

# Szakedolgozat

verzió 0.1

## Tartalomjegyzék

Bevezetés.....	4
Motiváció.....	4
A feladat.....	4
Felhasználói dokumentáció.....	6
A feladat.....	6
Fontosabb eszközök a megvalósításhoz.....	7
Teszt környezet.....	7
Hardware.....	7
Szoftver.....	7
Operációs rendszer.....	7
Python.....	7
Böngészők.....	8
JavaScript.....	8
Letöltés githubról.....	8
Installálás.....	9
Függőségek.....	9
Iptables-persistent.....	9
pip3.....	9
Python csomagok.....	10
Előkészületek.....	10
Linux service létrehozás.....	11
Konfigurálás.....	13
Konfigurációs változók.....	13
Konfigurációs opciók.....	13
Példa.....	15
Használat.....	16
Szerver oldal.....	16
./bin/server/rpd_server.sh.....	16
./bin/server/rpd_create_user.sh.....	16
./src/python/run_server.py.....	16
./src/python/create_user.py.....	16
Kliens oldal.....	17
Az oldal elérése.....	17
Bejelentkezés.....	20
A főoldal struktúrája.....	22
A főoldal gombjai.....	23

Fájl létrehozása menü.....	24
Fájl átnevezés.....	24
Txt/Phonebook fájl megnyitás.....	25
Txt fájl oldal struktúrája.....	26
Txt fájl létrehozása.....	27
Back menü: Visszalép a főoldalra Logout menü: Kijelentkezés File name mező: A fájl neve New password mező: A fájl jelszava New password again mező: A fájl jelszava még egyszer Create file gomb: Ez a gomb hozza létre a fájlt, meg fog jelenni egy üres fájl.....	27
A Create file gomb megnyomása után.....	27
Txt/Telefonkönyv fájl jelszóváltoztatás.....	29
Telefonkönyv fájl oldal struktúrája.....	31
Telefonkönyv kontakt.....	33
Telefonkönyv kontakt – Telefonszám módosítás.....	33
Telefonkönyv kontakt – Telefonszám hozzáadás.....	34
Telefonkönyv kontakt – Módosítás.....	34
Telefonkönyv – Új kontakt hozzáadása.....	35
Felhasználó létrehozása.....	36
Üzenetek megjelenítése.....	36
Hibaüzenetek.....	37
Lokális, kliens oldali hibák (LOCAL).....	37
Távoli, szerver oldali hibák (REMOTE).....	38
Fejlesztői dokumentáció.....	39
Megoldási terv.....	39
Adattárolás.....	39
Felhasználói adatok tárolása a szerveren.....	39
Felhasználó mappa generálása.....	39
Fájlnevek.....	40
Titkosított fájl (SecretFile).....	41
AESEncryptor formátuma.....	41
Txt fájl (.txt) formátuma.....	41
Telefonkönyv fájl (.phb) formátuma.....	41
Szerver oldal.....	42
Mappa és fájl struktúrájának áttekintése.....	42
Kliens oldal.....	44
Tesztelési terv.....	48
Előkészületek.....	48
1. eset: A szerver elindítása (black box).....	49
Elvárt eredmény.....	49
2. eset: Felhasználók létrehozása konzolból (black box).....	55
Elvárt eredmény.....	55
3. eset: Üresen hagyott mezők felhasználó létrehozása közben.....	57
Elvárt eredmény.....	57
4. eset: jelszó és jelszó még egyszer nem egyezik (CLI).....	57
Elvárt eredmény.....	57
5. eset: Létező felhasználó hozzáadása azonos jelszóval.....	58

Elvárt eredmény.....	58
6. eset: Létező felhasználó hozzáadása más jelszóval (cli).....	58
Elvárt eredmény.....	58
7. eset: Belépés hibás jelszóval (GUI).....	59
Elvárt eredmény.....	59
8. eset: Bejelentkezés valós felhasználókkal (GUI).....	59
Elvárt eredmény.....	60
9. eset: Felhasználó létrehozása (GUI).....	60
Elvárt eredmény.....	60
10. eset: Txt Fájl létrehozása.....	61
Elvárt eredmény.....	61
11. eset: Telefonkönyv fájl létrehozása.....	62
Elvárt eredmény.....	63
12. eset: Nézzük meg, hogy a szerveren tárolt adatok tényleg titkosak-e.....	64
A teszt közben létrejött felhasználók és fájlok.....	67
Felhasználók.....	67
Fájlok.....	67

# Bevezetés

## Motiváció

Jelen világunkban az információ érték, ezért gyakorlatilag mindenki visszaél vele.

Sajnos nem tudhatom azt, hogy az operációs rendszer, amit használok, mennyi információt gyűjt rólam, és mire használja fel. Ez nincs másképp az e-mail szolgáltatókkal, a különböző felhő alapú tárolókkal.

Nem tudhatom, hogy ha egy felhőben tárolom az adataimat, akkor vajon a Google, a Microsoft, a Facebook, az Apple vagy más cégek, akik ilyeneket szolgáltatnak, felhasználják-e őket. Ilyen szempontból mondjuk a megnevezettek még korrektek, mert az általános szerződési feltételeikben megfogalmazzák, hogy az adatainkat felhasználják.

Sajnos arra jelenleg nincs erőforrásom, hogy egy saját operációs rendszert írjak, vagy leellenőrizzek egy Linuxot, Open/Free BSD-t hogy vajon visszaél-e az adataimmal, így ezeknek el kell hinnem, hogy nem teszik. De tudok csinálni olyan programot, ami azt biztosítja számomra, hogy az adataimat a kliens oldalon titkosítva küldöm el a felhőbe, akkor a felhőben lévő cég nem tudhatja, hogy mik is voltak azok.

Így jött az ötlet, hogy először egy egyszerű szervert készítek, ahol fájlokat tudok tárolni, amikbe az egyszerűség kedvéért először csak szövegeket, vagy telefonkönyveket tudok tárolni.

Így hiába olvashatja az adott szerverszolgáltató az adataimat, nem fog hozzáférni az információhoz, mert az már a kliens oldalon titkosítva van.

Fontos volt számomra, hogy az általam készített program nyílt forráskódú legyen, hogy biztosítva legyen, hogy tényleg titkosít, és tényleg nem ment semmilyen adatot.

## A feladat

Egy olyan program írása, ami szöveges adatokat, és telefonkönyv adatokat olyan titkosan tart, amennyire csak lehetséges.

A program két részből áll. Egy szerverből és egy kliensből.

A kliensnek négy feladata van:

1. Telefonkönyv fájl és txt fájl létrehozása, megjelenítése, módosítása
  1. A telefonfájl fájlnál figyelni kell arra, hogy a memóriában mindig maximum egy kontaktnak legyenek titkosítatlanul az adatai.
2. A fájlok titkosítása, és visszafejtése, még a nevüket is titkosítani kell
3. A felhasználói adatok titkosítása a szerver elől (még a felhasználónevét is)
4. Kommunikáció a szerverrel (RPC segítségével)
  1. Autentikáció
  2. Fájlok letöltése, feltöltése, törlése.

A szerver oldalnak öt feladata van:

1. A felhasználók autentikációja
2. A felhasználók adatainak tárolása (fájlkiszolgáló)
  1. Minden felhasználónak létre kell hozni egy mappát, de figyelni kell rá, hogy a felhasználóról minél kevesebb információt tároljon, így hash-elést kell használni, hogy még a felhasználó neve se derülhessen ki.
  2. A fájlok eleve titkosan kell, hogy megérkezzenek, egy titkos névvel, és tartalommal
  3. Ezen fájlok manipulálása: átnevezés, létrehozás, felülírás, törlés.
3. A klienssel kommunikálás RPC-t használva.
4. A kliens statikus fájljainak kiszolgálása.
5. Biztosítani, hogy a kommunikáció is titkosan zajlik.

# Felhasználói dokumentáció

## A feladat

Egy olyan program írása, ami szöveges adatokat, és telefonkönyv adatokat olyan titkosan tart, amennyire csak lehetséges.

A program két részből áll. Egy szerverből és egy kliensből.

A kliensnek négy feladata van:

5. Telefonkönyv fájl és txt fájl létrehozása, megjelenítése, módosítása
  1. A telefonfájl fájlnál figyelni kell arra, hogy a memóriában mindig maximum egy kontaktnak legyenek titkosítatlanul az adatai.
6. A fájlok titkosítása, és visszafejtése, még a nevüket is titkosítani kell
7. A felhasználói adatok titkosítása a szerver előtt (még a felhasználónevét is)
8. Kommunikáció a szerverrel (RPC segítségével)
  1. Autentikáció
  2. Fájlok letöltése, feltöltése, törlése.

A szerver oldalnak öt feladata van:

1. A felhasználók autentikációja
2. A felhasználók adatainak tárolása (fájlkiszolgáló)
  1. Minden felhasználónak létre kell hozni egy mappát, de figyelni kell rá, hogy a felhasználóról minél kevesebb információt tároljon, így hash-elést kell használni, hogy még a felhasználó neve se derülhessen ki.
  2. A fájlok eleve titkosan kell, hogy megérkezzenek, egy titkos névvel, és tartalommal
  3. Ezen fájlok manipulálása: átnevezés, létrehozás, felülírás, törlés.

3. A klienssel kommunikálás RPC-t használva.
4. A kliens statikus fájljainak kiszolgálása.
5. Biztosítani, hogy a kommunikáció is titkosan zajlik.

## Fontosabb eszközök a megvalósításhoz

**AES256 algoritmus:** A fájlok, és a fájlok neveinek titkosításához

**SHA256 algoritmus (sózva):** a felhasználó nevek és jelszavak titkosításához, a felhasználói mappa létrehozásához, meg az AES kulcs generálásához.

**HTTPS:** Az adatok titkos továbbításához.

**tornado:** Python webservert, a statikus fájlok kiszolgálásáért, és az RPC legalsó rétegéért.

**Jsonrpcserver, simple-jsonrpc-js:** Az RPC kommunikációért (a **tornado** felett).

## Teszt környezet

### Hardware

RAM: 16GB (ez lehet, hogy kevés lesz sok felhasználóra.)

Processor: Intel(R) Core(TM) i7-4600U CPU @ 2.10GHz

### Szoftver

#### *Operációs rendszer*

**Distributor ID:** Ubuntu

**Description:** Ubuntu 18.04.4 LTS

**Release:** 18.04

**Codename:** bionic

#### *Python*

Python 3.6.9

<b>Csomag</b>	<b>Verzió</b>	<b>Hivatalos weblap</b>
tornado	6.0.3	<a href="https://www.tornadoweb.org/en/stable/">https://www.tornadoweb.org/en/stable/</a> <a href="https://github.com/tornadoweb/tornado/">https://github.com/tornadoweb/tornado/</a> <a href="https://pypi.org/project/tornado/">https://pypi.org/project/tornado/</a>
jsonrpcserver	4.1.2	<a href="https://github.com/bcb/jsonrpcserver">https://github.com/bcb/jsonrpcserver</a> <a href="https://pypi.org/project/jsonrpcserver/">https://pypi.org/project/jsonrpcserver/</a>
pandas	1.0.3	<a href="https://pandas.pydata.org/">https://pandas.pydata.org/</a> <a href="https://github.com/pandas-dev/pandas">https://github.com/pandas-dev/pandas</a> <a href="https://pypi.org/project/pandas/">https://pypi.org/project/pandas/</a>
pyexcel-ods	0.5.6	<a href="https://github.com/pyexcel/pyexcel-ods">https://github.com/pyexcel/pyexcel-ods</a> <a href="https://pypi.org/project/pyexcel-ods/">https://pypi.org/project/pyexcel-ods/</a>

## **Böngészők**

Google Chrome	80.0.3987.149	<a href="https://www.google.com/chrome/">https://www.google.com/chrome/</a>
Mozilla Firefox	74.0	<a href="https://www.mozilla.org/en-US/firefox/">https://www.mozilla.org/en-US/firefox/</a>

## **JavaScript**

Ecmascript 6

<b>Csomag</b>	<b>Verzió</b>	<b>Hivatalos weblap</b>
aes-js	3.1.2	<a href="https://www.npmjs.com/package/aes-js">https://www.npmjs.com/package/aes-js</a> <a href="https://cdn.rawgit.com/ricmoo/aes-js">https://cdn.rawgit.com/ricmoo/aes-js</a>
bootstrap	4.4.1	<a href="https://getbootstrap.com/">https://getbootstrap.com/</a>
jquery	3.4.1.slim	<a href="https://jquery.com/">https://jquery.com/</a>
js-sha256	0.9.0	<a href="https://www.npmjs.com/package/js-sha256">https://www.npmjs.com/package/js-sha256</a>
popper.js	1.16.0	<a href="https://popper.js.org/">https://popper.js.org/</a>
simple-jsonrpc-js	1.0.0	<a href="https://github.com/jershell/simple-jsonrpc-js">https://github.com/jershell/simple-jsonrpc-js</a>

## **Letöltés githubról**

1. git-tel

1. git installálás (ha nincs telepítve)

**sudo apt install git**



## 2. klónozás

1. **git clone** [https://github.com/somla/real\\_private\\_data.git](https://github.com/somla/real_private_data.git)

vagy

2. **git clone** [git@github.com:somla/real\\_private\\_data.git](https://github.com/somla/real_private_data.git)

vagy

### 3. Forokolod a saját repoid közé (fejlesztőknek)

## 2. Letöltés githubról zip formátumban

1. Egy böngészőben nyissuk meg ezt a linket:

[https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

2. Kattintsunk a **Clone or download** gombra

3. Kattintsunk a **Download ZIP** gombra

4. Tömörítsük ki

**unzip real\_private\_data-master.zip**

## Installálás

Ehhez egy VirtualBoxot használtam, arra feltelepítettem egy Ubuntut, így egy teljesen új linuxon van tesztelve, amin még nincs semmi.

