



# ความปลอดภัยคอมพิวเตอร์ (424)

## Open Web Application Security Project (OWASP)

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาชีวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์  
Email : songrit@npu.ac.th  
สาขาวิชาชีวกรรมคอมพิวเตอร์  
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

Revised 2020-06-26

# ผลให้ต รูปแบบการสอบปลายภาค

1

0

6

5

เดี่ยวข้อเขียน

เดี่ยวสอบ LAB

เดี่ยว CTF

คู่ CTF

# Agenda

---

- **แนะนำ OWASP**
  - สถาบันสร้างความมั่นคงปลอดภัยด้านเว็บ
  - Open Web Application Security Project
  - <https://owasp.org>
  - <https://www.facebook.com/groups/owaspthailand>
- **Juice Shop** เป็นหนึ่งในโครงการของ OWASP
  - เว็บเซอร์วิส พัฒนาด้วย Node.js (Angular, Express)
  - เป็นเว็บเซอร์วิส มีช่องโหว่สำคัญ ที่พบบ่อย
  - มีรูปแบบการโจมตีแบบ CTF
- เปิดตัว <https://web2020.npu.world>

# แนะนำ OWASP

---

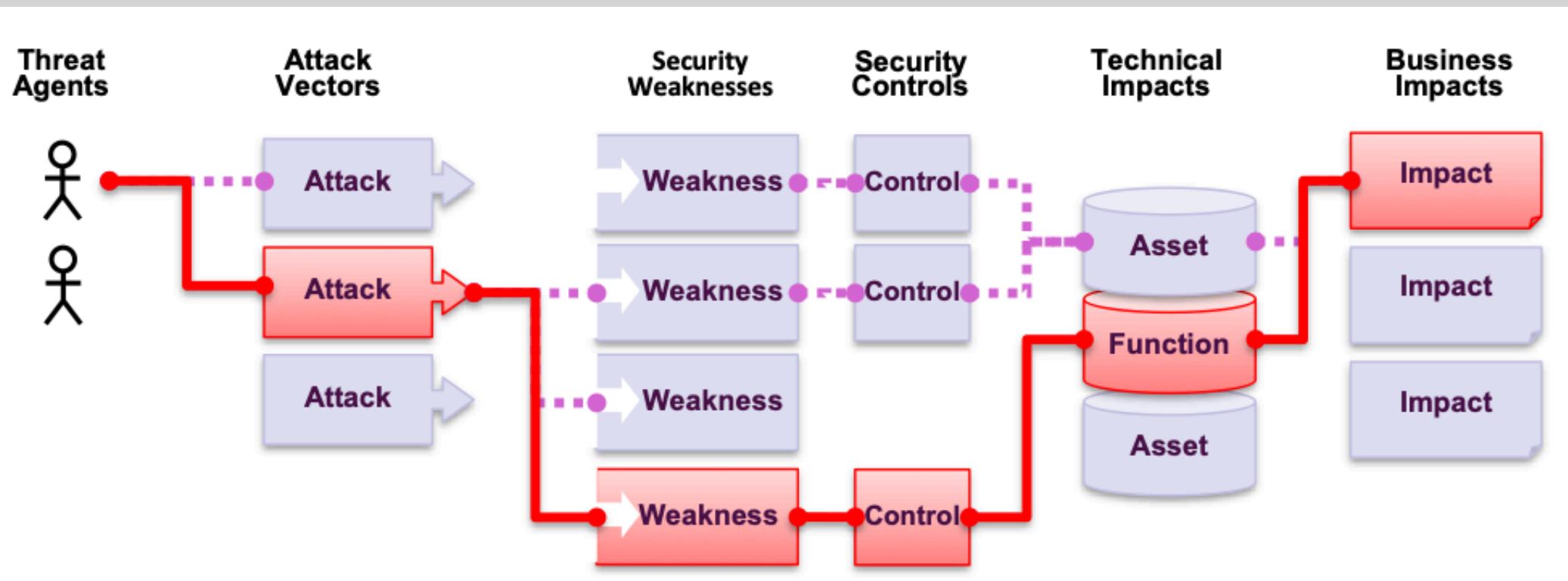
- เป็นการความปลอดภัยในเว็บเซอร์วิร์
- มีข้อมูลด้านความปลอดภัยเผยแพร่จำนวนมาก
- ที่มีชื่อเสียง OWASP Top Ten (10 ความเสี่ยงด้านความปลอดภัยของเว็บ)
  - ล่าสุดปี 2017 (ปี 2020 ยังไม่เผยแพร่)

