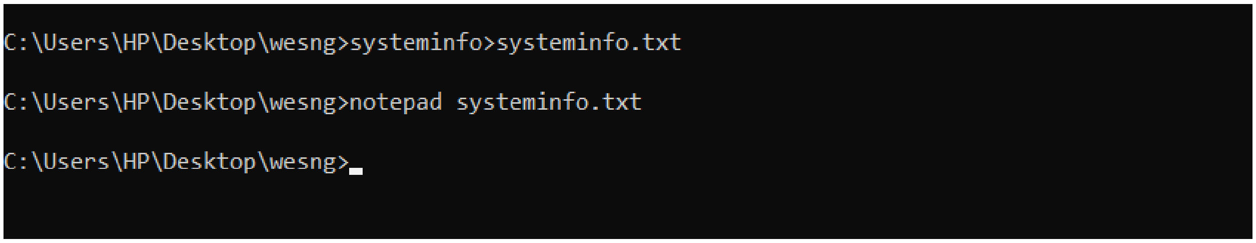
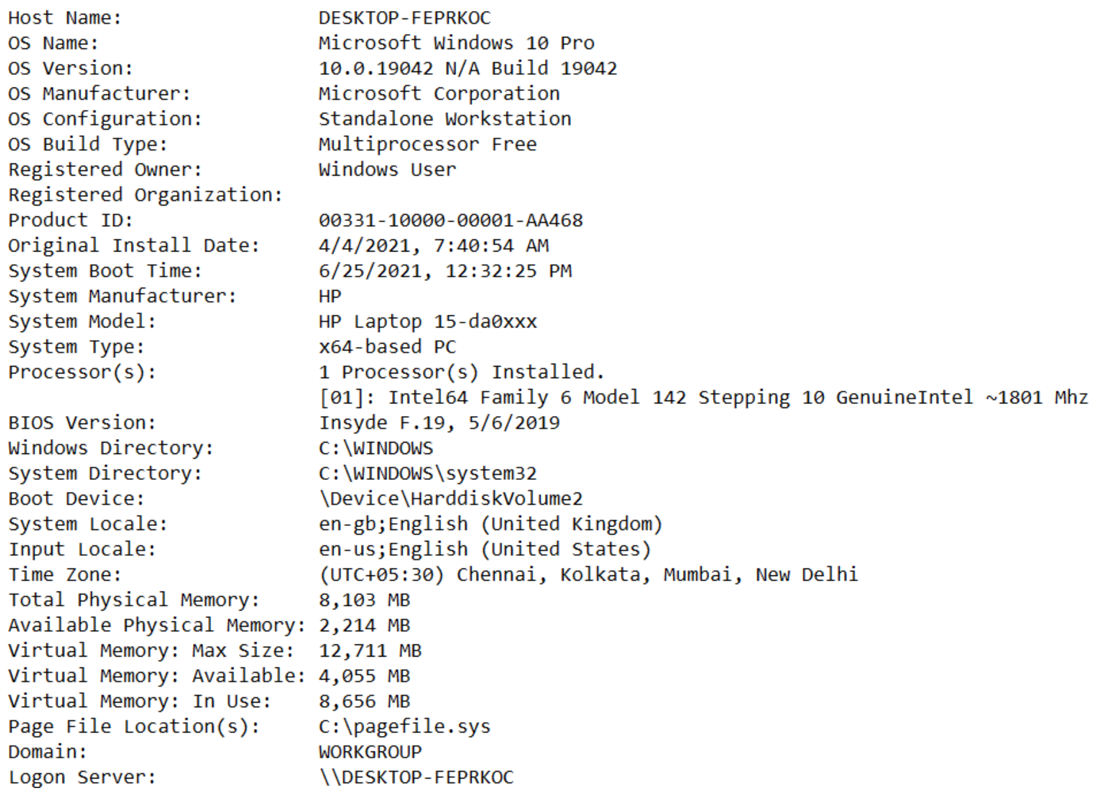
Secure Coding Lab Assignment-13

