Web Security

Basic

Kaibro (kaibrotw@gmail.com)

whoami

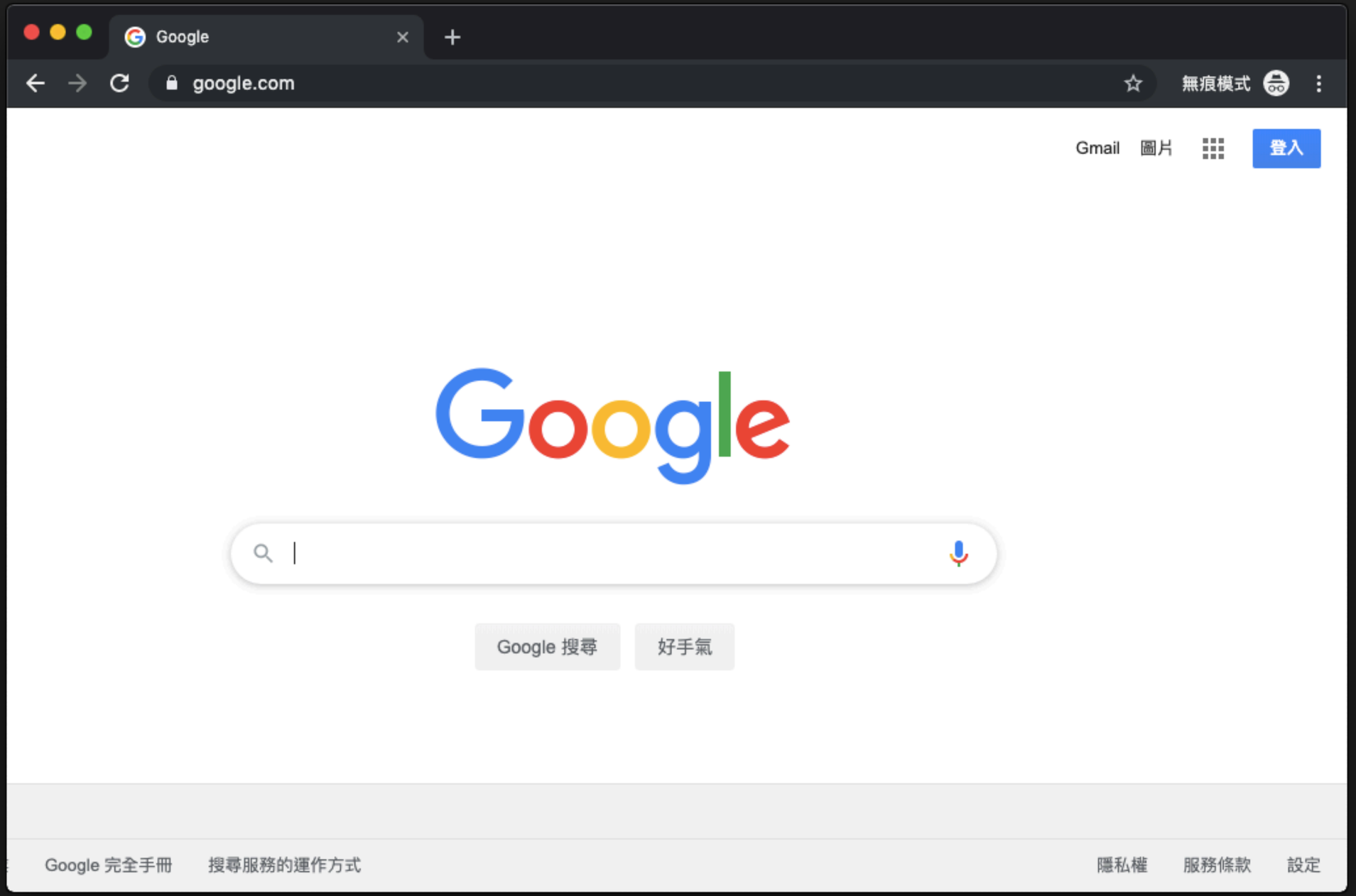
- Kaibro
- Web 🐶
- 電競選手 / 抓蟲獵人
- Balsn / DoubleSigma

Outline

- Basic
- Information Gathering
- PHP Feature
- Common Vulnerabilities

Basics

What is Web ?


Google
google.com
無痕模式
Gmail
圖片
登入
Google
Google 搜尋
好手氣
Google 完全手冊
搜尋服務的運作方式
隱私權
服務條款
設定

