Zadanie 3 (Autentifikácia)

October 14, 2024

Cieľom zadania je oboznámiť sa so základnými princípmi autentifikácie vo webových aplikáciach (t.j. prihlasovanie, overovanie hesiel, bezpečné ukladanie hesiel do databázy a pod.). V rámci tohto zadania budete dopĺňať funkcionalitu do jednoduchého web servera. Kostra je dostupná v súbore **zadanie_3.zip**. Podobne ako v predchádzajúcom zadaní, samotný webserver je implementovaný v jazyku Python prostredníctvom knižníc *Flask* [1] (jednoduchý framework na implementáciu webservera), *SQLAlchemy* [3] (rozšírenie pre Flask na podporu databáz), *Flask-Login* [2] (manažment pre používateľské relácie) a *FlaskWTF* [4] (podpora pre formuláre). Knižnice je možné nainštalovať pomocou príkazu:

```
pip install flask flask-sqlalchemy flask-wtf flask-login
```

Po spustení programu bude webový server bežať na adrese **127.0.0.1** a porte **1337**. Samotný server obsahuje tri stránky (a testovacieho používateľa s menom a heslom *test*):

- **login.html** - stránka na prihlasovanie, používateľ zadáva meno a heslo. Po správnom prihlásení pre presmerovaný na stránku **home.html**. Zo stránky je možné sa presmerovať na registračný formulár.
- **register.html** - stránka na registráciu používateľov. Používateľ zadáva meno a heslo (dvakrát). Zo stránky je možné sa presmerovať na stránku **login.html**.
- **home.html** - domovská stránka. K tejto stránke sa by sa mal dostať iba registrovaný používateľ po zadaní správneho mena a hesla. Stránka umožňuje odhlásiť používateľa.

Úlohy:

1. Implementujte kontrolu zložitosti hesla pri registrácii tak, aby umožnilo používateľom zadať iba heslo, ktoré spĺňa určité bezpečnostné štandardy. **Kritéria požadované na heslá popíšte a zdôvodnite**.

2. Implementujte bezpečné ukladanie používateľských hesiel do databázy. **Systém bezpečného ukladania hesiel popíšte a zdôvodnite**. Poznámka: na implementáciu použite vybranú kryptografickú knižnicu a systém implementujte pomocou jednotlivých primitív; používanie knižníc, ktoré ponúkajú hotovú funkcionalitu je **zakázané**.

3. Implementujte ochranu voči *brute-force* útokom na prihlasovanie (t.j. útočník skúša rôzne heslá pri prihlasovaní). **Ochranu popíšte a zdôvodnite**.

4. Implementujte ochranu voči slovníkovým heslám pri registrácii tak, aby používateľom nebolo umožnené sa registrovať s heslami typu *heslo* alebo *123456*. Poznámka: v prípade príliš veľkej databázy slovníkových hesiel danú databázu neodovzdávajte do AISu ale iba uveďte link v dokumentácii).

Deadline zadania je **29.10.2024** o **13:37**. Zadanie sa odovzdáva do **akademického informačného systému** (AIS) do zvoleného miesta odovzdania. Odovzdáva sa dokumentácia vo formáte **PDF** (!!!) a adresárová štruktúra projektu (okrem databázy a prípadného virtualného prostredia pre Python). Odovzdáva **jeden** člen z tímu.

Literatúra

[1] Flask. `https://flask.palletsprojects.com/en/3.0.x/`.

[2] Flask-login. `https://flask-login.readthedocs.io/en/latest/`.

[3] Flask-sqlalchemy. `https://flask-sqlalchemy.readthedocs.io/en/3.1.x/`.

[4] Flaskwtf. `https://flask-wtf.readthedocs.io/en/1.2.x/`.