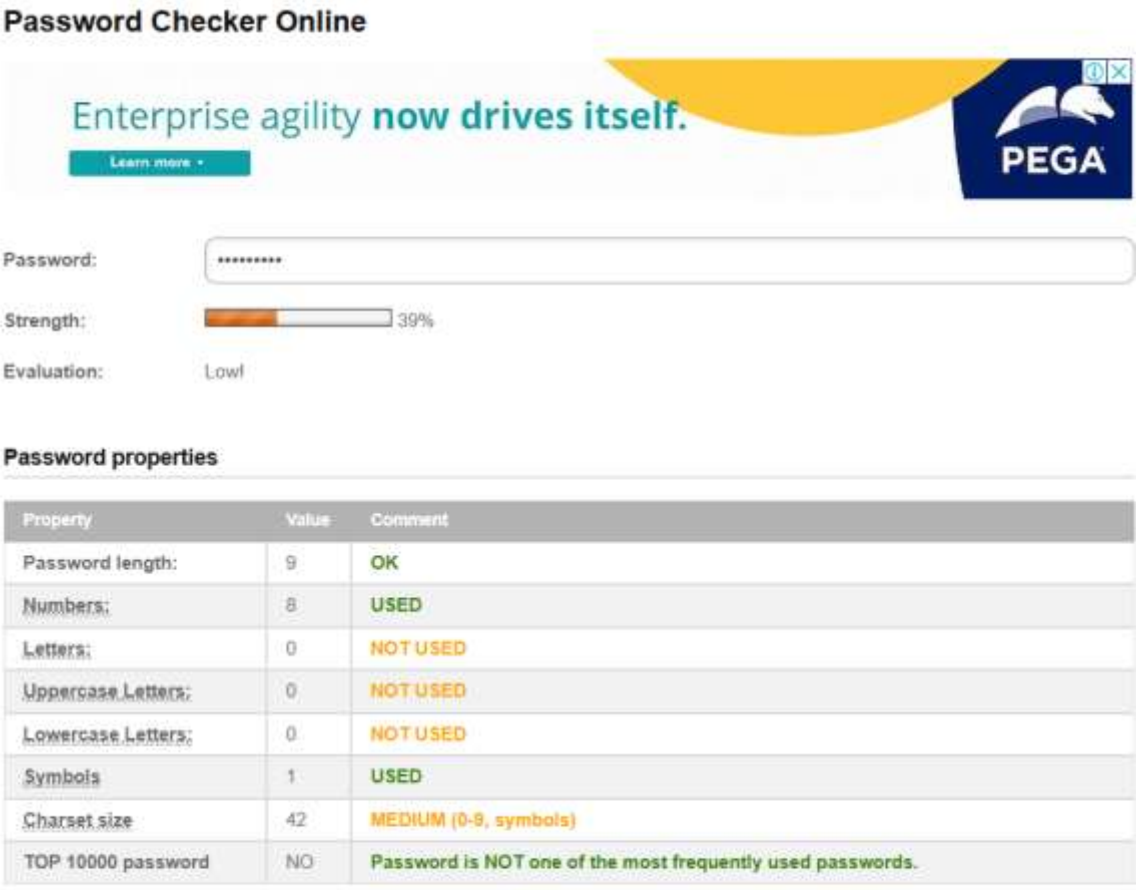
Task 6: Create a Strong Password and Evaluate Its Strength

- **Objective:** Understand what makes a password strong and test it against password strength tools

