Vulnerability Documentation

This is the documentation to test vulnerabilities in password managers found in the paper Analysis on the Security and Use of Password Managers. We have found five successful attacks that exploit vulnerabilities in Passbolt, Padlock and Encryptr.

Attacks

Userscripts

Before you start using any of the userscript attacks, you need to use a userscript manager.

For Chrome, use Tampermonkey.

For Firefox, use Greasemonkey.

Installing Scripts

Tampermonkey and Greasemonkey should automatically install the userscripts when you click the given install link. If you have trouble installing any userscript look at the wiki for your userscript manager.

Tampermonkey - https://tampermonkey.net/faq.php#Q102

Greasemonkey - https://wiki.greasespot.net/Greasemonkey_Manual:Installing_Scripts

Firefox is preferred because all the scripts will execute fully on Firefox.

Passbolt Fake Extension Installer

Install

MAKE SURE YOU REMOVE ALL OTHER USERSCRIPTS OR ELSE IT MAY NOT WORK

This script will change all links that download the passbolt extension to download a random script (we chose NoScript). For this to work you need to use Firefox (See Userscripts for more info).

After you install the program, you can use your own Passbolt server (look at Passbolt's medium blog for a tutorial on how to set it up), or you can use Passbolt's demo server. Make sure that you **don't** have Passbolt's extension installed, or else no links will show.

1. Go to your server's login page (For Passbolt's demo this is demo.passbolt.com).
2. Hover over the link that says `Download it here`.

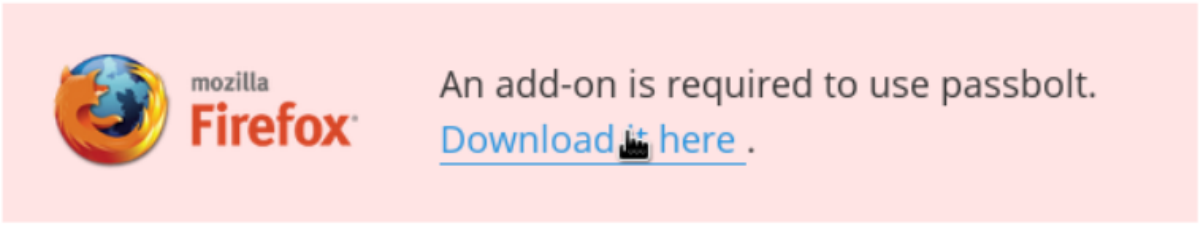

Figure 1: Hover over link

3. Look at the bottom left and notice that Firefox says the link goes to `https://www.passbolt.com/download/firefox`

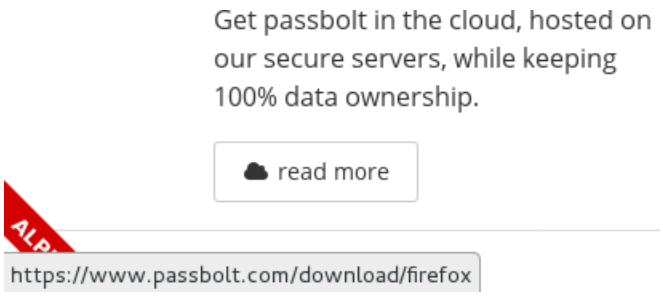

Figure 2: Firefox shows link still is Passbolt

4. Click on the link and press allow on the Firefox popup.

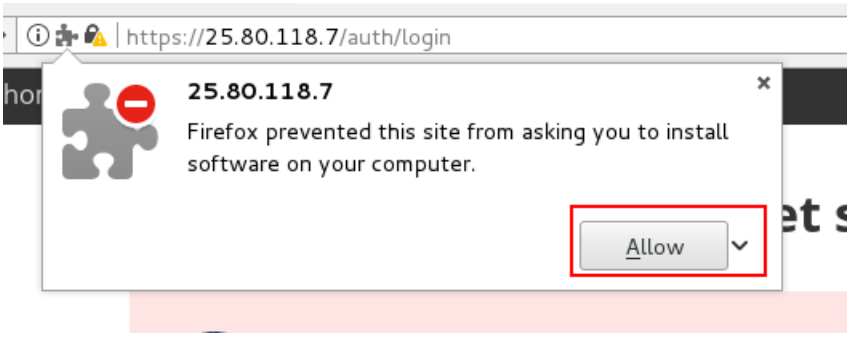

Figure 3: Allow server to install extension

5. Notice how Firefox is installing `Noscript` Rather than `Passbolt`.

The script made the link look like it was downloading a link from Passbolt but it changed the link to download a different link. This extension could have the logo and name of Passbolt and the user will be unlikely to see any foul play.

