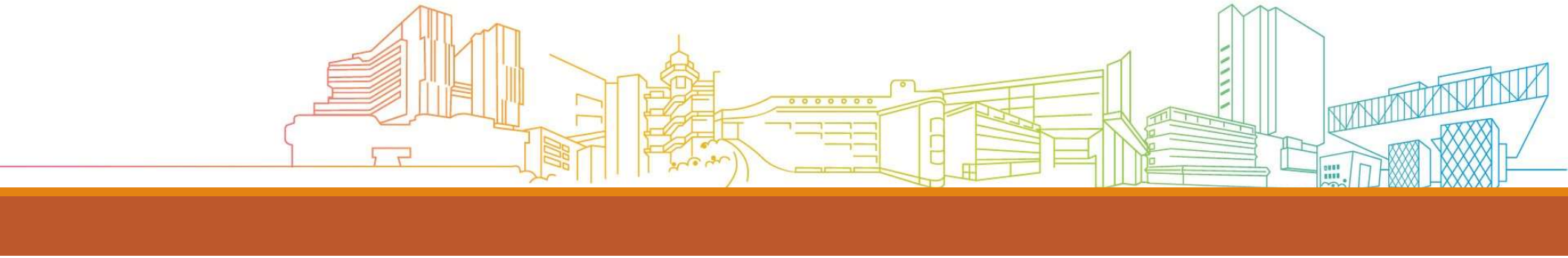
HKIIT x EDB Cybersecurity Seminar 2023

Common Web Vulnerabilities and Data Leak Identification



Event Type	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	quarter-to-quarter
Defacement	118	113	249	233	69	-70.4%
Phishing	5,033	7,141	13,574	2,804	1,120	-60.1%
Botnet (Bots)	3,642	3,684	2,285	2,583	2,227	-13.8%
Total	8,793	10,938	16,108	5,620	3,416	-39.2%

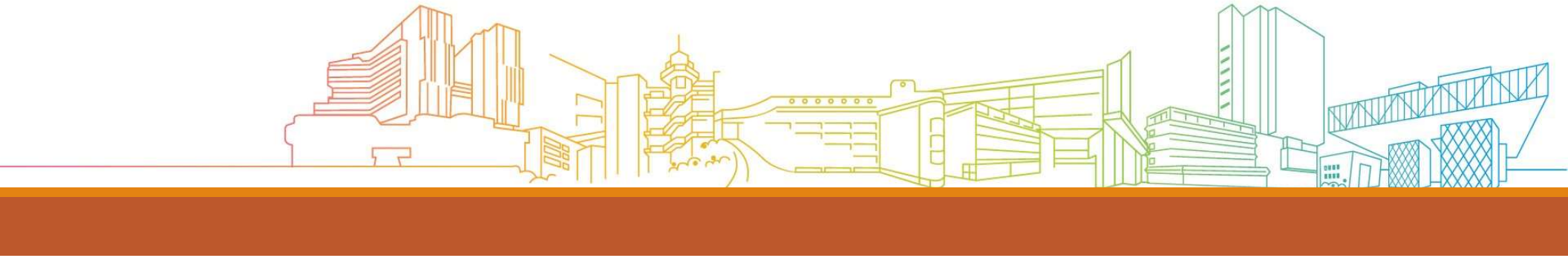
OWASP Top 10 (2021)

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- N) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- N) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://owasp.org/www-project-top-ten/



