

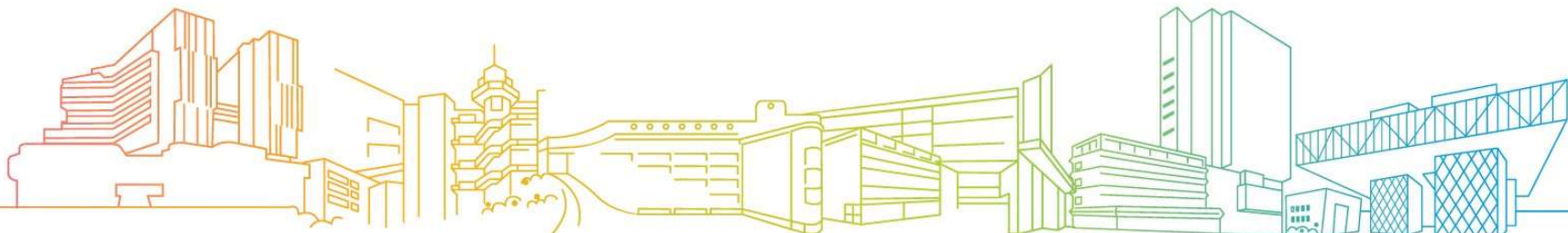


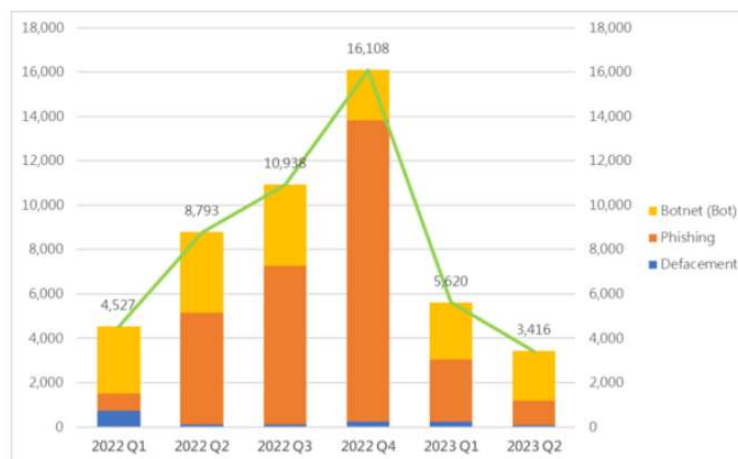
HKIIT x EDB Cybersecurity Seminar 2023

---

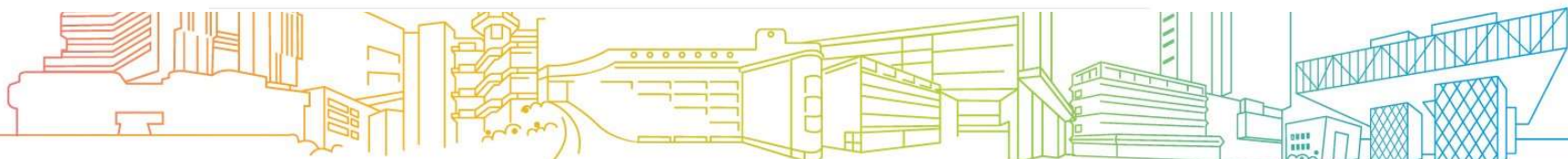
# Common Web Vulnerabilities and Data Leak Identification

---





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%
<b>Total</b>	<b>8,793</b>	<b>10,938</b>	<b>16,108</b>	<b>5,620</b>	<b>3,416</b>	<b>-39.2%</b>





