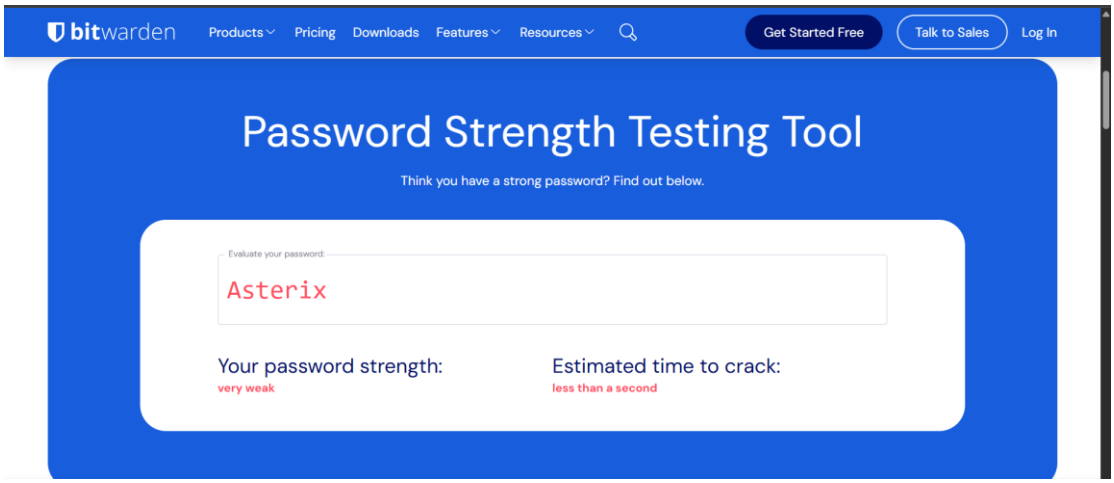
Password Strength Evaluation

Task:Create a strong password and evaluate its strength.
Date:July 1,2025

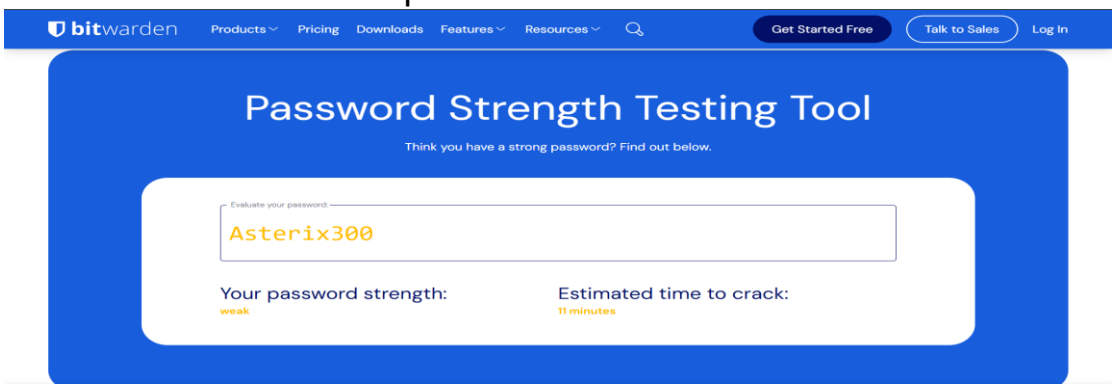
Objectives:
Understand what makes a password strong and test it against password strength tools.

Process

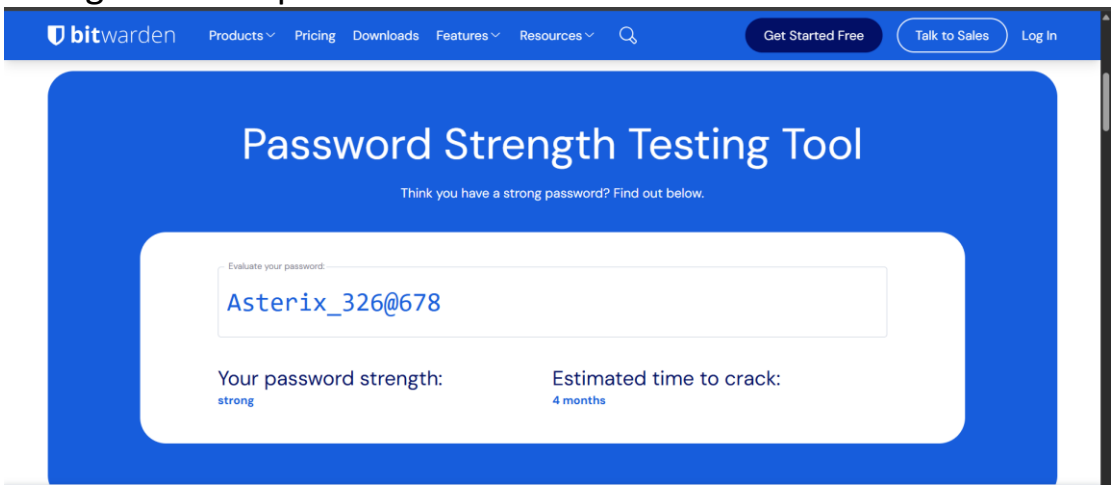
- I first went to a password testing site and starting typing passwords.
- First attempt:I typed a simple password without any number or special characters.It was rated very weak and estimated to be cracked in less than a second



- Second attempt:I added some numbers to the password.The strength improved slightly to weak and it would be around 11 minutes to crack the password.



- Final attempt:I used a combination of uppercase and lowercase,letters,numbers and special characters. The tool estimated it would take 4 months to crack this password- a significant improvement.



- This password strength detection actually comes from a password strength estimator “zxcvbn” developed by Dropbox.Unlike typical strength meters it doesn’t add rules like it needs number/symbol it uses pattern matching and real-world data to give more accurate feedback.

Summary

In this task, I explored how to create strong passwords and evaluate their strength using realistic methods. Instead of relying on traditional password rules (like including symbols or capital letters), I used **Dropbox's open-source tool "zxcvbn"**, which provides a more accurate way to estimate password strength.