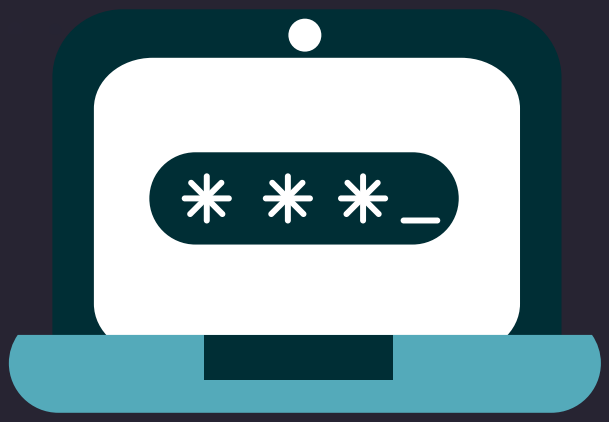
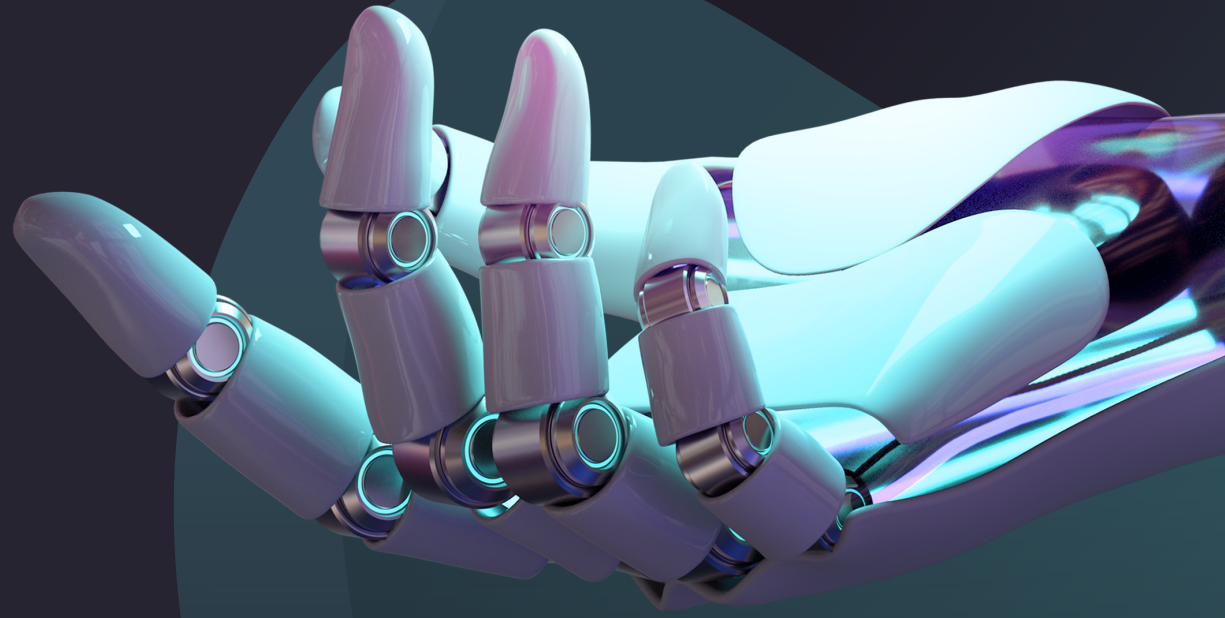
PASSWORD STRENGTH TESTER

(Second Deliverable: Overview of the main existing solutions)





PROJECT PREPARED BY:

RIMA BEN BRAHIM
ACHRAF BEN ABDALLAH
NOUR MAALEJ
FERYEL GRITLI

TECHNIQUES AND ALGORITHMS USED IN THE OWASP PASSWORD STRENGTH CHECKER:

- **Entropy:** OWASP uses the concept of entropy to calculate the strength of a password. Entropy is a measure of randomness or unpredictability, and it can be calculated using various methods, such as the number of possible characters in a password and the length of the password.

- **Dictionary attacks**: The OWASP password strength checker checks whether a password is a common dictionary word or phrase. This technique is used to prevent users from choosing easily guessable passwords.

- **Pattern matching:** The tool checks for patterns in the password, such as repeated characters, sequential numbers, or keyboard patterns (e.g., qwerty). Passwords with such patterns are generally weaker than those without.

- **Brute-force attacks:** The tool simulates a brute-force attack on the password by checking if it can be cracked using common techniques, such as trying all possible combinations of characters.

- **Common password lists:** OWASP maintains a list of common passwords that are known to be easily guessable or commonly used. The tool checks if the password is on this list and advises the user to choose a stronger password if necessary.

