1. What technique allows an attacker to bypass a login form using SQL Injection?
   A. UNION SELECT
   B. 1' OR '1'='1
   C. DROP TABLE users
   D. SELECT * FROM *

2. 2. Which of the following hashing algorithms is most vulnerable to brute-force attacks?
   A. SHA-512
   B. SHA-1
   C. bcrypt
   D. MD5

3. 3. You found a subdomain pointing to GitHub Pages, but the repository is deleted. What kind of attack is possible?
   A. XSS
   B. Subdomain Takeover

C. CSRF

D. SSRF

4. 4. In Linux, which permission combination allows privilege escalation via a script?

A. Read-only

B. 777

C. SUID

D. Immutable

5. 5. What tool can find JavaScript files and extract endpoints for bug bounty hunting?

A. Nikto

B. Amass

C. LinkFinder

D. Wapiti

💣 **Part 2: Practical Tasks (Submit Proof in Group)**

🫘 **Hidden Directory Challenge**

Tool: gobuster or dirsearch

Task:

Target: http://testphp.vulnweb.com

Find 3 hidden directories and list them.

📸 *Submit Screenshot of URLs found*

2. 💉 SQL Injection Task (Live Site)

Target:

http://testphp.vulnweb.com/artists.php?artist=1

Use sqlmap to extract:

✅ **All database names**

📸 *Submit terminal screenshot with --dbs result*

3. 🔐 Bruteforce Login Panel

Target: http://testphp.vulnweb.com/login.php

User: admin

Tool: hydra

Wordlist: rockyou.txt

📷 *Submit terminal screenshot of successful login*

4. 📦 Local File Inclusion (LFI)

Target: Simulate LFI using DVWA or your local vulnerable server
Payload: ?page=../../../../etc/passwd

📷 *Submit screenshot of contents of passwd file*

5. 🧠 JS Recon + Endpoint Extraction

Target: Any real website (e.g., https://hackerone.com)
Tool: LinkFinder or manual JS analysis
Task: Find and list at least 5 hidden endpoints or API URLs from JS files.

📷 *Submit screenshot of discovered URLs*

⬜ 📅 **Deadline: 2 Hours**

⬜ 📁 **Submit screenshots and answers in the group with your name**

⬜ 🧠 **Explanation = Bonus Points**

⬜ 🔍 **Creativity + New Tricks = Extra Respect in Group** 😎

- CYBER MIND SPACE