Varun Parikh
19BCE7202

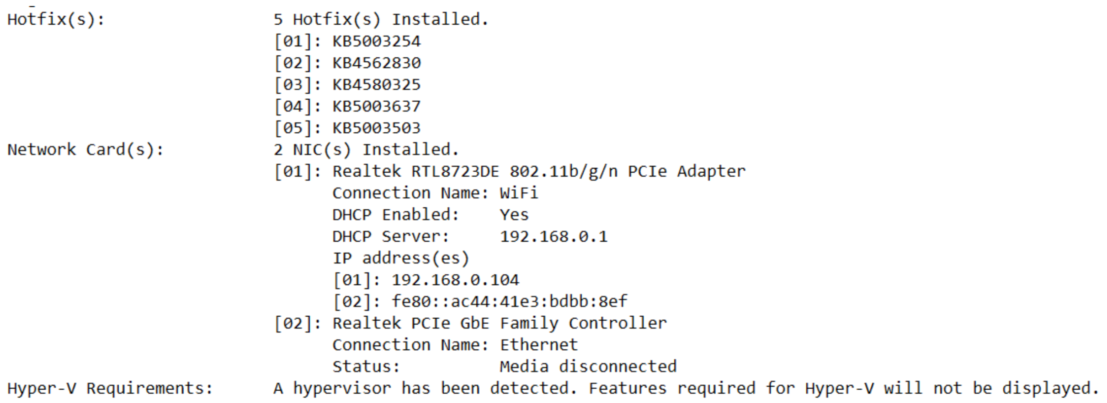
Creating systeminfo.txt file



```
C:\Users\HP\Desktop\wesng>systeminfo>systeminfo.txt

C:\Users\HP\Desktop\wesng>notepad systeminfo.txt

C:\Users\HP\Desktop\wesng>_
```



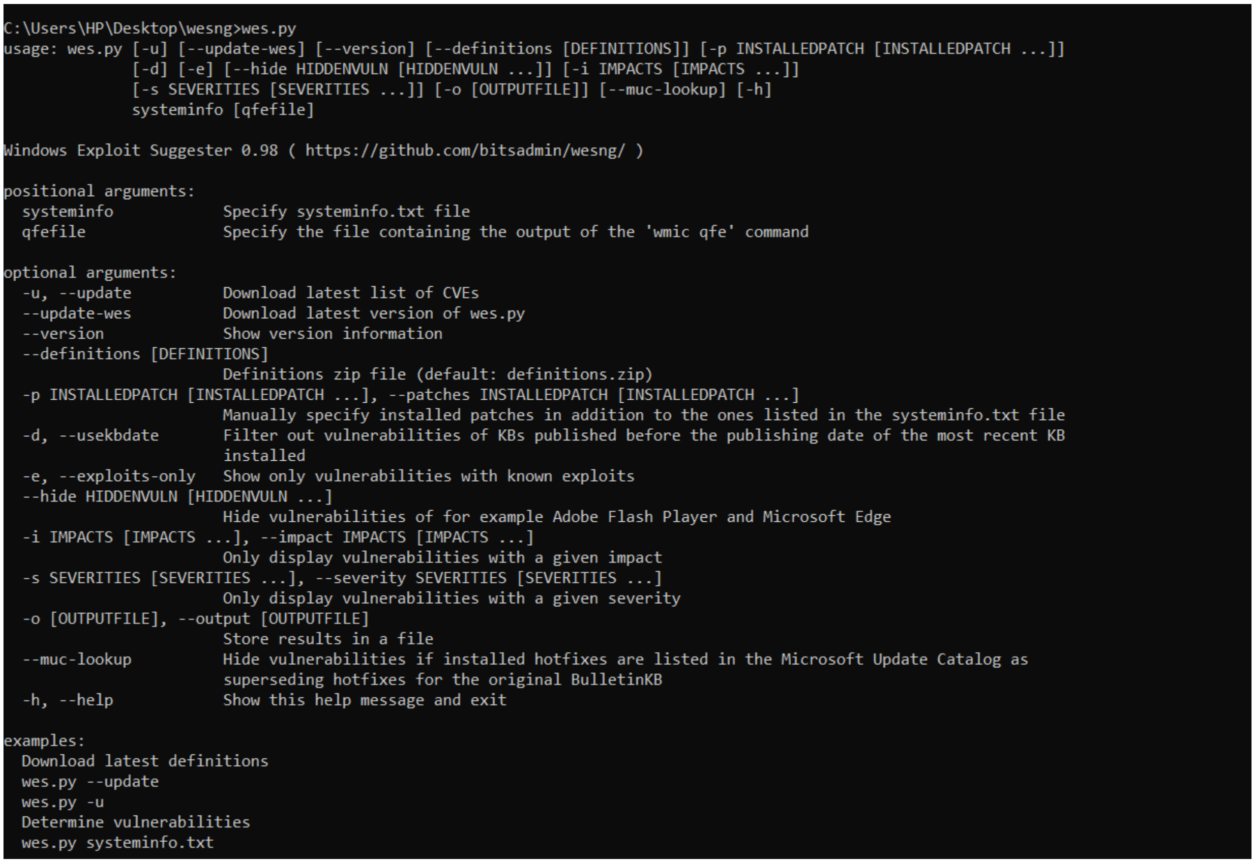
```
Host Name:                 DESKTOP-FEPRKOC
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00331-10000-00001-AA468
Original Install Date:     4/4/2021, 7:40:54 AM
System Boot Time:          6/25/2021, 12:32:25 PM
System Manufacturer:       HP
System Model:              HP Laptop 15-da0xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1801 Mhz
BIOS Version:              Insyde F.19, 5/6/2019
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,103 MB
Available Physical Memory: 2,214 MB
Virtual Memory: Max Size:  12,711 MB
Virtual Memory: Available: 4,055 MB
Virtual Memory: In Use:    8,656 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\DESKTOP-FEPRKOC
```



