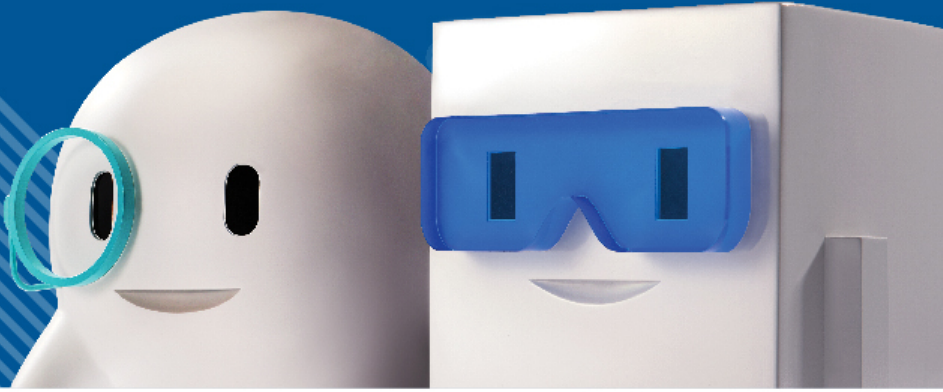
HKCERT
www.hkcert.org

HKPC

Improve Website Security with Health Check
加強網站保安由保安檢查做起



All-round Productivity Partner
全方位企業伙伴

Agenda

1. Understand the motive of hacking your website.
2. Impacts resulted from a hacked website.
3. Understand how easy to hack a vulnerable website.
4. Improve and maintain website security → starting from ‘health check’

Cybercriminal Activities

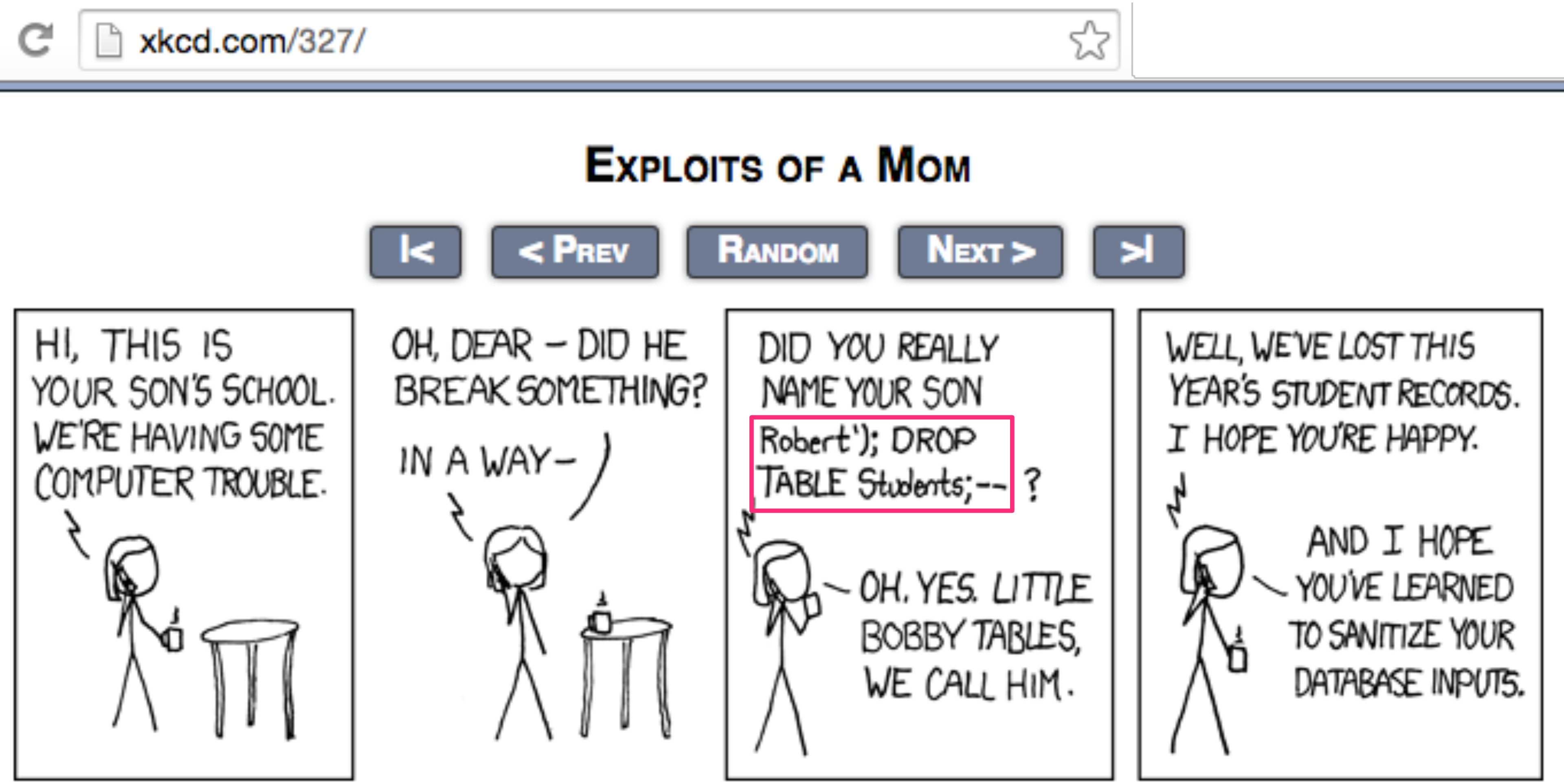
Objective	💰 💰 💰 💰 💰 💰 💰 💰 💰 💰	
Valuables	Data ☆ Financial information (e.g. online banking credentials, payment processor, POS etc.) ☆ Personal information (e.g. PII, health record etc.) ☆ Intellectual property	敲詐/破壞 Extortion/Vandalism (interrupt business operation) ☆ Interrupt website (e.g. DDoS) ☆ ‘Lock’ files/data (e.g. ransomware)
How to achieve	☆ Phishing (e.g. scam email/website) ☆ Advanced persistent threat (APT)	☆ Encrypt files/data (e.g. ransomware) ☆ Distributed denial of service (DDoS)
Tools & resources	☆ Server for hosting scam website ☆ Server for sending scam/spam email ☆ Server for hosting malware ☆ Bandwidth for launching DDoS	⇦ **‘Provided’ by YOUR vulnerable website**