If the script didn't work or there was problem testing, open an issue and we will come back to you.

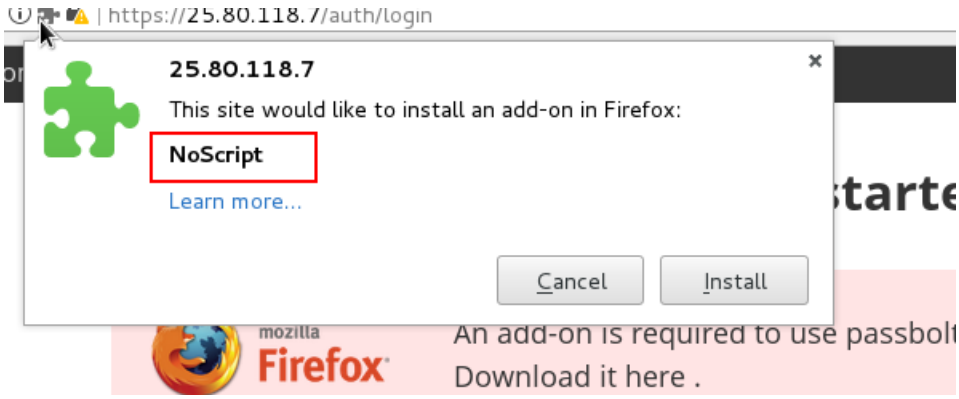

Figure 4: Downloads NoScript instead of Passbolt

Padlock Data Reset

Install

MAKE SURE YOU REMOVE ALL OTHER USERSCRIPTS OR ELSE IT MAY NOT WORK

This script will automatically reset all data on a Padlock account.

Padlock Application Setup

You first need to install Padlock and get the cloud connected. You can download Padlock here. You can use the Padlock cloud here, which is on a 30 day trial, or you can use your own Padlock cloud which you can install from here. If you use a custom server, you can check out my custompadlock repo which is a custom application that will allow the application to use `http://` so you don't have to get a certificate.

If you used my custom padlock application then the layout is not exactly the same but the steps are basically the same. I use the most updated version of padlock but the application on the official website is behind

Once you get your cloud and program running, go to the Padlock application itself. Log in to your account, and get to page that has `Import Data, Synchronize and Create Record`. Click on `Synchronize data > Open Padlock Cloud Settings`. If you use a custom server click on `use custom server > continue` and enter the IP of your server. Next press `get started` and then enter in your email (You can use a service like Guerrilla Mail to make multiple accounts). Then press `connect`. Go into your email and you should receive an email with a link. Click on the link and your application should be synced with the cloud. You can check this by clicking `synchronize` on the application. The application should say that it synced correctly. You can go back to the application and press the `<` in the top left twice until you get back to the screen with `Import Data, Synchronize and Create Record`. Click `Create Record` and enter an example name, like `test name` and then press `add`. Click on the box with `username` then click `edit`. You can now enter in an example username like `testusername`. Then click anywhere outside of the text box. Now click the box with `password` then click `Edit`. Enter in a password like `testpassword`. Then click anywhere outside of the box. Your screen should know look like

You can press on the top left `<` and then click on the three lines in the top left. Then click on `synchronize`. The bottom of the application should say application should say that it synchronized correctly. Next you need to test the syncing to ensure that the steps for testing the userscript should work. First, you need to reset the app

