Exercise 5: Find Vulnerabilities on Exploit Sites

Exploit sites contain details of the latest vulnerabilities of various OSes, devices, and applications.

Lab Scenario

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

A security professional must have the required knowledge to find vulnerabities on exploit sites and further mitigate them to enhance the organization's security infrastructure.

Lab Objectives

This lab demonstrates how to find the vulnerabilities of the target system using various exploit sites such as Exploit DB.

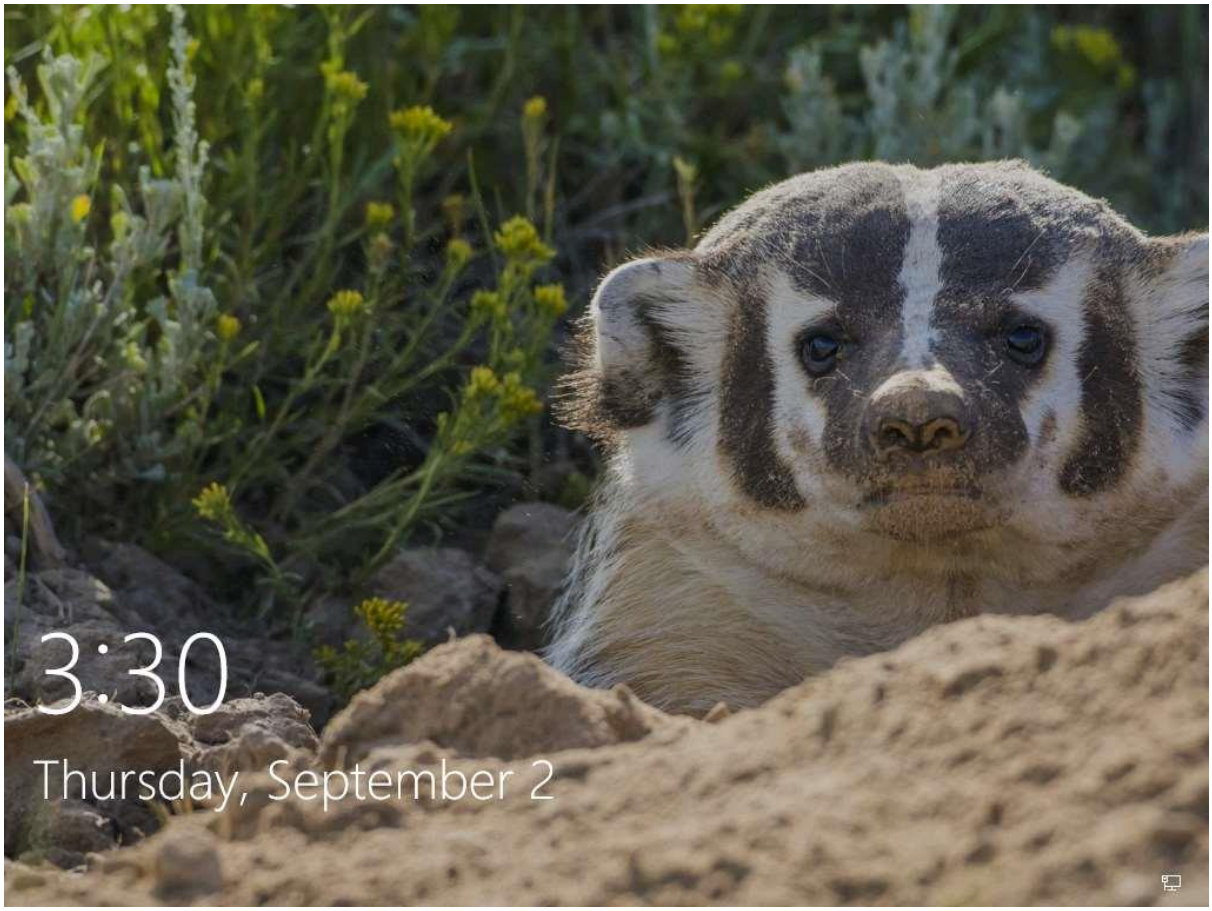
Overview of Exploit Sites

Exploit sites can be used to find relevant vulnerabilities about the target system based on the information gathered, the exploits from the database and exploitation tools such as Metasploit can be used, to gain remote access.