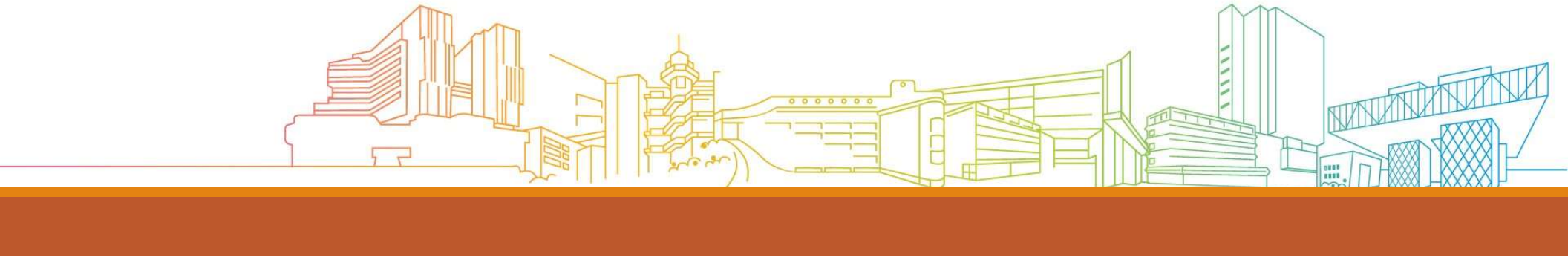
Agenda

Hacking with Search Engines

Data Leaking Market

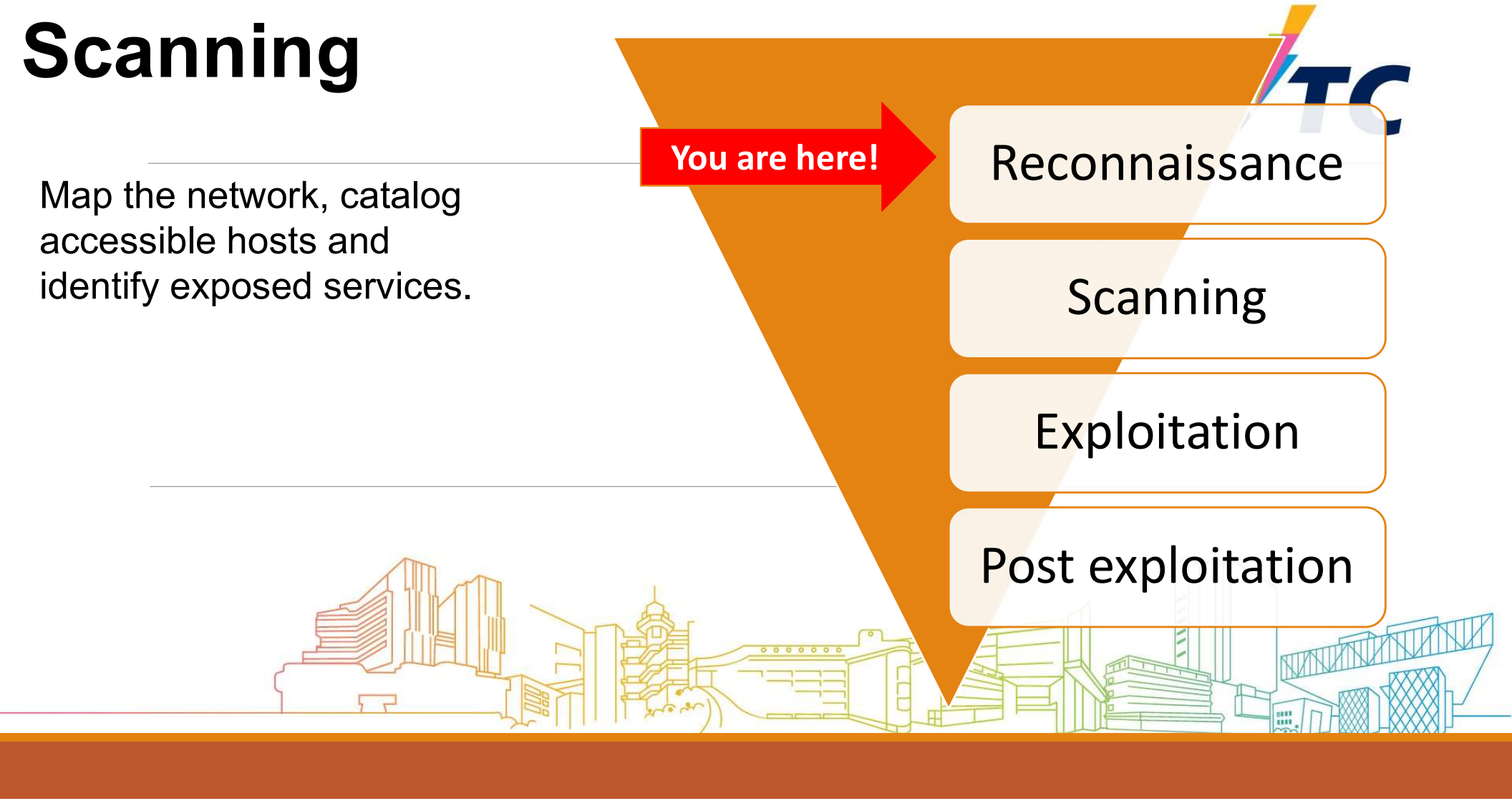
In-Service Training

Hands-On Lab (Onsite Only)



Scanning

Map the network, catalog accessible hosts and identify exposed services.

