

# Batch:A3 Roll No.:16010421119 Experiment No.:8

**Aim:** Demonstrating vulnerabilities and exploits with (CVE databases and Exploit db, with Metasploitable).

**Resources needed:** Common Vulnerabilities and Exposures (CVE) Database, National Vulnerability Database (NVD), Exploit Database (Exploit-DB), Metasploit Framework, VulnHub, Hack The Box (HTB), OWASP WebGoat, Practical Pentest Labs (PPL)

# Pre Lab/ Prior Concepts:

Students should have prior knowledge of the Understanding Vulnerabilities, Common Vulnerabilities and Exposures (CVE), Exploits and Exploitation, Exploit Database (Exploit-DB), Metasploit Framework, Metasploitable, Exploitation Process, and Network Fundamentals.

# Theory:

Understanding vulnerabilities and exploits is foundational in cybersecurity, providing crucial insights into potential weaknesses in systems and applications. This one-page theory delves into the comprehensive exploration of vulnerabilities through Common Vulnerabilities and Exposures (CVE) databases, Exploit DB, and hands-on experimentation on Metasploitable.

**Common Vulnerabilities and Exposures (CVE):** CVE serves as a standardized system for identifying and cataloging vulnerabilities and exposures. Each CVE entry provides a unique identifier, facilitating a common understanding across the cybersecurity community. Navigating the CVE database allows professionals to access detailed information about known vulnerabilities, including their descriptions, severity levels, and potential impacts.

**Exploit Database (Exploit-DB):** Exploit-DB stands as a repository for exploits and proof-of- concept code. Security researchers and professionals contribute to this database, sharing their discoveries and tools related to vulnerabilities. Exploit-DB provides a practical resource for understanding the real-world application of exploits, offering insights into the techniques used to compromise security.

**The Metasploit Framework:** Metasploit, an open-source penetration testing tool, plays a pivotal role in comprehending vulnerabilities and exploits. It boasts an extensive collection of exploits, payloads, and auxiliary modules. Metasploit allows security professionals to experiment with and validate the exploitation of vulnerabilities in controlled environments.

**Metasploitable Experiments:** Metasploitable, a deliberately vulnerable virtual machine, serves as an invaluable platform for hands-on experimentation. Security practitioners can actively apply their knowledge of vulnerabilities and exploits in a safe and isolated environment. By exploiting vulnerabilities on Metasploitable, individuals gain practical insights into the exploitation process, honing their skills in identifying, selecting, and executing exploits.

**Ethical Considerations and Responsible Conduct:** While engaging in experiments with vulnerabilities and exploits, ethical considerations and responsible conduct are paramount. Professionals must adhere to legal and ethical standards, ensuring that their activities are conducted in controlled environments and for educational purposes. Acknowledging the potential impact of exploitation on systems and data underscores the importance of ethical hacking practices.

# Procedure:

Understanding vulnerabilities and exploits involves a structured approach, incorporating the exploration of CVE databases, Exploit DB, and hands-on experimentation on platforms like Metasploitable. Here is a stepwise procedure for this comprehensive process:

# Step 1: Familiarize with CVE Databases

* Explore the CVE Database
* Study CVE Entries

# Step 2: Dive into Exploit-DB

* Visit Exploit-DB
* Explore Exploit Entries

# Step 3: Set Up a Lab Environment

* Download and Install Metasploitable
* Configure Networking

# Step 4: Experimentation on Metasploitable

* Identify Vulnerabilities
* Select an Exploit Module in Metasploit
* Configure and Execute the Exploit

