

# Common Security Issues

---

jnlin

# Security Principles

---

- Network Security is a very very big issue, can not full covered in this course
- CSO: Chief Security Officer
- Security is time-consuming
  - One Time Password
  - Forced splitting internet and intranet
    - EC sites in Taiwan
  - Long password
- KISS: Keep it simple and stupid

# Network Security Threats

---

- Virus / Torjans
- Adware / Spam
- Phishing / Fraud
- Hijacking
- Social Engineering / APT
- Denial of Service Attacks
- .....

The screenshot shows a news article from iThome. At the top, there's a banner for an IT EXPLAINED WEBINAR on April 6, 2020, from 14:30 to 15:20. The main headline reads: "駭客挾持BGP，竄改加密錢包DNS，盜走價值17萬美元的以太幣". Below the headline is a summary: "資安專家推測，駭客挾持BGP把Amazon Route 53服務的流量導至駭客操縱的DNS伺服器，將造訪MyEtherWallet的用戶導向偽造網站，誘MyEtherWallet錢包用戶輸入憑證，盜走用戶帳號內的以太幣。" There are social sharing buttons for Facebook and a photo of the author, Chen Mengli.



## 中國電信長期挾持經過美國與加拿大的流量

軍事網路專家協會(Military Cyber Professionals Association)在最新一期的「軍事網路事務」期刊中發表一篇研究報告，指出中國國營的中國電信長期利用架設在美國與加拿大的入網點(Point of Presence, PoP)挾持並監控通過當地的流量。全球網路是由數萬個自治系統(Autonomous System, AS)所組成，多半是由網路服務供應商(如ISP業者等)或大型組織(如Google等)所建立，他們之間是透過邊界閘道協定(Border Gateway Protocol, BGP)進行交流，BGP的優點之一是富有彈性，若傳輸路徑太過擁擠就可變更流量路徑，但同時也成為駭客

# The ideas

---

## □ Multiple layers of protection

- DMZ
- Splitting permission of users
  - Principle of least privilege
- Protected Network (e.g. VPN)

## □ Intrusion Detection

- Firewalls
- WAF

## □ Auditing

- Logging

# OWASP

---

- The Open Web Application Security Project
- <https://owasp.org>

# OWASP Top 10 Security Risks

- Published every 3 years
- The latest is 2017 version

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

# Injection

---

- Unproper escaping of input
- Cause data leak or data loss
- Examples
  - SQL injection
  - Javascript injection
    - XSS (Cross-site Scripting)
- Question: How to prevent it?

# CVE: Common Vulnerabilities and Exposures

□ CVE® is a list of entries for publicly known cybersecurity vulnerabilities.

□ Subscribe the RSS feed



## SSL Server Test

- Test the SSL configuration and potential risks
- <https://www.ssllabs.com/ssltest/>

 Qualys. SSL Labs

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.cs.nctu.edu.tw

**SSL Report: www.cs.nctu.edu.tw (140.113.235.48)**

Assessed on: Tue, 24 Mar 2020 08:06:41 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating

**A+**

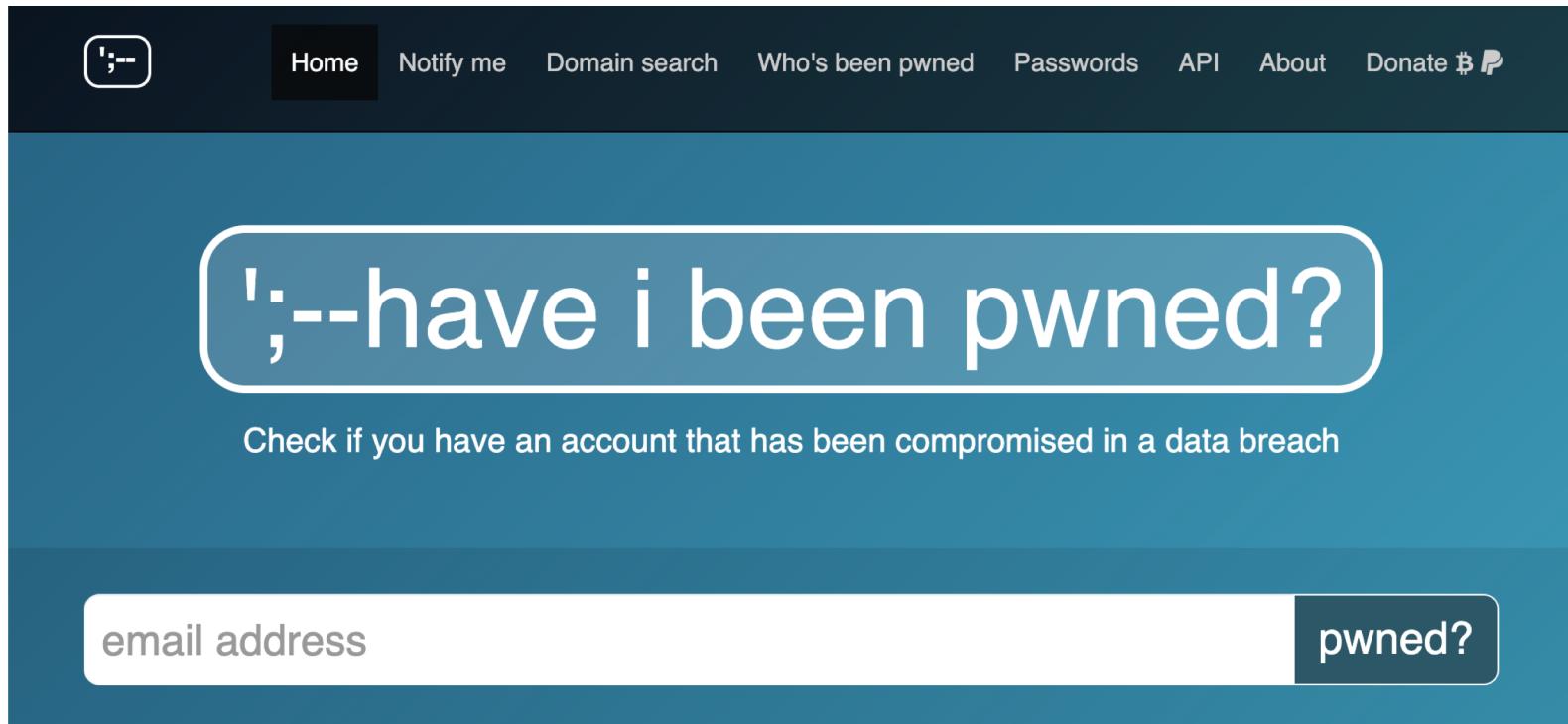
Category	Score
Certificate	100
Protocol Support	100
Key Exchange	90
Cipher Strength	90

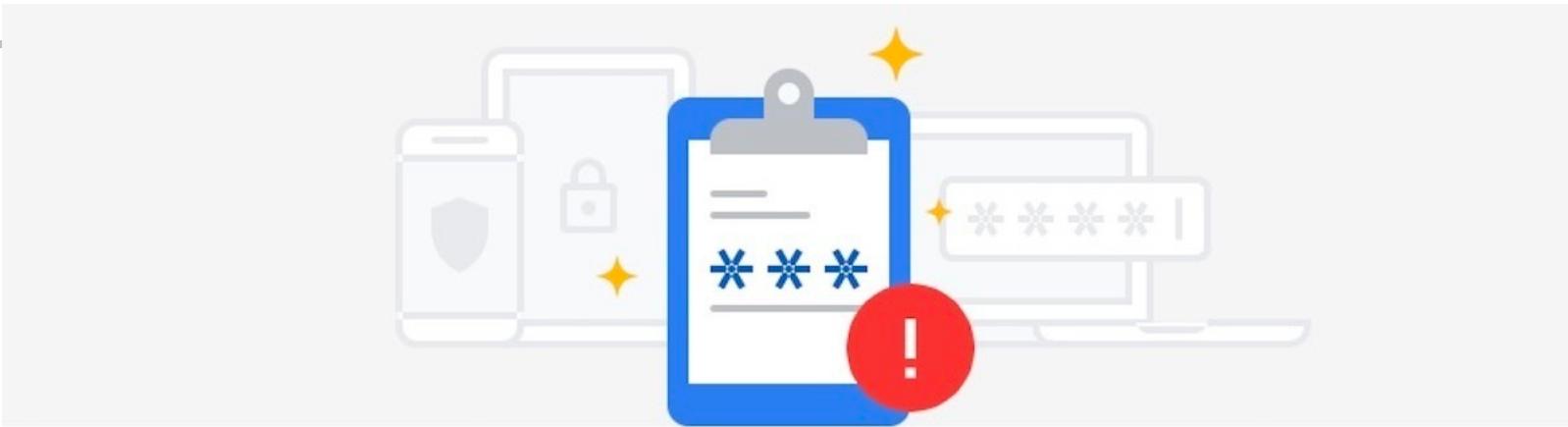
Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

