

Complete Security Notes (Combined From Your Searches)

1. XSS (Cross-Site Scripting)

- Occurs when user input is not escaped.
- Payload example: `alert('XSS')`
- Stored, Reflected, DOM-based XSS.
- Defense: Output encoding, CSP, input sanitization.

2. CSRF (Cross-Site Request Forgery)

- Forces authenticated users to perform unwanted actions.
- Works because browsers automatically send cookies.
- Not only with cookies: also HTTP Basic Auth, client certificates.
- Defense: CSRF tokens, SameSite cookies, re-authentication.

3. SQL Injection (SQLi)

- Allows attacker to manipulate SQL queries.
- UNION-based SQLi:
- Determine number of columns using ORDER BY.
- Example: `' UNION SELECT 1,2,3--`
- Oracle requires FROM DUAL.
- MySQL double dash must be `-- " (with space).`
- When columns don't match, use dummy values.

4. Privilege Concepts

- Database privileges: SELECT, INSERT, UPDATE, DELETE, EXECUTE.
- Least privilege principle.

5. Example SQL Table

CREATE TABLE logins (

```
id INT AUTO_INCREMENT,  
username VARCHAR(100) UNIQUE,  
password VARCHAR(100),  
date_of_joining DATETIME DEFAULT NOW(),  
PRIMARY KEY (id)  
);
```

Example inserts:

```
INSERT INTO logins(username, password) VALUES ('john','123');  
INSERT INTO logins(username, password) VALUES ('admin','pass');  
INSERT INTO logins(username, password) VALUES ('rahul','789');
```

6. Sensitive Data Exposure (CWE)

- Occurs when sensitive information is not properly protected.
- Example weaknesses: plaintext passwords, weak encryption.

7. CAPTCHA Not Implemented (CWE)

- Missing CAPTCHA can allow brute force attacks.

8. Version Disclosure (ASP.NET)

- Server reveals version like "X-Powered-By: ASP.NET"
- Attackers use version info to target vulnerabilities.

9. BIW Website vs Application

- Website: static + dynamic info, browser-based.
- Web application: functional, user input processed, authentication.

10. Thick Client

- Installed locally, interacts with server.

- Example: desktop apps, banking software.

11. CVSS Scoring (Full Notes)

Base Metrics:

- **AV (Attack Vector)**: N (Network), A (Adjacent), L (Local), P (Physical)
- **AC (Attack Complexity)**: L (Low), H (High)
- **PR (Privileges Required)**: N / L / H
- **UI (User Interaction)**: N / R
- **S (Scope)**: U / C
- **C//I/A Impacts**: N / L / H

Example:

AV:N / AC:L / PR:N / UI:N / S:U / C:H / I:H / A:L

This results in a critical score.