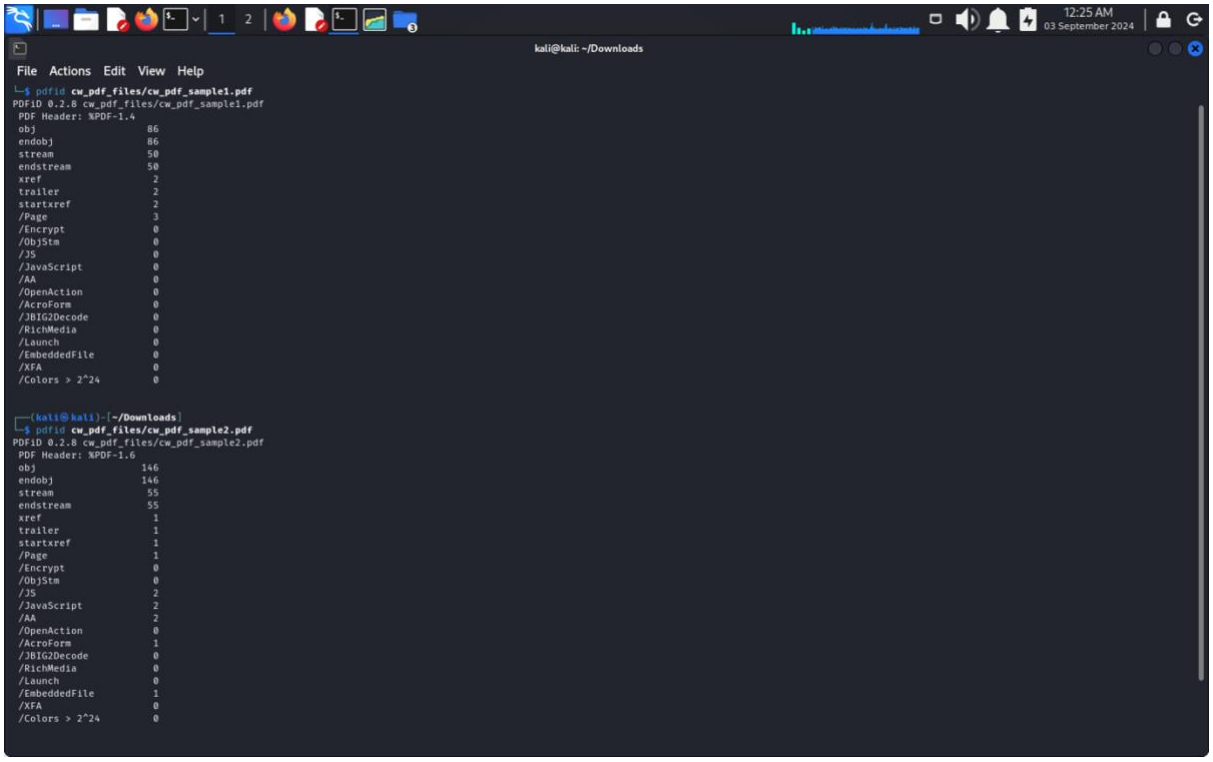
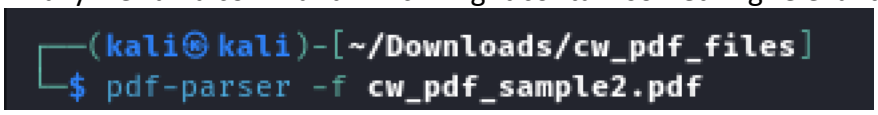
Umer Farooq i220518 CY-A

We open the file given using pdfid.
We see that only that the second file contains javascript and embedded file which could be possible ways for malicious content to enter.