# ระดับความเสี่ยง

- เกณฑ์การพิจารณาระดับความเสี่ยง

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Appli- cation Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

# การประเมินความเสี่ยงของเว็บแอป



# การจัดการความเสี่ยง (ระดับความเสี่ยง)

- <https://www.owasp-risk-rating.com>

## OWASP Risk Rating Calculator

Likelihood Factors		Impact Factors	
Threat Agent Factors	Vulnerability Factors	Technical Impact Factors	Business Impact Factors
Skill Level	Ease of Discovery	Loss of Confidentiality	Financial Damage
Motive	Ease of Exploit	Loss of Integrity	Reputation Damage
Opportunity	Awareness	Loss of Availability	Non-compliance
Size	Intrusion Detection	Loss of Accountability	Privacy Violation
Threat Agent Factor: Note (TAF: 0)		Technical Impact Factor: Note (TIF: 0)	
Vulnerability Factor: Note (VF: 0)		Business Impact Factor: Note (BIF: 0)	
Likelihood Factor: Note (LF: 0)		Impact Factor: Note (IF: 0)	
Overall Risk Severity: Note			

# 10 อันดับความเสี่ยงของเว็บสูงสุด (2017)

A1:2017-  
Injection

A2:2017-  
Broken  
Authentication

A3:2017-  
Sensitive Data  
Exposure

A4:2017-  
External Entities  
(XXE)

A5:2017-  
Broken Access  
Control

A6:2017-  
Security  
Misconfigurations

A7:2017-  
Cross-Site  
Scripting (XSS)

A8:2017-  
Insecure  
Deserialization

A9:2017-  
Components  
with Known  
Vulnerabilities

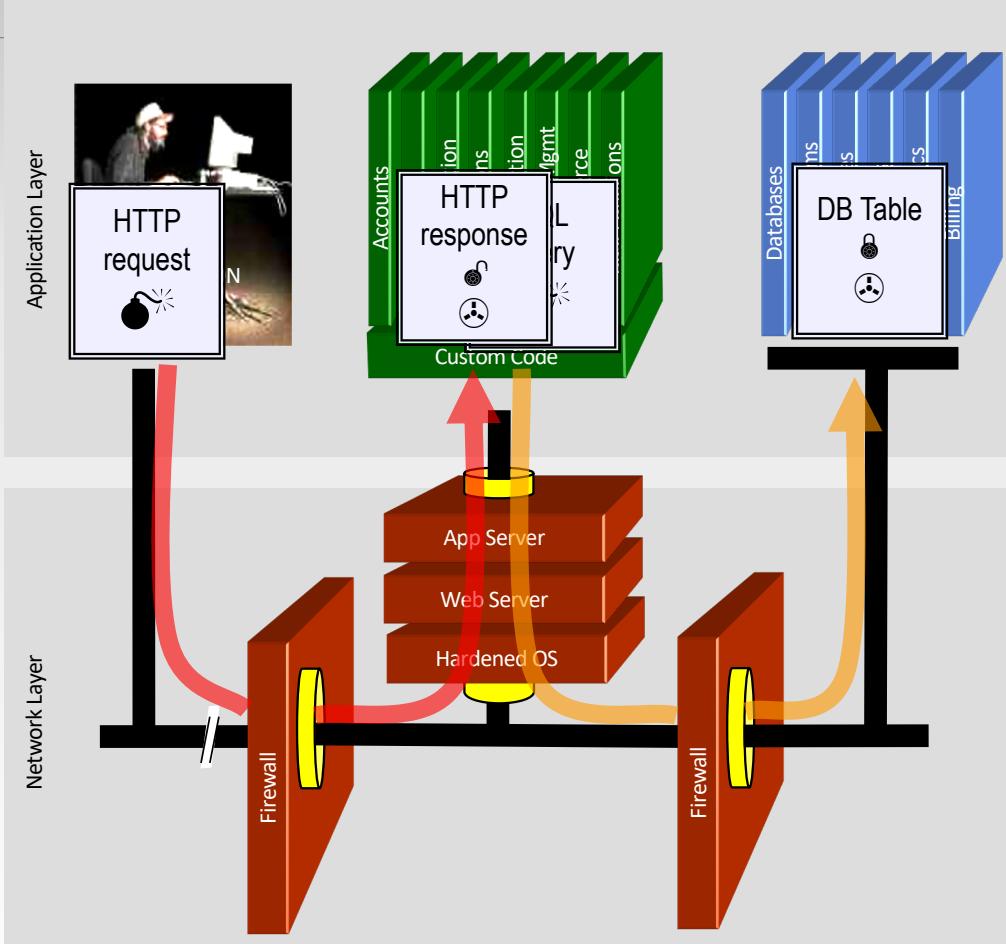
A10:2017-  
Insufficient  
Logging &  
Monitoring

