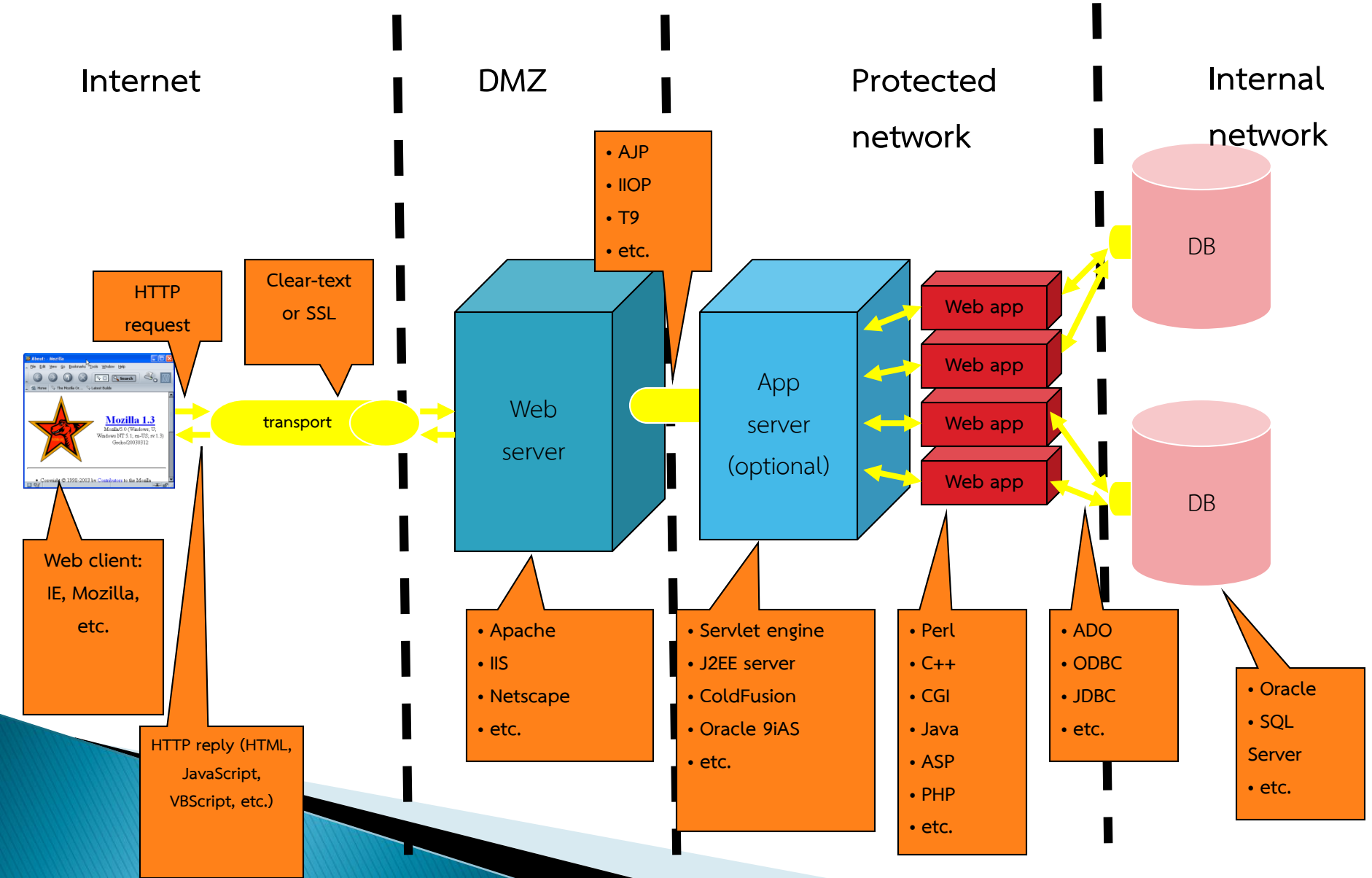
Web Attack and Protection

ดร. ธนัญชัย ตรีภาค

Example Web Application



Web Technology หมายถึงเทคโนโลยีอะไรบ้าง

!!!

รวมพลเกมเมอร์บุกยึด CAT TOWER คืนจากม๊อบ

1 ชม.

