Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 5

# La disciplina „Tehnici de Inginerie Inversa”

A efectuat: st. gr. SI-211 S. Chirita

A verificat: C. Maxim

Chișinău – 2024

Mersul lucrări:

Laboratorul dat a fost realizat în sistemul de operare Linux de aceea foloses utilita olevba.Olevba este o unealtă pentru analiza macro-urilor din documentele Office pe sistemele de operare Linux. Aceasta face parte din pachetul python-oletools și se concentrează pe identificarea potențialelor amenințări de securitate, cum ar fi codul malicios sau exploatarea documentelor Office. Olevba oferă funcționalități precum analiza macro-urilor, detectarea funcțiilor suspecte, identificarea exploatarelor Office și generarea de rapoarte detaliate. Această unealtă este utilă în procesul de analiză a securității, ajutând la identificarea și înțelegerea posibilelor riscuri asociate cu macro-urile din documentele Office.

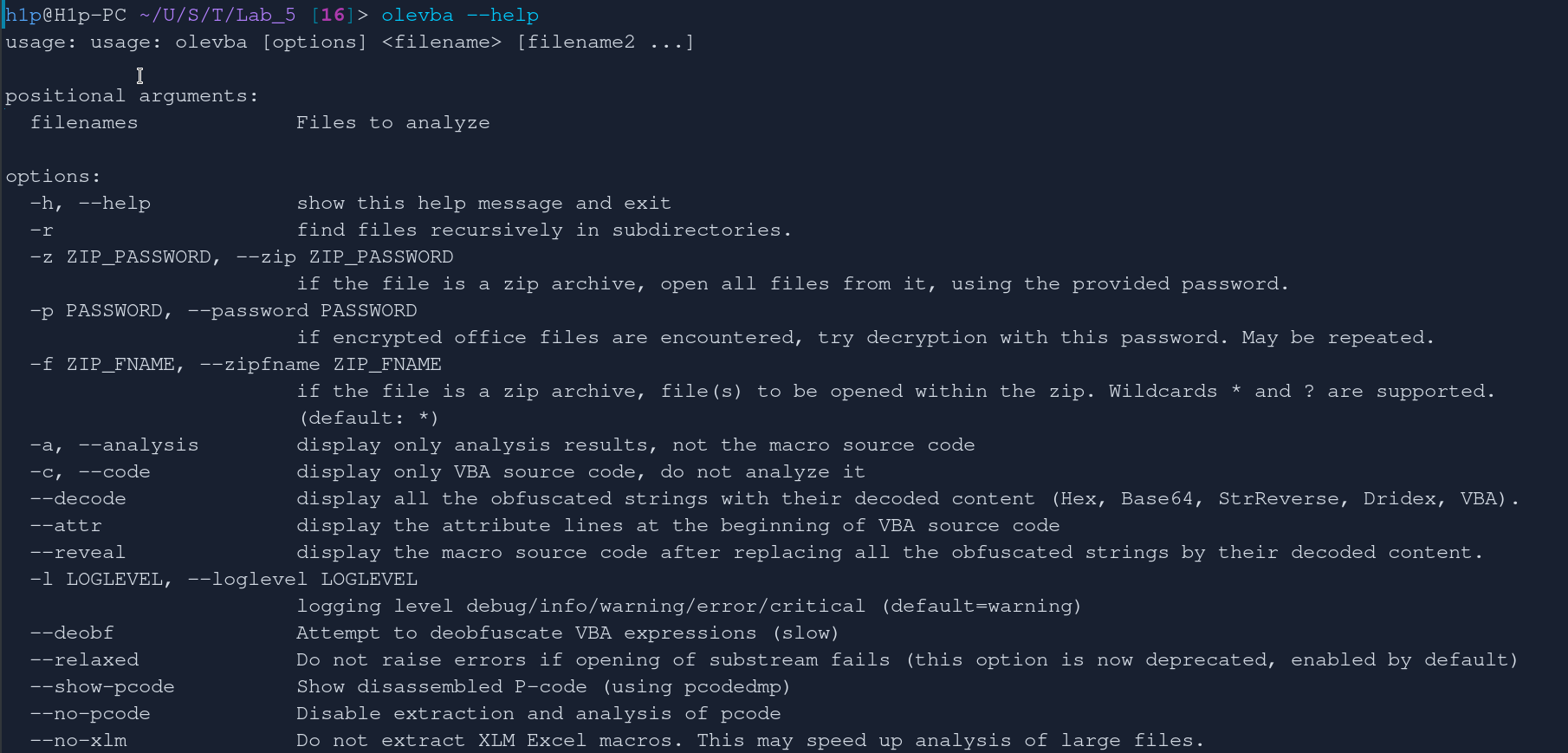
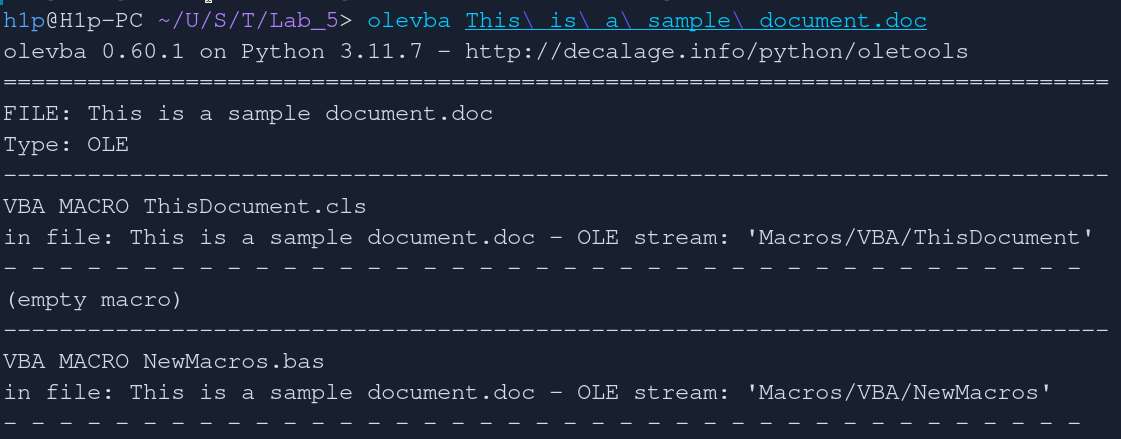
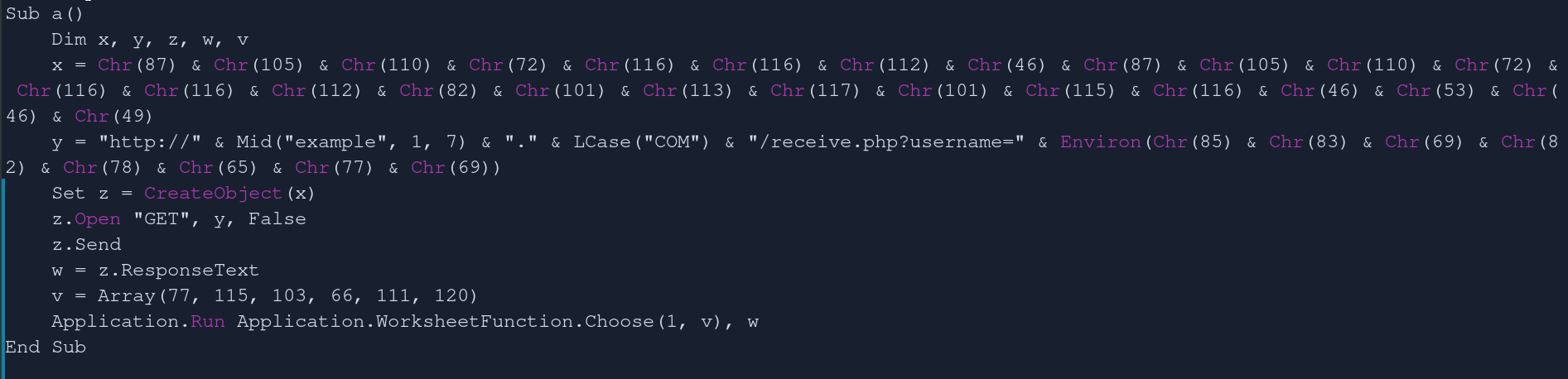