- **Tools Used :** password-checker online

- **Password Strength Evaluation:**



Password Checker Online

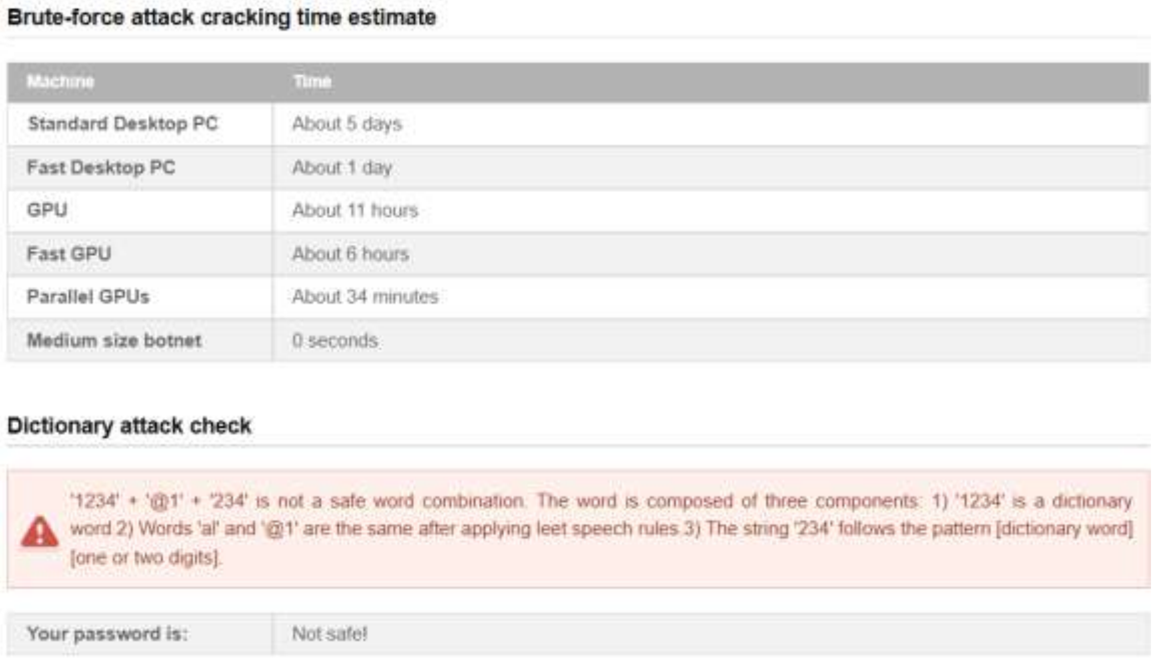
Password: ••••••••••

Strength: 39%

Evaluation: Low!

Password properties

Property	Value	Comment
Password length:	9	OK
Numbers:	8	USED
Letters:	0	NOT USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	0	NOT USED
