進攻就係最好概防守
An Attack is the Best to Defence

Presented by MC Lam

Why do you need to attack a WordPress?

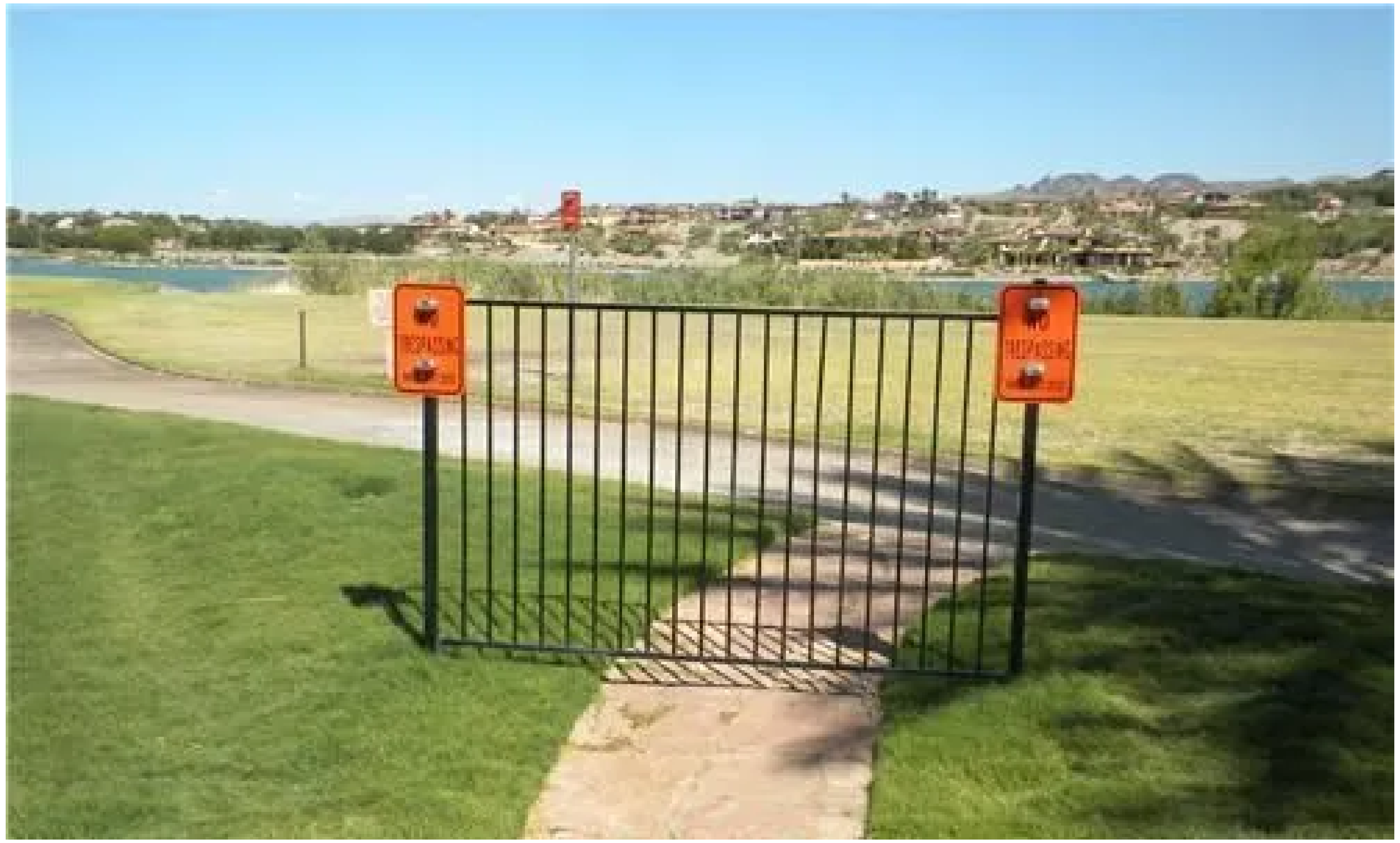
Why?

