Grado en Ingeniería Informática

Departamento de Ingeniería Informática

Seguridad en los Sistemas Informáticos

Práctica 3.1: Gestores de contraseñas

Autores:
Juan Boubeta Puig,
Jesús Rosa Bilbao y
David Ureba Moreno

Fecha:
7 de octubre de 2019

Índice

Índice de figuras

1. Objetivo

El objetivo de esta práctica es conocer los gestores de contraseñas más usados y su utilidad frente a otras malas prácticas como, por ejemplo, guardar la contraseña en el navegador.

2. Conocimientos previos

A continuación, se describen los conocimientos previos que han de conocerse para llevar a cabo esta práctica:

Gestor de contraseñas Aplicación que almacena usuarios, contraseñas, notas, etc. en una base de datos cifrada y protegida con una contraseña maestra. Además, algunos gestores permiten generar contraseñas seguras.

2FA (Segundo factor de identificación) Medida de seguridad extra que normalmente requiere de un código obtenido de una aplicación, un SMS o un fichero *llave*, aparte de las credenciales para acceder al servicio.

Entropía La aleatoriedad recogida por un sistema o una aplicación para su uso en criptografía o para otros usos que necesiten datos aleatorios.

3. Herramientas necesarias

En esta práctica vamos a hacer uso de *LastPass* (`https://www.lastpass.com/`), por ser de las pocas opciones *freemium* del mercado funcionales en Windows, Mac y Linux.

4. LastPass

LastPass es un gestor de contraseñas *freemium* que almacena las contraseñas cifradas en la nube (véase Figura 1). Se encuentra disponible como extensión para casi todos los navegadores.

Utiliza el cifrado AES de 256 bits con PBKDF2 SHA-256 y *hashes* con sal para garantizar una seguridad total en la nube (véase Figura 2).

Los datos son cifrados y descifrados en el dispositivo. La información guardada en la nube es secreta, incluso para *LastPass*. La contraseña maestra y las claves utilizadas para cifrar y descifrar los datos nunca se envían a los servidores de *LastPass*, tampoco se podrá acceder nunca a ellas.

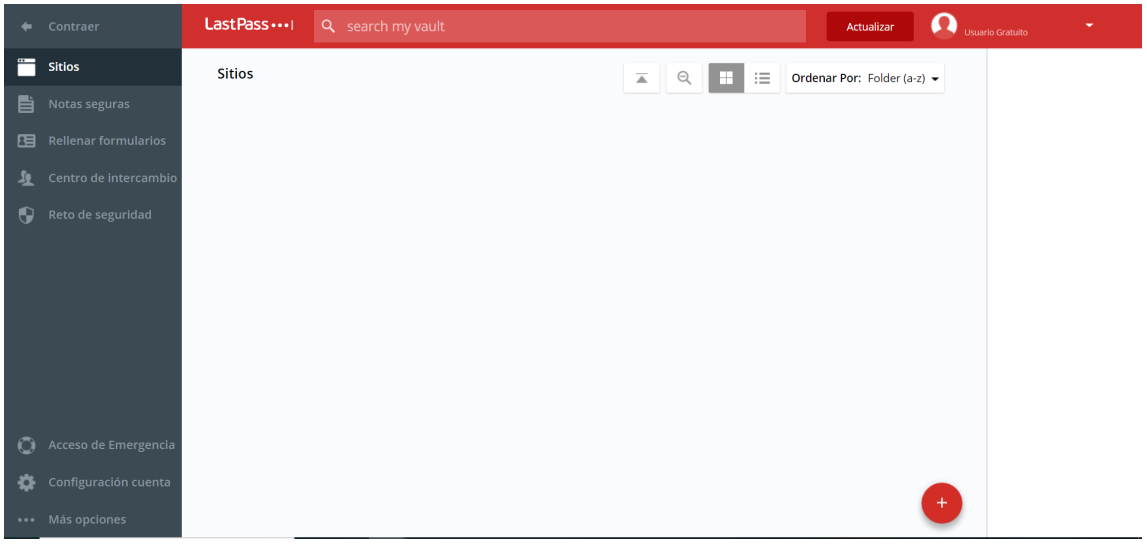

Figura 1: Interfaz de *LastPass*.

Figura 2: Seguridad en *LastPass*.

