CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	FireFoxrensics
Categoría	FORENSE
Dificultad	FÁCIL
Puntos	200

DESCRIPCIÓN DEL RETO

En este reto se ha guardado la contraseña para acceder a una determinada página web en un perfil de Firefox. Extraer dicho parámetro, así como la URL de la web para poder iniciar sesión y obtener la *flag*.

WRITEUP

1. Para este reto nos proporcionan el volcado de un perfil de Firefox, en este perfil se ha almacenado toda la información que el cliente ha buscado (historial, marcadores, credenciales, …).
2. Una vez identificado que se trata de un perfil de Firefox, lo más común es usar alguna herramienta para sacar las credenciales que estén almacenadas.
3. Para ello, utilizamos "firefox_decrypt" (https://github.com/unode/firefox_decrypt), que es una herramienta que permite extraer las contraseñas del perfil en texto plano.

---

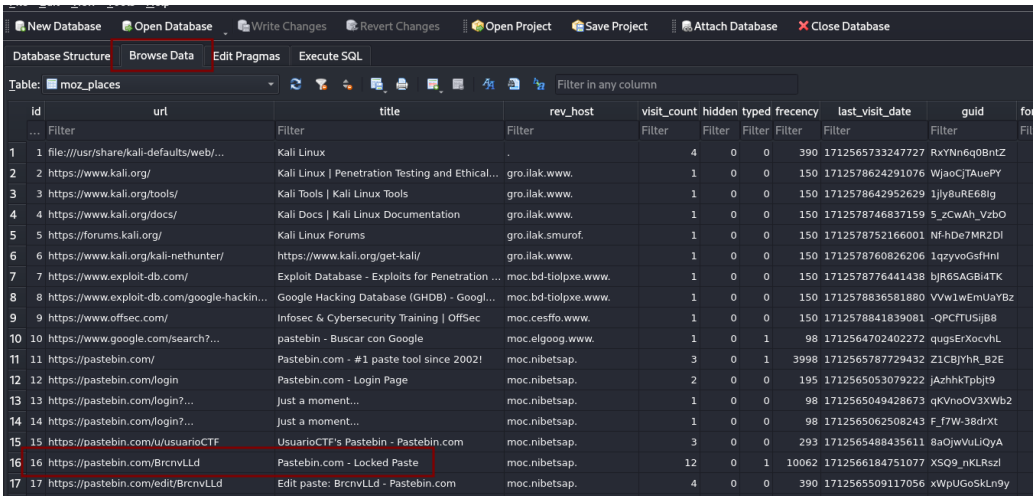
python3 firefox_decrypt

---

4. Seleccionamos el perfil de nuestro usuario, es decir, el que coincide con el nombre de la carpeta proporcionada:

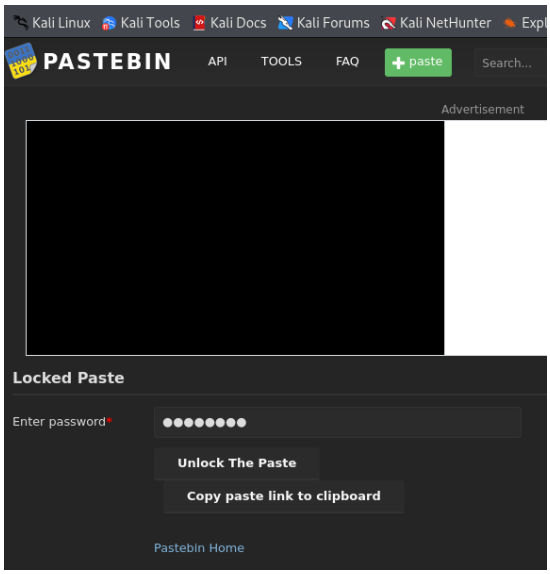
```
┌──(kali㉿kali)-[~/Downloads/firefox_decrypt]
└─$ python3 firefox_decrypt.py
Select the Mozilla profile you wish to decrypt
1 → cbay4ksb.CTFuser
2 → xc18vgvh.usuarioCTF
3 → ndx3tck0.default
4 → knpd1wun.default-esr
1

Website:   https://pastebin.com
Username: ''
Password: 'Tbv45haS'
```

5. Como respuesta, devuelve la contraseña y la web a la que esta pertenece. Sin embargo, vemos que no hay nombre de usuario por lo que no se puede acceder a ninguna cuenta.
6. Sabiendo que tenemos una contraseña que pertenece a pastebin pero sin ningún usuario, vamos a proceder a ver el historial de navegación, para ello existe una base de datos llamada “places.sqlite”.
7. Abrimos el archivo “places.sqlite” usando la herramienta “DB Browser for SQLite” (https://sqlitebrowser.org/), navegamos al apartado de “Browse Data” y buscamos una URL que pertenezca al dominio que necesitamos.