Motive 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

Impacts of hacked website

Technical	Business
• Take control of **server** (e.g. web shell) • Execute arbitrary code • File traversal • Take control of database • Gain admin privilege • Dump data • Website/Mail server blacklisted by Google / anti-virus app / firewall / mail server gateway	• Interrupt business operation: • No website as taken down for fixing • Lost in communication as website/mail server blacklisted • Reputation (e.g. what if every customer infected with ransomware after visiting your site) • Possible compliance/legal consequence: • Authority investigation (e.g. PCPD) • Law enforcement investigation (in theory) • Class action lawsuit



xkcd.com/327/

Exploits of a Mom

|<
< Prev
Random
Next >
>|
HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

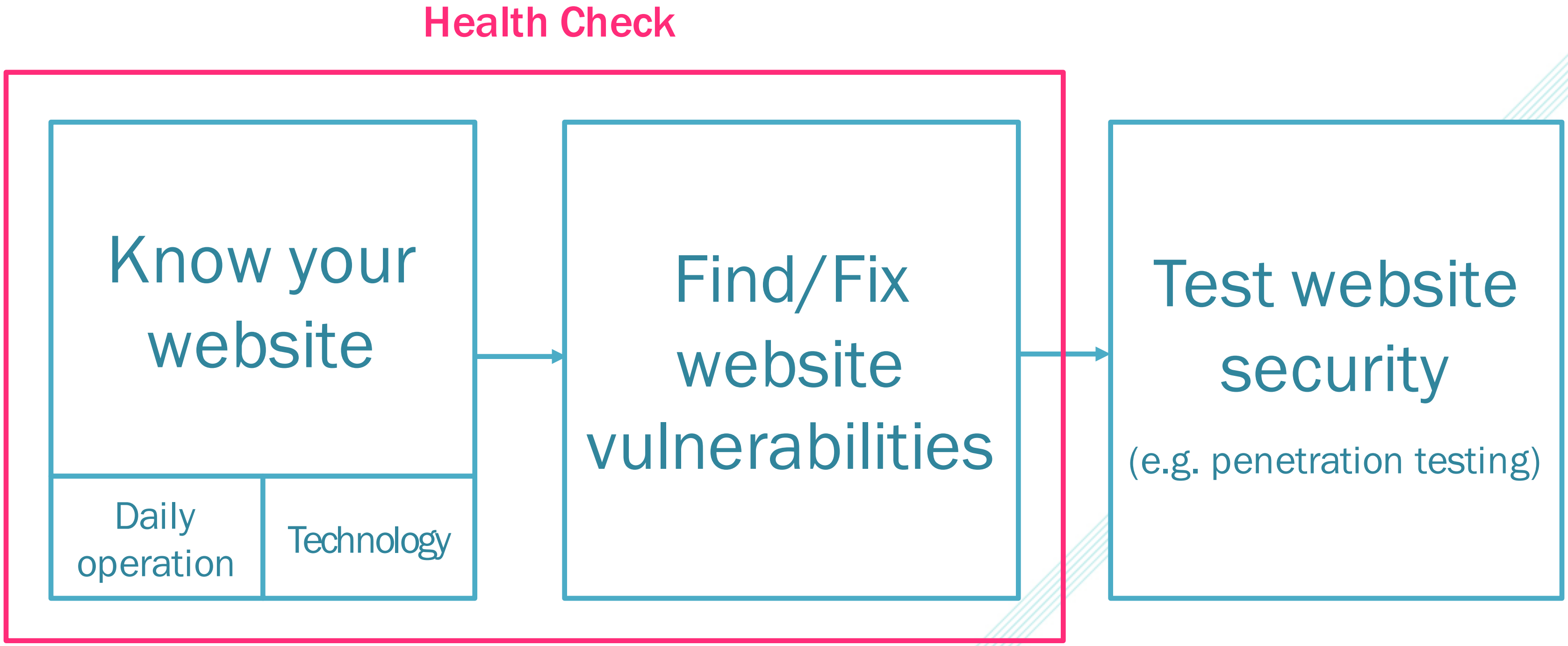
Hack your website

Break the perimeter → guess or get the admin password	Without breaking any perimeter → abuse website vulnerabilities
- Infect your computer (e.g. keylogged admin password). - Weak/Default password used for FTP or admin page - Phishing	- Abuse web server vulnerabilities 漏洞 - Abuse web app vulnerabilities - SQL injection - Cross site scripting - CSRF - …
- Not 'cost effective' (e.g. brute force attack)	- Tools and techniques (e.g. 'pentest', 'sqlmap', 'censys') already available and very handy for hacking **quickly** and **in bulk.**

Hack your website

- ‘Vulnerable website’ can mean:
  - web server (e.g. Linux + Apache, Windows + IIS), or/and
  - web app (e.g. Joomla, WordPress) is/are vulnerable
- Reasons for web server/app vulnerable:
  - No regular patch/update.
  - Outdated version.
  - Use vulnerable plugins.
  - Misconfiguration (e.g. too much privilege)
  - Web form input (e.g. contact us) implemented by developer/vendor → not enough input validation

Improve website security



Health Check

Know your website

Daily operation

Technology

Find/Fix website vulnerabilities

Test website security

(e.g. penetration testing)

‘Health Check’ → know your website

- Daily operation:
  - Purpose of your website to your business
  - How critical is your website to your business?
  - Who can update the content?
  - Who can view the data collected?
  - Who is the technical support?
  - Who develops your website?
  - Do you know what contacts were input in WHOIS record?
  - What are the ‘emergency contacts’ for your website?
  - Any regulatory/standard to comply for your website?
