Web Basic

@splitline

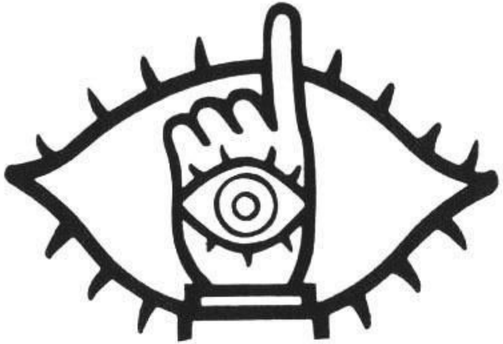
# whois this.guy

@splitline

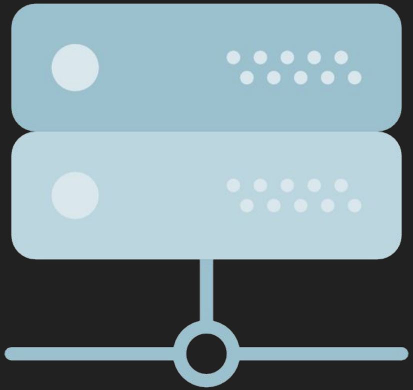
Web 🐶

SQLab @ NYCU CSIE

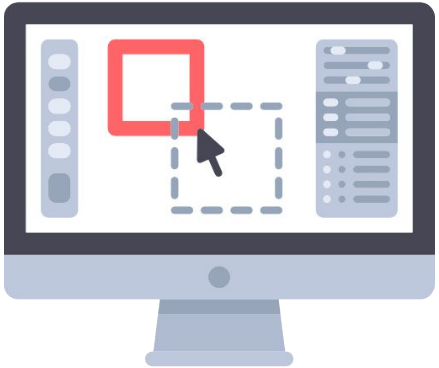
CTF @ 10sec



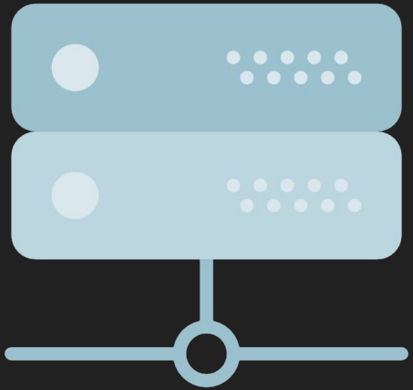
So, what is Web ?