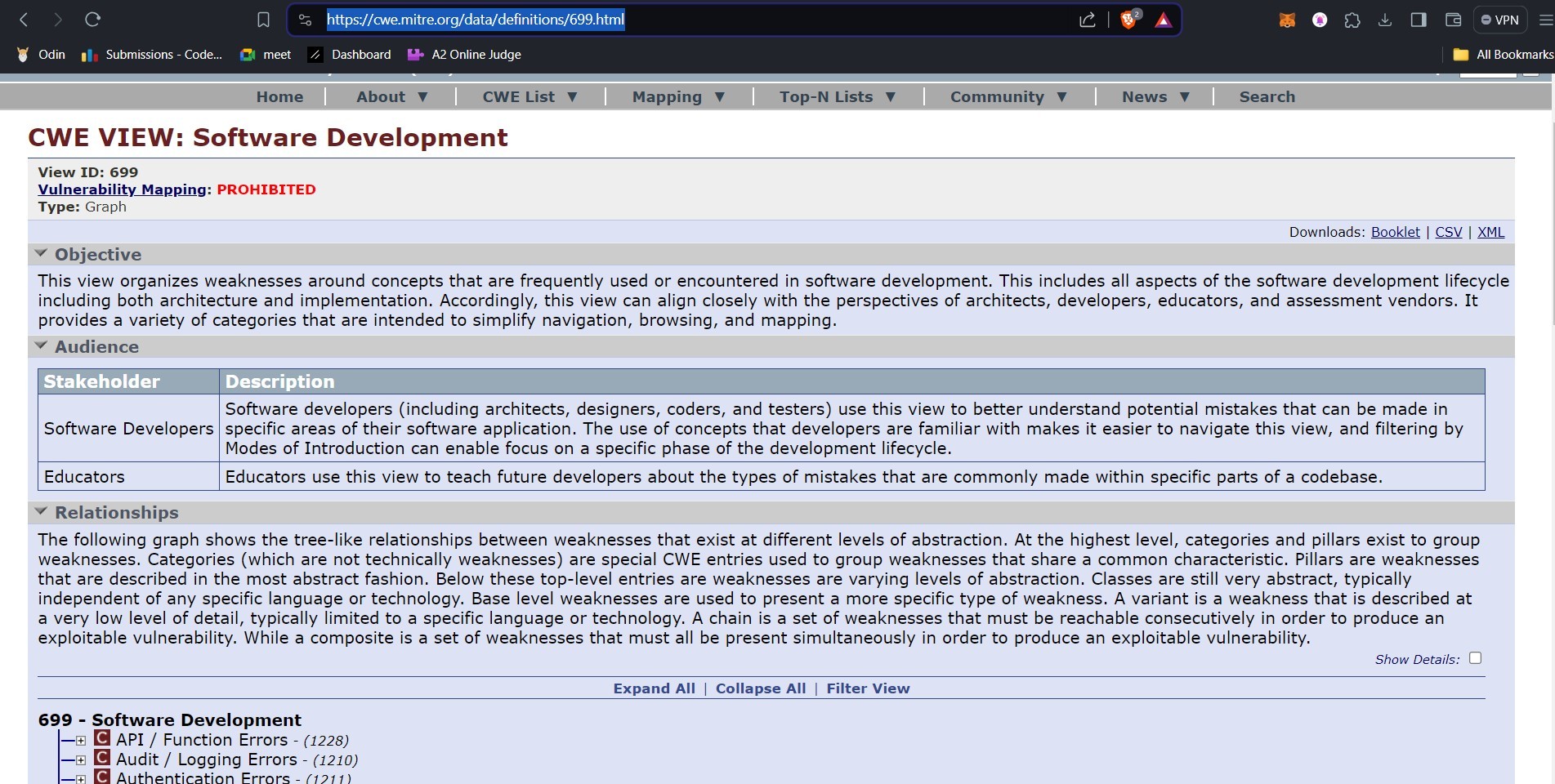
# Step 5: Analyze and Document Results

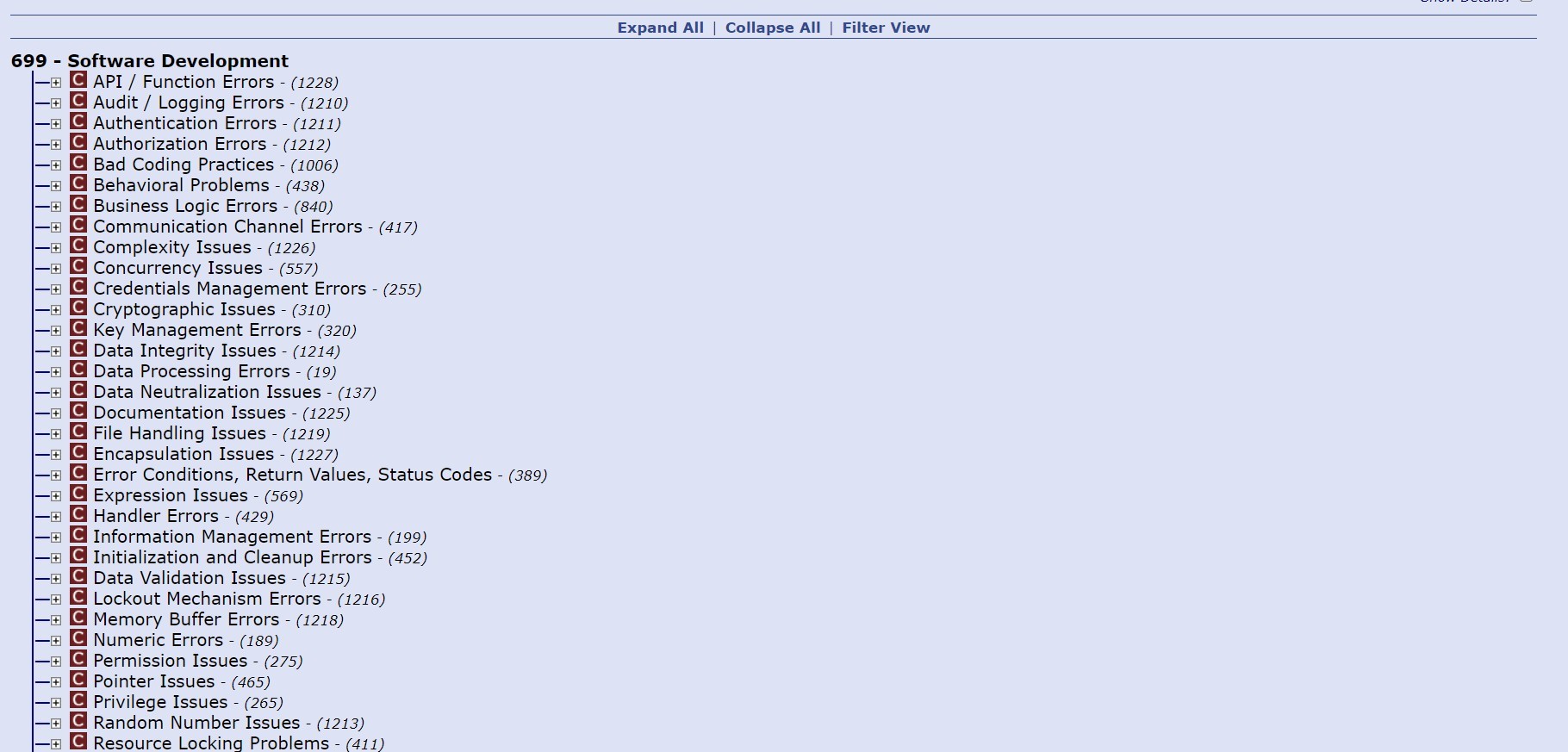
* Observe the Exploitation Process
* Document Findings