Frontend

Backend

Browser

Server

看得到的

HTML, Javascript, CSS

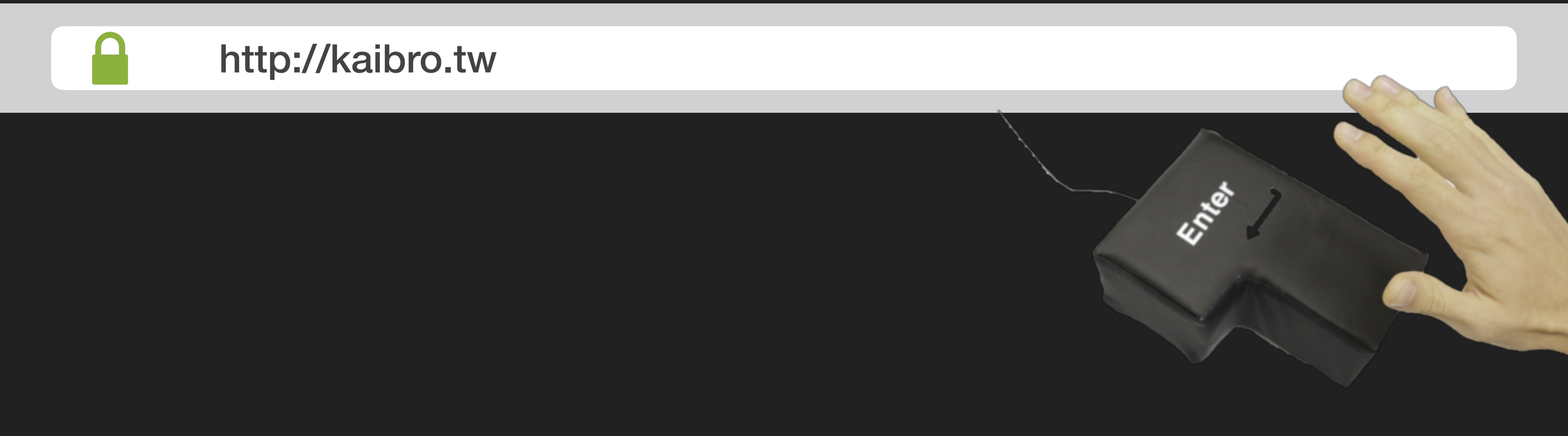
看不到的

Apache, PHP, MySQL, NodeJS

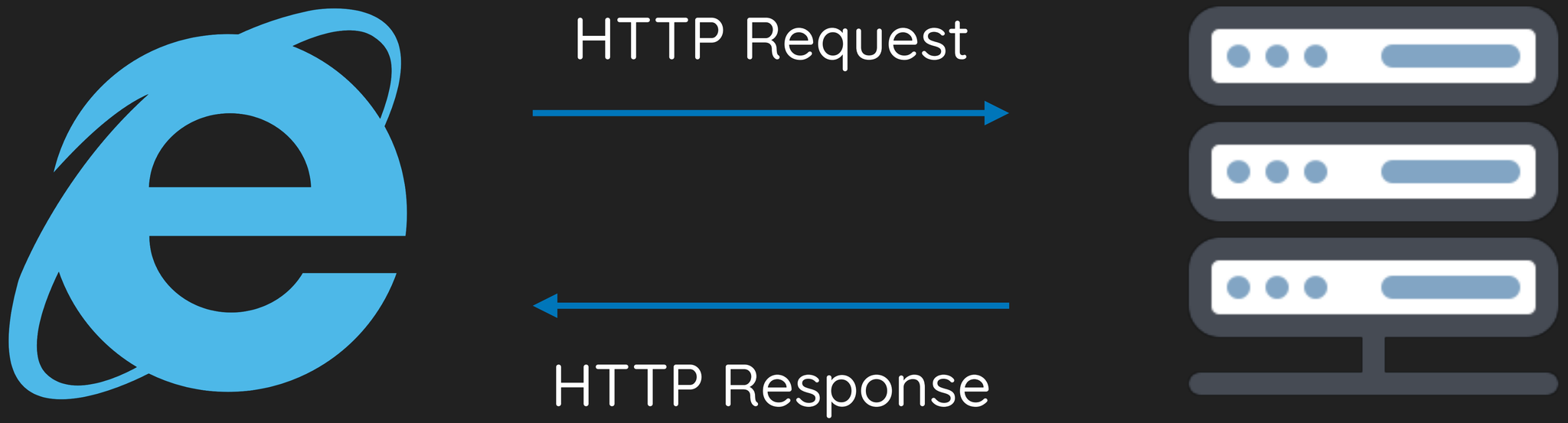
URL Components

HTTP Protocol

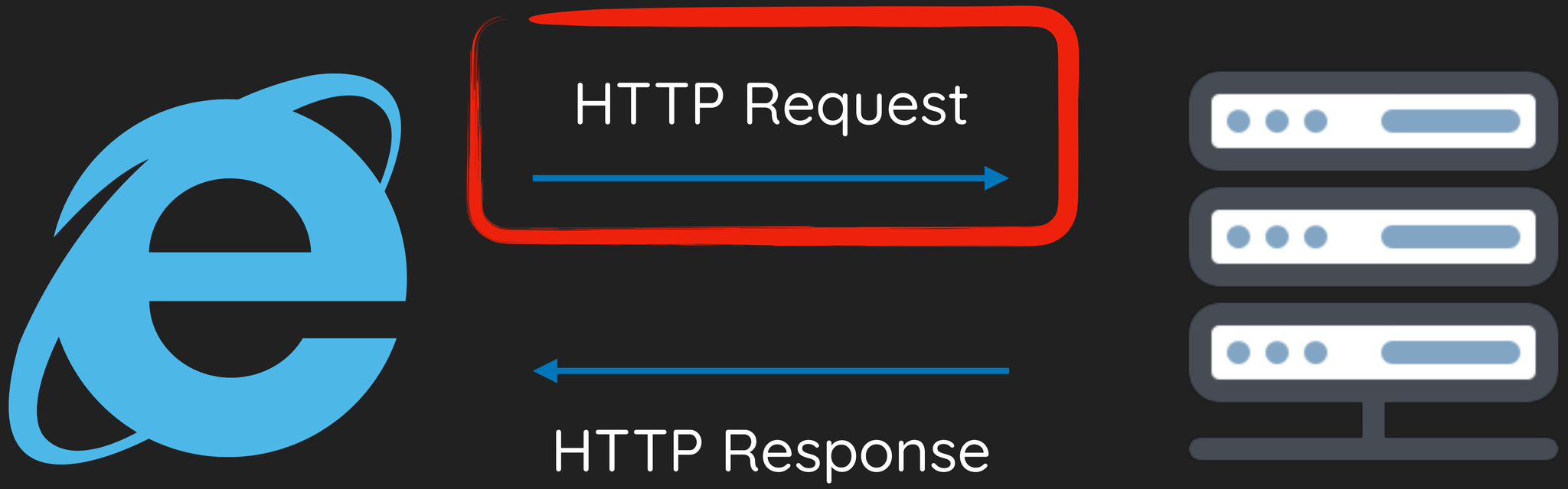
- 瀏覽器輸入網址後，中間發生啥事？



HTTP Protocol



HTTP Protocol



HTTP Protocol - Raw Request

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Cookie: sessionid=54875487
Connection: close
```

HTTP Method

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Cookie: sessionid=54875487
Connection: close
```