Symbols	1	USED
Charset size	42	MEDIUM (0-9, symbols)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.



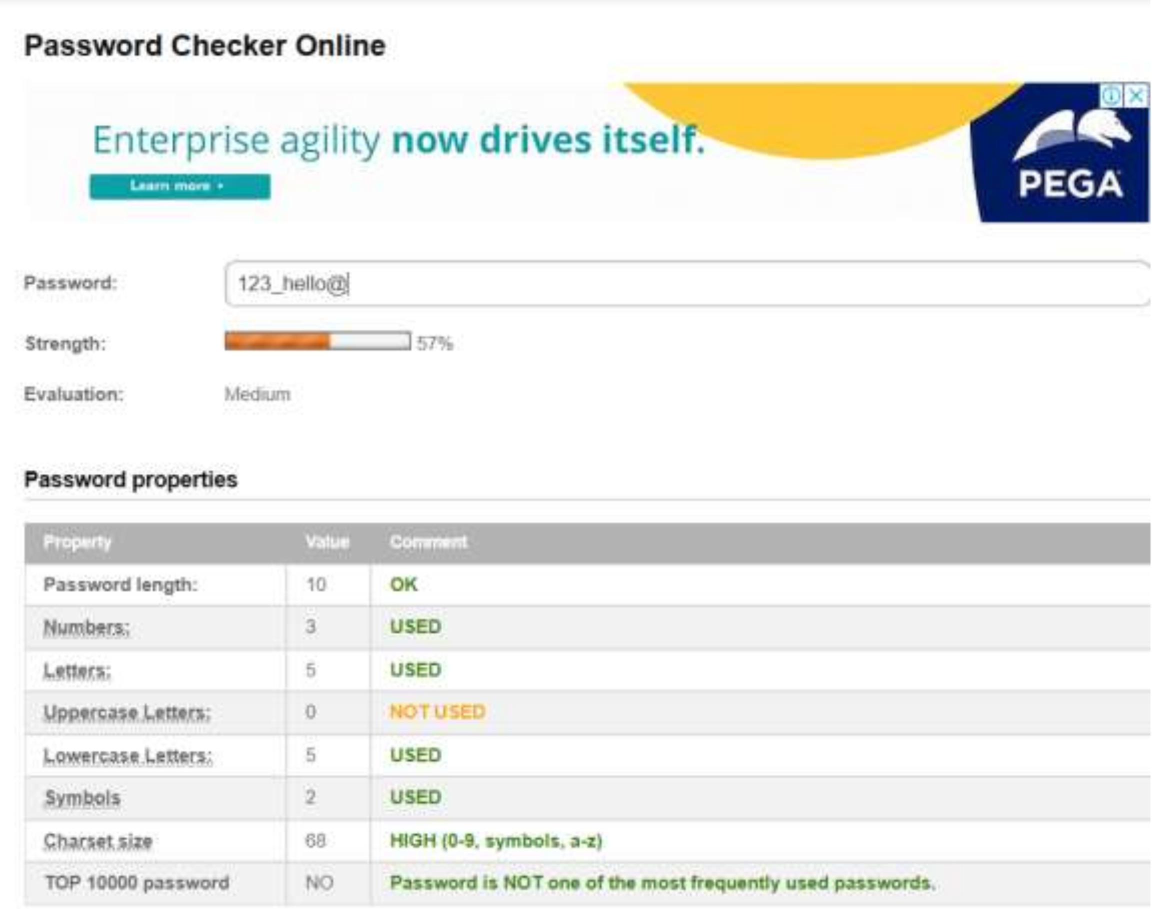
Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 5 days
Fast Desktop PC	About 1 day
GPU	About 11 hours
Fast GPU	About 6 hours
Parallel GPUs	About 34 minutes
Medium size botnet	0 seconds

