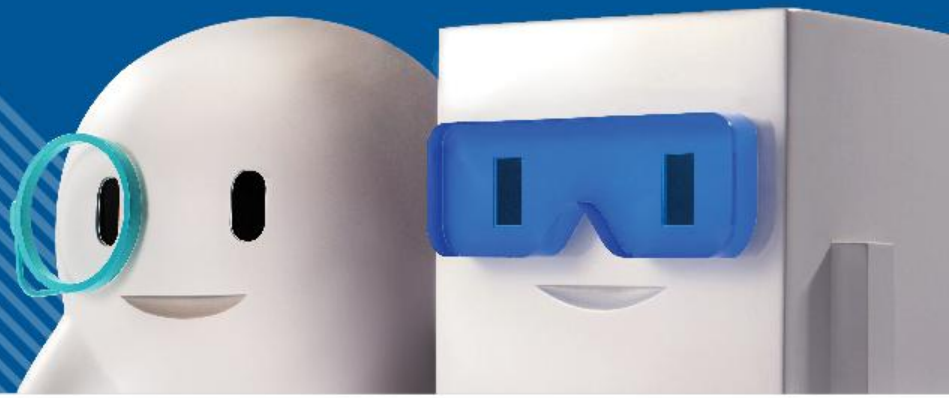
HKPC

HKCERT

Is Your SSL Website and Mobile App Really Secure?



All-round Productivity Partner
全方位企業伙伴

Agenda

- What is SSL / TLS
- SSL Vulnerabilities
  - PC/Server
  - Mobile
- Advice to the Public

Hong Kong Computer Emergency Response Team Coordination Centre

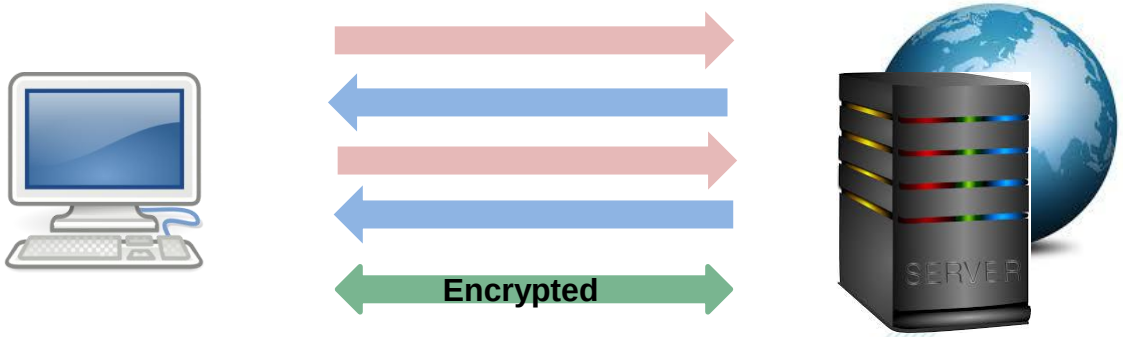
- 香港電腦保安事故協調中心 **(HKCERT)**
  - Established in 2001. Operated by HK Productivity Council
  - Provide Free-of-charge service to Public
  - Scope of services
    - Incident Handling, Response and Coordination
    - Dissemination of Alerts, Warnings and Security-related Information
    - Security Awareness Education
    - Coordination and Collaboration with Relevant parties on Security Preventive Measures
  - 24 hrs hotline: 8105-6060

What is SSL / TLS

- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) is a standard security technology for establishing an encrypted link between a server and a client (web browser).
  - Provides confidentiality and integrity of the data.
  - Also used to identify the owner.

- Without encryption, you information will be sent in plain test, you information can be captured from bad guy