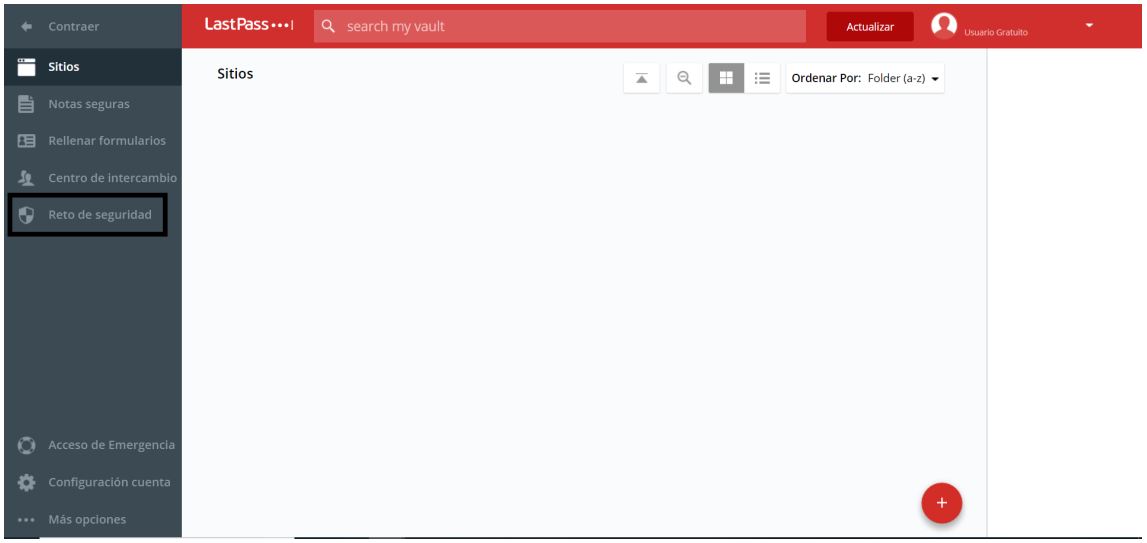

Figura 3: Localización del *Reto de seguridad*.

5. Ejercicios

A continuación, se describen los ejercicios a realizar en esta práctica.

5.1. Ejercicio 1

Imagina que trabajamos en una empresa y queremos hacer uso del gestor de contraseñas *LastPass*.

En primer lugar, cada estudiante deberá crearse un usuario junto con la contraseña maestra.

Nota: por motivos de seguridad, *LastPass* bloqueará el registro de tantas cuentas de usuario desde la misma IP, por lo tanto, se recomienda que cada estudiante use su teléfono móvil con su conexión de internet móvil y, entonces, utilice el ordenador para proseguir con la práctica.

- Haciendo uso del generador de contraseñas, genera 3 contraseñas **robustas**.
- Añade 3 nuevos sitios web en la aplicación y haz uso de ellos.
- Haciendo uso de los sitios anteriormente añadidos, realiza el reto de seguridad (véanse Figura 3 y Figura 4). Comenta aquellos resultados que te hayan resultado más llamativos.
- Comenta y explica brevemente, al menos, tres funcionalidades de LastPass que no hayas usado en esta práctica hasta el momento y que te parezcan

Figura 4: Iniciar el *Reto de seguridad*.

interesantes. Además, elige una de ellas, úsala y haz alguna captura de pantalla de su uso.

5.2. Ejercicio 2

Contesta a las siguientes preguntas:

- ¿Qué utilidad, desde el punto de vista de la seguridad, proporcionan los gestores de contraseñas?
- ¿Qué utilidad, desde el punto de vista malicioso, proporciona este tipo de aplicación?
- ¿Crees que este tipo de aplicación tiene todo lo necesario para generar y almacenar credenciales seguras? ¿Por qué?
- ¿Usarías en tu día a día un gestor de contraseñas? ¿Por qué?

6. Otros gestores de contraseñas

Existen muchos tipos de gestores de contraseñas. A continuación vamos a comparar los más conocidos.

