

Task - 6

Principles of Password

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

Tools: Online free password strength checkers

About:

What is a password:

A password is a secret string of characters used to verify a person's identity and integrity for the system, it helps protect accounts, data, and systems from unauthorized access.

By keeping it private, only the rightful user can gain access without passwords, sensitive could be easily stolen or misused

What do attacker's do

Most of the times the attackers or hacker try to brute-force the password to gain access to the data or Network

So, keeping a strong password is very much important for protecting Network or data and organizations.

Even a least privileged employ account also matters because, once the attacker gain access to network he can plan many attacks.

There are some rules for the password.

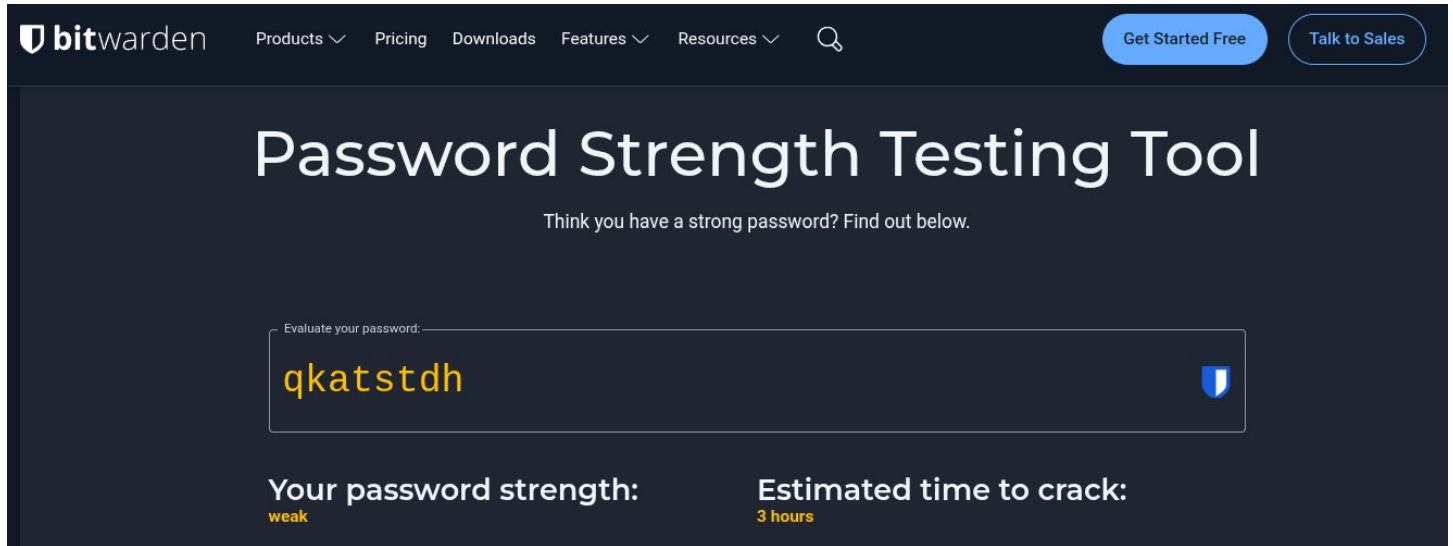
1. The length of the password must be more than 8 characters and recommend 10 characters
2. At least one special character
3. At least one number
4. Combination of uppercase and lowercase letters

Let us see why does these rule matters

Note: Hackers are not going to manually try each and every possibility, they use automated tools to crack passwords.