# Have I been pwned?

- Test if your email & password leaked
- <https://haveibeenpwned.com/>





## Check your passwords

A data breach on a site or app exposed your password. Chrome recommends checking your saved passwords now.



[Close](#)

[Check Passwords](#)

# Static analysis

---

- A testing methodology that analyzes source code to find security vulnerabilities
- Human review needed
  - Can not find authentication problems, access control issues, insecure use of cryptography
  - Large number of false positives
    - Difficult to “prove” that an identified security issue is an actual vulnerability.
- [https://owasp.org/www-community/Source Code Analysis Tools](https://owasp.org/www-community/Source%20Code%20Analysis%20Tools)

Dependencies

Dependents

**⚠ We found potential security vulnerabilities in your dependencies.**[Dismiss](#)

Some of the dependencies defined in your `package.json` have known security vulnerabilities and should be updated.

Only the owner of this repository can see this message.

[Learn more about vulnerability alerts](#)

These dependencies have been defined in `sarkartanzil.github.io`'s manifest files, such as `package.json`

**📦 Dependencies defined in `package.json` 11**

>  <a href="#">jquery / jquery</a>	 Known security vulnerability in ^ 1.11.3 ▾
>  <a href="#">twbs / bootstrap</a>	^ 3.3.7
>  <a href="#">BrowserSync / browser-sync</a>	^ 2.13.0
>  <a href="#">FontAwesome / Font-Awesome</a> font-awesome	^ 4.6.3
>  <a href="#">gulpjs / gulp</a>	^ 3.9.1
>  <a href="#">scniro / gulp-clean-css</a>	^ 2.0.10

# DoS: Denial of Service Attacks

- Make a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet
  
- Methods
  - Software bugs
  - Bad designed / implemented protocol
    - SYN Flooding
    - Amplification Attacks
  
- Exhaust all resources

UDP-based Amplification Attacks

Protocol	Bandwidth Amplification Factor
Memcached	50000 (fixed in version 1.5.6) <sup>[61]</sup>
NTP	556.9 (fixed in version 4.2.7p26) <sup>[62]</sup>
CharGen	358.8
DNS	up to 179 <sup>[63]</sup>
QOTD	140.3
Quake Network Protocol	63.9 (fixed in version 71)
BitTorrent	4.0 – 54.3 <sup>[64]</sup> (fixed in libuTP since 2015)
CoAP	10 – 50
ARMS	33.5
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

# DDoS: Distributed Denial of Service (1)

- The incoming traffic flooding the victim originates from many different sources
  - Maybe the sources have normal behavior
- Difficult to block all attacking source



# DDoS (2)

---

## □ Botnet

- Comprised computers with malicious software (zombies)
- Launch attacks if the botnet owner gets paid

## □ Clean Pipe

- Multiple layers of filter of DDoS traffic
- Lots of IDSs & IPSs
- “Wash” traffic and direct clean traffic to servers
  - False positive

# Conclusion

---

- Safe design lowers the security risk
  - Multiple layers of protection
  - Encrypt matters
- Logging and auditing
- Keep systems updated
  - Vulnerabilities feed
  - Human review