Default password attacks

Default passwords are a common vulnerability that can allow unauthorized access to systems and applications. Many devices, software, and services come preconfigured with default or hardcoded passwords for administrative or maintenance purposes. If these default credentials are not changed, they can be easily exploited by attackers to gain unauthorized access.Default passwords are often publicly available or can be found through various sources, such as:

- Vendor documentation and manuals
- Online databases and forums
- Hacking tools and wordlists

Attackers can use this information to attempt to log in to systems or services using the default credentials. Even if the default passwords are not publicly known, they can be guessed or brute-forced, especially if they follow common patterns or are based on easily identifiable information like product names or vendor names.Successful exploitation of default passwords can lead to severe consequences, including:

- Unauthorized access to sensitive data and systems
- Compromise of network devices and infrastructure
- Installation of malware or backdoors
- Disruption of services and operations

There are certain databases online that we can use to find out default passwords of different products like routers, printers and applications. Some of them are -

Open-Sez, Fortypoundhead, CIRT, Router Passwords and Default-Passwords.info

So, make sure to keep this in your methodology that whenever you see a login panel of an application. Just try to log in with its default credentials or common username and password combos like - **admin:admin**, **admin:password**, **admin:pass123** or **admin:12345**. I hope you got the point.