Lab Tasks

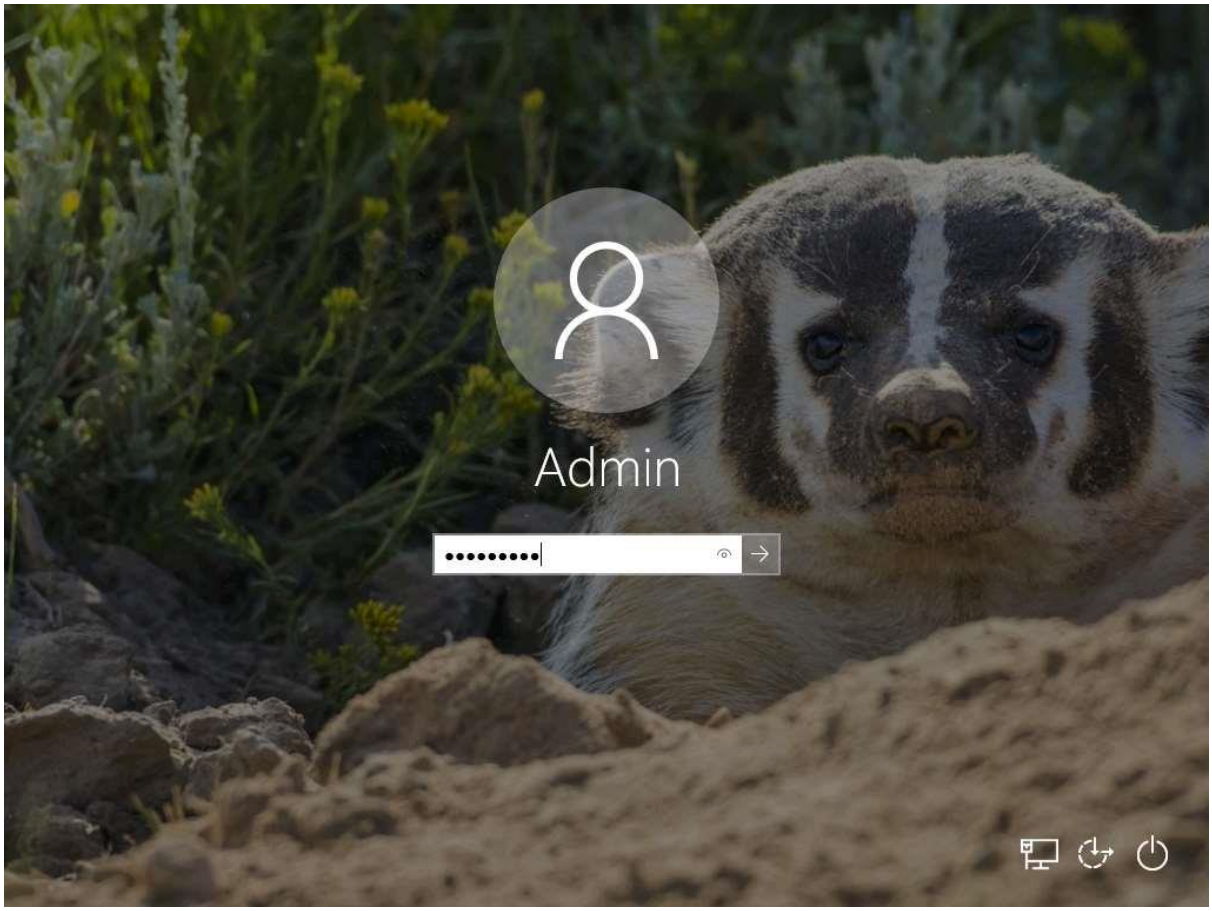
If you are already logged into **Admin Machine-1**, then skip to **Step#3**.

1. Click Admin Machine-1 to switch to the **Admin Machine-1** machine (as an attacker). Click Ctrl+Alt+Delete.



Alternatively, click the **Ctrl+Alt+Delete** button under the **Admin Machine-1** machine thumbnail in the **Resources** pane or click the **Ctrl+Alt+Delete** button under the **Commands** (**Thunder** icon) menu.

2. By default, the **Admin** user profile is selected. Click admin@123 to paste the password in the **Password** field and press **Enter** to login.



If the **Welcome to Windows** wizard appears, click **Continue**. In the **Sign in with Microsoft** wizard, click **Cancel**.

The **Networks** screen appears. Click **Yes** to allow the PC to be discoverable by other PCs and devices on the network.

