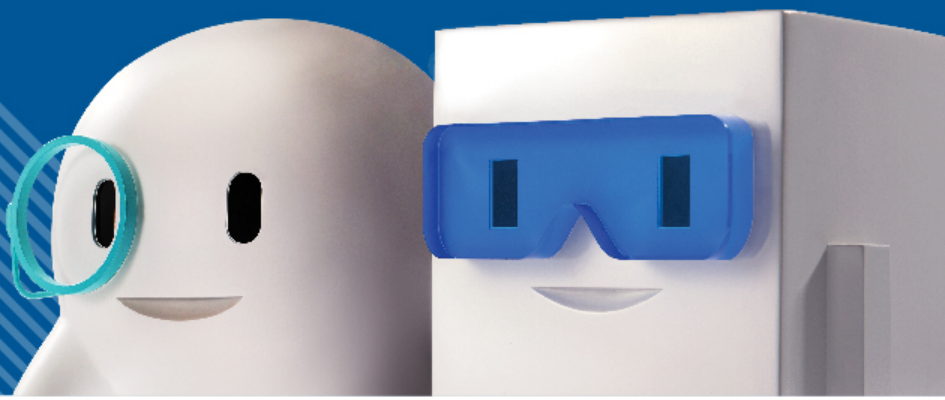
HKCERT
www.hkcert.org

HKPC

SME Free Web Security Health Check Pilot Scheme



Wally Wong MA, CISSP
Security Analyst
HKCERT

All-round Productivity Partner
全方位企業伙伴

Motives of hacking your website

Your website has...	Criminals can get...
Powerful CPU and bandwidth (you got a server!)	Use your power → DDoS attack others
24 x 7 service	24 x 7 phishing/malware hosted in your site
Visitors	Put malware in your site to infect your visitors

Business impacts of hacked website

- Blacklist → interrupt your communication
  - Examples: Google, anti-virus, firewall, mail server
- Reputation → trust of your products/services
- Possible regulatory/legal consequences
  - Authority investigation (e.g. PCPD)
  - Law enforcement investigation
  - Class action lawsuit

SME One 中小企一站通 | HKPC

Friends of SME One
中小企業網站免費保安檢查先導計劃

「網站」是企業推廣服務、客戶關係管理和網上交易服務的重要工具。然而，部分企業，尤其是中小企業(SMEs)，沒有足夠的資源去確保網站的安全。有見及此，SME One誠意為Friends of SME One提供「中小企業網站免費保安檢查先導計劃」，在專家指導下為中小企業的網站進行「檢查-行動-驗證」。計劃是免費的，並由香港生產力促進局轄下的香港電腦保安事故協調中心（HKCERT）舉辦，旨在向中小企業推廣網站保安的最佳實踐方法。

SME Free Web Security Health Check Pilot Scheme

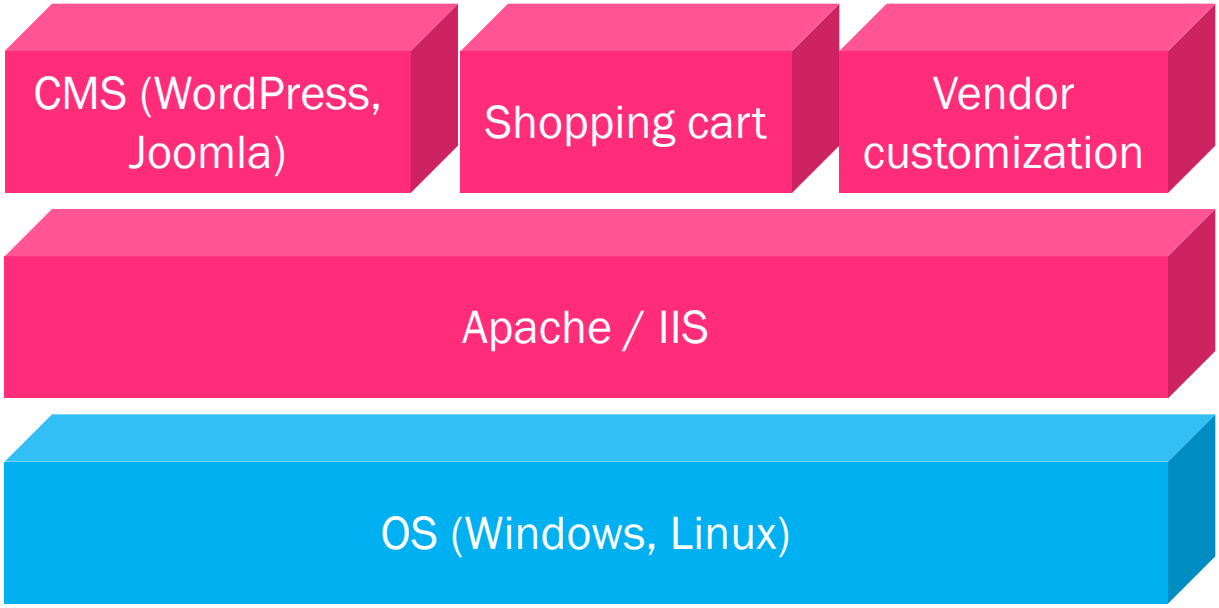
- Promote the best practice of “Check-Act-Verify” approach for website security health check to SME.
- Prerequisites:
  - You must has a website!
  - Willing to allocate resources for follow-up.
  - Apply: submit documents, arrange schedule

