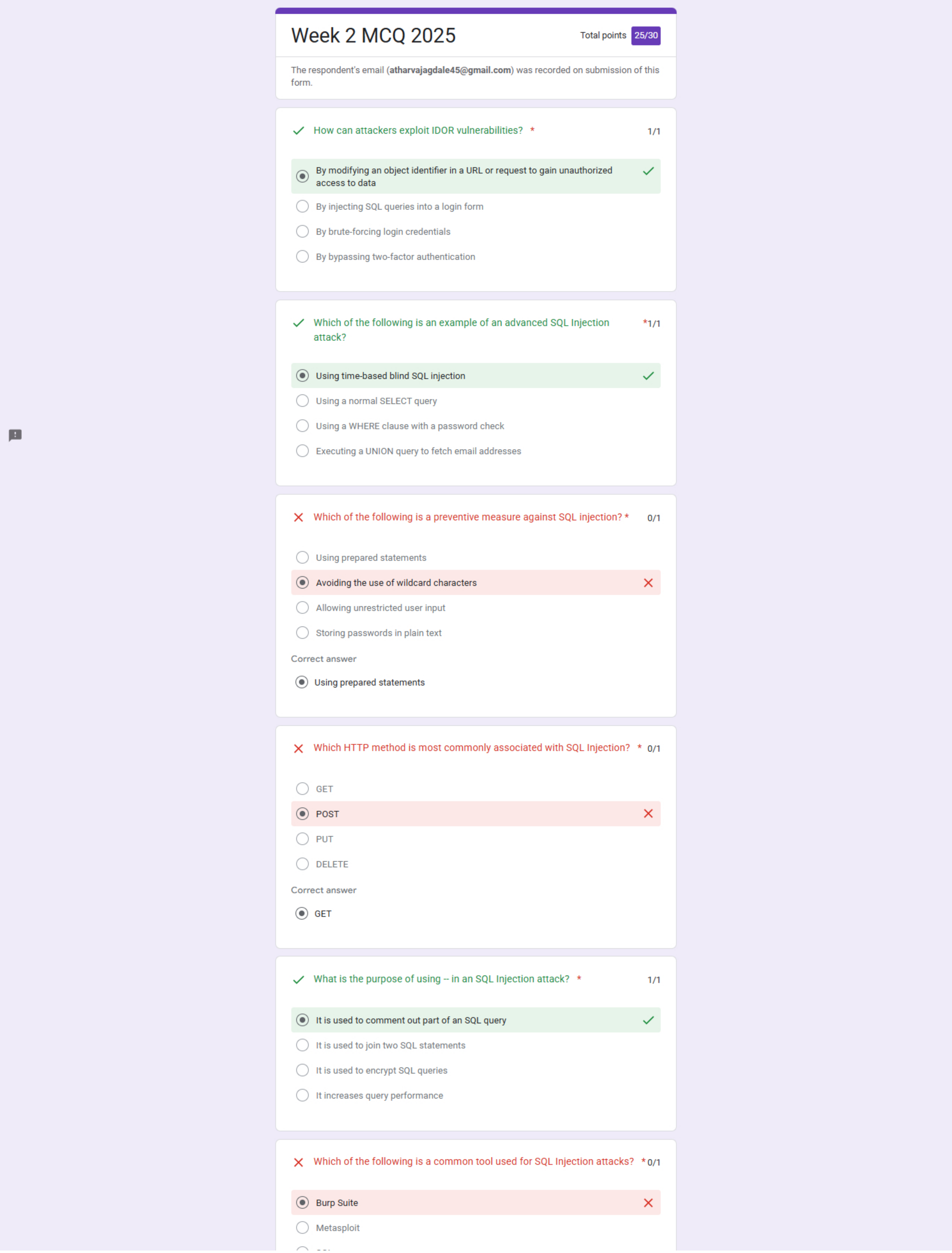


Week 2 MCQ 2025

Total points 25/30

The respondent's email (**atharvajagdale45@gmail.com**) was recorded on submission of this form.

✓ How can attackers exploit IDOR vulnerabilities? * 1/1

- ● By modifying an object identifier in a URL or request to gain unauthorized access to data ✓
- ○ By injecting SQL queries into a login form
- ○ By brute-forcing login credentials
- ○ By bypassing two-factor authentication

✓ Which of the following is an example of an advanced SQL Injection attack? * 1/1

- ● Using time-based blind SQL injection ✓
- ○ Using a normal SELECT query
- ○ Using a WHERE clause with a password check
- ○ Executing a UNION query to fetch email addresses

✗ Which of the following is a preventive measure against SQL injection? * 0/1

- ○ Using prepared statements
- ● Avoiding the use of wildcard characters ✗
- ○ Allowing unrestricted user input
- ○ Storing passwords in plain text

