SIC - Quiz 03- User Authentication

Domanda 1

Domanda 2

Domanda 2 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un vecchio sistema di password generava password di 8 caratteri utilizzando lettere minuscole e cifre (insieme di 36 caratteri) con un generatore di numeri pseudocasuali avente 2^{15} possibili valori iniziali (seed).
L'autore del sistema sosteneva che ci sarebbero voluti 112 anni per trovare via brute-force la password corretta, basandosi sullo spazio totale di password di 36^8 (circa 2800 miliardi).
Qual è il problema di sicurezza effettivo?

Scegli un'alternativa:

- a. L'alfabeto di 36 caratteri è troppo piccolo per generare password sicure
- b. Otto caratteri sono una lunghezza insufficiente indipendentemente dall'insieme di caratteri
- c. I generatori di numeri pseudocasuali sono troppo lenti per la generazione di password sicure
- d. Lo spazio effettivo delle password è solo 2^{15} (32.768) password possibili, non 36^8 (2800 miliardi)

Domanda 3

Domanda 3 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Si consideri un sistema in cui le password sono combinazioni di 4 caratteri da 26 caratteri alfabetici (senza distinzione maiuscole/minuscole).
Un avversario può tentare una password al secondo senza feedback fino al completamento del tentativo.
Qual è il tempo previsto per scoprire la password corretta?

Scegli un'alternativa:

- a. Circa 52 secondi (26 caratteri per ciascuna delle 4 posizioni)
- b. Circa 63,5 ore o 2,6 giorni (metà di 26^4 / 3600 secondi)
- c. Circa 5,3 giorni (26^4 / 86400 secondi)
- d. Circa 127 ore o 5,3 giorni (26^4 / 3600 secondi)

Domanda 4

Domanda 4 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un sistema utilizza password di 4 caratteri da 26 caratteri alfabetici (senza distinzione maiuscole/minuscole). Un avversario può tentare una password al secondo.
Il sistema fornisce feedback immediato segnalando un errore non appena viene inserito ogni carattere errato (come facevano alcuni vecchi sistemi).
Qual è il tempo previsto per scoprire la password corretta?

Scegli un'alternativa:

- a. Circa 52 secondi (in media 13 tentativi per posizione, 4 posizioni totali)
- b. Circa 127 ore (tutti i 26^4 tentativi / 3600 secondi)
- c. Circa 63,5 ore (metà di 26^4 tentativi / 3600 secondi)
- d. Circa 104 secondi (26 caratteri per posizione, 4 posizioni totali)

Domanda 5

Domanda 5 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un generatore di password fonetiche crea password utilizzando il pattern CVC (consonante, vocale, consonante) per ogni segmento, scegliendo due segmenti casualmente per formare password di sei lettere.
Dato: $V = \{a, e, i, o, u\}$ (5 vocali) e $C = \{b, c, d, f, \dots\}$ (21 consonanti)
Qual è la popolazione totale di password?

Scegli un'alternativa:

- a. $(21 + 5 + 21)^6 = 47^6$ password
- b. $21 \times 5 \times 21 \times 2 = 4.410$ password
- c. $21^3 \times 5^3 = 1.157.625$ password
- d. $(21 \times 5 \times 21)^2 = 2.205^2 = 4.862.025$ password

Domanda 6

Domanda 6 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un generatore di password fonetiche crea password utilizzando il pattern CVC (consonante, vocale, consonante) per ogni segmento, scegliendo due segmenti casualmente per formare password di sei lettere.
Dato: $V = \{a, e, i, o, u\}$ (5 vocali) e $C = \{b, c, d, f, \ldots\}$ (21 consonanti)
Qual è la probabilità che un avversario indovini una password correttamente al primo tentativo?

Scegli un'alternativa:

- a. 1/4.862.025 (circa $2{,}06 \times 10^{-7}$ o 0,00002%)
- b. 1/2.205 (circa $4{,}5 \times 10^{-4}$ o 0,045%)
- c. $1/(26^6)$ (circa $3{,}2 \times 10^{-9}$ assumendo l'alfabeto completo)
- d. $1/(21 \times 5 \times 21) = 1/2.205$