# 10 อันดับความเสี่ยงของเว็บสูงสุด (2017)

A1:2017-  
Injection

- Injection การส่งคำสั่ง
- Injection flaws มีข้อบกพร่องในเว็บ เปิดทางให้ส่งคำสั่งนอกเหนือจากปกติ
- เป้าหมาย injection เช่น SQL, NoSQL, OS หรือ LDAP
- เกิดจากไม่ได้คัดกรองข้อมูลก่อนส่งเข้าระบบ
- ผู้ร้ายส่งคำสั่งที่มีวัตถุประสงค์ต่างจากเดิม แต่เข้าในช่องทางปกติ

# SQL Injection – Illustrated



NPU ID:

PASSWORD:

1. มีเว็บเพจสำหรับรับข้อมูล
2. แฮกเกอร์ส่งข้อมูลเข้าช่องรับข้อมูล
3. เว็บแอปส่งต่อข้อมูลให้ฐานข้อมูล
4. ฐานข้อมูลได้รับข้อมูล และกำคำสั่งตามที่ได้รับ  
ได้ข้อมูลแล้วเข้ารหัส ส่งกลับเว็บเพจ
5. เว็บเพจอ่านรหัสและแสดงผลตามปกติ

# A1-2017 Injection : ตัวอย่าง

- SQL injection
- <http://a1.dyn.npu.world> (ใช้ VPN หรือเครือข่ายในคณะ จึงเข้าเว็บได้)

## SQL Injection - NPU Training

โปรแกรมนี้ออกแบบเพื่อใช้ศึกษาปัญหาจาก SQL injection flaws

ท่านสามารถล็อกอินโดยใช้รหัสผ่านด้านล่างนี้ หรือ ลงทะเบียนเป็นและเคาร์ซองท่านได้

- bob:password
- voldemort:horcrux

ข้อมูลเพิ่มเติม

- รีเซ็ต หรือตั้งค่าเริ่มต้นให้ฐานข้อมูล ไปที่ [reset database](#).
- ท่านสามารถดู SQL query เพิ่มคำสั่ง `?debug=true` บน URL
- เว็บแอพพลิเคชันนี้เขียนด้วยภาษา PHP มีช่องโหว่ด้าน SQL injection

# A1-2017 injection : SQL injection

Login Page 1 - Simple Login Bypass

Username:

Password:

id	username	password
1	admin	21232f297a57a5a743894a0e4a801fc3
2	bob	5f4dcc3b5aa765d61d8327deb882cf99
3	ramesh	9aeaed51f2b0f6680c4ed4b07fb1a83c
4	suresh	9aeaed51f2b0f6680c4ed4b07fb1a83c
5	alice	c93239cae450631e9f55d71aed99e918
6	voldemort	856936b417f82c06139c74fa73b1abbe
7	frodo	f0f8820ee817181d9c6852a097d70d8d
8	hodor	a55287e9d0b40429e5a944d10132c93e
65	rhombus	e52848c0eb863d96bc124737116f23a4