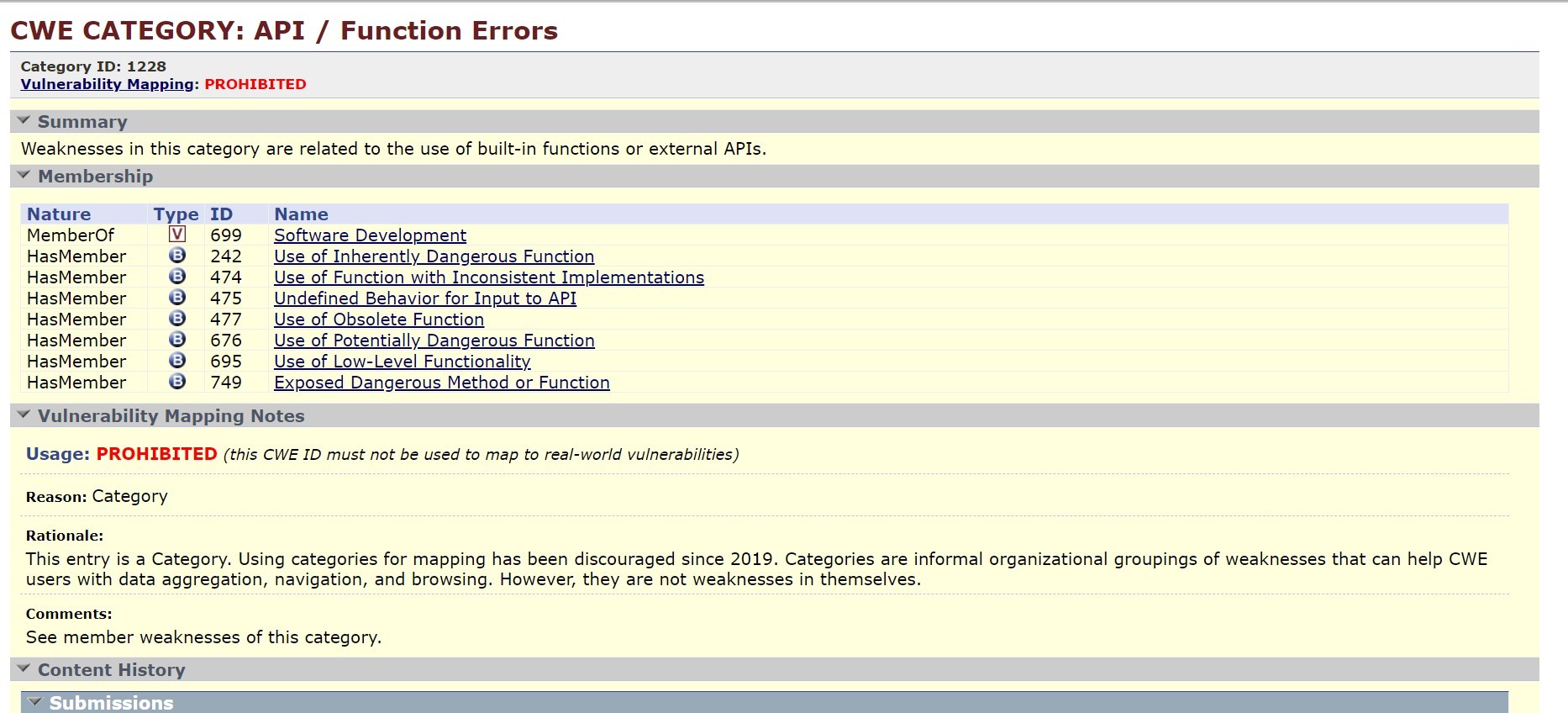
# Output (Code with result Snapshot)