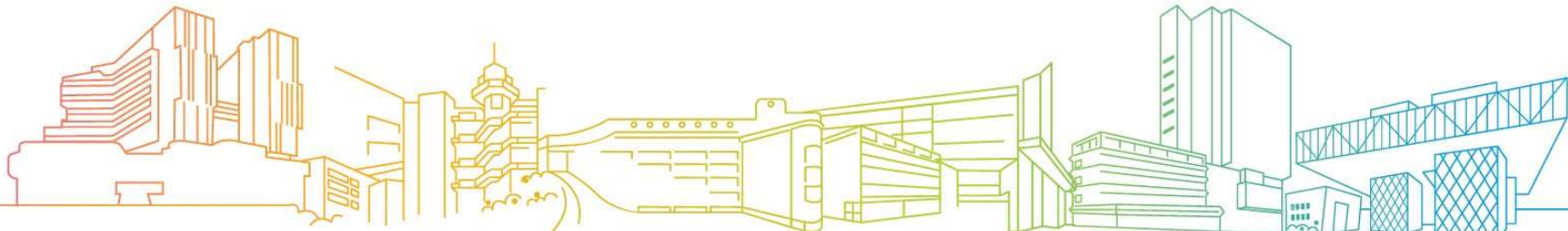
# OWASP Top 10 (2021)

2021

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- ➔ A06:2021-Vulnerable and Outdated Components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

\* From the Survey

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





# Agenda

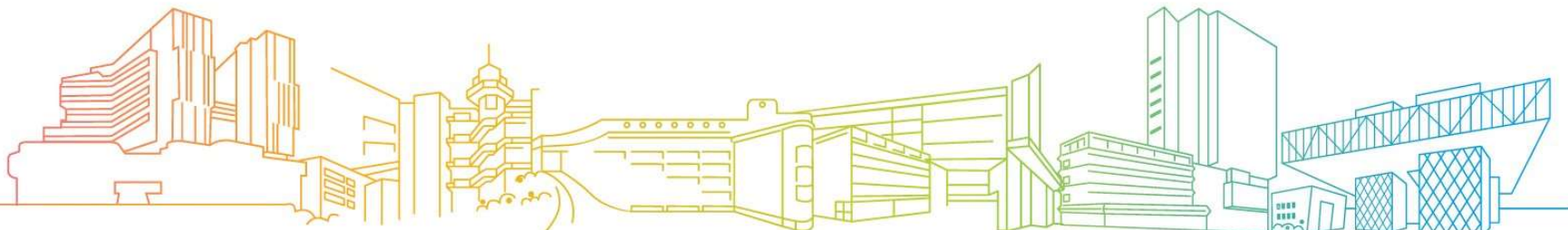
---

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.

You are here!

Reconnaissance

Scanning

Exploitation

Post exploitation

TC





# 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/>

**All**

News

Images

Videos

Maps

More

Settings

Tools

<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



password filetype:xlsx

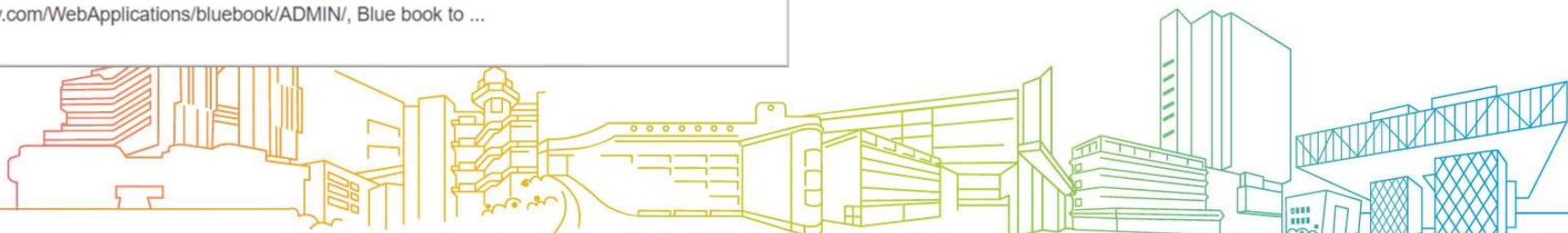
全部 圖片 影片 新聞 地圖 更多 設定 工具

約 23,600 項搜尋結果 (0.37 秒)

wikileaks.org › sony › docs › bonus › Password › radh... XLS 翻譯這個網頁

[radha passwords.xlsx - WikiLeaks](#)

26, spe support password --- BRa9ucus. 27, Techline no----791243265. 28. 29,  
http://screenland.spe.sony.com/WebApplications/bluebook/ADMIN/, Blue book to ...