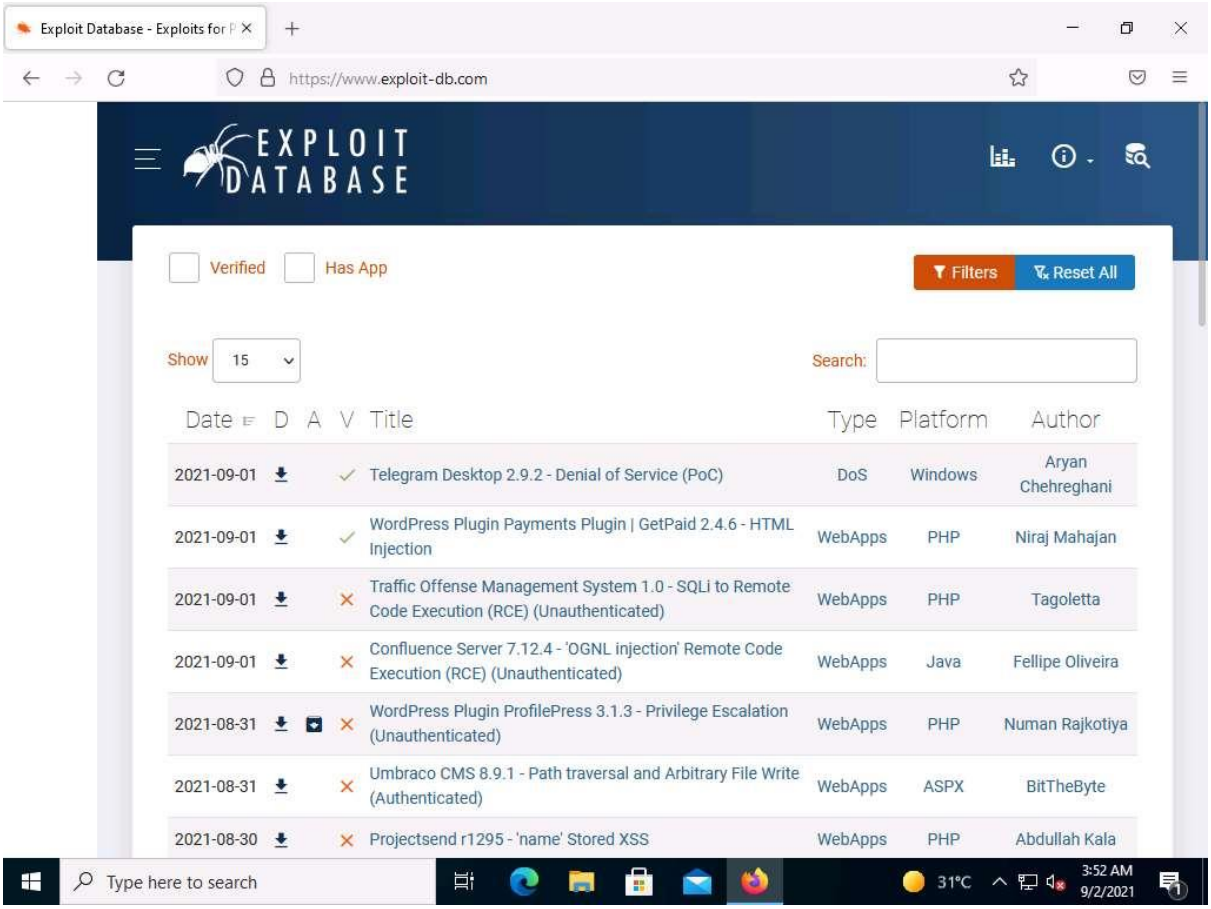
3. Open any web browser (here, **Mozilla Firefox**). Place your mouse cursor in the address bar of the browser, click https://www.exploit-db.com/ and press **Enter**.

   If a **User Account Control** pop-up appears, click **Yes**.

