Követelmény specifikáció

**A rendszerről röviden**

Az online rendszerünk felületet biztosít a járművek, ezen belül autók illetve motorok kölcsönzésére magánszemélyeknek különböző árakért, attól függően, hogy milyen járművet bérelnének mennyi időre.   
A járművek bérléseinek a költségeit **három árkategóriába** sorolhatjuk. Egy adott motor vagy autó igénybe vétele **1-7 napig** tartó időintervallumban a legdrágább, ez az első árkategóriába kerül, ezen felül lehetőség van **8-30 napig** tartó használatra (második árkategória), illetve **31-365 napig** is kikölcsönözhetjük, itt számoljuk fel a legkevesebb napidíjat. (pl.: a Mercedes CLA 220 napidíja az első árkategóriában 12190 Ft, a másodikban 10390 Ft, amíg a harmadikban 8290 Ft).

A rendszer **biztonsági és funkcionális hibákat** tartalmaz, ezek szemléltetésére alkalmas.

Az oldalra történt sikeres regisztrációt követően, és az azt követő belépés után van lehetőség a felhasználók számára a járművek kikölcsönzésére, ahol megadhatják, hogy mettől meddig szeretnék használni a kiválasztott autót vagy motort. A **tankolási költség a kölcsönző felet terheli**.

A regisztráció során kötelező megadni a lakcím adatokat, születési adatokat, illetve a személyes adatokat, ide tartozik a vezeték-és keresztnév, személyi igazolvány szám, anyja vezeték-és keresztneve, illetve opcionális az email és a telefonszám megadása. A felhasználói adatok megadása is kötelező, ide tartozik a felhasználónév, illetve az ehhez tartozó jelszó.

A rendszerben megkülönböztetjük az admin, illetve a felhasználók jogosultságait.

*Admin(ok) jogosultágai:*

* Autók hozzáadása az adatbázishoz
* Motorok hozzáadása az adatbázishoz
* Autók, motorok kilistázása
* Járművek keresése az oldalon
* Regisztrált tagok adatinak a kilistázása
* Összes kikölcsönzött jármű kilistázása (a kikölcsönző féllel együtt)
* Járművek adatainak módosítása, törlése
* Hozzászólások törlése

*Felhasználók jogosultságai:*

* Autók, motorok listázása
* Regisztráció, belépés, kilépés, jelszó módosítása
* Járművek keresése az oldalon
* Járművek kikölcsönzése
* Felhasználó által kikölcsönzött járművek listázása
* Saját adatok listázása
* Hozzászólás/vélemény írása

**Adatbázis**

Az adatbázis hét táblából épül fel, ezek közé tartozik a felhasználók, a bejelentkezett személyek, a járműtípusok, a járműkölcsönzés, az autók, a motorok és a márkák számára létrehozott táblázatok.  
Mindegyik táblázat rendelkezik egy egyedi azonosítóval, amelyet a rendszer automatikusan generál pl.: a regisztrációnál az adott felhasználó számára.

A **felhasználók** táblázatban azok a személyek szerepelnek, akik sikeresen végrehajtották a regisztrációt, nekik lehetőségük nyílik a web-es rendszer használatára, az elérhető jogosultságoknak megfelelően. A felhasználók üzenetet írhatnak az adminnak, ha esetleges hibákról számolnának be, vagy kérdést intéznének az oldalt üzemeltetője felé, illetve megjegyzéseket írhatnak az egyes járművekhez.

A rendszerbe **bejelentkezett személyek** ideiglenesen szerepelnek ebben a táblázatban, kilépés esetén törlődnek ebből a táblázatból.

Az **autómárka** tábla egy oszlopot tartalmaz, az autó márkájának a nevét, ez a tábla kulcsa is egyben.

Az **motormárka** tábla egy oszlopot tartalmaz, a motor márkájának a nevét, ez a tábla kulcsa is egyben.  
  
Az **autókölcsönzés** tábla tartalmazza az adott felhasználó által kikölcsönzött autó, ezen felül tartalmazza a kölcsönzés kezdetét és végét is.

Az **motorkölcsönzés** tábla tartalmazza az adott felhasználó által kikölcsönzött motort, ezen felül tartalmazza a kölcsönzés kezdetét és végét is.

Az **autók** táblázat tartalmazza a gépkocsik adatait, beleértve a márkáját, az adott márka típusát, a kölcsönzés kezdetén a km/h állását, a szállítható személyek számát, az üzemanyag fajtáját, a tank méretét, a hengerűrtartalmat, az autó teljesítményét, állapotát, fogyasztását stb.

A **motorokat** is ezen adatok mentén jellemezhetők, ehhez a táblához tartozik még a munkaütem is, amelyet a személygépkocsiknál nem szerepel.

A **hozzászólások** táblában szerepel egy egyedi azonosító, amely automatikusan növekszik, a hozzászólást író felhasználó felhasználóneve, illetve egy dátum oszlop is, amely a hozzászólás írásának a dátumát jelzi másodpercre pontosan.

**Használhatóság**

Belépés után válnak elérhetővé a szolgáltatások, amely csak úgy történhet meg, ha előtte sikeresen regisztrált az adott személy.