Resetting

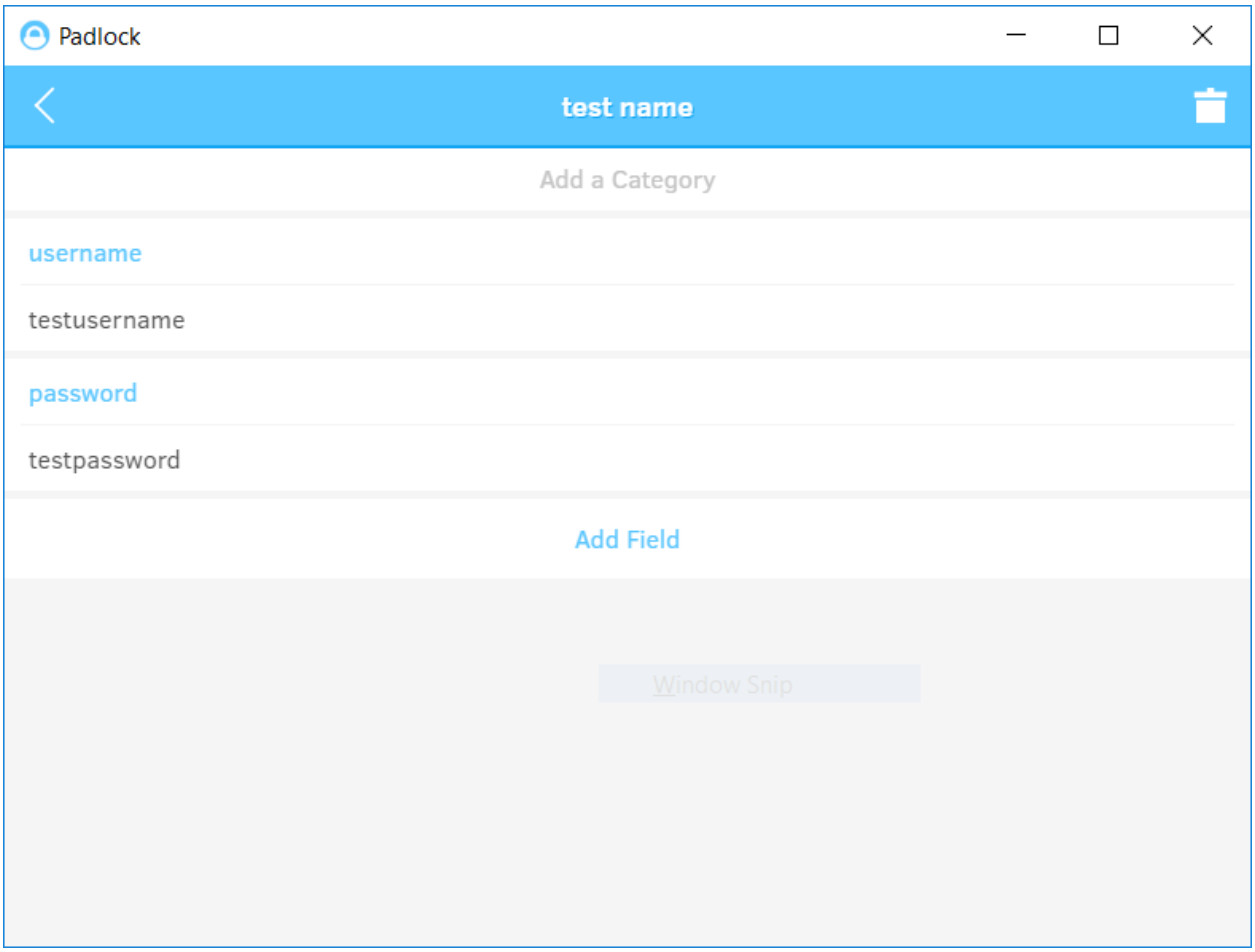

Figure 5:

To reset the application go to the screen that looks like

Click on the the three lines in the top left and then click `settings`. Next click `reset app`. Enter your master password and then your application should be reset.

Resync

After, resetting, create a new master password and log back into Padlock. You should see a menu with `Import Data, Synchronize and Create Record`. Click on `synchronize` and use the same email and server that you used before. Click on `get started`, enter your email, and go to your inbox. When you receive an email with the link, click on it and the application should be synced. After you click the link, go to the Padlock application and click on `synchronize` or `synchronize now` (whichever pops up). If you go to where your records are stored (press the `<` in the top left until you see it), you should see the entry we made earlier.