HTTP Method

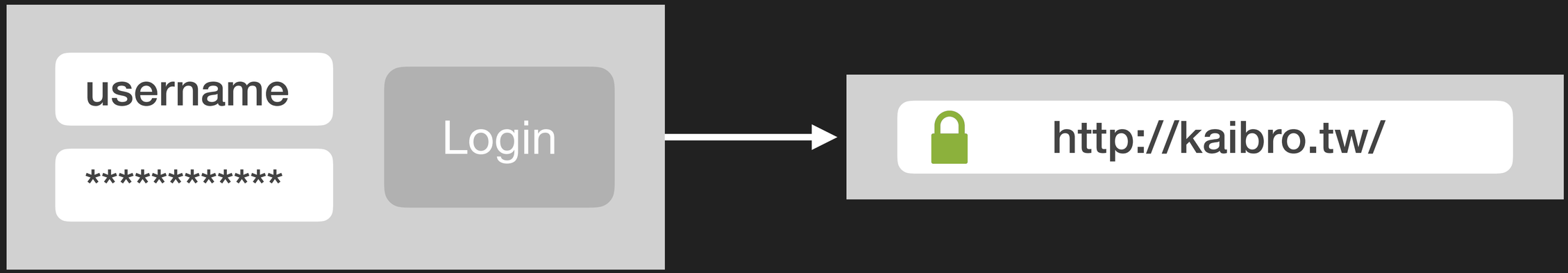
HTTP Method

- HTTP Method (Verb)
  - 代表**請求目的**
  - 常見有 GET、POST、HEAD、PUT、.....

HTTP Method

- GET

- POST




WHERE ARE THEY?!?!

POST Request

```
POST / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close

username=kaibro&password=123456
```

POST Request

```
POST / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Connection: close

username=kaibro&password=123456
```

HERE

CRLF Newline

```
POST / HTTP/1.1\r\n
Host: kaibro.tw\r\n
User-Agent: Mozilla/5.0 ... Firefox/56.0\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 31\r\n
Connection: close\r\n
\r\n
username=kaibro&password=123456
```

Request Path

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Cookie: sessionid=54875487
Connection: close
```

Request Path

HTTP Version

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Cookie: sessionid=54875487
Connection: close
```

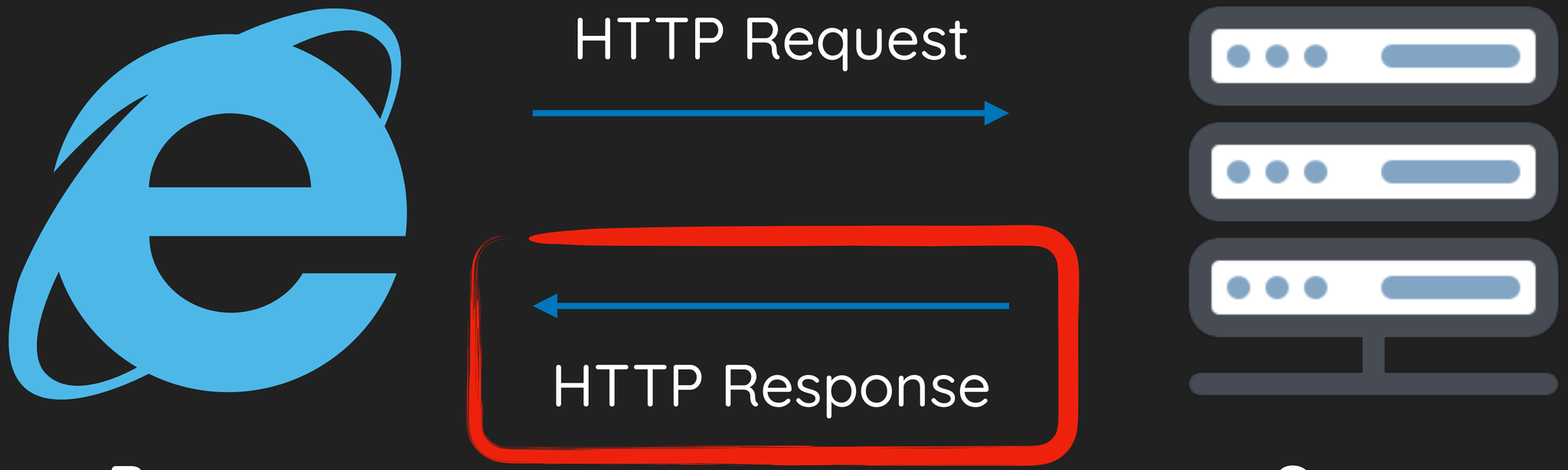
HTTP Version

HTTP Header Pairs

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 ... Firefox/56.0
Cookie: sessionid=54875487
Connection: close
```

HTTP Header (Key: Value)

HTTP Protocol



HTTP Response

```
HTTP/1.1 200 OK
Date: Sat, 12 Oct 2019 03:21:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 31
Connection: close
Content-Type: text/html; charset=UTF-8