- Login bypass attack

- ใช้คำสั่ง SQL บายพาสส์การป้องกัน

# SQL command

- show databases;
- use sqlitetraining;
- show tables;
- select \* from users;

	id	username	password
	1	admin	21232f297a57a5a743894a0e4a801fc3
	2	bob	5f4dcc3b5aa765d61d8327deb882cf99
	3	ramesh	9aeaed51f2b0f6680c4ed4b07fb1a83c
	4	suresh	9aeaed51f2b0f6680c4ed4b07fb1a83c
	5	alice	c93239cae450631e9f55d71aed99e918
	6	voldemort	856936b417f82c06139c74fa73b1abbe
	7	frodo	f0f8820ee817181d9c6852a097d70d8d
	8	hodor	a55287e9d0b40429e5a944d10132c93e
	65	rhombus	e52848c0eb863d96bc124737116f23a4

```
$q = "SELECT * FROM users where username='".$username."' AND password = '".md5($pass)."'";
```

```
SELECT * FROM users where username='Hacker' AND password = MD5(' hackerpass ') ;
```

```
SELECT * FROM users where username= 'bob' AND password = MD5('password') ;
```

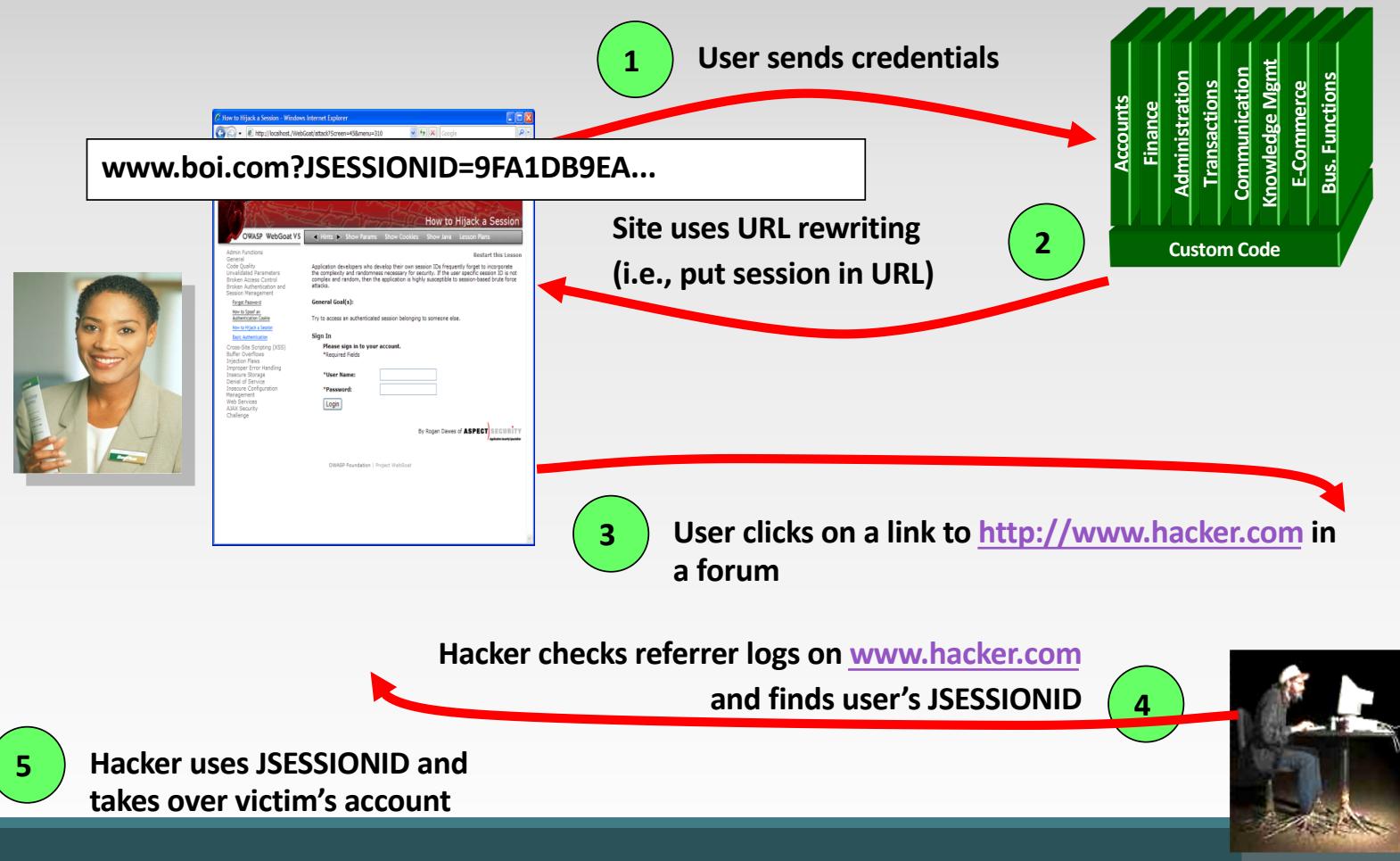
```
SELECT * FROM users where username='Hacker'' OR 1=1 ;--//' AND password = MD5(' hackerpass ') ;
```

