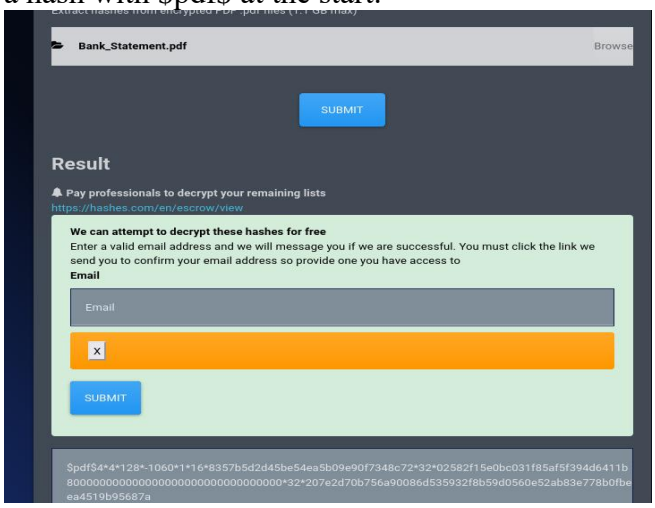
THE SILENT GUARDIAN

The challenge provides a password-protected PDF file, Bank_Statement.pdf. The goal is to bypass the password protection, extract the contents, and find the hidden flag.

PDFs use encryption that can be represented as a hash so I tried uploading the given pdf file to this site https://hashes.com/en/johntheripper/pdf2john now that I didn't have the pdf2john tool installed on my linux machine

Also this way seemed faster to me at the time. The upload was a hit as the output was a hash with pdf at the start.



I then copied the hash that was given and saved it in a hash.txt file

```
┌──(spike㉿SPIKE)-[~/Downloads]
└─$ hashcat hash.txt rockyou.txt -r /usr/share/hashcat/rules/best64.rule --sessi
on=pdf_ctf --show

hash.txt: Byte Order Mark (BOM) was detected
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

10500 | PDF 1.4 - 1.6 (Acrobat 5 - 8) | Document

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$pdf$4*4*128*-1060*1*16*8357b5d2d45be54ea5b09e90f7348c72*32*02582f15e0bc031f85af
5f394d6411b8000000000000000000000000000000*32*207e2d70b756a90086d535932f8b59d0
560e52ab83e778b0fbeea4519b95687a:037982
```

I then ran the hashcat command against the hash.txt file and my rockyou.txt wordlist

I also added the base64 rule which mutates the words from the list, included the pdf_ctf to save the session state incase I had an error and the show command to give me the displays of passwords if found

It hit and the password was displayed: ***037982*** booyah almost done

I then used the qpdf tool to manipulate my encrypted file gave it the retrieved password and the name of the file. The contents were to be saved in another file unlocked.pdf

I ran ls to confirm the creation of the file without any errors

```
┌──(spike㉿SPIKE)-[~/Downloads]
└─$ qpdf --password=037982 --decrypt Bank_Statement.pdf unlocked.pdf


┌──(spike㉿SPIKE)-[~/Downloads]
└─$ ls
activity-hijack     Downloads-backup   rockyou.txt   WhiteSur-gtk-theme
android-14          hash.txt           steg-env
Bank_Statement.pdf  LSB-Steganography  unlocked.pdf
```

Used the pdftotext with the new file and grep command given we know the flag format had to contain at least one of these and booyah the flag displayed in plain text

```
┌──(spike㉿SPIKE)-[~/Downloads]
└─$ pdftotext unlocked.pdf - | egrep -i 'flag\{|inm|CTF|flag'

Remember flag{inm_free_bank_to_mpesa_transactions}
```