

Password Strength Analyzer

Cyber Security | HTML, CSS, JavaScript | Mini Project | Beginner Level | Viva Questions & Answers

Student Name: _____

Roll No.: _____

Course / Class: _____

Institution: _____

Academic Session: _____

Guide / Faculty: _____

1. What is a Password Strength Analyzer?

A tool that evaluates password characteristics and provides an approximate strength assessment and improvement suggestions.

2. Why is this project related to cybersecurity?

Passwords are an important authentication factor, and weak passwords can increase exposure to guessing and credential attacks.

3. Which technologies are used?

HTML, CSS, and JavaScript.

4. Does the project require a server?

No. The intended application performs analysis locally in the browser.

5. What is a heuristic score?

A rule-based approximation that combines selected characteristics into an easy-to-understand strength indicator.

6. Why is password length important?

Longer, less predictable passwords generally provide a larger search space.

7. Why check character categories?

Character diversity can increase possible combinations, although diversity alone does not guarantee strength.

8. What are repeated patterns?

Patterns such as repeated characters or short repeated sequences that can make a password more predictable.

9. What are sequential patterns?

Simple predictable sequences such as consecutive letters or digits.

10. What is a common-password check?

It identifies passwords or patterns commonly used by many people and therefore more likely to be guessed.

11. Is the score proof that a password is secure?

No. It is an educational heuristic and cannot model every attacker or authentication system.

12. Does the project store passwords?

The intended design does not send the entered password to a server or database; it is analyzed in the browser.

13. Why is client-side processing useful?

It avoids requiring the password to be transmitted to a remote service for basic analysis.

14. How should real passwords be stored?

Use a dedicated password-hashing scheme such as Argon2id, scrypt, or bcrypt with appropriate salts and operational security.

15. What is responsive design?

A design approach that adapts the interface to different screen sizes and devices.

16. Can the project detect every compromised password?

No. It does not have universal knowledge of breach datasets.

17. How can it be improved?

Add entropy analysis, privacy-preserving breach checks, password generation, accessibility, localization, and stronger pattern analysis.

18. What is the purpose of show/hide?

It lets users verify what they typed while allowing the value to remain visually concealed when desired.

19. What is the main limitation?

The score is heuristic and should not be treated as a security guarantee.

20. What did you learn?

DOM manipulation, event handling, client-side validation, responsive UI design, pattern analysis, and basic cybersecurity concepts.