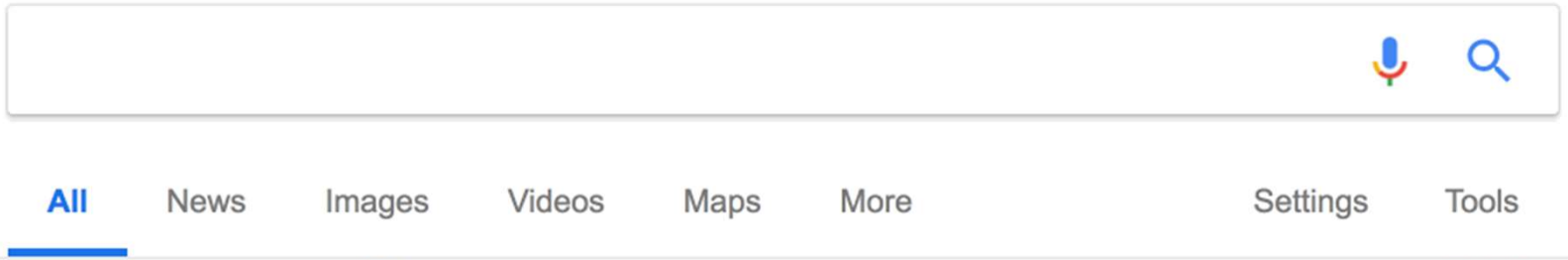


Search Command

Search engine commands (特定搜索指令)

Complex search queries (運算符號)

List : https://ahrefs.com/blog/google-advanced-search-operators/



http://index-of.co.uk/Google/Google-Hacking-by-Ali-Jahangiri.pdf

Command : filetype

Search for any kind of file **extensions(副檔名)** ,

- e.g. :Excel = filetype: xlsx

Stored **passwords** in a single file on public internet

https://securitytrails.com/blog/google-hacking-techniques

Search : password filetype:xlsx

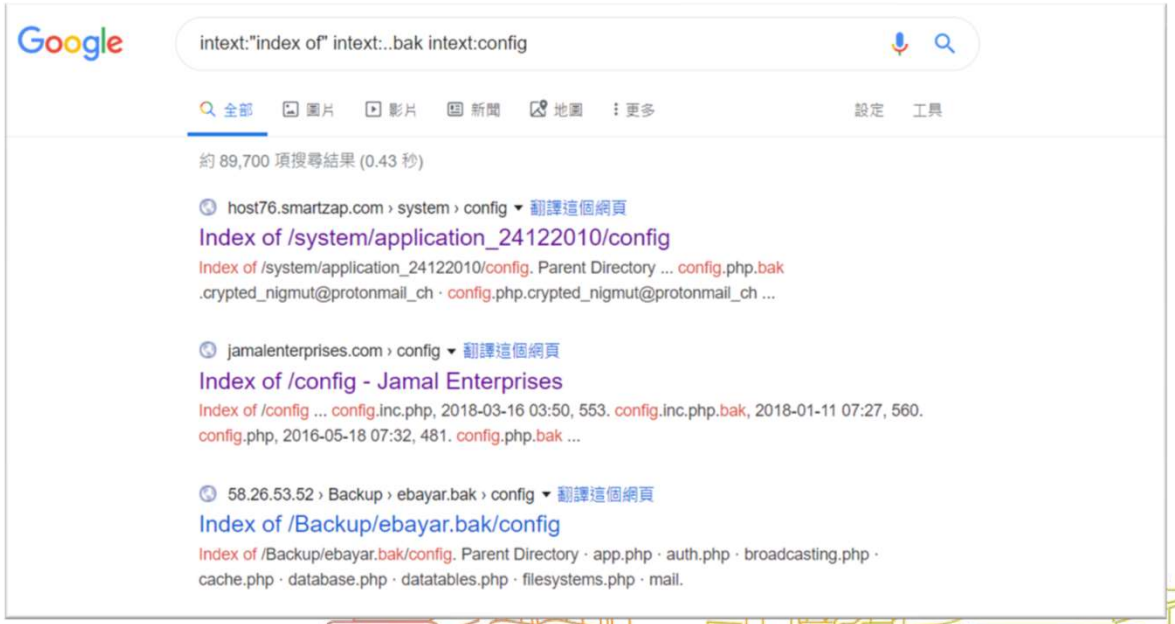
Command : intext

intext: useful to **locate pages** that contain certain characters or strings **inside their text (**於顯示文字中搜索特定字眼**)**

