Basic Security

Security Awareness

Privacy

Meaning

คือความเป็นส่วนตัวของข้อมูล รวมไปถึงการควบคุมสิทธิการเข้าถึงข้อมูลต่าง ๆ ความเป็นส่วนตัวมีได้ขอบเขตได้หลากหลายตั้งแต่ตัวบุคคล องค์กร ไปจนถึงประเทศชาติ ตัวอย่างข้อมูลส่วนตัว เช่น จดหมาย, บัญชีผู้ใช้งาน (Username), รหัสผ่าน(Password), รหัสบัตรประชาชน, บันทึกประจำวัน, ผลโหวตเลือกตั้ง เป็นต้น

Privacy Policy

คือนโยบายคุ้มครองความเป็นส่วนตัวของผู้ใช้ ใช้สำหรับแจ้งว่าเมื่อใช้บริการ ผู้ให้บริการจะใช้ข้อมูลที่เราให้ไปทำอะไรบ้าง หากต้องการทำงานที่ต้องการความปลอดภัยสูง ควรศึกษานโยบายนี้ให้ดี เพื่อป้องกันข้อมูลสำคัญถูกนำไปใช้ในทางที่ผิด เช่น เปิดเผยต่อบุคคลที่สาม

How to protect your Privacy

1. เก็บข้อมูลสำคัญ/อ่อนไหวไว้กับตัวเอง อย่าให้ผู้อื่นได้รู้ เช่น รหัสผ่านไม่ควรจดบันทึกไว้
2. ใช้รหัสผ่านในการเก็บข้อมูล
3. ใช้โปรแกรม Antivirus เพื่อป้องกันภัยจากไวรัสที่อาจทำลายหรือขโมยข้อมูลจากอุปกรณ์ของเรา
4. ใช้งานซอฟต์แวร์ และฮาร์ดแวร์ที่มีความน่าเชื่อถือสูง
5. อัพเดทซอฟต์แวร์ และ OS ให้ทันสมัยเสมอเพราะโดยปกติ รุ่นที่ใหม่กว่าจะออกอัพเดทเพื่อแก้ไขช่องโหว่เก่า ๆ
6. อย่าให้ข้อมูลกับคนอื่นมากเกินไป เราไม่สามารถมั่นใจได้ว่าข้อมูลที่เราให้ไป จะถูกเก็บเป็นความลับหรือไม่ หรือนำไปถูกใช้ในทางที่ผิดหรือไม่

Social Engineering

Meaning

คือศิลปะในการหลอกลวง/ตบตาโดยใช้หลักทางจิตวิทยาเพื่อทำให้ได้มาซึ่งสิทธิ ข้อมูล ทรัพย์สินต่าง ๆ หรือการกระทำตามที่ต้องการ โดยอาศัยความประมาท ความสับสน ความรู้เท่าไม่ถึงการณ์ของเหยื่อ ตัวอย่าง Social Engineering มีหลายแบบเช่น

1. **Phishing** คือการหลอกลวงเอาข้อมูลสำคัญผ่านทางแหล่งต่าง ๆ เช่น รหัสผ่าน, เลขบัตรเครดิตเป็นต้น สามารถพบได้หลากหลายรูปแบบ เช่น อีเมลปลอม, อีเมลข่มขู่, SMS หลอกลวง หน้าเว็บปลอม เป็นต้น
2. **Dumpster Diving** คือการค้นข้อมูลจากเอกสารที่ถูกทิ้ง ซึ่งเอกสารเหล่านั้นอาจมีข้อมูลสำคัญที่ต้องการอยู่แล้ว จากนั้นนำมารวบรวมกันแล้วสังเคราะห์เป็นข้อมูลสำคัญที่เราต้องการ วิธีนี้สามารถป้องกันได้โดยการทำลายเอกสารให้ใช้การไม่ได้ก่อนทิ้ง
3. **Water Holing** เป็นการใช้แนวคิดว่าคนเราจะถูกหลอกลวงได้ง่ายเมื่อเขาคิดว่าอยู่ในที่ซึ่งปลอดภัยและเป็น “ถิ่นของตนเอง” เช่น การฝังลิงก์ไวรัสไว้ในหน้าเว็บที่คนเชื่อถือ
4. **Impersonation** เป็นการหลอกว่าผู้ก่อเหตุเป็นบุคคลที่มีชื่อเสียง น่าเชื่อถือเพื่อหลอกเอาข้อมูลเช่น การบอกว่าเป็นตำรวจ การหลอกว่าเป็นดารา/นักธุรกิจดัง มักใช้ประกอบ Social Engineering รูปแบบอื่น
5. **Tailgating** เป็นการเข้าไปในพื้นที่ซึ่งผู้ก่อเหตุไม่ได้รับอนุญาตโดยการเดินตามคนที่สามารถเข้าไปได้เข้าไปในพื้นที่ หรือการใช้บัตรผ่านปลอม