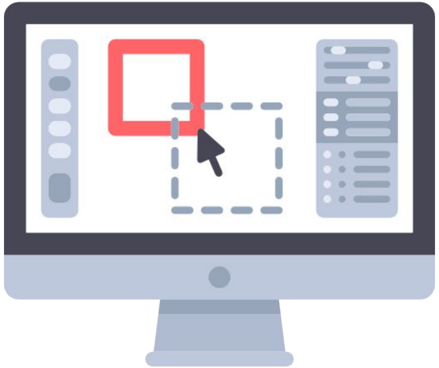
後端
Backend



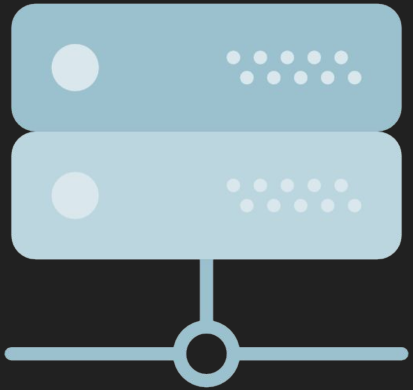
前端
Frontend



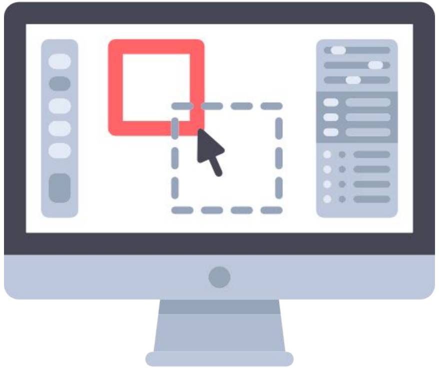
Browser



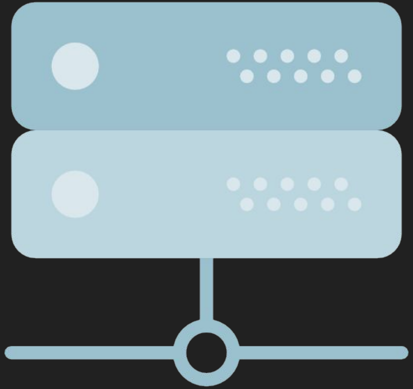
Server



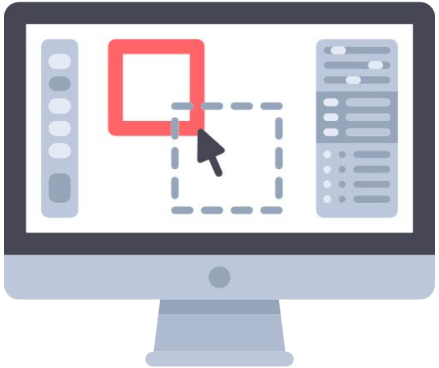
你看不到的



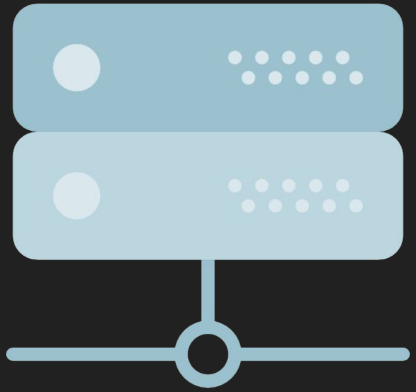
你看得到的



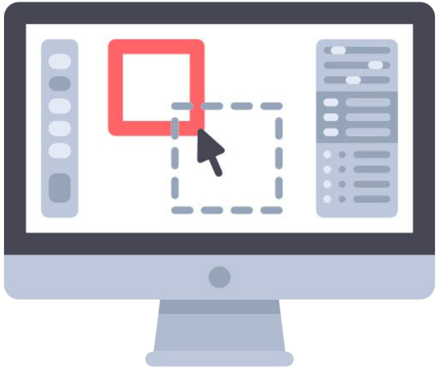
Command injection
Path traversal



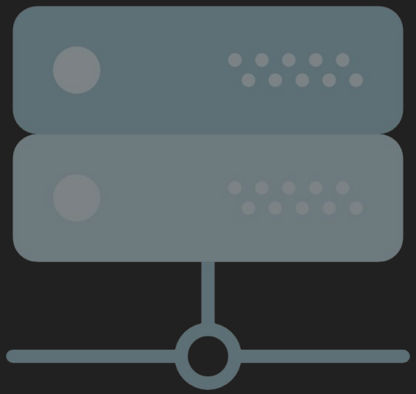
XSS



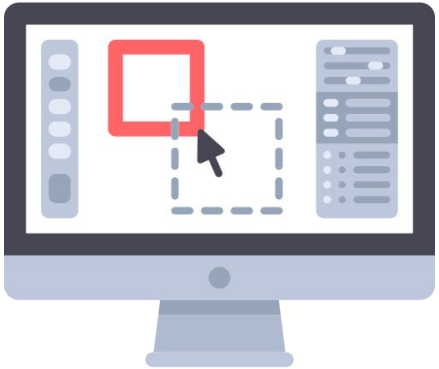
PHP, Node.js ...