Dictionary attack check

'1234' + '@1' + '234' is not a safe word combination. The word is composed of three components: 1) '1234' is a dictionary word 2) Words 'al' and '@1' are the same after applying leet speech rules 3) The string '234' follows the pattern [dictionary word] [one or two digits].

Your password is:	Not safe!

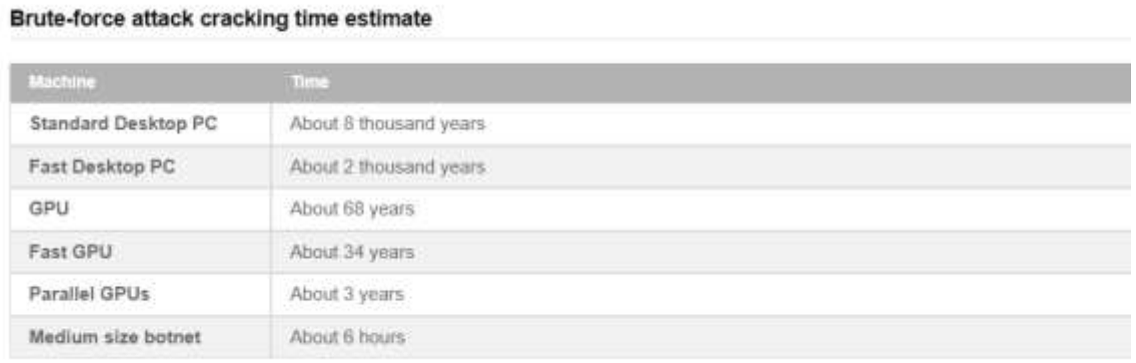


Password Checker Online

Password:	123_hello@
Strength:	57%
Evaluation:	Medium

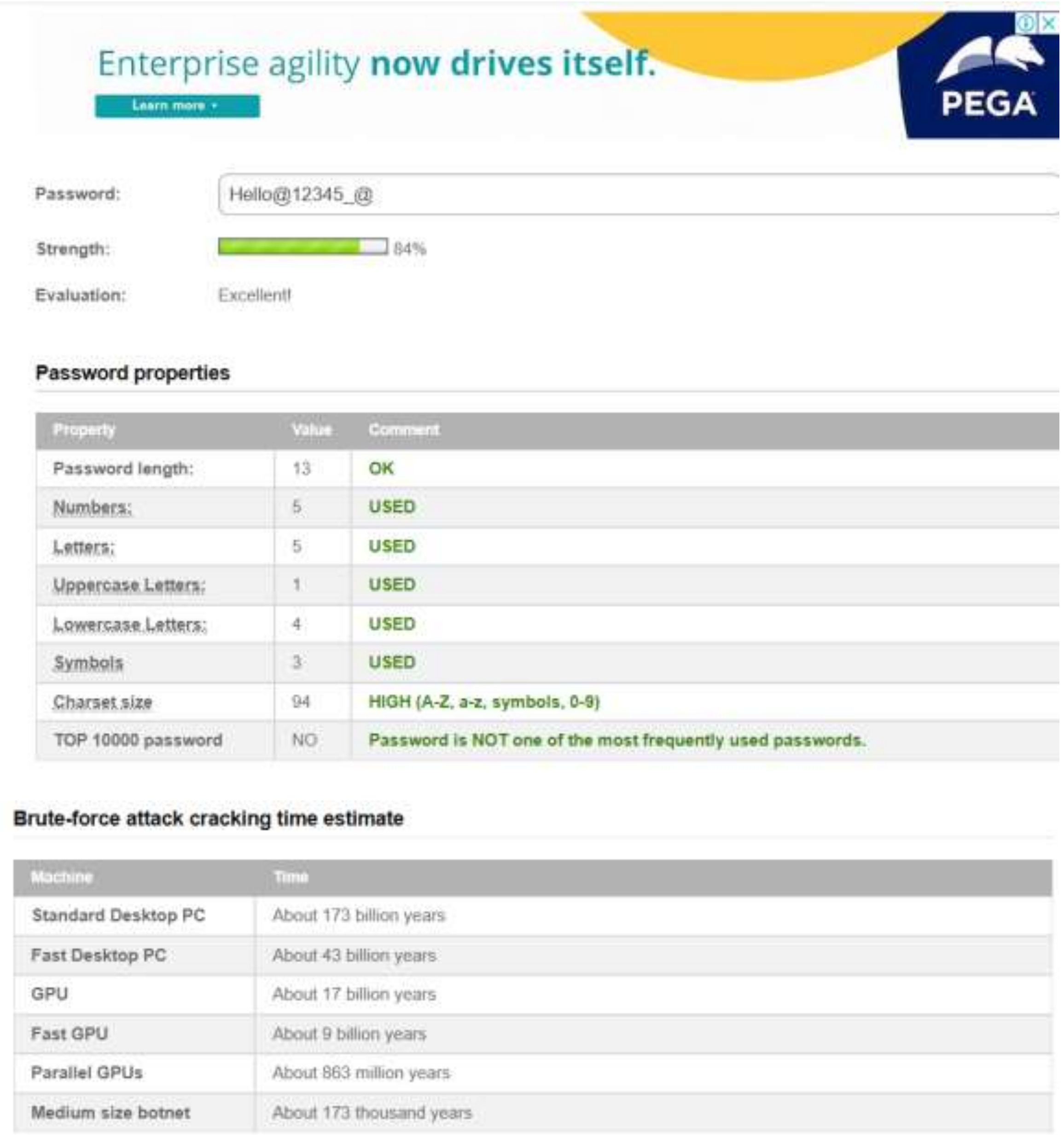
Password properties

Property	Value	Comment
Password length:	10	OK
Numbers:	3	USED
Letters:	5	USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	5	USED
Symbols	2	USED
Charset size	68	HIGH (0-9, symbols, a-z)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.



Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 8 thousand years
Fast Desktop PC	About 2 thousand years
GPU	About 68 years
Fast GPU	About 34 years
Parallel GPUs	About 3 years
Medium size botnet	About 6 hours