# A2:2017-Broken Authentication

A2:2017-Broken  
Authentication

- ครอบคลุมหลายกลุ่มปัจจหา
- กลไกเปลี่ยนรหัสผ่าน ไม่ถูกต้อง
- เปิดทางให้ใช้รหัสผ่าน กีบค่าเดาง่าย
- ควบคุม session ไม่ดีพอ

# Broken Authentication Illustrated



# A3:2017- Sensitive Data Exposure

A3:2017-  
Sensitive Data  
Exposure

- เกี่ยวข้องกับการแสดงผลข้อมูล ที่ควรเป็นความลับ
- การส่งผ่านข้อมูลระหว่างเว็บเซอร์วิส
- มีหลายเว็บแอพส่วนหนึ่งมี API สำหรับให้นักพัฒนาใช้
- ไม่มีการปกป้องข้อมูลอ่อนไหวดีพอ เช่น สถานะการเงิน ข้อมูลสุขภาพ หรือ
  - ข้อมูลใช้สามารถระบุตัวบุคคล
  - personally identifiable information (PII)

# A4:2017-XML External Entities (XXE)

A4:2017-XML  
External  
Entities (XXE)

- การอ้างถึง Object ในระบบจาก XML ให้เครื่องอิ้นสามารถเข้าถึงไฟล์ได้
- ข้อมูลคำแนะนำไฟล์ คุณสมบัติไฟล์ ฐานข้อมูล ที่ร่วมเหล่านี้นำสู่การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตได้

# A5:2017-Broken Access Control

A5:2017-  
Broken Access  
Control

- กลไกการป้องกันผู้ไม่ได้รับอนุญาตถูกโจรกรรม
- มีการเจาะระบบจากกลไกอ่อนแอดำ
- ทำให้เข้าถึง อ่านข้อมูล แก้ไขข้อมูลความลับ
- แก้ไขสิทธิการใช้ข้อมูล