วันนี้หลัง 4 ทุ่ม
กลุ่มผู้ที่รวมตัวกันเพื่อต่อต้านระบบซิงเกิลเกตเวย์ จะทำการถล่มเว็บไซต์เชิงสัญลักษณ์ ด้วยวิธีการ DdoS เนื่องจากเป็นวิธีการเชิงสัญลักษณ์เพราะเป็นวิธีที่ทุกคนที่มีโทรศัพท์และอินเตอร์เน็ตสามารถทำได้ เป็นการแสดงให้เห็นถึงพลังของประชาชน
อยากขอเชิญมาร่วมมือกันกับประชาชนผู้รักในความยุติธรรมของกฎหมาย โดยในวันที่ 30 กันยายนหลัง 4 ทุ่มเป็นต้นไป
เป้าหมายแรกของพวกเรา คือเว็บไซต์ของกระทรวงเทคโนโ,ยีและสารสนเทศ
http://www.mict.go.th/view/1/home
วิธีการ
1.ขอให้พวกท่านเชื่อมต่ออินเตอร์เน็ต เปิดเว็บไซต์ [http://www.mict.go.th] ขึ้นมา
2. กดปุ่มโหลดหน้าใหม่ หรือปุ่มรีเฟรช (Refresh) หรือกดปุ่ม F5 บนคีย์บอร์ดคอมพิวเตอร์รัวๆ โดยไม่ต้องยั้ง
เมื่อเว็บไซต์ดังกล่าวล่มไปแล้ว เราจะแจ้งเป้าหมายใหม่ให้ทราบ
มาเถิดเหล่าประชาชนผู้รักความยุติธรรม สิทธิเสรีภาพ และสิทธิในการเข้าถึงข้อมูล
จงกระจายข่าวนี้ร่วมกันซะ
(แหล่งข่าวไม่ประสงค์ออกนาม)

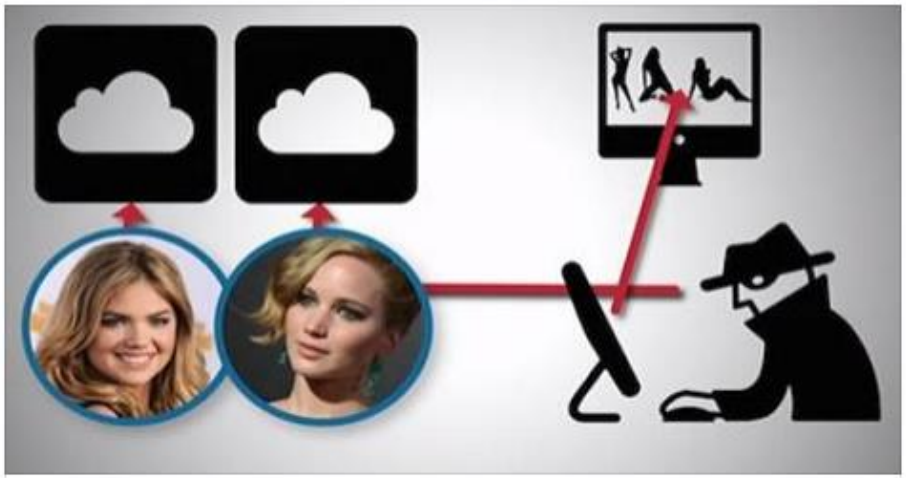
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นองค์กรหลักในการบริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ของประเทศ...

MICT.GO.TH

Any Questions ???

28 year old Russian is the owner of iCloud Hacks leaked images website
http://www.techworm.net/2014/10/sergei-kholodovskii-is-the-owner-of-icloud-hacks.html



Sergei Kholodovskii is the owner of iCloud Hacks leaked images website

Sergei Kholodovskii is the owner of iCloud Hacks leaked images website hosting neatly arranged celebrity images

TECHWORM.NET

Like · Comment · Share

9 people like this.

700,000 Dropbox Credentials Hacked, Hackers dump 'Dropbox Hacks Teasers' on Pastebin

http://www.techworm.net/2014/10/700000-dropbox-credentials-hacked-hacker-leaks-dropbox-hacks-teasers-pastebin.html

700,000 Dropbox credentials hacked, hacker leaks 'Dropbox Hacks Teasers' on Pastebin

700,000 Dropbox credentials hacked, hacker leaks 'Dropbox Hacks Teasers' on Pastebin 3 pastes online, more to follow says the hacker