<html><body>Hello</body></html>
```

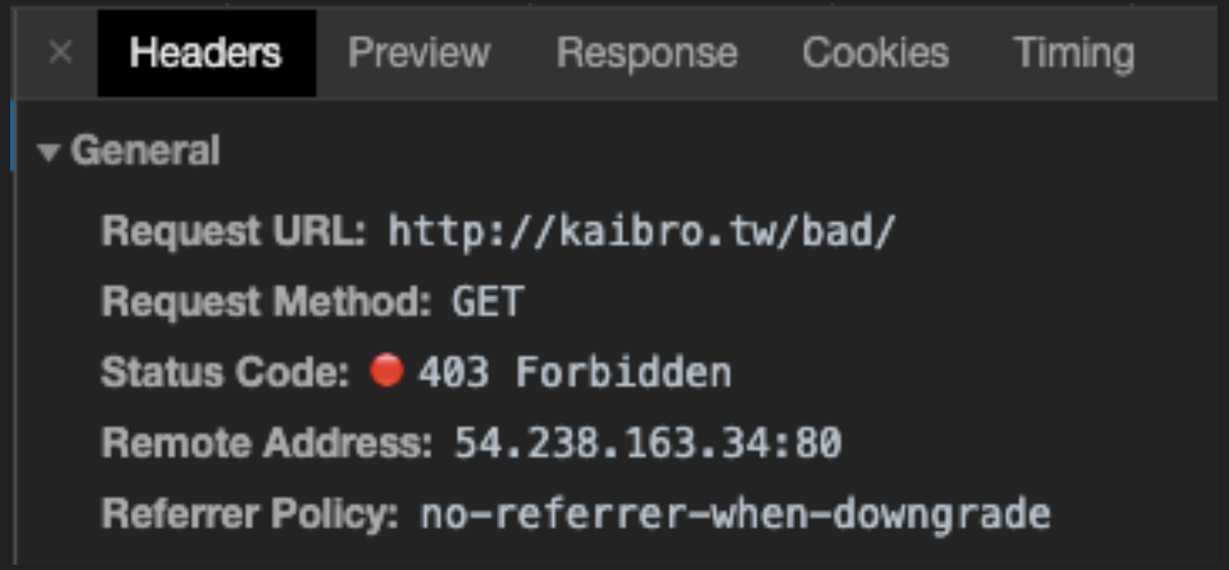
Status Code

```
HTTP/1.1 200 OK
Date: Sat, 12 Oct 2019 03:21:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 31
Connection: close
Content-Type: text/html; charset=UTF-8

<html><body>Hello</body></html>
```

Status Code

- 2XX: 正常
- 3XX: 重導向
- 4XX: Client端爛掉
- 5XX: Server端爛掉



200

OK

403

Forbidden

ICANHASCHEEZBURGER.COM

404

Not Found

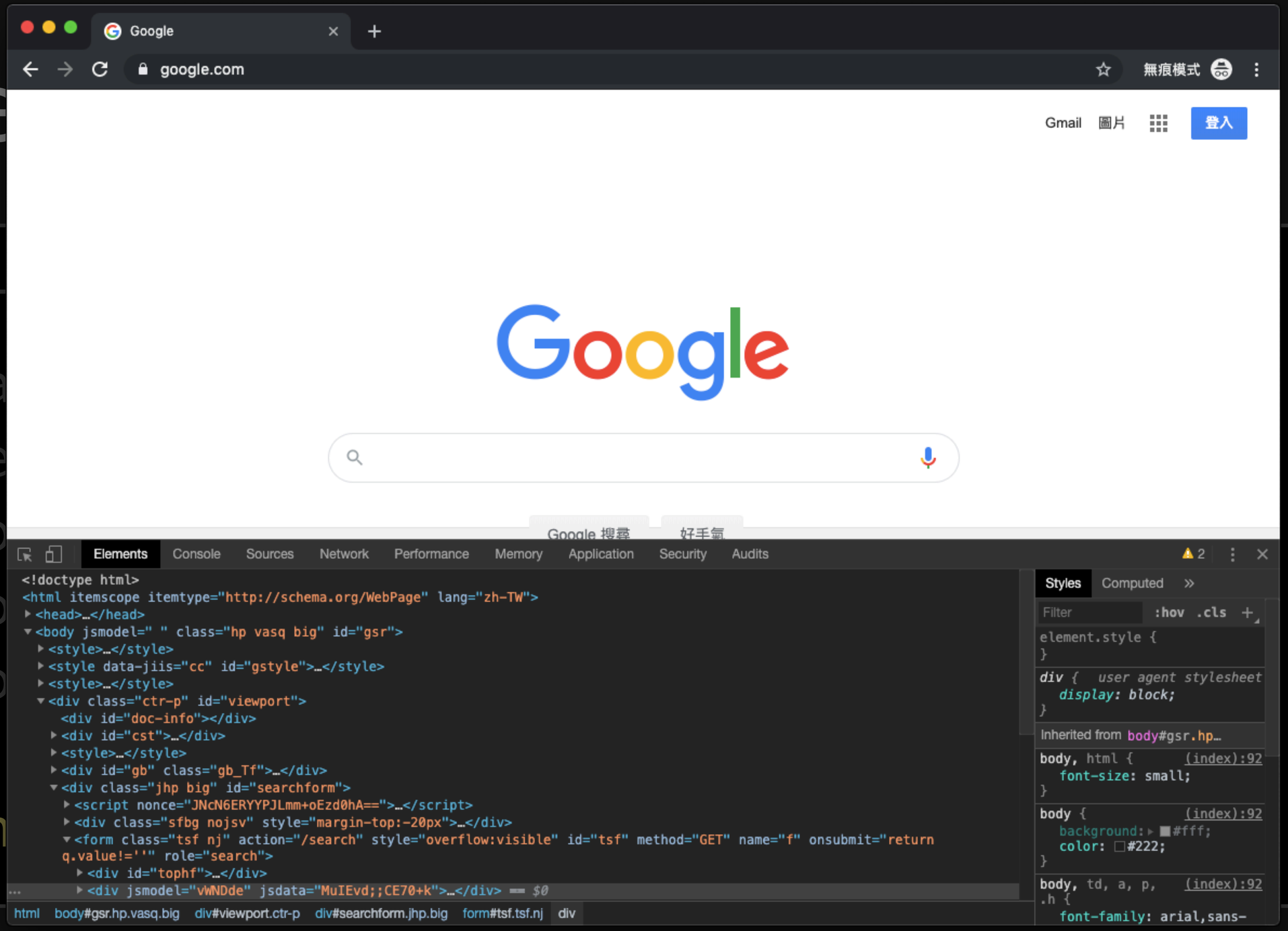
500

Internal Server Error

Response Body

