UPB  
Zadanie 3 – Autentifikácia

Riešitelia: Emília Čurillová, Filip Harvančík, Lenka Puškášová

**Úloha1(Lenka)**

* **Komplexita** –
  + komplexita hesiel nebude kontrolovaná – uživatelia majú tendenciu vymýšľať viac predikovateľné heslá ak sú nútení držať sa LUDS odporúčania – vtedy bude minimálna dĺžka 15
  + komplexita sa bude držať LUDS composition policy, vtedy bude minimálna dĺžka hesla 8 Zdroje

Odporúčania pre dĺžku a komplexitu hesla  
<https://www.strongdm.com/blog/nist-password-guidelines>

**Úloha2 ()**

**Úloha 3 (Emília)**

**Account Lockout (Zamknutie účtu)** - po 5 neúspešných pokusoch o prihlásenie sa používateľský účet dočasne zamkne na 15 minút.

* Databázová tabuľka users obsahuje stĺpce:
  + failed\_login\_attempts - počítadlo neúspešných pokusov
  + last\_failed\_login - čas posledného neúspešného pokusu
  + account\_locked\_until - čas, kedy sa účet odomkne
* Pri každom neúspešnom prihlásení sa inkrementuje failed\_login\_attempts, aktualizuje last\_failed\_login a ak failed\_login\_attempts >= 5, tak sa nastaví account\_locked\_until = teraz + 15 minút
* Pri kontrole prihlásenia sa skontroluje, či account\_locked\_until > aktuálny čas. Ak áno, používateľ vidí odpočítavanie so zostávajúcim časom. Po uplynutí lockout-u sa účet automaticky odomkne
* Automatický reset: Ak používateľ neskúšal prihlásiť viac ako 1 hodinu, počítadlo sa resetuje na 0 aby sa **predislo...**

**IP Rate Limiting (Obmedzenie pokusov z IP adresy)** - Maximálne 10 neúspešných pokusov o prihlásenie z jednej IP adresy za 15 minút.

* Databázová tabuľka login\_attempts zaznamenáva každý pokus:
  + Ip\_address - IP adresa klienta
  + timestamp - čas pokusu
  + success - či bol pokus úspešný (True/False)
* Pri každom pokuse o prihlásení:
  + Funkcia get\_recent\_attempts() spočíta neúspešné pokusy z danej IP za posledných 15 minút
  + Ak počet >= 10, prihlásenie sa zamietne s hláškou "Too many login attempts from your IP"
  + Po 15 minútach sa staré pokusy už nezapočítavajú (automatické "zabudnutie")
* Získavanie IP adresy podporuje proxy servery (X-Forwarded-For header)

**Auditovanie a Cleanup** - Každý pokus o prihlásenie sa zaznamenáva do databázy a staré záznamy sa automaticky čistia.

* Každý login pokus (úspešný aj neúspešný) sa uloží do login\_attempts
* Periodický cleanup sa spúšťa náhodne (každých 1000 requestov) a vymaže záznamy staršie ako 7 dní

Anti User Enumeration - Útočník nemôže zistiť, či používateľské meno existuje alebo nie.

* Rovnaká chybová hláška pre neexistujúceho používateľa aj zlé heslo

**Úloha 4 (Lenka)**

* **Slovníková kontrola hesla** – kontroluje sa, či heslo sa nenachádza v databáze kompromitovaných hesiel

Pri registrácii sa heslo lokálne hashuje pomocou SHA-1 a pošle sa len prvých 5 znakov hashu na HIBP (Have i been pwned) range API (https://api.pwnedpasswords.com/range/{prefix}). API vráti zoznam zvyšných suffixov a počty výskytov; ak sa lokálny suffix zhoduje s niektorým z odpovede, heslo je kompromitované a odmietne sa. Tento prístup používa **k-anonymitu**, takže server HIBP nikdy nevidí celé heslo ani celý hash

API pre kompromitovane hesla  
<https://haveibeenpwned.com/api/v3#:~:text=stealer%20logs%20APIs.-,Pwned%20Passwords,-Overview>