Ako testovať systém, kde sa menia práva používateľa?

Zmeny roly môžu výrazne ovplyvniť, čo používateľ vidí, čo môže robiť a čo má zakázané. A práve to je výzva pre testerov.

**Príklad zo života:**  
Máme interný systém, kde môže byť používateľ **zamestnancom**, **manažérom** alebo **adminom**. Každá rola má iné oprávnenia – napríklad zamestnanec môže vidieť len svoje dáta, manažér údaje svojho tímu a admin všetko vrátane nastavení systému.

**Na čo sa zamerať pri testovaní zmien rolí a oprávnení?**

1. **Správna dostupnosť funkcií**  
   ▫️ Po zmene roly sú dostupné len funkcie prislúchajúce danej roli?  
   ▫️ Nezostali aktívne žiadne “zakázané” tlačidlá?
2. **Skryté vs. zakázané akcie**  
   ▫️ Je rozdiel medzi tým, čo je skryté (nevidno) a čo je zakázané (vidno ale nefunguje)?  
   ▫️ Vie sa používateľ pomocou priameho linku dostať k akcii, ktorú by nemal?
3. **Zmena počas relácie**  
   ▫️ Čo sa stane, keď sa rola zmení počas toho, ako je používateľ prihlásený?  
   ▫️ Zmení sa UI dynamicky, alebo sa musí znovu prihlásiť?
4. **Roly vs. údaje**  
   ▫️ Zobrazujú sa len tie dáta, ktoré daná rola smie vidieť?  
   ▫️ Nedá sa pomocou filtrov či API vytiahnuť niečo, čo by nemalo byť dostupné?
5. **Audity a logovanie**  
   ▫️ Zaznamenáva sa, kto a kedy zmenil rolu?  
   ▫️ Dá sa dohľadať, aké oprávnenia boli pridelené a odstránené?
6. **Regresné testovanie pri každej zmene práv**  
   ▫️ Over, či nová úroveň prístupu nezrušila predchádzajúce funkčnosti  
   ▫️ Spusti testy opakovane po zmene konfigurácie rolí

Zmena oprávnení je citlivá vec – malá chyba a systém môže byť nechtiac zneužiteľný. Pri testovaní práv je potrebné mať oči otvorené **nielen pre UI**, ale aj pre **backendové volania, API a dáta.**

#testing #securitytesting #rolesandpermissions #QA #softwaretesting #manualtesting #testovanie #testautomation