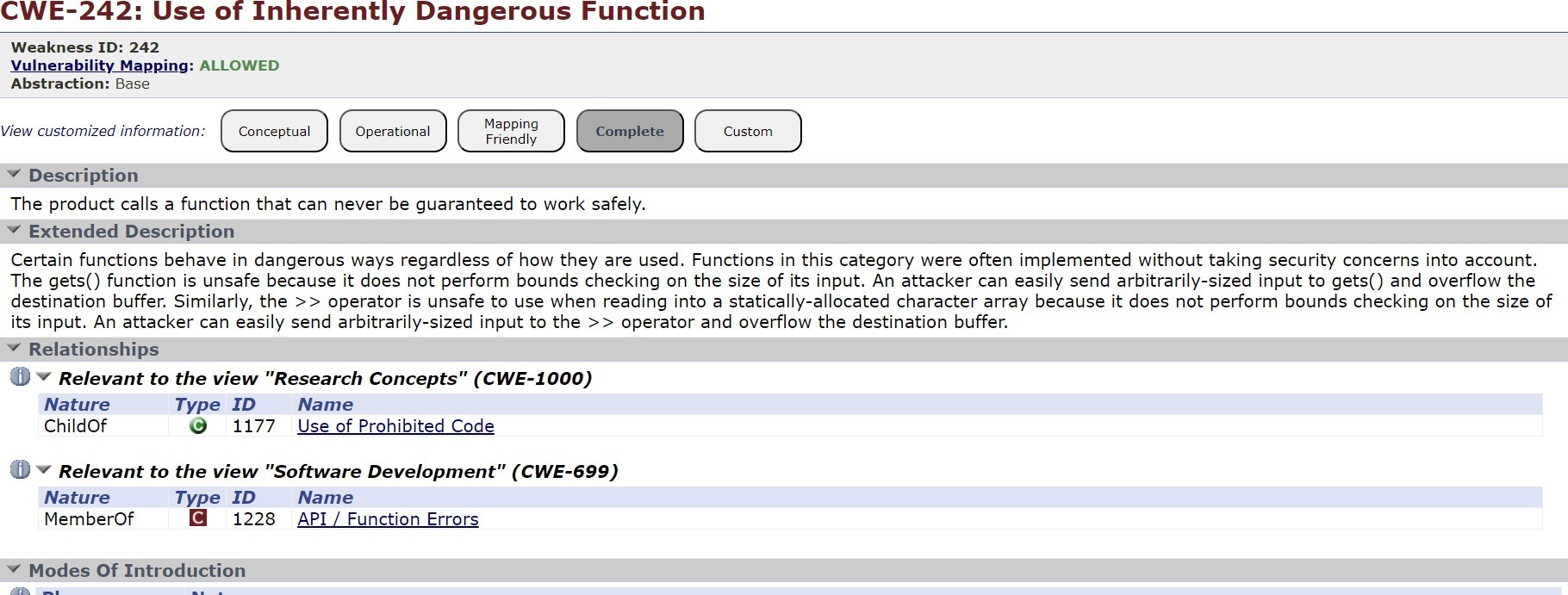
**Step 1: Familiarize with CVE Databases**