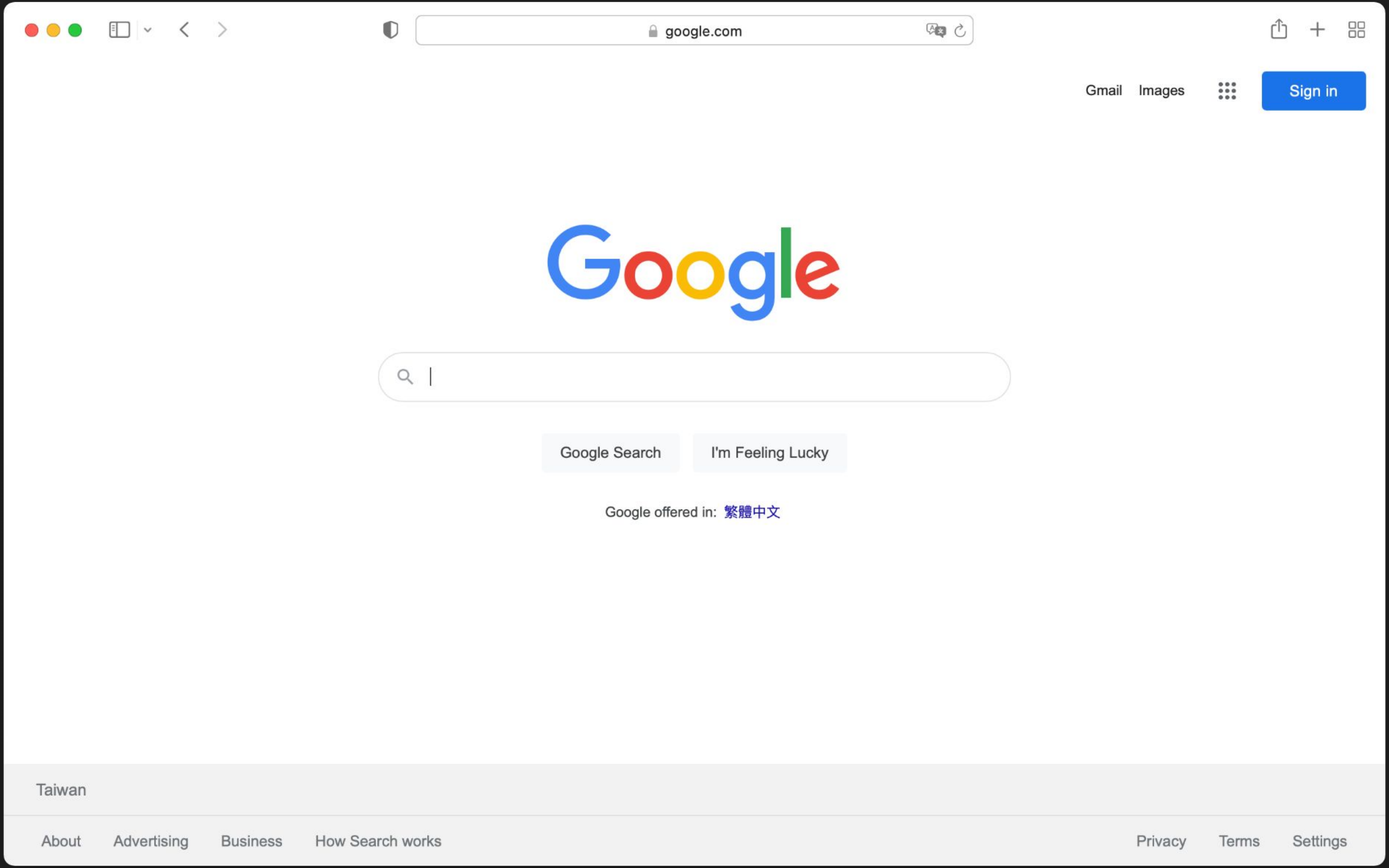
HTML / CSS / JavaScript



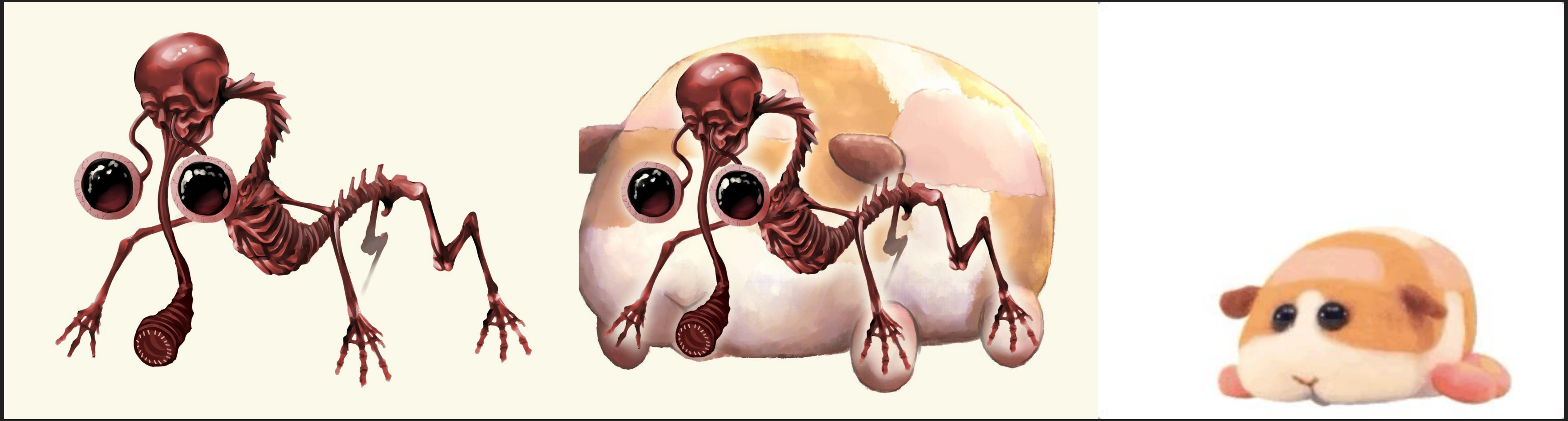
PHP, Node.js …



HTML / CSS / JavaScript


google.com
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Google offered in: 繁體中文
Taiwan
About
Advertising
Business
How Search works
Privacy
Terms
Settings

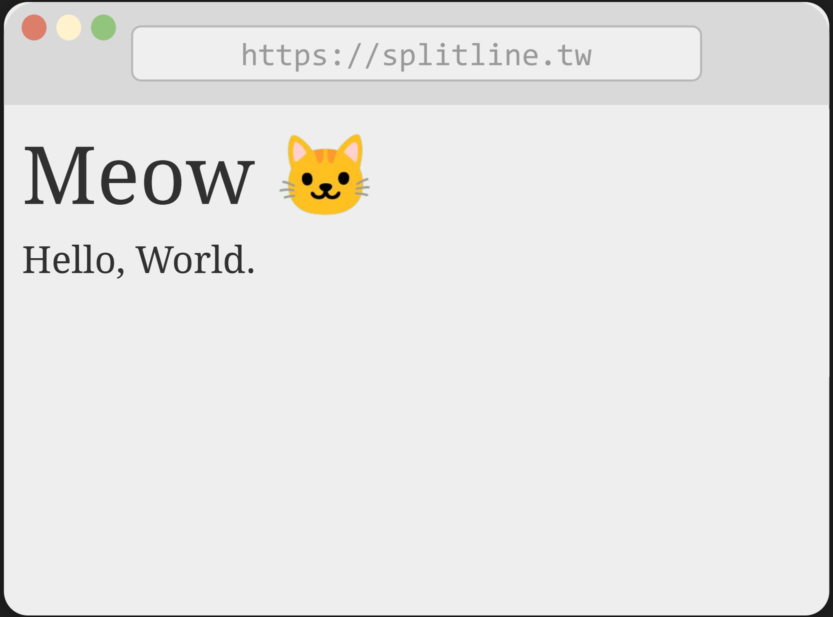
HTML × CSS × JavaScript



HTML

CSS

JavaScript

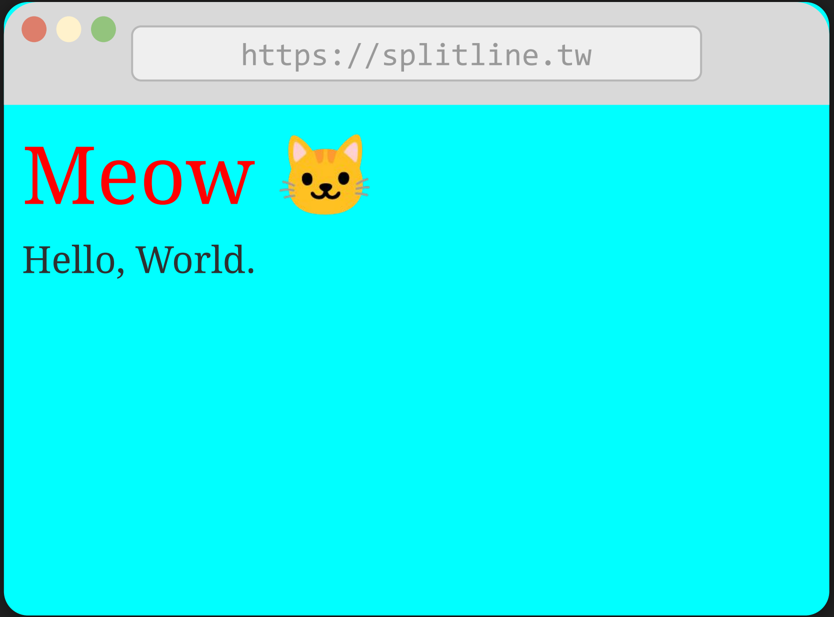


Meow 😺

Hello, World.

```
<!DOCTYPE html>
<html>
   <h1>Meow 😺</h1>
   <p>Hello, World.</p>
</html>
```