6. **Shoulder Surfing** เป็นการแอบดูข้อมูลของคนอื่นอย่างแนบเนียน ในขณะที่บุคคลเหล่านั้นยังทำ การกรอก / ดูข้อมูลนั้นอยู่ เช่น การแอบดูแชท การแอบดูรหัสผ่านคอมพิวเตอร์

Social Engineering Principles

1. **การตอบแทน** มักสร้างเหตุการณ์สักอย่างขึ้นมาให้เหยื่อไปช่วย แล้วหลอกลวงเรื่องการตอบแทนเหยื่อโดยมีข้อแลกเปลี่ยนที่ไม่เป็นธรรม เช่น แก๊งตกทอง, Good cop/Bad cop
2. **การสร้างพันธะสัญญาและความต่อเนื่อง** เป็นการชี้นำให้เหยื่อเกิดความผูกพันกับการกระทำบางอย่าง เช่น การปิดหน้าต่างลงทะเบียนกับเว็บด้วยคำว่า “I’ll sign up later.” หรือการทำ Click Shaming เมื่อกดไม่ซื้อสินค้าโปรโมชั่นว่า “No thanks, I hate cheap goods.”
3. **การเลียนแบบ** เป็นการทำสิ่งต่าง ๆ ให้เหยื่อรู้สึกว่าต้องทำตาม เคยมีการทดลองหนึ่งให้หน้าม้าไปยืนมองท้องฟ้าหลาย ๆ คน แล้วคนที่เดินผ่านไปมาในบริเวณนั้นส่วนใหญ่จะแหงนหน้ามองท้องฟ้าไปด้วย หรือการทดลองยืนหันหลังตอนเข้าลิฟต์ คนที่เพิ่งเข้าลิฟต์มาใหม่ก็จะหันหลังตามไปด้วย
4. **ความมีอำนาจ** ผู้คนมักทำตามบุคคลที่มีอำนาจ หรือมีชื่อเสียง ไม่ว่าการกระทำนั้น ๆ จะแปลกประหลาดเพียงใดก็ตาม
5. **ความชอบพอ** ผู้คนมักจะเชื่อในคนที่ตนเองชอบได้ง่ายกว่า มีการศึกษาว่าหลาย ๆ ครั้งเราไม่ได้ซื้อของ เพราะเราอยากได้แต่เราซื้อเพราะว่าเราชอบลักษณะของพนักงานที่ขายของให้เรา
6. **ความขาดแคลน** ผู้คนจะต้องการได้รับสิ่งของ / สัญญาเมื่อสิ่งนั้น ๆ หาได้ยาก หรือเหลือน้อยแล้ว เช่น การบอกว่าสินค้านี้ลดราคาเฉพาะวันนี้เท่านั้น

How to protect yourself from Social Engineering

1. ฝึกฝนตนเองให้มีความระมัดระวังตัวอยู่เสมอ
2. ออกนโยบาย และใช้งานแนวทางปฏิบัติเกี่ยวกับความปลอดภัยของข้อมูลองค์กร
3. รู้ว่าข้อมูลใดมีความสำคัญอย่างไร และปกป้องข้อมูลสำคัญไม่ให้ผู้อื่นรับรู้
4. ทำการสุ่มทดสอบเกี่ยวกับความปลอดภัยอยู่เสมอ
5. รู้ทันแนวทางการ Social Engineering
6. ทบทวนและประเมินหลักการปฏิบัติด้านความปลอดภัยอยู่เสมอ
7. ทำลายข้อมูลที่จะทิ้งแล้วเสมอ อย่าให้สามารถเก็บกู้ได้

Password

Password Attacking

การโจมตีเพื่อให้ได้มาซึ่งรหัสผ่านมีหลากหลายวิธี แต่วิธีซึ่งเป็นที่นิยมใช้งานมีดังนี้