# viewing https://cwe.mitre.org/data/definitions/699.html website to view at CWE of software



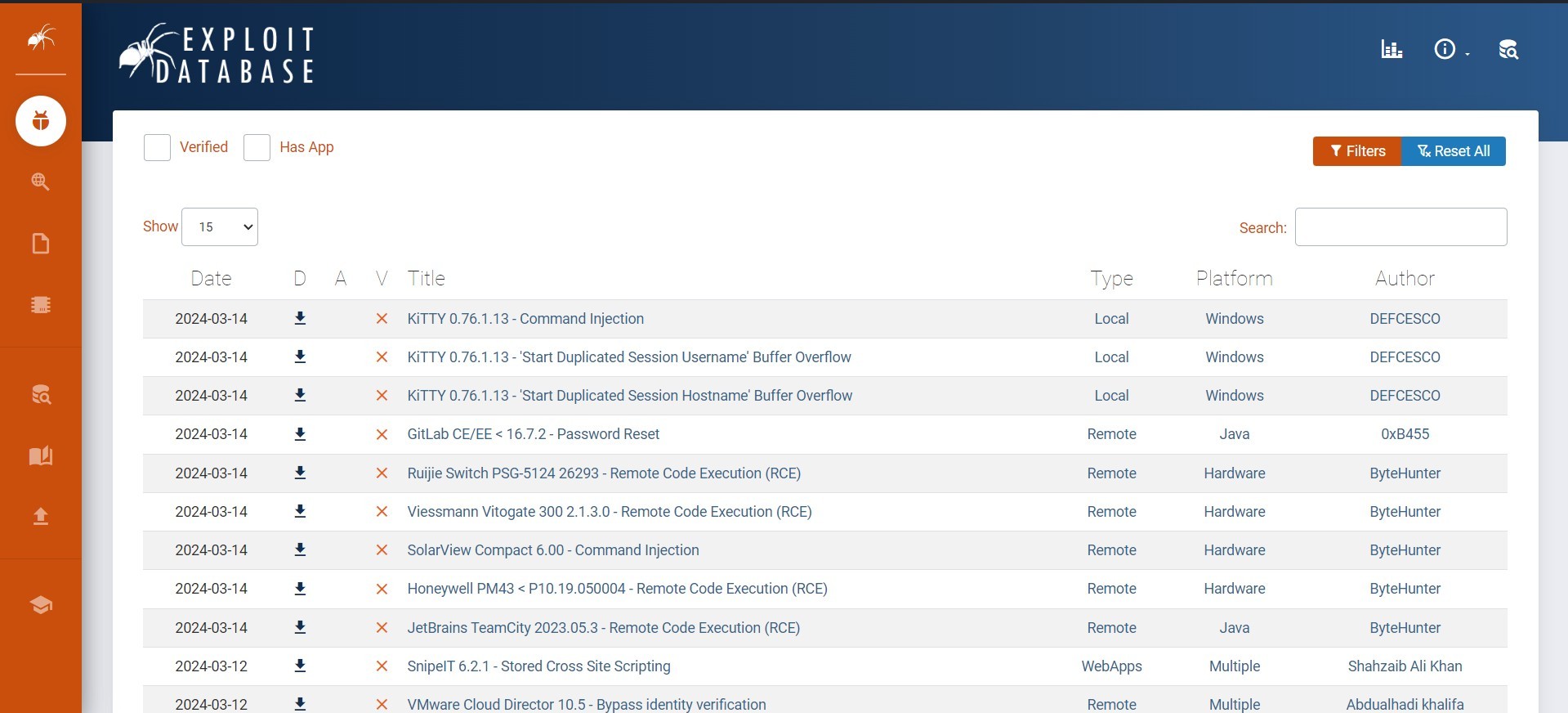
here we can see the particular CWE category

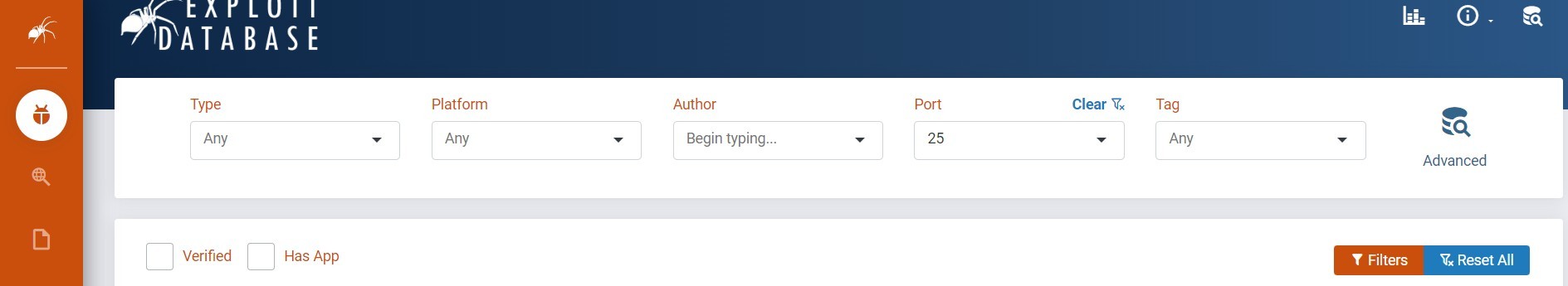


this allows us to see a particular CWE and see the information about this particular CWE