Domanda 7

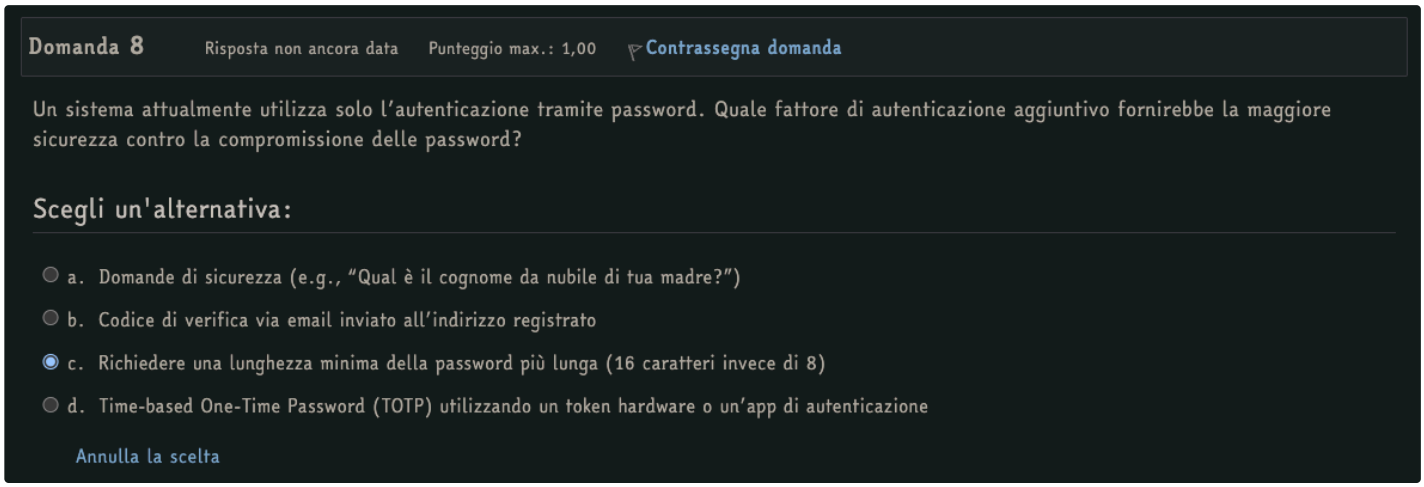
Domanda 7 Risposta non ancora data Punteggio max.: 1,00 Contrassegna domanda

Un amministratore di sistema sta implementando una politica delle password. Quali requisiti migliorano significativamente la sicurezza contro gli attacchi comuni? (Selezionare tutti quelli applicabili)

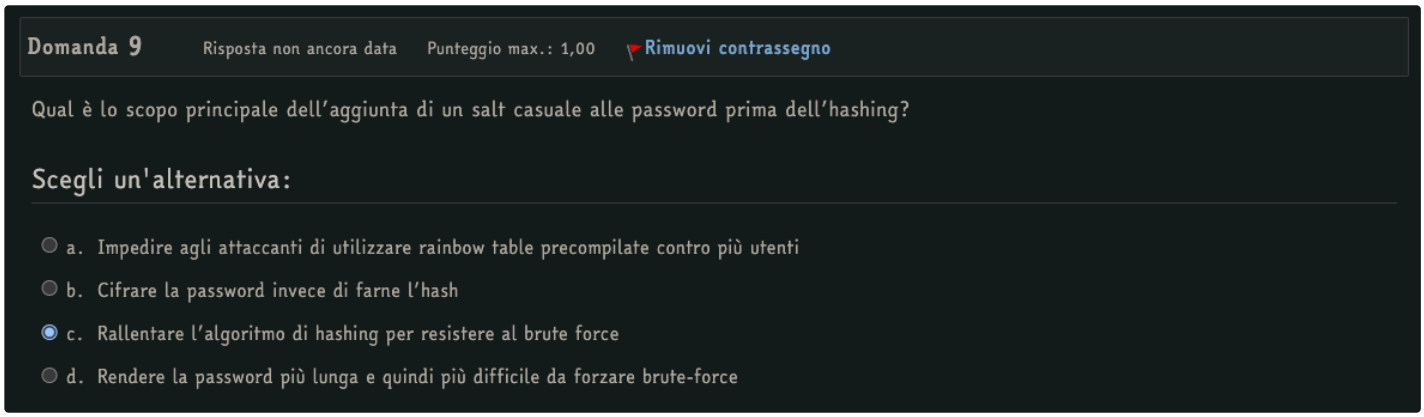
Scegli una o più alternative:

- [x] a. Verificare le password contro un dizionario di password comuni/compromesse
- [x] b. Implementare il blocco dell'account dopo tentativi falliti (con attenzione per evitare DoS)
- [ ] c. Richiedere che le password includano una parola del dizionario per memorabilità
- [x] d. Richiedere un mix di maiuscole, minuscole, cifre e caratteri speciali
- [ ] e. Mostrare un indicatore di forza della password basato solo sulla lunghezza
- [x] f. Lunghezza minima di 12 caratteri
- [x] g. Usare il rate limiting sui tentativi di autenticazione
- [ ] h. Includere il nome utente nella password per evitare password duplicate
- [ ] i. Permettere tentativi di autenticazione illimitati per evitare il blocco degli utenti
- [ ] j. Permettere agli utenti di riutilizzare le ultime 3 password

