

PandaManager



Nadav Shamir
Maya Raskin

What is Panda Manager?

Panda Manager is a password manager designed to prioritize the security of its stored passwords; passwords are stored split between two databases

it is composed out of four 4 main components:

- Chrome extension
- Proxy service
- 2 databases
- Backend for each database



Chrome Extension

Pages:

- Login/Register
- Generate password
- Vault

Scripts:

- autoFill
- autoSave



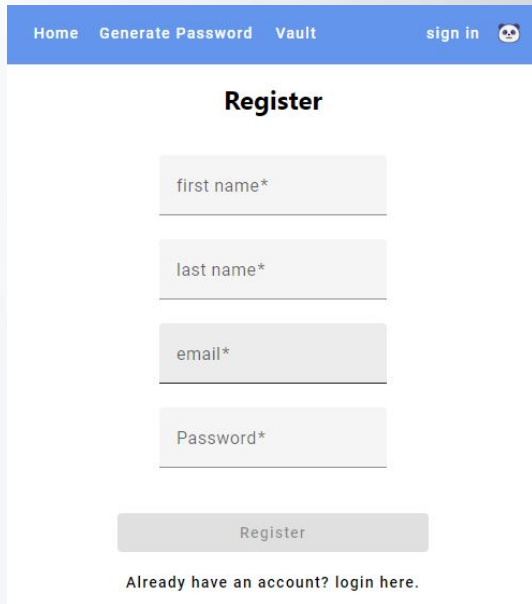
Chrome Extension

Pages:

- **Login/Register**
- Generate password
- Vault

Scripts:

- autoFill
- autoSave



Home Generate Password Vault sign in

Register

first name*

last name*

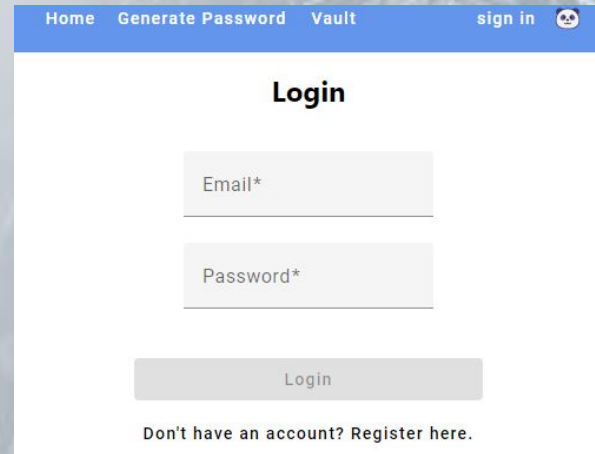
email*

Password*

Register

Already have an account? login here.

The screenshot shows a registration form with a blue header containing navigation links: Home, Generate Password, Vault, and sign in. The form title is 'Register'. It contains four input fields: 'first name*', 'last name*', 'email*', and 'Password*'. Below the fields is a 'Register' button and a link that says 'Already have an account? login here.'



Home Generate Password Vault sign in

Login

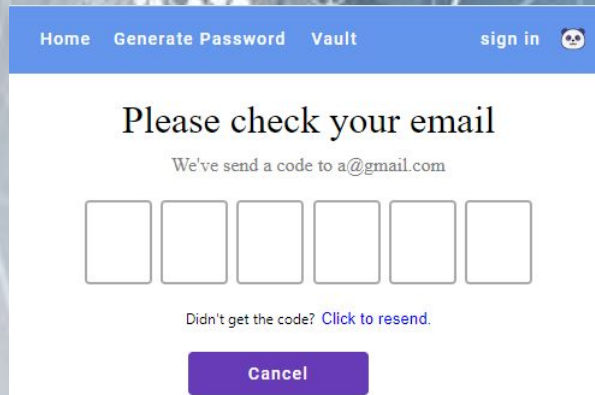
Email*

Password*

Login

Don't have an account? Register here.

The screenshot shows a login form with a blue header containing navigation links: Home, Generate Password, Vault, and sign in. The form title is 'Login'. It contains two input fields: 'Email*' and 'Password*'. Below the fields is a 'Login' button and a link that says 'Don't have an account? Register here.'



Home Generate Password Vault sign in

Please check your email

We've send a code to a@gmail.com

○ ○ ○ ○ ○ ○

Didn't get the code? [Click to resend.](#)

Cancel

The screenshot shows an email verification page with a blue header containing navigation links: Home, Generate Password, Vault, and sign in. The form title is 'Please check your email'. Below the title is a message: 'We've send a code to a@gmail.com'. There are six empty input boxes for the code. Below the boxes is a link that says 'Didn't get the code? Click to resend.' and a purple 'Cancel' button.