- Technology:
  - How is your website hosted?
  - What type of web server is used? Which version?
  - What type of PHP / ASP / CMS / web app is running? Which version?
  - Any regular patch for server/app?
  - Any backup of your website?
  - Any app or FTP server for updating/viewing your website content/data?
  - Any control panel login for your hosting account?
  - Any email server configured under your website domain?

What do you know about your website?	Implication	Consideration/Decision/Action
Role of your website: the only channel to convey information to your customers	Website also part of your business operation	How to ensure website down time within tolerable level?
Staff A and B responsible for updating website.	The security of their computers also critical.	Enough protection for their computers (or even their home computers)?
No patch applied to website for 4 years; Joomla 1.5.x being used.	Web server and Joomla (latest version 3.x) security 4 years 'lag behind'	Easy to hack your website → should you spend resources on further securing it, or building a new website?
WHOIS record not reviewed since domain registered; also no internal technical support	• Can some ex-employee still control your domain? • You may not know whom to contact if your website is hacked?	• Update and provide valid contacts in WHOIS record. • Prepare contact list for handling website problem.

‘Health Check’ → know your website

- Apart from technical factors, also know any operation factors affecting website security.
- Know how critical the website is to your business.
- Also act as initial ‘gap analysis’ → how far from ‘acceptable’ security level
- Update or prepare key contacts for handling website problem.
- As a reference for deciding next actions, e.g. further security checking or re-building/migrating the website etc.

‘Health Check’ → find/fix vulnerabilities

- Find/Fix vulnerabilities by ‘website scanning’:
  - The fastest way to identify any unpatched and potential security threat, and tell you how to fix them.
  - Some areas (e.g. login) may not be covered.
- Types of ‘website scanning’:
  - App specific scanning (e.g. Joomla, WordPress)
  - Website vulnerability scanner (www.hkcert.org/security-tools#SecAssTools)
- Some of the tools may be free, but may require technical knowledge or even vendor for usage and interpreting the result.

Maintain website 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.

😸 Thank You!