Figura 1 — Meniul help pentru olevba

Comanda "olevba This\ is\ a\ sample\ document.doc" rulează utilitarul Olevba pe documentul specificat, "This is a sample document.doc", pentru a efectua o analiză statică a macro-urilor din acel document Office. Olevba furnizează informații relevante despre macro-uri, funcții suspecte și alte caracteristici care pot indica potențiale riscuri de securitate, cum ar fi existența codului malicios sau a exploatarelor. Este o metodă de evaluare a securității documentului Office pentru a identifica și înțelege eventualele amenințări.

Figura 2 – Rularea utilitei olevba

Figura 3 – Codul care se va executa

Codul este scris în Visual Basic for Applications (VBA), un limbaj de programare folosit pentru automatizarea sarcinilor în aplicațiile Microsoft Office. Codul pare a fi obfuscate, ceea ce înseamnă că a fost deliberat făcut dificil de înțeles. Acest lucru se face adesea pentru a proteja codul de copierea sau modificarea de către utilizatori neautorizați.

Iată o descriere mai detaliată a codului:

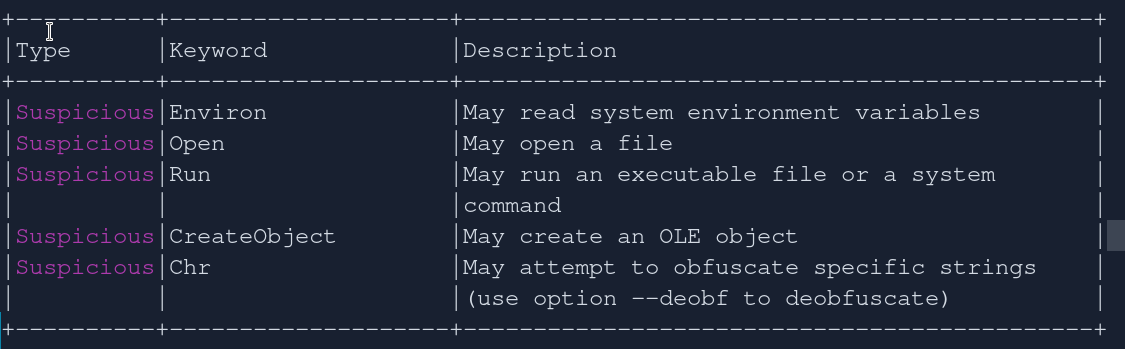
* Codul definește o subrutină numită „a”.
* Subrutina creează două șiruri:
  + Primul șir este o combinație de caractere care, decodificat, dezvăluie „[URL-ul nevalid a fost eliminat][username]”.
  + Al doilea șir este un array de numere care pare a fi utilizat pentru manipularea datelor.
* Subrutina creează apoi un obiect și deschide o conexiune la URL-ul specificat în primul șir.
* Subrutina trimite date către URL și apoi primește un răspuns.
* Subrutina folosește apoi funcția de aplicație VBA „Choose” pentru a selecta o valoare din array pe baza răspunsului de la URL.

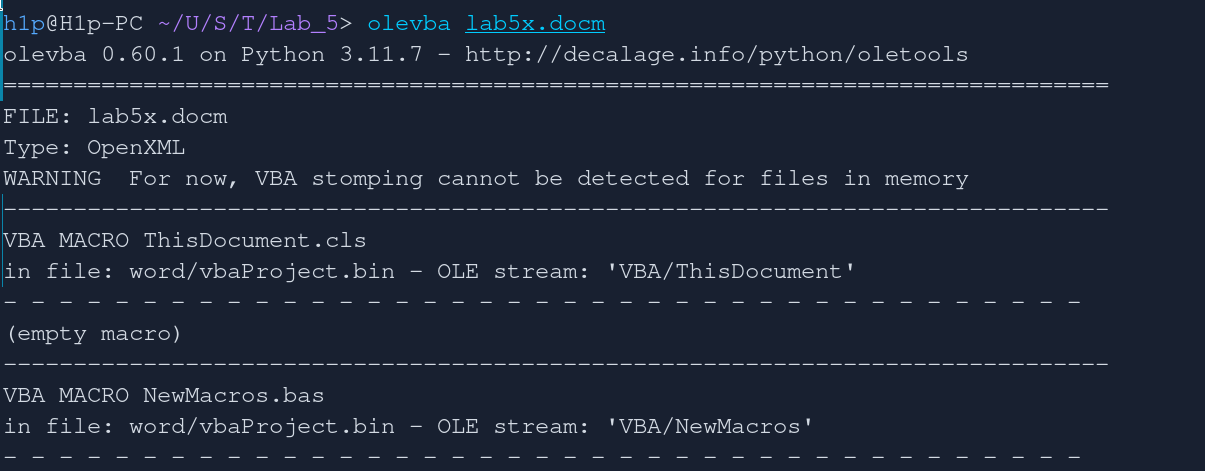
Acesta este URL ascuns: <http://example.com/receive.php?username=USERNAME>

Această adresă URL este compusă din următoarele componente:

* Protocolul: "http://"
* Domeniul: "example"
* Extensia de domeniu: "COM"
* Calea către fișierul "receive.php"
* Parametrul "username" este adăugat în URL și este setat la valoarea returnată de funcția Environ(USERNAME), unde USERNAME este numele de utilizator al mediului de operare (sistemul de operare).