Version number / software / feature name

https://securitytrails.com/blog/google-hacking-techniques

Command : intext:"index of" intext:..bak intext:config

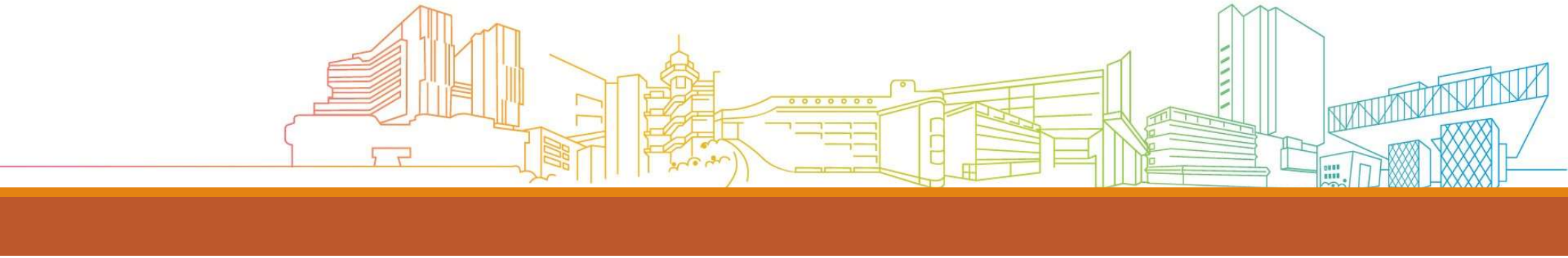


Improper "Directory Listing" configuration

Command – site : Filter for limiting the searching scope by the domain

https://medium.com/@cuncis/google-dork-cheat-sheet-for-finding-hidden-admin-panels-379e3414d486

intitle:”admin login” site:example.com — This searches for pages with “admin login” in the title of the page on a specific website



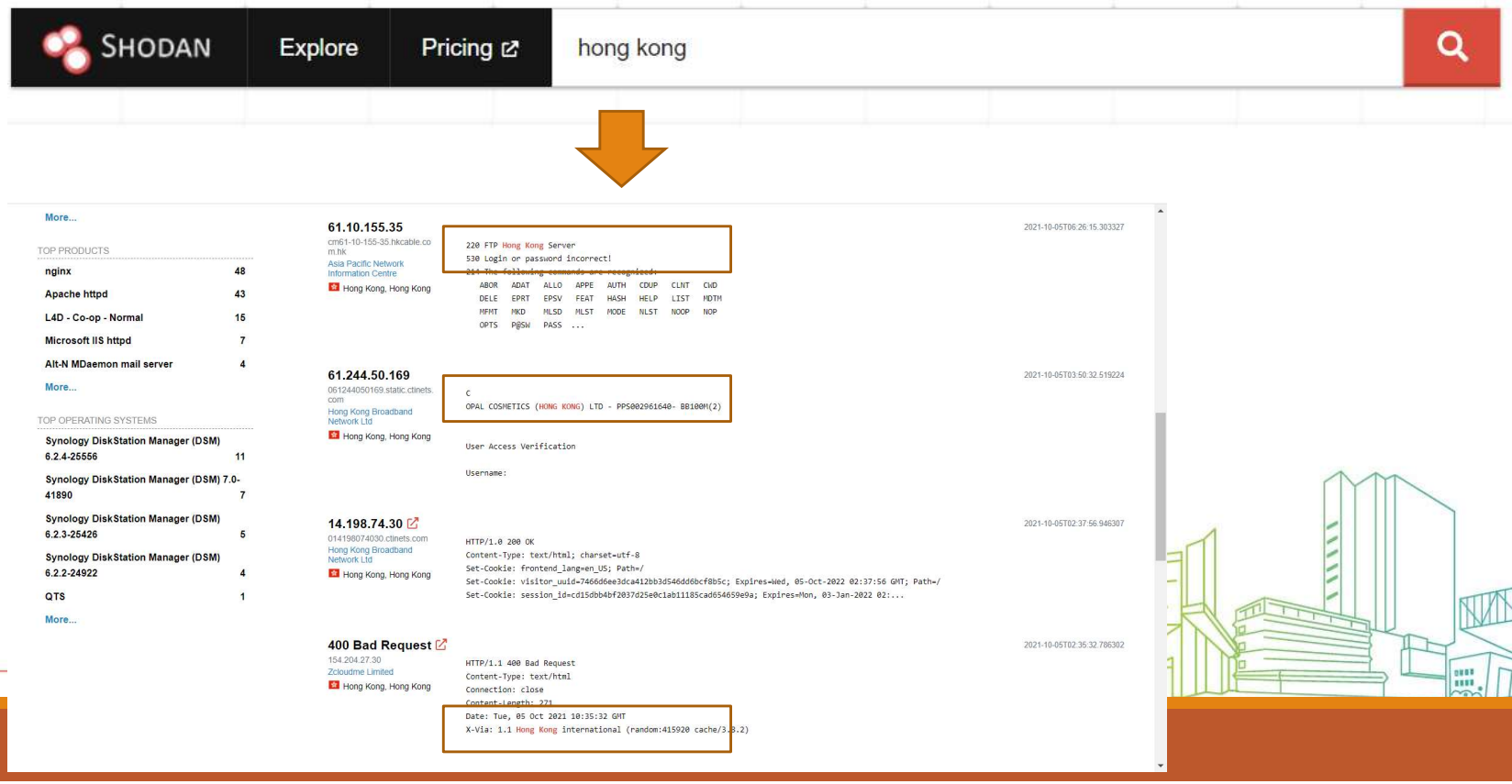
https://www.exploit-db.com/google-hacking-database

