TURVALLINEN OHJELMOINTI, TIE-30601

TENTTI 26.2.2020 Marko Helenius

Tentissä ei saa käyttää oheismateriaalia eikä laskinta.

1. Tarkastele oheisia ohjelmien osia. Mitä haavoittuvuuksia tai ongelmia niissä on, mitä niistä voi seurata ja miksi? Laita mukaan esimerkki tai tarvittaessa esimerkkejä vaarallisista syötteistä. Miten korjaisit ohjelmaa? (2 pistettä/kohta)

a)

```
#!/usr/bin/python
luku = 1.0
summa = 0.0
lkm=0
print "Annà luvut, 0 lopettaa"
while luku!=0:
    luku = float(input("Anna luku: "))
    summa += luku
    if (luku!=0):
        lkm += 1
keskiarvo = (summa / lkm)
print "Lukujen keskiarvo on ", keskiarvo
```

b)

```
#define MAX 2048

int main(int argc, char **argv) {
  char *taulukko;
  char *taulukko2 = (char *) malloc(MAX);
  taulukko = (char *) malloc(MAX);
  strcpy(taulukko, argv[1]);
  strcpy(taulukko2, taulukko);
  printf(taulukko2);
}
```

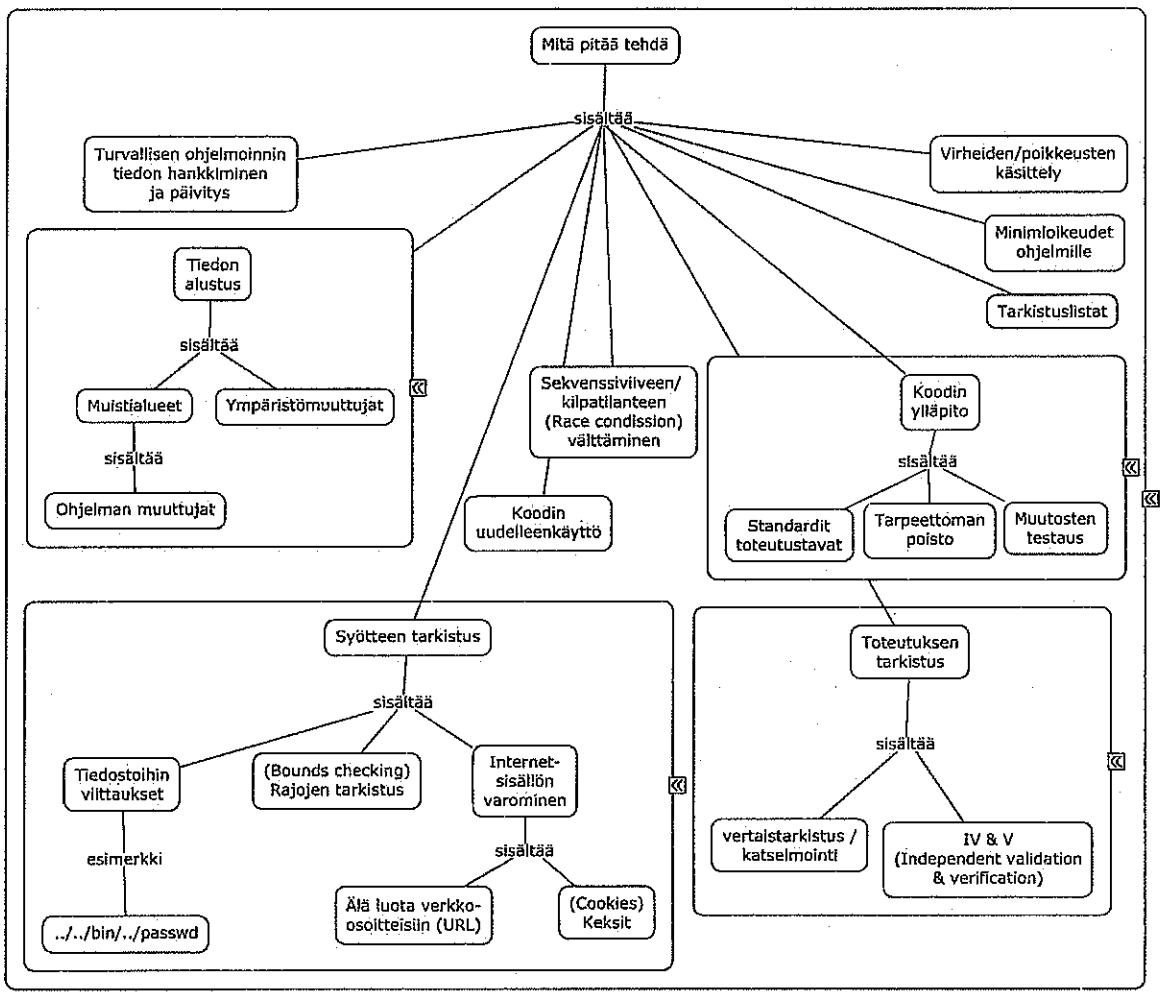
c)

```
//Ohjelma suoritetaan ylläpitäjän oikeuksilla peruskäyttäjänä (setuid root)
FILE *secure_file
...
//Tarkistetaan, että tiedosto on olemassa ja siihen on kirjoitusoikeudet
if ((access "/secure.txt", W_OK) == 0)){
   secure_file = fopen("/secure.txt", "wb+"); //Tiedosto avataan
...
   fclose(secure_file);
   }
```

2. Miten Cross-Site Request Forgery –haavoittuvuus (CSRF) toimii ja millä eri tavoin siltä voidaan suojautua?

3. Mitä ovat "Security User Stories" ja miten niitä käytetään ohjelmistokehityksessä?

4. Kirjoita oheisen kuvan perusteella essee.



Käännä!