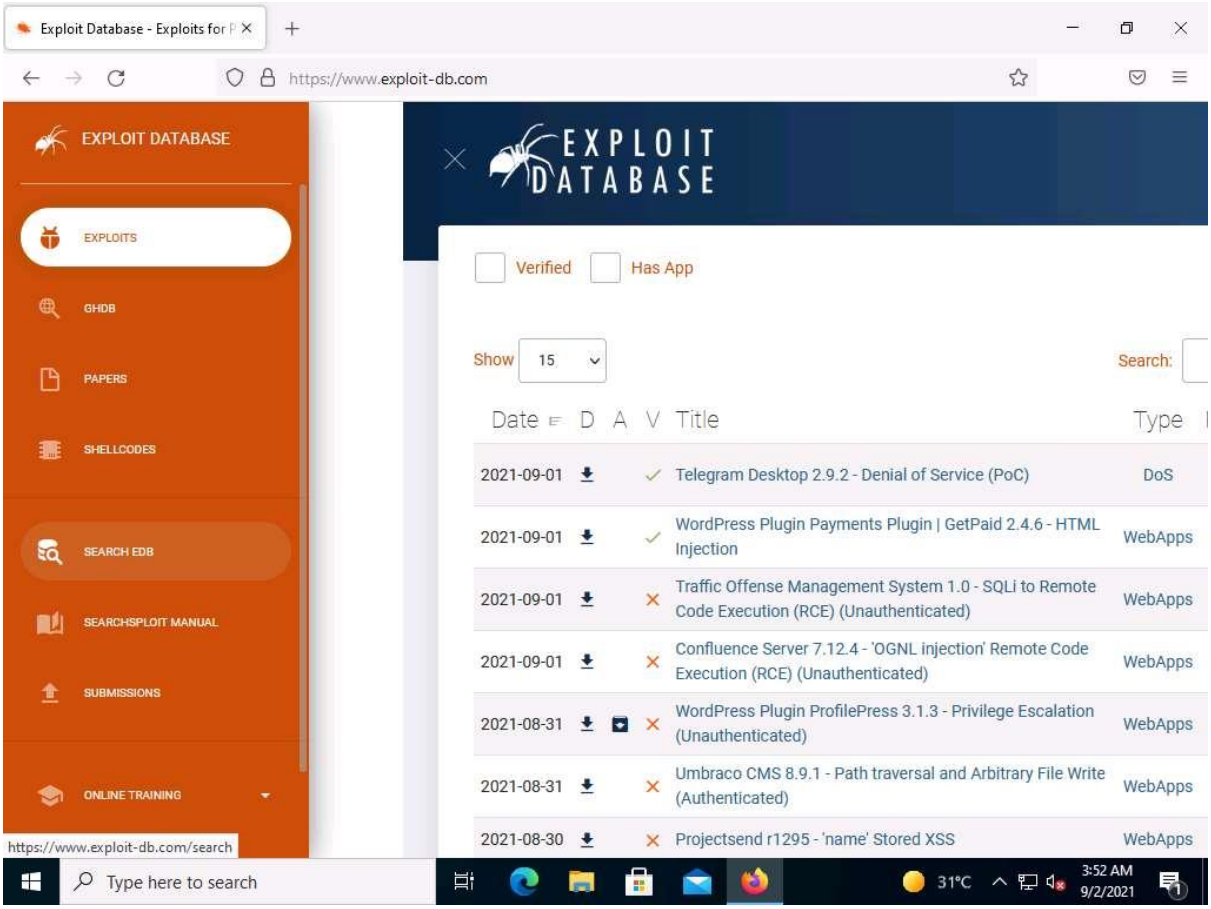
   If you are unable to browse **www.exploit-db.com**, then either use some other machine in the lab environment to browse the website or use your local machine to access the website to run the task.

4. The **Exploit Database** website appears. Click any of the latest vulnerabilities to view detailed information, or search for a specific vulnerability by entering its name in the **Search** field.

   If a **This website uses cookie** pop-up appears at the bottom, click **Allow all cookies**.