Google Hacking Database

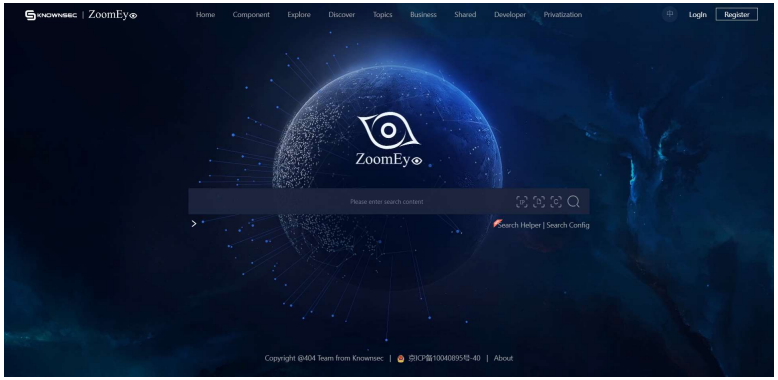
Show 15

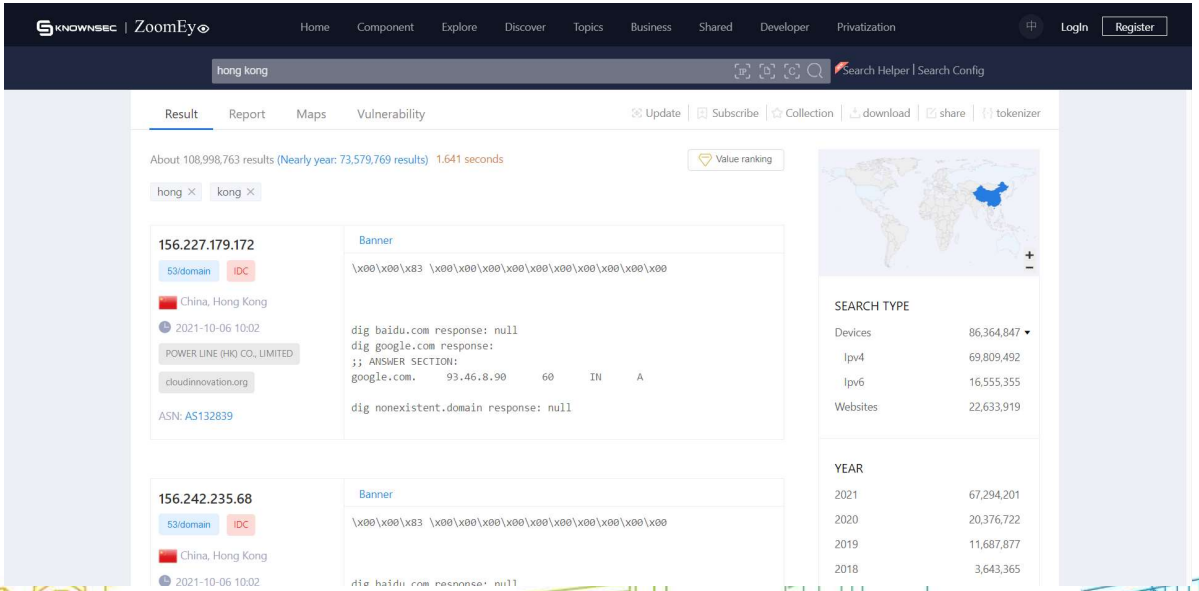
Date Added	Dork
2023-10-16	intitle:"Index of" inurl:/backup/ "wp-config"
2023-10-02	intitle:"index of" "backup.zip"
2023-05-26	intitle:"Index of" inurl:/backup/ "admin.zip"
2023-05-26	Re: "index of /backup.sql
2023-05-05	inurl:"wp-content" intitle:"index.of" intext:backup"
2023-04-20	intext:"Index of" intext:"backup.tar"
2023-02-22	inurl:backup filetype:sql
2022-06-16	intitle:index of /backup private
2022-06-15	=?UTF-8?Q?=E2=80=9CIndex_of_/backup=E2=80=9D?=
2021-11-08	intitle:"database" "backup" filetype:sql
2021-10-28	intitle:"index of" "/backup/sql"
2021-10-13	intitle: "index of" "admin" "/backup"
2021-10-06	intitle: "index of backup.xml"
2021-10-06	intitle: "index of backup.php"
2021-05-21	intitle:"Server Backup Manager SE"