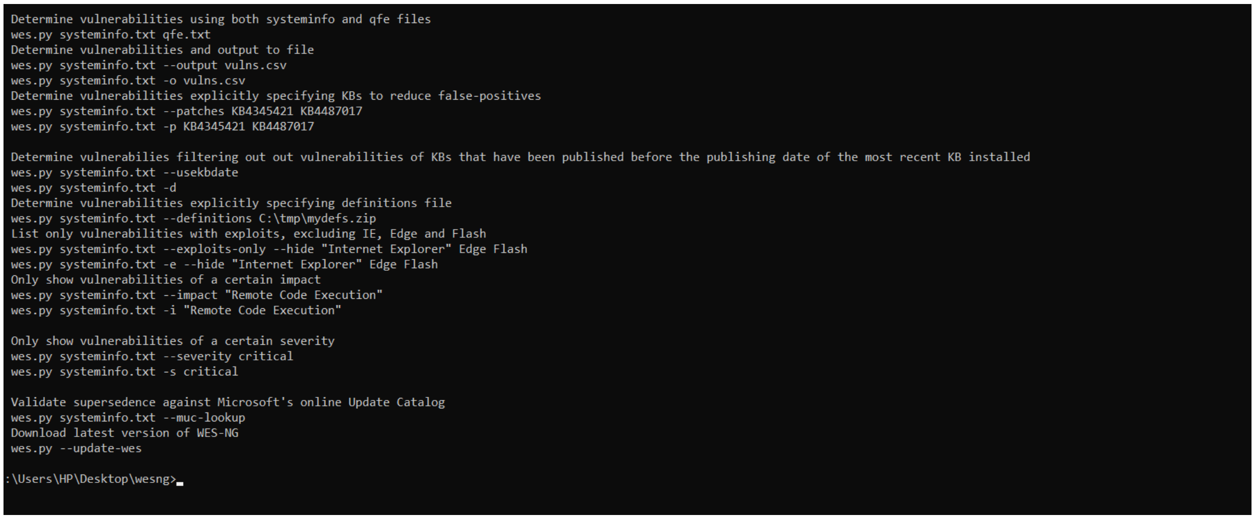
```
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5003254
                           [02]: KB4562830
                           [03]: KB4580325
                           [04]: KB5003637
                           [05]: KB5003503
Network Card(s):           2 NIC(s) Installed.
                           [01]: Realtek RTL8723DE 802.11b/g/n PCIe Adapter
                                 Connection Name: WiFi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.0.1
                                 IP address(es)
                                 [01]: 192.168.0.104
                                 [02]: fe80::ac44:41e3:bdbb:8ef
                           [02]: Realtek PCIe GbE Family Controller
                                 Connection Name: Ethernet
                                 Status:          Media disconnected
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

Wesng

>>wes.py

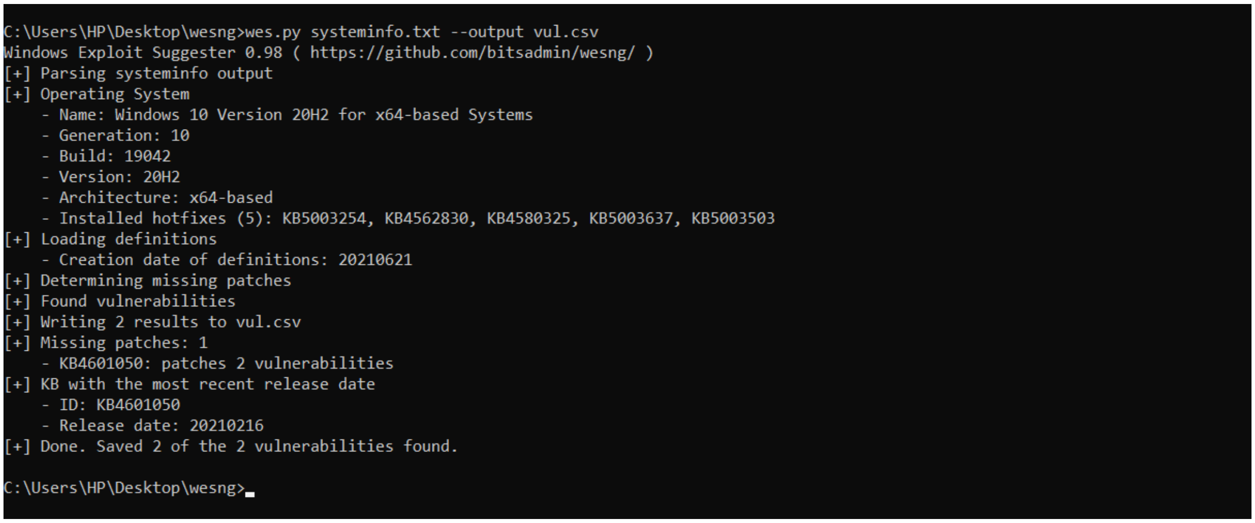