01. Compliance Requirement: To perform Formal pentest

02. New Hong Kong ordinance requirement (?)

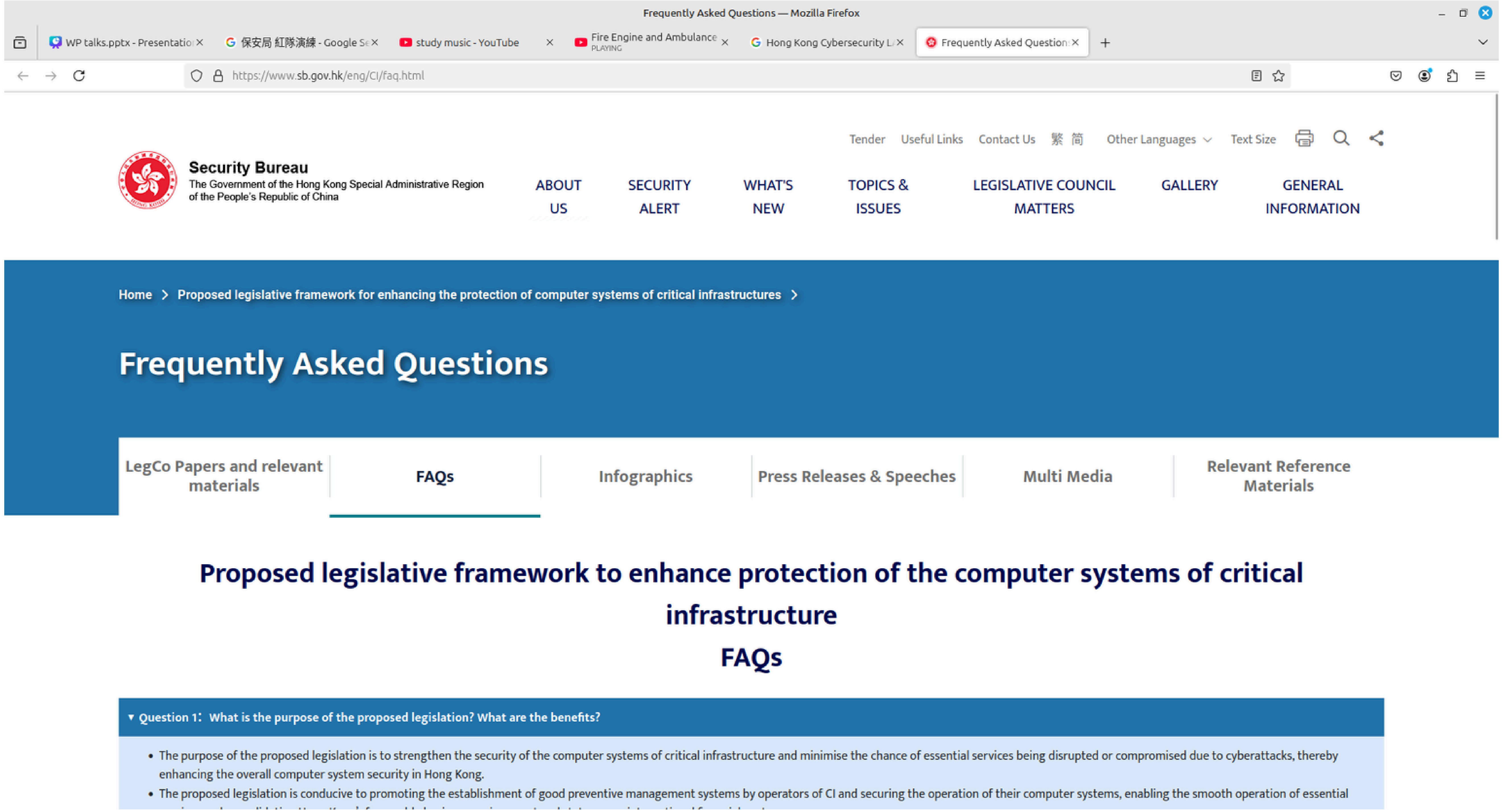
03. Avoid illusion of Safety

Illusion of Safety



關鍵基礎設施電腦系統安全條例

- 保安局 – 加強保護關鍵基礎設施電腦系統安全 — 建議立法框架
- 進行電腦系統保安風險評估（至少每年一次）
- 根據 – 立法會保安事務委員會討論文件
- https://www.sb.gov.hk/chi/special/CI/Panel%20Paper%20(C).pdf
  - Page 31 – 風險評估涵蓋的範圍，包括安全漏洞評估 （Vulnerability assessment）及滲透測試（ Penetration test）