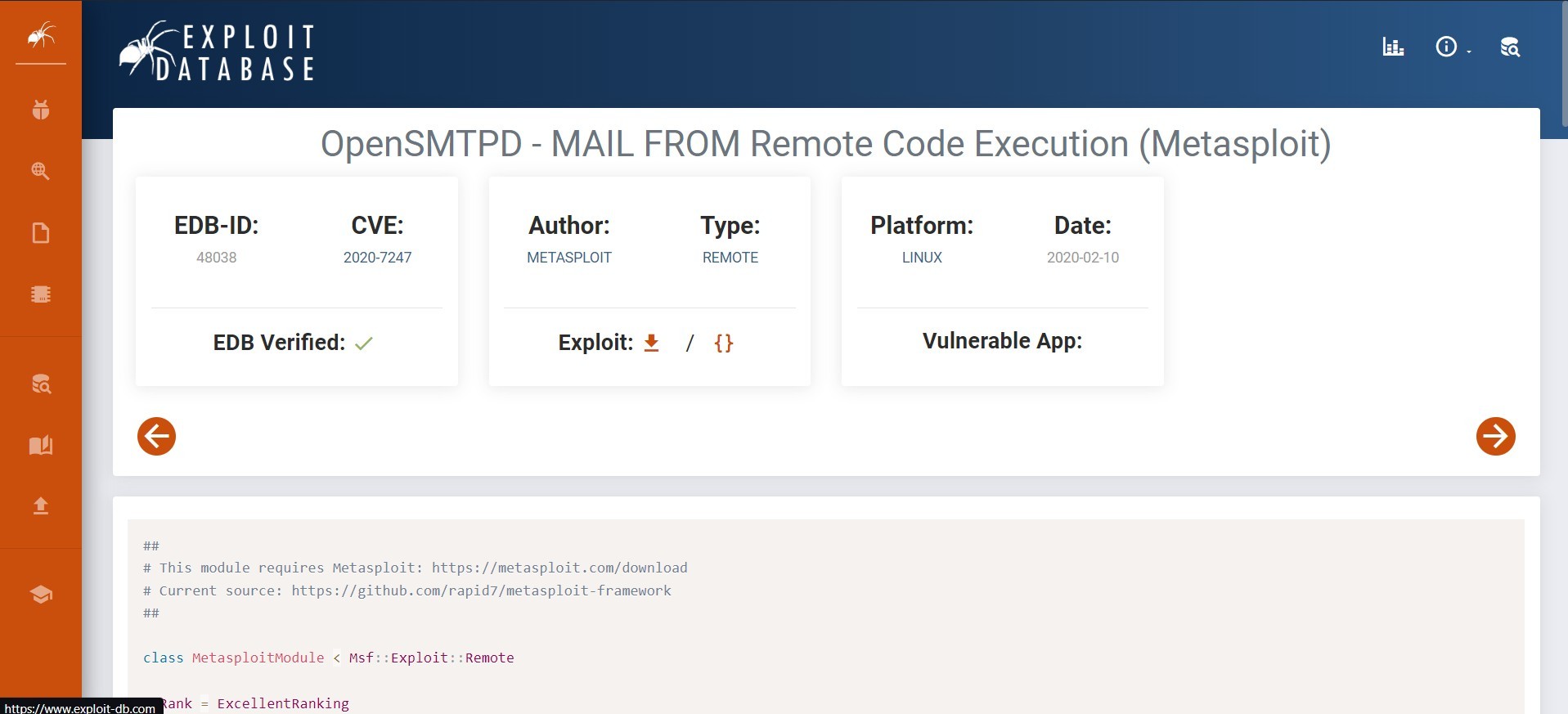
# Step 2: Dive into Exploit-DB

this is the home page of exploit db that lets us see all the exploits available

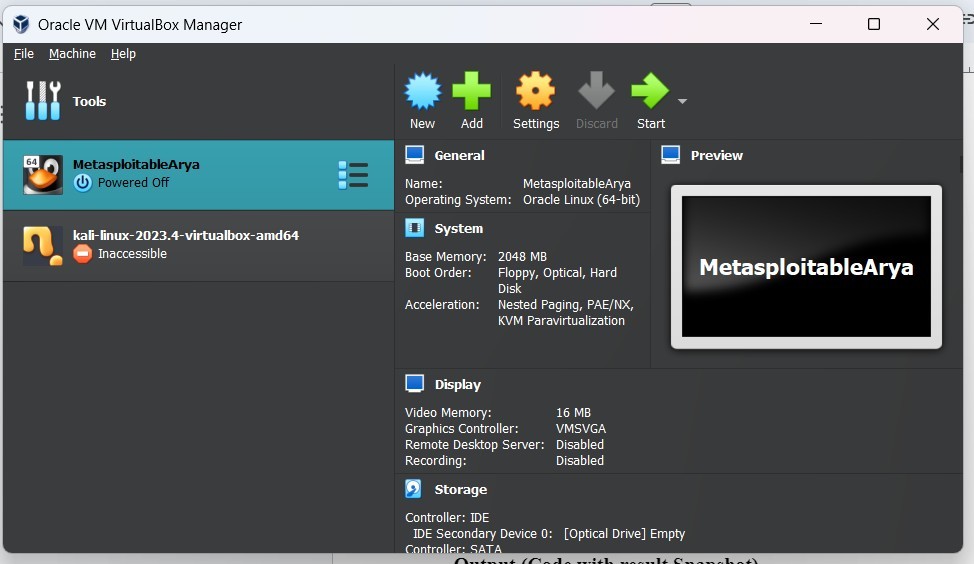


exploit db lets us add various filters depending upon the type, platform, author, port or look for any particular tag that you might be looking for