SME Free Web Security Health Check Pilot Scheme

- 35 SME companies joined in March 2016.
- First round of website scanning for participants completed, with scan results presented in report:
  - Website vulnerability severity levels
  - Classify vulnerabilities into 6 types
  - Business impacts
  - Titles of vulnerabilities found
  - Remediation advice for technical staff to fix problems
- Next: second round coming soon after participants followed up the findings

Vulnerability Scanning

- Misconfiguration / Vulnerability management
- Weak authentication / access control / encryption
- Weak input validation



Summary

Scanning schedule

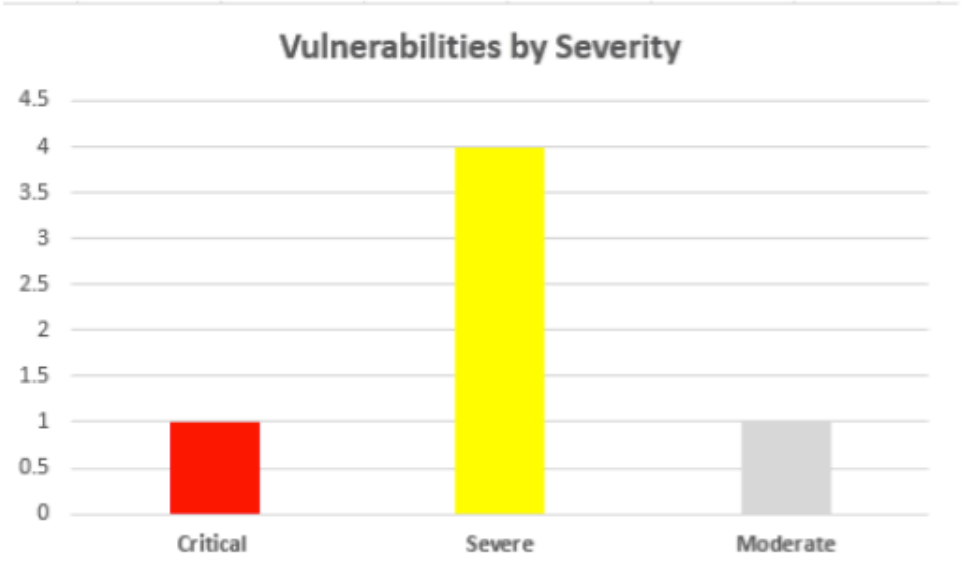
Site Name	Start Time	Status
www.sample.com.hk - 1st	12/06/2016 15:00, HKT	Success

Website information

Node	Operating System	Aliases
201.123.255.xx	Linux 2.6.X	• www.sample.com.hk

The audit was performed on one system which was found to be active and was scanned.

Figure 1. Vulnerabilities by Severity



Vulnerability and Impact

Vulnerability: Vulnerability (Software Update) Management

Impact

- Financial damage may be incurred if your website was compromised through any unpatched vulnerability due to the affected application.

Vulnerability: Weak Input Validation

Impact

- Weakness of your website may be exposed.
- Exposure of the website weakness may attract attacker to compromise the website.
- The sensitive data used or gathered by your website may be exposed due to the compromise.
- Distribution of phishing/malware may also be caused by the compromise, and may affect your clients.
- Reputation loss or regulatory/legal liability may be incurred.

Vulnerability: Weak Encryption

Impact

- The sensitive data used or gathered by your website may be exposed.
- Reputation loss or regulatory/legal liability may be incurred.

Vulnerability: Weak Access Control

Impact

- Possible unauthorized access to your website admin page and/or sensitive data.
- The sensitive data used or gathered by your website may be exposed.
- Reputation loss or regulatory/legal liability may be incurred.