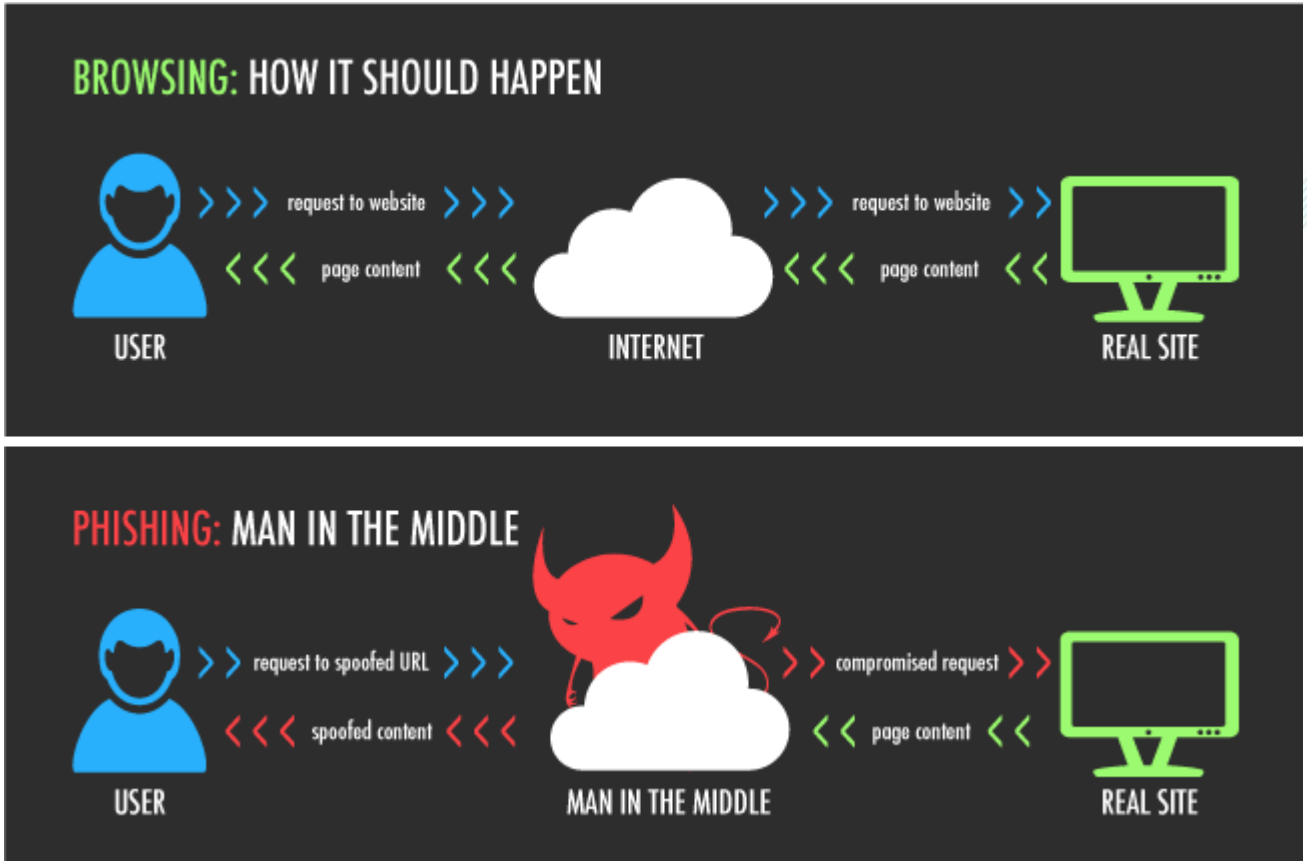
How does it work



Key	Cipher	Hash
RSA	SHA-2	HMAC-MD5
Diffie-Hallman	3DES	HMAC-SHA
DSA	AES	

Key	Cipher	Hash
RSA	SHA-2	HMAC-MD5
Diffie-Hallman	3DES	HMAC-SHA
DSA	AES	

Man in the Middle Attack

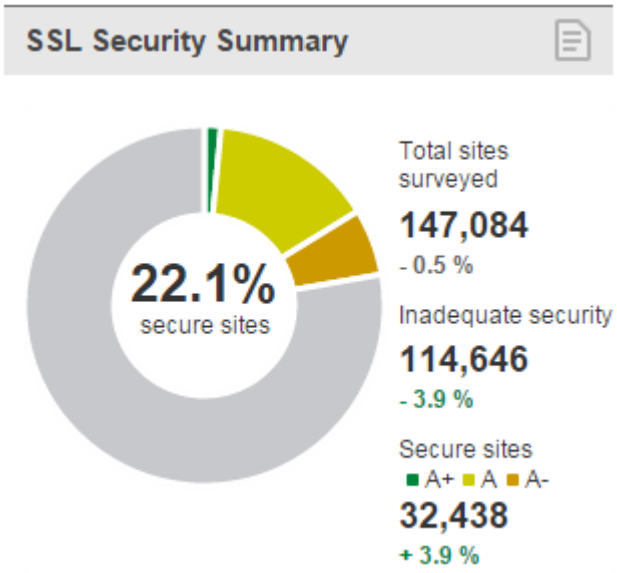


Source: DigiCert

SSL Pulse

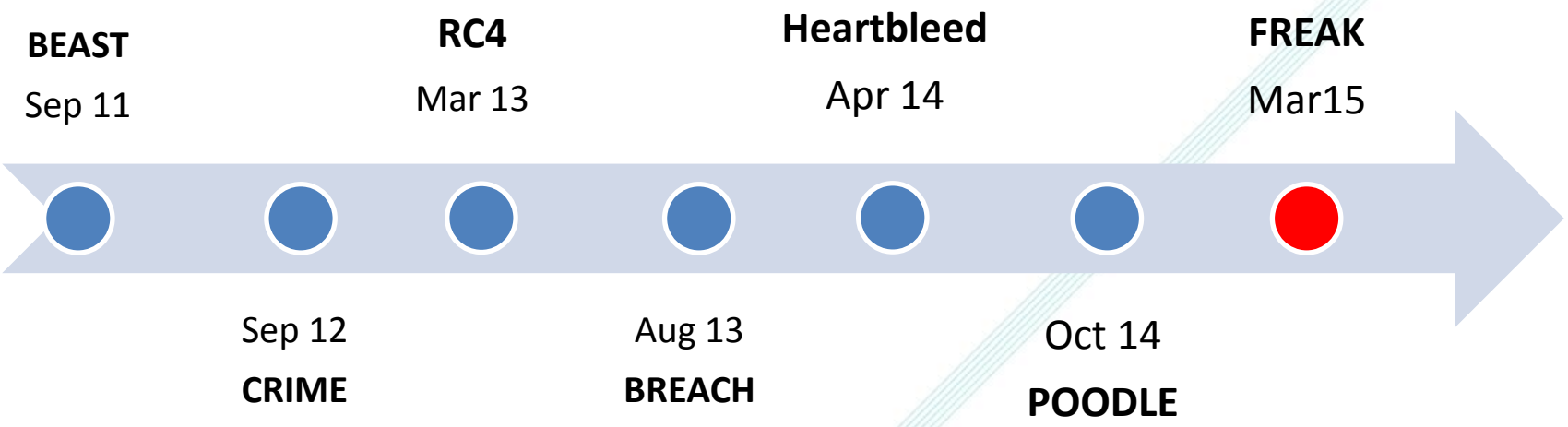
Effective Security of SSL

- Total sites surveyed **147,084**
- 77.9% of sites surveyed have inadequate security. **114,646** (-3.9% compared to last month)