6.1. Keepass

Keepass [3] es un administrador de contraseñas gratuito y de código abierto (véase Figura 5). Es oficialmente compatible con los sistemas operativos macOS y Linux

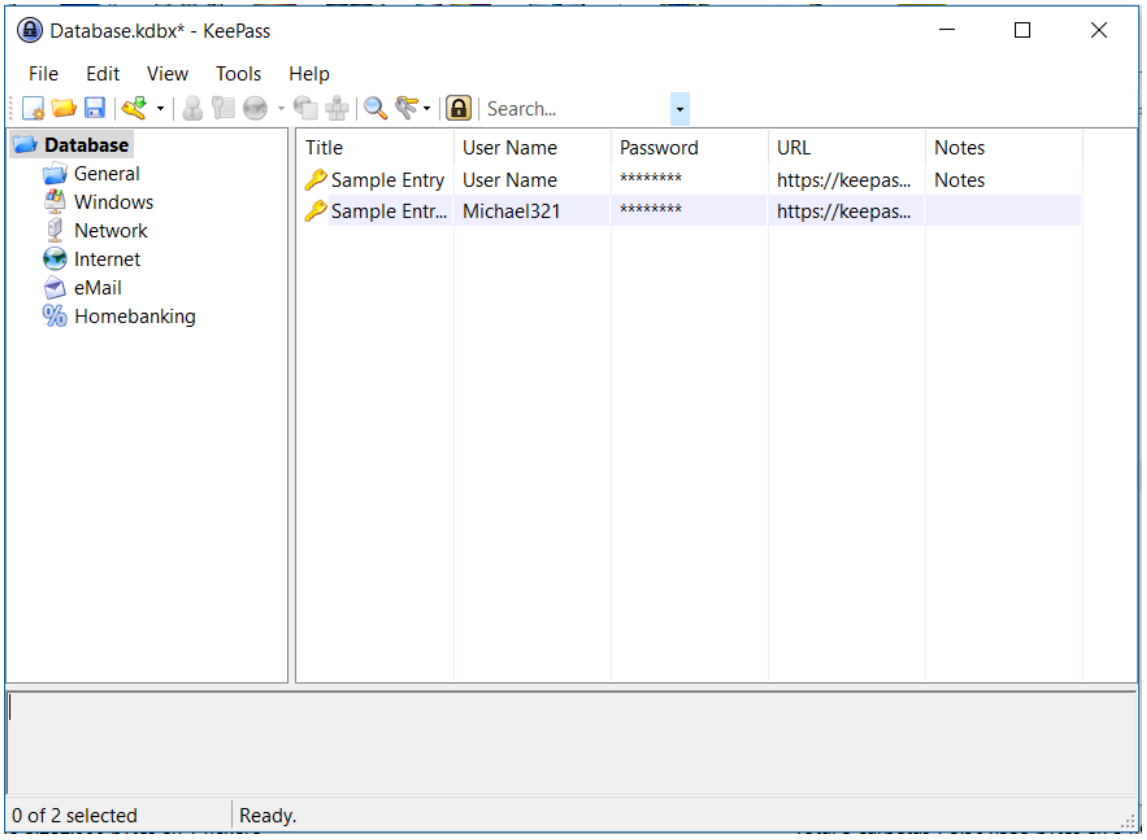

Figura 5: Interfaz de *KeePass*.

a través del uso de Mono. Existen varios puertos no oficiales para dispositivos con Android, iOS, Windows Phone y BlackBerry.

6.2. *TeamPass*

TeamPass [2] es un gestor de contraseñas colaborativo *open source* (véase Figura 6), que funciona bajo *PHP* y *MySQL*.

Entre sus características destacamos las siguientes: acceso único de usuario y roles [administrador, manager, usuario], y grupos de usuarios. Además de la contraseña, se puede utilizar un 2FA de Google.

Todas las contraseñas son cifradas con el algoritmo AES y podemos importar bases de datos desde *Keepass*.