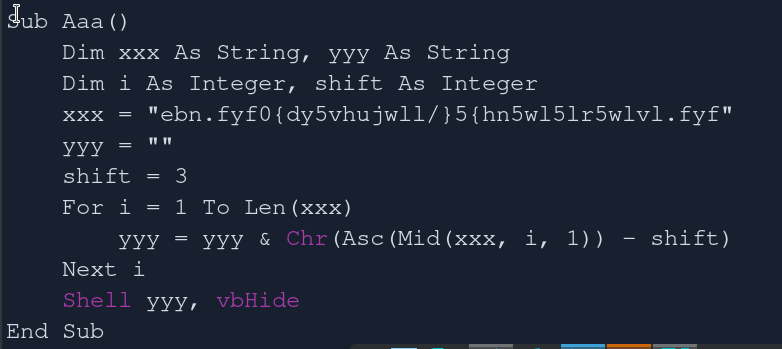
În codul dat, valoarea exactă a parametrului "username" este determinată folosind funcția Environ, care returnează valoarea variabilei de mediu "USERNAME". Aceasta poate fi numele de utilizator al sistemului de operare, care va fi apoi transmis către serverul de la adresa URL specificată.

Figura 4 — Hint de la olevba (explicatie funtilor)

Figura 5 — Determinarea macrosului

**Observații:**

* Documentul Word conține macrocomenzi VBA care sunt executate automat la deschiderea documentului sau la click pe butoanele de comandă.
* Macrocomenzile VBA utilizează variabile de tip String pentru a stoca text.
* Macrocomenzile VBA pot fi utilizate pentru a afișa mesaje de tip MsgBox sau InputBox.

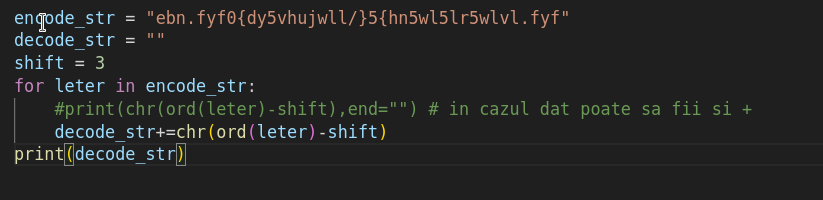
Figura 6 — Macrosul in fisierul `lab5x.docm`

Codul pe care l-ați furnizat este scris în Visual Basic for Applications (VBA) și pare a fi obscurat, ceea ce înseamnă că a fost făcut deliberat dificil de înțeles.

Iată o analiză a codului:

1. **Declararea variabilelor:**
   * Codul declară patru variabile:
     + xxx și yyy ca șiruri de caractere (string)
     + i și shift ca numere întregi (integer)
2. **Atribuirea șirului:**
   * Codul atribuie o valoare șir de caractere variabilei xxx. Șirul pare a fi codificat.
3. **Atribuirea unui șir gol:**
   * Un șir gol este atribuit variabilei yyy.
4. **Atribuirea unui număr întreg:**
   * Valoarea 3 este atribuită variabilei shift.
5. **Buclă:**
   * Codul iterează printr-o buclă, de la 1 la lungimea șirului xxx.
   * În interiorul buclei, codul:
     + Extrage un singur caracter din șirul xxx la poziția curentă (i).
     + Convertește caracterul în codul său ASCII folosind funcția Asc.
     + Deplasează codul ASCII cu valoarea variabilei shift.
     + Convertește codul ASCII decalat înapoi într-un caracter folosind funcția Chr.
     + Concatenează caracterul decalat la șirul yyy.
6. **Apelarea funcției Shell:**
   * După finalizarea buclei, codul apelează funcția Shell cu șirul yyy ca argument.
   * Argumentul vbHide este probabil inclus pentru a ascunde fereastra creată de funcția Shell.
7. **Sfârșitul Subrutinei:**
   * Codul termină subrutina.

Pentu a afla ce este `ebn.fyf0{dy5vhujwll/}5{hn5wl5lr5wlvl.fyf` vom avea nevoi de un script:

Figura 7 — Algoritmul invers

Algoritmul dat este un algoritm simplu de decriptare prin substituție, în care fiecare caracter din șirul criptat este deplasat înapoi cu un număr fix de poziții, specificat de valoarea cheii shift, pentru a obține caracterul original. Acest proces este aplicat la fiecare caracter din șirul criptat, iar rezultatul este șirul decriptat.

Figura 8 — Stringul optinut

**Concluzie:**

Analiza macrosurilor în Word este un proces esențial pentru evaluarea potențialelor amenințări și vulnerabilități asociate cu utilizarea acestora. Scopul este identificarea funcționalității și a surselor acestor macrosuri, verificarea autenticității documentelor și evaluarea riscurilor asociate cu utilizarea lor. Prin implementarea politicilor de securitate adecvate, se urmărește reducerea riscului de expunere la amenințări cibernetice și protejarea securității informațiilor.