- 22.1% of sites are secure. **32438** (+3.9% compared to last month)



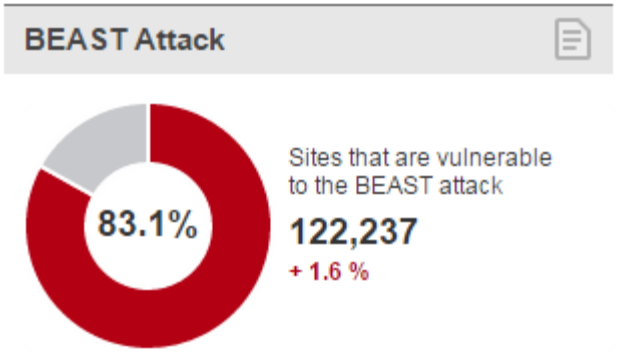
Source: Trustworthy Internet Movement

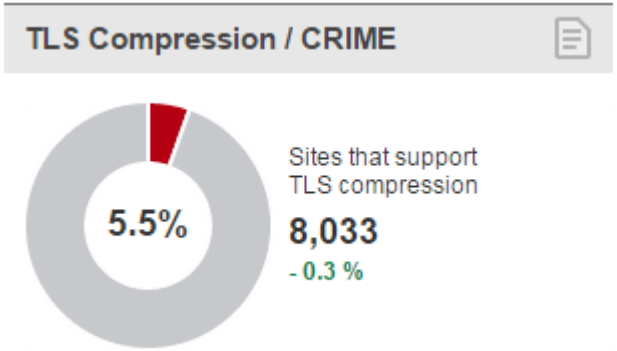
SSL Vulnerabilities timeline



BEAST / CRIME

- Discovered in Sep 11, vulnerability on SSL 3.0 and TLS 1.0
- POC: Capable to decrypt PayPal authentication cookie and access PayPal account.
- Switched to RC4 stream cipher (Found weakness on Mar 13)