If you see something similar to this, then you have succesfully synced Padlock to the cloud!

If you had a problem with the above, open an issue and we will come back to you.

Testing Script

To test the script, install the script with the link given above (See installing scripts).

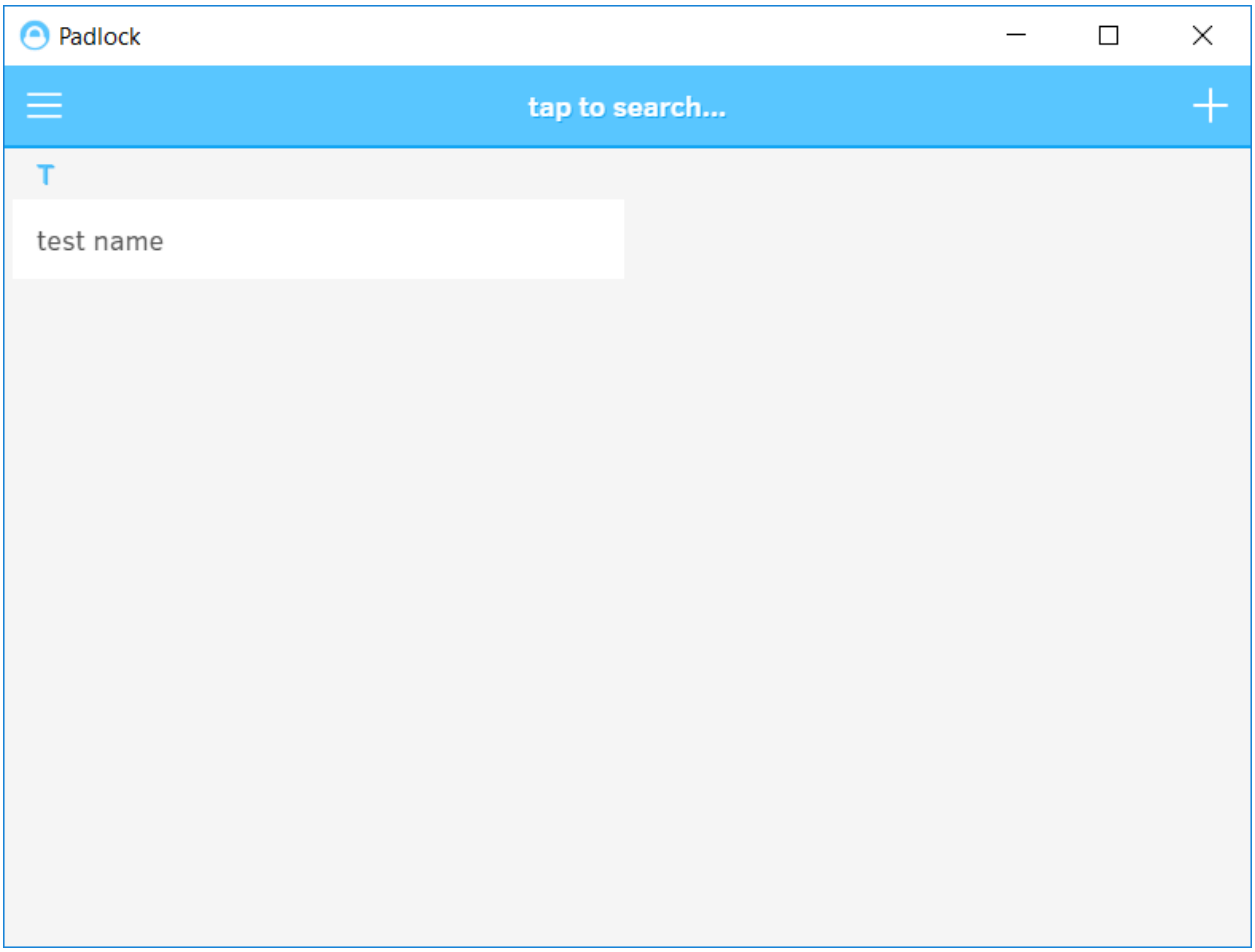

Figure 6: padlock

Once you install the script make sure you have usernames and passwords stored in the cloud (this is done in padlock application setup). Now reset your application (see resetting).