# A6:2017-Security Misconfiguration

A6:2017-  
Security  
Misconfiguratio  
n

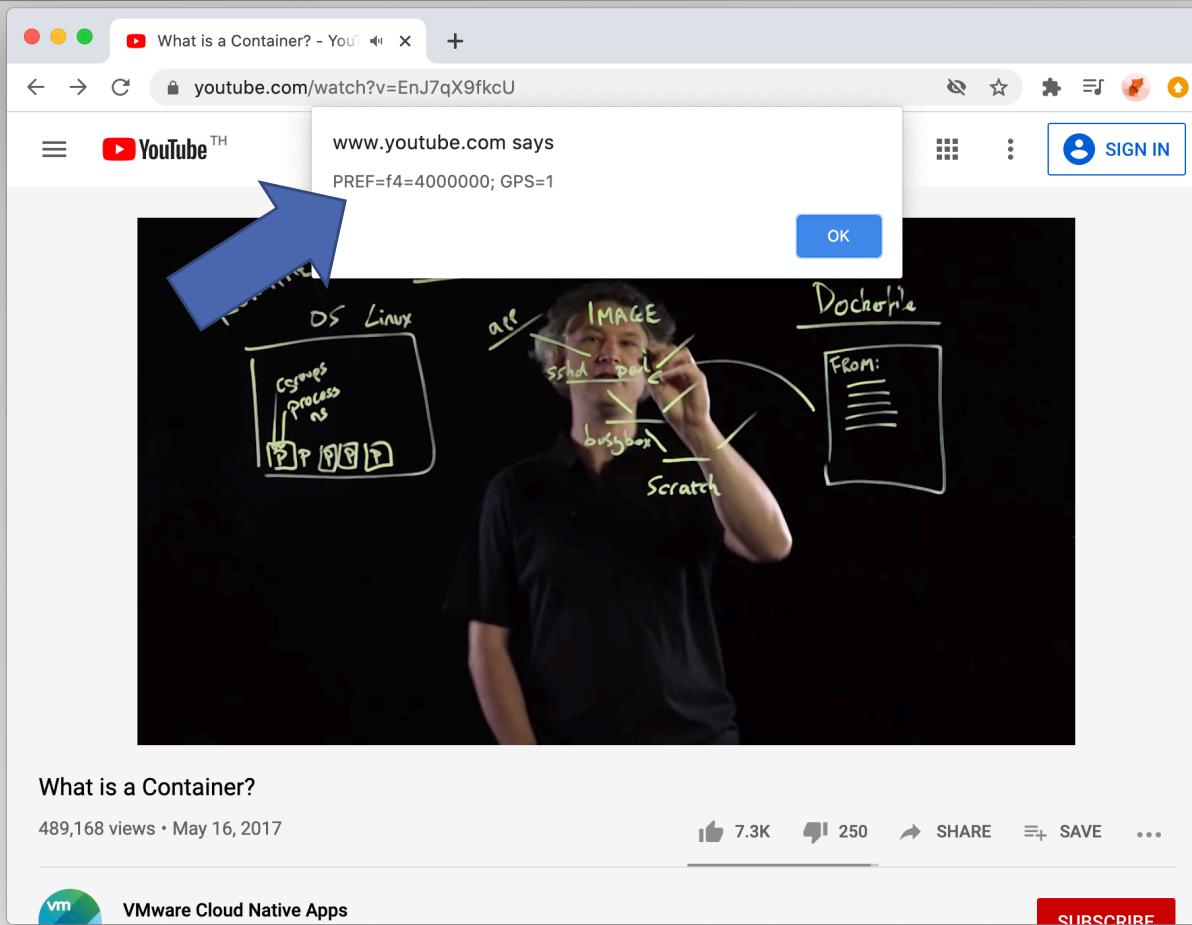
- การเซตค่าด้วยความปลอดภัยผิดพลาด
- เป็นปัญหาพบบ่อย
- มีการกำหนดค่าด้านความปลอดภัยไม่ถูกต้อง
- มีการกำหนดค่าไม่ถูกต้อง
- เกี่ยวข้องกับทั้งแอพพลิเคชัน ระบบปฏิบัติ และ อุปกรณ์เครือข่าย

# A7:2017- Cross-Site Scripting (XSS)

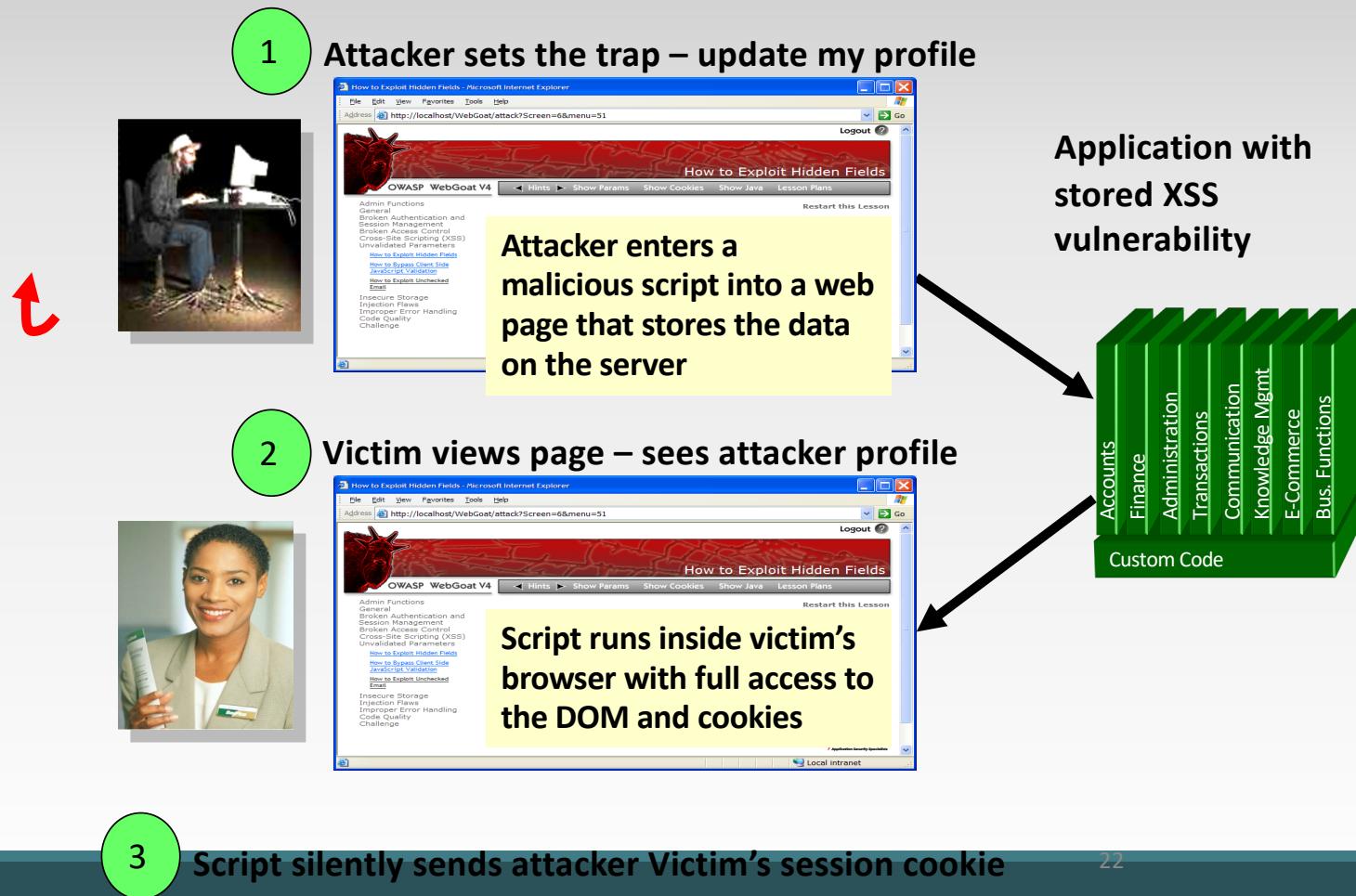
A7:2017- Cross-Site Scripting (XSS)