- **Custom rules:** The tool allows administrators to define custom rules for password strength, such as minimum length, complexity requirements, and other policies.

THE CHARACTERISTICS, ADVANTAGES, AND LIMITS OF THE EXISTING SOLUTIONS:

Security.org:

Characteristics:

- Multi-factor password strength analysis: Security.org's password testing likely employs a multi-factor analysis approach, considering factors such as password length, complexity, uniqueness, and whether it has been exposed in previous data breaches.
- Customized password rule settings: Their tool may allow users to customize password rule settings based on their specific needs, such as minimum password length, and the use of uppercase and lowercase letters, numbers, and special characters.
- Password hashing: Security.org may use password hashing techniques to ensure that passwords are not transmitted or stored in plain text and are more secure.

Advantages:

- Comprehensive security resources: Security.org provides a wealth of information on a variety of security and privacy topics, including antivirus software, password managers, VPNs, and more. This information is presented in an easy-to-understand format, making it accessible to users of all skill levels.
- Unbiased reviews and recommendations: The website provides unbiased reviews and recommendations on security products and services. The reviews are based on thorough testing and analysis, and the recommendations are designed to help users make informed decisions about the best security solutions for their needs.
- User-friendly tools: Security.org offers a range of user-friendly tools to help users improve their online security, such as a password strength checker, a VPN speed test, and a DNS leak test. These tools are free to use and require no technical expertise.
- Educational content: In addition to product reviews and recommendations, Security.org provides educational content on a range of security and privacy topics. This includes guides on how to create strong passwords, how to protect yourself from identity theft, and how to secure your home network.
- Active community: Security.org has an active community of users and security experts who can offer advice and support on a range of security-related issues. This community is a valuable resource for users looking to improve their security and privacy online.

Limits:

- Limited password testing coverage: Security.org may not be able to test all types of passwords, especially those used for specialized purposes or with uncommon formats.
- Limited accuracy: While Security.org's password testing tool is designed to provide a comprehensive assessment of password strength, its accuracy may depend on a variety of factors, such as the quality and completeness of the data it uses.
- No guarantees: Security.org does not provide any guarantees or warranties regarding the accuracy or effectiveness of its password testing services.

Bitwarden:

Characteristics:

- Bitwarden offers a password strength report that analyzes the strength of user passwords based on several factors, including length, complexity, and the use of common patterns or dictionary words. The report provides users with a score out of 100 and recommendations for improving the strength of their passwords.
- Bitwarden also offers a feature that checks for compromised passwords. This feature scans user passwords against a database of known compromised passwords and alerts users if any of their passwords have been compromised in a data breach.

Advantages:

- Strong encryption: Bitwarden uses strong end-to-end encryption to protect your passwords and other sensitive data. This means that your information is kept secure both in transit and at rest.
- Cross-platform compatibility: Bitwarden is available on a wide range of platforms, including Windows, macOS, Linux, iOS, Android, and more. This makes it easy to access your passwords and other information from any device.
- Free and paid plans: Bitwarden offers both free and paid plans, depending on your needs. The free plan offers basic password management features, while the paid plan includes additional features like secure file storage and advanced two-factor authentication options.
- Open-source: Bitwarden is open-source software, which means that its code is freely available for inspection by anyone. This helps to ensure that the software is secure and trustworthy.
- Secure sharing: Bitwarden allows you to securely share passwords and other sensitive information with other users. This feature is particularly useful for families or small teams who need to share access to certain accounts.

Limits:

- limited scope: Bitwarden's password strength report only considers factors such as length and complexity, and may not take into account other important considerations such as the use of unique passwords for different accounts.
- False sense of security: While Bitwarden's compromised password feature is helpful in identifying if a password has been previously compromised, it may not detect all instances of compromised passwords or account breaches.
- No protection against phishing: Bitwarden's password testing features do not protect against phishing attacks, where attackers trick users into giving away their passwords through fake login pages or other methods

NordPass:

Characteristics:

- Password strength report: NordPass provides a comprehensive password strength report for each saved password, which includes a breakdown of password length, complexity, and whether it has been compromised in a data breach.
- Dark web monitoring: NordPass' monitoring feature checks for any instances of compromised data associated with a user's email address or other personal information on the dark web, alerting users if any are found.
- Customizable password generation.
- Two-factor authentication: NordPass supports two-factor authentication, providing an additional layer of security for user accounts.

Advantages:

- Two-factor authentication: NordPass offers several two-factor authentication options, including biometric authentication (such as fingerprint recognition) and one-time passwords (such as Google Authenticator). This helps to add an extra layer of security to your account.
- Secure sharing: NordPass allows you to securely share passwords and other sensitive information with other users. This feature is particularly useful for families or small teams who need to share access to certain accounts.
- Password generator: NordPass has a built-in password generator that can create strong, unique passwords for you, which helps you to create more secure passwords without having to come up with them yourself.