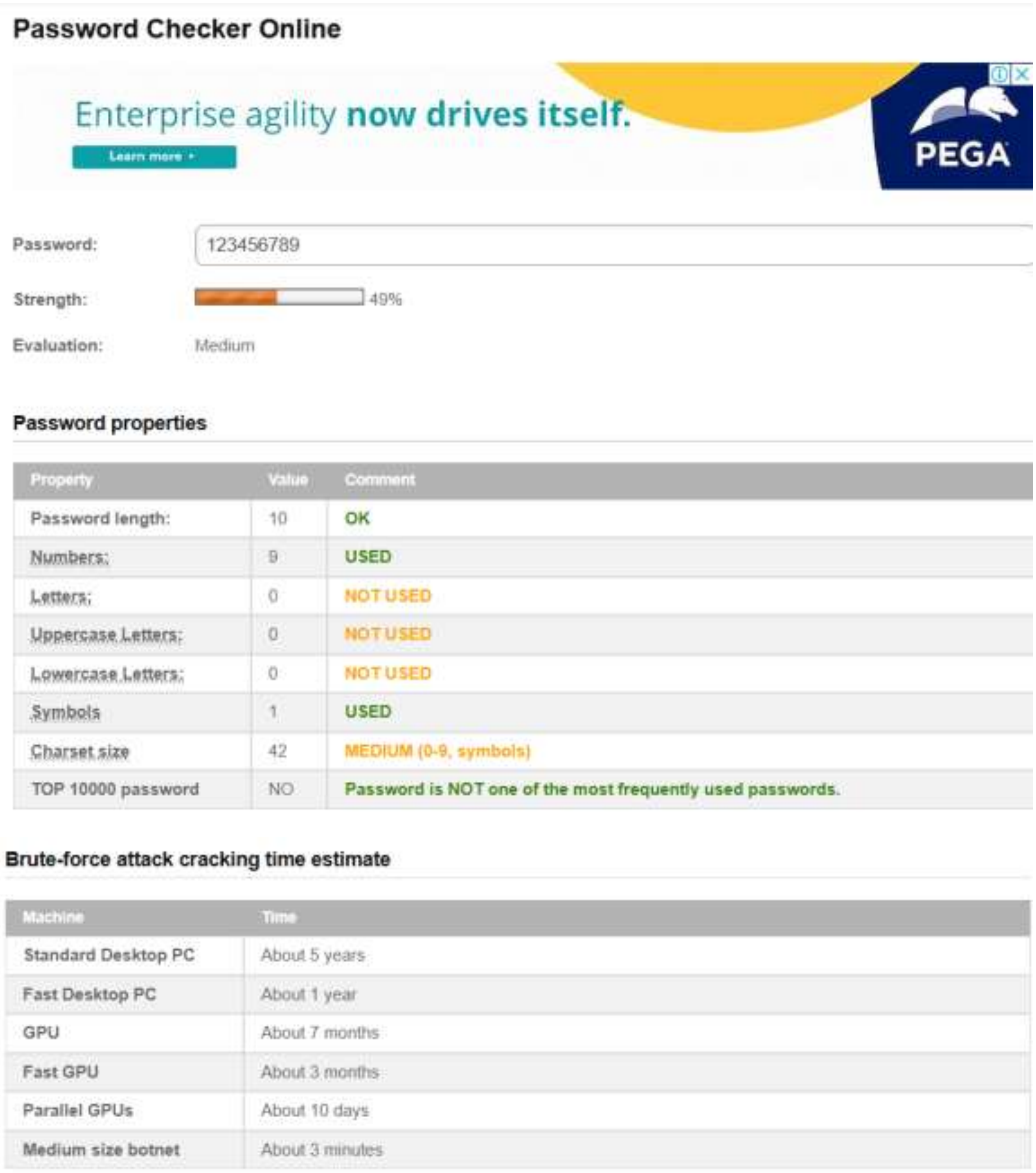
Password:	Hello@12345_@
Strength:	84%
Evaluation:	Excellent!

Password properties

Property	Value	Comment
Password length:	13	OK
Numbers:	5	USED
Letters:	5	USED
Uppercase Letters:	1	USED
Lowercase Letters:	4	USED
Symbols	3	USED
Charset size	94	HIGH (A-Z, a-z, symbols, 0-9)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 173 billion years
Fast Desktop PC	About 43 billion years
GPU	About 17 billion years
Fast GPU	About 9 billion years
Parallel GPUs	About 863 million years
Medium size botnet	About 173 thousand years