```
HTTP/1.1 200 OK
Date: Sat, 12 Oct 2019 03:21:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 31
Connection: close
Content-Type: text/html; charset=UTF-8

<html><body>Hello</body></html>
```

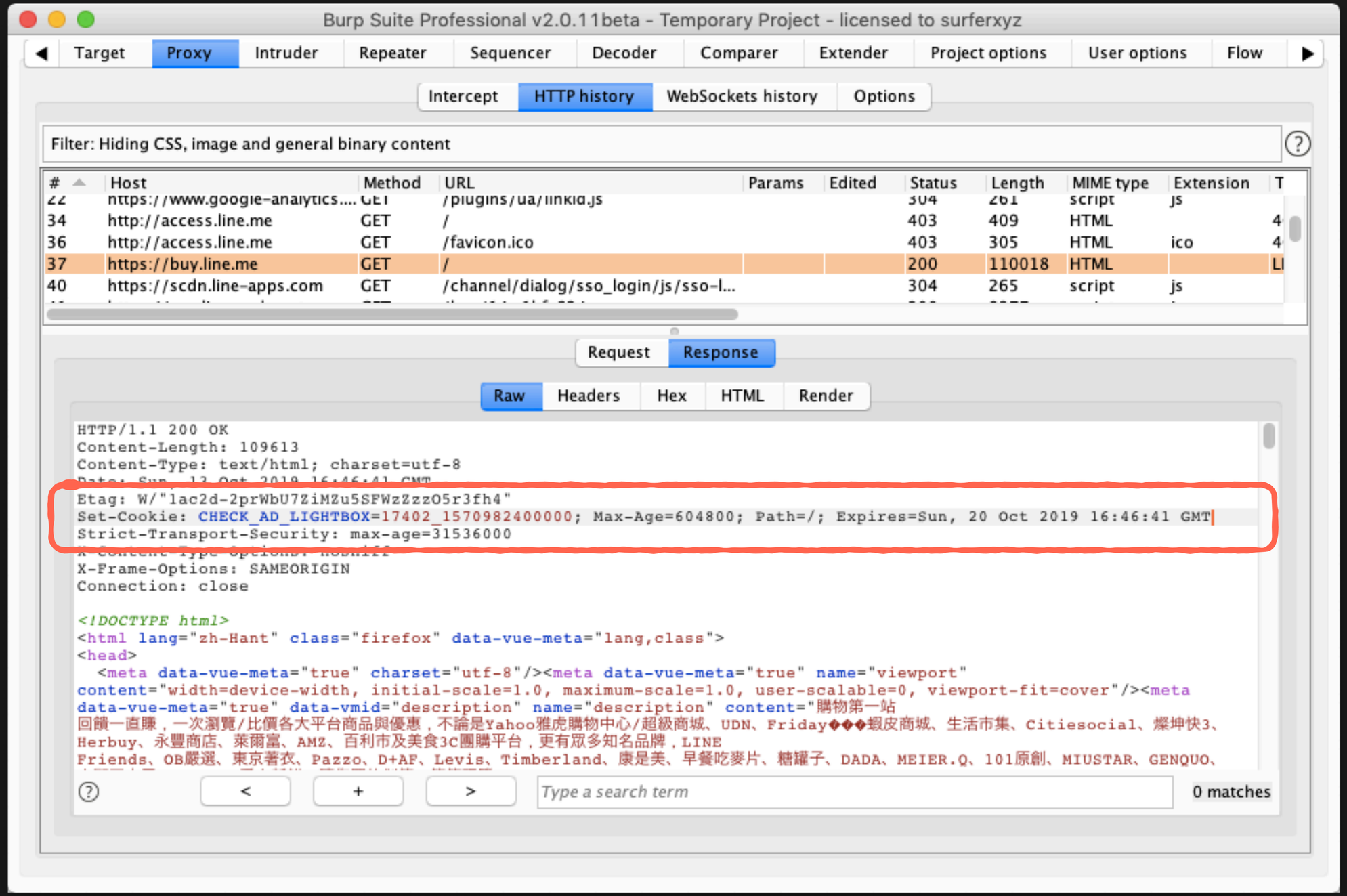

Google
google.com
無痕模式
Gmail
圖片
登入
Google
Google 搜尋
好手氣
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
<!doctype html>
<html itemscope itemtype="http://schema.org/WebPage" lang="zh-TW">
<head>…</head>
<body jsmodel=" " class="hp vasq big" id="gsr">
<style>…</style>
<style data-jiis="cc" id="gstyle">…</style>
<style>…</style>

…
<style>…</style>
…

<script nonce="JNcN6ERYYPJLmm+oEzd0hA==">…</script>
…
<form class="tsf nj" action="/search" style="overflow:visible" id="tsf" method="GET" name="f" onsubmit="return
q.value!='' " role="search">
…
… == $0
html
body#gsr.hp.vasq.big
div#viewport.ctr-p
div#searchform.jhp.big
form#tsf.tsf.nj
div
Styles
Computed
Filter
:hov .cls
element.style {
}
div { user agent stylesheet
display: block;
}
Inherited from body#gsr.hp…
body, html { (index):92
font-size: small;
}
body { (index):92
background: #fff;
color: #222;
}
body, td, a, p, (index):92
.h {
font-family: arial,sans-

Cookie

- 網站在訪客電腦留下的小段訊息
- 用途
  - 彌補 HTTP 無狀態 (Stateless) 的不足
  - 提升用戶體驗
  - 記錄登入資訊 (e.g. Session ID)


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Flow
Intercept
HTTP history
WebSockets history
Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension
34 http://access.line.me GET / 403 409 HTML
36 http://access.line.me GET /favicon.ico 403 305 HTML ico
37 https://buy.line.me GET / 200 110018 HTML
40 https://scdn.line-apps.com GET /channel/dialog/sso_login/js/sso-l... 304 265 script js
Request
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Content-Length: 109613
Content-Type: text/html; charset=utf-8
Etag: W/"1ac2d-2prWbU7ZiMZu5SFWzZzzO5r3fh4"
Set-Cookie: CHECK_AD_LIGHTBOX=17402_1570982400000; Max-Age=604800; Path=/; Expires=Sun, 20 Oct 2019 16:46:41 GMT