Next, log in to the dashboard for the cloud server that you used with the script active. To do this, go to the url of your server. For the padlock cloud this is at cloud.padlock.io. Use the email you used in the setup and a link should be given to your email.

Upon clicking the link, the userscript will autoclick things on the screen so the page will change. Make sure that the script is active before you click the link.

Depending on your computer, the website will change 1-10 times. This is dependent on when the script and buttons load on the screen. When the website stops changing the top of your screen should show `Your data has been reset successfully!`.

Now resync your padlock application (see resync for the steps). Upon resync, you should see that no entries are restored. All the data has been cleared.

If the script didn't work or there was problem testing, open an issue and we will come back to you.

Padlock Access Remover

INSTALL

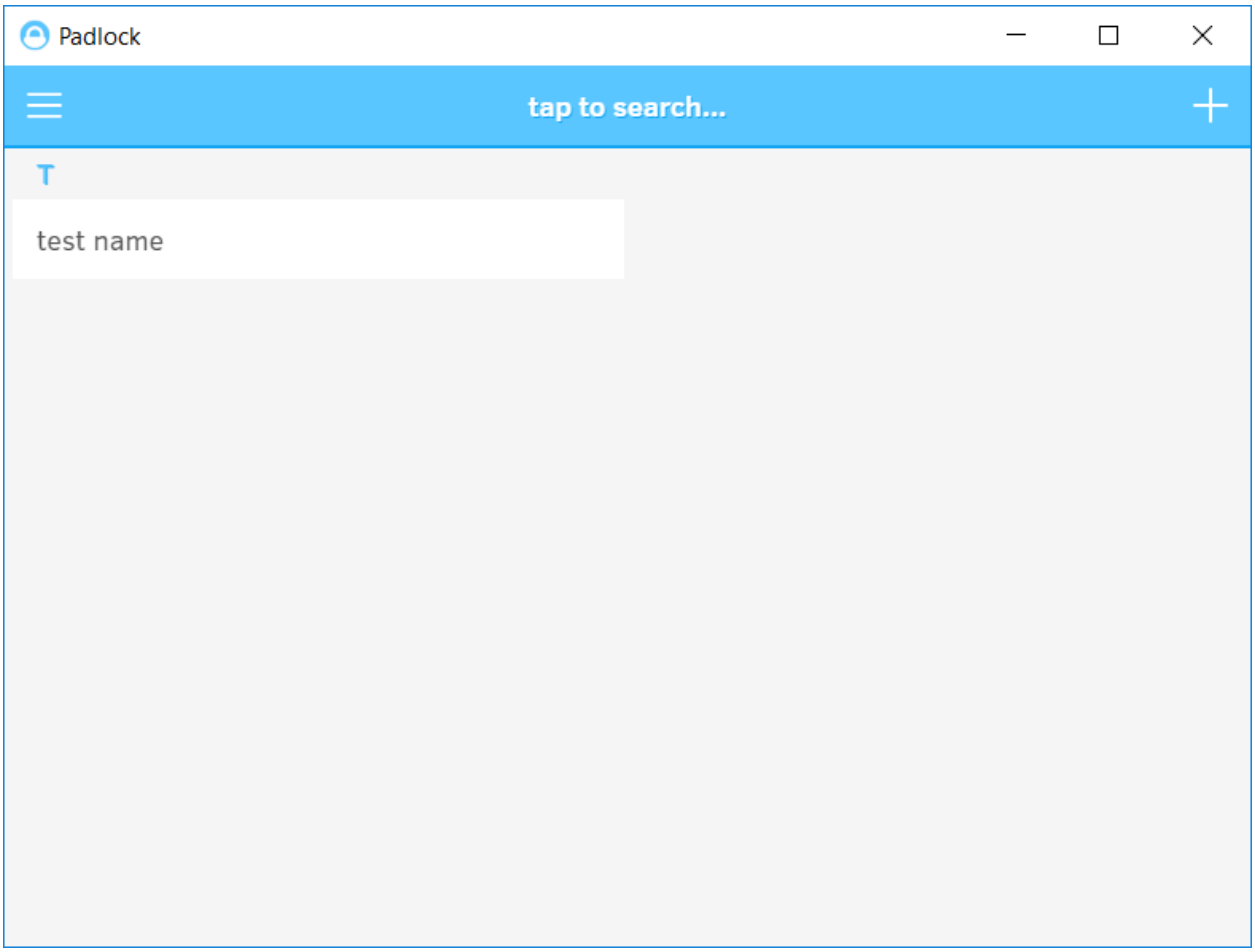

Figure 7: Padlock

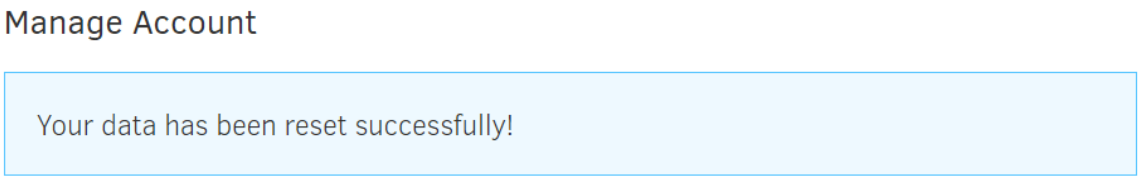

Figure 8: Padlock

MAKE SURE YOU REMOVE ALL OTHER USERSCRIPTS OR ELSE IT MAY NOT WORK

Padlock Application Setup

See Padlock Application Setup above.

Testing Script

To test the script, install the script with the link given above (See installing scripts).

Make sure that you went through all the steps of Padlock Application Setup.

Next, log in to the dashboard for the cloud server that you used with the script active. To do this, go to the url of your server. For the padlock cloud this is at cloud.padlock.io. Use the email you used in the setup and a link should be given to your email.

Upon clicking the link, the userscript will autoclick things on the screen so the page will change. Make sure that the script is active before you click the link.

Once you click the link, you might end up at `https://cloud.padlock.io/subscribe/` with a page saying `Bad Request: No stripe token provided`. This is normal. Go back to the application. You should see a message saying `It seems you have disconnected from Padlock C.loud. Please reconnect ...`. The script revoked your access to your account, but it did not reset your data.

If the script didn't work or there was problem testing, open an issue and we will come back to you.