https://[www.exploit-db.com/exploits/48038](http://www.exploit-db.com/exploits/48038) look at this website to view the particular exploit which is about remote code execution which allows the attacker to send email



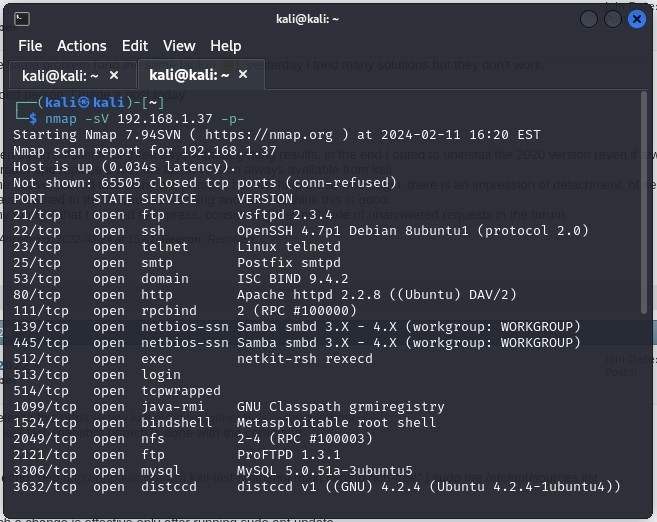
# Step 3: Set Up a Lab Environment

as the virtualbox already contains metasploitable we skip this step

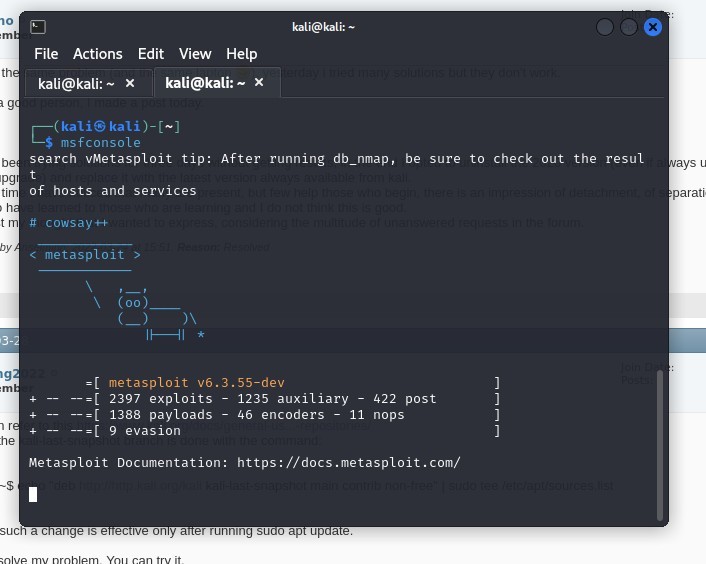
# Step 4: Experimentation on Metasploitable

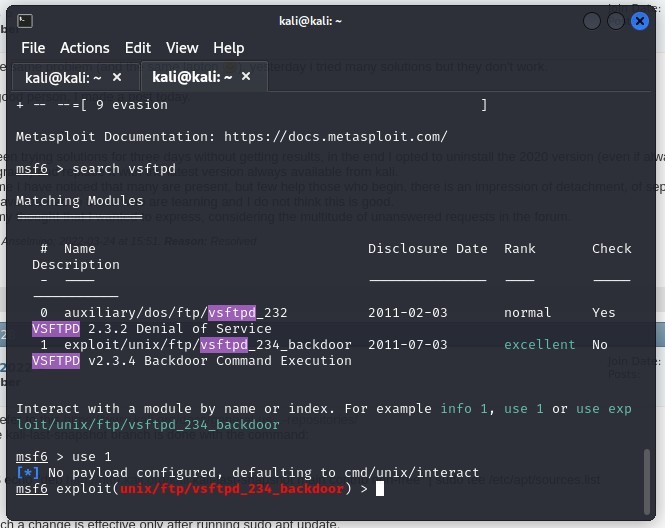
run ifconfig to get both the OS IP address