## Függőségek

### ***iptables-persistent***

Csak ha portforwardingolni akarunk

**sudo apt-get install iptables-persistent**

### ***pip3***

**sudo apt install python3-pip**

## ***Python csomagok***

**sudo pip3 install tornado**

**sudo pip3 install pandas**

**sudo pip3 install pyexcel-ods**

**sudo pip3 install jsonrpcserver**

## **Előkészületek**

1. Menjünk abba a mappába, ahova letöltöttük a programot

**cd ./real\_private\_data**

2. hozzunk létre egy könyvtárat az adatoknak (nem muszáj itt, de akkor át kell állítani a config-ban lásd a Konfiguráció fejezetet)

**mkdir data**

3. hozzunk létre SSL-kulcsot, vagy ha van saját, akkor másoljuk be a .key mappába, vagy adjuk meg a helyét a config.json-ban (lásd a Konfiguráció fejezetet)

**mkdir .key;**

**openssl req -x509 -out rpd.crt -keyout rpd.key \**

**-newkey rsa:2048 -nodes -sha256 \**

**-subj '/CN=localhost' -extensions EXT -config <( \**

**printf "[dn]\nCN=localhost\n[req]\ndistinguished\_name = dn\n[EXT]\n**

**nsubjectAltName=DNS:localhost\nkeyUsage=digitalSignature\**

**nextendedKeyUsage=serverAuth");**

**cd ..**

4. Hozzunk létre egy mappát a generált javascript fájloknak

**mkdir src/web/generated/**

5. Másoljuk le a config.sample.json-t a config.json-ra

**cd src/python**

**cp config.sample.json config.json**

**cd ../..**

6. Hozz létre legalább egy felhasználót

```
./bin/server/rpd_create_user.sh
```

7. Ha minden jól sikerült, akkor el kell, hogy tudjuk indítani a szerveret

```
./bin/server/rpd_server.sh
```

## Linux service létrehozás

A Linux service automatikusan indul, amikor a linux elindul, és újraindul, ha a folyamat valamiért leáll. Én itt egy alapbeállítást mutatok be, további információért nézz utána a Linux folyamatoknak, és a **systemctl** parancsnak

1. Ehhez érdemes egy új felhasználót létrehozni, nálam ez “rpd-server” lesz  
**sudo adduser rpd-server**
2. hozzunk létre egy új mappát az adatoknak  
**sudo mkdir -p /var/local/rpd/data**  
**sudo chown rpd-server:rpd-server /var/local/rpd/data**
3. Csináljunk egy kulcsot a szerverünknek (lásd feljebb: Előkészületek 3. lépés)  
aminek az rpd-server a tulajdonosa
4. Csináljunk egy config fájlt a service-nek
  1. Másoljuk le a sample config-ot  
**cd {project\_dir}/src/python**  
**cp config.sample.json config.service.json**
  2. Írjuk át a “config.service.json”-t
    1. data\_dir:”/var/local/rpd/data”
    2. secure\_port:10443
    3. open\_port:10080
    4. crt\_file:<crt fájl helye>
    5. key\_file:<key fájl helye>
5. Csináljunk egy service fájlt:

1. másoljuk le a sample-t  
**cd {project\_dir}/src/service**  
**cp rpd.sample.service rpd.service**
2. állítsuk be az “rpd.service”-t
  1. ExecStart=/home/rpd-server/real\_private\_data/bin/server/rpd\_server.sh --configFile "[[dir\_project]]/src/python/config.service.json"
  2. User=rpd-server
6. Hozzunk létre felhasználót (felhasználókat)  
**su rpd-server**  
**./bin/server/rpd\_create\_user.sh --configFile ./src/python/config.service.json**
7. Másoljuk be a service fájlt a linux service könyvtárba  
**sudo cp rpd.service /etc/systemd/system/**  
**systemctl daemon-reload**  
**systemctl start rpd**  
**systemctl enable rpd**
8. Csináljunk port forwardingot, hogy a 80-as és a 443 portokról lehessen elérni a szervert  
**sudo iptables -t nat -A OUTPUT -o lo -p tcp --dport 80 -j REDIRECT --to-port 10080**  
**sudo iptables -t nat -A OUTPUT -o lo -p tcp --dport 443 -j REDIRECT --to-port 10443**  
**sudo iptables -i <interface> -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10080**  
**sudo iptables -i <interface> -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 10443**  
**su**  
**iptables-save > /etc/iptables/rules.v4**  
**ip6tables-save > /etc/iptables/rules.v6**

## Konfigurálás

A konfigurálás két féle lehet.

Vagy fájlból, vagy command line argumentumként megadva.

A command line argumentumnak nagyobb prioritása van.

Kötelező, hogy legyen config fájl.

A konfigurációs paraméterek lehetnek publikusak, ez azt jelenti, hogy a kliens oldalon is láthatóak.

A nem publikus konfigurációs beállítások csak a szerver oldalon láthatóak.

## Konfigurációs változók

A konfigurációban vannak változók amiket [[változó név]]-ként érünk el.

Például: `./rpd_server.sh -logLevel /var/tmp/log[[now]].log`

`./rpd_server.sh -logLevel /var/tmp/log20200330_163019.log` lesz, vagy valami hasonló

Változó név	Leírás	Példa
[[dir_project]]	A projekt gyöker könyvtára	
[[dir_src]]	A projekt src könyvtára	
[[dir_web]]	A projektben lévő web könyvtára	
[[dir_python]]	A projektben lévő python fájlok könyvtára	
[[now]]	Az aktuális idő ÉvHóNap_ÓraPercMásodperc formában	20200330_163019
[[today]]	A mai nap ÉvHóNap formában	20200330

## Konfigurációs opciók

Név	Leírás	Alapérték	Opcionális	Publikus
configFile	Config json, ez az a konfigurációs fájl, amiből a beállítások jönnek: config.json	./config.json	Igen	Nem

Név	Leírás	Alapérték	Opcionális	Publikus
debug	Debug mód, ha be van kapcsolva, akkor több ellenőrzés van, több log van, de az a logLeveltől is függ.	False	Igen	Igen
logLevel	logLevel, értékei lehetnek CRITICAL - 50 ERROR - 40 WARNING - 30 INFO - 20 DEBUG -10 NOTSET – 0 Lásd: <a href="https://docs.python.org/3/library/logging.html">https://docs.python.org/3/library/logging.html</a>	INFO	Igen	Nem
logFile	Log fájl, helye, ha nem töltjük ki, akkor nem logolunk fájlba, csak a consolera.		Igen	Nem
logFormat	Log formátuma, ahogy a python várja lásd: <a href="https://docs.python.org/3/library/logging.html#logging.Formatter">https://docs.python.org/3/library/logging.html#logging.Formatter</a>	[% (asctime)s] [% (levelname)s] ] % (message)s	Igen	Nem
show_rpc_message	Mutassuk-e az rpc üzeneteket	False	Igen	Nem
open_port	Indítunk egy http szerveret is, ami átírányít a https szerverre, ennek a portja	8080	Igen	Nem
debug_open_port	Debug módban indítunk egy http szerveret, ami nem titkos, ez segítheti a debuggolást, de nem biztonságos, így production rendszerbe nem fut	8081	Igen	Nem
secure_port	A szerver portja, https kapcsolat	8443	Igen	Nem
host	a host neve, átírányításnál fontos	localhost	Igen	Nem
crt_file	Certification fájl az SSL-hez	None	Nem	Nem
key_file	Key fájl az SSL-hez	None	Nem	Nem
web_root	a statikus fájlok könyvtára	None	Nem	Nem
data_dir	Az adatok mappája, ide lesznek elmentve a titkos fájljai a felhasználóknak	None	Igen	Nem

Név	Leírás	Alapérték	Opcionális	Publikus
test_dir	Egy mappa a tesztekhez	/var/tmp/ real_private_ data	Igen	Nem
salt	Egy hash "só" a kliens oldalra	My own Salt	Igen	Igen
server_salt	Egy hash "só" a szerver oldalra	Server salt	Igen	Nem
enable_create_user	Engedélyezzük, hogy felhasználók is létre tudjanak hozni új felhasználókat, ha nem, akkor csak a szerveren lehet új felhasználókat létrehozni commandline paranccsal.	False	Igen	Igen
defaultRpcClient	Az alapértelmezett RPC metódus neve. jelenleg SimpleJsonRpcWebSocketClientService vagy	SimpleJsonRpcWebSocketClientService	Igen	Igen
hideMessageTime	Az üzenetek elrejtése előtti idő ezredmásodpercben	5000	Igen	Igen
show_encrypted_data	Mutassa a weblapon a titkosított adatot	False	Igen	Igen

## Példa

my\_config.json

```
{
  "debug":false,
  "logLevel":"INFO",
  "logFile":"/var/tmp/rpd_{{now}}.log",
  "host":"localhost",
  "open_port":8080,
  "secure_port":8443,
  "crt_file": "[[dir_project]]/.key/rpd.crt",
  "key_file": "[[dir_project]]/.key/rpd.key",
  "web_root": "[[dir_project]]/src/web",
  "data_dir": "[[dir_project]]/data"
}
```

ha most meghívjuk a programot

```
./rpd_server.sh --configFile --logLevel /var/tmp/log_{{now}}.log --configFile
my_config.json --data_dir "[[dir_project]]/data2"
```

akkor a command line data dir fog érvényesülni.

## Használat

### Szerver oldal

Alapjában véve a **./bin** mappában vannak a futtatható fájlok, ott van egy **server** és egy **tools**

A **server** mappában vannak a szerverhez kellő dolgok, a **tools** mappában a fejlesztéshez szükséges toolok, ezért azokat majd a fejlesztői dokumentációban fogom részletezni.

***./bin/server/rpd\_server.sh***

Lásd ***./src/python/run\_server.py***

***./bin/server/rpd\_create\_user.sh***

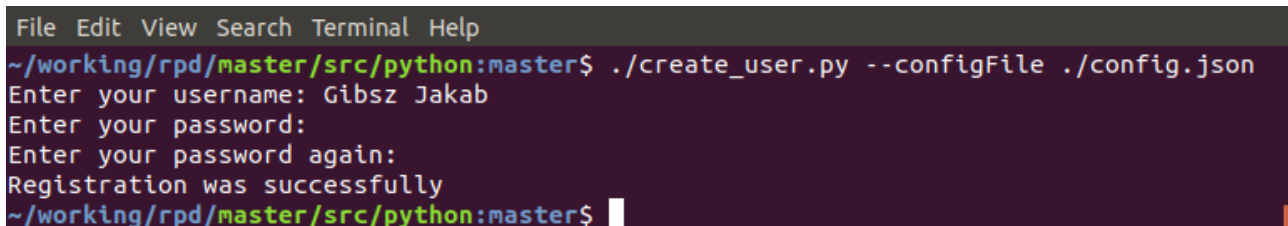
Lásd ***./src/python/create\_user.py***

***./src/python/run\_server.py***

Maga a szerver, a beállításokat lásd a **Konfigurálás** fejezetet, alapértelmezettként a **./src/python/config.json** fájlt fogja betölteni **--configFile**

***./src/python/create\_user.py***

Felhasználó létrehozása, érdemes beállítani a **--configFile**-t, alapértelmezettként a **./src/python/config.json** fájlt használja.



```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile ./config.json
Enter your username: Gibsz Jakab
Enter your password:
Enter your password again:
Registration was successfully
~/working/rpd/master/src/python:master$
```

**Enter your username:** Írd be a felhasználónevet



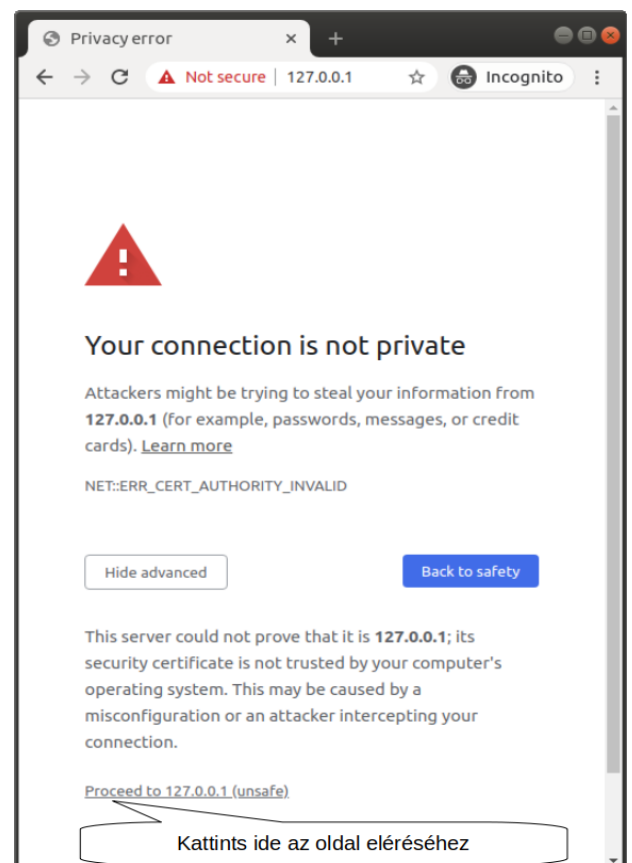
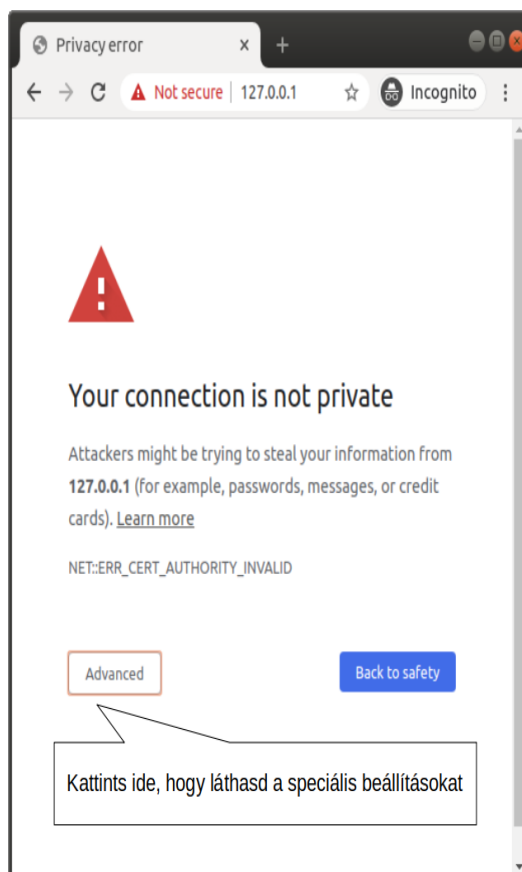
**Enter your password:** Írd be a jelszót

**Enter your password again:** Írd be a jelszót megint

## Kliens oldal

### *Az oldal elérése*

Az oldalt az épp aktuális címén lehet elérni a böngészőben, de ha nem akarunk SSL hitelesítést venni, akkor sajnos a böngésző “nem biztonságos”-nak fogja látni az oldalunkat.