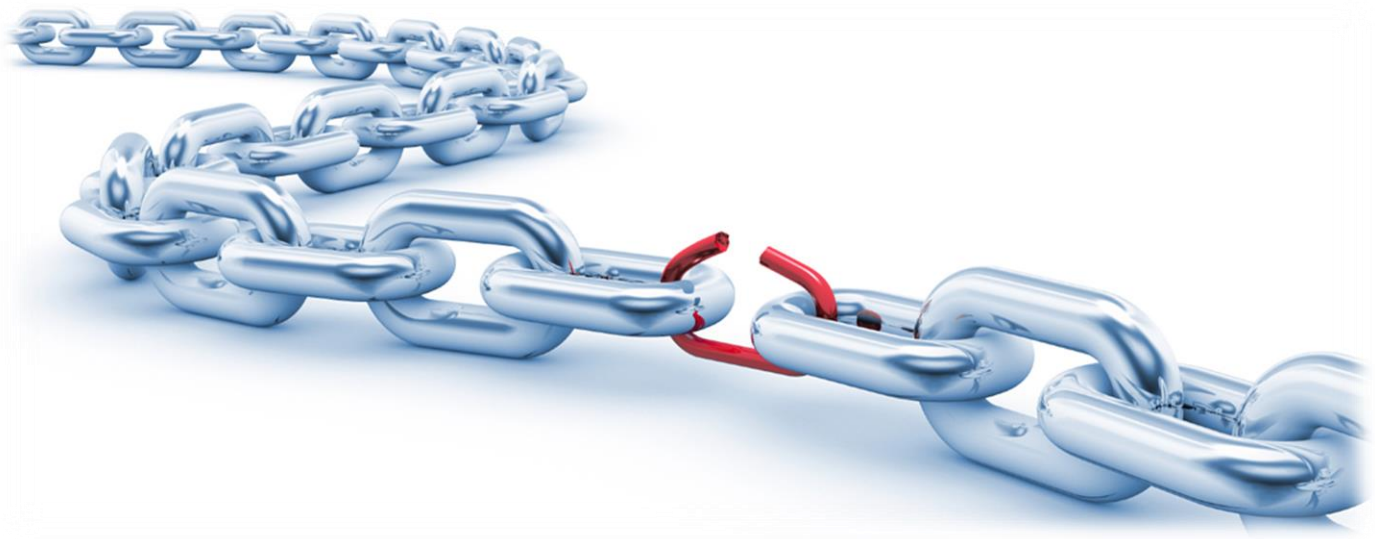
TECHWORM.NET

Like · Comment · Share

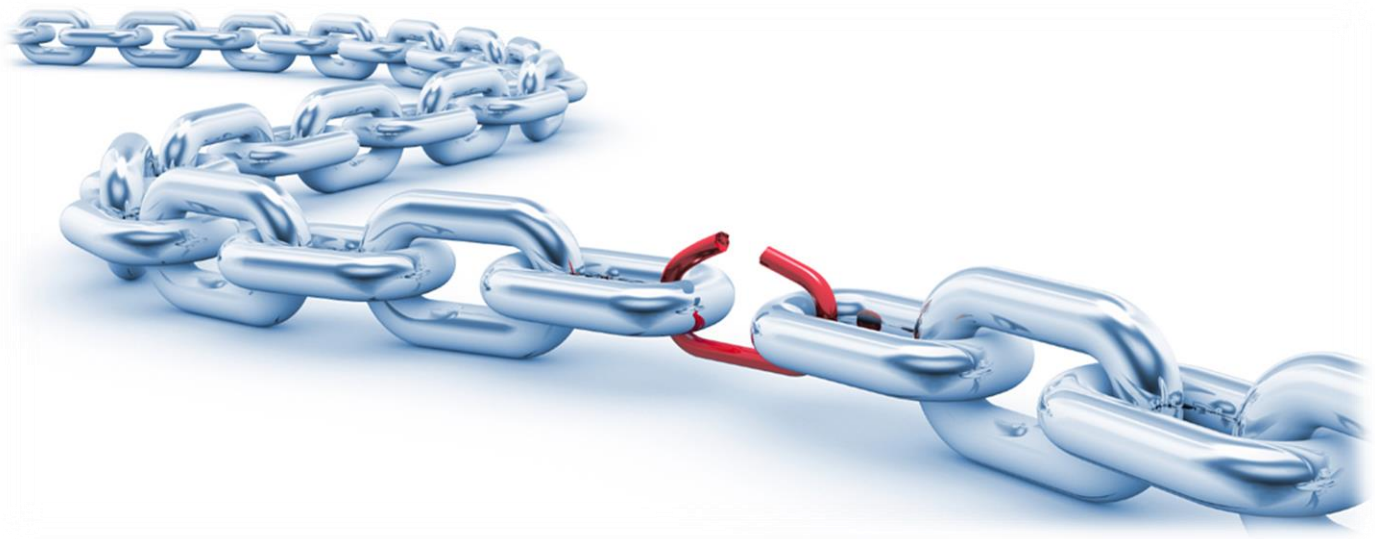
Any Questions ???