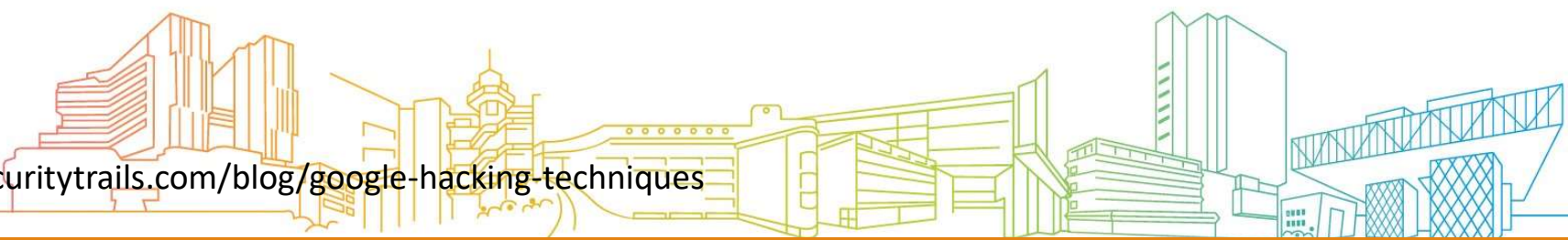
# Command : intext

---

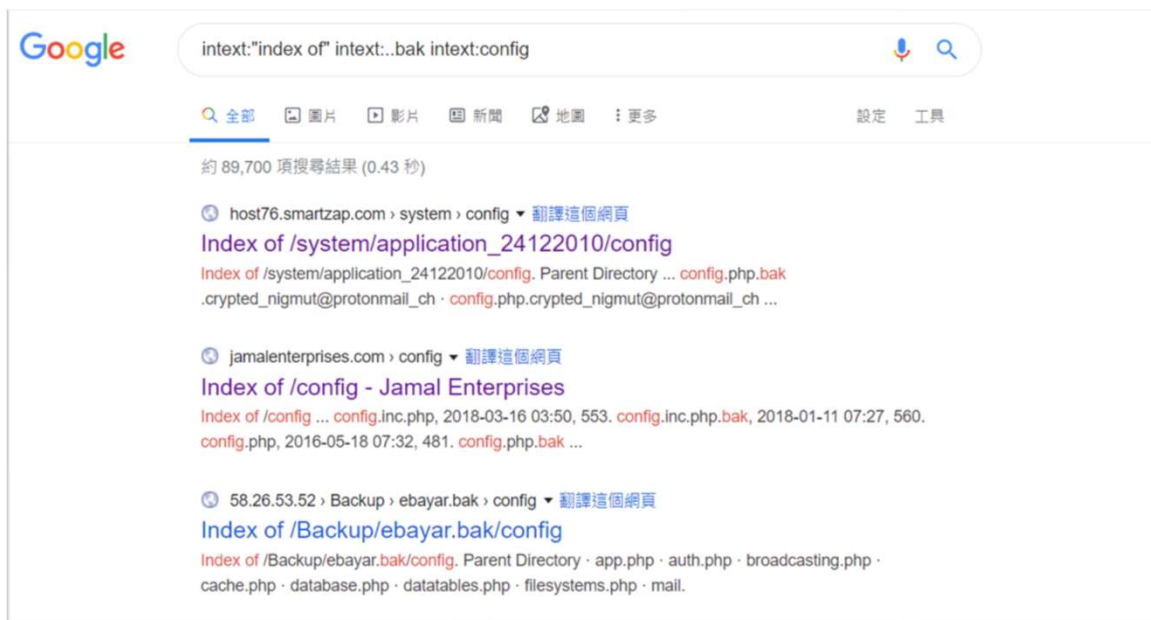
intext: useful to **locate pages** that contain certain characters or strings **inside their text** (於顯示文字中搜索特定字眼)

Version number / software / feature name

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



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



Improper "Directory Listing" configuration

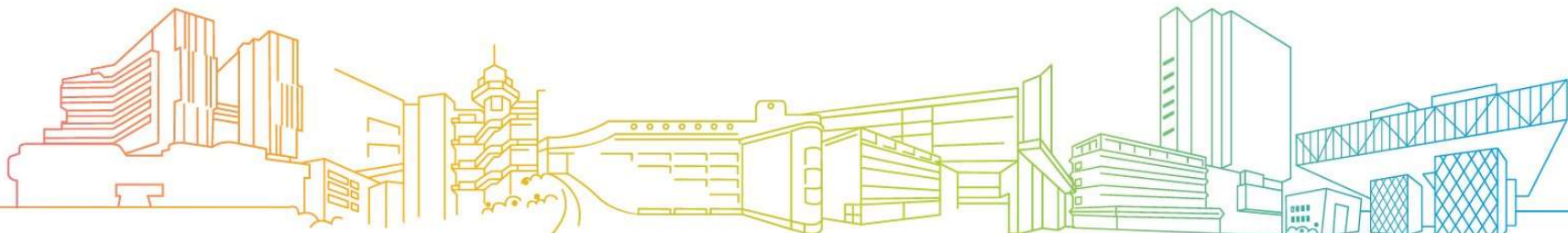




## Command – site : Filter for limiting the searching scope by the domain

<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/



SHODAN Explore Pricing [hong kong](#)



More...

TOP PRODUCTS

nginx	48
Apache httpd	43
L4D - Co-op - Normal	15
Microsoft IIS httpd	7
Alt-N MDAemon mail server	4

More...

TOP OPERATING SYSTEMS

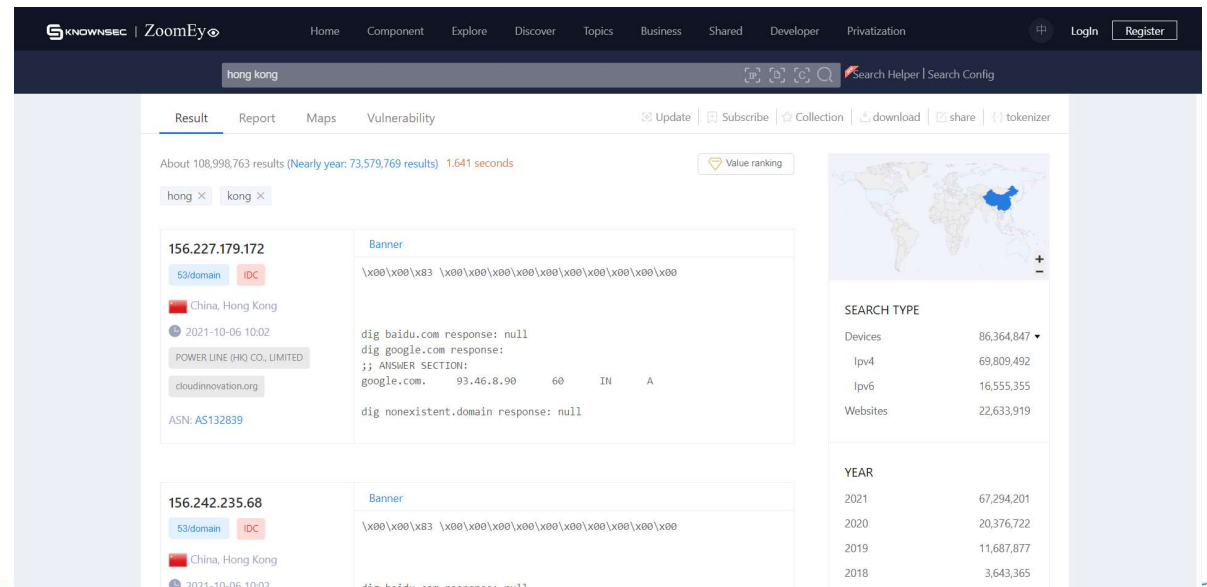
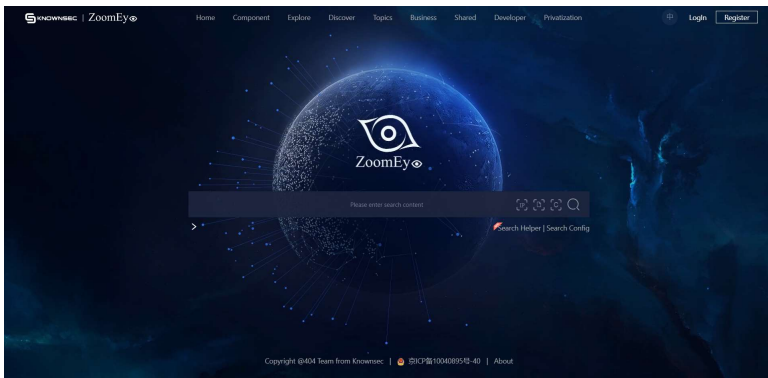
Synology DiskStation Manager (DSM) 6.2.4-25556	11
Synology DiskStation Manager (DSM) 7.0-41890	7
Synology DiskStation Manager (DSM) 6.2.3-26426	5
Synology DiskStation Manager (DSM) 6.2.2-24922	4
QTS	1

More...

<b>61.10.155.35</b> cn61-10-155-35.hkccable.com Asia Pacific Network Information Centre Hong Kong, Hong Kong	<pre>220 FTP Hong Kong Server 530 Login or password incorrect! 421 The following commands are recognized: ABOR ADAT ALLO APPE AUTH CDUP CLNT CMD DELE EPRT EPSV FEAT HASH HELP LIST MDTM MHPT MKD MLSD MLST MODE NLST NOOP NOP OPTS PqSW PASS ...</pre>	2021-10-05T06:26:15.303327
<b>61.244.50.169</b> 061244050169.static.ctinets.com Hong Kong Broadband Network Ltd Hong Kong, Hong Kong	<pre>C OPAL COSMETICS (HONG KONG) LTD - PPS002961640- BB100H(2)  User Access Verification  Username:</pre>	2021-10-05T03:50:32.519224
<b>14.198.74.30</b> 014198074030.ctinets.com Hong Kong Broadband Network Ltd Hong Kong, Hong Kong	<pre>HTTP/1.0 200 OK Content-Type: text/html; charset=utf-8 Set-Cookie: frontend_lang=en_US; Path=/ Set-Cookie: visitor_uid=7466d6ee3dca412bb3d5464dd6bcf8b5c; Expires=Wed, 05-Oct-2022 02:37:56 GMT; Path=/ Set-Cookie: session_id=cd15dbb4bf2837d25e0c1ab11185ca0654659e9a; Expires=Mon, 03-Jan-2022 02:...</pre>	2021-10-05T02:37:56.946307
<b>400 Bad Request</b> 154.204.27.30 Zcloudme Limited Hong Kong, Hong Kong	<pre>HTTP/1.1 400 Bad Request Content-Type: text/html Connection: close Content-Length: 271  Date: Tue, 05 Oct 2021 10:35:32 GMT X-Via: 1.1 Hong Kong International (random:415920 cache/3.3.2)</pre>	2021-10-05T02:35:32.786302



https://www.zoomeye.org/



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



# Black Market



The screenshot shows the Leakbase website interface. At the top, there is a navigation bar with links for Home, What's new, Members, Link Directory, Upgrade, TG Channel, and Membership. Below this is a 'Welcome guest!' message with a disclaimer and a list of utility buttons like 'FAQ CREDITS', 'UPGRADE', 'ACCOUNT', 'SETTINGS', 'RULES', 'CONTACT', 'BB-CODES', 'LANGUAGE', and 'PRICING TOOLS'. The main content area is divided into 'New Messages' and 'New Topics'. The 'New Messages' section lists 12 items, including '100% Valid Card', 'Carva.com Database 2019 [Request]', 'Usa Data', 'Bearfax Crypto Exchange Users Database', 'Www.campanigroup.it Database', '3M Yahoo Base', 'New Cpanel Login', '350K Uti-Log-Pass [Tag - Git]', 'Crypto Leak 2023 (Coinbase - Binance - Blockchain) Uti/Login/Pass', 'The Philippines Mix Id Or Passport Photo With Half-Length Photo Of 100 Copies (Part 2)', 'Ccn Numben Card 100% Valid', and '110 11 270 50K Cnmbne - Amreconth Cloud'. The 'New Topics' section shows a list of forum topics with columns for Forum, Reply, Viewing, Time, and Answered. Topics include 'Big Database Leaks', 'Mixed Database (Random)', 'Databases Without Passwords', 'Accounts', 'Logs and Backups', 'Database Crypto & BTC', 'Clouds Pack', and 'Mixed Database (Random)'. At the bottom, there is a search bar and 'Online statistics'.

https://www.ransomlook.io/leaks



The screenshot shows a web browser window with the URL [ransomlook.io](https://www.ransomlook.io). The browser's address bar and tabs are visible at the top. The website's main content area has a dark background and includes a search bar at the top left with the placeholder text "type to search". Below the search bar is the RansomLook logo, which features a small dinosaur icon and the text "RansomLook".

The main heading reads "Welcome to RansomLook!". To the right of this heading is a large circular logo featuring a detailed illustration of a green and yellow T-Rex's head with its mouth open, showing sharp teeth. The text "RANSOMLOOK.IO" is written in a white, sans-serif font along the top inner edge of the circle.

On the left side of the dashboard, there is a vertical navigation menu with the following items: "Dashboard" (highlighted in green), "Recent posts", "Status", "Groups profiles", "Ransomware Notes", "Forums & Market", "Leaks", "Telegrams", "Tweets", "Cryptocurrencies", and "Stats".

The main content area displays statistics for November 13th, 2023:

- Currently tracking **157** groups across **261** relays & mirrors - **73** currently online
- There have been **17** posts within the last 24 hours
- There have been **223** posts within the month of november
- There have been **1717** posts within the last 90 days
- There have been **4529** posts within the year of 2023
- There have been **11370** posts since the dawn of ransomlook
- There are **84** custom parsers indexing posts

At the bottom of the dashboard, there is a footer with the text: "About... - Follow us on Mastodon & BlueSky - Contribute on GitHub - RansomLook © 2022-2023".







# Solution?

---

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

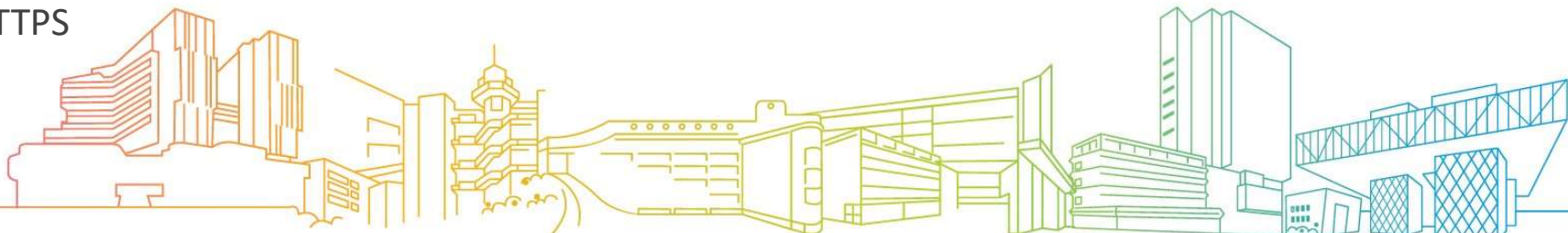
Using VPN / SSL VPN to access internal resource (Intranet)

Apply 2-Factor Authentication

Also....

Keeps update the system

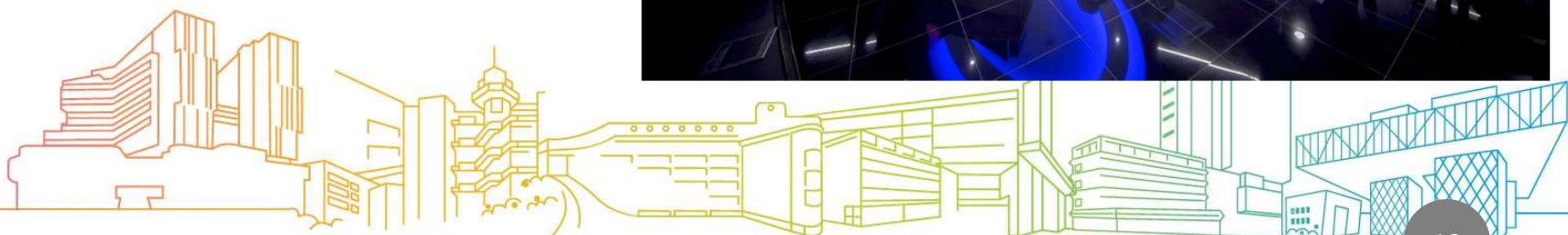
Enable HTTPS



# Cybersecurity Centre



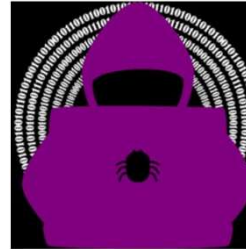
- Cyber Range
- Penetration testing Lab
- Malware Analysis Lab



# Facilities



CyberRange



Purple Team Training System

SIEM



Malware Analysis and Reverse Engineering Tools



Hardware Security Training Kit



# Targets

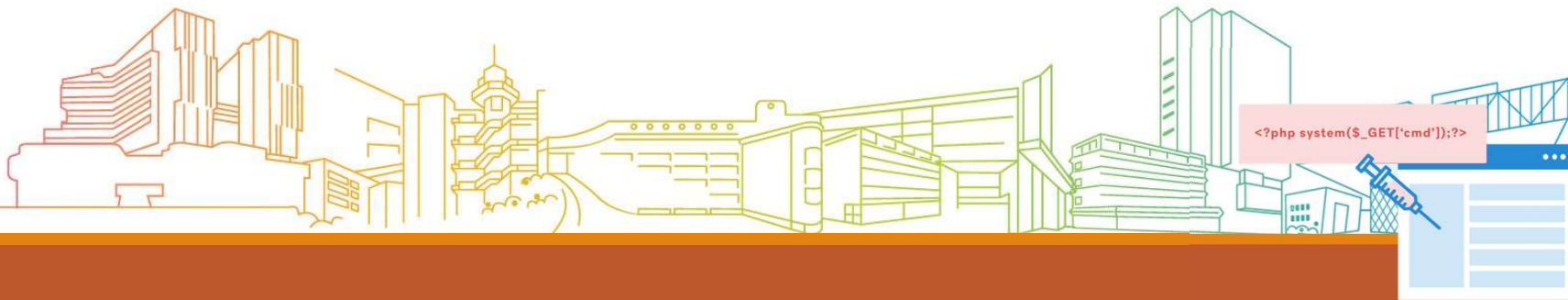


# The Lab for Today

---



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



### 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)		

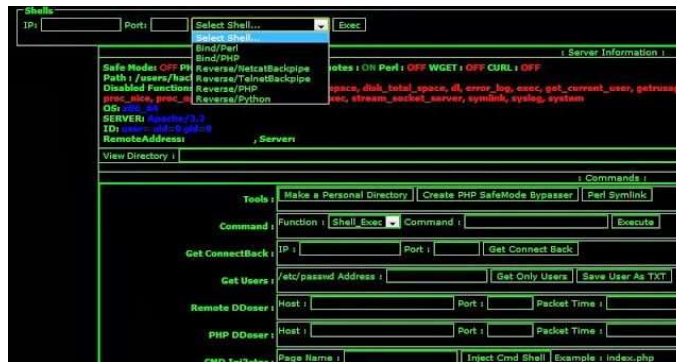
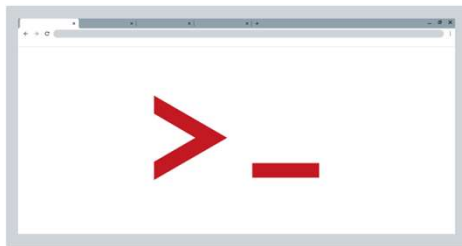
<https://cpe.vtc.edu.hk/en/admission/programmes/%E7%B6%B2%E9%A0%81%E7%A8%8B%E5%BC%8F%E6%BB%B2%E9%80%8F%E6%B8%AC%E8%A9%A6%E8%AD%89%E6%9B%B8/IT524055Q/1>



# 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](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