## Bejelentkezés

### RPC Client:

SimpleJsonRpcWebSocketClientService: a kommunikációhoz használjuk a SimpleJsonRpcWebSocketClient-et, ez egy websocket alapú kommunikáció.

Előnye, hogy folyamatos kapcsolat van a szerver, és a kliens között,

Hátránya, hogy így folyamatosan van kommunikációs forgalom, de csak elhanyagolható.

SimpleJsonRpcPOSTClientService: HTTP post alapú kommunikációt biztosít.

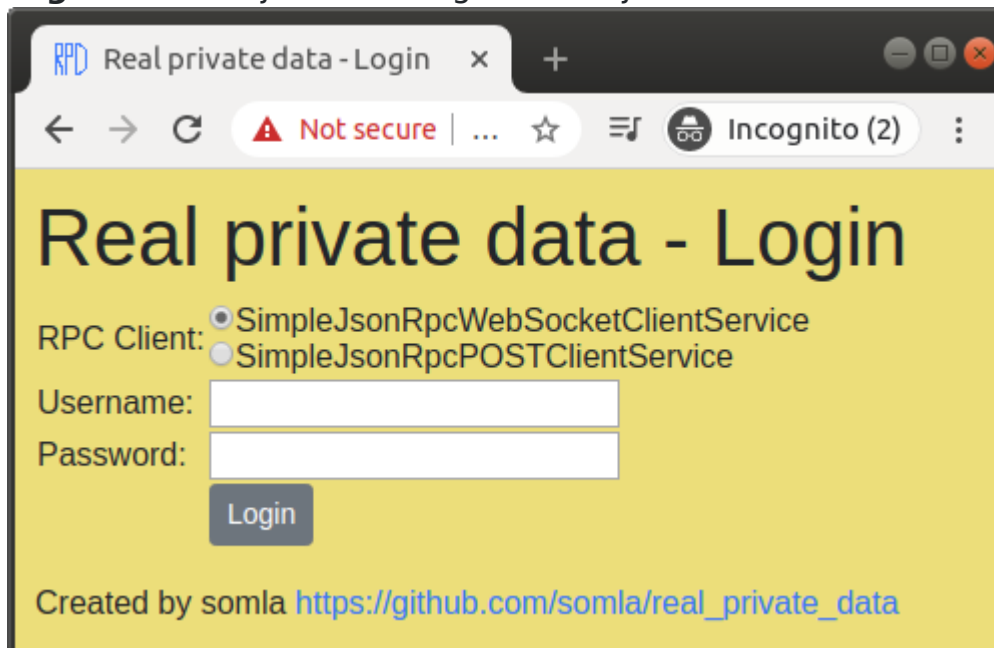
Előnye, hogy csak akkor van kommunikáció, amikor szervertől kérünk valamit.

Hátránya, hogy mindig új kapcsolatot kell létesíteni.

**Username:** felhasználónév

**Password:** jelszó

**Login:** bejelentkezés gomb a bejelentkezéshez



The screenshot shows a web browser window with the title 'Real private data - Login'. The address bar indicates the page is 'Not secure' and is being viewed in 'Incognito (2)' mode. The page has a yellow background and contains the following elements:

- RPC Client:** A radio button selection where 'SimpleJsonRpcWebSocketClientService' is selected.
- Username:** A text input field.
- Password:** A text input field.
- Login:** A blue button.
- Footer:** Text stating 'Created by somla' followed by a link to [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data).

## A főoldal struktúrája

The screenshot shows the 'Real private data - Main' web application running on localhost:11443. The interface has a yellow header and a dark navigation bar. A callout 'Címsor' points to the main title. The navigation bar contains links: 'Create File', 'Change password', 'Create user', and 'Logout'. A callout 'Menüsor' points to this navigation bar. Below is a 'Files' section with a table of files. A callout 'Lábléc' points to the footer text. A callout 'Fájlok listája' points to the file list table.

Real private data - Main

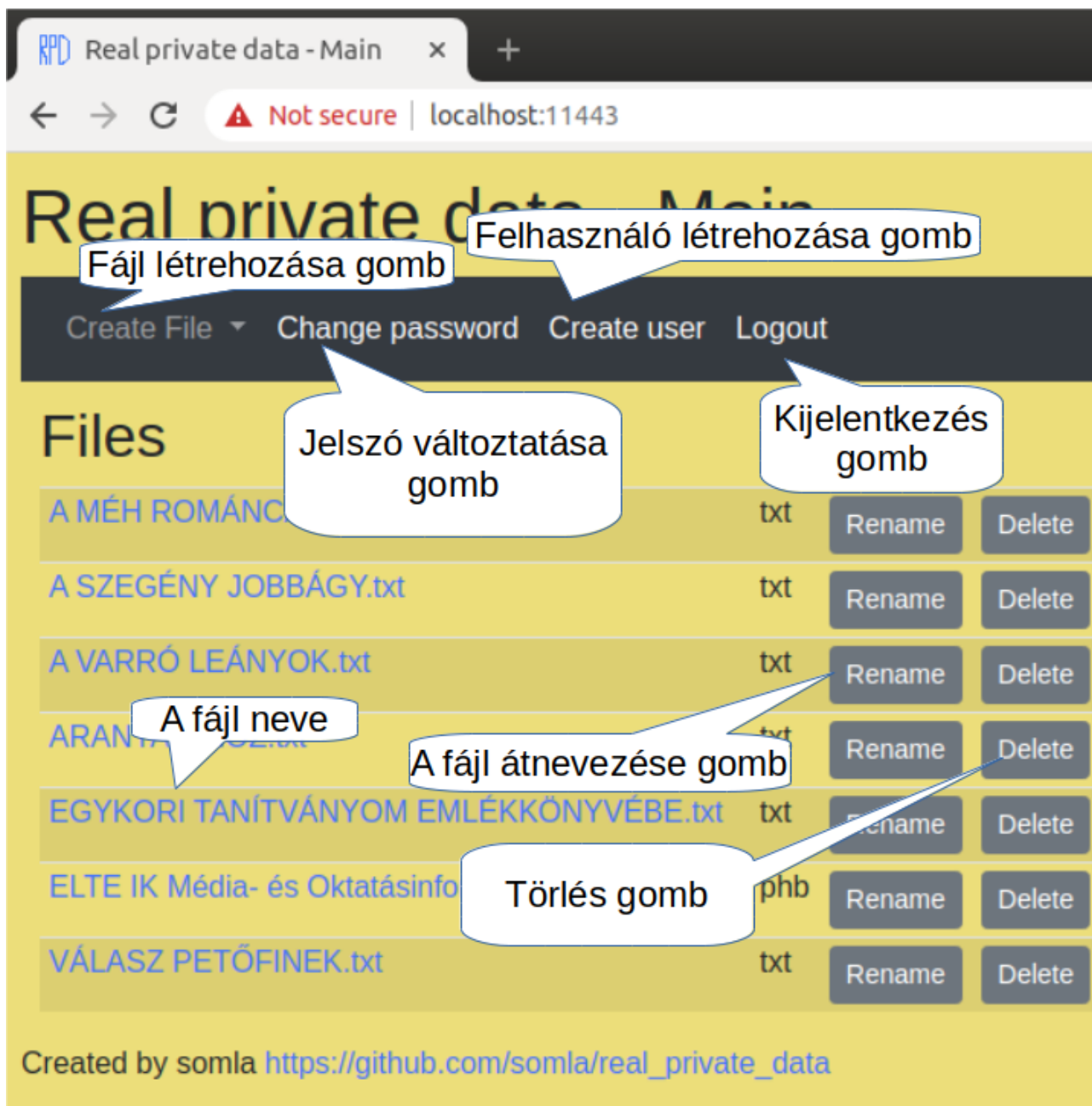
Create File ▾ Change password Create user Logout

### Files

A MÉH ROMÁNCA.txt	txt	Rename	Delete
A SZEGÉNY JOBBÁGY.txt	txt	Rename	Delete
A VARRÓ LEÁNYOK.txt	txt	Rename	Delete
ARANYAIMHOZ.txt	txt	Rename	Delete
EGYKORI TANÍTVÁNYOM EMLÉKKÖNYVÉBE.txt	txt	Rename	Delete
ELTE IK Média- és Oktatásinformatikai Tanszék.phb	phb	Rename	Delete
VÁLASZ PETŐFINEK.txt	txt	Rename	Delete

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

## A főoldal gombjai

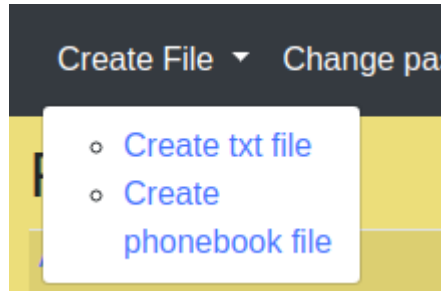


### Felhasználó létrehozása gomb

Ez a gomb csak akkor jelenik meg, ha a **enable\_create\_user** opció **True** (lásd Konfigurálás fejezet)

### A fájl neve

Ha rákattintasz, megnyitja a fájlt.