https://www.shodan.io/



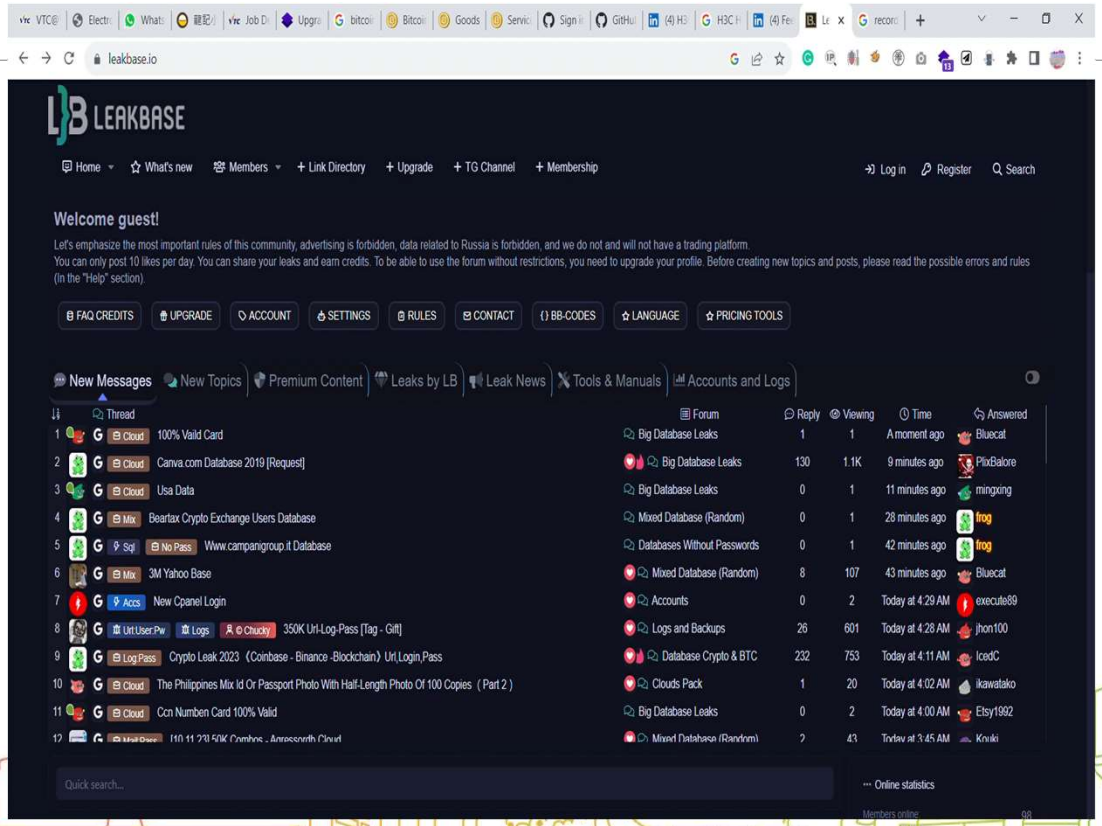
https://www.zoomeye.org/



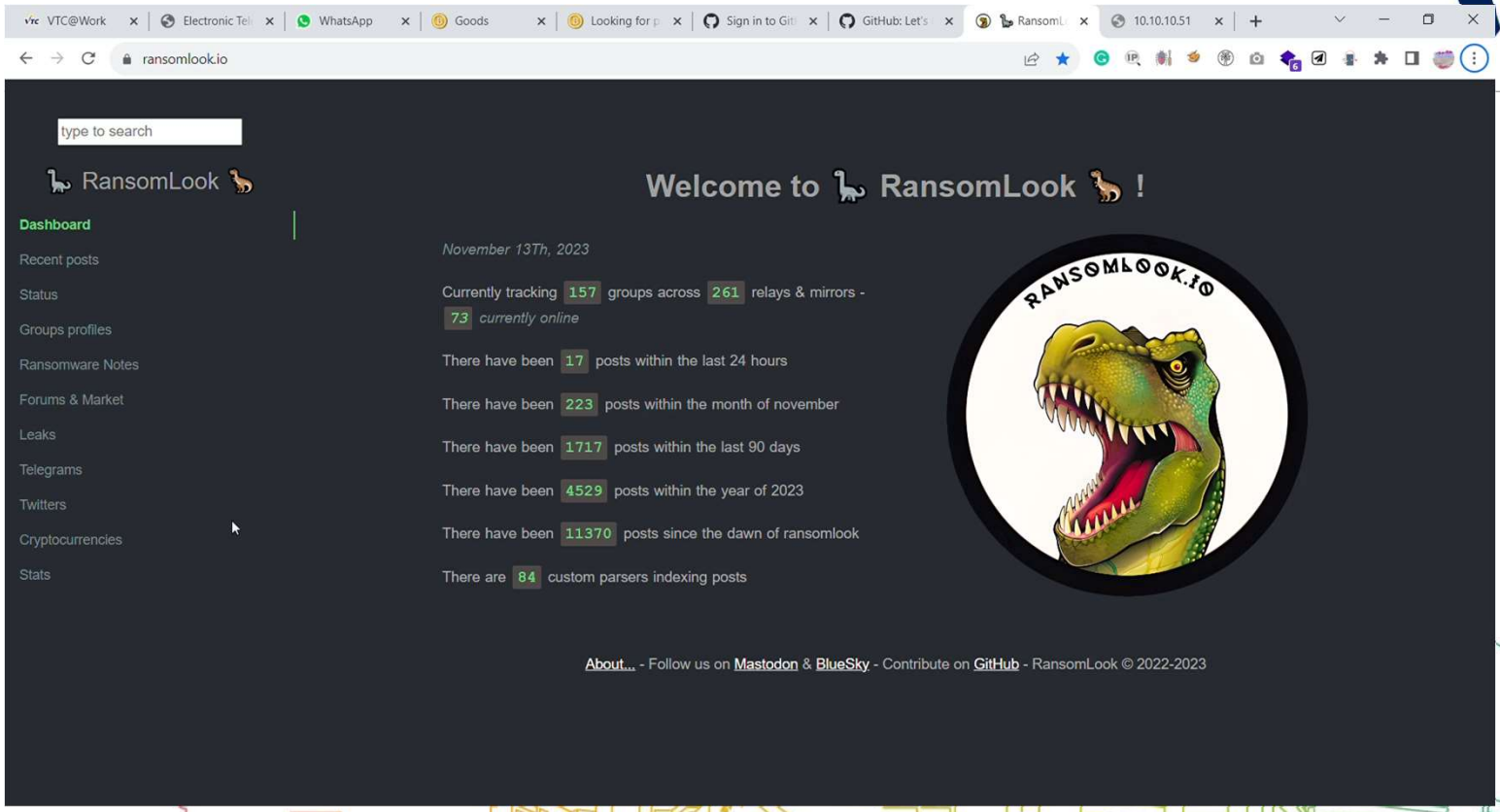


https://ivre.rocks/#in-a-nutshell

Black Market



https://www.ransomlook.io/leaks



Solution?

Access control to the System management page / the page content (Server settings / Application-level controls)

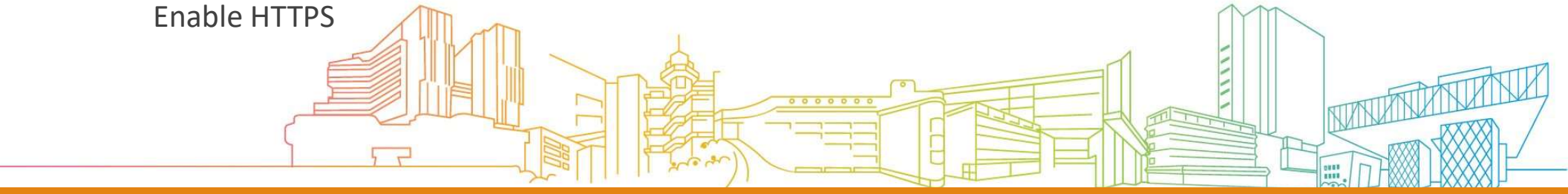
Using VPN / SSL VPN to access internal resource (Intranet)

Apply 2-Factor Authentication

Also….