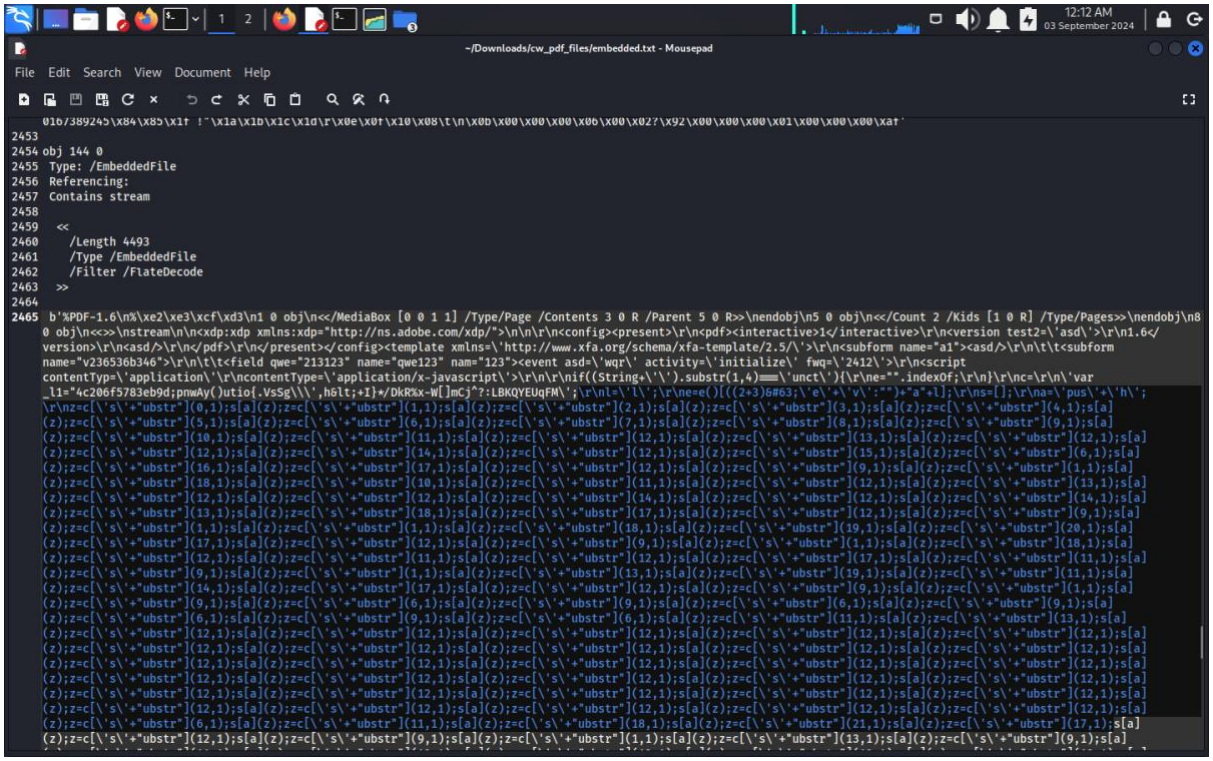
Thus we begin scanning the 2nd pdf. First searching for /JS and /Names we find no leads.

Finally we run.a command which might contain something relevant.



so I redirect the output in a file.

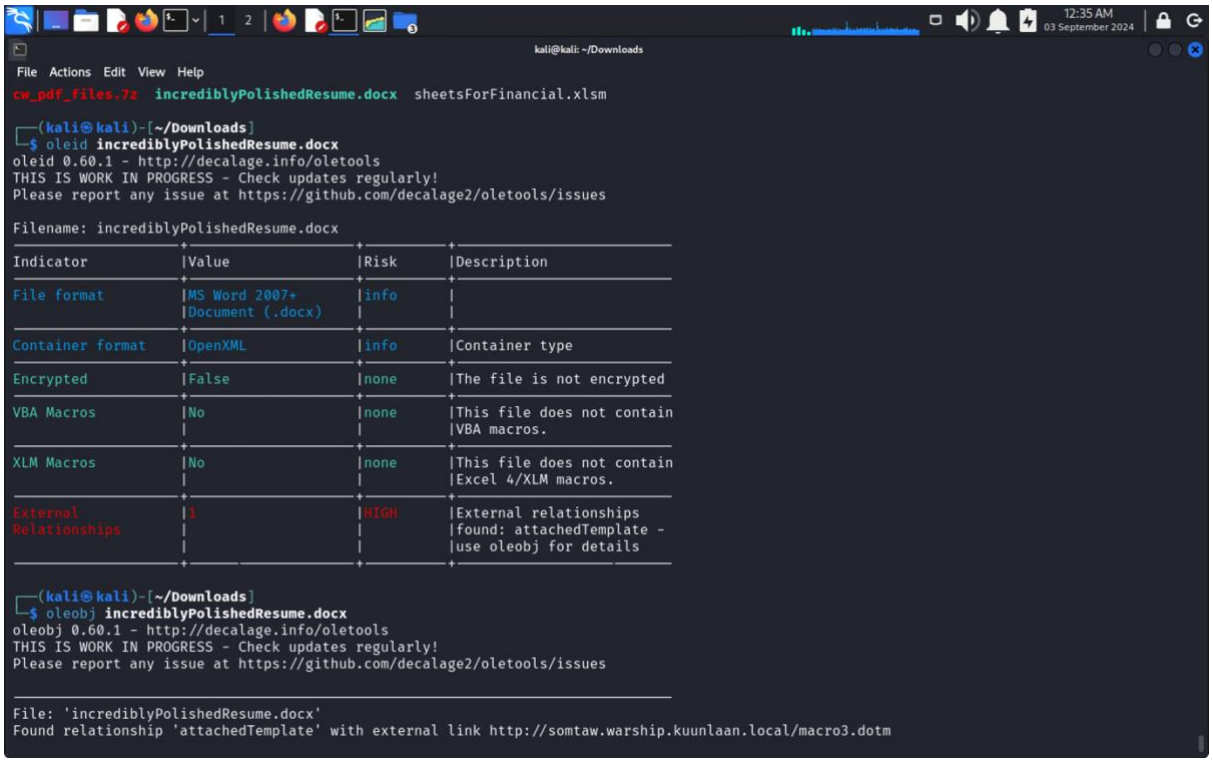
Skimming through the file I see some possibly obfuscated code.