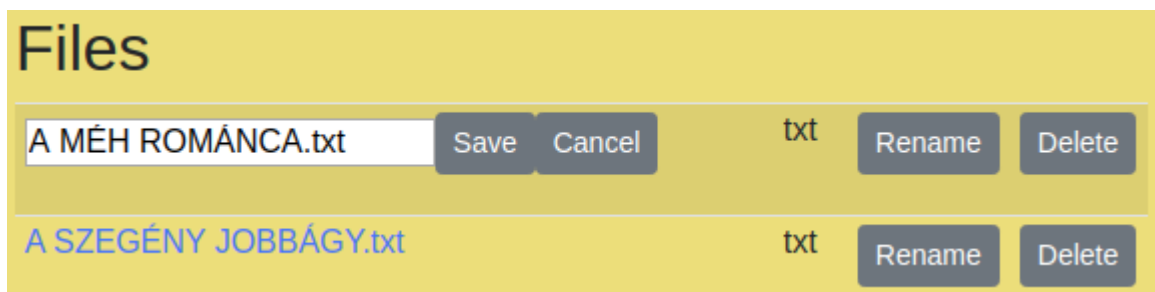


### Fájl létrehozása menü

**Create txt file:** Létrehoz egy txt fájlt

**Create phonebook file:** Létrehoz egy telefonkönyv fájlt

### Fájl átnevezés

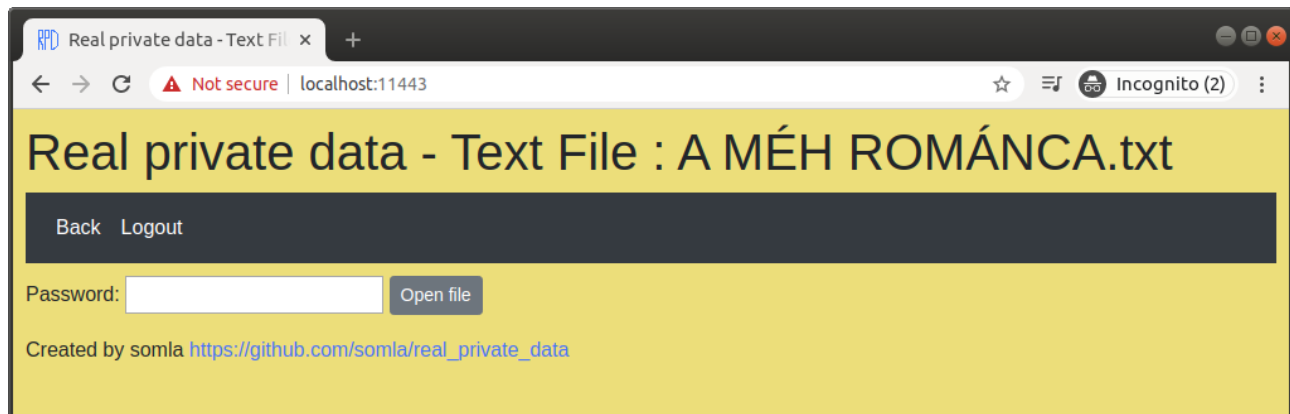


**Fájl neve mező:** Ide kell beírni az új nevét a fájlnek

**Save gomb:** Elmenti a névváltoztatást

**Cancel gomb:** Megszakítja a névváltoztatást

## ***Txt/Phonebook fájl megnyitás***



Ahhoz, hogy megnyissunk egy fájlt, ahhoz be kell írunk a fájl jelszavát

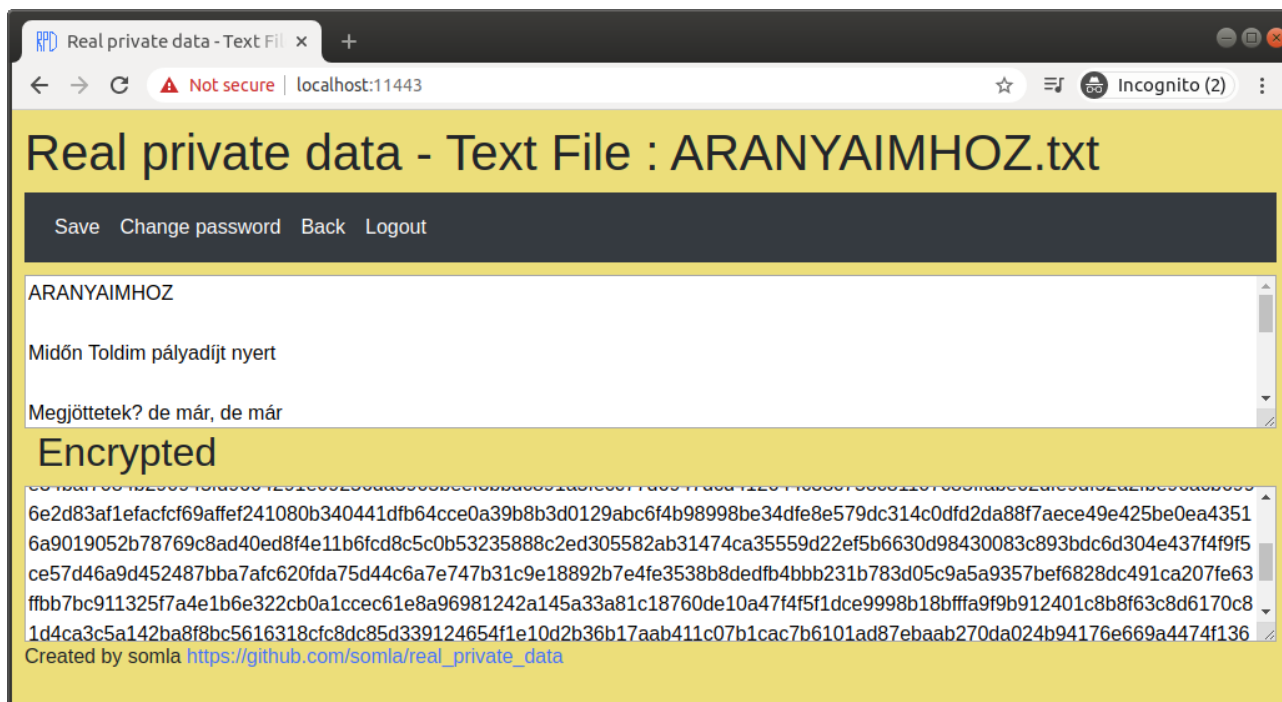
**Back menü:** Visszalép a főoldalra

**Logout menü:** Kilép

**Password mező:** Ide kell írni a fájl jelszavát, hogy megnyissuk

**Open file gomb:** Megnyitja a fájlt

## Txt fájl oldal struktúrája



<b>Save menü:</b>	Elmenti a txt fájlt
<b>Change password menü:</b>	Megváltoztatja a fájl jelszavát
<b>Back menü:</b>	Visszamegy a főoldalra
<b>Logout menü:</b>	Kijelentkezik az oldalból
<b>Txt mező:</b>	A txt fájl tartalma, ez szerkeszthető
<b>Encrypted mező:</b>	A txt fájl titkosítva, ez csak akkor látszik, ha a <b>show_encrypted_data</b> konfiguráció <b>True</b> (Lásd <b>Konfiguráció</b> fejezet)

## Txt fájl létrehozása

RPD Real private data - Text File x +

← → ↻ ⚠ Not secure | localhost:11443

# Real private data - Text File

Back Logout

File name:

New password:

New password again:

Create file

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

<b>Back menü:</b>	Visszalép a főoldalra
<b>Logout menü:</b>	Kijelentkezés
<b>File name mező:</b>	A fájl neve
<b>New password mező:</b>	A fájl jelszava
<b>New password again mező:</b>	A fájl jelszava még egyszer
<b>Create file gomb:</b>	Ez a gomb hozza létre a fájlt, meg fog jelenni egy üres fájl.

**A Create file gomb megnyomása után**



RPD Real private data - Text File x +

← → ↻ ⚠ Not secure | localhost:11443

# Real private data - Text File

Save Change password Back Logout

File name:

New password:

New password again:

test\_file1

## Encrypted

e8771c851655a9f7f9d5760746a99334e80ec7af98c18767c5db533ddbfaae  
abfb23d592732b11fccdf6459abc3acfcca5f5219f29f0f3c5fa5a8eb7c83ca9

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

**Save menü:** Elmenti a fájlt

**Change password menü:** Jelszóváltoztatás

Fontos, hogy a fájl csak a **Save** gomb lenyomásával mentődik el, ha a fájl létezik, akkor hibát ír. Apró hiba, hogy ezután ismét meg kell nyomni a **Create file** gombot, a fájl átnevezése után (**File name** mező), majd utána megint a **Save** gombot valamikor javítani fogom, hogy intuitívabb legyen.

## *Txt/Telefonkönyv fájl jelszóváltoztatás*

Real private data - Text File x +

← → ↻ ⚠ Not secure | localhost:11443

# Real private data - Text

Save Change password Back Logout

## Change password

Old password:

New password:

New password again:

Change password Cancel

ARANYAIMHOZ

Midőn Toldim pályadíjt nyert

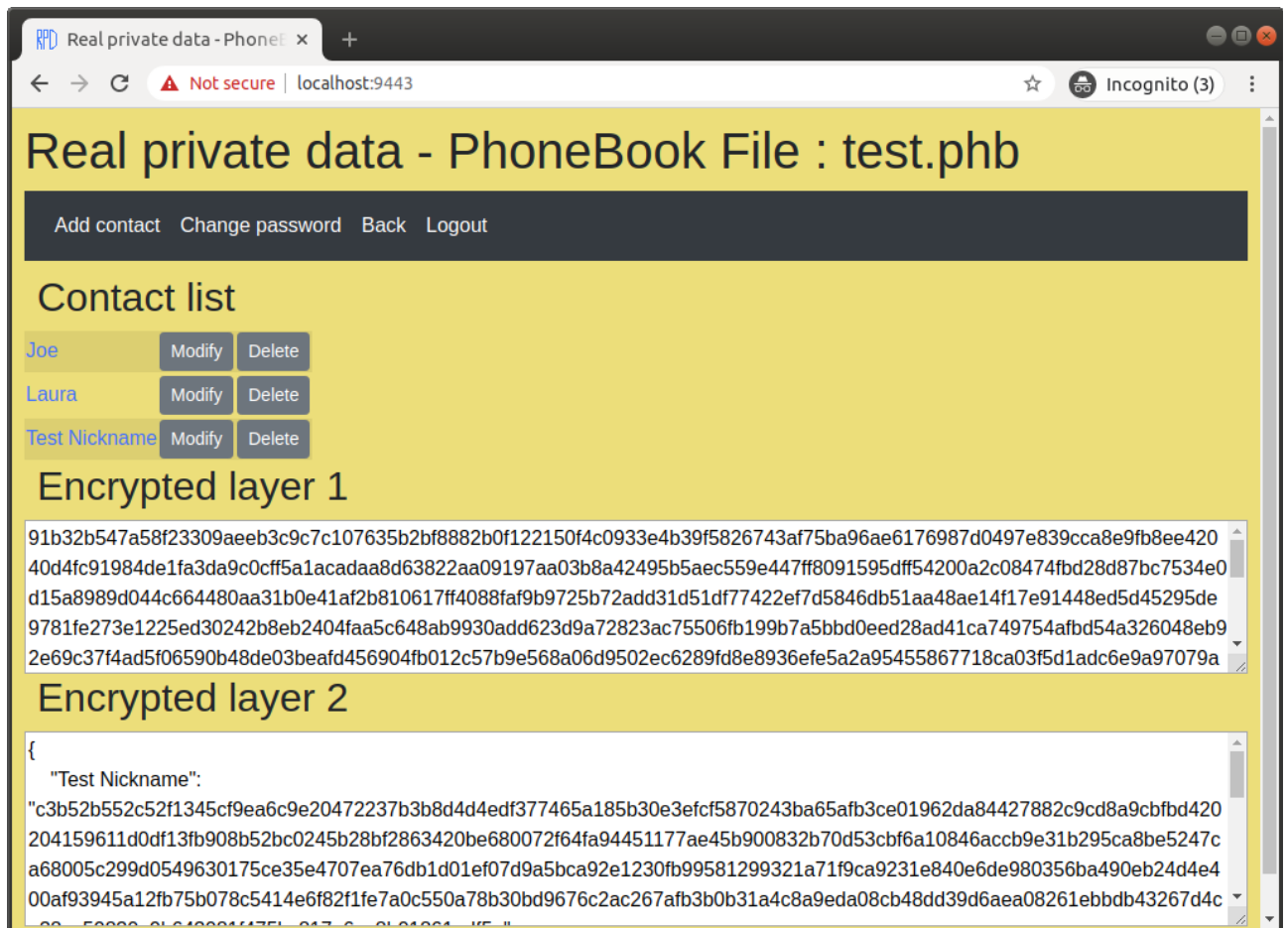
Megjöttetek? de már, de már

## Encrypted

02dfe9df52a2fbe96acb6996e2d83af1efacfcf69affef2410

- |                                 |   |
|---------------------------------|---|
| <b>Old password mező:</b>       | Ide kell írni a fájl régi jelszavát           |
| <b>New password mező:</b>       | Ide kell írni a fájl új jelszavát             |
| <b>New password again mező:</b> | Ide kell írni a fájl új jelszavát még egyszer |
| <b>Change Password gomb:</b>    | Elmenti az új jelszót                         |
| <b>Cancel gomb:</b>             | Megszakítja a jelszóváltoztatást              |

## Telefonkönyv fájl oldal struktúrája



1. Menü
  1. Add contact: Új telefonkönyvbejegyzés hozzáadása
  2. Change password: A fájl jelszavának megváltoztatása
  3. Back: Vissza a főmenüre
  4. Logout: Kilépés
2. Contact list
  1. Első oszlop: A kontakt beceneve, ha rákattintunk, akkor több információ is megjelenik a kontaktról, ha még egyszer rákattintunk, akkor eltűnnek az információk
  2. Második oszlop: **Modify** gomb, monodíthatunk a kontakt információin
  3. Harmadik oszlop: **Delete** gomb, törli a kontaktot

3. Encrypted layer 1: A kétrétegű titkosítás 1. rétegét mutatja (hexadecimális számok)

Ez a réteg kerül fel a szerverre

4. Encrypted layer 2: A kétrétegű titkosítás 1. rétegét mutatja (hexadecimális számok)

Ez a réteg van a memóriában, csak akkor dekódolja a második réteget, ha rákattintunk egy kontaktra, és akkor is csak annak a kontaktnak az információit csomagolja ki

Az **Encrypted layer 1** és az **Encrypted layer 2**, csak akkor látszik, ha beállítjuk a **show\_encrypted\_data** konfigurációt **True**-ra (Lásd Konfigurálás fejezet)

### **Telefonkönyv kontakt**

The screenshot shows a contact form for a contact named 'Laura'. The form has a yellow header bar with the name 'Laura' on the left and 'Modify' and 'Delete' buttons on the right. Below the header, the form fields are as follows:

- Nickname: Laura
- Fullname: Laura Brown
- Address: UK, London
- Phone numbers: mobil 111 34235 (with 'Modify' and 'Delete' buttons next to the number)
- Description: My coworker

There is also an 'Add phone number' button below the phone numbers field.