1. **Brute Force Attack** เป็นการทดลองแทนค่ารหัสผ่านไปเรื่อย ๆ จนกว่าจะเจอรหัสผ่านที่ถูกต้อง เป็นวิธีการที่ใช้เวลานานมากแต่การันตีว่าสามารถหารหัสผ่านได้แน่นอน
2. **Dictionary Attack** เป็นการใช้รายการรหัสผ่านที่ผู้คนนิยมใช้งานมาแทนค่าไปเรื่อย ๆ จนกว่าจะเจอรหัสผ่านที่ถูกต้อง ข้อดีคือเร็วกว่าการทำแบบ Brute Force แต่ข้อเสียคือไม่สามารถใช้หารหัสผ่านที่ซับซ้อน หรือไม่มีใน Dictionary ได้ ตัวอย่าง Dictionary เช่น rockyou.txt
3. **Phishing** ซึ่งได้อธิบายในส่วนของ Social Engineering ไว้เรียบร้อยแล้ว
4. **Rainbow Table Attack** เป็นการใช้ Rainbow Table ซึ่งเป็นตารางที่คำนวณค่าแฮช (Hash) ของรหัสผ่านหลาย ๆ รหัสไว้ล่วงหน้า เพื่อคาดเดารหัสผ่าน
5. **Credential Stuffing** เป็นการใช้ข้อมูลผู้ใช้ที่รั่วไหลมาแล้วทำการพยายามเข้าสู่ระบบ มักใช้บอทในการทำงาน ซึ่งจะนำไปสู่การได้ข้อมูลผู้ใช้ที่เจาะได้มากขึ้นอีกเรื่อย ๆ สามารถป้องกันได้โดยการใช้ Multi-Factor Authentication หรือการทำ Captcha เป็นต้น
6. **Password Spraying** เป็นการทดลองใช้รหัสผ่านเดียวในการพยายามเข้าถึงบัญชีผู้ใช้หลาย ๆ บัญชี วิธีนี้จะแตกต่างจากวิธีอื่นซึ่งเน้นไปที่การเข้าถึงบัญชี ๆ เดียว
7. **Keylogger Attack** เป็นการตรวจจับว่ามีการกดคีย์บอร์ดปุ่มใดบ้างในขณะใดขณะหนึ่ง ซึ่งกรณีนี้จะสนใจเมื่อมีการกรอกข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรเครดิต เป็นวิธีที่มักจะใช้มัลแวร์ (Malware) มาช่วยในการตรวจจับแล้วทำการส่งข้อมูลไปให้ผู้โจมตีต่อ

Secure Password

1. อย่าใช้รหัสผ่านที่ผู้คนใช้กันบ่อยหรืออยู่ใน Dictionary
2. ใช้รหัสผ่านที่ยาวตั้งแต่ 15 ตัวอักษรขึ้นไป
3. ใช้อักขระให้หลากหลายประกอบไปด้วยตัวเลข ตัวอักษรพิมพ์เล็ก และพิมพ์ใหญ่ และมีอักขระพิเศษผสมอยู่
4. เมื่อทำการแทนค่าตัวอักษรเป็นตัวเลข ไม่ควรแทนค่าด้วยสิ่งที่ผู้คนนิยมใช้กันเช่น DOORBELL - D00R8337 พูดให้ง่ายก็คือ LEET อย่างชาญฉลาดนั่นเอง
5. อย่าใช้รหัสผ่านที่เป็นลำดับบนคีย์บอร์ดซึ่งจำได้ง่าย เช่น QWERTY
6. ใช้ Passphrase แทน Password
7. อย่าใช้รหัสผ่านที่มีข้อมูลเกี่ยวข้องกับตัวเราเช่น วันเกิด, ชื่อแฟน, เบอร์โทรศัพท์
8. ใช้ Password Generator ที่เชื่อถือได้
9. ใช้ Password Manager ที่เชื่อถือได้
10. อย่าเก็บรหัสผ่านไว้ หากจำเป็นต้องเก็บ ให้เก็บไว้ในที่ซึ่งมีแต่ตนเองเท่านั้นที่รู้

Passphrase

คือรหัสผ่านรูปแบบหนึ่งซึ่งไม่ใช่แค่คำหรือตัวเลข แต่เป็นการนำคำหลาย ๆ คำมารวมกันเป็นวลีหรือประโยคซึ่งยากต่อการคาดเดา ซึ่งวิธีนี้จะสามารถทำให้รหัสผ่านเรายาวมากขึ้น เราจำได้ง่าย แต่คนอื่นคาดเดาได้ยาก หลักการตั้ง Passphrase ซึ่งเป็นที่นิยมมีอยู่ 2 แบบคือ