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
Connection: close
<!DOCTYPE html>
<html lang="zh-Hant" class="firefox" data-vue-meta="lang,class">
<head>
<meta data-vue-meta="true" charset="utf-8"/><meta data-vue-meta="true" name="viewport"
content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0, viewport-fit=cover"/><meta
data-vue-meta="true" data-vmid="description" name="description" content="購物第一站
回饋一直賺，一次瀏覽/比價各大平台商品與優惠，不論是Yahoo雅虎購物中心/超級商城、UDN、Friday◆◆◆蝦皮商城、生活市集、Citiesocial、燦坤快3、
Herbuy、永豐商店、萊爾富、AMZ、百利市及美食3C團購平台，更有眾多知名品牌，LINE
Friends、OB嚴選、東京著衣、Pazzo、D+AF、Levis、Timberland、康是美、早餐吃麥片、糖罐子、DADA、MEIER.Q、101原創、MIUSTAR、GENQUO、
Type a search term
0 matches

Cookie & Session

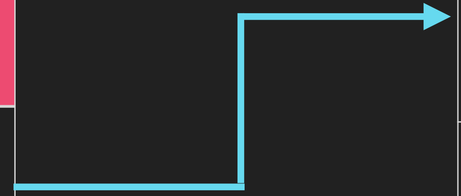
- 如何判斷一個請求是來自哪個使用者？
- 如何避免使用者 A 假冒成使用者 B？
- Server 如何判斷使用者已經登入？

Cookie & Session

- Cookie 存放 Session ID（號碼牌）
- Session (飲料) 存放 ID 對應的資料

Name	Value
SESSIONID	meow

Client (Cookie)



ID	SESSION
seadog	...
seacat	...
meow	user=kaibro
hotdog	...

Server

Cookie & Session

- Cookie 存放 Session ID（號碼牌）
- Session (飲料) 存放 ID 對應的資料

Name	Value
SESSIONID	meow

Client (Cookie)

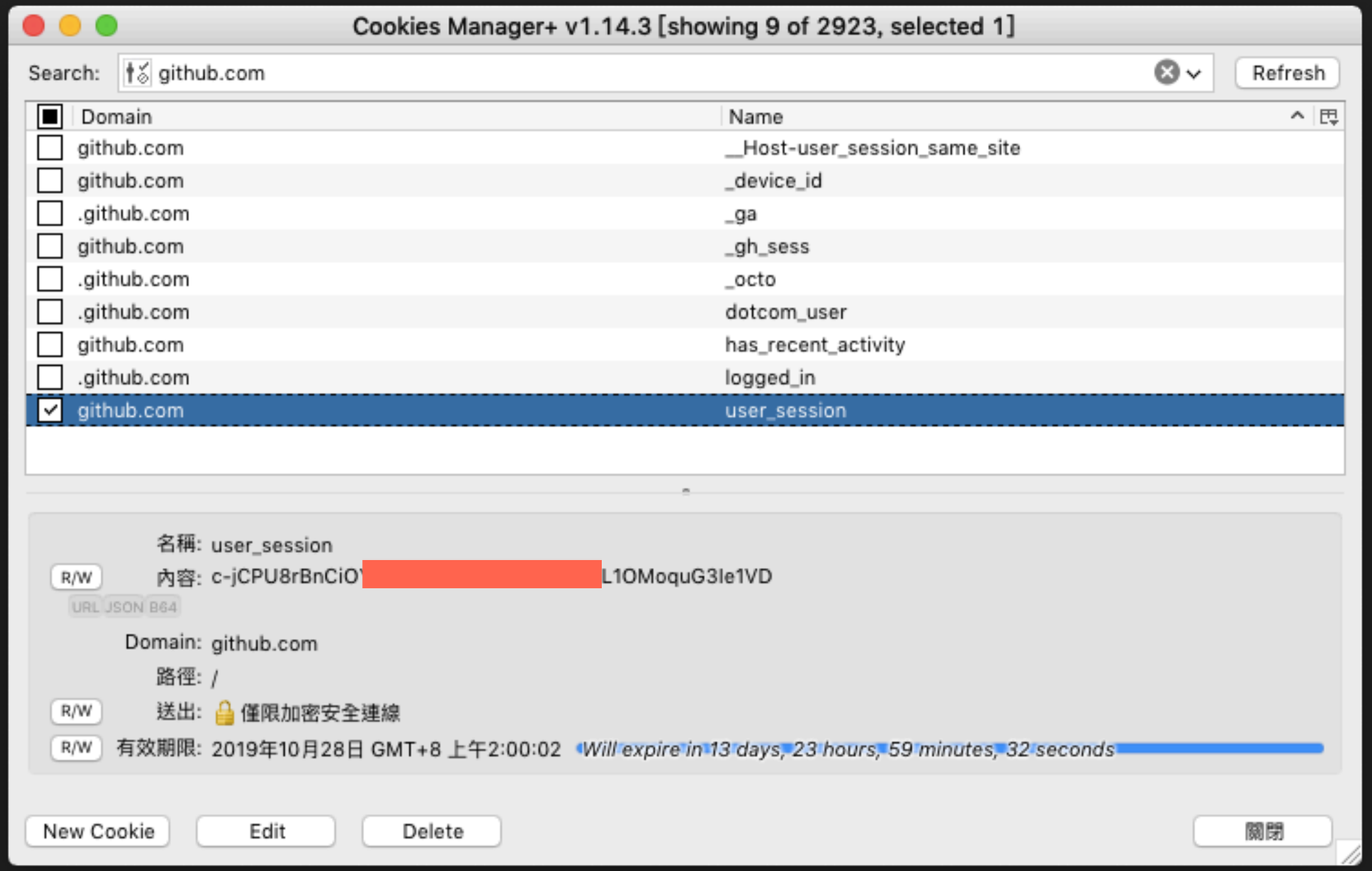
ID	SESSION
seadog	...
seacat	難以竄改
meow	user=kaibro
hotdog	...

Server

Cookie-based Session

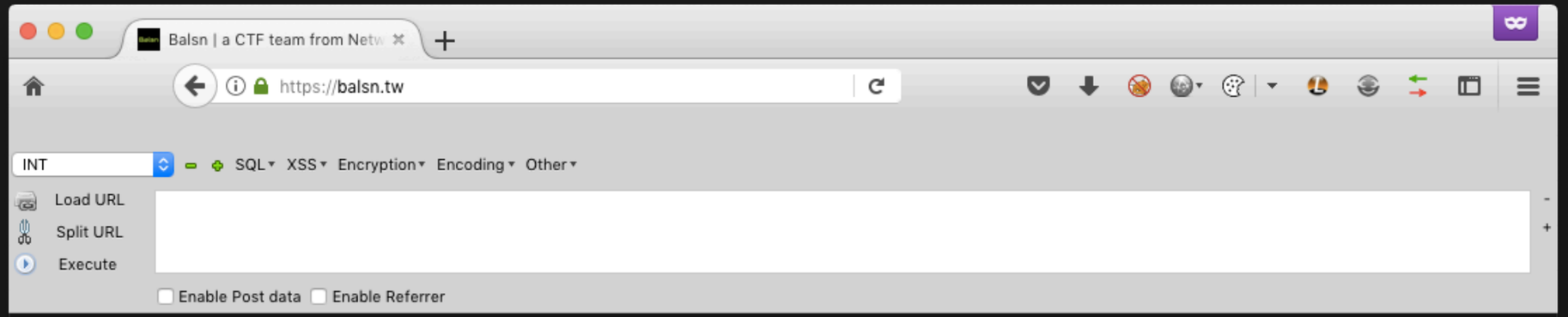
- 簡單說就是把 Session 放在 Cookie 裡
  - Data 經過加密
  - 難以竄改 (算法 & Key 未知)

Cookie-based Session



Essential Tools

- Hackbar
- Burp Suite



Balsn

a CTF team from Network Security Lab of National Taiwan University

About | Members | Awards | Contact | Writeups | CTFtime | Twitter

Balsn

News

Balsn CTF 2019 has ended!

Congrats to top 3 here and Taiwan Star:

>> 1st: hxp
>> 2nd: LC ↳ BC
>> 3rd: PPP
>> Taiwan 1st: 新竹沒放假QAQ

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Flow | Deserialization Scanner | Wsdler

1 × | 2 × | 3 × | 4 × | 5 × | 6 × | 7 × | 8 × | 9 × | ...

Go | Cancel | < | > | Target: https://balsn.tw

Request

Raw | Headers | Hex