- Nickname:** A kontakt beceneve
- Fullname:** A kontakt teljes neve
- Address:** A kontakt címe
- Phone numbers:** A kontakt telefonszámai
- Description:** A kontaktról egy leírás
- Modify gomb:** A telefonszám módosítása
- Delete gomb:** A telefonszám törlése
- Add phone number gomb:** Telefonszám hozzáadása

## Telefonkönyv kontakt – Telefonszám módosítás

Laura

Modify Delete

Nickname: Laura  
Fullname: Laura Brown  
Address: UK, London

Phone numbers: mobil 111 34235 Save Cancel Modify Delete

Add phone number

Description: My coworker

**Típus mező:** mobil, vagy office (irodai) vagy home (otthoni) lehet a telefon típusa

**Szám mező:** a telefonszám

**Save gomb:** Elmenti a módosítást

**Cancel gomb:** Megszakítja a módosítást

## Telefonkönyv kontakt – Telefonszám hozzáadás

Laura

Modify Delete

Nickname: Laura  
Fullname: Laura Brown  
Address: UK, London

Phone numbers: mobil 111 34235 Modify Delete

Add phone number

Save

Description: My coworker

**Típus mező:** mobil, vagy office (irodai) vagy home (otthoni) lehet a telefon típusa

**Szám mező:** a telefonszám

**Save gomb:** Elmenti a módosítást

## Telefonkönyv kontakt – Módosítás

Laura

Modify Delete

Save Cancel

Nickname: Laura

Fullname: Laura Brown

Address: UK, London

Description: My coworker

- Save gomb:** Elmenti a módosítást
- Cancel gomb:** Megszakítja a módosítást
- Nickname mező:** A kontakt beceneve
- Fullname mező:** A kontakt teljes neve
- Address mező:** A kontakt címe
- Description mező:** A kontaktról egy leírás

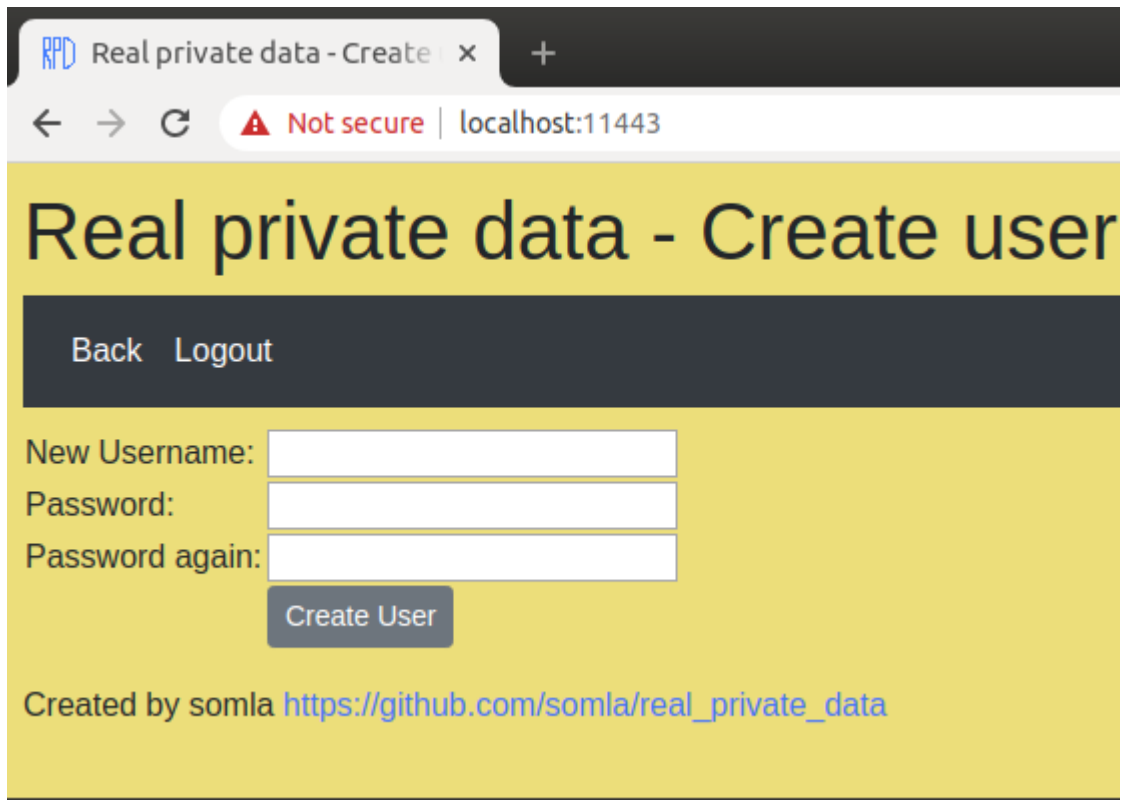
## Telefonkönyv – Új kontakt hozzáadása

The screenshot shows a web browser window with the title 'Real private data - PhoneE'. The address bar indicates 'localhost:9443' and a 'Not secure' warning. The page has a yellow background. At the top, there is a dark navigation bar with links: 'Add contact', 'Change password', 'Back', and 'Logout'. Below this, there are two buttons: 'Save' and 'Cancel'. The main form area contains several input fields: 'Nickname:', 'Fullname:', 'Address:', and 'Description:'. Below these is a section for 'Phone numbers:' with an 'Add phone number' button. The form is currently empty.

- Save gomb:** Elmenti az új kontaktot
- Cancel gomb:** Megszakítja a kontakt hozzáadását
- Nickname mező:** A kontakt beceneve
- Fullname:** A kontakt teljes neve
- Address:** A kontakt címe
- Description:** A kontaktról egy leírás
- Add phone number:** Új telefonszám hozzáadása (láts feljebb)

Megjegyzés: amikor létrehozunk egy Telefonkönyvfájlt, akkor jön igazából létre, amikor az első kontaktot hozzáadtuk.

## Felhasználó létrehozása



The screenshot shows a web browser window with the title 'Real private data - Create user'. The address bar shows 'localhost:11443' with a 'Not secure' warning. The page has a yellow background. At the top, there is a dark grey bar with 'Back' and 'Logout' links. Below this, there are three input fields: 'New Username:', 'Password:', and 'Password again:'. A 'Create User' button is positioned below the password fields. At the bottom, it says 'Created by somla' followed by a GitHub link.

Real private data - Create user

Back Logout

New Username:

Password:

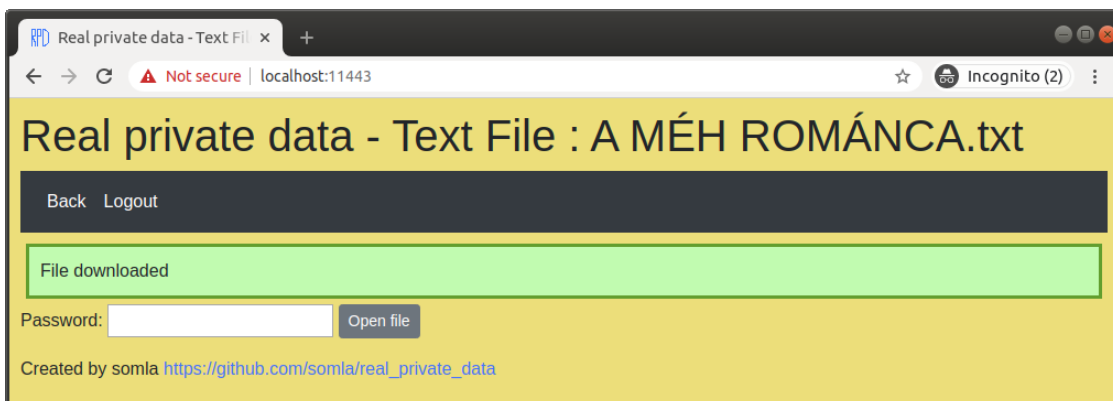
Password again:

Create User

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

- New Username mező:** Új felhasználó neve
- Password mező:** Új felhasználó jelszava
- Password again mező:** Új felhasználó jelszava megint
- Create User gomb:** A felhasználó létrehozása

## Üzenetek megjelenítése



The screenshot shows a web browser window with the title 'Real private data - Text File'. The address bar shows 'localhost:11443' with a 'Not secure' warning. The page has a yellow background. At the top, there is a dark grey bar with 'Back' and 'Logout' links. Below this, there is a green box with the text 'File downloaded'. Below the green box, there is a 'Password:' label followed by an input field and an 'Open file' button. At the bottom, it says 'Created by somla' followed by a GitHub link.

Real private data - Text File : A MÉH ROMÁNCA.txt

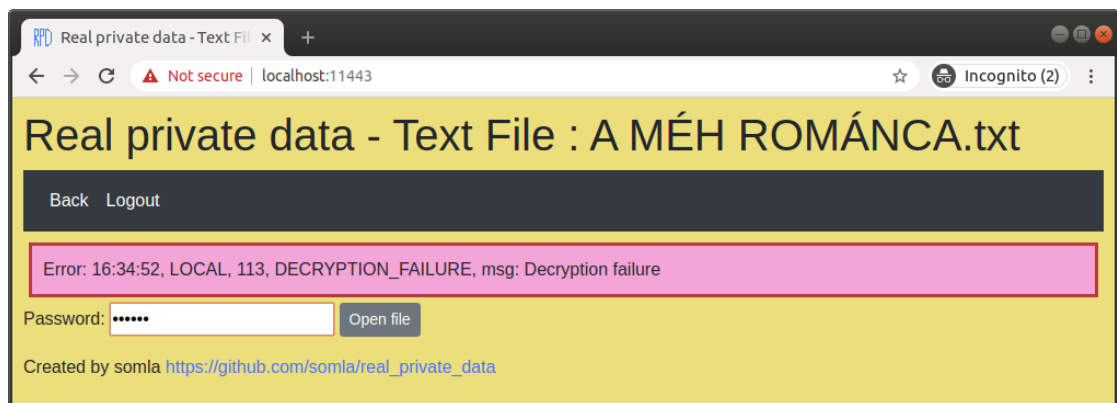
Back Logout

File downloaded

Password:  Open file

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)





Az üzenetek a menüsor alatt jelennek meg.

Ha valami sikeres volt, akkor zöld háttérük lesz, ha sikertelen, akkor piros.

A hibaüzenetekről lásd a **Hibaüzenetek** fejezetet

## Hibaüzenetek

Két fajta hiba lehet, lehet kliens oldali (**LOCAL**) és lehet szerver oldali (**REMOTE**) hiba.

A kliens oldali hibák kódjai **1xx** a szerver oldaliak **2xx** alakúak

Egy hibának van kódja, hibaüzenete, és esetleg további adata (például távoli függvény hibánál a függvény hibaüzenete)

### Lokális, kliens oldali hibák (LOCAL)

Kód	Hibanév	Hibaüzenet (angolul)	Hibaüzenet (magyarul)
101	CONNECTION_ERROR	Connection error	Kapcsolat hiba
102	LOCAL_CALL_ERROR	Function call local error	Lokális függvényhiba
103	ALREADY_LOGEDIN	You are already logged in	Már be vagy jelentkezve
104	EMPTY_USERNAME_PASSWORD	Empty username and/or password and/or password password again	Üres felhasználónév és/vagy jelszó és/vagy a jelszó mégegyszer mező üres
105	PASSWORD_NOT_EQUAL_PASSWORD2	Password and password again is not equal	A jelszó és a jelszó mégegyszer nem egyezik

Kód	Hibanév	Hibaüzenet (angolul)	Hibaüzenet (magyarul)
106	PASSWORD_PASSWORD2_EMPTY	Password, and/or password again is empty	Üres jelszómező
107	PASSWORD_PASSWORD2_OLDPASSWORD_EMPTY	Password, and/or password again is empty and or oldPassword	A régi jelszó és/vagy az új jelszó és/vagy az új jelszó még egyszer üres
108	EMPTY_FILE_FIELD	File field is empty	A fájl mező üres
109	DOWNLOAD_ERROR	Download error	Hiba letöltéskor
110	CONTACT_ALREADY_IN_LIST	The contact has been already in the contact list	A kapcsolat már a kapcsolat listában van
111	CONTACT_NOT_FOUND	Contact not found	A kapcsolat nem található
112	SUDDENLY_LOGGED_OUT	Suddenly logged out	Hirtelen kijelentkeződött
113	DECRYPTION_FAILURE	Decryption failure	A visszafejtés sikertelen

#### Távoli, szerver oldali hibák (REMOTE)

Kód	Hibanév	Hibaüzenet (angolul)	Hibaüzenet (magyarul)
201	MISSING_USERNAME_PASSWORD	Missing username and/or password	Hiányzó felhasználónév és/vagy jelszó
202	BAD_USERNAME_PASSWORD	Bad username and/or password	Hibás felhasználónév és/vagy jelszó
203	REMOTE_FUNCTION_ERROR	Remote function error	Távoli függvény hiba
204	USER_REGISTERED	User has been already registered	A felhasználó már regisztrálva van
205	DISABLED_CREATE_USER	Disabled create new user	Nincs engedélyezve új felhasználó hozzáadása
206	FILE_EXIST	File has been already exist	A fájl már létezik
207	FILE_NOT_EXIST	File not exist	A fájl nem létezik

# Fejlesztői dokumentáció

## Megoldási terv

A projekt két részből áll. Egy szerverből, és egy kliensből. A szerver pythonban íródik, a kliens JavaScript-ben.

A szervernek két szerepe van.

1. a statikus (html, és JavaScript) fájlok kiszolgálása
2. a felhasználók fájljainak tárolása (fontos, hogy a szerver a felhasználókról minél kevesebbet tudjon, így minden, titkosan fog érkezni a szerverhez: felhasználó név, jelszó, fájlnev, fájl tartalom.)

## Adattárolás

### *Felhasználói adatok tárolása a szerveren*

A szerveren van egy mappa a felhasználóknak, ezt a **data\_dir** konfigurációval állíthatjuk be, hogy hol legyen.

Ebben a mappában minden felhasználónak létrehozunk egy új mappát, amiben a már titkos adatokat tároljuk.

A felhasználó mappájába a már előre titkosított fájlok vannak titkosított névvel.