1. **Revised Passphrase Method** เป็นการนำคำที่ยาก ไม่คุ้นเคย ชื่อเฉพาะ คำภาษาต่าง ๆ มาตั้งรวมกันเป็นรหัสผ่าน เช่น MatlabHelios500HitlerPakaewYeti

2. **Sentence Method หรือ Bruce Schneiner Method** เป็นการนำประโยคมาดัดแปลงตามหลักการตั้งรหัสผ่านเช่น The Old Duke is my favorite pub in South London แล้วเอาแค่ 2 ตัวแรกแต่ละคำมาเป็นรหัสผ่านจะได้ ThOlDuismyfapuinSoLo

Password/ passphrase	Time to crack		Easy to remember	Comments
	Brute force attack	Dictionary attack		
password123	Instantly. Less than AU$0.01	Instantly. Less than AU$0.01	Very easy (too easy)	One of the most commonly-used passwords on the planet.
Spaghetti95!	48 hours AU$587.50	Less than half an hour AU$6.10	Easy	Some complexity in the most common areas, and very short length. Easy to remember but easy to crack
5paghetti!95	24 hours AU$293.70	Less than 1 hour AU$12.20	Somewhat easy	Not much more complexity than above with character substitution, and still short length. Easy to remember but easy to crack.
A&d8J+1!	2.5 hours AU$30.60	2.5 hours AU$30.60	Very difficult	Mildly complex, but shorter than the above passwords. Hard to remember, easy to crack (against BFA).
I don't like pineapple on my pizza!	**More than 1 year. More than AU$107,222.40**	**More than 40 days. More than AU$11,750.40**	**Easy**	**Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember and very difficult to crack.**

https://www.cyber.gov.au/acsc/view-all-content/guidance/comparison-password-vs-passphrase

Attacking Types

1. **Dos DDos :** Dos = การ Flood Traffic ของเป้าหมาย ให้ไม่สามารถทำงานได้ DDos = ใช้หลายเครื่องโจมตี (Distributed Denial of Services)
2. **Smurf attack :** ปลอมเป็นไอพีของเหยื่อ และทำการ Broadcast ICMP Packets ไปให้เครื่องอื่นๆในnetwork เครื่องอื่น ๆ ในเครือข่ายจะ Response ไปที่เครื่องของเหยื่อ ทำให้ Traffic jam ทำงานไม่ได้ นับเป็น DDos รูปแบบนึง
3. **Spoofing :** การปลอมเป็นบุคคล, องค์กร หรืออื่นๆที่ไม่ใช่เรา
4. **Man in the Middle** : การแอบดักฟัง/แก้ไขการเชื่อมต่อระหว่างกัน
5. **Replay Attack :** เป็นรูปแบบหนึ่งของ Man in the middle (lower form) โดยการดักแพ็คเก็ต session password และสิ่งที่ใช้ยืนยันตัวตนอื่นๆ เพื่อนำไปปลอมตัวเป็นคนอื่น
6. **Password Attack :** เหมือนดังที่กล่าวไปก่อนหน้านี้
7. **Dns Poisoning :** การใส่ข้อมูลที่ผิดลง DNS ex. Local dns to malicious site
8. **Typosquatting / URL Hijacking :** ตั้งชื่อคล้ายของจริง หลอกให้คนเชื่อ
9. **Watering Hole Attack :** ปล่อยของอันตรายไว้บนเว็บที่ปลอดภัย
10. **Zero-day Vulnerabilities :** ช่องโหว่ที่รู้ หรือไม่รู้ที่อยู่ใน Version ที่ Deploy ไปแล้ว
11. **App Attack**
    a. Buffer Overflow app : จะจองบัพเฟอร์ไว้ให้ข้อมูล ถ้าเกินจะเกิดปัญหา อาจเขียนทับที่เดิม ไปทับที่อื่นๆ (Arbitrary Code, Memory Layout)
    b. Integer overflow : int เกิน to heap Overflow
12. **SQL Injection :** ใส่ input เป็น code ให้query หรือทำสิ่งไม่พึงประสงค์ เช่น
    a. statement = "**SELECT** * **FROM** users **WHERE** name = '" + userName + "';"
    b. ' OR '1'='1
    c. **SELECT** * **FROM** users **WHERE** name = '' **OR** '1'='1';
    d. **SELECT** * **FROM** users **WHERE** name = '' **OR** '1'='1' -- ';
    e. a';**DROP TABLE** users; **SELECT** * **FROM** userinfo **WHERE** 't' = 't
    f. **SELECT** * **FROM** users **WHERE** name = 'a';**DROP TABLE** users; **SELECT** * **FROM** userinfo **WHERE** 't' = 't';
13. **XSS / Cross Site Scripting**
    a. Stored XSS : โค้ดอันตรายถูกเก็บไว้บนserverที่ไว้ใจได้แบบถาวร
    b. Reflected XSS : โค้ดอยู่ในlink linkไปที่เว็บที่ไว้ใจได้ ที่มีช่องโหว่ submit codeไปที่เว็บ reflecกลับมาที่ browser