- XSS เป็นความผิดพลาดจากเว็บแอพพลิเคชัน
- ที่เปิดทางให้ข้อมูลจากภายนอกสามารถแสดงผลบนเพ็จได้โดยไม่ตรวจสอบ
- บ่อยครั้งที่โปรแกรมเมอร์ต้องการไปอ่านข้อมูลจากเว็บไซต์ภายนอก เพื่อแสดงผลเว็บต้นเอง
- javascript:alert(document.cookie)
- javascript:alert(document.cookie)

# Cross-Site Scripting (XSS)



# Cross-Site Scripting Illustrated



# A8:2017- Insecure Deserialization

A8:2017-  
Insecure  
Deserialization

- การรับข้อมูลเข้าสู่ระบบอย่างไม่ปลอดภัย เป็นช่องทางให้เกิดการโจมตีระยะไกล (remote code execution : RCE)
- แฮกเกอร์สามารถดักฟัง คัดลอกข้อมูล นำกลับมาส่งช้า เพื่อให้ อัพเกรดสิทธิ์สูงขึ้น

# A9:2017 – Using Components with Known Vulnerabilities

A9 - Using Components with Known Vulnerabilities

- การยังคงใช้ซอฟต์แวร์ หรือ API ที่มีช่องโหว่
- ตัวอย่างเช่น เปิดให้ยังคงใช้จ่ายซอฟต์แวร์เวอร์ชันเก่า(ที่มีปัญหาด้านความปลอดภัย) ทำงานร่วมกับซอฟต์แวร์รุ่นใหม่
- การเปิดให้ซอฟต์แวร์รุ่นเก่ายังคงใช้งานได้ ด้วยสิทธิ์เท่ากับซอฟต์แวร์รุ่นใหม่จะทำให้การควบคุมด้านความปลอดภัยทำได้ยาก

# A10:2017-Insufficient Logging & Monitoring

A10:2017-  
Insufficient  
Logging &  
Monitoring

- เก็บข้อมูลตรวจสอบไม่เพียงพอ
  - ข้อมูลการ login, ข้อมูลการติดต่อ
- ไม่สามารถตรวจสอบได้ว่ามี แอคเเกอร์เข้ามาในระบบ
- ตำแหน่งบันทึกข้อมูลไม่ปลอดภัย
- ระยะเวลาเก็บข้อมูลไม่นานพอ (ควรมากกว่า 200วัน)