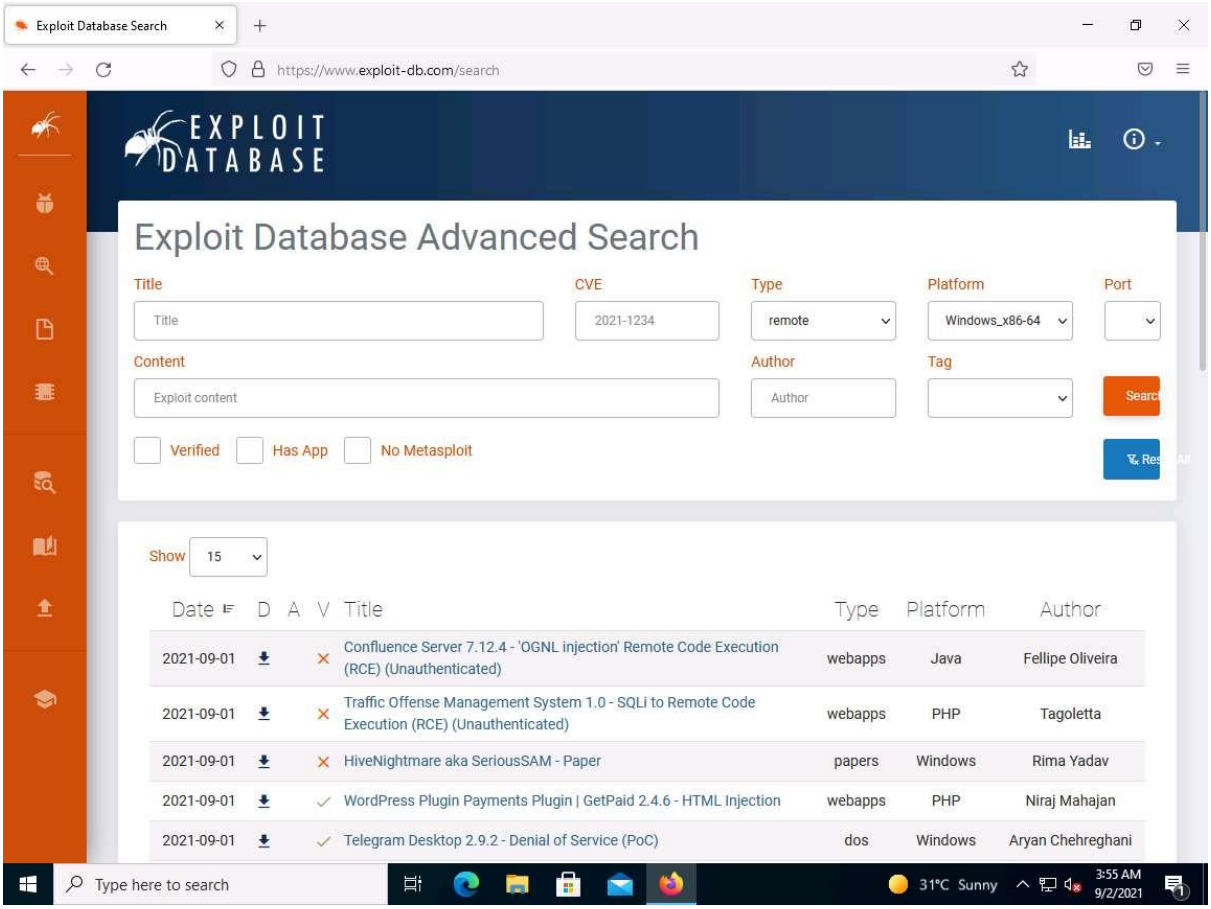


5. Move the mouse cursor to the left-pane of the website and select the **SEARCH EDB** option from the list to perform an advanced search.

