ako používateľ A, nesmiem vidieť zostatky, IBANy ani výpisy používateľa B – a naopak.

V jednej firme, kde som testovala, sa stalo, že backend posielal viac údajov, než bolo potrebné. Frontend síce zobrazoval len povolené dáta, ale systém posielal aj iné. Tester si to všimol pri kontrole komunikácie medzi aplikáciou a serverom – teda pri štandardnej validácii, ktorú robíme, aby sme sa uistili, že aplikácia neodhalí informácie navyše. Tento príklad ukazuje, že bezpečnosť musí byť riešená už na úrovni backendu, nie len skrytím na obrazovke.

**Ako otestovať obmedzenie prístupu k citlivým údajom:**

1. **Testuj s viacerými rolami**

* Over, že zákazník vidí len svoje dáta.
* Manažér má prístup len k účtom svojich podriadených.
* Admin má len tie oprávnenia, ktoré sú skutočne potrebné.

1. **Priame volanie API**

* Skús zavolať endpoint s iným ID účtu alebo klienta.
* Očakávaj chybovú hlášku alebo prázdnu odpoveď, nikdy nie dáta iného používateľa.

1. **Manipulácia s URL**

* Ak aplikácia používa URL s parametrami (napr. /account/1234), skús ich manuálne zmeniť.
* Dáta iného používateľa sa nesmú zobraziť.

1. **Testovanie prístupových tokenov**

* Použi token jedného používateľa pre dopyt na účet iného.
* Backend musí prístup odmietnuť.

1. **Kontrola logov**

* Over, že v logoch sa neukladajú celé čísla účtov alebo IBANy v čitateľnej podobe.
* Citlivé údaje majú byť maskované alebo anonymizované.

1. **Negatívne scenáre**

* Skús prístup bez prihlásenia.
* Skús prístup s expirovaným tokenom.
* Over, že systém vráti bezpečnú chybu (napr. 401 Unauthorized, 403 Forbidden).

1. **Regresné testy**

* Po každej zmene backendu alebo oprávnení zopakuj testy, aby sa neotvorili nové bezpečnostné diery.

Dostupnosť citlivých údajov je jedným z najkritickejších miest v bankovníctve a financiách. Jedna chyba môže znamenať únik dát, pokuty a stratu dôvery klientov. Preto je dôležité testovať prístupové obmedzenia systematicky a nielen „kliknutím cez UI“.

**#softwaretesting #securitytesting #QA #banking #testovanie**