A regisztráció során **egyedi felhasználónév** megadása kötelező, ha már foglalt a megadni kívánt név, akkor erről a rendszer egy hibaüzenetet küld.

Az **telefonszám megadása nem kötelező**, viszont az email-cím mező nem maradhat kitöltetlenül a regisztráció sorám.  
Ha sikeres a regisztráció, akkor a rendszer átirányítja a felhasználót a belépés oldalra, ahol adminként, vagy felhasználóként léphet be.  
Amennyiben adminként lép be, akkor autókat, motorokat adhat hozzá az adatbázishoz, ezeket törölheti vagy módosíthatja. Ezen felül megtekintheti a regisztrált tagokat és az online felhasználókat, valamint a hozzászólásokat is törölheti.

**Használhatóság**  
A rendszer felhasználóbarát, könnyen átlátható, kinézete minimalista.  
A fejlécben szerepelnek a fontosabb linkek, menüpontok. Az egyesek menüpontok esetén, ha az egeret ráirányítjuk, megjelennek további linkek legördülő lista formájában, ezen linkekre kattintva rákereshetünk egy adott járműre.  
A keresés menüpont esetén lehetőség van márkák, márka típusok keresésére.  
A regisztráció más oldalaknál a megszokott módon történik, elfelejtett jelszó esetén a rendszer üzenetet küldd a felhasználó email-címére. A belépéshez elegendő a felhasználónév és a jelszó.  
A rendszer tíz perc inaktivitás esetén kilépteti a felhasználót az oldalról az adatok védelme érdekében. A járművek táblázatosan jelennek meg, ezen belül a „Bérlés” gombra kattintva van lehetőség kölcsönzésre.

**Támogatottság**

A rendszer PHP nyelven íródott, az adatbázis kezelése PHP-be ágyazott MySQL kódokkal lett megvalósítva. A rendszer bármely böngészőből való megnyitásra alkalmas.

**Kinézet**

Az web-es rendszerben a kék szín dominál, és minden oldalon megjelenik ugyanaz a hat linkből álló fejléc, amelyek közé tartozik az „Autók”, „Motorok”, „Vélemény”, „Kezdőlap”, „Keresés”, „Profilom”.

Ha az egeret az Autók vagy Motorok fölé irányítjuk, akkor automatikusan megjelenik ezen linkek alatt egy legördülő lista, amely tartalmazza az adatbázisban szereplő járműveket. A fejléc görgetés hatására sem tűnik el a képernyőről, így lehetőség van ezek használatára még egy adott oldal alján is.   
A kezdőlapon az öt legújabb autó és motor jelenik meg táblázatos formában, minden fontos adattal együtt.  
Minden járműhöz tartozik egy kép, kattintásra ezek a képek nagyobb méretben is megjelennek.

A regisztrációs oldal alján, ha minden adatot kitöltöttünk, akkor a „Regisztráció”-ra kattintva véglegesíthetjük a műveletet, persze ha jelezzük előtte, hogy elolvastuk és elfogadtuk a felhasználói feltételeket.

**A rendszer hibái**A rendszer **egyaránt funkcionális és biztonsági hibákat** is tartalmaz, ezek bemutatására alkalmas.

A helyes megoldások /\* \*/ (kommentek) között találhatók az adott php file-ben.

**Biztonsági hibák:**1, A regisztráció során a program nem jelzi hibaüzenettel, hogyha a megadott jelszavak nem egyeznek meg. A megadott jelszavak lehetnek különbözőek, ennek ellenére is sikeresen lehet regisztrálni a rendszerbe.

2, Annak ellenére, hogy minden személy különböző személyi igazolványszámmal rendelkezik, a rendszer nem ellenőrzi ezt le, így egy már az adatbázisban szereplő személyi igazolványszámmal is sikeresen regisztrálhatunk.

3, Az e-mail cím megadásánál is hasonló hibával találkozhatunk. A rendszer nem ellenőrzi, hogy az adott email-cím szerepel-e már az adatbázisban, ezért ha egy olyan email-címet adunk meg, amely szerepel a felhasználó táblában, akkor sem ír ki a program hibaüzenet, és sikeresen regisztrálhatunk.  
  
4, A rendszer csak azt ellenőrzi, hogy az adott felhasználó szerepel-e már az adatbázisban, a felhasználóneveknek ugyanis különbözőnek kell lenniük, mert ez az adott tábla kulcsa, viszont foglalt email-cím, foglalt sz.i.g szám, valamint hibás jelszó megadásával is sikeresen végrehajthatjuk a regisztrációt. Az adatbázisban a jelszavak egyszerű szövegként jelennek meg, nem titkosítva (pl.: nem md5 hash-ként, amely egy 32 karakterből álló jelsorozat), így aki hozzáfér az adatbázis tartalmához, az láthatja a jelszavunkat. Ez az oka annak, hogy a belépésnél nem számít, hogy a jelszót kis-vagy nagybetűvel adjuk meg.  
pl a Hello szó md5-ként: 8b1a9953c4611296a827abf8c47804d7  
pl a hello szó md5-ként: 5d41402abc4b2a76b9719d911017c592  
Láthatjuk, hogy itt egy karakter különbözik(kis –és nagybetű), és mennyire különböző jelsorozattal jelennek meg.  
  