### Felhasználó mappa generálása

Bemenet: felhasználónév, jelszó

1. shaAlgoritmus = SHA256Salty(theConfig.server\_salt)
2. felhasználó\_hash = shaAlgoritmus(felhasználónév)
3. jelszó\_hash = shaAlgoritmus(jelszó)
4. felhasználó\_mappa = shaAlgoritmus(concat(felhasználó\_hash, jelszó\_hash ))

## Megjegyzések

1. a 2. és 3. lépés jellemzően a kliens oldalon történik meg (csak a CLI regisztrálásnál történik szerver oldalon), így a szerver már a felhasználó nevét is titkosan kapja meg.
2. Az SHA256Salty algoritmus kicserélhető, és ki is kell cserélni hosszútávon valami lassabbra
3. A theConfig.server\_salt konfigurálható, lásd a konfigurációs fejezetet
4. az SHA256Salty visszatérési értéke hexadecimális számrendszerben ábrázolt számok (00-ff)
5. Az SHA256Salty algoritmust lásd lejjebb

## Fájlnevek

A titkosítatlan fájlnevek tartalmazzák a fájlok kiterjesztését (jelenleg .txt vagy .phb (szöveges fájl, vagy telefonkönyv fájl))

A fájlnevek a következőképp generálódnak (ez minden esetben a kliens oldalon történik)

Bemenet: jelszó, fájlnev

1. shaAlgoritmus = SHA256Salty(theConfig.server\_salt)
2. fájl\_név\_hash = shaAlgoritmus(concat(jelszó, jelszó))
3. fájl\_név = AESEncryptor(fájl\_név\_hash, fájl\_név)

## Megjegyzések:

1. Az shaAlgoritmus cserélhető, és érdemes is lesz valami lassabbra cserélni
2. AESEncryptor algoritmust lásd lejjebb. (ez is cserélhető lesz)
3. Jelenleg ugyanazt a jelszót használom a fájlok nevének titkosításához, mint a szerver eléréséhez, de másképp hash-elem le. (a szervernél szimplán a jelszót hashelem, itt meg a jelszót kétszer leírva hashelem, de ha a szerver oldali jelszót sikerül feltörni, akkor ezt is.

### ***Titkosított fájl (SecretFile)***

A titkos fájl két részből áll:

Van egy fájlnev (lásd feljebb), és egy fájl tartalom.

A Titkosított fájl tartalmának felépítése:

titkosítatlan\_tartalom = concat(időbélyeg, "|", tartalom)

titkosított tartalom: AESEncryptor(fájl jelszó, titkosítatlan\_tartalom)

Megjegyzések

1. az időbélyeg 1970 január 1. 0:00:00 másodpercétől eltelt másodpercek száma
2. Az AESEncryptor majd kicserélhető lesz

### ***AESEncryptor formátuma***

1. hash = sha256(adat)
2. titkosítatlan = concat(hash, adat)
3. titkosított = AES256(titkosítatlan)

Megjegyzés

1. A hash egy ellenőrző összeg, és mindig 64 hosszú string (0-f), mert 16-os számrendszerben van ábrázolva
2. A kimenet byte sorozat.

### ***Txt fájl (.txt) formátuma***

A txt fájl 4 rétegből áll.

1. titkosítatlan szöveg ( txt )
2. Minden txt fájl egy Titkosított fájl ( <időbélyeg>|<txt> )
3. Minden Titkosított fájl AESEncryptor-t használ, így (<hash><időbélyeg>|<txt>) alakú
4. Az AES titkosított adat

### ***Telefonkönyv fájl (.phb) formátuma***

Három rétegből áll:

1. Titkosított adat (AESEncryptor-ral titkosítva)

2. Az első kicsomagolás után

```
{  
  "becenév1":<titkosított kontakt adat>,  
  "becenév2":<titkosított kontakt adat>  
}
```

3. Titkosítatlan kontakt adat

```
{  
  "full_name":<teljes név>,  
  "phone_numbers":[  
    {  
      "type":<telefon típus>,  
      "number":<telefonszám>  
    }  
  ]  
  "address":<cím>,  
  "description":<leírás>  
}
```

Megjegyzések:

1. Az AESEncryptor kicserélhető lesz
2. A <titkosított becenévadat> is ugyanazzal az jelszóval, és ugyanazzal az encryptorral van jelenleg titkosítva.
3. Mivel a <titkosított kontakt adat> külön titkosítva van, így a memóriában mindig csak egy kontaktnak látszanak az adatai.

## Szerver oldal

### ***Mappa és fájl struktúrájának áttekintése***

src/web

└─ [common](#) - A gyakran használt egyszerű függvények, osztályok helye

| └─ [dictgenerator.py](#) - JSON-t generál dictionaryből

- | | — [generatedby.py](#) - HTML és JavaScript fájlokba írja bele, melyik fájl, és mikor generálta (még fejleszteni kell)
- | | — [\\_\\_init\\_\\_.py](#) - Csomag init fájlja
- | | — [kill\\_log.py](#) - Ha valamiért leáll a program, loggoljuk ki
- | | — [singleton.py](#) - Singleton osztály
- | | — [the\\_project\\_paths.py](#) - A projekt fontosabb mappáit tartalmazza
- | — [config](#) - A projekt összes beállítását itt egyben kezelem
- | | — [arg.py](#) - A beállítások argumentum típusai
- | | — [config\\_base.py](#) - A the\_config őse. Garantálja, hogy singleton legyen
- | | — [config\\_factory.py](#) - A config osztály létrehozója
- | | — [\\_\\_init\\_\\_.py](#) - A csomag inicializálója
- | | — [the\\_config.py](#) - A konfigurációs opciók (ide lehet új beállításokat rakni)
- | | — [the\\_config\\_variables.py](#) - A konfigurációs változók, amiket aztán fel lehet használni a konfiguráció írásakor
- | | — [tools.py](#) - Segéd eszközök a konfigurációhoz
- | — [data\\_manager](#) - A felhasználói adatok kezelése
- | | — [file\\_manager.py](#) - Fájlok (és mappák) kezelése
- | | — [\\_\\_init\\_\\_.py](#) - A csomag inicializálója
- | — [error\\_object](#) - Központosított hiba objektumok, a szerveren és a kliens oldalon is elérhetőek
- | | — [enum2.py](#) - Enum kibővítése
- | | — [error\\_object.py](#) - Egy Hiba objektum osztálya
- | | — [error\\_type\\_enum.py](#) - A hibák típusának enum-ja
- | | — [error\\_type.py](#) - Egy hiba típus osztálya
- | | — [error\\_types.py](#) - Az összes fajta hiba típus (új hibatípust ide kell felvenni)
- | | — [get\\_error\\_type\\_dict.py](#) - Egy json-t csinál a hibatípusokból
- | | — [\\_\\_init\\_\\_.py](#) - A projekt inicializálója
- | — [js\\_generator](#) - JavaScript-et generál
- | | — [\\_\\_init\\_\\_.py](#) - A projekt inicializálója
- | | — [js\\_generator.py](#) - JavaScript generátor
- | — [log](#) - Logokért felelős csomag
- | | — [\\_\\_init\\_\\_.py](#) - A csomag inicializálója
- | | — [log.py](#) - A python logging inicializálása
- | — [rpc\\_wrapper](#) - A szerver és a kliens közötti kommunikációért felelős osztály "felső rétege", a meghívható függvények gyűjteménye, és autentikálás biztosítása
- | | — [auth\\_wrapper.py](#) - A hitelesítésért felelős wrapper függvény

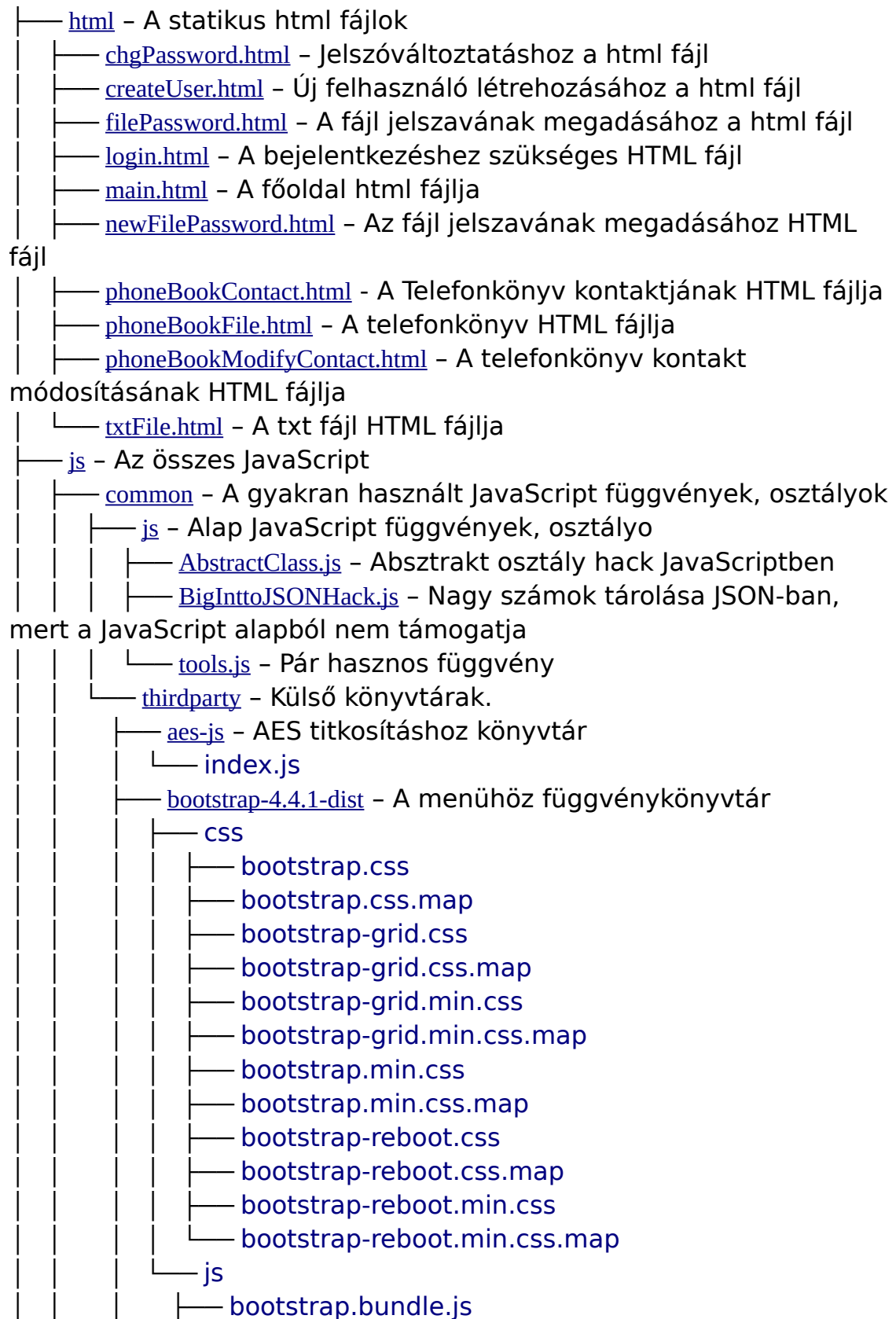
- | | [\\_\\_init\\_\\_.py](#) - A csomag inicializálása
- | | [rpc\\_wrapper.py](#) - A függvények, amiket a kliens is elér
- | | [web\\_method.py](#) - Jelzi az prc\_wrapperben, ha egy függvény elérhető a kliens oldalon is
- | — [server](#) - Tornado webserver, mind a statikus adatok kiszolgálásáért, mind az RPC “alsó rétegéért felel”
- | | — [data\\_request\\_handler.py](#) - A generált adatokért: felel
- generated/data.js
- | | — [\\_\\_init\\_\\_.py](#) - A csomag inicializálása
- | | — [redirector\\_request\\_handler\\_factory.py](#) - HTTP szerver, ami átirányít a titkosított szerverre
- | | — [rpc\\_request\\_post\\_handler\\_factory.py](#) - JSON RPC hívások POST protokollon keresztül
- | | — [rpc\\_request\\_ws\\_handler\\_factory.py](#) - JSON RPC hívások WebSocket protokollon keresztül
- | | — [rpc\\_wrapper\\_factory.py](#) - Az RPC szerver létrehozása
- | | — [web\\_request\\_handler\\_factory.py](#) - A statikus fájlok kiszolgálója
- [sha256Salty](#) - Hashelés SHA256 szózással csomagja
- | | — [\\_\\_init\\_\\_.py](#) - Csomag inicializálása
- | | — [sha256Salty2.py](#) - Az egyik szózott hash algoritmus
- | | — [sha256Salty.py](#) - A másik szózott hash algoritmus
- [config.json](#) - Config fájl (nem verziókövetett)
- [config.sample.json](#) - Config fájl példa verziókövetett
- [config.test.json](#) - Config fájl, a config.\*.json fájlok nem verziókövetettek kivétel a sample
- [create\\_user.py](#) - Felhasználó létrehozása
- [run\\_server.py](#) - szerver inicializálása, és futtatása
- [tools\\_create\\_config\\_csv.py](#) - A configokból csinál csv-t
- [tools\\_create\\_config\\_ods.py](#) - A configokból csinál ods-t
- [tools\\_create\\_html\\_file\\_dict.py](#) - A statikus html fájlok nevéből csinál egy JSON-t
- [tools\\_getclasses.py](#) - Az összes html fájlból kinyeri a class mezőket

## Kliens oldal

src/web

- | — [generated](#) - A generált fájlok mappája
- | | — [data.js](#) - Adatok (theConfig, errorObjects,...)
- | | — [theHtmlClasses.js](#) - HTML Classes