```
C:\Users\HP\Desktop\wesng>wes.py
usage: wes.py [-u] [--update-wes] [--version] [--definitions [DEFINITIONS]] [-p INSTALLEDPATCH [INSTALLEDPATCH ...]]
              [-d] [-e] [--hide HIDDENVULN [HIDDENVULN ...]] [-i IMPACTS [IMPACTS ...]]
              [-s SEVERITIES [SEVERITIES ...]] [-o [OUTPUTFILE]] [--muc-lookup] [-h]
              systeminfo [qfefile]

Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )

positional arguments:
  systeminfo            Specify systeminfo.txt file
  qfefile               Specify the file containing the output of the 'wmic qfe' command

optional arguments:
  -u, --update          Download latest list of CVEs
  --update-wes          Download latest version of wes.py
  --version             Show version information
  --definitions [DEFINITIONS]
                        Definitions zip file (default: definitions.zip)
  -p INSTALLEDPATCH [INSTALLEDPATCH ...], --patches INSTALLEDPATCH [INSTALLEDPATCH ...]
                        Manually specify installed patches in addition to the ones listed in the systeminfo.txt file
  -d, --usekbdate       Filter out vulnerabilities of KBs published before the publishing date of the most recent KB
                        installed
  -e, --exploits-only   Show only vulnerabilities with known exploits
  --hide HIDDENVULN [HIDDENVULN ...]
                        Hide vulnerabilities of for example Adobe Flash Player and Microsoft Edge
  -i IMPACTS [IMPACTS ...], --impact IMPACTS [IMPACTS ...]
                        Only display vulnerabilities with a given impact
  -s SEVERITIES [SEVERITIES ...], --severity SEVERITIES [SEVERITIES ...]
                        Only display vulnerabilities with a given severity
  -o [OUTPUTFILE], --output [OUTPUTFILE]
                        Store results in a file
  --muc-lookup          Hide vulnerabilities if installed hotfixes are listed in the Microsoft Update Catalog as
                        superseding hotfixes for the original BulletinKB
  -h, --help            Show this help message and exit

examples:
  Download latest definitions
  wes.py --update
  wes.py -u
  Determine vulnerabilities
  wes.py systeminfo.txt
```



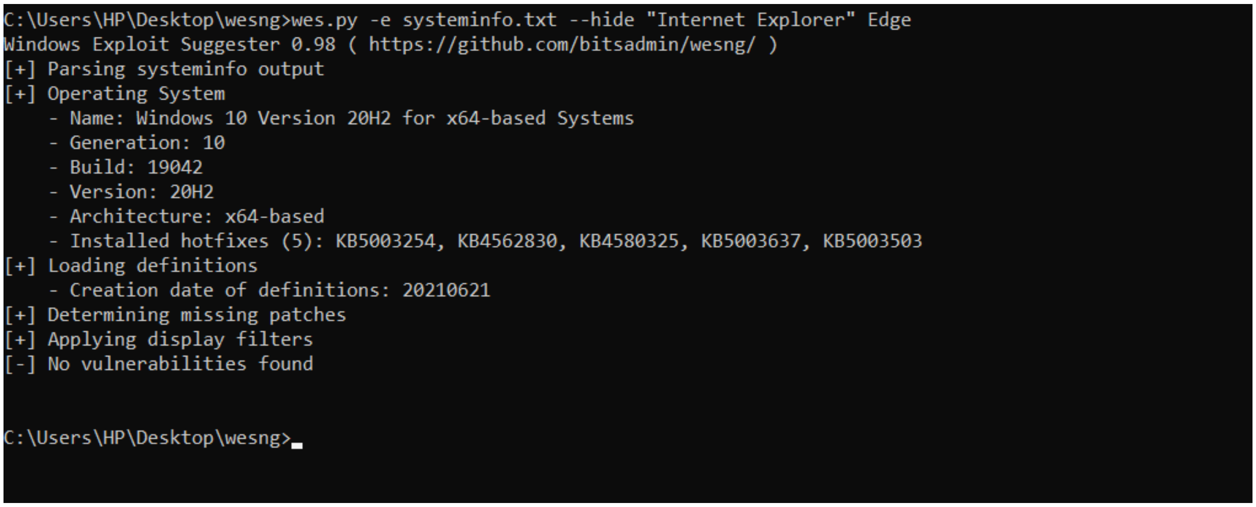
```
 Determine vulnerabilities using both systeminfo and qfe files
 wes.py systeminfo.txt qfe.txt
 Determine vulnerabilities and output to file
 wes.py systeminfo.txt --output vulns.csv
 wes.py systeminfo.txt -o vulns.csv
 Determine vulnerabilities explicitly specifying KBs to reduce false-positives
 wes.py systeminfo.txt --patches KB4345421 KB4487017
 wes.py systeminfo.txt -p KB4345421 KB4487017

 Determine vulnerabilies filtering out out vulnerabilities of KBs that have been published before the publishing date of the most recent KB installed
 wes.py systeminfo.txt --usekbdate
 wes.py systeminfo.txt -d
 Determine vulnerabilities explicitly specifying definitions file
 wes.py systeminfo.txt --definitions C:\tmp\mydefs.zip
 List only vulnerabilities with exploits, excluding IE, Edge and Flash
 wes.py systeminfo.txt --exploits-only --hide "Internet Explorer" Edge Flash
 wes.py systeminfo.txt -e --hide "Internet Explorer" Edge Flash
 Only show vulnerabilities of a certain impact
 wes.py systeminfo.txt --impact "Remote Code Execution"
 wes.py systeminfo.txt -i "Remote Code Execution"

