Ako testovať prístupové oprávnenia cez backend alebo API  
(áno, aj 401 ≠ 403)

Predstavte si interný systém na správu podujatí – organizátori môžu pridávať eventy, upravovať detaily alebo pozývať účastníkov. Dobrovoľníci majú prístup len na čítanie. A bežní používatelia môžu vidieť len verejné podujatia. Všetko beží cez REST API.

Ako otestovať, že oprávnenia fungujú správne?

**Čo všetko treba otestovať:**

1. **Autorizácia vs. autentifikácia**
   * **401 Unauthorized**: nedodaný alebo neplatný token → používateľ nie je prihlásený
   * **403 Forbidden**: token je platný, ale používateľ nemá práva na danú akciu
2. **Rôzne úrovne oprávnení**
   * prihlásený organizátor môže POST /events, PATCH /events/:id
   * dobrovoľník môže len GET /events
   * anonymný používateľ môže len GET /events?public=true
3. **Neplatné tokeny alebo chýbajúce hlavičky**
   * token s preklepom alebo expirovaný → očakávaj **401**
   * žiadny token → **401**
   * token iného používateľa → **403**, ak má práva inde
4. **Zmena rolí počas relácie**
   * zmena práv by sa mala prejaviť okamžite alebo po relogine – otestuj oba prípady
5. **Cross-role útoky**
   * napr. dobrovoľník skúsi zmeniť detail eventu → **403**
   * bežný používateľ sa pokúsi získať zoznam všetkých e-mailov → **403**
6. **Prístup k neexistujúcim alebo cudzím záznamom**
   * GET /events/99999 (neexistujúce ID) → **404**
   * GET /events/5 (ak patrí inej organizácii) → **403** alebo **404** (podľa politiky)
7. **Či sú tokeny viazané na IP alebo User-Agent**
   * niektoré systémy vyžadujú tokeny len z rovnakého zariadenia – over
8. **Ošetrenie zneužitia**
   * príliš veľa 401/403 za krátky čas → test rate limiting alebo blokovanie
9. **Záznam v logoch alebo auditných stopách**
   * pokusy o neoprávnený prístup by mali byť zaznamenané
10. **Automatizované testy**

* odporúča sa vytvoriť sadu testov pre rôzne role + pozitívne aj negatívne scenáre

**Bonus**: Testuj aj cez rôzne frontend klienty – web, mobil, CLI – každý môže posielať hlavičky trochu inak.

Dobré testovanie oprávnení je o *hraniciach* – kto má čo vidieť a robiť. A hlavne, čo nemá.

**#APItesting #BackendTesting #Authorization #AccessControl #SecurityTesting #TesterNaLinkedIne**