Tema 8 – Lab SSI

Ex 1:

a) Adevarat – odata realizata prajitura nu o putem readuce la starea initiala;
b) Fals - https://security.stackexchange.com/questions/37454/why-are-md5-collisions-dangerous
c) Adevarat
d) Adevarat - http://www.sha1-online.com/
e) Fals deoarece nu putem decripta;
f) Adevarat – altfel ar putea ingreuna o sumedenie de sisteme informatice incat ar deveni neplacute de folosit;
g) Fals - https://www.md5online.org/md5-decrypt.html

Ex 3:

a) Metoda prezentata este vulnerabila deoarece in caz de atacatorul ghiceste cheia poate decripta foarte usor parola in plain text;

b) - Este de remarcat faptul ca a folosit bcrypt (care este mai convenabil pentru stocarea parolelor) in locul unor alternative precum sha256;

- Cu toate acestea, este problematica hashuirea username-urilor deoarece putem avea doua username-uri diferite cu acelasi hash, iar al doilea utilizator va fi restrictionat degeaba.

c) - De data asta se foloseste sha256 care nu este tocmai cea mai buna metoda pentru stocarea parolelor;

- Nu se face hash cu salt sau hash-uirea repetata a parolelor (astfel exista riscul ca la un numar ridicat de parole domeniul de variatie al hash-uirii sa fie scazut si sa se repete valorile);

d) Caracterul aleatoriu al salvarii parolelor este aproape inexistent ceea ce face metoda expusa vulnerabila la dictionary attack;

e) Nu este recomandat nici macar sha256 pentru stocarea parolelor, cu atat mai putin md5 care prezinta o probabilitate mare de intalnire a coliziunilor.