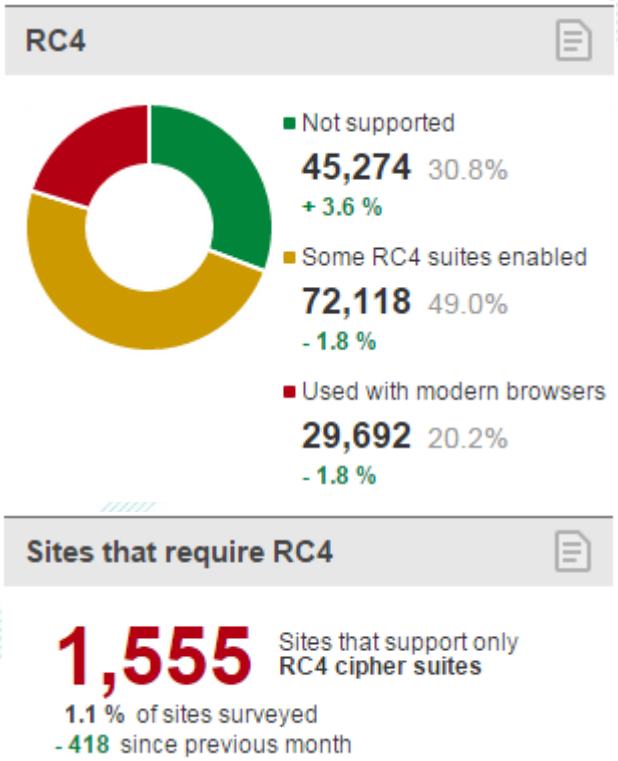


- Discovered in Sep 12
- Hacker can hijack the session by decrypting the session cookie
- Vulnerable (TLS 1.0, SPDY protocol (google), older versions browsers and application that uses TLS compression)

Source: Trustworthy Internet Movement

RC4

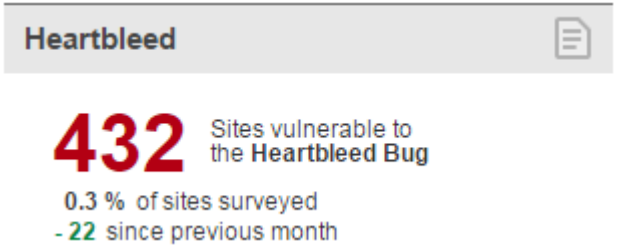
- RC4 suite was recommended as mitigation of BEAST attack.
- Broken in Mar 2013
- 30.8% not support RC4
- 49% support some RC4 suites
- 20.2% website support RC4



Source: Trustworthy Internet Movement

Heartbleed

- Heartbleed bug in the OpenSSL cryptographic software library. Discovered in Apr 14
- Hacker can retrieve sensitive information from the memory of vulnerable server
- Affects email, website, IM and VPNs
- Also exist in mobile device.
- 432 websites vulnerable to the Heartbleed Bug (-22 sites since previous month)

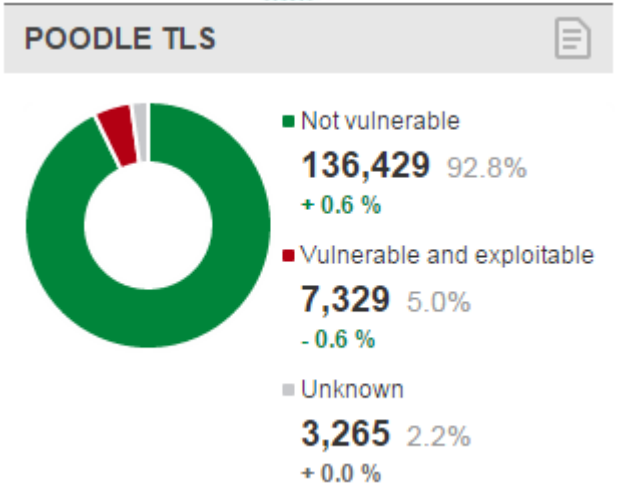


https://www.hkcert.org/openssl

Source: Trustworthy Internet Movement

Poodle

- Discovered in Apr 14
- Attacker can eavesdrop the encrypted content under SSL v3.0
- If SSL 3.0 cannot be disabled, stop backward compatibility function
  - TLS_FALLBACK_SCSV
- Upgrade OpenSSL
- Disable SSL 3.0 on user and server side
- 5% still vulnerable to the Poodle attack