Findings

This security scan focus on a well-known critical web application vulnerability and the scanning results listed as below:

Severity Levels: Critical, Severe, Moderate and Low

Item No.	Severity Level	Vulnerability Title	Type
1	Critical	Blind SQL Injection	Weak Input Validation
2	Severe	jQuery Vulnerability: CVE-2016-0819	Vulnerability (Software Update) Management
3	Severe	Missing HttpOnly Flag From Cookie	Weak Encryption
4	Severe	Browsable web directory	Weak Access Control
5	Severe	HTTP TRACE Method Enabled	Server Misconfiguration
6	Moderate	FTP access with anonymous account	Weak Authentication

Remediation

For those identified security problems, there are some advices to fix them.

Please kindly refer to Remediation Advice (Remediation.xlsx) for proposed actions.

Distribution of Industry in Participants

Industry	Count	% of total 26
Manufacturing	5	19%
Wholesale / Retail	5	19%
Import / Export Trades	3	12%
Information Technology	3	12%
Legal / Accounting / Marketing / Business Service / Consultancy	2	8%
Others	2	8%
Personal Beauty / Fitness	2	8%
Banking / Finance / Insurance / Securities	1	4%
Community & Social Services	1	4%
Construction / Architecture / Decoration	1	4%
Media / Publication	1	4%

Business Values of Your Website

Business value of website (can select more than 1)	Count	% of total 26
Showcase goods/services/work	21	81%
Customer can use service via website	13	50%
Provide online purchase	9	35%
Save time and cost	9	35%
Retain customer loyalty	7	27%
Global customers access 24/7	7	27%

Distribution of Vulnerability Classification

Classification of vulnerabilities	Count	% of total 229
Vulnerability (Software Update) Management	86	38%
Weak Input Validation	54	24%
Weak Encryption	36	16%
Server Misconfiguration	35	15%
Weak Access Control	14	6%
Weak Authentication	4	2%

Distribution of Vulnerability Severity Levels

Severity levels of vulnerabilities	Count	% of total 229
Severe	174	76%
Moderate	37	16%
Critical	14	6%
Low	4	2%

Industry vs Number of Vulnerabilities

Industry	Count	# companies	Average
Wholesale / Retail	59	5	11.8
Manufacturing	35	5	7.0
Import / Export Trades	16	3	5.3
Legal / Accounting / Marketing / Business Service / Consultancy	15	2	7.5
Information Technology	13	3	4.3
Community & Social Services	10	1	10.0
Construction / Architecture / Decoration	10	1	10.0
Others	8	2	4.0
Personal Beauty / Fitness	7	2	3.5
Banking / Finance / Insurance / Securities	3	1	3.0
Media / Publication	1	1	1.0

Online Transaction vs Vulnerabilities

Classification of vulnerabilities	Provide online transaction	No online transaction
Vulnerability (Software Update) Management	75	11
Weak Input Validation	40	14
Server Misconfiguration	18	17
Weak Encryption	14	22
Weak Access Control	12	2
Weak Authentication	2	2

Improve and maintain security

- Assessment:
  - Follow-up with ‘remediation advice’.
  - Limitations of hosting company for follow-up (e.g. shared hosting)
- Infrastructure:
  - Secure WordPress/Joomla hosting
  - Hosting company guaranteed to provide secure features, e.g. regular patch, secure shopping cart, encryption etc.
  - Web application firewall (not to confuse with network firewall)
  - Cloud services
- Detection:
  - Google Webmasters tools (www.google.com/webmasters/hacked)
  - mxtoolbox.com/blacklists.aspx

Improve and maintain security

- User
  - Maintain user workstation security.
- Website
  - Regular patch, update, scanning of web app/server
  - CMS specific security checking (e.g. file integrity)
  - Regular offline backup
- Prepare for emergency
  - Business contingency plan
  - Drill for website down/hacked
  - Provide reachable contact on website/WHOIS so that organizations like HKCERT can contact you if your site was found hacked.
- If your website does not function any more, remove it completely (note: you may need to keep the domain).

Takeaway

- Many cybercriminals hacked your website because they want your resources, which put your website as part of their criminal activities (e.g. distributing ransomware).
- Hacked website could affect your reputation and business operation.
- Your website will become vulnerable if you don't care about its security. Hacking your vulnerable website is not as hard as you think.
- Use 'health check' as the beginning of improving website security, regardless of the size of your organization and industry.

HKCERT
www.hkcert.org

Thank You!

HKPC