- [TxtFile.js](#) - Txt fájl osztály, ami SecretFile
    - [pageloader](#) - Az oldalak letöltésével, és betöltésével foglalkozik
    - [HtmlDownloader.js](#) - A html oldalak letöltése
      - [PageLoaderService.js](#) - Az oldalak betöltése
      - [UserManager](#) - A felhasználókkal foglalkozik
      - [UserManagerService.js](#) - A felhasználók osztálya
      - [UserManagerServiceMock.js](#) - A felhasználók osztályának kimockolt verziója
  - [interfaces](#) - Interfészek
    - [encrypt](#) - Titkosítók
      - [Iencryptor.js](#) - Kétirányú titkosító interface
      - [Ihash.js](#) - Egy irányú titkosító interface
    - [file](#) - Fájl interfészek
      - [IsecretFile.js](#) - Titkos fájl interfész
    - [RPC](#) - RPC interfészek
      - [IRPCClient.js](#) - RPC kliens interfész
    - [UserManager](#) - User manager interfészek
      - [IuserManagerService.js](#) - User manager interfész
  - [lib](#) - Könyvtárak
    - [encrypt](#) - Titkosító könyvtárak
      - [AESEncryptor.js](#) - Kétirányú titkosító könyvtár AES-t használva
      - [SHA256Salty.js](#) - Egyirányú titkosító könyvtár SHA256-ot használva szóva
    - [ErrorObject](#) - Hiba objektum könyvtár
      - [ErrorObject.js](#) - Hiba objektum könyvtár
    - [RPCWrapper](#) - RPC wrapper könyvtár
      - [RpcClients.js](#) - Az elérhető RPC kliensek tárolója (window.theRpcClients)
    - [RPCWrapperService.js](#) - Az összes elérhető RPC függvény
    - [SimpleJsonRpc](#) - A SimpleJsonRpc osztályok az adatátvitelhez
    - [SimpleJsonRpcPOSTClientService.js](#) - RPC adatátvitel HTTP POST protokollal
    - [SimpleJsonRpcWebSocketClientService.js](#) - RPC adatátvitel WS protokollal
  - [test](#) - tesztek
    - [webtest](#) - webtesztek
    - [lib](#) - könyvtárak a webteszthez

- | | | | — [createFile.js](#) - robotkattintgatással fájl létrehozása
- | | | | — [login.js](#) - robotkattintgatással bejelentkezés
- | | | | — [phonebook.js](#) - robotkattintgatással telefonkönyv manipulációk
- | | | | — [tools.js](#) - eszközök a web-teszthez
- | | | | — [dataMedia.js](#) - Telefonkönyv adatok az ELTE oldaláról
- | | | | — [getDataFromMedia.js](#) - adatok letöltéséhez segéd szkript az ELET oldaláról
- | | | — [testPhoneBookAddContacts.js](#) - Egy teszt, ami létrehoz egy telefonkönyvet, és feltölti adatokkal
- | | — [htmlFileDict.js](#) - A htmlFájlok JSON-ja
- | | — [main.js](#) - A main JavaScript fájl
- | — [style](#) - Az oldal stílusa
- | — [bootstrap.min.css](#) - Bootstrap-hoz stílus lap
- | — [bootstrap.min.css.map](#) - Bootstrap-hoz stílus lap
- | — [style.css](#) - saját stílus lap
- | — [favicon.ico](#) - ikon
- | — [index.html](#) - főoldal
- | — [testPhoneBook.html](#) - A telefonkönyv teszt indítása

## Tesztelési terv

A txt fájlok teszteléséhez Arany János összes költeményeit használom:

<https://mek.oszk.hu/00500/00597/html/index.htm>

A telefonkönyvek teszteléséhez az ELTE honlapján elérhető telefonszámokat használom:

1. ELTE IK Média- és Oktatásinformatikai Tanszék > A Tanszékről > Oktatók és munkatársak

<https://mot.inf.elte.hu/munkatarsak>

## Előkészületek

Létrehozok egy üres adatbázist a projekt mellé, és megcsinálom a szükséges config fájlt:

```
{
"host": "localhost",
```

```

"logFile":"/var/tmp/rpd_test_[[now]].log",
"open_port":11080,
"secure_port":11443,
"enable_create_user": true,
"logLevel":"DEBUG",
"show_encrypted_data": true,
"crt_file": "[[dir_project]]/../../key/rpd.crt",
"key_file": "[[dir_project]]/../../key/rpd.key",
"web_root": "[[dir_project]]/src/web",
"data_dir": "[[dir_project]]/../../test_data"
}

```

## 1. eset: A szerver elindítása (black box)

`./run_server --configFile config.test.json`

### *Elvárt eredmény*

#### 1. Loggolja a konfigurált beállításokat:

```

[2020-04-08 12:25:01,276][INFO] Loglevel: INFO
[2020-04-08 12:25:01,440][INFO] Runner command: ./run_server.py --configFile
config.test.json
[2020-04-08 12:25:01,440][INFO] Config:
[2020-04-08 12:25:01,440][INFO] configFile: config.test.json
[2020-04-08 12:25:01,440][INFO] debug: False
[2020-04-08 12:25:01,440][INFO] logLevel: INFO
[2020-04-08 12:25:01,440][INFO] logFile: /var/tmp/rpd_test_20200408_122501.log
[2020-04-08 12:25:01,440][INFO] logFormat: [%s][%(levelname)s] %
(message)s
[2020-04-08 12:25:01,440][INFO] show_rpc_message: False
[2020-04-08 12:25:01,440][INFO] open_port: 11080
[2020-04-08 12:25:01,440][INFO] debug_open_port: 8081
[2020-04-08 12:25:01,440][INFO] secure_port: 11443
[2020-04-08 12:25:01,441][INFO] host: localhost
[2020-04-08 12:25:01,441][INFO] crt_file:
/home/somla/working/rpd/master/../../key/rpd.crt
[2020-04-08 12:25:01,441][INFO] key_file:
/home/somla/working/rpd/master/../../key/rpd.key
[2020-04-08 12:25:01,441][INFO] web_root: /home/somla/working/rpd/master/src/web
[2020-04-08 12:25:01,441][INFO] data_dir:
/home/somla/working/rpd/master/../../test_data

```

```
[2020-04-08 12:25:01,441][INFO] test_dir: /var/tmp/real_private_data
[2020-04-08 12:25:01,441][INFO] salt: My own Salt
[2020-04-08 12:25:01,441][INFO] server_salt: Server salt
[2020-04-08 12:25:01,441][INFO] enable_create_user: True
[2020-04-08 12:25:01,441][INFO] show_encrypted_data: True
[2020-04-08 12:25:01,441][INFO] defaultRpcClient:
SimpleJsonRpcWebSocketClientService
[2020-04-08 12:25:01,441][INFO] hideMessageTime: 4000
```

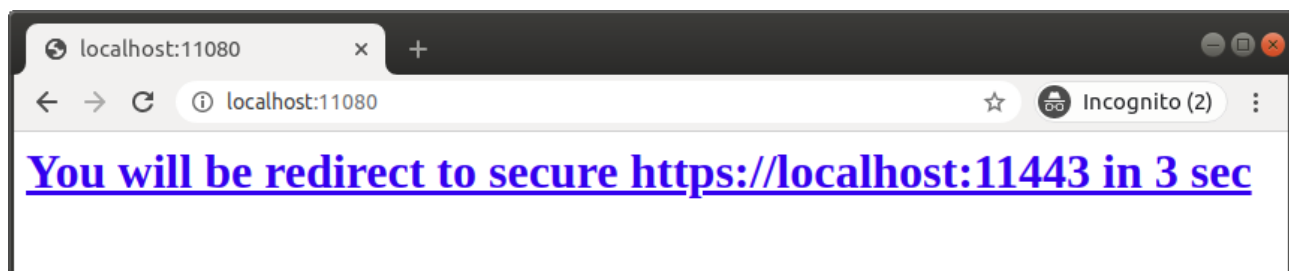
## 2. logolja a szerver elérhetőségeit:

```
[2020-04-08 12:25:01,443][INFO] HTTPS Server starting... https://localhost:11443/
[2020-04-08 12:25:01,444][INFO] HTTP redirect Server starting...
http://localhost:11080/
```

## 3. írja ki őket a /var/tmp/rpd\_test\_\*.log (a \* helyére az aktuális dátumot várom)

A /var/tmp/rpd\_test\_20200408\_122501.log fájl tényleg létrejött, és tényleg ugyanaz van benne, mint a képernyőn.

## 4. A <http://localhost:11080/> -re kattintva jussunk el az átirányító oldalra, és az irányítson át minket a titkosított oldalra



3 másodperc múlva



## 2. eset: Felhasználók létrehozása konzolból (black box)

2 felhasználót fogok létrehozni

**Felhasználónév:** test\_user1 **password:** password1

**Felhasználónév:** test\_user2 **password:** password2

```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: test_user1
Enter your password:
Enter your password again:
Registration was successfully
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: test_user2
Enter your password:
Enter your password again:
Registration was successfully
~/working/rpd/master/src/python:master$
```

### *Elvárt eredmény*

1. Hozzon létre két felhasználói mappát:

```
File Edit View Search Terminal Help
~/working/rpd/test_data$ ls
a6685c94348208f0316c8ba67b0df0897a7f820c286a126649c81bf42aa13fd2
d4efaef0a0d894920ccc97ada5a54f04555a1621d4c050e7af8348b598daeee7
~/working/rpd/test_data$
```

2. Be tudjak lépni a felhasználókkal, ezt lásd lejjebb a bejelentkezés tesztelésénél.

### 3. eset: Üresen hagyott mezők felhasználó létrehozása közben

Vagy a felhasználónevet, vagy a jelszó mezőt, vagy mindkettőt hagyjuk üresen

#### *Elvárt eredmény*

Username and/or password is empty üzenet, a data dir változatlan hagyása

```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username:
Enter your password:
Enter your password again:
Username and/or password is empty
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username:
Enter your password:
Enter your password again:
Username and/or password is empty
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: user
Enter your password:
Enter your password again:
Username and/or password is empty
~/working/rpd/master/src/python:master$
```

### 4. eset: jelszó és jelszó mégegyszer nem egyezik (CLI)

```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: Gibbs Jakab
Enter your password:
Enter your password again:
password and password again is not equal
~/working/rpd/master/src/python:master$
```

#### *Elvárt eredmény*

Hibaüzenet, test\_data dir ne változzon



## 5. eset: Létező felhasználó hozzáadása azonos jelszóval

Meg kell jegyezzem, hogy itt a felhasználónév és a jelszó páros azonosít egy felhasználót, így például **User1/password1** és **User1/password2** nem ugyanaz a felhasználó.

Gondolkodtam ennek javításán, de nem igazán lehetséges úgy, hogy ne adjon többlet információt a szerver üzemeltetőjének a felhasználóról.

test\_user1/password1

```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: test_user1
Enter your password:
Enter your password again:
Error:User has been already registrated
~/working/rpd/master/src/python:master$
```

### *Elvárt eredmény*

Hibaüzenet, test\_data dir ne változzon

## 6. eset: Létező felhasználó hozzáadása más jelszóval (cli)

test\_user1/password2 létrehozása

```
File Edit View Search Terminal Help
~/working/rpd/master/src/python:master$ ./create_user.py --configFile config.test.json
Enter your username: test_user1
Enter your password:
Enter your password again:
Registration was successfully
~/working/rpd/master/src/python:master$
```

### *Elvárt eredmény*

1. Hozzon létre egy új felhasználói mappát

```
File Edit View Search Terminal Help
~/working/rpd/test_data$ ls
703b4893807033a93c5c2782ea515205c2fccd1ee8cc8e7958ece471a1dbad2c
a6685c94348208f0316c8ba67b0df0897a7f820c286a126649c81bf42aa13fd2
d4efaef0a0d894920ccc97ada5a54f04555a1621d4c050e7af8348b598daeee7
~/working/rpd/test_data$
```

2. Be tudjak lépni az új felhasználóval, ezt lásd lejjebb a bejelentkezés tesztelésénél.

## 7. eset: Belépés hibás jelszóval (GUI)

Bejelentkezés a következő felhasználókkal

Felhasználónév	Jelszó
I am not exist	I am not exist
test_user1	almafa
test_user2	dinnye

(SimpleJsonRpcWebSocketClientService és SimpleJsonRpcPOSTClientService segítségével is)

### *Elvárt eredmény*

Hibaüzenet

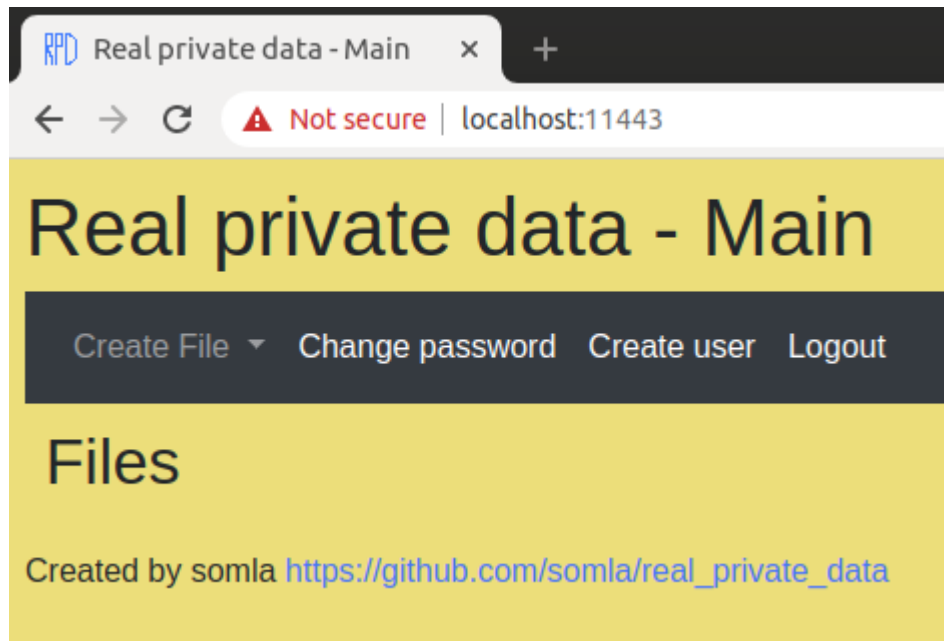
## 8. eset: Bejelentkezés valós felhasználókkal (GUI)

Bejelentkezés a következő felhasználókkal (SimpleJsonRpcWebSocketClientService és SimpleJsonRpcPOSTClientService segítségével is)

Felhasználónév	Jelszó
test_user1	password1
test_user1	password2
test_user2	password2

### ***Elvárt eredmény***

Bejelentkezés az oldalra, és a main oldalra irányítás.