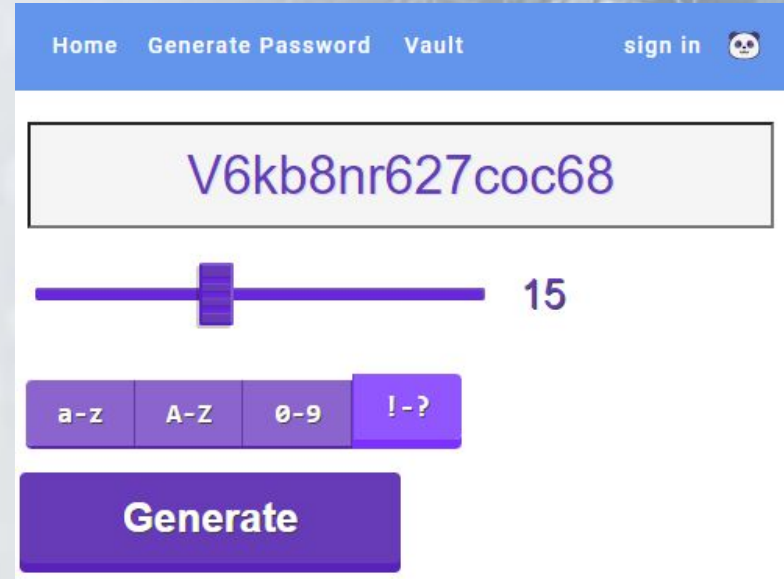
Chrome Extension

Pages:

- Login/Register
- **Generate password**
- Vault

Scripts:

- autoFill
- autoSave



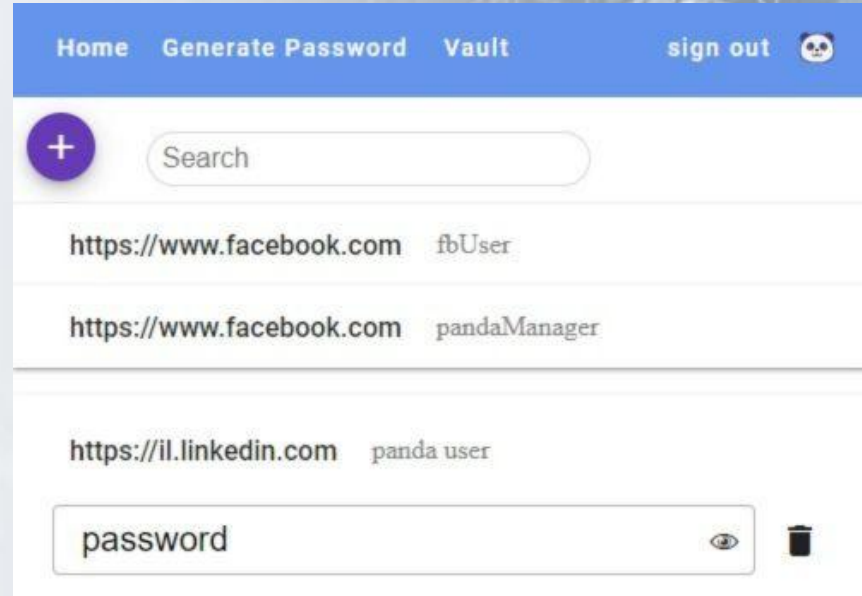
Chrome Extension

Pages:

- Login/Register
- Generate password
- **Vault**

Scripts:

