CSE-2010 Secure Coding Lab-13

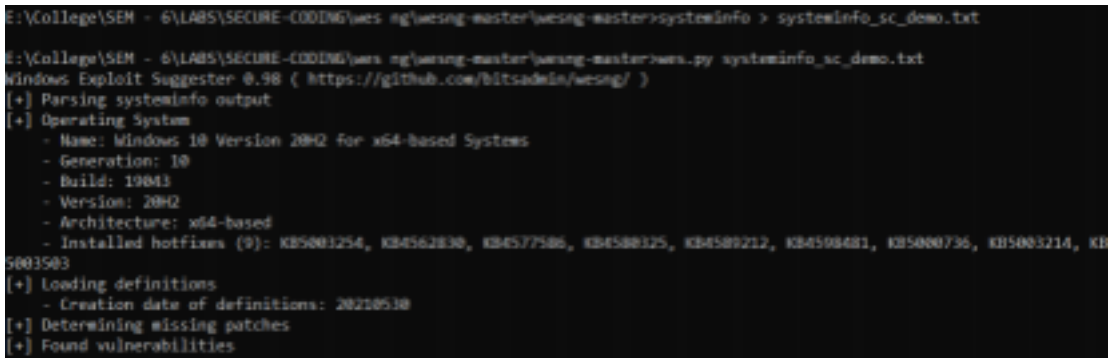
Name :- Amritmoy Pain

Reg. No. :- 18BCE7344

Windows exploit suggester:

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

Double click on the setup.py to setup windows exploit suggester. Now open command prompt do as follows

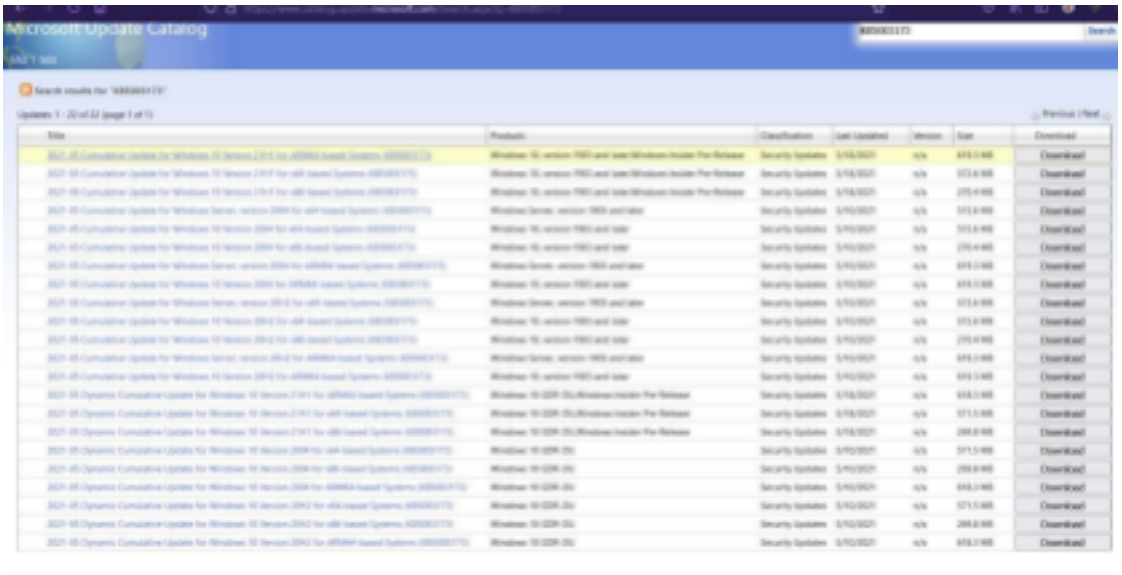


Pipe the systeminfo as a txt file to the wes.py and it will list all the vulnerabilities in the system. At last it will give you all the patches that are required to patch the vulnerabilities as below.

```
[+] 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 go to the Microsoft catalog to download the required hotfixes I will be like below.



Download the appropriate hotfixes for your pc type **winver** in start to get the version of the pc you are using. Download your hotfixes and fix your vulnerabilities.

C \W\ndows\SysTe m32\r md exe

```
Severity: Important
```

Impact: Security Feature Bypas:

Eypla it n/a

Date 20210511

CVE CVE -202-1 31208

KB KB500317 3

Title: Windows Container Manager Service Elevation of Privilege Vulnerability

ATTer ted produr t tTi ndo ys 10 Vension 20H2 Ton xñ4-based Sy s terns ATTer ted r omponenI T s s uEng C UA

Severity: Important

Impact: Elevation of Privilege

Eypla it n/a

Date 20210511

CVE CVE -202-1 31208

KB KB500317 3

Title: Windows Container Manager Service Elevation of Privilege Vulnerability

ATTer ted produr t tTi ndo ys 10 Vension 20H2 Ton xñ4-based Sy s terns ATTer ted r omponenI T s s uEng C UA

Severity: Important

Impact: Elevation of Privileg(

Eypla it n/a

Date 20210511

CVE CVE-2021-28476

KB KB500317 3

Tit1e Hypen-V Remote code Eyerut ion vv1nerabi 1ity

ATTer ted produr t tTi ndo ys 10 Vension 20H2 Ton xñ4-based Sy s terns ATTer ted r omponenI T s s uEng C UA

Severity c r it i r a1

Amparl R emol e c ode Exe r ut hon

Eypla it n/a

Date 20210511

CVE CVE-2021-28476

KB KB500317 3

Tit1e Hypen-V Remote code Eyerut ion vv1nerabi 1ity

ATTer ted produr t tTi ndo ys 10 Vension 20H2 Ton xñ4-based Sy s terns ATTer ted r omponenI T s s uEng C UA

Severity c r it i r a1

Amparl R emol e c ode Exe r ut hon

Eypla it n/a

[+] Missing patches: 2

- KB5003173 pat r he s 50 vulne rabi 1it ie s
- KB4601050 pat r he s 2 vulne rabi 1it ie s

[+ KB tvdth the mo s l ne r ent ne1ease date

- ID KB500317 3
- Relea s e date 20210511

[+ d Done . D i s p let' ing 82 of the 82 vu lne ceb i l it ie s I ound .