Source: Trustworthy Internet Movement

FREAK

- Discovered in Mar 15
- Attacker can intercept HTTPS connections between client and servers
- Force the connection to use weak encryption.
- Decrypt and alter sensitive data
- Upgrade OpenSSL
- Upgrade Browser version
- Use stronger cipher suite

FREAK Attack: Client Check

https://freakattack.com/clienttest.html

Is your Mobile App Safe?

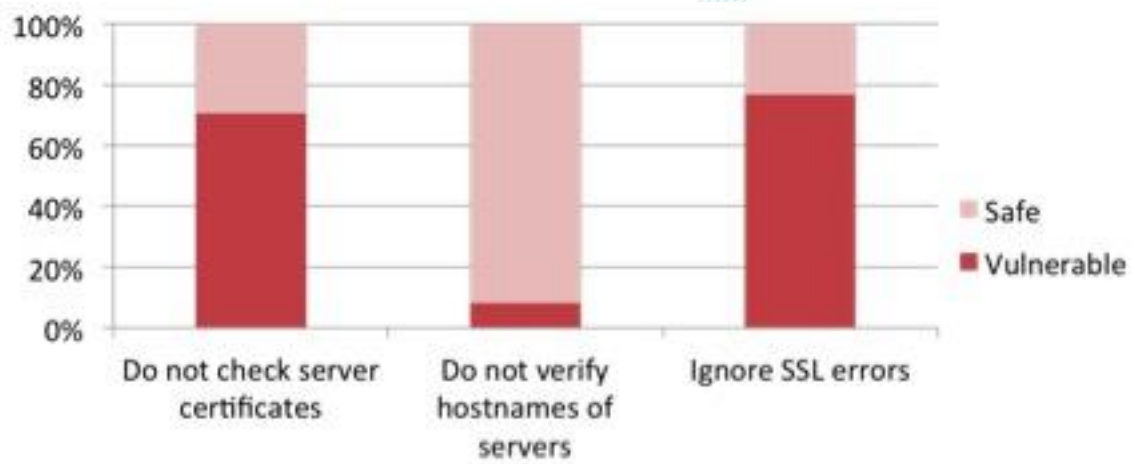
- CERT Coordination Center at Carnegie Mellon University (CERT/CC) published a list of popular Android apps that fail to properly validate SSL certificates, exposing users to man-in-the-middle (MITM) attacks. (Sep 2014)
  - Use a MITM appliance to analysis
  - > 23K FREE apps failed on the test
  - Notified apps develop/vendor about the vulnerabilities

Android apps that fail to validate SSL

https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4/edit#gid=1053404143

Is your Mobile App Safe?

- FireEye analyzed 1,000 of the most popular free apps offered on Google Play and found that 68% of them are vulnerable.
  - 448/674 apps (~73%) mobile apps use SSL/TLS to communicate with remote server, but do not check certificates
  - 50/674 (~8%) use their own hostname verifiers that do not check hostnames
  - 285 apps use Webkit, 219 (~77%) ignore SSL errors generated in WebKit



Is your Mobile App Safe?

- McAfee examine the most frequently downloaded apps from CERT/CC Android apps spreadsheet.
  - 18/25 apps are still vulnerable to MITM attacks
  - Ex: Mobile Photo editor with > 1M downloads
    - Use social network and cloud services account to share photos (login credentials can be intercepted)
  - Mobile apps remain unsecure even the vendor was informed the vulnerabilities after 1 month

Is your Mobile App Safe?

Suggestions:

- Enterprise should test both 3rd party and in-house developed mobile apps.
- Upgrade your mobile OS and Apps.
- Avoid using the Apps on untrusted networks.