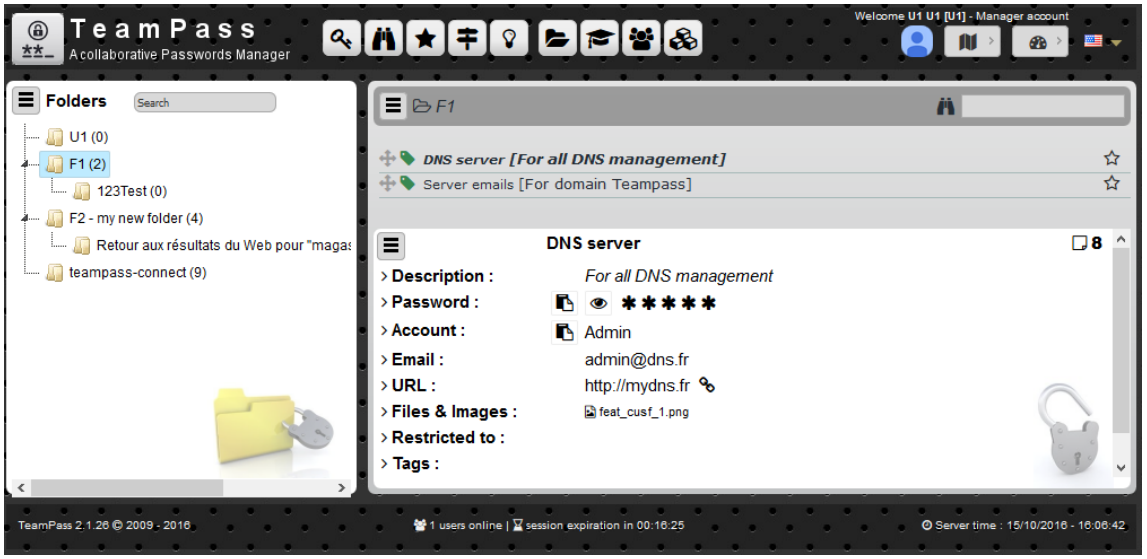

Figura 6: Interfaz de *TeamPass*.

6.3. SysPass

SysPass [4] es un gestor de contraseñas colaborativo *open source*, que también funciona bajo *PHP* y *MySQL*.

Tiene características similares a *TeamPass*: acceso único de usuario y roles [administrador, manager, usuario], y grupos de usuarios. También permite utilizar un 2FA de Google.

Todas las contraseñas son cifradas con el algoritmo AES y podemos importar bases de datos desde *Keepass*. Visualmente varía respecto a *TeamPass*, ya que *SysPass* utiliza *Material Design* [1] (véase Figura 7).

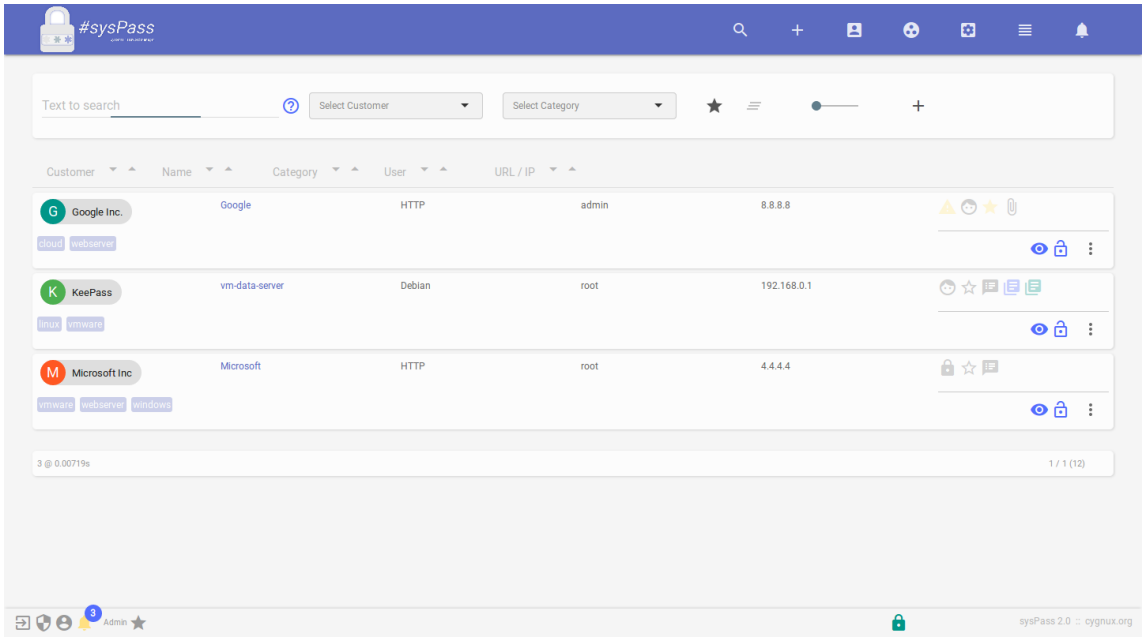

Figura 7: Interfaz de *SysPass*.

Referencias

[1] Apache: *Material Design*. `https://material.io/guidelines/`. [Última consulta: 2019-03-01].

[2] nilsteampassnet: *TeamPass - Collaborative Passwords Manager*. `https://github.com/nilsteampassnet/TeamPass`. [Última consulta: 2019-03-01].

[3] Dominik Reichl: *KeePass Password Safe*. `https://keepass.info/`. [Última consulta: 2019-03-01].

[4] uxsmin: *sysPass - Systems Password Manager*. `https://github.com/nuxsmin/sysPass`. [Última consulta: 2019-03-01].