HTML



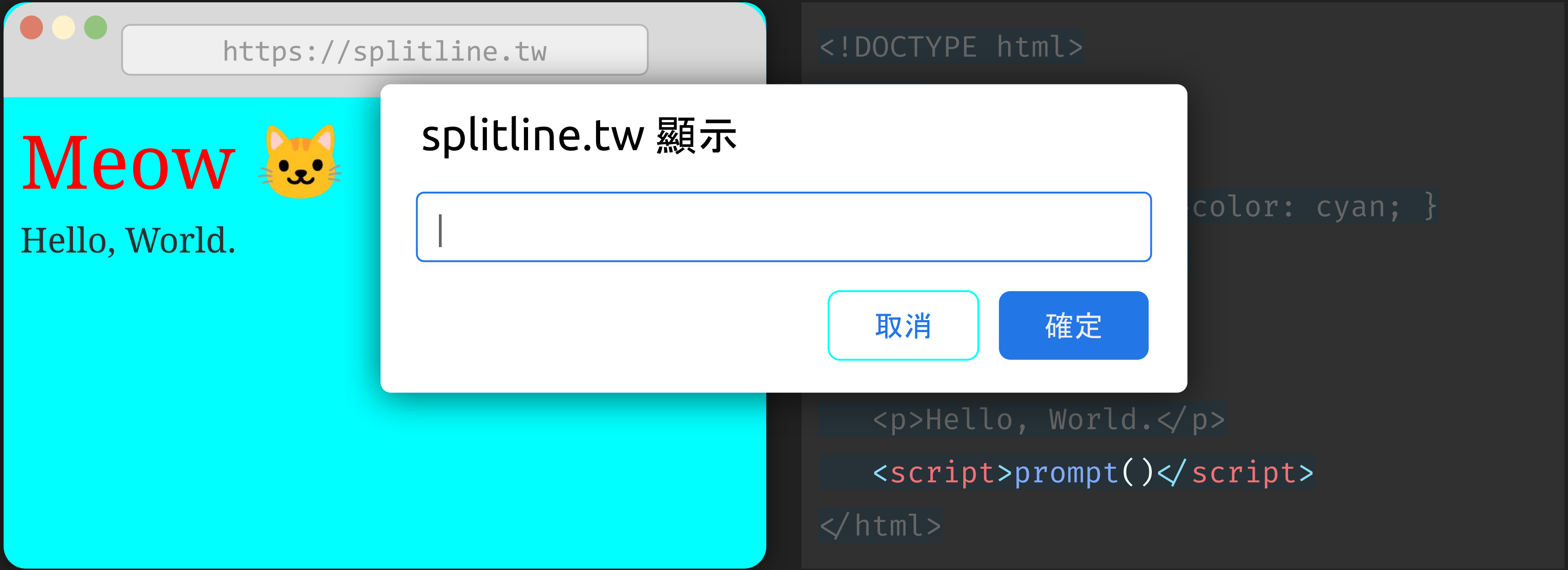
https://splitline.tw

Meow 🐱

Hello, World.

```
<!DOCTYPE html>
<html>
    <style>
    body { background-color: cyan; }
    h1 { color: red; }
    </style>
    <h1>Meow 🐱</h1>
    <p>Hello, World.</p>
</html>
```

CSS



Meow 🐱

Hello, World.

splitline.tw 顯示

```
<!DOCTYPE html>
                   color: cyan; }
   <p>Hello, World.</p>
   <script>prompt()</script>
</html>
```

JavaScript

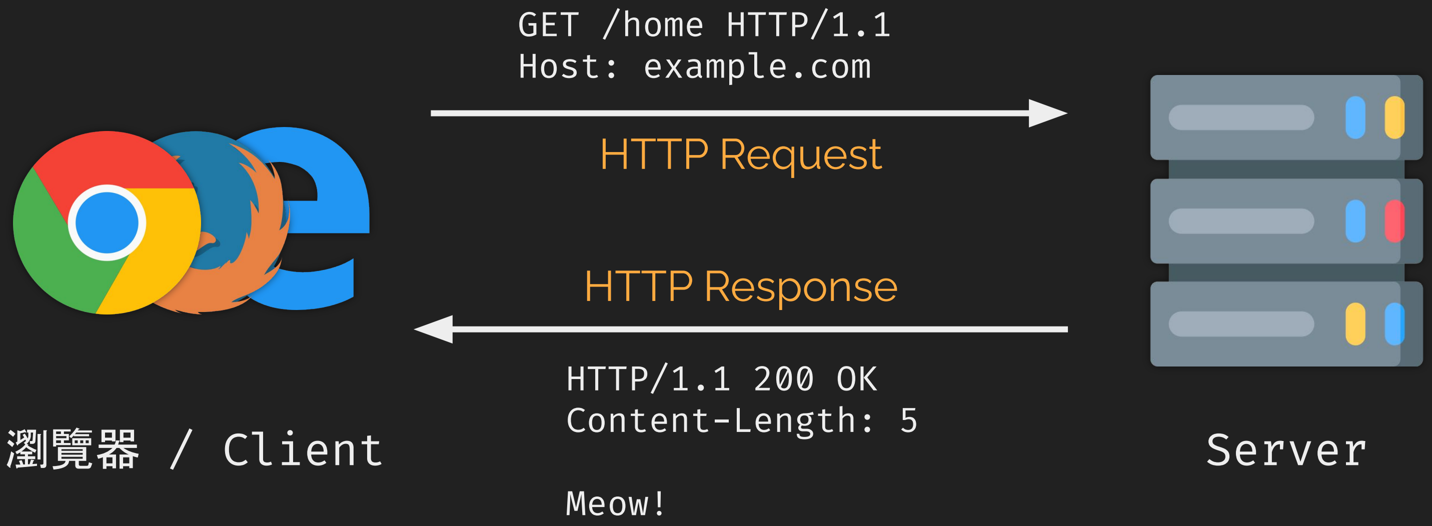
前端	前端框架/套件	Bootstrap, jQuery, React…
前端	Web 前端語言	HTML, CSS, JavaScript
後端	Web 開發框架	Laravel, Express, Spring, Flask…
後端	Web 後端語言	PHP, Node.js, Java, Python…
	伺服器	Apache, Nginx, IIS …
	資料儲存	Database, Cache, File Storage
	運作環境	OS(Linux/Windows), Cloud, Container

Browser
(Client)

HTTP://

HTTP Protocol

HyperText Transfer Protocol



```
GET /home HTTP/1.1
Host: example.com
```

HTTP Request

HTTP Response

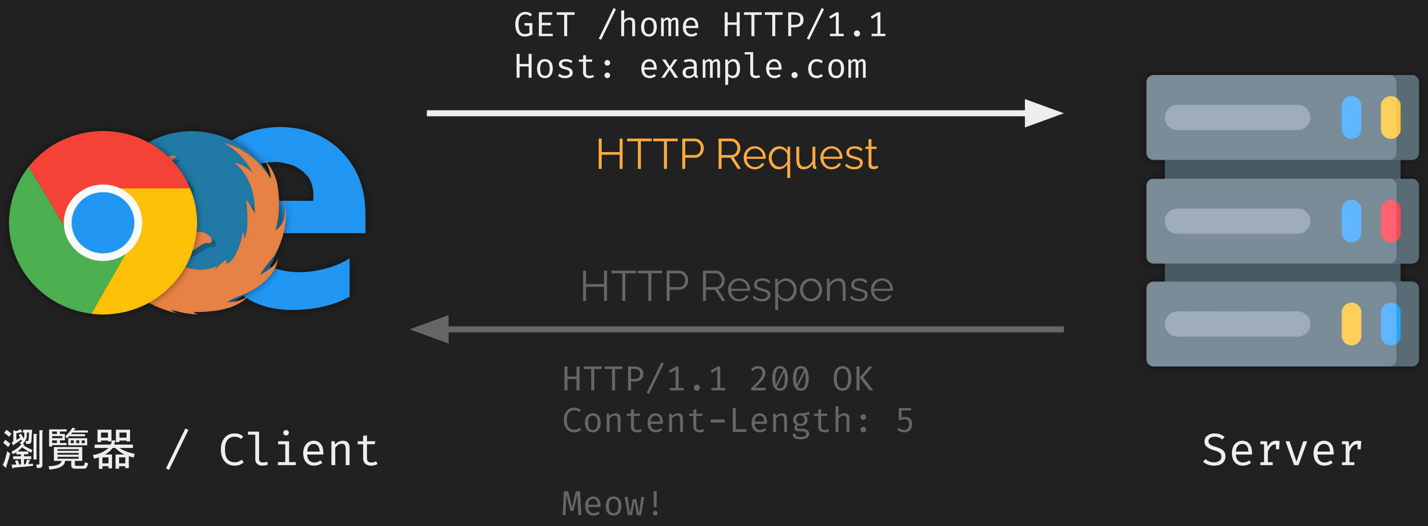
```
HTTP/1.1 200 OK
Content-Length: 5

Meow!
```

