Scenario

Fai parte del team di sicurezza in crescita di un'azienda per appassionati e collezionisti di sneaker. L'azienda si sta preparando a lanciare un'app mobile che semplifica l'acquisto e la vendita di scarpe da parte dei clienti.

Stai eseguendo un modello di minaccia dell'applicazione utilizzando il framework PASTA. Passerai attraverso ciascuna delle sette fasi del framework per identificare i requisiti di sicurezza per la nuova app dell'azienda di sneaker.

Descrizione: La nostra applicazione dovrebbe connettere in modo fluido venditori e acquirenti. Dovrebbe essere facile per gli utenti registrarsi, accedere e gestire i propri account. La privacy dei dati è una nostra grande preoccupazione. Vogliamo che gli utenti si sentano sicuri del fatto che trattiamo le loro informazioni in modo responsabile.

Gli acquirenti dovrebbero poter inviare messaggi diretti ai venditori per qualsiasi domanda. Dovrebbero anche avere la possibilità di valutare i venditori per incoraggiare un buon servizio. Le vendite dovrebbero essere chiare e veloci da elaborare. Gli utenti dovrebbero avere diverse opzioni di pagamento per un processo di acquisto fluido. Una corretta gestione dei pagamenti è fondamentale perché vogliamo evitare problemi legali.

PASTA worksheet

Stages	Sneaker company
I. Define business and security objectives	● ***Fornire un'esperienza utente fluida e sicura*** – *consentire registrazione, accesso e gestione degli account in modo semplice, proteggendo la privacy dei dati.* ● ***Favorire l'interazione e la fiducia tra utenti*** – *permettere messaggi diretti tra acquirenti e venditori e implementare un sistema di valutazioni per incoraggiare un buon servizio.*

	● ***Garantire transazioni chiare e sicure*** *– offrire diverse opzioni di pagamento e gestire correttamente le vendite per evitare problemi legali.*
II. Define the technical scope	List of technologies used by the application: ● *Application programming interface (API)* ● *Public key infrastructure (PKI)* ● *SHA-256* ● *SQL* Ho scelto di dare priorità alle **API di terze parti** perché rappresentano un punto di ingresso esterno nell'app e possono introdurre vulnerabilità non controllate direttamente dal nostro team. Se compromesse, potrebbero esporre dati sensibili degli utenti o permettere accessi non autorizzati. Valutarle per prime riduce il rischio di exploit esterni.
III. Decompose application	Analizzo come l'app gestisce la ricerca delle scarpe nel database. SQL garantisce che i dati siano recuperati correttamente, mentre le API e la PKI proteggono le informazioni durante la comunicazione tra app e server. Questo permette di identificare eventuali punti deboli nella sicurezza dei dati degli utenti.
IV. Threat analysis	● ***Attacchi alle API di terze parti*** *– un hacker potrebbe sfruttare vulnerabilità nelle API per accedere a dati sensibili degli utenti, come password o informazioni sulle carte di credito.* ● ***Phishing o ingegneria sociale*** *– un attacco mirato a dipendenti o utenti potrebbe compromettere le credenziali di accesso, permettendo accessi non autorizzati al sistema e ai dati dell'app.*
V. Vulnerability analysis	● ***Vulnerabilità nelle API di terze parti*** *– se non correttamente protette, le API potrebbero permettere a un attaccante di accedere o manipolare dati sensibili degli utenti.* ● ***Modulo di pagamento non sicuro*** *– se i dati delle carte di credito non vengono crittografati correttamente con AES o se la PKI non è implementata correttamente, le*

	informazioni finanziarie potrebbero essere compromesse.
VI. Attack modeling	L'albero di attacco mostra in modo chiaro come un malintenzionato potrebbe sfruttare le vulnerabilità individuate. Ad esempio, potrebbe partire da un'API compromessa o da un modulo di pagamento poco sicuro per accedere a dati sensibili. Evidenzia anche come attacchi tecnici e trucchetti di ingegneria sociale possano combinarsi per ottenere accessi non autorizzati o rubare informazioni importanti.
VII. Risk analysis and impact	1. **Controlli di accesso e gestione delle identità** – Assicurarsi che solo utenti autorizzati possano accedere a dati e sistemi sensibili, con autenticazione forte (ad esempio MFA). 2. **Crittografia dei dati** – Proteggere i dati a riposo e in transito per impedire che informazioni sensibili possano essere intercettate o rubate. 3. **Aggiornamenti e patch regolari** – Mantenere software e sistemi aggiornati per ridurre le vulnerabilità sfruttabili dagli attaccanti. 4. **Monitoraggio e rilevamento delle anomalie** – Implementare sistemi di logging e monitoraggio per individuare attività sospette e rispondere rapidamente a possibili attacchi.