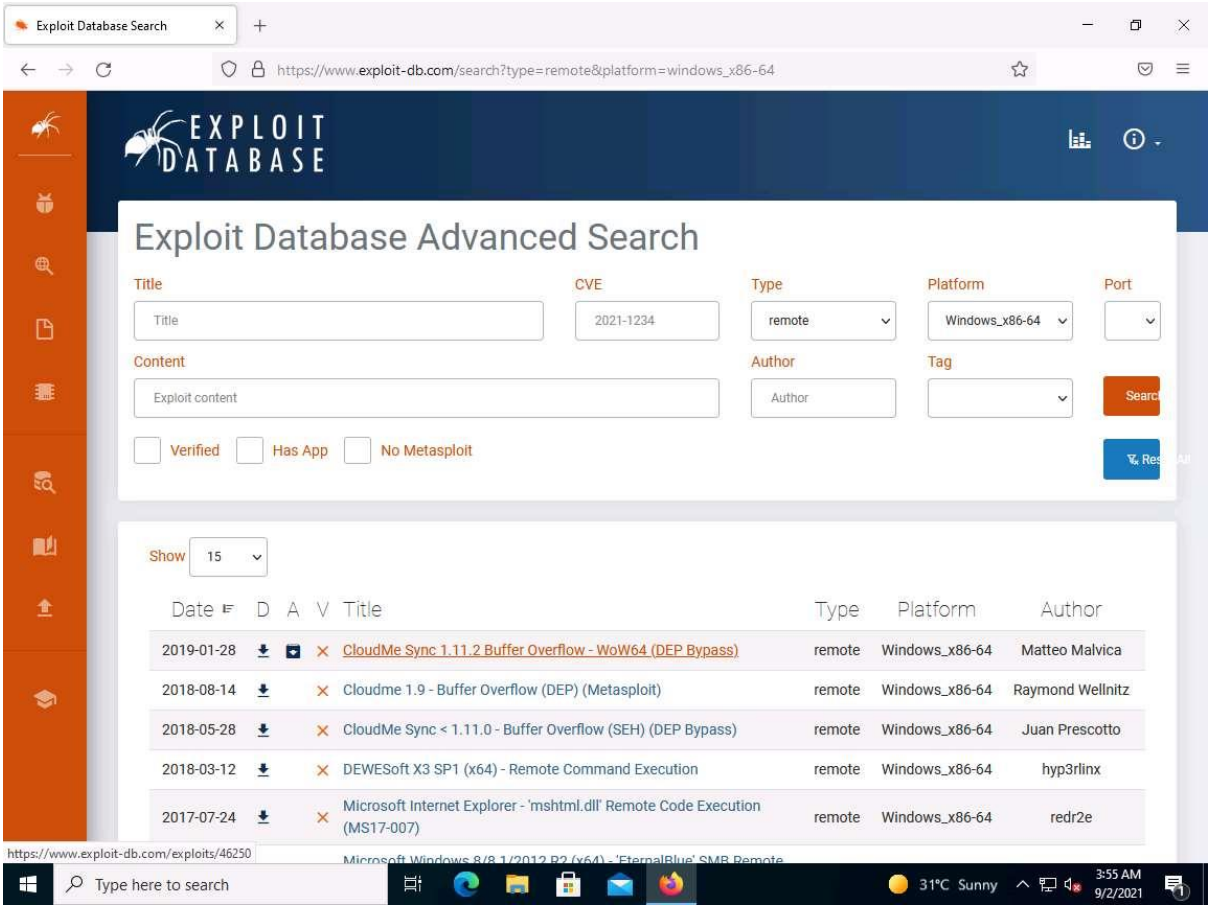


6. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

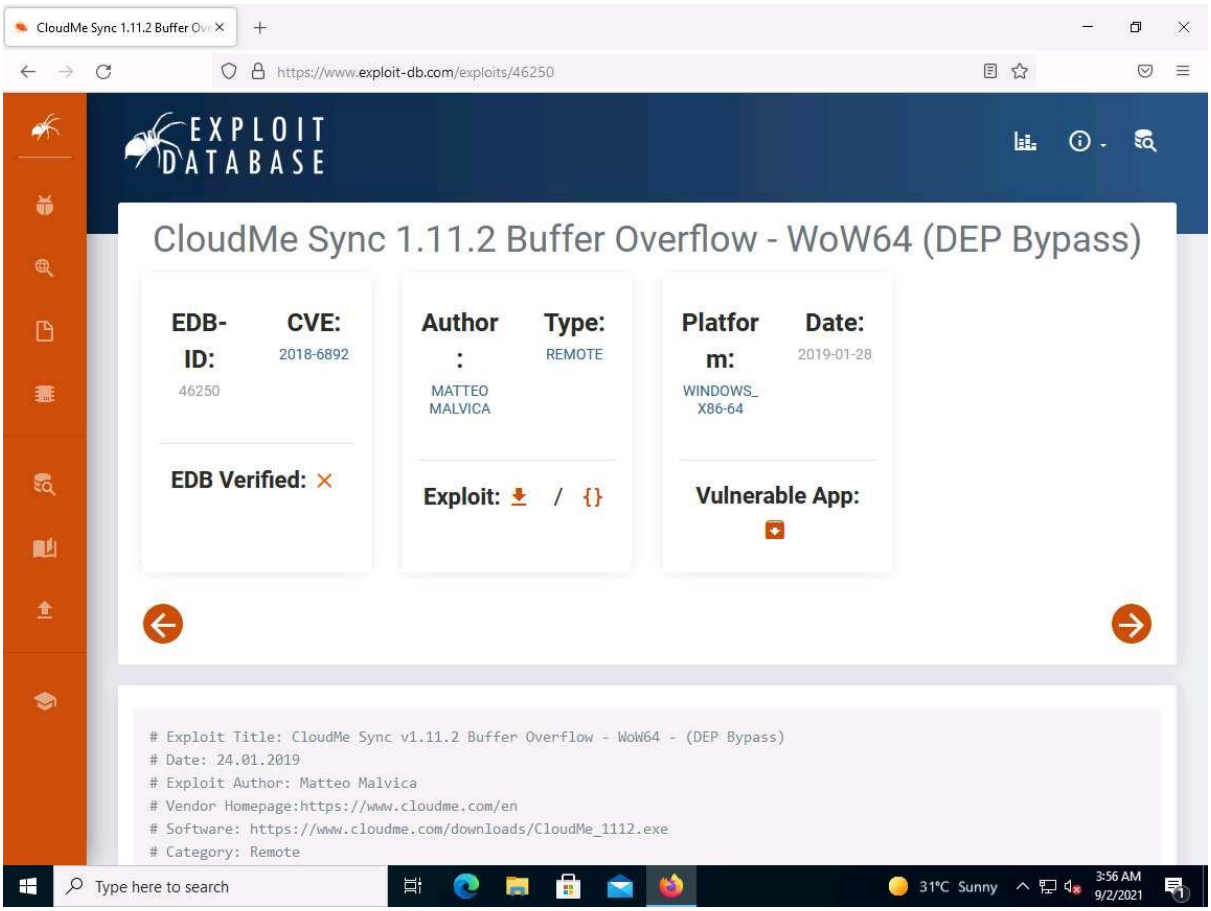
   Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.