瀏覽器 / Client

Server

HTTP Protocol

HyperText Transfer Protocol



```
GET /home HTTP/1.1
Host: example.com
```

HTTP Request

HTTP Response

```
HTTP/1.1 200 OK
Content-Length: 5

Meow!
```

瀏覽器 / Client

Server

HTTP Request

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

\r\n: HTTP 使用 CR(\r)LF(\n) 換行

HTTP Request: Method

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

- 動詞，用來表達使用者發出這個請求想幹嘛
- 常見的有 GET, POST, PUT, DELETE, PATCH, HEAD …

HTTP Request: Path

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

```
http://example.com/login?redirect=%2f#login-form
```

Path + Query Parameter

HTTP Request: Protocol version

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

- **HTTP/0.9 ~ 1.1**	Text-based protocol
- **HTTP/2**	Binary protocol
- **HTTP/3**	QUIC protocol (UDP)

HTTP Request: Header

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

- 提供 HTTP request 要告訴 server 的一些附加資訊
- More: MDN | HTTP headers - HTTP

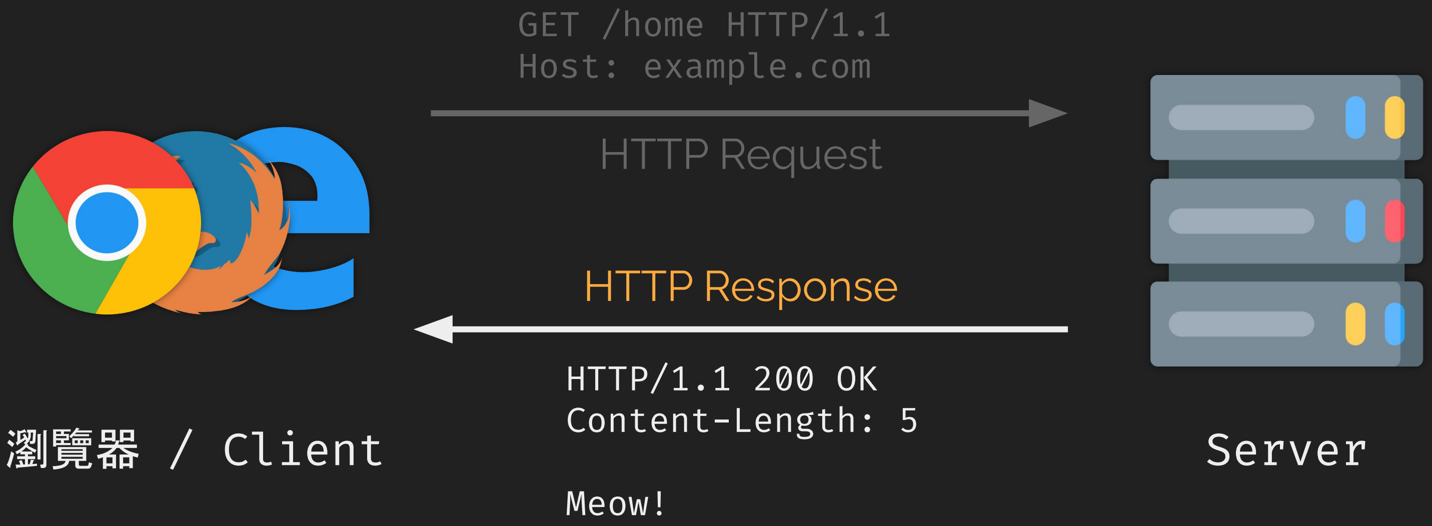
HTTP Request: Body

```
POST /login?redirect=%2f HTTP/1.1\r\n
Host: example.com\r\n
Referer: http://example.com/home\r\n
User-Agent: Mozilla/5.0 …\r\n
Content-Length: 32\r\n
\r\n
username=admin&password=p455w0rd
```

- POST / PATCH / PUT 會帶上這段資訊
- GET 等 method 通常不會出現此部分

HTTP Protocol

HyperText Transfer Protocol



```
GET /home HTTP/1.1
Host: example.com
```

```
HTTP/1.1 200 OK
Content-Length: 5

Meow!
```

HTTP Response

```
HTTP/1.1 200 OK
Content-Length: 9527\r\n
Content-Type: text/html; charset=UTF-8\r\n
Date: Fri, 1 Jan 2077 13:33:37 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
<!DOCTYPE html><html><head> ... </head><body> ... </body></html>
```

\r\n：HTTP 使用 CR(\r)LF(\n) 換行

HTTP Response

```
HTTP/1.1 200 OK
Content-Length: 9527\r\n
Content-Type: text/html; charset=UTF-8\r\n
Date: Fri, 1 Jan 2077 13:33:37 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
<!DOCTYPE html><html><head> … </head><body> … </body></html>
```

Protocol version and Response status

# HTTP Status Code

- 1xx: 修但幾勒 101 Switching Protocol
- 2xx: 👍 200 OK
- 3xx: 走開 301 Moved Permanently
- 4xx: 你怪怪的 403 Forbidden
- 5xx: 我怪怪的 500 Internal Server Error

HTTP Status Codes Decision Diagram

🐱 http.cat / 🐶 httpstatusdogs.com

HTTP Response

```
HTTP/1.1 302 Found
Content-Length: 35\r\n
Content-Type: text/html; charset=UTF-8\r\n
Location: https://example.com/\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
Redirecting to <a href="/">/</a> ...
```

Protocol version and Response status

HTTP Response: Header

```
HTTP/1.1 200 OK
Content-Length: 9527\r\n
Content-Type: text/html; charset=UTF-8\r\n
Date: Fri, 1 Jan 2077 13:33:37 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
<!DOCTYPE html><html><head> ... </head><body> ... </body></html>
```

提供 server 要告訴 client 的一些附加資訊

（有可能從而洩露/得知一些伺服器環境）

HTTP Response: Body

```
HTTP/1.1 200 OK
Content-Length: 9527\r\n
Content-Type: text/html; charset=UTF-8\r\n
Date: Fri, 1 Jan 2077 13:33:37 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
<!DOCTYPE html><html><head> ... </head><body> ... </body></html>
```

HTML / JavaScript / Image / Whatever ...