Frequently Asked Questions — Mozilla Firefox
WP talks.pptx - Presentation
保安局 紅隊演練 - Google Se
study music - YouTube
Fire Engine and Ambulance
PLAYING
Hong Kong Cybersecurity L
Frequently Asked Question
https://www.sb.gov.hk/eng/CI/faq.html
Tender
Useful Links
Contact Us
繁
简
Other Languages
Text Size
Security Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China
ABOUT US
SECURITY ALERT
WHAT'S NEW
TOPICS & ISSUES
LEGISLATIVE COUNCIL MATTERS
GALLERY
GENERAL INFORMATION
Home
Proposed legislative framework for enhancing the protection of computer systems of critical infrastructures
LegCo Papers and relevant materials
FAQs
Infographics
Press Releases & Speeches
Multi Media
Relevant Reference Materials

Frequently Asked Questions

Proposed legislative framework to enhance protection of the computer systems of critical infrastructure

FAQs

▼ Question 1： What is the purpose of the proposed legislation? What are the benefits?

- The purpose of the proposed legislation is to strengthen the security of the computer systems of critical infrastructure and minimise the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer system security in Hong Kong.
- The proposed legislation is conducive to promoting the establishment of good preventive management systems by operators of CI and securing the operation of their computer systems, enabling the smooth operation of essential

