**NicePass is the lightest and the most secure password manager,**

* using the same password on multiple websites is risky and once the password is leaked from one of those websites, all your accounts will be at risk.
* by using a traditional password manager, you delegate managing your passwords to a third party. that works well but if the third party got compromised your passwords will be compromised.

**NicePass solves all of these problems, while also being the lightest password manager, open-source, and totally free to use. But how it works:**

* you remember only one main password and then generate a new secure password for each website you visit.
* NicePass does not store your passwords on a server and not even on your local machine.
* Instead, each time you want to connect to one of your accounts a password will be computed.
* we use a deterministic one-way algorithm to generate the password using your main password and the domain name of the accounts you want to access.
* this way you always get the same password for the website.
* but no one else can generate it if he doesn't have your main password
* and even if multiple accounts got compromised and a malicious actor got your passwords for these accounts there is no way he can reverse the algorithm and know your main password, so your other accounts will be secure.
* NicePass will generate at least a 90bit password that will require more than 10000 years to be brute-forced using the fastest supercomputer in the world.

NicePass is open source and anyone is invited to contribute and add more functionalities.