Tudorache Alexandru-Theodor

Grupa 342

Laborator 7

Securitatea Sistemelor Informatice

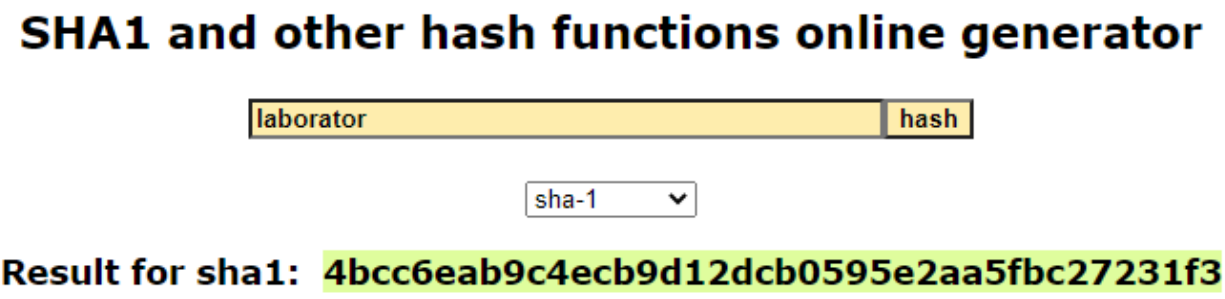
1.

a) Adevarat

b) Fals

c) Adevarat

d) Adevarat



e) Fals

f) Fals

g) Fals

3.

- Exemplul 1

  Valoarea secretKey-ului este scrisa explicit in cod. (Este hard-codata)

  Pentru stocarea parolei ar trebui folosita o functie hash.

- Exemplul 2

  Numele user-ului este hash-uit, desi acest lucru nu este necesar. (Redundanta)

- Exemplul 3

Hash-uirea este facuta fara a folosi un salt. Ar trebui utilizat un salt.

Deoarece se face o singura iteratie de SHA, parola poate fi sparta cu usurinta. Ar trebui folosite mult mai multe iteratii de SHA pentru ca parola sa fie stocata in siguranta.

- Exemplul 4

Valorea salt-ului este scrisa explicit in cod. (Este hard-codata)

- Exemplul 5

Hash-uirea este facuta fara a folosi un salt. Ar trebui utilizat un salt.

Functia hash MD5 nu este considerate sigura la coliziuni. Ar trebui folosita functie de hash-uire a parolei.