5, A belépés során a Jelszó mező típusa nem „password”, hanem egyszerű „text”, így látható lesz, hogy milyen jelszót használunk a belépés során.

6, Belépés előtt a rendszer nem engedi, hogy az url átírásával megnyissunk egy adott oldalt (pl index.php helyett fooldal.php), de ha beléptünk, aztán az url átírás már nem probléma, akár az admin oldalára is beléphetünk ezzel a módszerrel.  
  
7, Ha rákattintunk egy autó vagy motor kölcsönzésére, majd megadjuk a kölcsönzés kezdeti dátumát és a kölcsönzés végének a dátumát, akkor a rendszer nem ellenőrzi, hogy az adott autó vagy motor abban az időpontban már le van-e a foglalva vagy sem.(auto\_kolcsonzes.php, motorok\_kolcsonzese.php)  
  
8, Az árak egy input mezőben jelennek meg, melynek tartalmát átírva máris egy kedvezőbb áron kölcsönözhetjük ki a kívánt járművet.

9, A rendszer nem ellenőrzi, hogy egy évnél több időre kölcsönöztük-e ki a járművet, ennek ellenére is sikeresen végrehajthatjuk ezt a műveletet.  
  
10, A rendszer nem ellenőrzi, hogy az adott kezdeti, vagy kölcsönzés végének a dátuma múltbeli időpont vagy sem, pl.: ha kezdetnek egy 2015-ös dátumot adunk meg, akkor is sikeres lehet a jármű kibérlése. (helyes kód: auto\_kolcsonzes\_action.php)  
  
11, A program nem ellenőrzi, hogy a kezdeti dátum korábbi időpont-e a kölcsönzés végének az időpontjánál. Pl.: ha a kezdeti dátum: 2017-12-10, míg a kölcsönzés végének a dátuma 2017-12-09, a kölcsönzés sikeres lehet.  
  
12, Ha sikeresen kikölcsönöztünk egy autót, (vagy motort, de ebben a példában legyen autó) akkor a  
az auto\_kolcsonzes\_action.php url-jében megjelennek az aktuális kölcsönzés adatai,   
  
**Funkcionális** hibák közé tartozik a regisztráció alján szereplő jelölőnégyzet (Elolvastam és elfogadom a felhasználói feltételeket), amelyet a leírás alapján kötelező lenne bejelölni a sikeres regisztrációhoz, de ennek elmulasztása esetén sem jelez a rendszer hibát, a regisztráció ennek ellenére is sikeres.

**Funkcionális** hibák közé tartozik, hogy a rendszer nem ellenőrzi, hogy a regisztrálni kívánt személy  
rendelkezik-e jogosítvánnyal, illetve betöltötte-e a 18. életévét, (ugyanis születési dátumnak akár egy 2017-es dátumot is megadhatunk) ugyanis ha fiatalkorú, illetve nincs megfelelő kategóriájú jogosítványa, akkor nem bérelhetne járművet.  
  
**Biztonsági** hibák közé tartozik, hogy bármely url-t beírva megjelenik a kívánt oldal (pl.: ha az admin belép a rendszerbe, akkor a rendszer átnavigálja egy másik url-re, de ha ezt az url-t beírjuk, akkor nem kell tudni az admin jelszavát, sem a felhasználónevét, mégis megjelenik számunkra az a felület, amely csak az admin számára lenne elérhető belépés után.)

**Biztonsági** hibákhoz tartozik, hogy a **jelszavak nem titkosítottak**.  
  
A **rendszer nem véd** az SQL injection ellen. [[1]](#footnote-1)Az SQL injection egy olyan (általában webes alkalmazásokban megtalálható) sérülékenység, amelynek során a támadó képes az alkalmazás által lefuttatott SQL utasításba oly módon karaktereket beszúrni, hogy a beszúrt karakterek egy része már ne adatként, hanem SQL utasításként értelmeződjenek. A bejuttatott kódrészlet által a támadó képes lehet új rekordokat beszúrni, vagy akár az egész adatbázist letölteni. A forráskódban kikommentezve szerepel a helyes PHP kód ennek elkerülésére.  
  
[[2]](#footnote-2)A leggyakoribb ellenlépés az, hogy egész egyszerűen „escape-elik” a fejlesztők a "speciális",

SQL query-k metakaraktereiként ismert karaktereket (idézőjel, aposztróf, pontosvessző, mínuszjel stb.), ilyen pl.:

$felhasznalo\_nev = $mysqli->real\_escape\_string($felhasznalo\_nev);

Ez meglehetősen jó védelmet biztosít a legegyszerűbb SQL injection támadásokkal szemben.

1. http://sec2013.crysys.hu/blog/egy-halalos-injekcio/ [↑](#footnote-ref-1)
2. http://secblog.stratis.hu/2009/04/webalkalmazasok-biztonsagi-hibai-5-sql.html [↑](#footnote-ref-2)