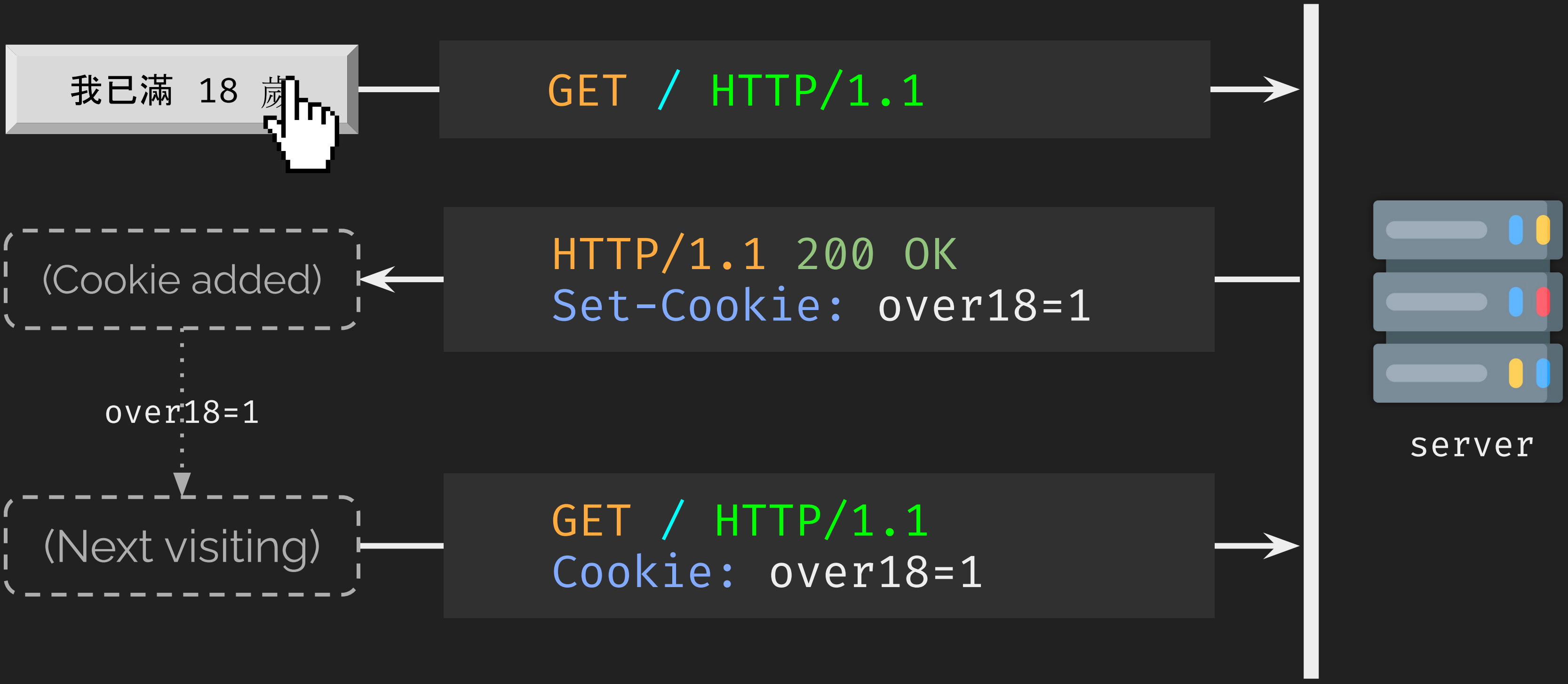
Cookie

- 紀錄使用者資訊的一小段資料
- 跟 domain name 和 path 綁定

Visit https://splitline.tw:8080

Domain	Path	Cookie
splitline.tw	/	meow=123
google.com	/	session=c8763
...	...	...

Cookie



我已滿 18 歲

```
GET / HTTP/1.1
```

(Cookie added)

```
HTTP/1.1 200 OK
Set-Cookie: over18=1
```

over18=1

(Next visiting)

```
GET / HTTP/1.1
Cookie: over18=1
```

Cookie 屬性

- HttpOnly
  - 無法在 JavaScript 中利用 document.cookie 取得
- Secure
  - 只有在透過 https:// 傳輸時才會被送出到伺服器
- Expires=<date>
  - cookie 會在設定的日期與時間之後失效
  - 沒設定則會在瀏覽器關閉後自動失效
- Max-Age=<seconds>
  - cookie 會在設定的秒數之後失效
  - 優先級比 Expires 高

Session

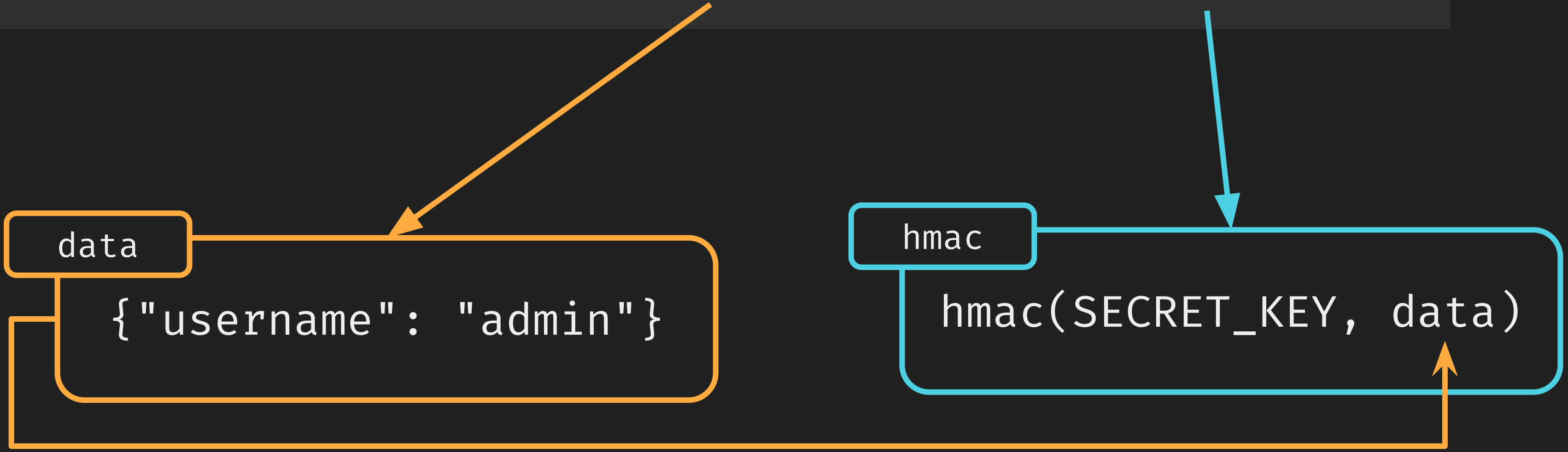
```
GET / HTTP/1.1
Cookie: sessionid=8b25bf2a843de1fa
```