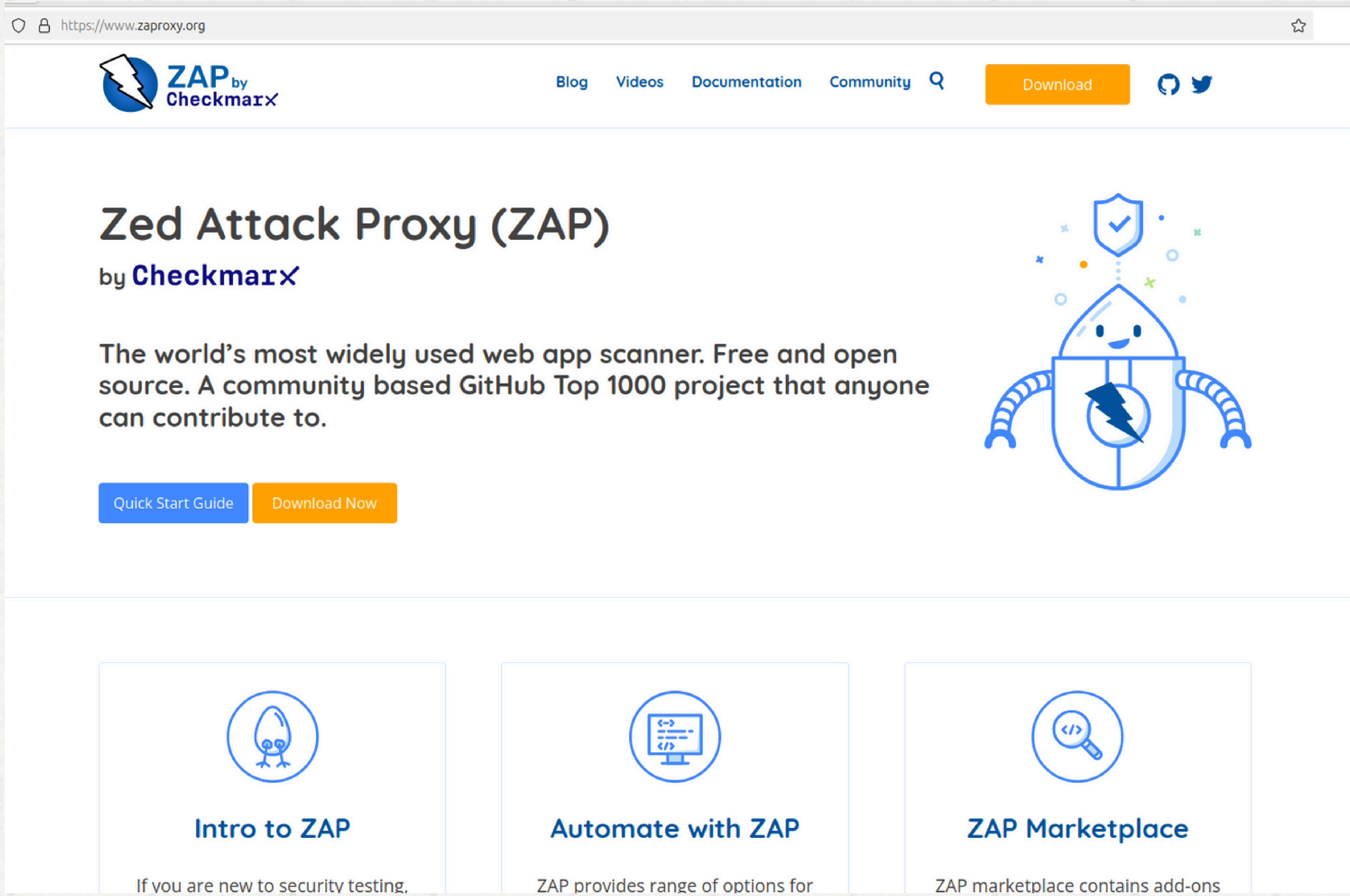
https://www.sb.gov.hk/eng/CI/faq.html

What’s in my toolbox

- OWASP –ZAProxy
- WPScan
- ReserveShell

- Brupsuite

ZAP



Zed Attack Proxy (ZAP)

by Checkmarx

The world's most widely used web app scanner. Free and open source. A community based GitHub Top 1000 project that anyone can contribute to.

Intro to ZAP

If you are new to security testing,

Automate with ZAP

ZAP provides range of options for

ZAP Marketplace

ZAP marketplace contains add-ons

What can Zaproxy do?

Automatic Vulnerability scan

Marketplace for more additional feature

Manual scan

ZAP

DEMO

What is WPScan

It is a vulnerability Scan tailor-made for WordPress website.
It has community edition
https://wpscan.com/

How to use WPScan

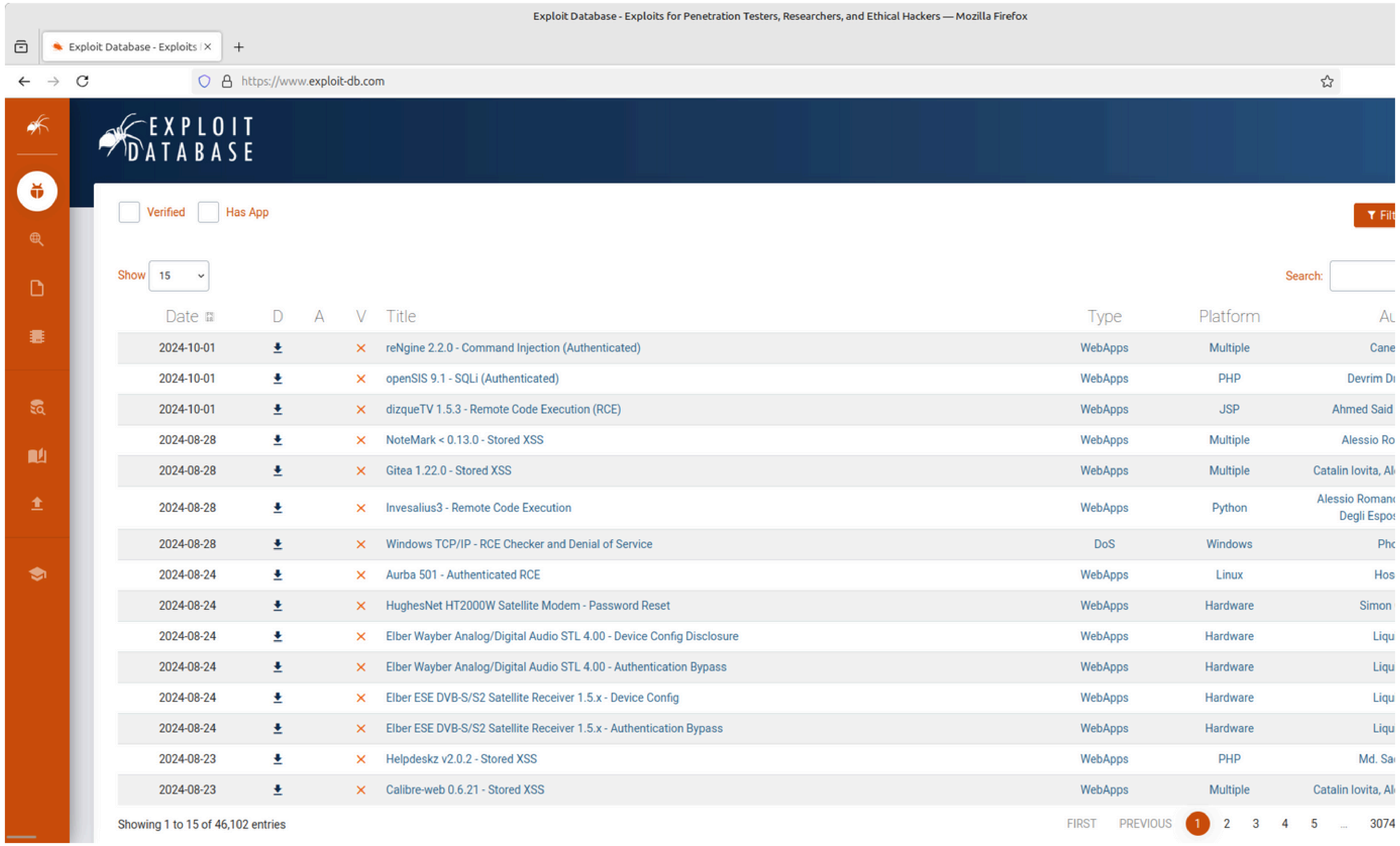
(read cheatsheet)

