□ Risk Summary Table

Vulnerability	OWASP Top 10 Mapping	Severity	Impact Summary	Recommended Mitigation
SQL Injection (SQLi)	A1: Injection	High	Allows attacker to execute arbitrary SQL queries and extract sensitive data from the database.	Use **parameterized queries (Prepared Statements)** and apply **input validation**.
Reflected Cross-Site Scripting (XSS)	A7: Cross-Site Scripting	□ Medium–High	Lets attacker inject malicious JavaScript to steal cookies or perform unintended actions.	**Escape output**, sanitize inputs, and implement a **Content Security Policy (CSP)**.
Command Injection	A1: Injection	High	Enables execution of system-level commands, risking server compromise.	Apply **strict input validation**, use **safe APIs**, enforce **least privilege**, and deploy a **WAF**.
Cross-Site Request Forgery (CSRF)	A5: Broken Access Control / Insecure Design	High	Forces authenticated users to perform unauthorized actions without consent.	Implement **CSRF tokens**, validate **session identity**, and require confirmation for sensitive requests.