Server

Session ID	Data
bc84a40359835cc7	{"username": "admin"}
8b25bf2a843de1fa	{"username": "meow"}
0f79e18fbd21ac7a	{"username": "guest"}
...	

Signed Cookie

```
GET / HTTP/1.1
Cookie: session=eyJ1c2VybmFtZSI6ICJhZG1pbiJ9.CAAEGc3 ...
```



data

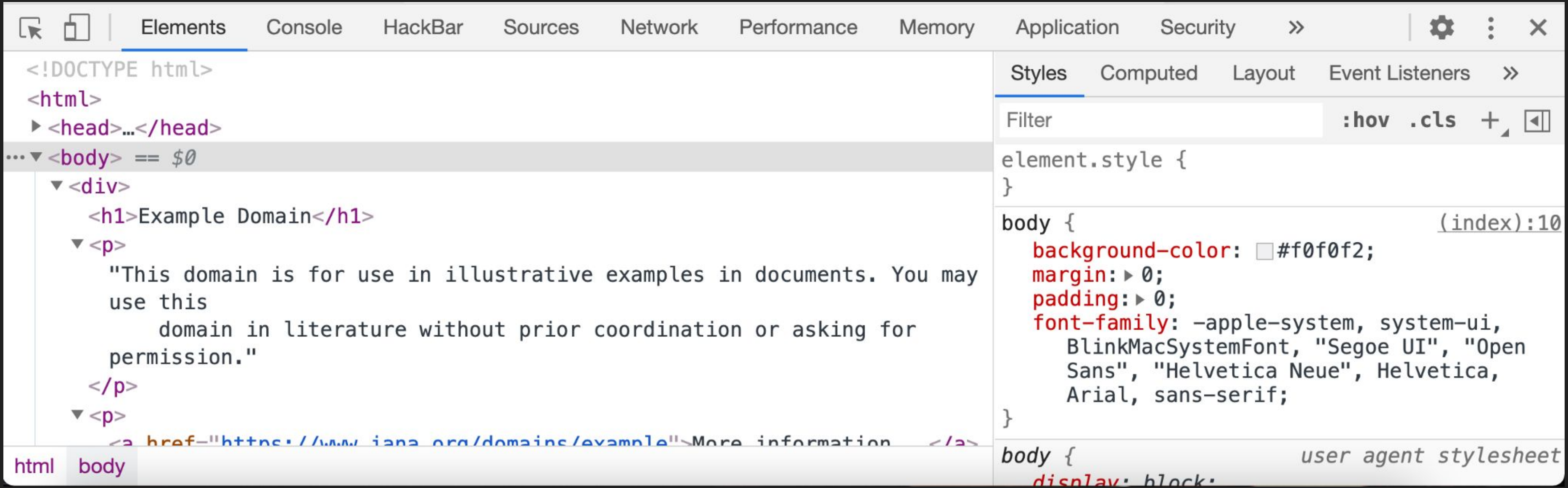
{"username": "admin"}

hmac

hmac(SECRET_KEY, data)

Some Tools You Might Need

F12: Developer Tools



```
<!DOCTYPE html>
<html>
▶ <head>…</head>
… ▼ <body> == $0
    ▼ <div>
        <h1>Example Domain</h1>
      ▼ <p>
          "This domain is for use in illustrative examples in documents. You may
          use this
              domain in literature without prior coordination or asking for
          permission."
        </p>
      ▼ <p>
          <a href="https://www.iana.org/domains/example">More information...</a>
```