การบุกรุกระบบ มีขั้นตอนพื้นฐานอย่างไร

ช่องโหว่ (Vulnerability) หมายถึงอะไร



http://www.cvedetails.com



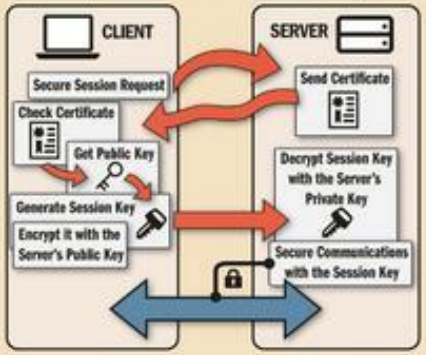
การอาศัยช่องโหว่ (Exploit) คืออะไร

ตัวอย่าง Exploit

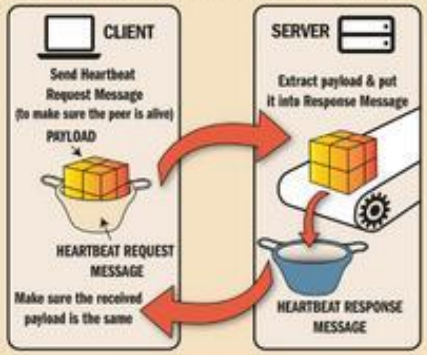
- Heartbleed – OpenSSL Exploit
- Shellshock – Bash Exploit

HEARTBLEED - THE OPENSSL HEARTBEAT EXPLOIT

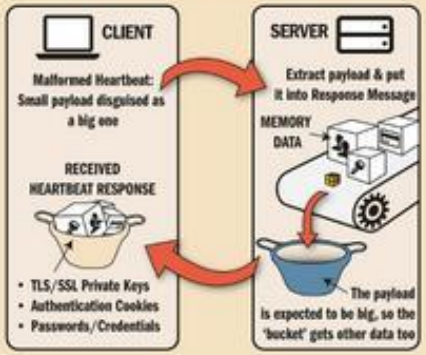
HOW TLS (TRANSPORT LAYER SECURITY) WORKS

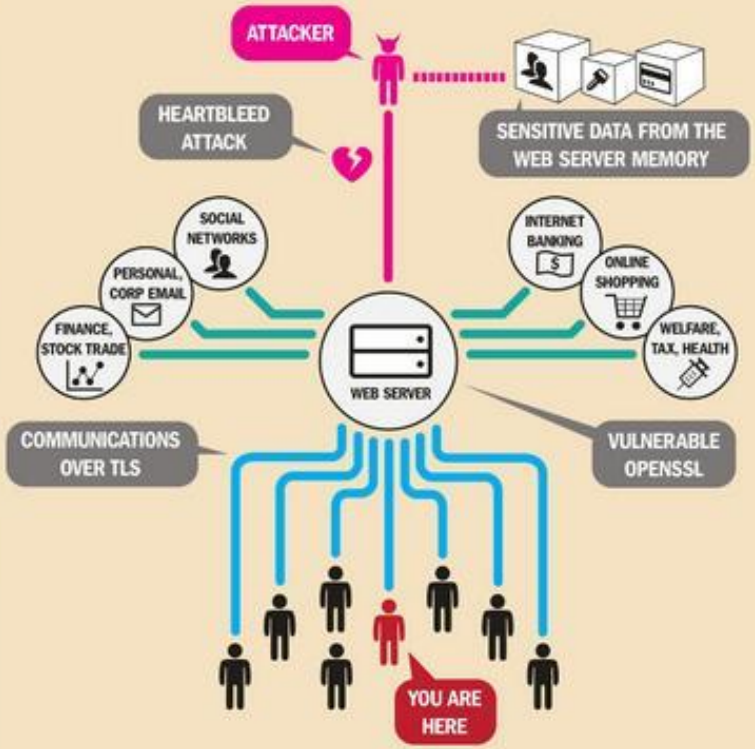


HOW HEARTBEAT EXTENSION FOR TLS WORKS

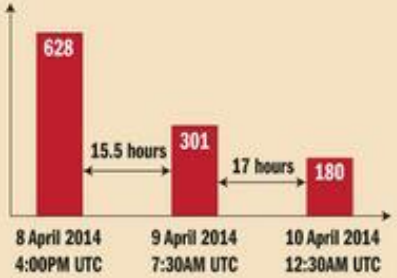


HOW THE HEARTBLEED EXPLOIT WORKS





NUMBER OF THE VULNERABLE WEBSITES AMONG TOP 10,000



RECOMMENDATIONS

- Check & Upgrade OpenSSL
- Change passwords & keys
- Apply IDS signatures
- Buy a new TLS certificate