Keeps update the system

Enable HTTPS

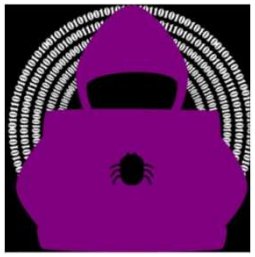


Cybersecurity Centre

- Cyber Range
- Penetration testing Lab
- Malware Analysis Lab

Facilities

CyberRange



Purple Team Training System

SIEM

Malware Analysis and Reverse Engineering Tools

Hardware Security Training Kit

Targets

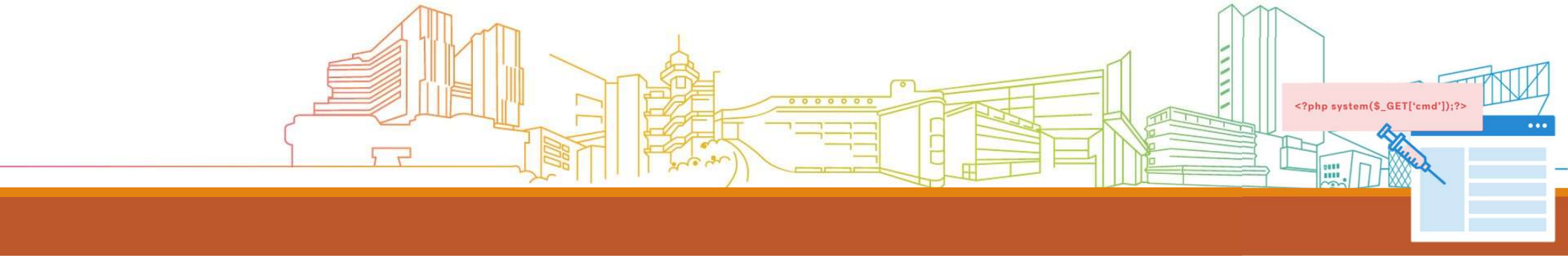
Competitions
Events
Workshops
Taster Programmes

Professional Courses

Raise public awareness of cybersecurity

The Lab for Today

1. Scan the targeted hosts for available ports
2. Discover the services running on the server
3. Find the vulnerabilities on the running web pages
4. Injection the backdoor by using the vulnerabilities found
5. Accessing to the backdoor and run the malicious commands



Certificate in Web Application Penetration Testing

Certificate in Web Application Penetration Testing

IVE - Information Technology

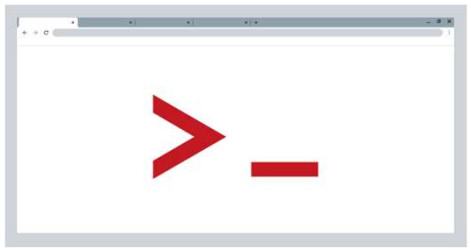
IVE

Overview

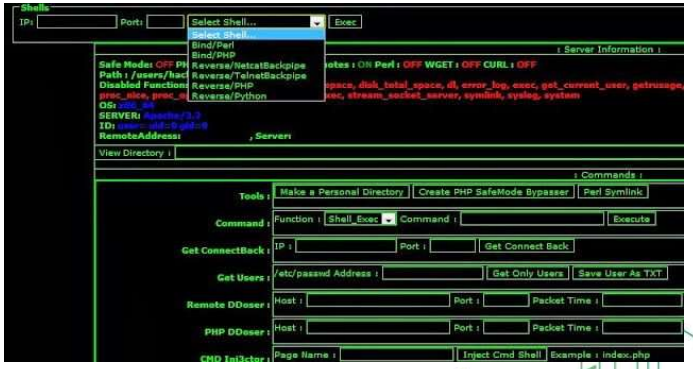
Programme Code	IT524055Q	QF Level	4
Subject Area	Information Technology	QF Credits	30
Programme Type	Certificate	QF Registration No.	22/000203/L4
Offering Institution	IVE - Information Technology	QF Registration Validity Period	2022.09.01-2026.08.31
Contact Hours	60		
Duration	60 Hour(s)		

https://cpe.vtc.edu.hk/en/admission/programmes/%E7%B6%B2%E9%A0%81%E7%A8%8B%E5%BC%8F%E6%BB%B2%E9%80%8F%E6%B8%AC%E8%A9%A6%E8%AD%89%E6%9B%B8/IT524055Q/1

Web Shell



A Web shell is a script that can be uploaded to a web server that **enables remote administration** of the machine. A web shell can be written in any language that the target web server supports.



https://simple.wikipedia.org/wiki/Web_shell

Using the features (weakness) of PHPMyAdmin to inject the PHP codes into the webserver.

Accessing the injected backdoor page to run malicious commands