User Input Attacks

Both user input attacks were built in C# for use only on Windows devices. They work in much the same way. Both of the attacks save plain-text logs with timestamps. Every 10 minutes, the attacks send the logs to our email and delete them from the victim's computer.

Keylogger Attack

The keylogger saves every key press and click into a plain-text file. It attaches a timestamp at the beginning of each log and after 30 seconds of inactivity.

Clipboard Reader

The clipboard reader checks four times every second to see if the contents of the clipboard have changed. Every time it detects a change, it logs the timestamp and clipboard contents.

Installation

Both of these attacks can be hidden in the installation of a different program and set up to run every time Windows boots up. For our purposes, we combined both attacks into a single installation.

In order to test, first go to this link and download one of the below files:

- Manual-start program: download loggers.zip
- Windows-startup installer: download setup.exe

If you download the manual-start, unzip the file and skip to Setup

If you download the installer, the files will be saved in the following location:
`C:\Users\<WINDOWS ACCOUNT NAME>\AppData\Local\Fake Microsoft Process`

Setup

In the folder where you saved the file should be a file called config.json
Enter in your email and password. The program will send you emails from yourself with the logs attached. You must use a gmail account. Example:

```
{
    "email": "exampleaccount@gmail.com",
    "password": "examplePassw0rd"
}
```

Next you must click this link to allow less secure apps.

Now double click temps.exe to run the program. For testing purposes we have set the program to email you every 40 seconds instead of 10 minutes, so type, copy/paste, etc and check your email after 40 seconds.

Stopping the Program

When you are done testing, press `Ctrl + Alt + Delete` to open Task Manager. Look for `temps` under background processes and end the process.

If you used the Windows-startup installer and you want to remove it from your startup processes, press `Ctrl + Alt + Delete` to open Task Manager. Click on the `Startup` tab on the top bar of Task Manager. Click on `temps` and click `Disable`.