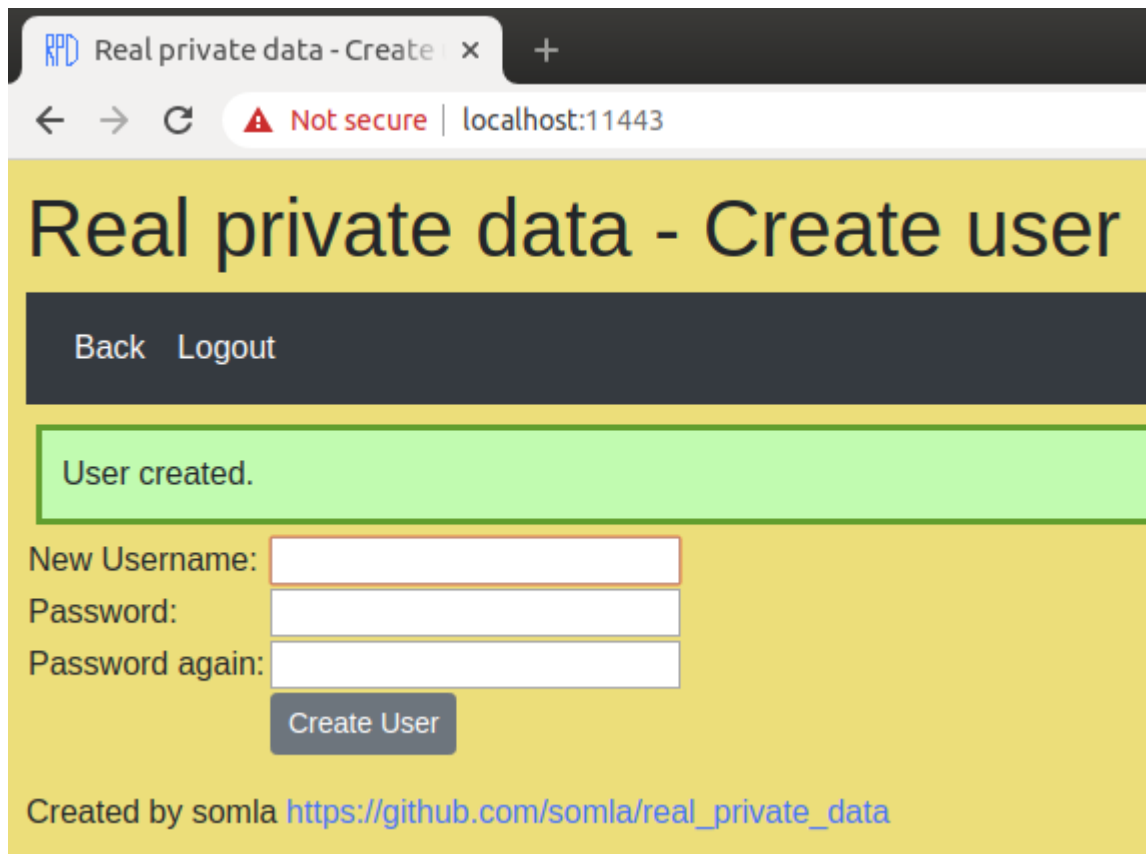


### **9. eset: Felhasználó létrehozása (GUI)**

**test\_user3/password3** létrehozása

### ***Elvárt eredmény***

1. sikeres létrehozás



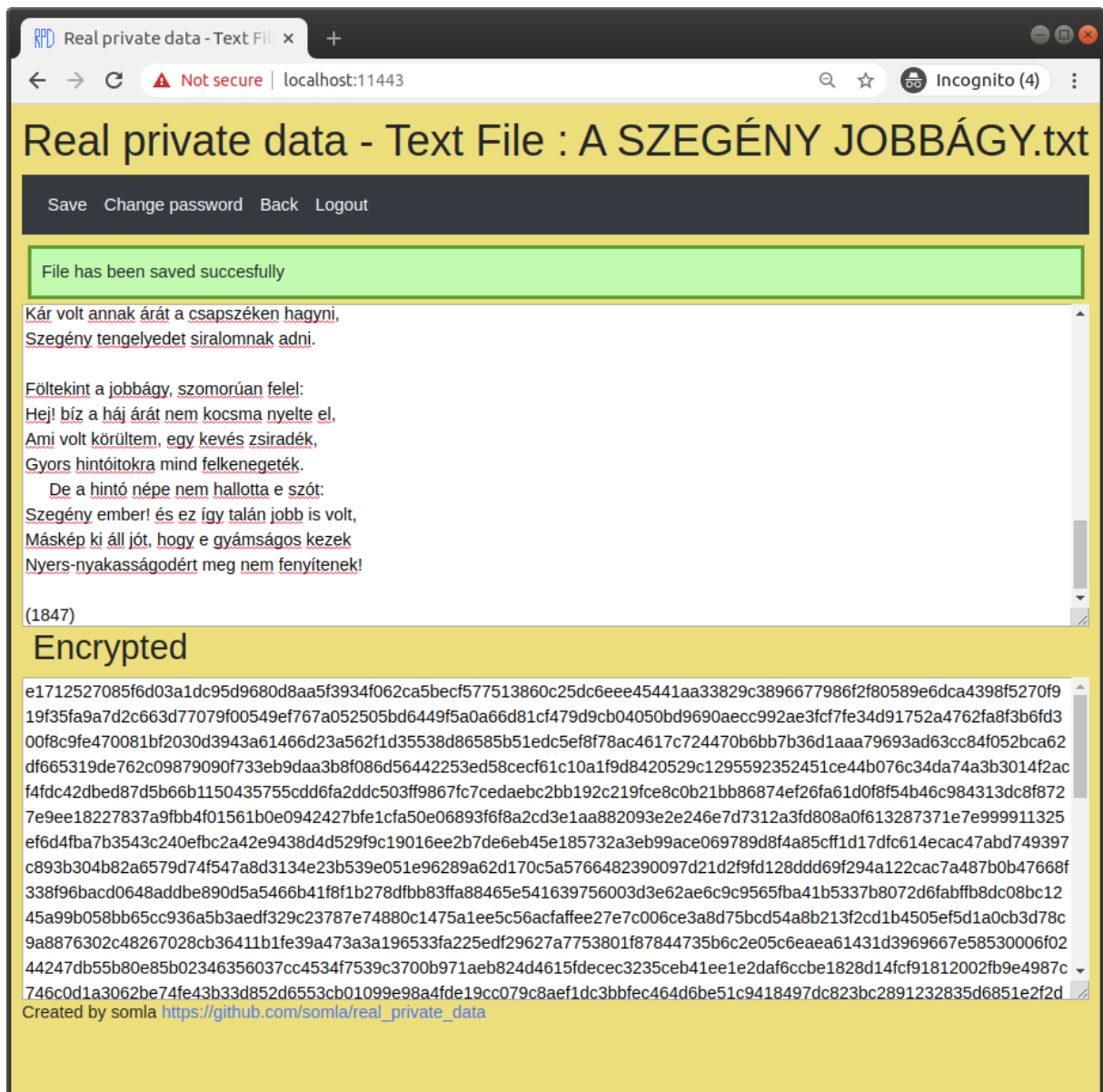
2. sikeres bejelentkezés az új felhasználóval (lásd **8. eset: Bejelentkezés valós felhasználókkal (GUI)** ).

## 10. eset: Txt Fájl létrehozása

Hozzunk létre pár txt fájlt.

### ***Elvárt eredmény***

A fájlok létrejönnek, és meg is tudjuk őket nyitni, lásd lejjebb



## 11. eset: Telefonkönyv fájl létrehozása

Ehhez csináltam egy teszt robotot, ami létrehoz egy Telefonkönyv fájlt, és feltölti adatokkal.

<https://localhost:11443/testPhoneBook.html>

**waitTime:** Megmondja, hogy mennyit várjon a teszt két művelet között

**username:** Melyik felhasználóval lépjen be

**password:** Mi a felhasználó jelszava

**fileName:** Mi legyen a létrehozandó fájl neve

**filePassword:** Mi legyen a jelszava

The screenshot shows a web browser window with the title 'Real private data - Login'. The address bar shows 'Not secure | localh...' and 'Incognito (2)'. The page has a yellow background. The main heading is 'Real private data - Login'. Below it, there is a section for 'RPC Client' with two radio buttons: 'SimpleJsonRpcWebSocketClientService' (selected) and 'SimpleJsonRpcPOSTClientService'. Below this are input fields for 'Username:' and 'Password:', followed by a 'Login' button. A 'Test' section follows, containing input fields for 'waitTime:' (400), 'username:' (test\_user1), 'password:' (password1), 'fileName:' (ELTE IK Média- és Oktatásir), and 'filePassword:' (Media), with a 'Start Test' button. At the bottom, it says 'Created by somla' followed by a GitHub link.

Real private data - Login

RPC Client: ☒ SimpleJsonRpcWebSocketClientService  
☐ SimpleJsonRpcPOSTClientService

Username:

Password:

Login

Test

waitTime:

username:

password:

fileName:

filePassword:

Start Test

Created by somla [https://github.com/somla/real\\_private\\_data](https://github.com/somla/real_private_data)

### ***Elvárt eredmény***

A fájl létrehozása, és a telefonkönyv adatok tárolása.

## **12. eset: Nézzük meg, hogy a szerveren tárolt adatok tényleg titkosak-e**

1. Kilistázzuk a mappákat tee paranccsal
2. megnézzük a fájlokat cat paranccsal
3. megnézzük a fájlokat hexdump paranccsal

```

File Edit View Search Terminal Help
~/working/rpd/test_data$ tree
.
├── 703b4893807033a93c5c2782ea515205c2fccd1ee8cc8e7958ece471a1db
ad2c
├── a6685c94348208f0316c8ba67b0df0897a7f820c286a126649c81bf42aa1
3fd2
│   ├── 003fc8ec29bc1a8c50f0c4408a674344176e37208b13fa017e0e32e6
46d9ca6b8b54d4258da4db6b9aa9e611ee252faa641e684129e07424e22807ea
3ea471b50bad5c2758bcc37bfc5eced07028fb66d7d085
│   ├── 043fceba26bd15d153a493458d344618413b6b27df1ef901290f3de1
408ac83fd80e83248af78a6d9ba5b21fef2579ab62166b142fe12421b2295de2
39ac74b50bad42be94b320afd4a2d1b7129f88b22efa86af09d91
│   ├── 066acdba28ea1ad053f2c4168c624b4f126a6a77d61af855225736e5
408a9d3fdd55d427d8f08a6acefdb512b6297ea9311b6e172be12425b77257e0
3aae21e40bdf50aa88b5aa64fb5c577f4a13ce
│   ├── 076ccdb42ce846df00f7ce11dc66404c133b3f25df13aa53230f36b9
168d9f32db0584278cf08a3cccac013e4277bae641e60142ce02874e27e5ce7
3cf871e50fca48af9ea6aa09e7524392b33fec8b22e6a80bc9c5a0c49a4cf1ee
85b4c6640bfc21732aebcc512bf5
│   ├── 5136c9ef2de715d057a7c7108e3d444c433e6c71d848ff017c0567b6
1b8acf6bd501852388a38b6dcef9e740e3202efe30186f142ce87725e47906e1
6fab72e70bad47a583a620ba935f4892bf25e307e886853cf0
│   ├── 516fc9bd27ed1a8a50a094438d30441a416c3b22d818ae012d0f30b7
44dfcb6cdf54d3738df0da6ec9f8e113ef2378ff301f681578e82220e92a57b6
3aa824e81c4e90a890a7b909e3565994ae2df306e6e3df30fc91
│   └── 5668cdbf7ae6428851f293178132401d156e6927dd18f8042b5733b3
1b889f6c8b03d9278ea48f38ceacb611b5257efd644d61117eb32521b02d52b3
61a476b70fc145a1f1bda809fed0a435570a976860018264cb8e91e8a24cd9d6
a719364520c7838e01c5834c73d59bdd29d96144ff8fcf3385
├── cd1699c8134c04ca727a99e2652250e7fd37bbfce14e9c41a539fe67b3bf
e17a
└── d4efaef0a0d894920ccc97ada5a54f04555a1621d4c050e7af8348b598da
eee7

4 directories, 7 files
~/working/rpd/test_data$

```

Itt látható, hogy mind a mappák (felhasználók nevei), és a benne lévő fájlok nevei is titkosítottak.





## A teszt közben létrejött felhasználók és fájlok

### *Felhasználók*

Felhasználónév	Jelszó
test_user1	password1
test_user1	password2
test_user2	password2
test_user3	password3

### *Fájlok*

Felhasználó	Fájl	Jelszó
test_user1/password1	A MÉH ROMÁNCA.txt	Petofi
test_user1/password1	A SZEGÉNY JOBBÁGY.txt	Petofi
test_user1/password1	A VARRÓ LEÁNYOK.txt	Petofi
test_user1/password1	ARANYAIMHOZ.txt	Petofi
test_user1/password1	EGYKORI TANÍTVÁNYOM EMLÉKKÖNYVÉBE.txt	Petofi
test_user1/password1	VÁLASZ PETŐFINEK.txt	Petofi
test_user1/password1	ELTE IK Média- és Oktatásinformatikai Tanszék.phb	Media