 Only show vulnerabilities of a certain severity
 wes.py systeminfo.txt --severity critical
 wes.py systeminfo.txt -s critical

 Validate supersedence against Microsoft's online Update Catalog
 wes.py systeminfo.txt --muc-lookup
 Download latest version of WES-NG
 wes.py --update-wes

:\Users\HP\Desktop\wesng>
```

>>wes.py systeminfo.txt --output vul.csv



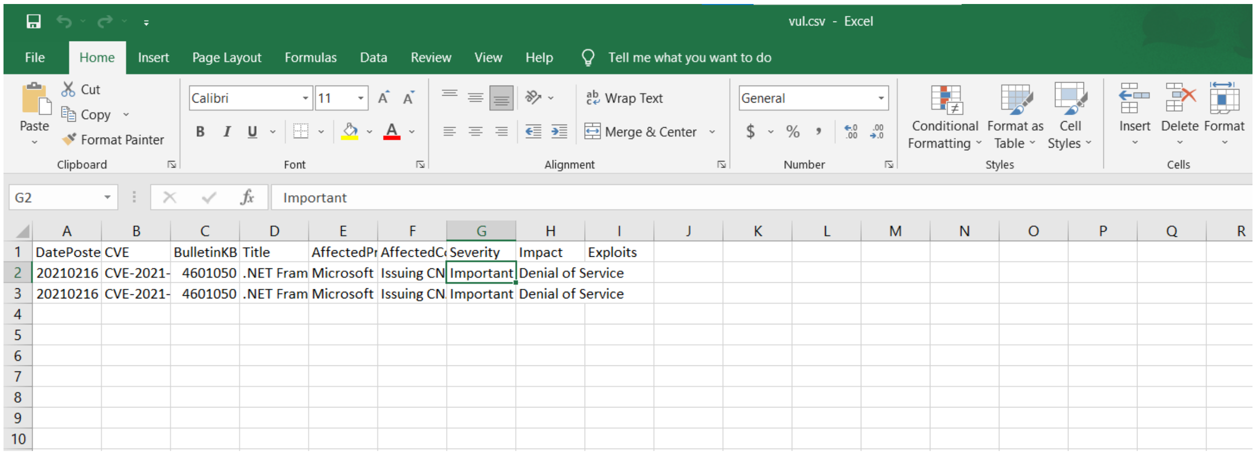
```
C:\Users\HP\Desktop\wesng>wes.py systeminfo.txt --output vul.csv
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19042
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (5): KB5003254, KB4562830, KB4580325, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210621
[+] Determining missing patches
[+] Found vulnerabilities
[+] Writing 2 results to vul.csv
[+] Missing patches: 1
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB4601050
    - Release date: 20210216
[+] Done. Saved 2 of the 2 vulnerabilities found.

C:\Users\HP\Desktop\wesng>
```

Patching



```
C:\Users\HP\Desktop\wesng>wes.py -e systeminfo.txt --hide "Internet Explorer" Edge
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19042
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (5): KB5003254, KB4562830, KB4580325, KB5003637, KB5003503
[+] Loading definitions
    - Creation date of definitions: 20210621
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found


C:\Users\HP\Desktop\wesng>
```

All the vulnerabilities are stored in vul.csv



	A	B	C	D	E	F	G	H	I
1	DatePoste	CVE	BulletinKB	Title	AffectedPr	AffectedC	Severity	Impact	Exploits
2	20210216	CVE-2021-	4601050	.NET Fram	Microsoft	Issuing CN	Important	Denial of Service	
3	20210216	CVE-2021-	4601050	.NET Fram	Microsoft	Issuing CN	Important	Denial of Service	
4									
5									
6									
7									
8									
9									
10									