You may use some cheatsheet so that you can quickyly get used to WPScan commend.

https://wpscan.com/blog/wpscan-cli-cheat-sheet-poster/

Go through the cheat-sheet and Demo

Existing Exploit research / Sharing



Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers — Mozilla Firefox

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Au
2024-10-01	⬇		✕	reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Cane
2024-10-01	⬇		✕	openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Di
2024-10-01	⬇		✕	dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said
2024-08-28	⬇		✕	NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Ro
2024-08-28	⬇		✕	Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Al
2024-08-28	⬇		✕	Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano Degli Espos
2024-08-28	⬇		✕	Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Pho
2024-08-24	⬇		✕	Aurba 501 - Authenticated RCE	WebApps	Linux	Hos
2024-08-24	⬇		✕	HughesNet HT2000W Satellite Modem - Password Reset	WebApps	Hardware	Simon
2024-08-24	⬇		✕	Elber Wayber Analog/Digital Audio STL 4.00 - Device Config Disclosure	WebApps	Hardware	Liqu
2024-08-24	⬇		✕	Elber Wayber Analog/Digital Audio STL 4.00 - Authentication Bypass	WebApps	Hardware	Liqu
2024-08-24	⬇		✕	Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Device Config	WebApps	Hardware	Liqu
2024-08-24	⬇		✕	Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Authentication Bypass	WebApps	Hardware	Liqu
2024-08-23	⬇		✕	Helpdeskz v2.0.2 - Stored XSS	WebApps	PHP	Md. Sa
2024-08-23	⬇		✕	Calibre-web 0.6.21 - Stored XSS	WebApps	Multiple	Catalin Iovita, Al

Showing 1 to 15 of 46,102 entries

Demo platform introduce

- COlddbox
- https://www.vulnhub.com/entry/colddbox-easy,586/

Explanation – Reserve Shell

What is ReserveShell?

•

A Shell is a tools which offer to a user (usually administrator) to control a computer. User type “command” to instruct the computer to do something. Shell code will be a set of instruction. Which is repeatable.

Reserve Shell is a tools which instruct the application to offer the shell using. Usually these are hacking tools.

Example on PHP pentest monkey

Initial Findings

After using ZAProxy, WPScan and reserveShell. We have the following findings

01. SQL injection pages has been discovered

02. User Creditial is weak

03. IReserveShell has not been blocked

Other tools

What is Burpsuite community edition?

- What can it do?
- More than vulnerability scanner
- Burp Spider
- (Works as a proxy)