Password Checker Online

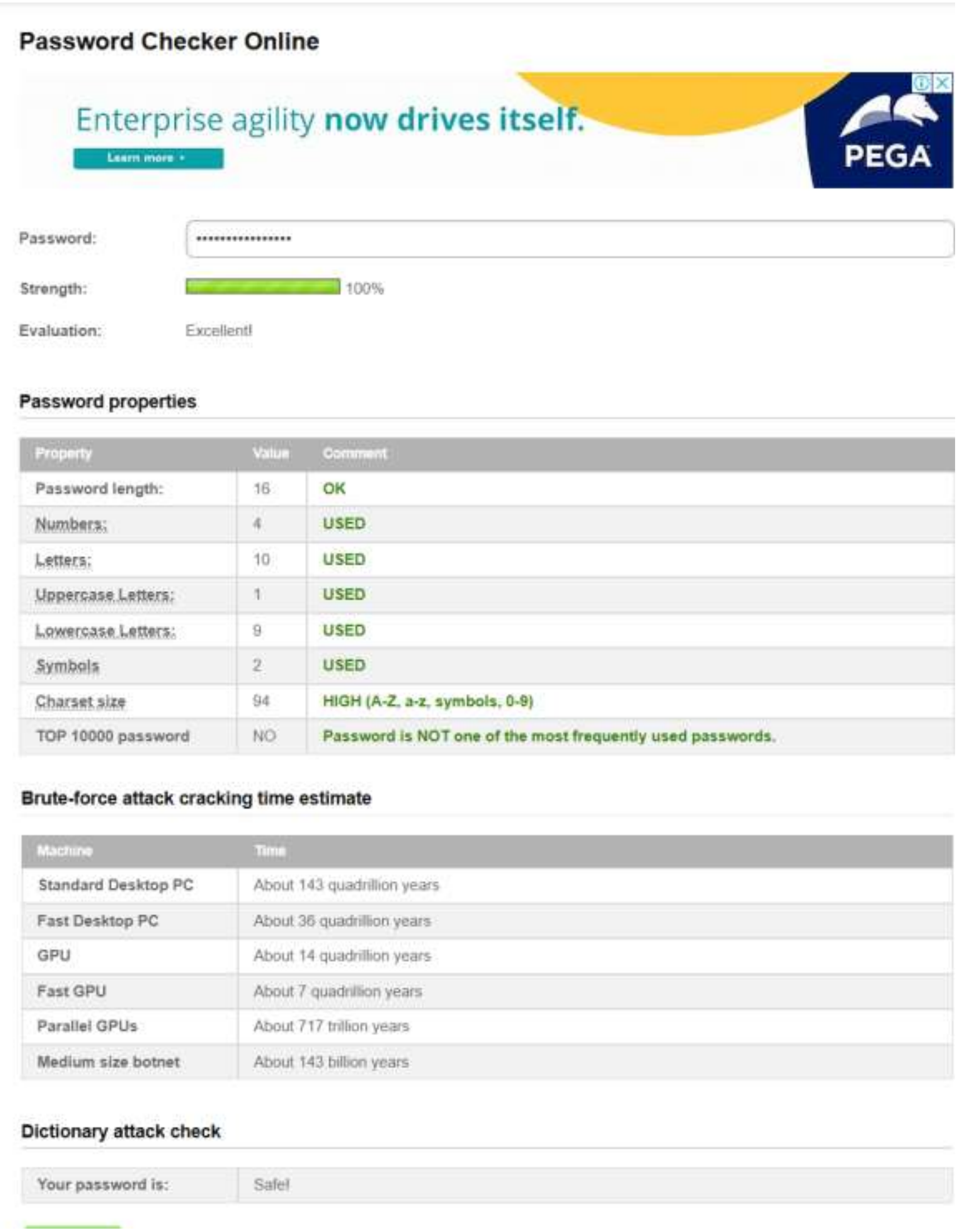
Password:	123456789
Strength:	49%
Evaluation:	Medium

Password properties

Property	Value	Comment
Password length:	10	OK
Numbers:	9	USED
Letters:	0	NOT USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	0	NOT USED
Symbols	1	USED
Charset size	42	MEDIUM (0-9, symbols)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 5 years
Fast Desktop PC	About 1 year
GPU	About 7 months
Fast GPU	About 3 months
Parallel GPUs	About 10 days
Medium size botnet	About 3 minutes



Password Checker Online

Password:	••••••••••••••••
Strength:	100%
Evaluation:	Excellent!

Password properties

Property	Value	Comment
Password length:	16	OK
Numbers:	4	USED
Letters:	10	USED
Uppercase Letters:	1	USED
Lowercase Letters:	9	USED
Symbols	2	USED
Charset size	94	HIGH (A-Z, a-z, symbols, 0-9)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 143 quadrillion years
Fast Desktop PC	About 36 quadrillion years
GPU	About 14 quadrillion years
Fast GPU	About 7 quadrillion years
Parallel GPUs	About 717 trillion years
Medium size botnet	About 143 billion years

Dictionary attack check

Your password is:	Safe!

Password	Strength (%)	Evaluation	Crack Time (Standard PC)
1234@1234	39%	Low	5 days
123_hello@	57%	Medium	8 thousand years
Hello@12345_@	84%	Excellent	173 billion years
123456789	49%	Medium	5 years

- **Analysis & Observations:**
  - Passwords with only numbers or basic patterns (e.g., 123456789) are weak and easily guessable.
    - Mixing symbols, uppercase, lowercase, and longer length significantly increases strength.
    - A strong password like 'Hello@12345_@' has an estimated crack time of trillions of years on average PCs.
    - Avoid dictionary-based patterns and use a combination of random characters.

- **Best Practices for Creating Strong Passwords:**
  Use at least 12–16 characters.
  Include uppercase and lowercase letters.
  Add numbers and special characters (!, @, #, etc.).
  Avoid common patterns like '1234', names, or dictionary words.
  Use passphrases or password managers to remember complex passwords.

- **Conclusion:**
  Creating a strong password is essential for protecting online identities. This task demonstrates how password strength checkers help in evaluating and guiding users to build secure passwords.