	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date	guid
1	1	file:///usr/share/kali-defaults/web/...	Kali Linux	.	4	0	0	390	1712565733247727	RxYNn6q0BntZ
2	2	https://www.kali.org/	Kali Linux | Penetration Testing and Ethical...	gro.ilak.www.	1	0	0	150	1712578624291076	WjaoCjTAuePY
3	3	https://www.kali.org/tools/	Kali Tools | Kali Linux Tools	gro.ilak.www.	1	0	0	150	1712578642952629	1jly8uRE68Ig
4	4	https://www.kali.org/docs/	Kali Docs | Kali Linux Documentation	gro.ilak.www.	1	0	0	150	1712578746837159	5_zCwAh_VzbO
5	5	https://forums.kali.org/	Kali Linux Forums	gro.ilak.smurof.	1	0	0	150	1712578752166001	Nf-hDe7MR2Dl
6	6	https://www.kali.org/kali-nethunter/	https://www.kali.org/get-kali/	gro.ilak.www.	1	0	0	150	1712578760826206	1qzyvoGsfHnI
7	7	https://www.exploit-db.com/	Exploit Database - Exploits for Penetration ...	moc.bd-tiolpxe.www.	1	0	0	150	1712578776441438	bJR6SAGBi4TK
8	8	https://www.exploit-db.com/google-hackin...	Google Hacking Database (GHDB) - Googl...	moc.bd-tiolpxe.www.	1	0	0	150	1712578836581880	VVw1wEmUaYBz
9	9	https://www.offsec.com/	Infosec & Cybersecurity Training | OffSec	moc.cesffo.www.	1	0	0	150	1712578841839081	-QPCfTUSijB8
10	10	https://www.google.com/search?...	pastebin - Buscar con Google	moc.elgoog.www.	1	0	1	98	1712564702402272	qugsErXocvhL
11	11	https://pastebin.com/	Pastebin.com - #1 paste tool since 2002!	moc.nibetsap.	3	0	1	3998	1712565787729432	Z1CBJYhR_B2E
12	12	https://pastebin.com/login	Pastebin.com - Login Page	moc.nibetsap.	2	0	0	195	1712565053079222	jAzhhkTpbjt9
13	13	https://pastebin.com/login?...	Just a moment...	moc.nibetsap.	1	0	0	98	1712565049428673	qKVnoOV3XWb2
14	14	https://pastebin.com/login?...	Just a moment...	moc.nibetsap.	1	0	0	98	1712565062508243	F_f7W-38drXt
15	15	https://pastebin.com/u/usuarioCTF	UsuarioCTF's Pastebin - Pastebin.com	moc.nibetsap.	3	0	0	293	1712565488435611	8aOjwVuLiQyA
16	16	https://pastebin.com/BrcnvLLd	Pastebin.com - Locked Paste	moc.nibetsap.	12	0	1	10062	1712566184751077	XSQ9_nKLRszl
17	17	https://pastebin.com/edit/BrcnvLLd	Edit paste: BrcnvLLd - Pastebin.com	moc.nibetsap.	4	0	0	390	1712565509117056	xWpUGoSkLn9y

8. En el historial encontramos la URL (https://pastebin.com/BrcnvLLd), así que accedemos y verificamos que la contraseña que hemos encontrado es la contraseña de este post.



9. Al acceder, encontramos un post con la *flag*:

CTF

USUARIOCTF MAR 21ST, 2024 (EDITED) 15 0 NEVER

text 0.06 KB | None

```
1. CTF flag: UGR_ETSIIT_CTF24{F1r3f0x_3xp0s3_Y0ur_Cr3d3nt141s}
```