CIA Triad

ย่อมาจากคำว่า Confidentiality, Integrity และ Availability เป็นแกนหลักในการศึกษาเกี่ยวกับด้าน Information Security แต่ละส่วนสามารถขยายความได้เป็นดังนี้

Confidentiality

Confidentiality หรือความปลอดภัยของข้อมูล คือข้อมูลมีการเก็บรักษาไว้ดีหรือไม่ ใครสามารถเข้าถึงข้อมูลนี้ได้บ้างตัวอย่างที่เกี่ยวข้องกับด้านนี้ เช่น การเก็บรักษาเอกสารสำคัญ, การเก็บรักษารหัสผ่าน, การสื่อสารเนื้อหาสำคัญในพื้นที่สาธารณะ เป็นต้น

การป้องกันความปลอดภัยของข้อมูลในโลกไซเบอร์มีได้หลายรูปแบบ เช่น การเข้ารหัสลับข้อมูล, การสื่อสารผ่านโปรโตคอล HTTPS, การใช้ Two-Factor Authentication เป็นต้น

Integrity

Integrity หรือความถูกต้องของข้อมูล คือข้อมูลที่ได้รับหรือเก็บไว้ ต้องมีความถูกต้อง ไม่ถูกดัดแปลงให้เป็นอย่างอื่น เช่น เมื่อเราทำการดาวน์โหลดไฟล์มา ไฟล์ที่เราได้รับต้องเหมือนกับต้นทาง ไม่มีความเสียหายเกิดขึ้นขณะดาวน์โหลดหรือมีการดัดแปลงไฟล์ให้คุณสมบัติเปลี่ยนไป

ในชีวิตประจำวันเราสามารถตรวจสอบความถูกต้องของข้อมูลได้อย่างง่ายดาย เช่น การถามทวนซ้ำเพื่อให้มั่นใจว่าเข้าใจถูกต้องตรงกัน แต่สำหรับคอมพิวเตอร์แล้วหากเราใช้วิธีการ “ถามซ้ำ” จะเป็นการใช้เวลานาน จึงมีการคิดค้นวิธีการตรวจสอบความถูกต้องขึ้นมาวิธีหนึ่งเรียกว่า Hashing โดยจะทำการนำข้อมูลและคุณสมบัติต่าง ๆ ของไฟล์มาผ่านกระบวนการทางคณิตศาสตร์เพื่อสร้างชุดของตัวอักษรออกมาชุดหนึ่งซึ่งไม่สามารถแปลงกลับไปเป็นข้อมูลเดิมได้ ข้อมูลชุดเดิมจะได้ค่า Hash ออกมาเป็นค่าเดิมเสมอ ตัวอย่างวิธีการ Hashing เด่น ๆ เช่น MD5, SHA-1, SHA-2 เป็นต้น

Availability

Availability หรือความพร้อมในการใช้งาน คือข้อมูล และบริการต้องสามารถเข้าถึงได้โดยผู้ใช้ที่มีสิทธิ์ในการเข้าถึงได้ยู่เสมอ เช่นจะดูตารางเรียนในเว็บไซต์มหาวิทยาลัยก็ต้องดูได้เสมอ ไม่ใช่ว่าตอนนี้ดูได้แต่ว่าวันต่อมากลับดูไม่ได้

