

DESIGN AND IMPLEMENTATION OF PASSWORD MANAGER FOR WEB BROWSER

Ms. Neetu Anand¹, Piyush Mankad²

¹Assistant Professor, Department of Computer Science, Maharaja Surajmal Institute, Janakpuri, New Delhi, India

²UG Student, BCA, Maharaja Surajmal Institute, Janakpuri, New Delhi, India

Abstract: *In the modern world, with the increase in the services provided through the internet, a typical person uses a lot of websites which are providing diverge services such as social networking, job hunting, banking, e-mails, push messaging, e-commerce websites, matrimonial services, electronic newspapers and magazines, discussion groups, educational websites and blogs. These websites may be providing us with different services using various technologies but they have one thing in common, they all require you to have an account in order for you to access those services or to get a premium membership. So many accounts requires a lot of passwords to remember, so we end up using simple passwords instead of complex ones, which are easy to hack, jeopardising our privacy and endangering our personal as well as professional information. A Password manager helps you with just that, it provides you with an interface where you can store all your passwords of the various accounts you use and get an access to them with just a single master password. It's easy and most of all safe.*

Keywords: Password Manager, Chrome extension, MySQL

I. INTRODUCTION

A Password manager stores all your account's passwords along with the usernames (so that you can have more than one account on that website) and the website name as well (so as to automatically fill out the username and password for the particular account). [1]A Password manager stores all the passwords in an encrypted database so that even if the security gets breached the passwords retrieved by hackers are only a set of hash code and hold no meaning in general until deciphered.

In addition, to keep passwords secured, password manager offers a variety of other services one of them being *Password generator*. Even with the use of a password manager people tend to use simple passwords consisting of only lower case letters which are fairly easy to guess when a dictionary attack is launched. On the other hand, a *password generator* give rise to an alphanumeric password consisting of both lower and upper case alphabets along with numbers and includes special characters sometimes. [2]These types of complex passwords are quite hard to guess and take a considerable amount of time to break, but the good part is that you can leave the task of remembering these passwords to the password manager. Another feature of a password manager is the *Automatic form filling option*. While surfing the internet you may come across several websites which may require you to fill up some significant amount of your personal information like address, mobile numbers, and first and last names' etcetera. The password manager stores all this information of in its usual encrypted database and gives you an option of filling the form automatically when you come across one.

II. SOFTWARE TECHNOLOGY REVIEW

In this section, we talk about the several software that was used to make this extension.

1. Google Chrome extension

Unlike an Enterprise application a Website or system software, an extension is a small software program embedded in the browser to add functionalities and enhance the browsing experience. Extensions enable users to customize their browser functionalities and modify them to their specific requirements and preferences[3].

An extension is built on HTML, CSS, JavaScript- the same technology that we use to build our websites and are used for the same defined purpose that is HTML is used for structuring the page, CSS is used for styling and JavaScript is used as a scripting language. Apart from this, an extension can be single purpose or multi-purpose meaning that it can have several components and a range of functionalities so it can go from being a single icon on a screen acting as a notifier or be a big application that can override the entire page. Extensions do not depend on the content from the web as they are zipped into a .crx file, which the user installs.

2. MySQL

MySQL is relational database system that we are using to store passwords. MySQL is an open-source software that uses SQL (Structured Query Language) to carry out all the requests of fetching and storing the data in the database apart from this, it is easy to learn. [4] In a relational database, the data is stored in the form of organized and well-described tables from which the data can be retrieved by running several queries in SQL language without disorienting or changing the structure of the database.

Because the database is stored in the servers and can be accessed only through a server sided language we take the help of PHP. PHP is used to carry out several SQL queries for accessing the database.

III. DEVELOPMENT

Several processes that are required for the development are listed here

1. Manifest file

A manifest file stores all the information like name, description, version, manifest version and several default actions like popup, icon, keyboard shortcut commands about that particular extension and It is important for every extension to have a manifest file. A manifest file stores data in JSON format and looks like as shown in figure 1

Fig 1: Manifest File

```
1 {  
2   "name": "Password Manager",  
3   "description": "stores your passwords",  
4   "version": "1.0",  
5   "manifest_version": 2,  
6   "browser_action": {  
7     "default_popup": "pass.html",  
8     "default_icon": "lock16.png"  
9   }  
10 }
```

2. HTML file

An HTML is where you put all the pages that are to be displayed and used. Initially, the HTML file displayed is the one that is specified in the manifest file. You can add links to several files depending on the functionalities for example we can add these two links:

1. for adding websites to the database
2. for displaying all the websites and passwords

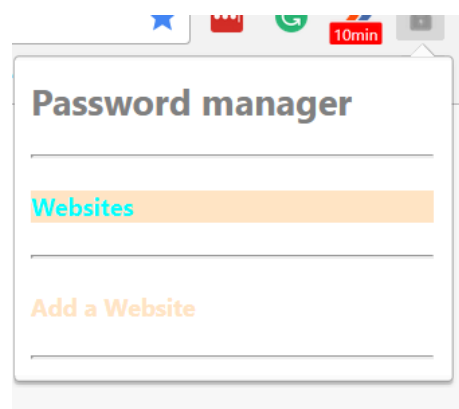
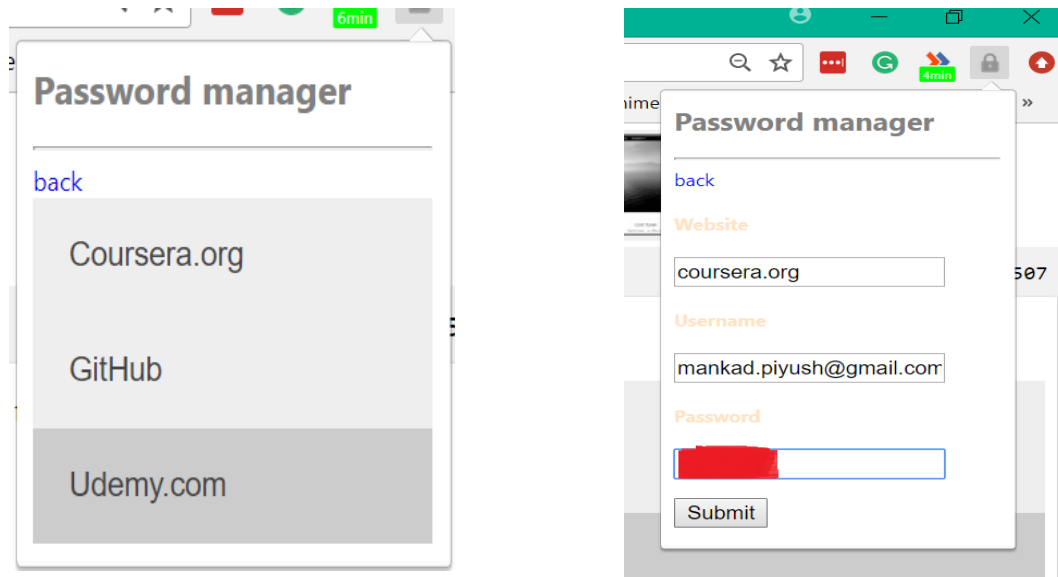


Fig 2: Adding links to File

In order to add websites we have specified three fields namely website name, username and password. All of these fields are inputted and on the click of submit button a form action takes place that adds these fields to the database[5].

After successfully adding these websites you can successfully retrieve them from the 'Websites' tab

Fig3: Adding website to File



IV. CONCLUSION

Password manager is very crucial and critical software and is used to protect sensitive information. It is also quite helpful in storing passwords and the user don't have to open a separate file to view their passwords as the extension needed is embedded into the browser itself. Millions of online users are taking the benefits of these type of applications, benefits includes 1) It has been not require to keep a text pad to store the username and passwords 2) It also deny the requirement of storing private information that might get hacked on mobiles or tablets. 3) It is also not needed to remember all the information by the users. 4) Users need not to worry about hacking as password manager is designed by using encryption technology. Finally, our works shows that it is certainly possible to create a system that is endow with security, utilizable and require low computation and least storage overhead, using standard cryptographic tools.

References

- 1) Agile Bits, Inc. 1password agile keychain design. http://help.agilebits.com/1Password3/agile_keychain_design.html.
- 2) Blanchou, M. and Youn, P.(2013)Password managers exposing passwords everywhere," <https://isecpartners.github.io/whitepapers/passwords/2013/11/05/Browser-Extension-Password-Managers.html>, 2013.
- 3) Blasko , G, Narayanaswami, C., and Raghunath, M.(2005) A Wristwatch-Computer Based Password-Vault. Technical report, IBM Research Division, 2005.
- 4) Belenko and D. Sklyarov. "Secure Password Managers and \Military-Grade Encryption" on Smartphones: Oh, Really? Technical report, Elcomsoft Co. Ltd. 2012. <http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf>.
- 5) "The importance of using strong passwords," <https://msdn.microsoft.com/nb-no/enus/library/ms851492%28v=winembedded.11%29.aspx>.