Tudorache Alexadru-Theodor
Grupa 342

Examen
Securitartea Sistemelor Informatice

Subiecte netratate: 1(h), 2(c), 3, 4

1.

a) Fals. Decriptarea, folosind OTP, a textului criptat 0x253505ba folosind cheia 0x717056ee este mesajul clar TEST.

b) Adevărat

c) Fals. Un atac de tip Man-in-the-Middle este un atac activ sau pasiv.

d) Adevărat

e) Fals. Este recomandat sa se foloseasca AES pentru transmiterea fisierelor in mod criptat.

f) Adevărat

g) Fals. SHA256(PAROLA)= 0x467b4a3eca61a4e62447400d93fc35d4295c08ffa2b04ae942f4de03fa62f464

i) Adevărat

j) Adevărat

2.

a)

În aplicația web menționată, un principiu de securitate care este satisfăcut este Principiul diversității. În această aplicație sunt folosiți diferiți algoritmi criptografici pentru ascunderea datelor: funcția hash proprietară `H`, AES-ECB.

b)

În aplicația web menționată, un principiu de securitate care nu este satisfăcut este Principiul securității prin proiectare. În această aplicație câmpurile de introducere a datelor nu sunt sanitizate și validate, iar acest fapt reprezintă o vulnarabilitate a

sistemului. În câmpul respectiv se pot introduce date ce pot corupe aplicația/baza sa de date. Un exemplu de astfel de atac este atac de tipul SQL Injection.

d)

Atacatorul se folosește de funcționalitatea de resetare a parolei. Cum link-ul de schimbare a parolei este generat folosind un PRNG cunoscut care primește ca seed username-ul și ziua curentă, acesta poate fi obținut și de atacator folosind același PRNG și seed. Având link-ul respectiv, el resetează parola utilizatorului și se folosește de noua parolă pentru a se loga în cont.