This might contain the javascript code that is malicious.

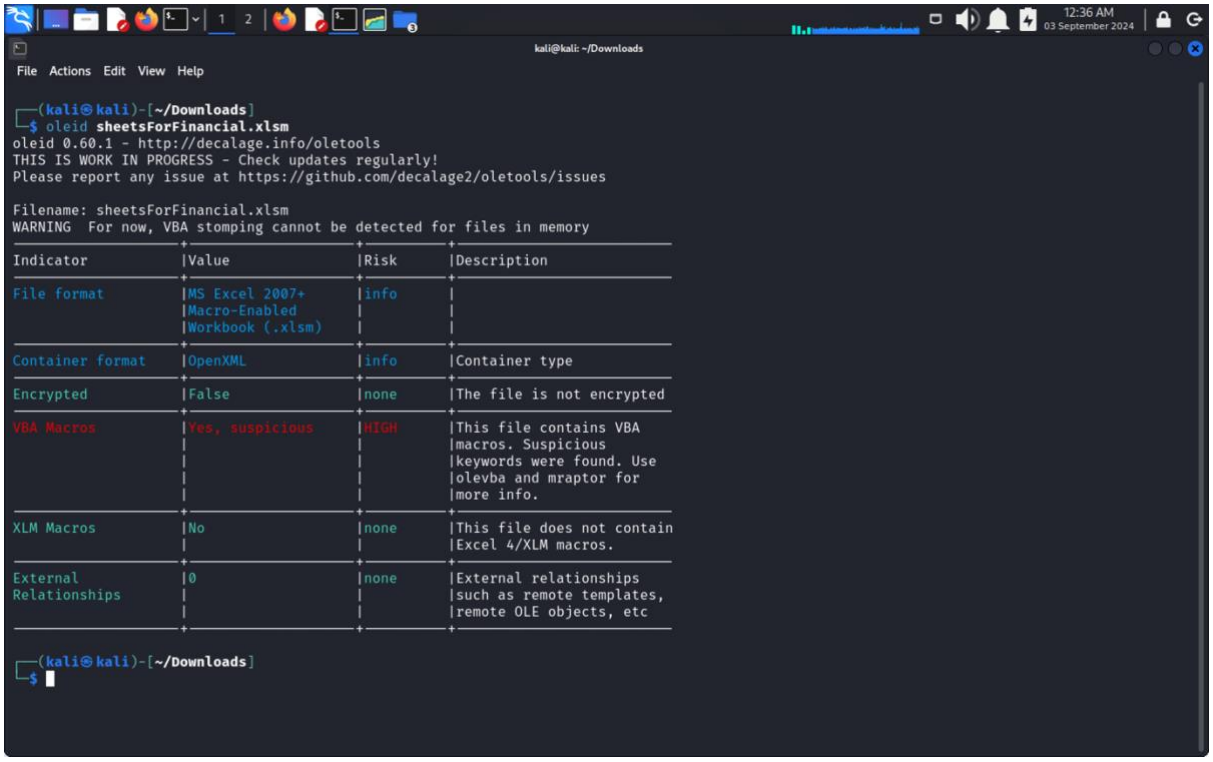
Task 2:

Scanning the first docx file we see that It contains external entities. Using the oleobj tool we see the external link it references.



At the bottom we can see the link.

The second file we use the same oleid tool again.



We see it contains malicious macros.

Running olevba and mraptor for more info.