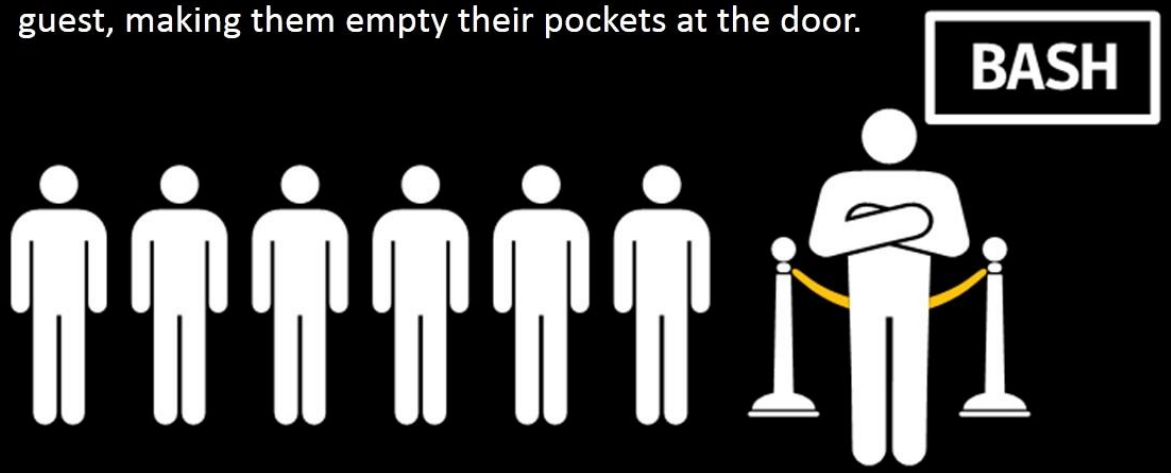
E: cyberresponse@baesystems.com
E: marketingai@baesystems.com
W: www.baesystems.com/ai

Applied Intelligence

BAE SYSTEMS

How Shellshock Works

Think of Shellshock as the doorman at a nightclub called, "Bash". Normally, the doorman knows exactly who to let into the party by checking a list of approved commands, and by screening each guest, making them empty their pockets at the door.



In the case of the Shellshock bug, the doorman asks the next person in line to empty his pockets(the unexpected command, executed by the attacker), and to put the contents in a basket (the environment variable).

The doorman checks his list to allow the good command in, while the basket with the unexpected command in it goes on ahead, unchecked. With the unexpected command inside, the attacker now has free reign to wreak havoc in the club.

environment variable).

The doorman checks his list to allow the good command in, while the basket with the unexpected command in it goes on ahead, unchecked. With the unexpected command inside, the attacker now has free reign to wreak havoc in the club.

Norton by Symantec

กิจกรรม :

- 1. กำหนด Framework ของ Web Application
  - XAMPP , LAMP
  - Appserv
  - Microsoft Framework
  - อื่นๆ
- 2. ซอฟต์แวร์ที่ใช้ ปีที่แล้วมีช่องโหว่ และ Exploit สำคัญ (CVSS >=8) อะไรบ้าง
- 3. ต้องปรับปรุงระบบอย่างไรบ้าง เพื่อให้ระบบมีความปลอดภัย

การทำงานของ TCP/IP ที่ทำให้เกิดความไม่ปลอดภัยคืออะไร

พฤติกรรมของ Social Network ที่ทำให้เกิดความไม่ปลอดภัย มีอะไรบ้าง

การทำงานของ Web Technology ที่ทำให้เกิดความไม่ปลอดภัยคืออะไรบ้าง

OWASP Top 10 - 2013

คำอธิบายที่สั้นที่สุด
คืออะไร...

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Known Vulnerable Components
- A10 – Unvalidated Redirects and Forwards

ในฐานะ User ต้องตระหนักถึงภัยคุกคามจาก Web Technology อะไรบ้าง

ในฐานะผู้ดูแลระบบ Web Application ต้องตระหนักถึงภัยคุกคามอะไร

ในฐานะ Web Application Developer ต้องตระหนักถึงภัยคุกคามอะไร

การป้องกัน Web Attack ทำได้อย่างไร

จะมั่นใจได้อย่างไรว่าจะไม่เกิดความเสียหายจาก Web Attack

สรุป / บทเรียน