SQL injection :

Phase	Time	Learning Outcome	Teaching/Learning Objectives	Learning Activities	Teacher/trainer activities (What is the role of the teacher/trainer and what is he/she going to do?)	Communication and Collaboration form	Resources, tools, and media
Introduction and orientation	20 minutes	- Understand the concept and risks of SQL injection attacks Define what SQL injection is and how it can be exploited - Identify the potential consequences of SQL injection attacks - Understand the role of user input in SQL injection vulnerabilities	- Students will be able to understand and describe the concept and risks of SQL injection attacks.- Students will be able to define what SQL injection is and explain how it can be exploited.- Students will be able to identify the potential consequences of SQL injection attacks.- Students will be able to understand the role of user input in SQL injection vulnerabilities.	- Use AR technology to watch SQL injection attack simulations - Use AR technology to interact with different types of SQL injection attacks - Discussion (Q&A, brainstorming)	Initiate the lesson with an example of an SQL injection attack. Facilitate AR simulations and interactions while ensuring clear understanding through guided discussions and addressing any emerging questions or misconceptions about SQL injection.	Verbal and Guided Communication and collaboration form: teacher - student, student-student; remote or on site, synchronous or asynchronous .	AR glasses, LMS
Lesson Execution	15 minutes	- Analyze real-world examples of SQL injection attacks - Examine case studies of successful SQL injection attacks - Analyze the techniques used by attackers to exploit SQL vulnerabilities - Identify the potential impact of SQL injection on databases and systems - Evaluate the best practices for preventing SQL injection attacks - Assess the importance of input validation and sanitization in preventing SQL injection - Evaluate the effectiveness of	- Students will be able to analyze real-world examples of SQL injection attacks.- Students will be able to examine case studies of successful SQL injection attacks.- Students will be able to analyze the techniques used by attackers to exploit SQL vulnerabilities.- Students will be able to identify the potential impact of SQL injection on databases and systems.- Students will be able to evaluate the best practices for preventing SQL injection attacks.- Students will be able to assess the	- Discussion (Q&A, brainstorming)	Provide comprehensive insights into real-world SQL injection attacks through case studies, guide through discussions to enable critical thinking regarding SQL vulnerabilities and the effectiveness of various prevention techniques.	Verbal and Guided Communication and collaboration form: teacher - student, student-student; remote or on site, synchronous or asynchronous .	AR glasses, LMS

		parameterized queries and prepared statements - Identify strategies for secure coding practices to mitigate SQL injection risks	importance of input validation and sanitization in preventing SQL injection.- Students will be able to evaluate the effectiveness of parameterized queries and prepared statements.- Students will be able to identify strategies for secure coding practices to mitigate SQL injection risks.				
Evaluation	10 minutes	- Evaluate what is SQL injection and what's not - Compare different types of SQL injection attacks	- Students will be able to evaluate and differentiate what constitutes SQL injection and what does not.- Students will be able to compare different types of SQL injection attacks based on their characteristics and impacts.	- Students will answer an online evaluation assessment/lesson feedback in the LMS and they will get the results	Steer students through the online evaluation, offering assistance where needed, ensuring all feedback is securely collected, and assuring students of the constructive use of their valuable feedback.	Written Evaluation Verbal and Guided Communication and collaboration form: teacher - student, student-student; remote or on site, synchronous or asynchronous .	LMS/Quiz