Universiteti i Prishtinës
Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike

Projekti në lëndën Siguria e të Dhënave

Faza e tretë

Blerim Rexha, Arbnor Halili, Edon Gashi

Maj 2020

Abstrakt: Në fazën e tretë të projektit ju do ta zgjeroni programin tuaj me menaxhim të fjalëkalimeve dhe vërtetim të autenticitetit përmes nënshkrimeve digjitale. Ju lusim ta lexoni me kujdes këtë dokument dhe të veproni sipas udhëzimeve.

Përmbajtja

Kërkesat

Detyra juaj është ta zgjeroni programin ekzistues të fazës së parë dhe të dytë me komanda të reja si dhe t'i avansoni ato ekzistueset.

Pasi që do ta zgjeroni programin ekzistues, ju duhet ta vazhdoni punën në të njëjtin repository dhe me të njëjtën gjuhë programuese. Pra, duhet ta keni parasysh që:

- Duhet të vazhdohet programi ekzistues, e jo të krijohet i ri.
- Kërkesat të plotësohen ashtu siç janë specifikuar.
- Të gjitha veprimet të kryhen nga programi i njëjtë, pra jo nga një program për secilën komandë.
- Kodet që i merrni të gatshme nga interneti duhet të referencohen në `README`.

Në rast se vendosni ta ndryshoni platformën ose gjuhën programuese, ju duhet t'i ri-implementoni të gjitha kërkesat e fazës së parë dhe të dytë në gjuhën e re, përndryshe konsiderohen të paplotësuara dhe ju anulohen pikët e arritura.

Rregullat për përpunimin e argumenteve janë të njëjta me fazat e kaluara: Në rast se argumentet mungojnë ose janë të jo-valide, atëherë do ta shfaqni një tekst me udhëzime rreth përdorimit dhe do ta mbyllni programin me kod dalës (exit code) 1. Poashtu, nëse gjatë ekzekutimit ka ndonjë dështim për shkak të hyrjeve jo-valide ose ndonjë gabimi gjatë shkrim-leximit në fajlla, programi duhet ta trajtojë gabimin dhe ta shfaqë në ekran një mesazh përshkrues.

Në vazhdim e gjeni specifikimin e komandave, ku përfshihen edhe shembuj të përdorimit të tyre.

Komanda create-user

Sintaksa: `ds create-user <name>`

Ju do ta zgjeroni komandën `create-user` ashtu që gjatë krijimit të shfrytëzuesit të kërkohet edhe fjalëkalimi.

Fjalëkalimi duhet të kërkohet përmes inputit, pasi që nuk preferohet të figurojë në histori. Fjalëkalimi duhet të ketë gjatësinë së paku 6 karaktere dhe duhet të përmbajë së paku një numër ose simbol.

Shembull:

```
$ ds create-user edon
Jepni fjalekalimin: fiek2018
Perserit fjalekalimin: fiek2018
Eshte krijuar shfrytezuesi 'edon'
Eshte krijuar celesi privat 'keys/edon.xml'
Eshte krijuar celesi publik 'keys/edon.pub.xml'

$ ds create-user arbnor
Jepni fjalekalimin: siguria
Gabim: Fjalekalimi duhet te permbaje se paku nje numer ose simbol.

$ ds create-user blerim
Jepni fjalekalimin: siguria_1
Përsërit fjalekalimin: siguria
Gabim: Fjalekalimet nuk perputhen.
```

Pikë shtesë: Të lexohet fjalëkalimi pa echo të simboleve në ekran (sikur `read -s`).

Kur krijohet shfrytëzuesi ju do ta ruani në bazë të shënimeve. Shënimet mund t'i ruani sipas dëshirës, psh. nëpër fajlla ose në ndonjë DBMS.

Fjalëkalimin e shfrytëzuesit do ta ruani në formë të sigurt përmes hash algoritmeve dhe salting. Detajet e mënyrës së gjenerimit dhe ruajtjes janë sipas dëshirës.

Komanda delete-user

Kur të thirret kjo komandë do të fshihen edhe të gjitha të dhënat e shfrytëzuesit nga baza e shënimeve.

Komanda login

Sintaksa: `ds login <name>`

Teston çiftin shfrytëzues/fjalëkalim. Në rast suksesi lëshohet një token i nënshkruar i cili mund të përdoret për autentikim të shfrytëzuesit.