```
GET / HTTP/1.1
Host: balsn.tw
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

< | + | > | Type a search term | 0 matches

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Server: GitHub.com
Last-Modified: Mon, 07 Oct 2019 12:34:55 GMT
ETag: W/"5d9b30ef-3ed8"
Access-Control-Allow-Origin: *
Expires: Mon, 14 Oct 2019 20:30:19 GMT
Cache-Control: max-age=600
X-Proxy-Cache: MISS
X-GitHub-Request-Id: 8754:6BC9:63DF74:6AC111:5DA4D87D
Content-Length: 16088
Accept-Ranges: bytes
Date: Mon, 14 Oct 2019 20:20:19 GMT
Via: 1.1 varnish
Age: 0
Connection: close
X-Served-By: cache-hnd18734-HND
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1571084419.339908,VS0,VE172
Vary: Accept-Encoding
X-Fastly-Request-ID: 9e433194dd21b77e3ebdae2e3dc33b8f5da766d4

<!DOCTYPE html>
<html lang="en-US">
  <head>
    <meta charset='utf-8'>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet"
href="/assets/css/style.css?v=dfd0c52ale35dd9f24e90eff9087f2a671bb9f1b">
          <link rel="icon" type="image/x-icon" sizes="16x16 24x24 32x32
48x48 64x64 96x96 128x128 256x256" href="images/favicon.ico">