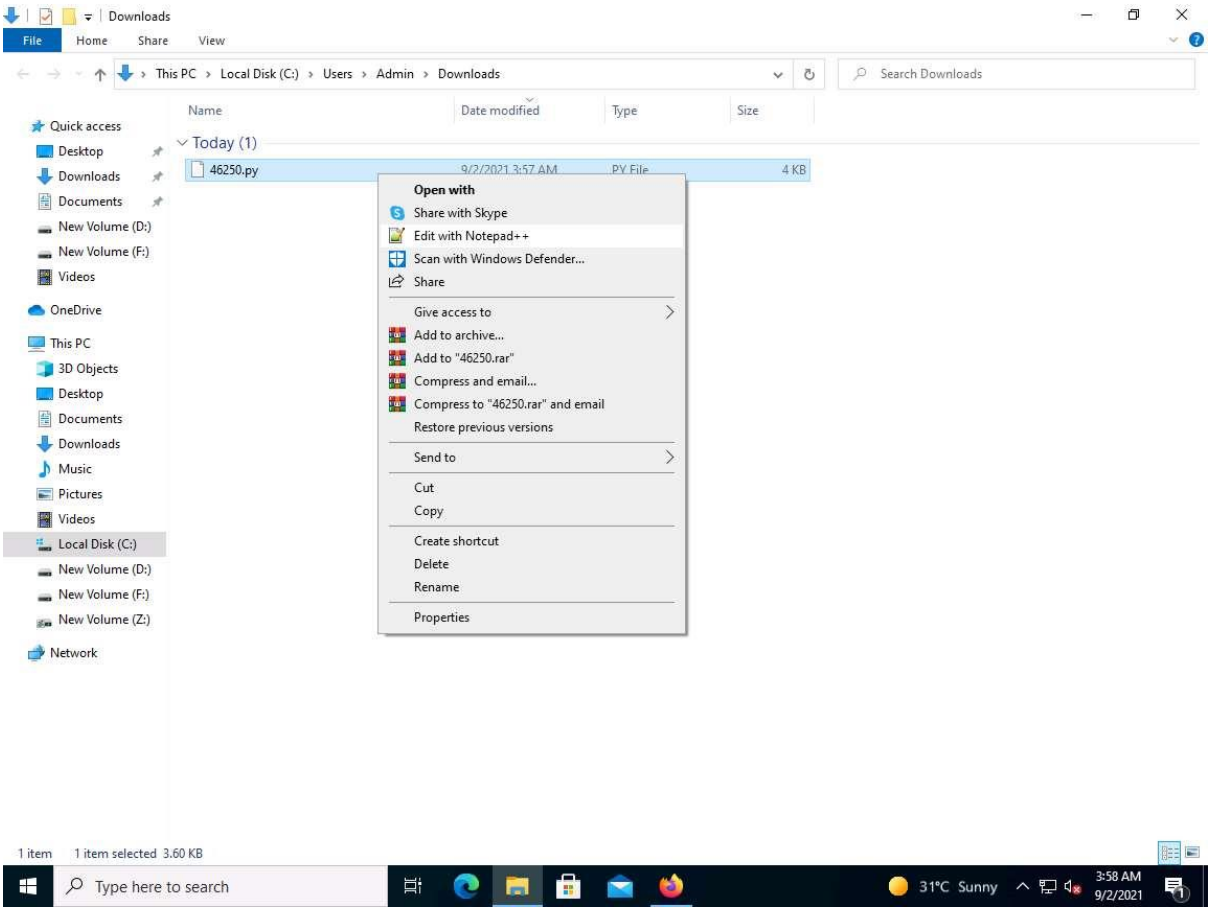
7. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.
8. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**.