Refer link:

- Android SSL Security – Security with HTTPS and SSL
  http://developer.android.com/training/articles/security-ssl.html

Advice to the Public

- Patch the system and application vulnerability
- Use Stronger SSL/TLS protocol version
  - SSL 1.0 – 3.0 is an obsolete and insecure version.
  - Use TLS 1.2 or above
- Use stronger Cipher Suite
  - SHA-1 and MD5 is an obsolete hash algorithm. (from 2015, browser will alert users if the websites is using SHA-1 certificate and no longer be accepted after 1 Jan 2017.
  - Insecure encryption algorithm: DES, 3DES, RC4
  - Use SHA-2

Advice to the Public

- Perfect Forward Secrecy (PFS) and SHA-2 for certificates. These options provide a higher level of protection.
  - Use ECDHE “Elliptical Curve, Diffie-Hellman, Ephemeral signed “
  - Ex: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256 Bit keys.
- Use HTTP Strict Transport Security (HSTS) to force server/client negotiation to use SSL

Advice to the Public

- **Digital Certificates should be signed with SHA2, except root certificates**
  Certificate Chain of Trust
  - SHA2 signed end certificate must be chained to SHA2 signed intermediate certificates.
  - SHA-1-based signatures for trusted root certificates (offline).

Usage of SSL Certificate

- Not only used to secure connection between browser and server, but also….
  - Encrypt communication (SMTP, FTP, SSH, applications, etc.)
  - Email message
  - Authentication (2 Factor authentication)
  - Signing (pdf, docx, application,etc.)

HKCERT will disable SSL v3.0

- **CAs will stop issuing SHA-1 based certificate by Jan 1, 2016**
- **No longer support SSL 2.0 and SSL 3.0 by June 1, 2015**
- **Alert IE6 users (i.e. using SSL 3.0 or below).**
  - Redirect to another page that warns them to upgrade their Windows and browser..
    HKCERT 給 Internet Explorer 6 瀏覽器用戶的提示
    https://www.hkcert.org/sslalert
- **Use digital certificate signed by SHA-2** ~~SHA-1~~
- **Drop weak algorithms**
  - AES ~~DES~~, ~~3DES~~
  - SHA-2 ~~RC4~~, ~~MD5~~, ~~SHA-1~~
- **Support forward secrecy**
  - DHE, ECDHE

HKCERT will disable SSL v3.0 from June 1, 2015 onwards
https://www.hkcert.org/my_url/blog/15012902

Recommendations to Cryptography

Protocol	Server Key & Certificate		Cipher Suite			Client side policy
TLS1.2	2048	SHA2	AES	SHA2	FS	HSTS
TLS1.1						
TLS1.0						

Minimum standard

SSL 3.0	1024	SHA1	RC4	SHA1	
SSL 2.0			3DES	MD5	
			DES		

Not Recommend

Compatibility issues

Who are affected?

- Windows XP and Internet Explorer 6 users
  - Internet Explorer 6 does not support TLS encryption. From June 1, 2015 onwards you will not be able to browse the HKCERT website.
- Users whose browsers are configured to support SSL 3.0 only and not supporting TLS.

Upgrade your browser to latest version

- Internet Explorer version 11 and above
- Chrome version 40 and above
- Firefox version v35 and above

SSL Server Test

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > testing.hkcert.org

SSL Report: [redacted].hkcert.org ([redacted])

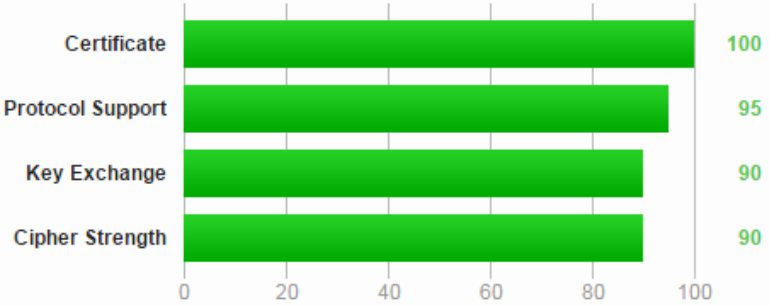
Assessed on: Thu Apr 16 00:51:21 PDT 2015 | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Browser Test

QUALYS SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36

Protocol Support

Your user agent has good protocol support.

Your user agent supports TLS 1.2, which is the best available protocol version at the moment.

FREAK Vulnerability (Experimental)

Your user agent is not vulnerable.

For more information about the FREAK attack, please go to www.freakattack.com.

To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

POODLE Vulnerability

Your user agent is not vulnerable.