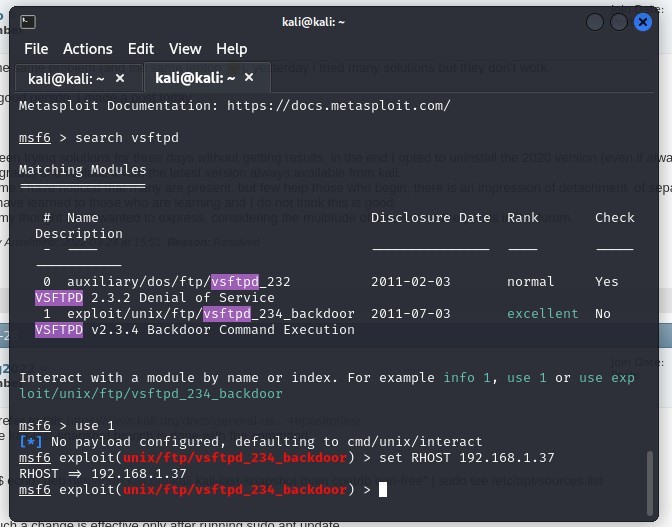
# Scanning metasploitable using nmap on kali

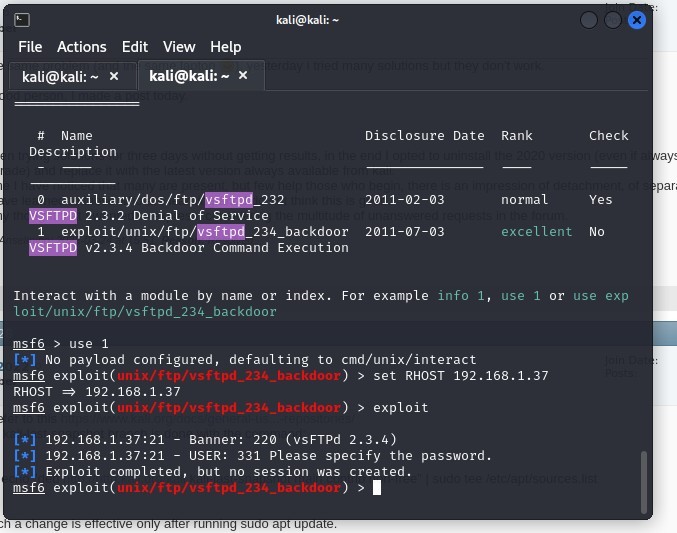


**Use metasploit framework to run attacks on metasploitable2**









# Post Lab Questions: -

1. Describe the process you followed to identify vulnerabilities on the Metasploitable virtual machine. Which tools did you use, and what specific vulnerabilities did you discover?

To identify vulnerabilities on the Metasploitable virtual machine, I followed these steps using various tools:

**Scanning with Nmap**:

I initiated a network scan using Nmap to identify open ports and services running on the Metasploitable VM.

Command: nmap -A <ip\_address>

**Exploitation using Metasploit**:

Based on the identified vulnerabilities, I searched for corresponding exploit modules in Metasploit. Command: search vsftpd

After finding relevant exploits, I configured and executed them against the vulnerable services on Metasploitable.

Manual Verification:

I manually verified the success of exploitation by observing any system changes, gaining unauthorized access, or retrieving sensitive information.

Specific vulnerabilities discovered during this process could include:

VSFTPD Backdoor Vulnerability (CVE-2011-2523): A backdoor was discovered in the VSFTPD version running on Metasploitable, allowing unauthorized access.

1. Evaluate the effectiveness of your documentation during and after the experiment. What details did you record, and how would this documentation aid in analysis, reporting, or future reference?

The documentation maintained throughout and after the experiment proved instrumental in evaluating the effectiveness of our vulnerability assessment and exploit experimentation. Recorded details included comprehensive descriptions of vulnerabilities identified, steps taken during exploitation attempts, screenshots or logs capturing the exploitation process, and outcomes observed. This documentation aids in thorough analysis by providing a clear trail of actions taken, facilitating root cause analysis in case of failures or unexpected results. Additionally, it serves as a foundation for reporting findings to stakeholders, ensuring transparency and clarity in communicating discovered vulnerabilities and associated risks. Furthermore, the documentation serves as a valuable resource for future reference, enabling the replication of experiments, refinement of methodologies, and continuous improvement in security practices.

# Outcomes: CO3 Understand attack methodology

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

**Understood various CWE and ran an exploit on metasploitable using metasploit**

# Signature of faculty in charge with date References:

1.https://[www.exploit-db.com/](http://www.exploit-db.com/) 2.https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

3.https://[www.hackers-arise.com/post/working-with-exploits-using-exploit-db-to-find-exploits](http://www.hackers-arise.com/post/working-with-exploits-using-exploit-db-to-find-exploits)