Correct answer

- ● Using prepared statements

✗ Which HTTP method is most commonly associated with SQL Injection? * 0/1

- ○ GET
- ● POST ✗
- ○ PUT
- ○ DELETE

Correct answer

- ● GET

✓ What is the purpose of using -- in an SQL Injection attack? * 1/1

- ● It is used to comment out part of an SQL query ✓
- ○ It is used to join two SQL statements
- ○ It is used to encrypt SQL queries
- ○ It increases query performance

✗ Which of the following is a common tool used for SQL Injection attacks? * 0/1

- ● Burp Suite ✗
- ○ Metasploit

○ SQLmap

○ Nessus

Correct answer

● SQLmap

✓ What is a common way to test for IDOR vulnerabilities? * 1/1

● Manipulating parameters in the URL or request to see if unauthorized access occurs ✓

○ Running SQL queries to test for vulnerabilities

○ Sending malicious scripts through form submissions

○ Examining the source code of the application

✓ Which of the following can help prevent IDOR in applications? * 1/1

● Using opaque, randomized tokens for object references ✓

○ Using static identifiers for objects

○ Storing passwords in plain text

○ Avoiding encryption altogether

✓ In an IDOR attack, what would an attacker typically modify in the HTTP request? * 1/1

● URL parameter or session identifier ✓

○ HTTP headers

○ Request method (GET/POST)

○ User-Agent string

✓ Which of the following characters is commonly used in SQL Injection attacks? * 1/1

○ *

● ' ✓

○ #

○ &

✓ Which of the following is a possible consequence of a successful SQL Injection attack? * 1/1

○ Server compromise

○ Data breach

○ Unauthorized access to the admin panel

● All of the above ✓

✓ What is one way to prevent unauthorized object access in IDOR scenarios? * 1/1

● Use access control lists (ACLs) to validate the user's authorization for a specific object ✓

○ Allow access based solely on user roles

○ Encrypt all URL parameters

○ Avoid logging out users during session expiration

✓ Which of the following is a potential impact of IDOR on financial applications? *1/1

● Unauthorized transactions or balance viewing ✓

○ Loss of user authentication tokens

○ Unauthorized access to logs

○ Data format corruption

✓ What does SQL Injection (SQLi) allow an attacker to do? * 1/1

○ Execute arbitrary commands on the server

○ Modify or delete data in the database

○ Retrieve sensitive data from the database

● All of the above ✓

✓ Which of the following is an example of an IDOR attack? * 1/1

● Accessing a user's profile by modifying the user ID in the URL ✓

○ Brute-forcing a password

○ Injecting SQL queries into a form field

○ Performing a denial-of-service attack

✗ Which of the following can be an indication that a website is vulnerable to SQL Injection? *0/1