1. The length of the password must be more than 8 characters and recommend 10 characters

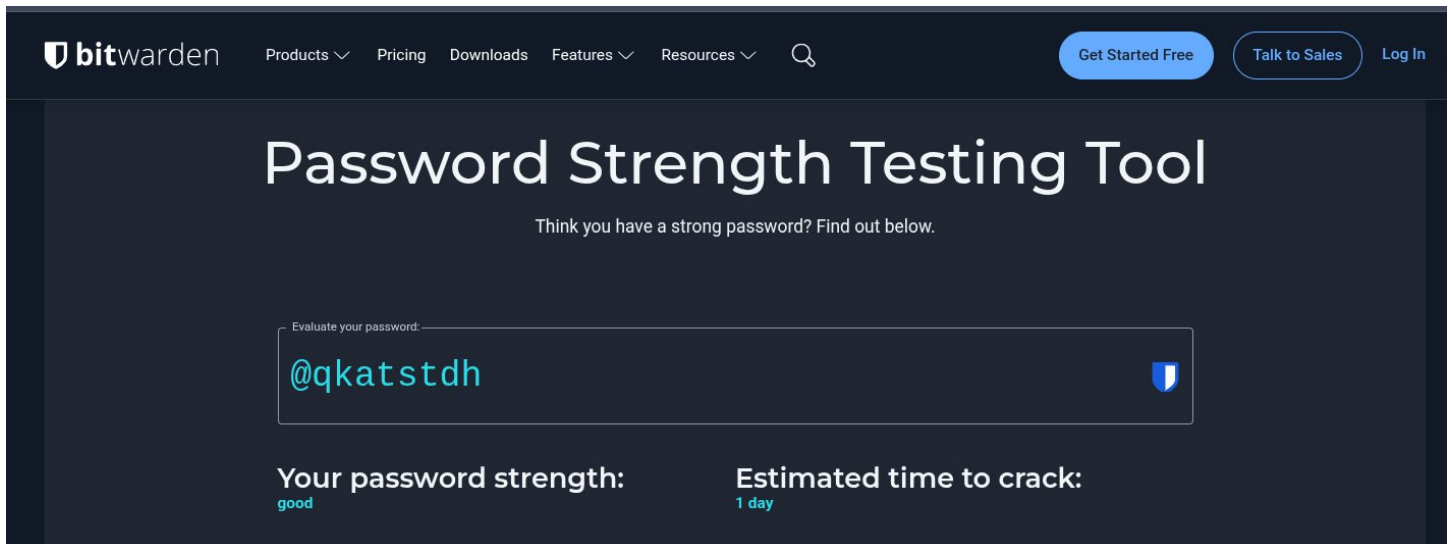
See the Simple 8 characters password only lower case takes 3 hours



The screenshot shows the Bitwarden Password Strength Testing Tool interface. The header includes the Bitwarden logo and navigation links: Products, Pricing, Downloads, Features, Resources, and a search icon. On the right, there are buttons for 'Get Started Free' and 'Talk to Sales'. The main heading is 'Password Strength Testing Tool' with a subtext 'Think you have a strong password? Find out below.' Below this is a text input field labeled 'Evaluate your password:' containing the password 'qkatstdh'. To the right of the input field is a shield icon. At the bottom, two results are displayed: 'Your password strength: weak' and 'Estimated time to crack: 3 hours'.

Field	Value
Evaluated Password	qkatstdh
Strength	weak
Estimated Time to Crack	3 hours

2. At least one special character, and include the first rule also



The screenshot shows the Bitwarden Password Strength Testing Tool interface with the same header and navigation as the first image. The main heading is 'Password Strength Testing Tool' with the subtext 'Think you have a strong password? Find out below.' The text input field labeled 'Evaluate your password:' now contains the password '@qkatstdh'. The results at the bottom are updated: 'Your password strength: good' and 'Estimated time to crack: 1 day'.

Field	Value
Evaluated Password	@qkatstdh
Strength	good
Estimated Time to Crack	1 day

See we added just a '@' symbol at starting , for a normal computer it takes 1 day to crack with brute-force attack.

3. Including rule 1 & 2, now implement rule 3, at least one number

The screenshot shows the Bitwarden Password Strength Testing Tool interface. At the top, there is a navigation bar with the Bitwarden logo, links for Products, Pricing, Downloads, Features, and Resources, and buttons for 'Get Started Free', 'Talk to Sales', and 'Log In'. The main heading is 'Password Strength Testing Tool' with the subtext 'Think you have a strong password? Find out below.' Below this, there is a text input field labeled 'Evaluate your password:' containing the password '@qkat9stdh'. The password is highlighted in a light blue box. Below the input field, there are two results: 'Your password strength: good' and 'Estimated time to crack: 12 days'.

By adding a number it takes 12 days to crack

4. Combination of uppercase and lowercase letters

The screenshot shows the Bitwarden Password Strength Testing Tool interface. At the top, there is a navigation bar with the Bitwarden logo, links for Products, Pricing, Downloads, Features, and Resources, and buttons for 'Get Started Free', 'Talk to Sales', and 'Log In'. The main heading is 'Password Strength Testing Tool' with the subtext 'Think you have a strong password? Find out below.' Below this, there is a text input field labeled 'Evaluate your password:' containing the password '@qKaF90t|dH'. The password is highlighted in a light blue box. Below the input field, there are two results: 'Your password strength: good' and 'Estimated time to crack: 12 days'.

