

# SECURE CODING LAB-13

NAME : G SINDHU

REG NO. : 18BCN7098

Windows exploiter:

This is a tool that helps you to identify the vulnerability in your windows system.

Github link:

Now open the command prompt

```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Gurra>cd C:\wesng-master

C:\wesng-master>python wes.py --update
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Updating definitions
[+] Obtained definitions created at 20210607

C:\wesng-master>python wes.py Systeminfo.txt
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
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: None
[+] Loading definitions
    - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Found vulnerabilities
```

Send the systeminfo as a text file to wes.py to list all the vulnerabilities.

Systeminfo - Notepad

File Edit Format View Help

OS Name Microsoft Windows 10 Home  
Version 10.0.19042 Build 19042  
Other OS Description Not Available  
OS Manufacturer Microsoft Corporation  
System Name DESKTOP-5VG4MVL  
System Manufacturer HP  
System Model HP ENVY x360 Convertible 15-bp1xx  
System Type x64-based PC  
System SKU 1KS77UA#ABA  
Processor Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz, 1992 Mhz, 4 Core(s), 8 Logical Processor(s)  
BIOS Version/Date Insyde F.22, 24-07-2017  
SMBIOS Version 3.0  
Embedded Controller Version 32.60  
BIOS Mode UEFI  
BaseBoard Manufacturer HP  
BaseBoard Product 83C8  
BaseBoard Version 32.60  
Platform Role Mobile  
Secure Boot State On  
PCR7 Configuration Elevation Required to View  
Windows Directory C:\WINDOWS  
System Directory C:\WINDOWS\system32  
Boot Device \Device\HarddiskVolume1

Date: 20210216  
CVE: CVE-2021-24111  
KB: KB4601050  
Title: .NET Framework Denial of Service Vulnerability  
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems  
Affected component: Issuing CNA  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20210216  
CVE: CVE-2021-24111  
KB: KB4601050  
Title: .NET Framework Denial of Service Vulnerability  
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 20H2 for x64-based Systems  
Affected component: Issuing CNA  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20210511  
CVE: CVE-2020-24588  
KB: KB5003173  
Title: Windows Wireless Networking Spoofing Vulnerability  
Affected product: Windows 10 Version 20H2 for x64-based Systems  
Affected component: Issuing CNA  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20210511  
CVE: CVE-2020-24588  
KB: KB5003173  
Title: Windows Wireless Networking Spoofing Vulnerability  
Affected product: Windows 10 Version 20H2 for x64-based Systems  
Affected component: Issuing CNA  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20210511  
CVE: CVE-2020-24587  
KB: KB5003173

```
Date: 20210511
CVE: CVE-2020-24587
KB: KB5003173
Title: Windows Wireless Networking Information Disclosure Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Information Disclosure
Exploit: n/a

Date: 20210511
CVE: CVE-2020-26144
KB: KB5003173
Title: Windows Wireless Networking Spoofing Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Spoofing
Exploit: n/a

Date: 20210511
CVE: CVE-2020-26144
KB: KB5003173
Title: Windows Wireless Networking Spoofing Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Spoofing
Exploit: n/a

Date: 20210511
CVE: CVE-2021-28455
KB: KB5003173
Title: Microsoft Jet Red Database Engine and Access Connectivity Engine Remote Code Execution Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Remote Code Execution
Exploit: n/a

Date: 20210511
CVE: CVE-2021-28455
KB: KB5003173
Title: Microsoft Jet Red Database Engine and Access Connectivity Engine Remote Code Execution Vulnerability
```

```
Severity: Important
Impact: Remote Code Execution
Exploit: n/a
```

```
Date: 20210511
CVE: CVE-2021-28479
KB: KB5003173
Title: Windows CSC Service Information Disclosure Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Information Disclosure
Exploit: n/a
```

```
Date: 20210511
CVE: CVE-2021-28479
KB: KB5003173
Title: Windows CSC Service Information Disclosure Vulnerability
Affected product: Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Important
Impact: Information Disclosure
Exploit: n/a
```

```
Date: 20210511
CVE: CVE-2021-26419
KB: KB5003173
Title: Scripting Engine Memory Corruption Vulnerability
Affected product: Internet Explorer 11 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.html
```

```
Date: 20210511
CVE: CVE-2021-26419
KB: KB5003173
Title: Scripting Engine Memory Corruption Vulnerability
Affected product: Internet Explorer 11 on Windows 10 Version 20H2 for x64-based Systems
Affected component: Issuing CNA
Severity: Critical
Impact: Remote Code Execution
Exploit: http://packetstormsecurity.com/files/162570/Internet-Explorer-jscript9.dll-Memory-Corruption.html
```

```
Exploit: n/a
```

```
[+] Missing patches: 2
- KB5003173: patches 50 vulnerabilities
- KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
- ID: KB5003173
- Release date: 20210511
```

```
[+] Done. Displaying 52 of the 52 vulnerabilities found.
```

## Now fix all the vulnerabilities as shown:

```
C:\Users\Gurra>cd C:\wesng-master
C:\wesng-master>python wes.py systeminfo.txt -p KB4601050 KB5003173
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
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: None
  - Manually specified hotfixes (2): KB4601050, KB5003173
[+] Loading definitions
  - Creation date of definitions: 20210607
[+] Determining missing patches
[-] No vulnerabilities found
```

```
C:\wesng-master>python wes.py -e Systeminfo.txt --hide "Internet Explorer" Ed
WARNING:root:chardet module not installed. In case of encoding errors, install chardet using: pip3 install chardet
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: None
[+] Loading definitions
  - Creation date of definitions: 20210607
[+] Determining missing patches
[+] Applying display filters
[-] No vulnerabilities found
```

You can see “No vulnerabilities are found”.