Mënyra e ruajtjes së tokenit është sipas dëshirës, psh. ju mund ta lëshoni një JWT, një XML të nënshkruar, ose ndonjë format të vet-definuar. Me rëndësi është që për nënshkrim të tokenit të përdoret çelësi privat i shfrytëzuesit, ndërsa për vërtetim të nënshkrimit të përdoret çelësi publik i shfrytëzuesit.

Tokeni skadon pas 20 minutave. Tokeni mund të përdoret vetëm për shfrytëzuesin për të cilin është lëshuar.

Shembull:

```
$ ds login edon
Jepni fjalekalimin: fiek2018
Token: dG9rZW5pIGkgbmVuc2hrcnVhci4u...

$ ds login arbnor
Jepni fjalekalimin: 123
Gabim: Shfrytezuesi ose fjalekalimi i gabuar.
```

Pikë shtesë: Të lexohet fjalëkalimi pa echo të simboleve në ekran (sikur `read -s`).

Komanda status

Sintaksa: `ds status <token>`

Jep informata rreth tokenit.

```
$ ds status dG9rZW5pIGkgbmVuc2hrcnVhci4u...
User: edon
Valid: po
Skadimi: 21/05/2020 17:23
```

Nëse tokeni ka skaduar, nuk ka nënshkrim valid, ose nuk ekziston shfrytëzuesi, atëherë tokeni nuk konsiderohet valid.

Komanda write-message

Kjo komandë zgjerohet ashtu që mund ta pranojë edhe opsionin `--sender <token>`.

Nëse specifikohet ky opsion, atëherë mesazhi merr formën e zgjeruar:

```
ciphertext =
  base64(utf8(<name>)) . base64(<iv>) . base64(rsa(<key>))
  . base64(des(<message>)) . base64(utf8(<sender>))
  . base64(signature(des(<message>)))
```

Vlera `sender` është emri i shfrytëzuesit që i korrespondon tokenit `token`. Komanda dështon nëse tokeni nuk është valid ose ka skaduar.

Nëse validohet tokeni me sukses, atëherë nënshkrimi bëhet me çelësin privat të dërguesit `sender`.

Komanda read-message

Komanda `read-message` zgjerohet ashtu që nëse figuron pjesa e dërguesit/nënshkrimit në mesazh, atëherë do të tentohet verifikimi i atij nënshkrimi duke përdorur çelësin publik të dërguesit.

Nëse mungon pjesa e dërguesit/nënshkrimit, atëherë komanda e injoron dhe vepron sikur në fazën e dytë.

Shembull:

```
$ ds read-message "ZWRvbg==.MTIzNDU2Nzg=.cnNhKGZpZWsyMDE4KQ==.ZGVz..."
Marresi: edon
Mesazhi: Takimi mbahet te premten ne ora 11:00
Derguesi: arbnor
Nenshkrimi: valid
```

Ekziston mundësia që marrësi nuk e ka çelësin publik të dërguesit:

```
$ ds read-message "ZWRvbg==.MTIzNDU2Nzg=.cnNhKGZpZWsyMDE4KQ==.ZGVz..."
Marresi: edon
Mesazhi: Takimi mbahet te premten ne ora 11:00
Derguesi: arbnor
Nenshkrimi: mungon celesi publik 'arbnor'
```

Vlerësimi

Kjo fazë vlerësohet me maksimalisht 10 pikë.

Ju do të gjykoheni në bazë të:

- Kërkesave të plotësuara.
- Cilësisë së kodit.
- Korrektësisë në menaxhimin e repository.
- Njohurive teorike.
- Njohurive teknike.

Dorëzimi

Repository ekzistues mund ta përditësoni deri më datën **07.06.2020 23:59**.

Në `README` duhet të figurojnë këto informata:

1. Udhëzimet për kompajllimin dhe ekzekutimin e programit.
2. Detajet e implementimit për:
    - Skemën e ruajtjes së fjalëkalimeve.
    - Mënyrën e ruajtjes së shënimeve.
    - Strukturën e tokenëve të lëshuar.

Gjithashtu kujdesuni ta keni ose ta përditësoni `.gitignore` adekuate ashtu që mos të ngarkohen fajlla të padobishëm në repository.

Kujdes: Cilido lloj i plagjiaturës, qoftë në kod apo në përshkrim, do të ndëshkohet me **0 pikë për të gjitha grupet ku gjendet materiali i kopjuar**, pavarësisht se cili grup e ka punuar i pari.