○ Error messages revealing database details

○ Lack of user authentication

○ Frequent logins and logouts

● All of the above ✗

Correct answer

● Error messages revealing database details

✓ What does 'blind SQL Injection' refer to? * 1/1

● An attack where the attacker cannot see the results of their query ✓

○ An attack where the SQL query runs automatically

○ An attack that uses a CAPTCHA to bypass input restrictions

○ An attack based on SQL query execution time

✓ What is an Insecure Direct Object Reference (IDOR) vulnerability? * 1/1

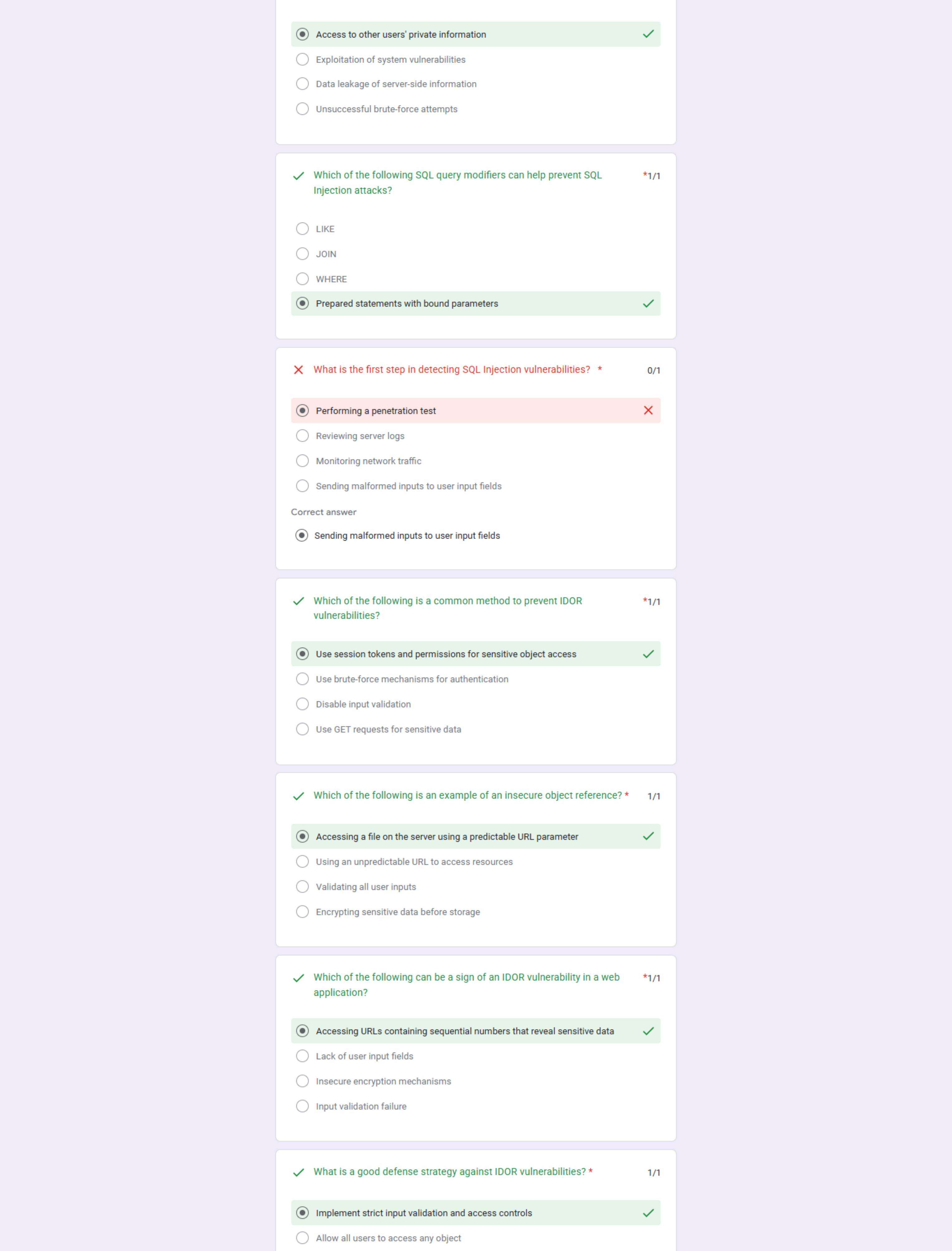
● A flaw where unauthorized users can access or modify data by manipulating input parameters ✓

○ A flaw that allows attackers to bypass authentication

○ A flaw that only affects server-side scripts

○ A vulnerability specific to web browsers

✓ Which of the following is an example of a potential impact of an IDOR attack? *1/1



● Access to other users' private information ✓

○ Exploitation of system vulnerabilities

○ Data leakage of server-side information

○ Unsuccessful brute-force attempts

✓ Which of the following SQL query modifiers can help prevent SQL Injection attacks? *1/1

○ LIKE

○ JOIN

○ WHERE

● Prepared statements with bound parameters ✓

✗ What is the first step in detecting SQL Injection vulnerabilities? * 0/1

● Performing a penetration test ✗

○ Reviewing server logs

○ Monitoring network traffic

○ Sending malformed inputs to user input fields

Correct answer

● Sending malformed inputs to user input fields

✓ Which of the following is a common method to prevent IDOR vulnerabilities? *1/1

● Use session tokens and permissions for sensitive object access ✓

○ Use brute-force mechanisms for authentication

○ Disable input validation

○ Use GET requests for sensitive data

✓ Which of the following is an example of an insecure object reference? * 1/1

● Accessing a file on the server using a predictable URL parameter ✓

○ Using an unpredictable URL to access resources

○ Validating all user inputs

○ Encrypting sensitive data before storage

✓ Which of the following can be a sign of an IDOR vulnerability in a web application? *1/1

● Accessing URLs containing sequential numbers that reveal sensitive data ✓

○ Lack of user input fields

○ Insecure encryption mechanisms

○ Input validation failure

✓ What is a good defense strategy against IDOR vulnerabilities? * 1/1

● Implement strict input validation and access controls ✓

○ Allow all users to access any object

○ Use a generic identifier for objects

○ Allow unrestricted query parameters

✓ What does the 'UNION' SQL operator do in the context of SQLi? * 1/1

○ Unites two database tables

● Retrieves data from multiple queries ✓

○ Deletes data from a table

○ Modifies table structures

✓ Which of the following is an example of an SQL injection attack? * 1/1

○ SELECT * FROM users WHERE username='admin' AND password='1234';

● SELECT * FROM users WHERE username='' OR 1=1; --'; ✓

○ SELECT * FROM products WHERE price > 100;

○ UPDATE users SET password='newpassword' WHERE username='admin';

✓ What is one reason why IDOR vulnerabilities are so common? * 1/1

● Developers often fail to validate object access rights properly ✓

○ Web applications do not use encryption

○ Web servers have no session management

○ Input validation is not necessary for web applications

✓ What is the main risk associated with an IDOR vulnerability? * 1/1

○ Information disclosure

○ Data corruption

● Access control bypass ✓

○ Denial of service

✓ What is the primary risk of an SQL Injection vulnerability? * 1/1

○ Information disclosure

○ Data modification

○ Authentication bypass

● All of the above ✓