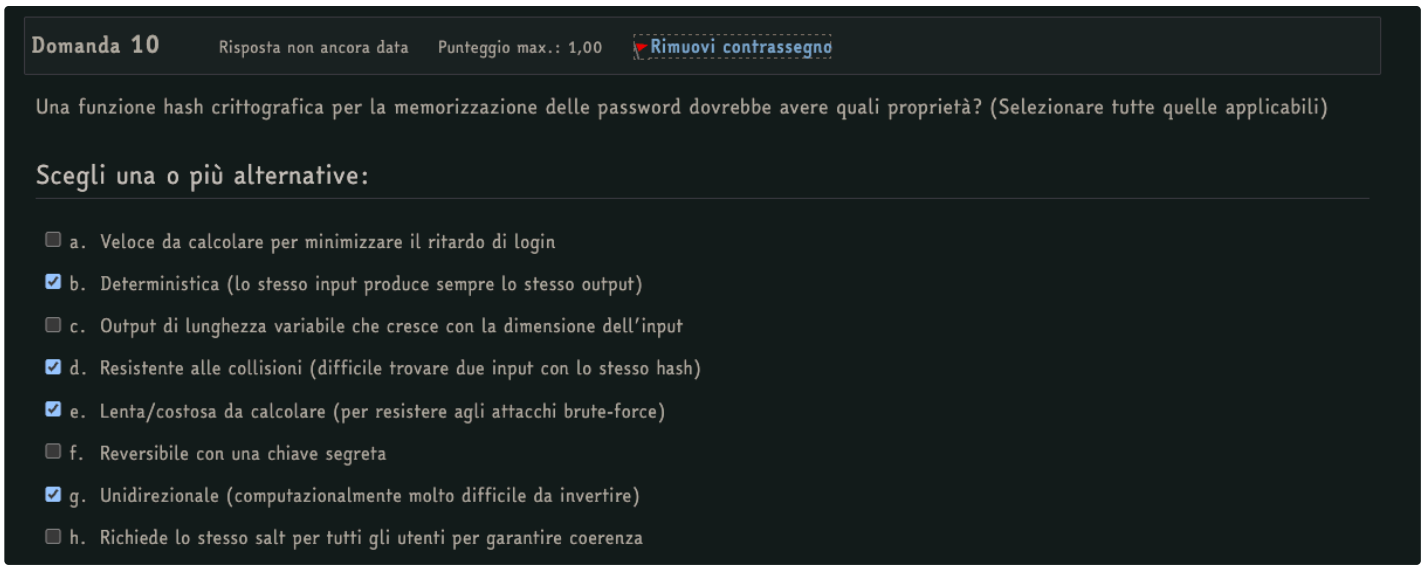
Domanda 8



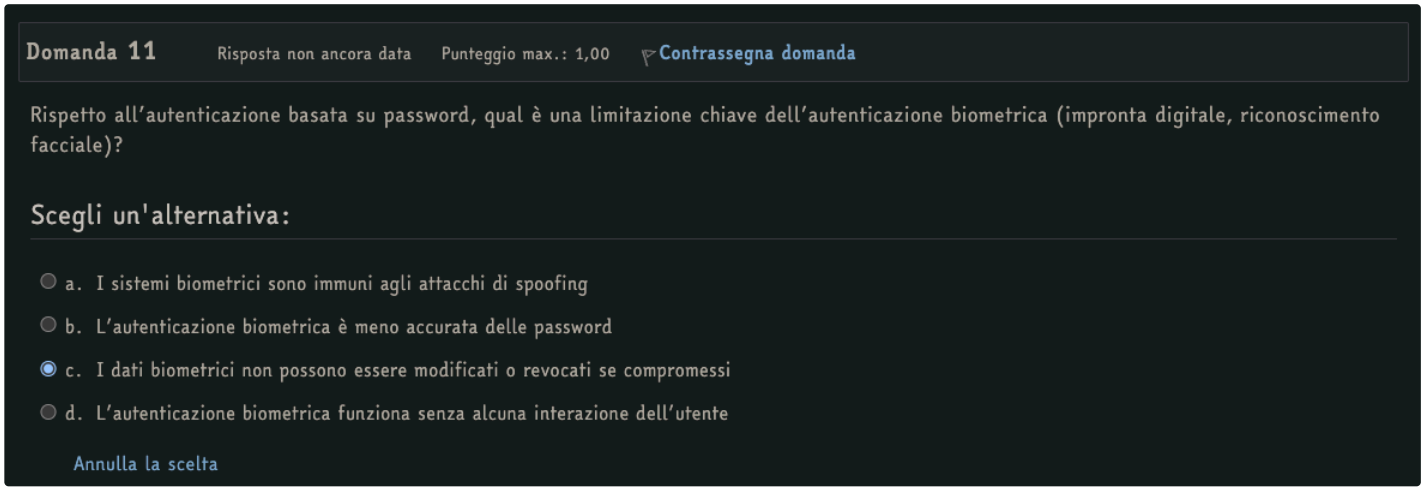
Domanda 9



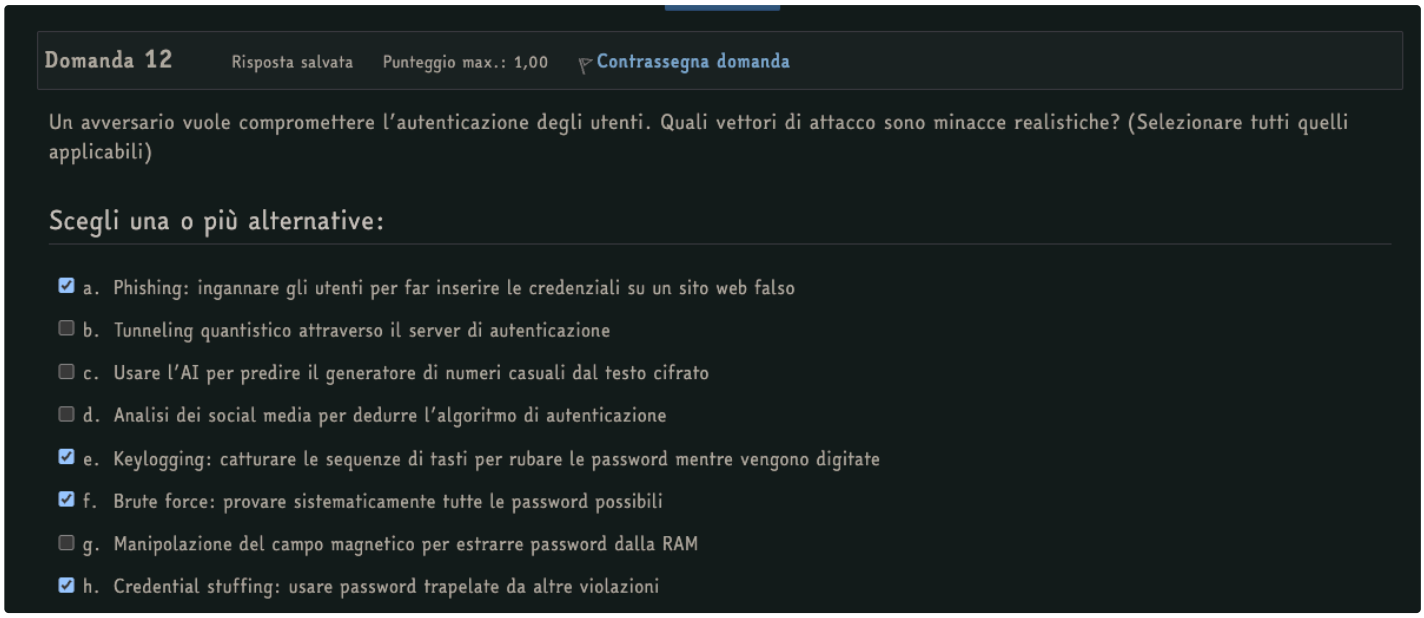
Domanda 10


Domanda 10
Risposta non ancora data
Punteggio max.: 1,00
Rimuovi contrassegno
Una funzione hash crittografica per la memorizzazione delle password dovrebbe avere quali proprietà? (Selezionare tutte quelle applicabili)
Scegli una o più alternative:
a. Veloce da calcolare per minimizzare il ritardo di login
b. Deterministica (lo stesso input produce sempre lo stesso output)
c. Output di lunghezza variabile che cresce con la dimensione dell'input
d. Resistente alle collisioni (difficile trovare due input con lo stesso hash)
e. Lenta/costosa da calcolare (per resistere agli attacchi brute-force)
f. Reversibile con una chiave segreta
g. Unidirezionale (computazionalmente molto difficile da invertire)
h. Richiede lo stesso salt per tutti gli utenti per garantire coerenza

Domanda 11


Domanda 11
Risposta non ancora data
Punteggio max.: 1,00
Contrassegna domanda
Rispetto all'autenticazione basata su password, qual è una limitazione chiave dell'autenticazione biometrica (impronta digitale, riconoscimento facciale)?
Scegli un'alternativa:
a. I sistemi biometrici sono immuni agli attacchi di spoofing
b. L'autenticazione biometrica è meno accurata delle password
c. I dati biometrici non possono essere modificati o revocati se compromessi
d. L'autenticazione biometrica funziona senza alcuna interazione dell'utente
Annulla la scelta

Domanda 12



Domanda 13