

Analyse des risques

A - Besoins de sécurité (4 pts)

L'analyse suivante a été produite concernant l'US **Parier pour les membres**.

title	description	Points	Sprint	D	I	C	P
Member-40 Parier		100	<input type="checkbox"/>	●	●	●	●

1. Justifiez chacun des besoins de sécurité de l'US Parier (Disponibilité, Intégrité, Confidentialité, Preuve) en rappelant leur signification.
2. Proposez des solutions à mettre en place répondant à chacun de ces besoins.

B - Scenarii de risque : Abuser stories (4 pts)

1. Rappelez la notion d'abuser story.
2. Identifiez, dans le cadre de l'application **Paris 2024**, 3 scenarii de risque (abuser stories) et rédigez les.

C - Protection CSRF (3 pts)

1. Rappelez la notion d'attaque de type CSRF (Cross Site Request Forgery), illustrez par un exemple.
2. Expliquez et détaillez le principe de protection mise en oeuvre par Spring Security pour éviter de telles attaques.

D - Attaques XSS (2 pts)

1. Expliquez ce qu'est une attaque XSS (avec exemple d'illustration).
2. Précisez quel composant de Spring permet d'éviter de telles attaques, et indiquez comment.

E - Injections SQL (3 pts)

1. Expliquez le principe d'une injection SQL (illustrez par un exemple)
2. De quelle manière JPA (Hibernate) permet t-il de les éviter ?

F - Mots de passe (4 pts)

1. Donnez le principe d'une attaque par force brute, citez différents types d'attaques utilisant ce principe.
2. Proposez au moins 3 solutions à mettre en oeuvre pour lutter contre ce type d'attaques.