For more information about the POODLE attack, please read this blog post.

Other Useful Resources

- **Qualys SSL Test for Browsers (including FREAK and POODLE tests)**
  https://www.ssllabs.com/ssltest/viewMyClient.html

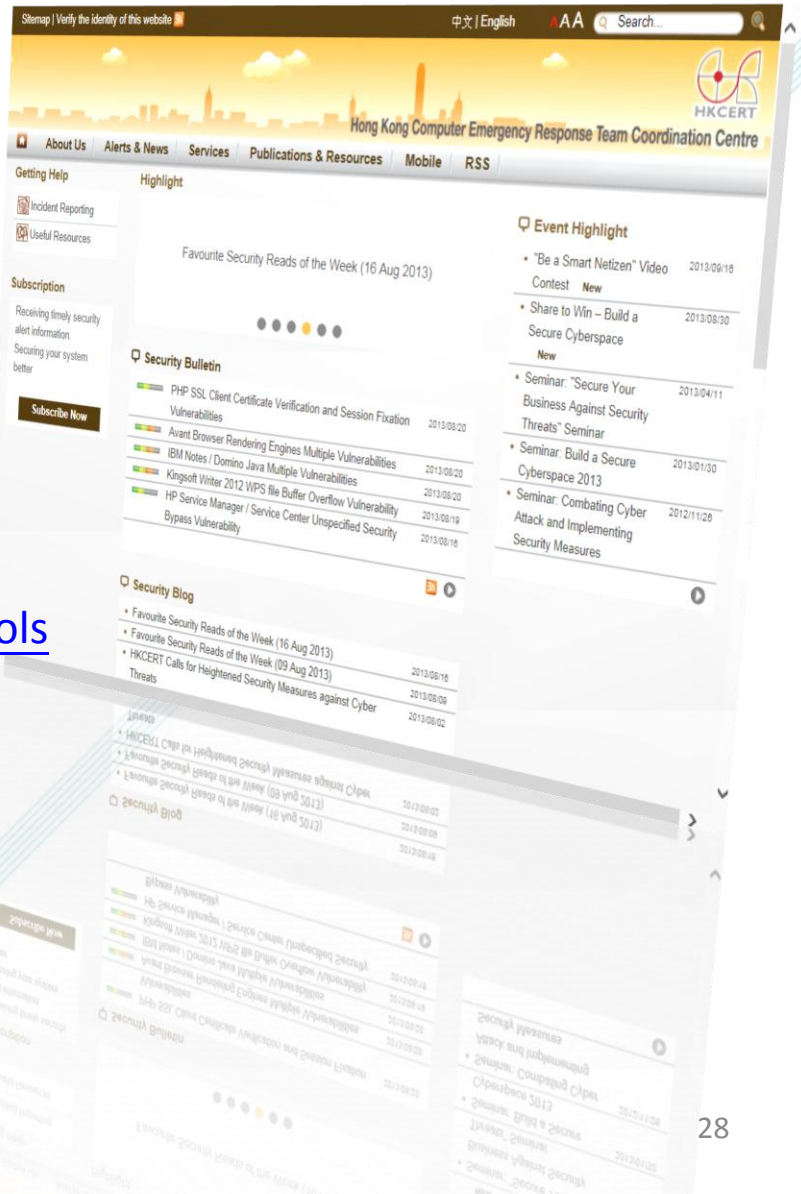
- **Qualys SSL Labs - SSL Server Test**
  https://www.ssllabs.com/ssltest/index.html

- **Qualys SSL Labs - SSL/TLS Deployment Best Practices**
  https://www.ssllabs.com/projects/best-practices/

- **Digicert – Enabling Perfect Forward Secrecy**
  https://www.digicert.com/ssl-support/ssl-enabling-perfect-forward-secrecy.htm

HKCERT Security Guidelines & Handbooks

- **Security Guideline**
  - https://www.hkcert.org/security-guideline
- **Security Tools**
  - https://www.hkcert.org/security-tools
- **Mobile Security Tools**
  - https://www.hkcert.org/mobile-security-tools
- **HKCERT Mobile App**
  - Search by keyword: **HKCERT**



Available on the App Store

ANDROID APP ON Google play

Q&A

HKCERT Contact

8105-6060

hkcert@hkcert.org

www.hkcert.org

香港電腦保安事故協調中心