Basic Cyber Security

Malware

Malicious Software คือโปรแกรมที่สร้างขึ้นเพื่อประสงค์ร้ายต่อเครื่องเพื่อใช้ล้วงข้อมูล หรือทำลายระบบคอมพิวเตอร์ของผู้ใช้ มีหลายประเภท เช่น

1. **Adware** เพื่อทำการโฆษณาโดยที่เราไม่ต้องการโดยอัตโนมัติ
2. **Backdoor** ทำให้สามารถเข้าถึงอุปกรณ์ของผู้อื่นได้โดยไม่ต้องผ่านระบบรักษาความปลอดภัยของอุปกรณ์นั้น ๆ
3. **Bot** คือซอฟต์แวร์ที่ทำงานประสงค์ร้ายโดยอัตโนมัติ โดยอาจใช้งานเครื่องของผู้ใช้อื่นเป็นตัวแทนของ Bot เช่น Botnets ที่สร้างเพื่อ DDoS หรือ Spambot ที่ใช้ส่ง Spam
4. **Bug** เกิดจากความผิดพลาดโปรแกรมที่อาจเป็นช่องโหว่ให้ผู้ไม่ประสงค์ดีสร้างความเสียหายได้
5. **Logic Bomb** จะทำงานตามเงื่อนไขที่ผู้โจมตีเป็นคนกำหนด เช่น เมื่อถึงวันที่กำหนด เมื่อมีการทำงานตรงเหตุการณ์บางอย่าง
6. **Ransomware** เข้ารหัสไฟล์ทำให้ไม่สามารถใช้งานไฟล์ได้ ซึ่งต้องจ่ายค่าไถ่ให้ hacker เพื่อถอดรหัสไฟล์คืนซึ่งไม่สามารถการันตีได้ว่าจะได้คืนหรือไม่ Ransomware หลาย ๆ ตัวมีผู้สามารถแก้ไขการเข้ารหัสได้แล้ว
7. **Rootkit** ควบคุมเครื่องและเข้าใช้จากระยะไกล สามารถซ่อนตัวได้แนบเนียน ทำให้ลบและตรวจจับยาก (ทำงานในระดับ Kernel: ชั้นติดต่อระหว่าง Hardware และ Software) มักเป็นหน่วยเสริมให้มัลแวร์ตัวอื่น ๆ
8. **Spyware** ทำการเก็บข้อมูลจากผู้ใช้แล้วส่งให้ hacker เช่น keylogger
9. **Trojan Horse** ทำตัวเสมือนโปรแกรมปกติเพื่อหลอกให้โหลดมาใช้งาน เมื่อใช้แล้วจะเปิดช่องโหว่ให้ hacker เข้าควบคุมหรือขโมยข้อมูลได้
10. **Virus** สามารถทำให้อุปกรณ์อื่น ๆ “ติดเชื้อ” ได้โดยผ่าน Script file, Document file ที่ต้องสั่งใช้งานก่อน เกิดผลกระทบได้หลายอย่าง เช่น ขโมยข้อมูล เครื่องช้า หยุดทำงาน
11. **Worm** แพร่กระจายผ่าน Network และ Internet โดยใช้ช่องโหว่ของ OS เพื่อสร้างความเสียหาย ลบไฟล์ สร้างไฟล์ ขโมยไฟล์ ส่วนใหญ่มักกระจายผ่าน E-mail โดยแนบไฟล์ที่มี worm ไปด้วย

OWASP Top 10 2017

เป็นการจัดลำดับช่องโหว่ด้าน Cybersecurity ที่พบได้มากที่สุด 10 อันดับภายใน ค.ศ. 2017 รายการเป็นดังนี้