Limits:

- Limited free version: While NordPass offers a free version of its password manager, it is limited in terms of the number of passwords that can be stored and the features available.
- No password sharing for free version: The free version of NordPass does not allow for password sharing,
- No automatic password change: NordPass does not have an automatic password change feature.
- No protection against phishing.

The Kaspersky Password Strength Meter:

Characteristics:

- Password strength evaluation: The tool evaluates passwords and provides a score from 1 to 100, indicating the strength of the password.
- Complexity: The tool evaluates the complexity of the password based on the use of upper and lowercase letters, numbers, and symbols.
- Dictionary check: The tool checks if the password is a common word or combination of words found in a dictionary
- Brute-force attack resistance: The tool evaluates the password's resistance to brute-force attacks, where an attacker tries to guess the password by trying all possible combinations.

Advantages:

- Easy to use: The Kaspersky Password Strength Meter is simple and easy to use. You just need to type in your password and the tool will evaluate its strength.
- Accurate: Kaspersky has a reputation for developing strong security products, and this tool is no exception. The password strength evaluations provided by this tool are reliable and accurate.
- Customizable: The tool allows you to customize the evaluation criteria, so you can adjust the parameters to better fit your specific needs.
- Educational: The tool provides feedback on why certain passwords are stronger than others, which helps users to better understand how to create strong passwords in the future.

Limits:

- Lack of personalization: The tool does not take into account the user's personal information, such as name or date of birth, which can make passwords easier to guess
- Limited functionality: The tool only evaluates the strength of passwords and does not offer password management or storage.
- False sense of security: While the tool provides a score indicating the strength of the password, it does not guarantee that the password is unbreakable or that it cannot be guessed by an attacker.

The UIC (University of Illinois at Chicago) Password Strength Test:

Characteristics:

- Length-based scoring system: The UIC Password Strength Test assigns points based on the length of the password, with longer passwords receiving higher scores.
- Complexity-based scoring system: The tool also considers the complexity of the password, taking into account the use of upper and lower case letters, numbers, and special characters.
- Uniqueness-based scoring system: The UIC Password Strength Test also checks the uniqueness of the password by comparing it against a database of commonly used passwords.
- Instant feedback: The tool provides instant feedback to users, indicating whether their password is weak, medium, or strong, and offering suggestions for improvement.
- Free to use: The UIC Password Strength Test is a free tool available to anyone with internet access.

Advantages:

- Easy to use: The UIC Password Strength Test is simple and easy to use. You just need to type in your password and the tool will evaluate its strength.
- Accurate: The tool uses a sophisticated algorithm to evaluate the strength of passwords, which provides reliable and accurate results.
- Customizable: The tool allows you to customize the evaluation criteria, so you can adjust the parameters to better fit your specific needs.
- Educational: The tool provides feedback on why certain passwords are stronger than others, which helps users to better understand how to create strong passwords in the future.
- No data storage: The UIC Password Strength Test does not store any data or record any information about the passwords that are evaluated, which helps to maintain user privacy.

Limits:

- Limited criteria: The tool only evaluates passwords based on length, complexity, and uniqueness, and does not take into account other important factors such as how often the password is changed or whether it has been compromised in a data breach.
- Reliance on user input: The accuracy of the test is dependent on the user's ability to accurately enter their password.
- Lack of context: The tool does not take into account the specific context of the password, such as whether it is being used for a personal or business account.

Google Password Checkup:

Characteristics:

- Password analysis: Google Password Checkup analyzes the strength of the user's password and provides recommendations for improving it.
- Password breach detection: The tool checks if the user's password has been involved in any known data breaches and alerts them if it has been compromised.
- Two-factor authentication: Google Password Checkup encourages users to enable two-factor authentication as an added layer of security.
- Privacy protection: The tool uses encryption to protect the user's password and data, and does not store or share any sensitive information.
- Integration with Google accounts: Google Password Checkup is integrated with Google accounts, making it easy for users to access and use the tool

Advantages:

- Easy to use: The tool is simple and easy to use. It's integrated into your Google account, so you don't need to install any additional software.
- Comprehensive: The tool checks the security status of all of the passwords associated with your Google account, which provides a comprehensive overview of your password security.
- Real-time alerts: If the tool identifies any compromised or weak passwords, it will provide real-time alerts and recommendations for improving your password security.
- Free: The tool is completely free to use, which makes it accessible to anyone who wants to improve their online security.

Limits:

- Limited scope: Google Password Checkup only checks passwords against known data breaches and may not detect new or emerging threats.
- User awareness: Users must be aware of and willing to use the tool to improve their password security.
- No guarantee of security: While Google Password Checkup can help users improve their password security, there is no guarantee that their passwords will not be compromised in the future.