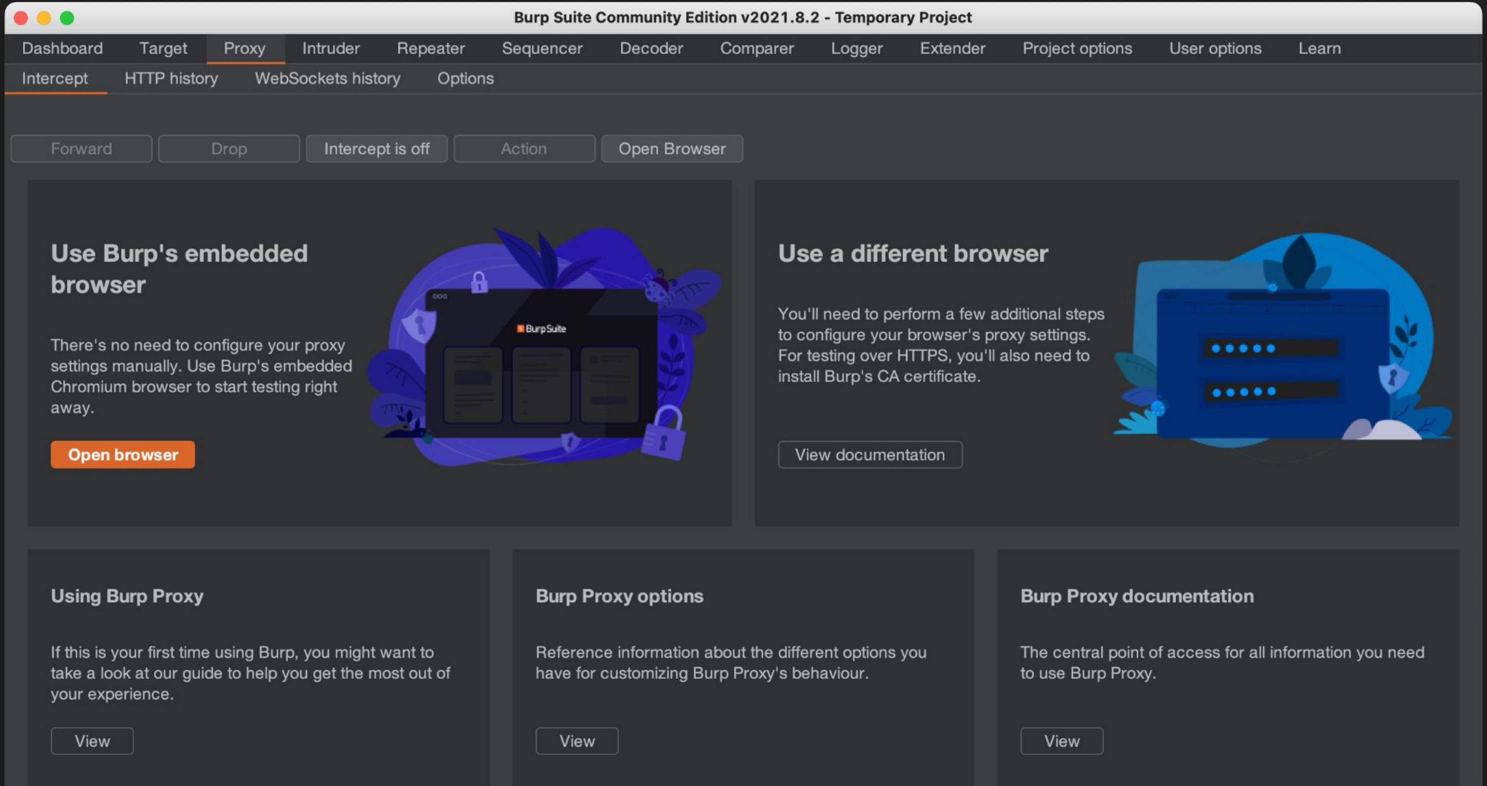
```
element.style {
}
body {                                                        (index):10
    background-color: □#f0f0f2;
    margin: ▶ 0;
    padding: ▶ 0;
    font-family: -apple-system, system-ui,
       BlinkMacSystemFont, "Segoe UI", "Open
       Sans", "Helvetica Neue", Helvetica,
       Arial, sans-serif;
}
body {                                          user agent stylesheet
    display: block;
```

cURL Cheatsheet

```
curl 'https://example.com'
       -i/--include                    # Show response header
       -v/--verbose                    # Show more message (?)
       -d/--data 'key=value&a=b'       # HTTP POST data
       -X/--request 'PATCH'            # Request method
       -H/--header 'Host: fb.com'      # Set header
       -b/--cookie 'user=guest;'       # Set cookie
       -o/--output 'output.html'       # Download result
```

[Tips] Convert curl syntax to other languages https://curl.trillworks.com

Burp Suite



Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

Lab: HTTP Adventure

PHP: Quick introduction

```
<html><p>Meow</p><?php /* Your code here ... */ ?></html>
```

```
echo "Hello, world!";
```

`$variable = 'value';`	變數皆會以 $ 開頭
`$_GET['id']`	GET 的參數會擺進 $_GET 陣列
`$_POST['username']`	POST 的參數會擺進 $_POST 陣列
`$_COOKIE['over18']`	Cookie 可從 $_COOKIE 陣列存取
`$_REQUEST`	= $_GET + $_POST + $_COOKIE

Web Security

號稱最好上手的資安領域？騙人的吧

Lab: Cat Shop

恭喜🎉 你已經學會了

Broken Access Control

×

Bussiness Logic Vulnerabilities

Broken Access Control

- /admin_panel 根本沒驗證使用者身份？
- /admin 403 Permission Denied
    - /admin/delUser ???

垂直越權

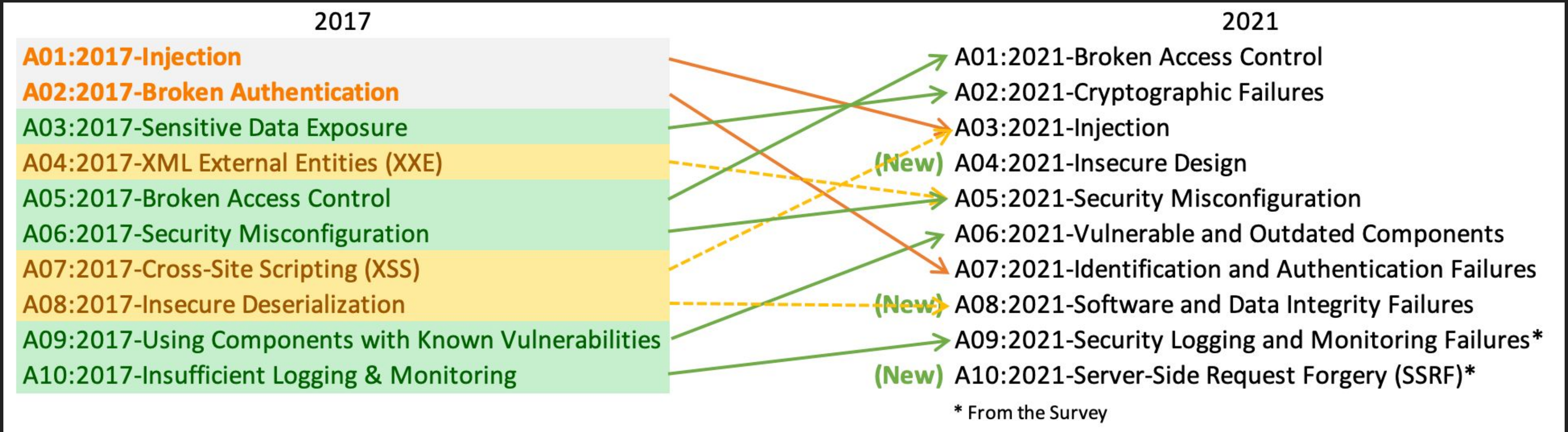
普通用戶 → 管理員

- /myAccount?user=5
- /myAccount?user=6 ???

水平越權

使用者A → 使用者B

OWASP Top 10 | 2017 → 2021



2017

- A01:2017-Injection
- A02:2017-Broken Authentication
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- (New) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- (New) A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- (New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey