

SECURE CODING CSE-2010

LAB-7

Name - Vishal Dung Dung

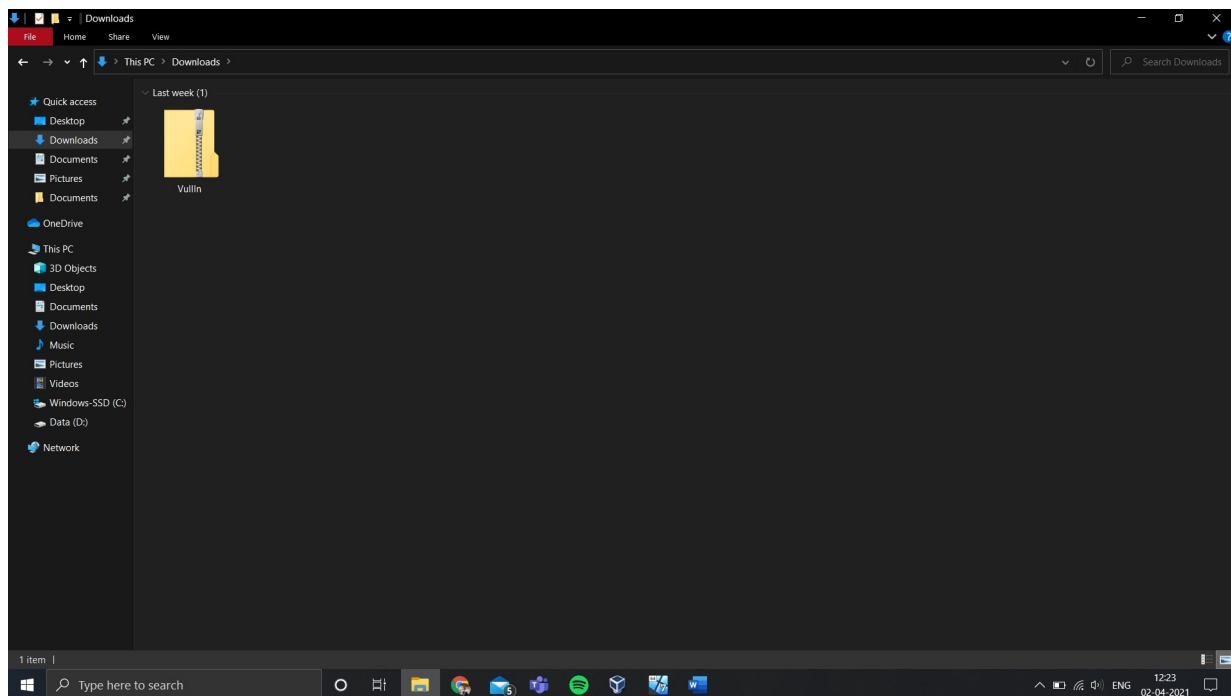
Reg no - 18BCN7053

Slot - L23-L24

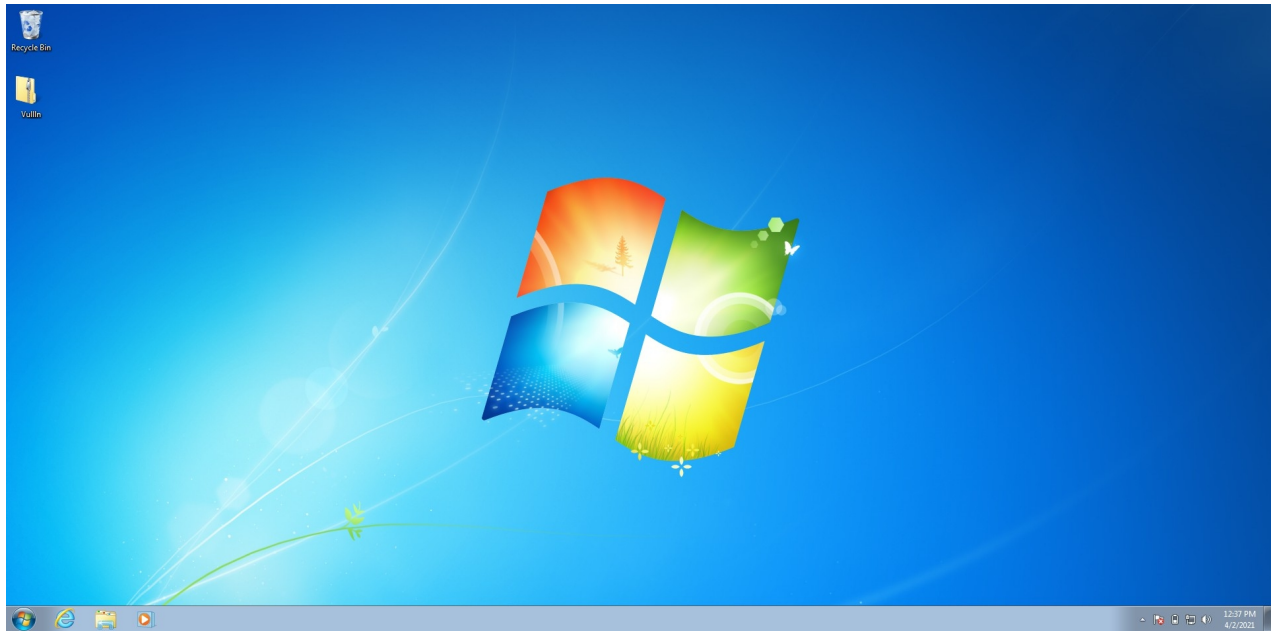
Working with the memory vulnerabilities

TASKS :

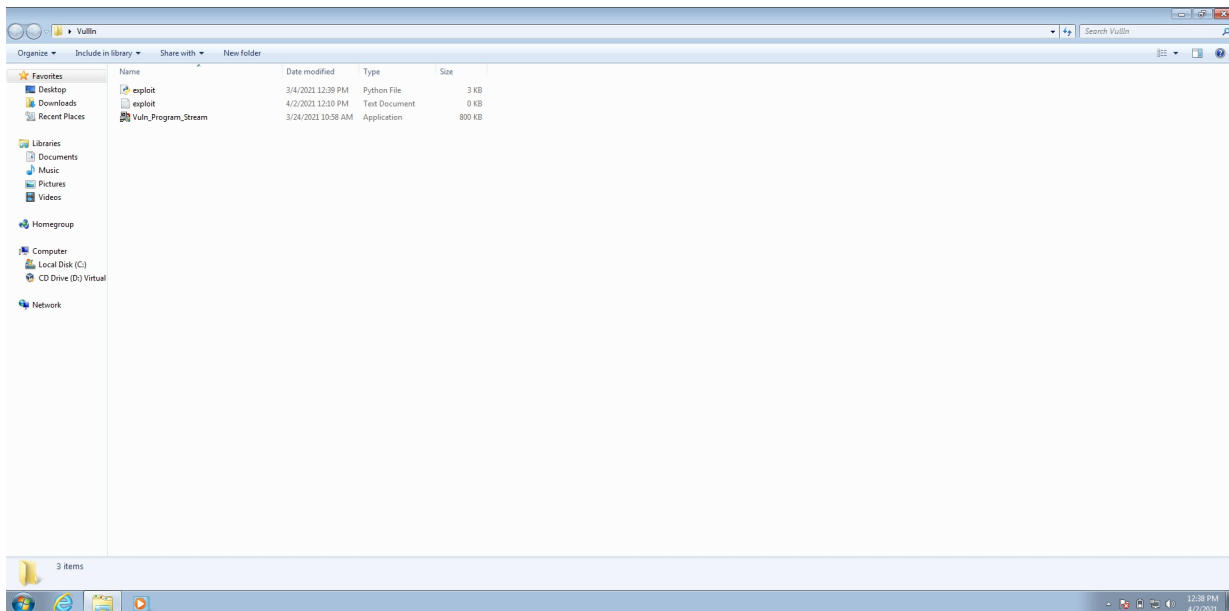
Download Vulln.zip from teams.



- **Deploy a virtual windows 7 instance and copy the Vuln.zip into it.**



- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**



The screenshot shows the Python Software Foundation website for the 2.7.0 release. The browser's address bar shows the URL `https://www.python.org/download/releases/2.7/`. The page content includes a list of links for more information, a 'Download' section with a warning about production releases, and a list of supported download formats. A Windows security warning dialog is overlaid on the bottom, asking if the user wants to run or save a file named `python-2.7.msi` (15.1 MB).

https://www.python.org/download/releases/2.7/

Python Software Foundation [US] Search...

MSN India | Breaking News, En... Python 2.7.0 Release | Pyth...

- What's new in 2.7?
- Change log for this release.
- Online Documentation
- Report bugs at <http://bugs.python.org>.
- Help fund Python and its community.

Download

This is a production release. Please report [any bugs](#) you encounter.

We currently support these formats for download:

- Gzipped source tar ball (2.7.0) (sig)
- Bzipped source tar ball (2.7.0) (sig)
- Windows x86 MSI Installer (2.7.0) (1) (sig)
- Windows X86-64 MSI Installer (2.7.0) (1) (sig)
- Mac installer disk image (2.7.0) for OS X 10.5 and later (sig). It contains code for PPC, i386, and x86-64.
- 32-bit Mac installer disk image (2.7.0) for OS X 10.3 and later (sig).
- Windows help file (sig)

The source tarballs are signed with Benjamin Peterson's key (fingerprint: 12EF 3DC3 8047 DA38 2D18 A589 99CD EA80 A413 5B38). The Windows installer was signed by Martin von Lowis' public key, which has a key id of 7D9DC8D2. The Mac installers were signed with Ronald Oussoren's key, which has a key id of E6DF025C. The public keys are located on the [download page](#).

MD5 checksums and sizes of the released files:

```

35F5C46972...F19af3d5046C6E123...dF-14826384 Python-2.7.0-...

```

Do you want to run or save **python-2.7.msi** (15.1 MB) from **python.org**?

⚠ This type of file could harm your computer.

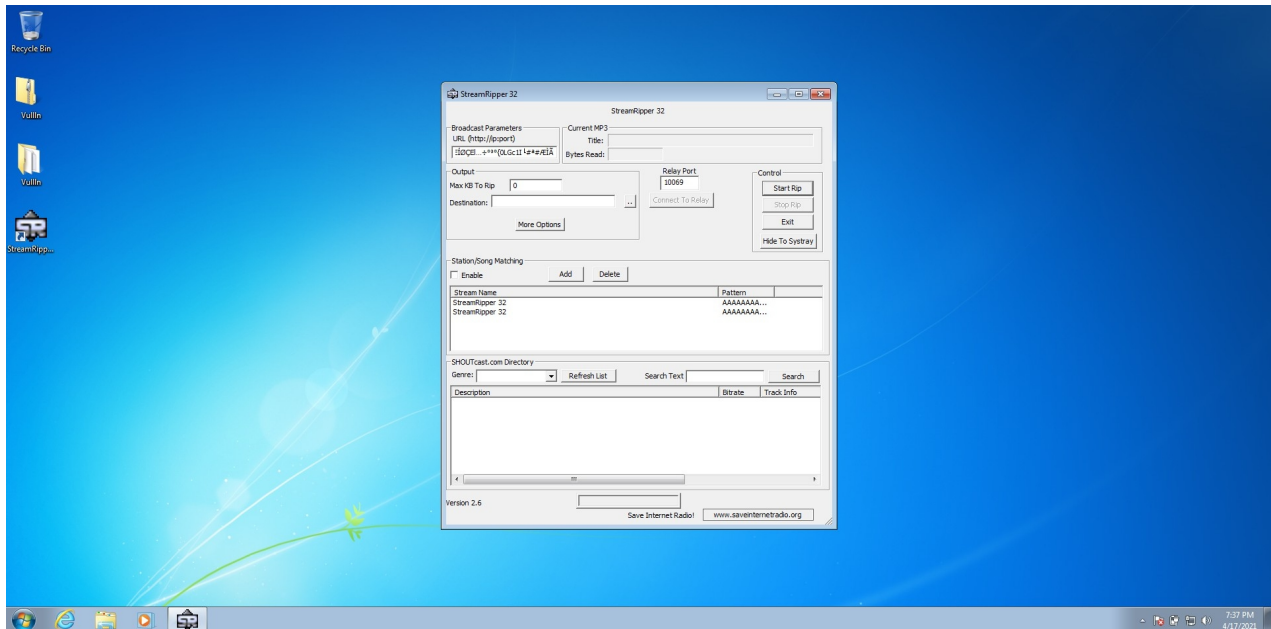
Run Save Cancel

12:39 PM 4/2/2002

[illegible]

-

Copy paste the generated payload in different text fields of stream ripper to check for the vulnerabilities



Vulnerability found-

