Exploit Vulnerabilities

**Task 1 – Introduction**

In this room, we are going to be going over some means of identifying vulnerabilities and coupling our research skills to learn how these can be abused.

Additionally, you will find some publicly available resources that are essential additions to your skill set and tools when performing vulnerability research and exploitation. You will then get to apply all of this into a practical challenge at the end of the room.

**Task 2 – Automated Vs. Manual Vulnerability Research**

There is a myriad of tools and services available in cybersecurity for vulnerability scanning. Ranging from being commercial (and footing a heavy bill) to open-source and free, vulnerability scanners are convenient means of quickly canvassing an application for flaws.



**Answer the question:**

1-You are working close to a deadline for your penetration test and need to scan a web application quickly. Would you use an automated scanner? (Yay/Nay)

Ans - Yah

2-You are testing a web application and find that you are able to input and retrieve data in a database. What vulnerability is this?

Ans- injection

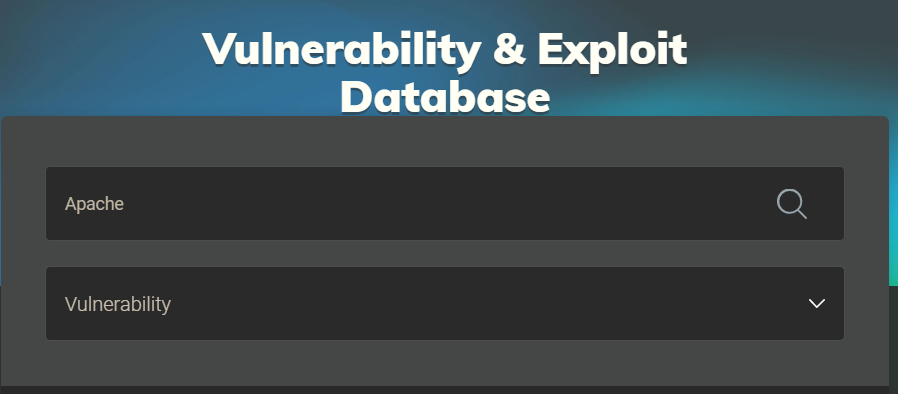
3-You manage to impersonate another user. What vulnerability is this?

Ans – broken access control

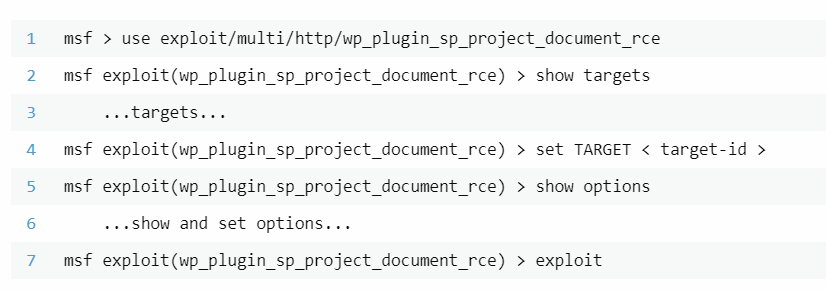
**Task 3 – Finding Manual Exploits**

**Rapid 7**

Much like other services such as Exploit DB and NVE, Rapid7 is a vulnerability research database. The only difference being that this database also acts as an exploit database. Using this service, you can filter by type of vulnerability (I.e. application and operating system).