1. **Injection** เป็นการใส่ Malicious Code เข้าไปสู่ระบบและหลอกให้ระบบทำงานคำสั่งเหล่านั้น
2. **Broken Authentication** อาศัยช่องโหว่ในการระบุตัวตนผู้ใช้งาน เพื่อทำการปลอมแปลงเป็นบุคคลอื่น หรือยกระดับสิทธิ์การเข้าถึงของตนเอง
3. **Sensitive Data Exposure** คือการปล่อยข้อมูลอ่อนไหวให้ผู้อื่นได้รับรู้ผ่านหน้าเว็บหรือ API
4. **XML External Entities (XXE)** เป็นการใช้ XML ในการโจมตีบริการที่ใช้ XML มักใช้เพื่อเอาข้อมูลไฟล์หรือเข้าถึง Backend
5. **Broken Access Control** การจำกัดสิทธิการเข้าถึงข้อมูลที่ผิดพลาดหรือไม่มี
6. **Security Misconfiguration** ไม่มีการตั้งค่าความปลอดภัยที่เหมาะสม เช่น การแสดง Error Log ให้คนอื่นเห็น หรือใช้ Default Username / Password หรือ
7. **Cross-Site Scripting XSS** การฝัง Javascript ไว้ที่เว็บที่ทำงานเพื่อขโมยข้อมูล หรือสร้างความเสียหายให้กับผู้ใช้งาน/เจ้าของเว็บไซต์
8. **Insecure Deserialization** เป็นการแฝงคำสั่งอันตรายเข้าสู่ระบบโดยอาศัยช่องโหว่ของการถอดรหัสออบเจกต์
9. **Using Components with Known Vulnerabilities** ใช้ฮาร์ดแวร์ หรือซอฟต์แวร์ที่มีช่องโหว่อันเป็นที่รู้จัก
10. **Insufficient Logging & Monitoring** การขาดความระมัดระวัง และตรวจตราการโจมตีระบบ

Community

- สอนแฮกเว็บแบบแมว ๆ
- 2600 Thailand
- IEEE Cybersecurity Community
- สยามถนัดแฮก

CTF

Cybersecurity เป็นการแข่งขันด้าน Cybersecurity ประเภทหนึ่ง โดยผู้เข้าแข่งขันจะพยายามเอา Flag ซึ่งเปรียบเสมือนข้อมูลสำคัญออกมาให้ได้ด้วยความรู้ทางคอมพิวเตอร์ สามารถแบ่งประเภทได้เป็น 4 แบบหลัก ๆ คือ

1. **Jeopardy** จะมีลักษณะการแข่งขันจะเป็นการทำโจทย์แต่ละข้อซึ่งอาจมีความเกี่ยวเนื่องกันแต่ละข้อมีหมวดหมู่ที่แตกต่างกัน
2. **Attack - Defend** จะแบ่งผู้เข้าแข่งขันเป็น 2 ทีม คือ Red Team ซึ่งมีหน้าที่พยายามเข้ายึดระบบโดยนำ Flag ออกมาที่ซ่อนอยู่ออกมา และ Blue Team มีหน้าที่ป้องกันการโจมตีระบบ
3. **King of the Hill** จะแข่งโดยให้ผู้เข้าแข่งขันทุกทีมพยายามยึดเซิร์ฟเวอร์ให้ได้นานที่สุด โดยจะเป็นการผสมการโจมตี และการป้องกันไปในตัว
4. **Linear CTF** โจทย์จะมีความเกี่ยวเนื่องกัน ต้องทำโจทย์ก่อนหน้าก่อนถึงจะสามารถทำโจทย์ข้อต่อไปได้ ในที่นี้จะเน้นไปที่การแข่งขันในรูปแบบ Jeopardy

โจทย์การแข่งขันแบบ Jeopardy จะแบ่งโจทย์เป็นประเภทต่าง ๆ ได้หลากหลายรูปแบบเช่น

1. **Network** : PCAPs, Communication, Port Knocking
2. **Crypto** : การเข้ารหัส/ถอดรหัสข้อความ
3. **Web** : HTTP, Web technology, JS, XSS, SQL injection, Directory Traversal
4. **Forensics** : Steganography, Windows forensics, Linux forensics
5. **Binary** : reverse engineer
6. **Pwnables** : Buffer overflow, format string
7. **Real Life** : โลกความจริง
8. **Trivia/Recon** : ความรู้ทั่วไป/google search

CTF Website

- www.root-me.org
- picoctf.org
- www.hackthebox.eu
- https://ctf.hacker101.com
- https://ctftime.org
- https://overthewire.org

การบ้าน

1. ทำการสมัครเข้าใช้งานเว็บไซต์ PicoCTF (picoctf.org)
2. ให้ตั้งค่ารหัสผ่านเป็นรูปแบบ Passphrase
3. ไปที่หมวด Practice เลือก All Category แล้วทำข้อต่อไปนี้
    a. Lets Warm Up
    b. The Numbers
    c. 2Warm
    d. Insp3ct0r
    e. Glory of the Garden
    f. Vault-door-training
    g. Warmed Up

ส่ง Flag ผ่าน Google Form ภายในวันจันทร์ที่ 19 ตุลาคม พ.ศ. 2563