

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)

**SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME**

Usa questa pagina per la brutta, staccala, non consegnarla.

**Cognome:** \_\_\_\_\_ **Nome:** \_\_\_\_\_ **Matricola:** \_\_\_\_\_

**Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)**

Usa questa pagina per la brutta, staccala, non consegnarla.



Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

**Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)**

2. Gli attacchi al login possono essere classificati in on-line (in cui il prompt di login è accessibile via rete) e off-line (in cui il database utenti/password è disponibile in locale all'attaccante con gli hash delle password). Compila la seguente tabella.

	On-line	Off-line
Che contromisure suggerisci per i due tipi di attacchi?		
Quali sono secondo te le criticità o difficoltà principali per l'attaccante?		
Quali sono secondo te le criticità o difficoltà principali per chi deve mitigare il rischio di un tale tipo di attacchi?		

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)

3. **Birthday attack.** Descrivi il birthday attack per gli hash crittografici. In particolare, descrivi obiettivo dell'attacco, principio statistico su cui è basato e impatto sulle tecniche di firma digitale.

Obiettivo.

Principio statistico su cui si basa.

Impatto sulla firma digitale.

4. **Sicurezza del codice (XSS e CSRF).** Rispondi alle seguenti domande sulla sicurezza delle WEB applications.

4.1. Descrivi un attacco XSS (cross-site scripting) facendo un esempio con degli stralci di codice e spiegando cosa avviene, lato client e lato server passo passo.

4.2. Che tecnica potrebbe usare il browser per accorgersi di un XSS durante l'esecuzione?

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)

**4.3.** Descrivi un attacco CSRF (cross-site request forgery) facendo un esempio e spiegando cosa avviene lato client e lato server, in quali condizioni l'attacco funziona e il ruolo della sessione.

**4.4.** Descrivi le tipiche contromisure per contrastare gli attacchi CSRF.

**5. Auditing.** Rispondi alle seguenti domande circa vari aspetti dell'auditing in ambito cybersecurity.

**5.1.** Descrivi in sintesi l'idea di auditing in ambito cybersecurity.

**5.2.** Descrivi in sintesi che cosa è un Sistema di gestione della sicurezza (SGSI).

**5.3.** Descrivi in sintesi che rapporto c'è tra le attività di auditing e il SGSI.

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

Cybersecurity – 21 settembre 2021 – 4 CFU (la tesina vale 2 CFU)

5.4. Descrivi in sintesi che cosa è un SIEM.

5.5. Descrivi in sintesi che supporto fornisce il SIEM nell'ambito dell'auditing.

6. Bitcoin, transazioni, UTXO.

6.1. Descrivi la struttura di una transazione, cosa sono gli UTXO e da dove vengono i fee per i miners legati a quella transazione. Un disegno può aiutare a descrivere la situazione.

6.2. Descrivi da dove vengono i fee per i miners legati ad una transazione

6.3. Quando una transazione *spende* dei bitcoin cosa fornisce per provare che chi ha creato la transazione è il proprietario dei bitcoin? Spiega.