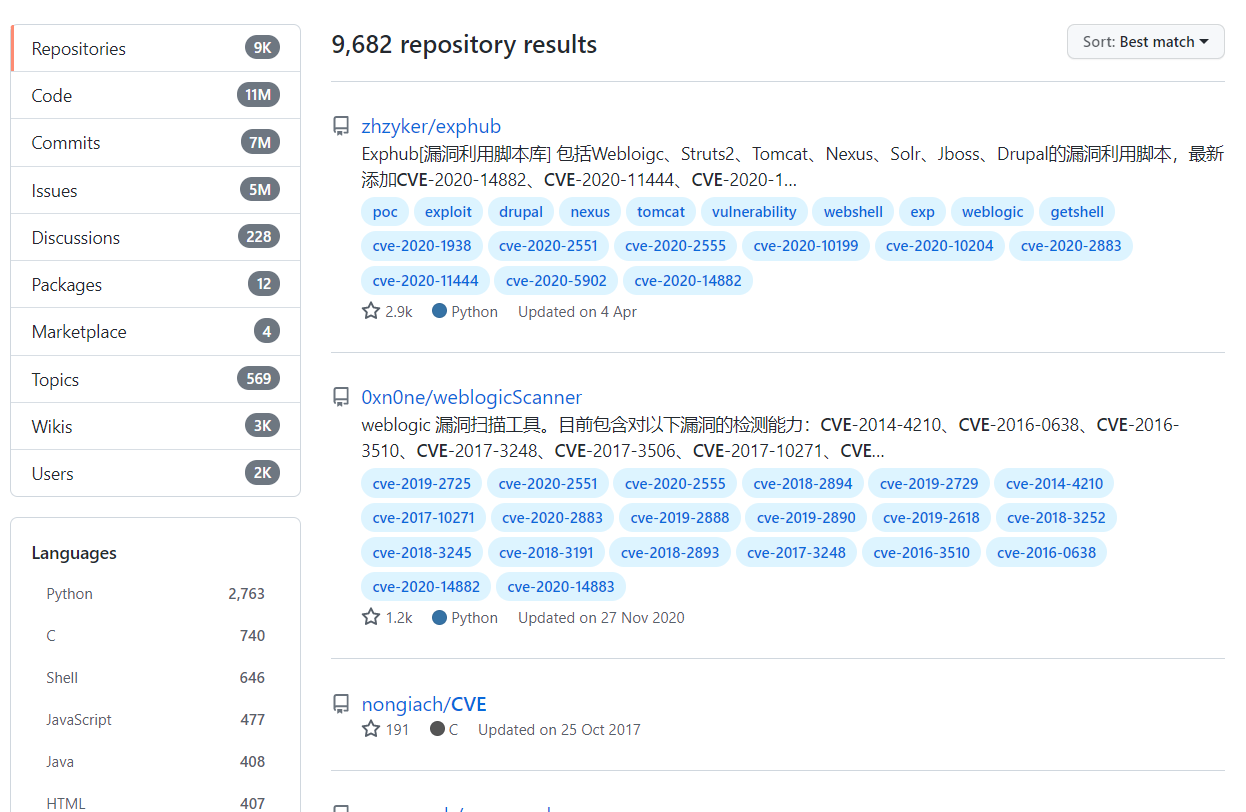
Additionally, the database contains instructions for exploiting applications using the popular Metasploit tool. For example, this entry on Rapid7 is for “Wordpress Plugin SP Project & Document”, where we can see instructions on how to use an exploit module to abuse this vulnerability.



**Github**

GitHub is a popular web service designed for software developers. The site is used to host and share the source code of applications to allow a collaborative effort. However, security researchers have taken to this platform because of the aforementioned reasons as well. Security researchers store & share PoC’s (Proof of Concept) on GitHub, turning it into an exploit database in this context.

GitHub is extremely useful in finding rare or fresh exploits because anyone can create an account and upload – there is no formal verification process like there is with alternative exploit databases. With that said, there is also a downside in that PoC’s may not work where little to no support will be provided.



GitHub uses a tagging and keyword system, meaning that we can search GitHub by keywords such as “PoC”, “vulnerability”, and many more. At the time of writing, there are 9,682 repositories with the keyword “cve”. We are also able to filter the results by programming language.

**Searchsploit**

Searchsploit is a tool that is available on popular pentesting distributions such as Kali Linux. It is also available on the TryHackMe AttackBox. This tool is an offline copy of Exploit-DB, containing copies of exploits on your system.

You are able to search searchsploit by application name and/or vulnerability type. For example, in the snippet below, we are searching searchsploit for exploits relating to Wordpress that we can use – no downloading necessary!

searchsploit wordpress

WordPress Theme Think Responsive 1.0 - Arbitr | php/webapps/29332.txt

WordPress Theme This Way - 'upload\_settings\_i | php/webapps/38820.php

WordPress Theme Toolbox - 'mls' SQL Injection | php/webapps/38077.txt

WordPress Theme Trending 0.1 - 'cpage' Cross- | php/webapps/36195.txt

WordPress Theme Uncode 1.3.1 - Arbitrary File | php/webapps/39895.php

**Answer the question:**

1 – What website would you use as a security researcher if you want to upload a Proof of concept?

Ans – github

2 – You are performing a penetration test at a site with no internet connection. What tool could you use to find exploit to use?

Ans – searchsploit

**Task 4 – Example of Manual Exploitation**

We can use the information gathered from task 2 in this room to exploit the vulnerable service. Ultimately, one of the most effective vulnerabilities that we can exploit is the ability to execute commands on the target that is running the vulnerable application or service.

For example, being able to execute commands on the target that is running the vulnerable application or service will allow us to read files or execute commands that we previously wouldn’t be able to perform using the application or service alone. Additionally, we can abuse this to gain what is known as a foothold to the machine. A foothold is an access to the vulnerable machine’s console, where we can then begin to exploit other applications or machines on the network.

**Task 5 – Practical: Manual Exploitation**

1 - Find out the version of the application that is running. What are the name and version number of the application?

Ans – Online Book store v1.0 #you can find this web page

2 - Now use the resources and skills from this module to find an exploit that will allow you to gain remote access to the vulnerable machine.

3 - Use this exploit against the vulnerable machine. What is the value of the flag located in a web directory?

Ans - THM{BOOK\_KEEPING} # Search on Exploit-DB that Book store online 1.0 – Then you got a RCE file download it, and run python3 file.py [URL]