# Bevezetés

Feladatunk egy olyan online áruház létrehozása, amiben egyedi formátumú animált képeket lehet böngészni. A webshoppal szembeni elvárás, hogy a felhasználók és az adminisztrátorok egyaránt tudják használni. A rendszertől az alábbi feladatok támogatása elvárt:

* A felhasználók számára elérhetővé váljanak az egyes funkciók a regisztrálás után.
* Az adminisztrátorok menedzselhessék az egyes felhasználók profilját és tevékenységét.

# Követelmények

A fejlesztés első lépése a funkcionális és a biztonsági követelmények meghatározása. Az egyeztetések után megállapítottuk a funkcionális követelményeket. Az eredményeket UML use case diagramok segítségével dokumentáltuk. A biztonsági követelmények meghatározásához a Threat, Risk, Vulnerability Analysis módszert használtuk.

## Funkcionális követelmények

Összeállítottuk a rendszerrel szembeni funkcionális követelményeket. A webshopnak kétféle felhasználója lesz (felhasználók, adminisztrátorok), így erre a két felhasználási esetre kell felkészíteni.

* A felhasználóknak lehetővé kell tenni az alábbi funkciókat: CAFF böngészése, keresése, feltöltése és vásárlása, kommentelés, regisztráció, bejelentkezés, adataik módosítása.
* Az adminisztrátoroknak az alábbi funkciók elérését kell lehetővé tenni: CAFF törlése, komment törlése és módosítása, felhasználó regisztrálása és törlése, felhasználó adatainak módosítása.

## Biztonsági követelmények és célok

Az online áruház felhasználókkal és adminisztrátorokkal kerülhet interakcióba. Ezek az interakciók bizalmi kéréseket vetnek fel, hiszen a viselkedésüket nem tudjuk kontrollálni. A webshop működéséhez a felhasználók adatait eltároljuk.

A biztonsági követelményeket hat nagy kategóriába soroljuk: CIA és AAA:

* Bizalmasság
* A felhasználók személyes adatait csak ők maguk, illetve az adminisztrátorok ismerhetik meg. Az adminisztrátoroknak biztosítva van a megismerhetőség.
* Az adminisztrátorok minden felhasználó adatait megismerhetik.
* Integritás
* A felhasználók csak a saját személyes adataikat módosíthatják.
* Csak adminisztrátorok jogosultak CAFF bejegyzése/kommentek törlésére.
* Csak adminisztrátorok törölhetnek felhasználót és módosíthatják más felhasználók adatait.
* Elérhetőség
* Az adminisztrátorok kérésre bármikor törölhetnek CAFF bejegyzéseket, regisztrálhatnak vagy törölhetnek felhasználókat, illetve módosíthatják adataikat.
* Autentikáció
* A felhasználók csak a regisztráció után jelentkezhetnek be.
* A felhasználók csak bejelentkezés után módosíthatják a felhasználói adataikat, tölthetnek le, illetve fel, vásárolhat és kommentelhetnek.
* Autorizáció
* A CAFF-ok feltöltése és letöltése, valamint a kommentelés szerepkörökhöz kötött tevékenység.
* A CAFF törlése, komment törlése, komment módosítása, felhasználó regisztrálása és törlése, valamint más felhasználó adataink módosítása szerepkörhöz kötött.
* Auditálás
* A felhasználók tevékenységét naplózni kell.

Ezek alapján meghatározhatjuk a biztonsági célokat. Célunk a biztonságos adattárolás, a felhasználói fiókok menedzselése, a szerepkör alapú hozzáférés-védelem és a naplózás.

## Threat assessment

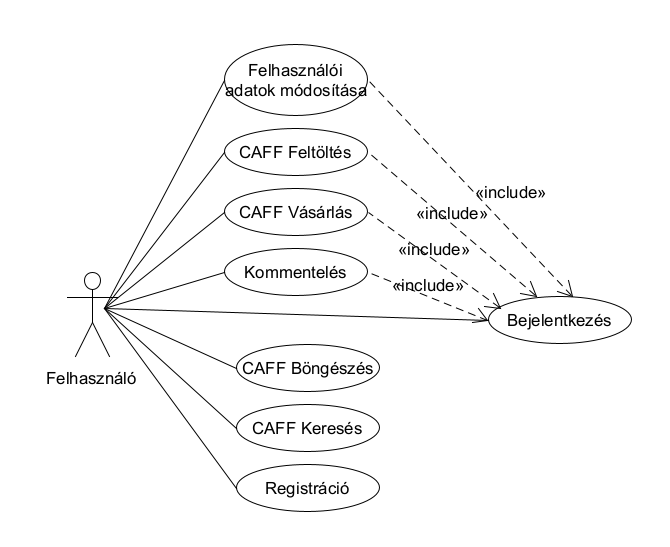
A threat assessmenr két részből áll, az assetek azonosításából és assetekre leselkedő veszélyek azonosításából. Az assetek megállapításához iteratívan kell elemeznünk a rendszer use case-eit, figyelembe véve a biztonsági követelményeket. Az azonosításhoz a STRIDE keretrendszert alkalmaztuk.