- autoFill
- autoSave



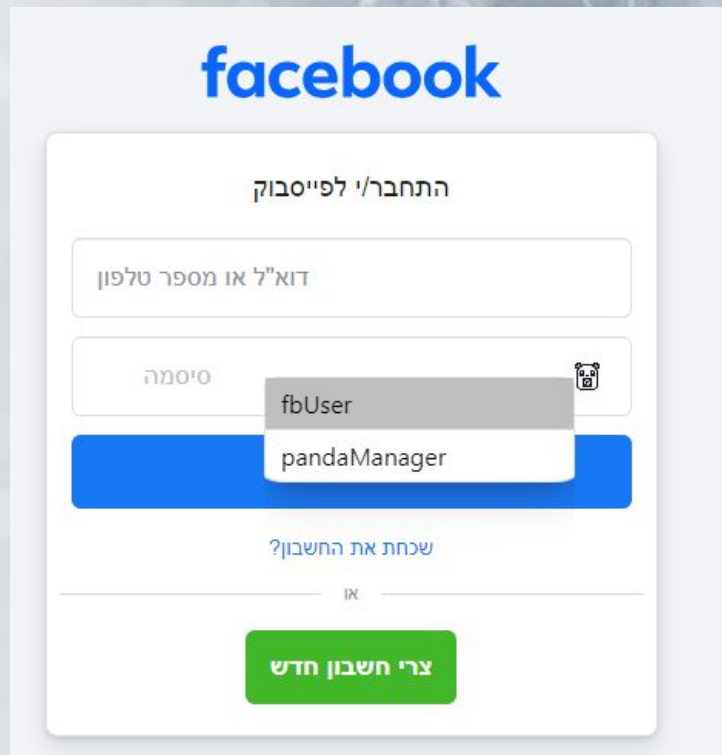
Chrome Extension

Pages:

- Login/Register
- Generate password
- Vault

Scripts:

- **autoFill**
- autoSave



The image shows a screenshot of the Facebook login page in Hebrew. At the top, the Facebook logo is displayed in blue. Below it, the text "התחברו/י לפייסבוק" (Log in to Facebook) is centered. There are two input fields: the first is for the phone number or email address, labeled "דוא"ר או מספר טלפון", and the second is for the password, labeled "סיסמה". A dropdown menu is open over the password field, showing two options: "fbUser" and "pandaManager". Below the input fields, there is a blue button with the text "שכחת את החשבון?" (Forgot your account?). At the bottom, there is a green button with the text "צרי חשבון חדש" (Create a new account).

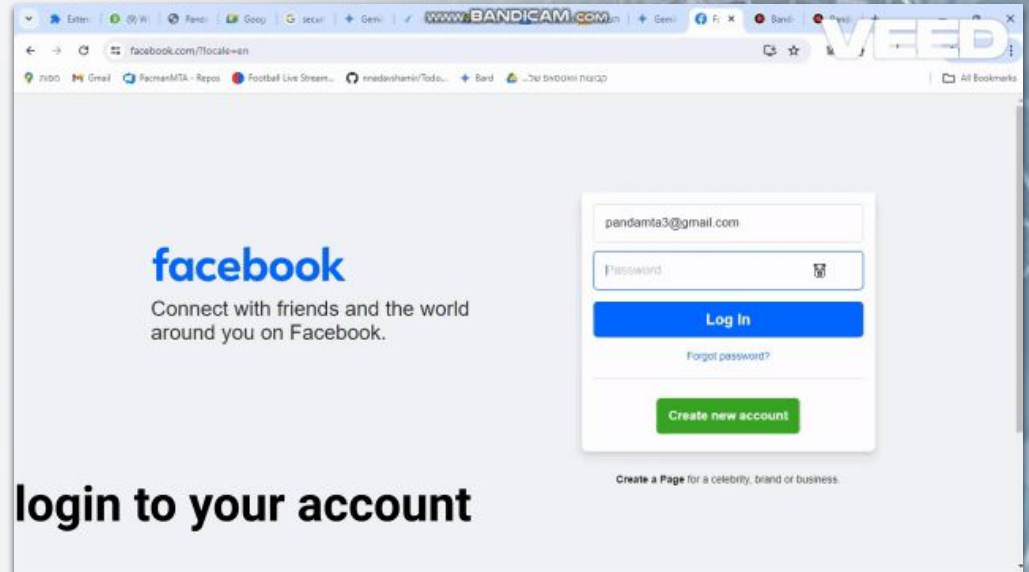
Chrome Extension

Pages:

- Login/Register
- Generate password
- Vault

Scripts:

- autoFill
- autoSave



Encryption

- Generate salt
- Encryption key (bcrypt)
- AES256 encrypt
- Pill creation

customSalt

`bcrypt(customSalt, "mypassword") = key`

`AES256(key, "mySecret") = encryptedData`

Pill

customSalt encryptedData

Encryption - Security

Resistant to attacks such as:

- MITM
- Brute Force
- Known Passwords Dictionaries



Databases

- 2 MongoDB clusters, each on a different region
- Hold the split info



Backends

- Main purpose - secure API to the credentials DB
- “Close” to the sensitive data
- Distribution - 2 distinct providers
- Distinct



Proxy

- Main purpose - API, backends orchestrator
- Protocol between the client & the proxy
- Also manages OTP, authorization, reverts



Security - Architecture

- 2 distinct providers
 - Provider is selected randomly
 - Secrets are stored in the providers vaults
 - App authorization + OTP for untrusted devices
 - Passwords have no meaning for the backends
 - DBs are accessible only from their matching backend
- 