9. Detailed information is displayed regarding the selected vulnerability such as EDB-ID, CVE, author, type, platform, and published date, as shown in the screenshot below.
10. Click on the download icon ( ) in the **Exploit** section to download the exploit code.

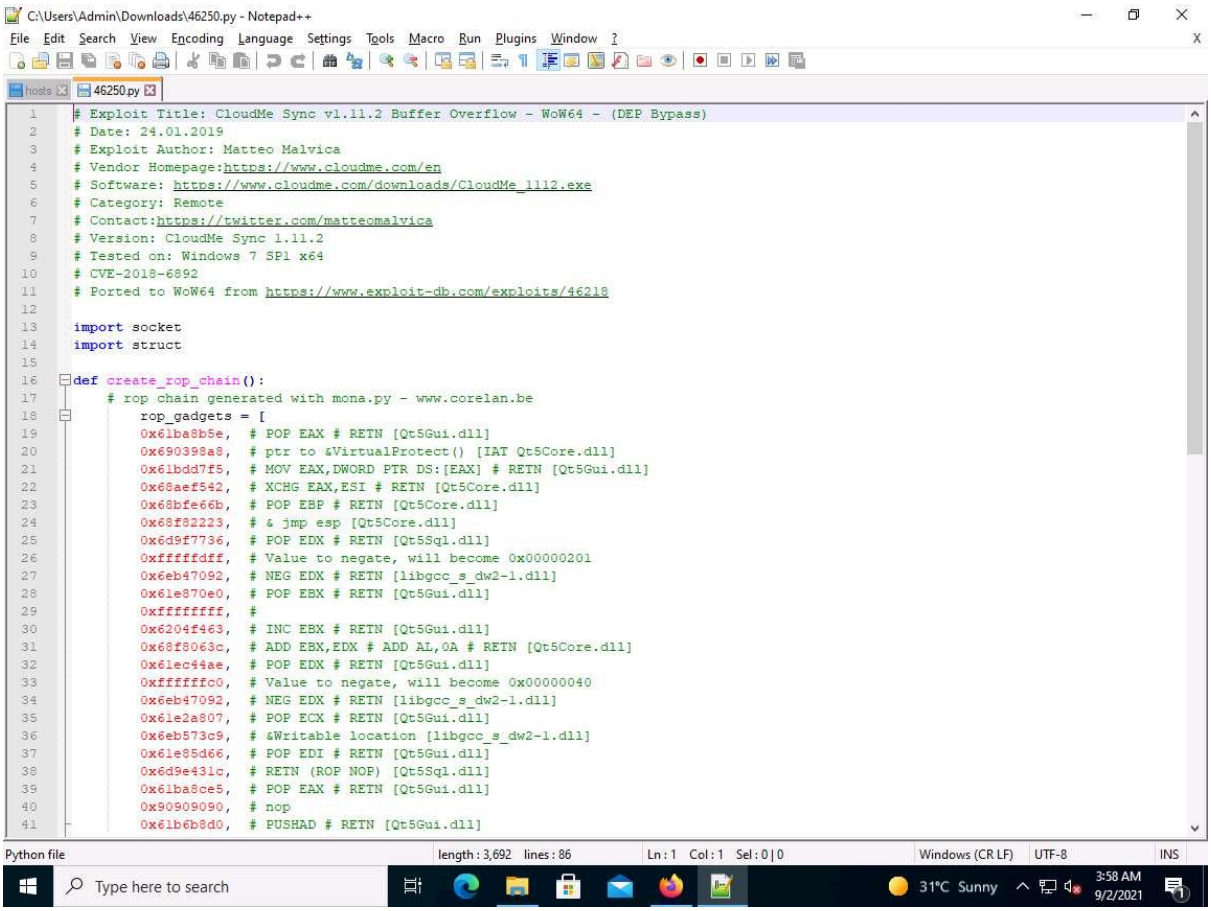


11. The **Opening file** pop-up appears. Select the **Save File** radio button and click **OK** to download the exploit file.
12. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.



13. A **Notepad++** windows appears, displaying the exploit code, as shown in the screenshot below.

    If a **Notepad++ update** pop-up appears, click **No**.



14. This exploit code can further be used to exploit vulnerabilities in the target system.
15. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
16. Close all open windows and document all the acquired information.