### Assetek megállapítása

A webshop komponenseinek részletezéséhez egyesével, iteratívan elemeznünk kell a use case-eket, így megállapíthatjuk az asseteket. A Threat, Risk, Vulberability Analysis során háromfajta assetet különítünk el:

* fizikai assetek
* emberi assetek
* logikai assetek

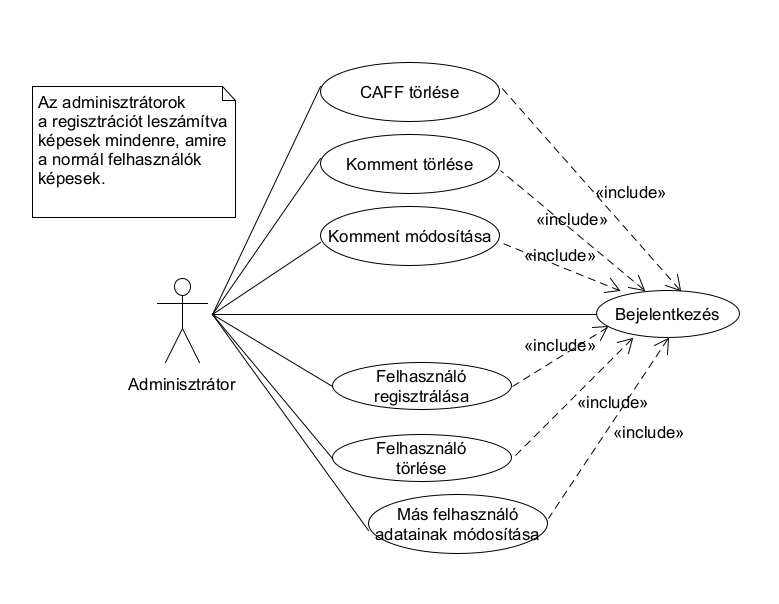
A felhasználók többfajta use case-ben jelennek meg: felhasználói adatok módosítása, CAFF feltöltése, CAFF vásárlása, kommentelés, CAFF böngészése, CAFF keresése, regisztráció és bejelentkezés. Ezeket az 1. ábra foglalja össze, ahol jól láthatóak az egyes tevékenységek közötti megkötések is. Adatok módosításához, CAFF feltöltéséhez, vásárlásához és kommenteléshez a felhasználónak előbb be kell jelentkeznie.

A use case-ek segítségével megállapíthatók a megvalósításukhoz szükséges assetek. Az üzemeltetéshez szükség van fizikai assetekre, szerverekre és fizikai gépekre. A szerverek pontos száma nagyban függ a felhasználók számától. A use case-ek alapján egyenlőre emberi assetként egyedül a felhasználó állapítható meg.

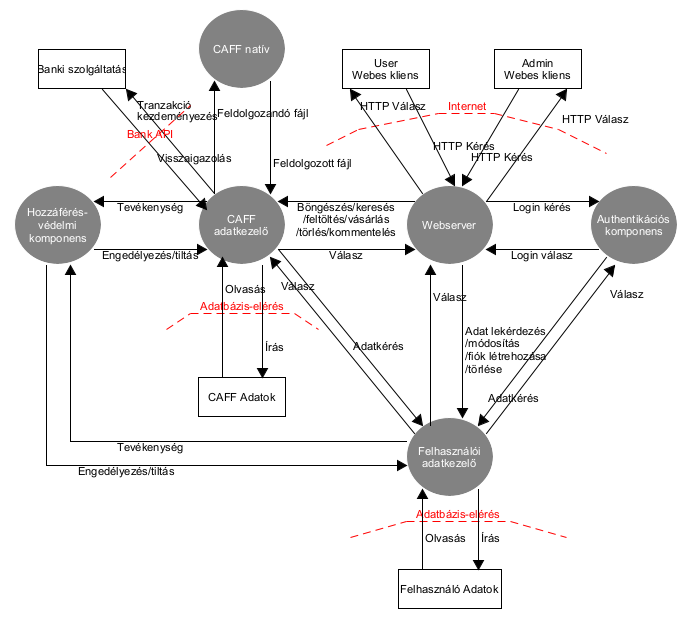
1. ábra Felhasználókhoz köthető use case-ek

A logikai assetek azonosításához végig kell gondolnunk az egyes use case-ek megvalósításához szükséges adatfolyamot. A webshopot böngészőben fogjuk megjeleníteni. Mivel egyes tevékenységek bejelentkezéshez kötöttek, ezért szükség lesz egy autentikációt megvalósító komponensre. Ennek szüksége van a felhasználók adataira, amit egy adatbázisban fogunk tárolni. A felhasználóknak biztosítani kell, hogy megnézhessék és módosíthassák a felhasználói adataikat. Szükséges egy hozzáférés-védelmi komponens beépítése is. Egy CAFF adatkezelő komponens fog felelni a fájlokkal kapcsolatos tevékenységekért. Köztük a vásárlásért, amihez szüksége van banki szolgáltatásra.

Az adminisztrátorok szintén többfajta use case-ben jelennek meg: CAFF törlése, komment törlése, komment módosítása, felhasználó regisztrálása, felhasználó törlése, más felhasználó adatainak módosítása. Ezeket az 2. ábra foglalja össze. Jól látható, hogy minden tevékenységhez be kell jelentkeznie az adminisztrátornak.

A use case-ket megvizsgálva egy új emberi asset állapítható meg, az adminisztrátor. Illetve a CAFF törlés új interakciót jelent a CAFF adatkezelővel, ezért ezt fel kell vennünk az oda érkező lehetséges kérések közé. Új elemnek számít a komment törlése és módosítása, valamint a felhasználó törlése. Az asseteket összefoglaló adatfolyam a 3. ábrán látható.

2. ábra Adminisztrátorokhoz köthető use case-ek



3. ábra Adatfolyam