It also takes 12 days to crack

These rules are good but there are one more rule which specifically should not do

Note: In any password should not use data of birth, years, pet names, parents names, mobile numbers, vehical names, place or area names in the passwords

Ex:

Rocky@2010

Priya#1987

Bullet_5678

Delhi\$2002

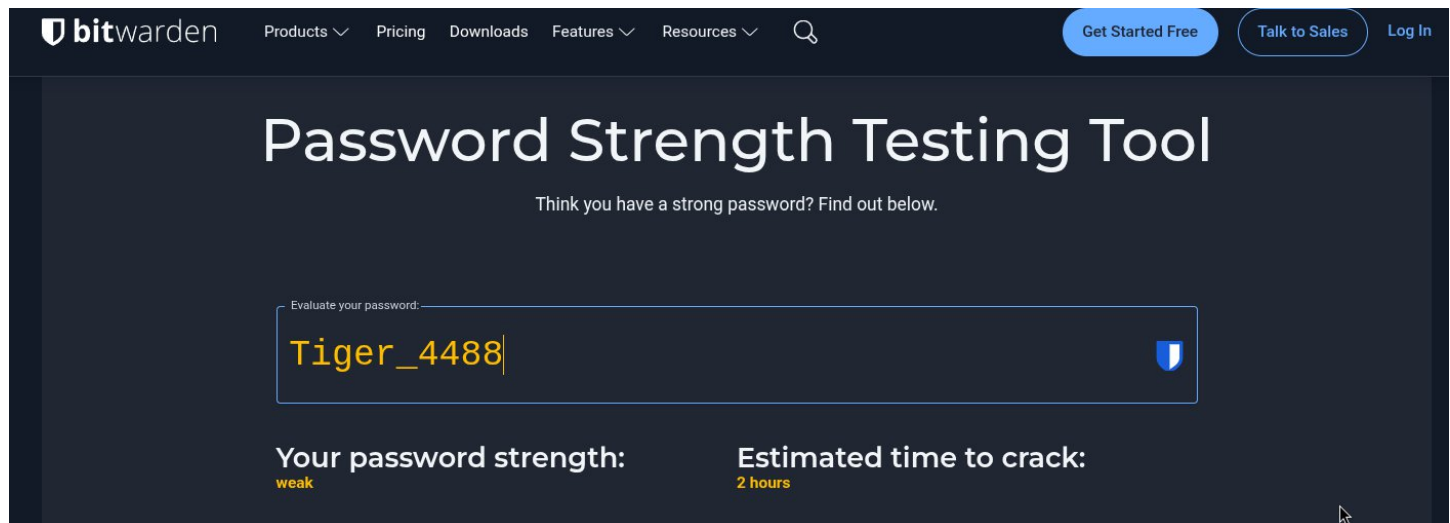
Shadow!9920

Honda#7865

Mumbai@1999

Tiger_4488

See the result of this password: Tiger_4488



The screenshot shows the Bitwarden Password Strength Testing Tool interface. At the top, there is a navigation bar with the Bitwarden logo, links for Products, Pricing, Downloads, Features, and Resources, and buttons for 'Get Started Free', 'Talk to Sales', and 'Log In'. The main heading is 'Password Strength Testing Tool' with a subtext 'Think you have a strong password? Find out below.' Below this is a text input field labeled 'Evaluate your password:' containing the text 'Tiger_4488'. To the right of the input field is a small Bitwarden logo. Below the input field, there are two sections: 'Your password strength:' with the result 'weak' in orange, and 'Estimated time to crack:' with the result '2 hours' in orange.

It follows all the rules numbers , special characters more than 8 , characters and uppercase and lower case letters
But it's too easy to them to get these kind of details , and with one information you may leak other's also

Summary:

Password complexity directly increases security by making guessing attacks much harder. Longer passwords exponentially raise the total possible combinations, slowing brute-force attacks. Including uppercase, lowercase, numbers, and special characters expands the character set, making each position harder to guess. Avoiding personal information prevents attackers from using social engineering or dictionary-based guesses, forcing them to attempt full-scale, time-consuming cracking methods.