<!-- Begin Jekyll SEO tag v2.5.0 -->
<title>Balsn | a CTF team from Network Security Lab of National Taiwan
University</title>
<meta name="generator" content="Jekyll v3.8.5" />
```

< | + | > | Type a search term

Done | 16,731 b

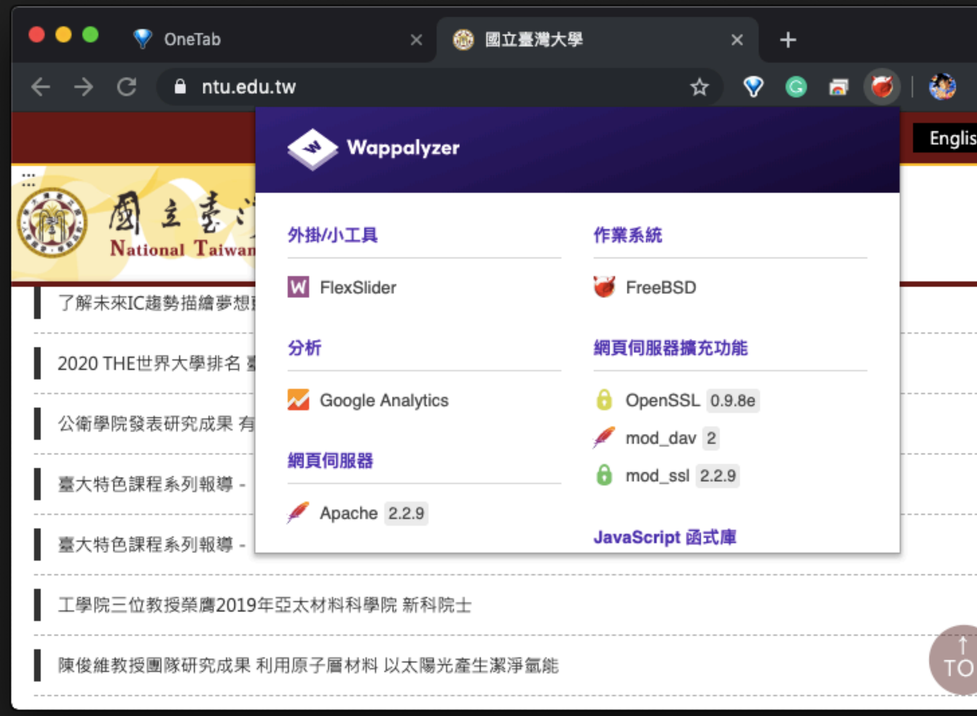
Information Gathering

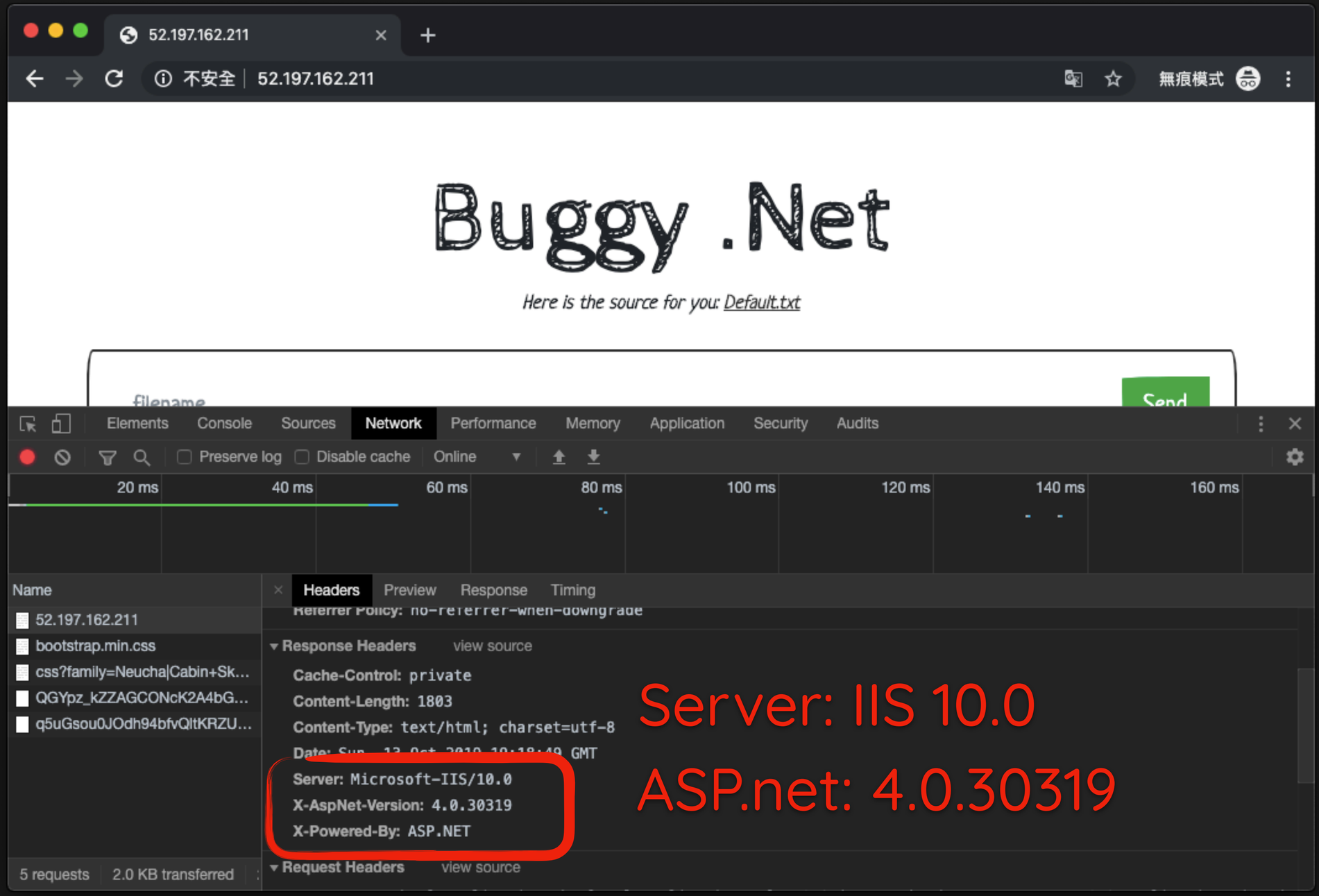
Recon (Reconnaissance)

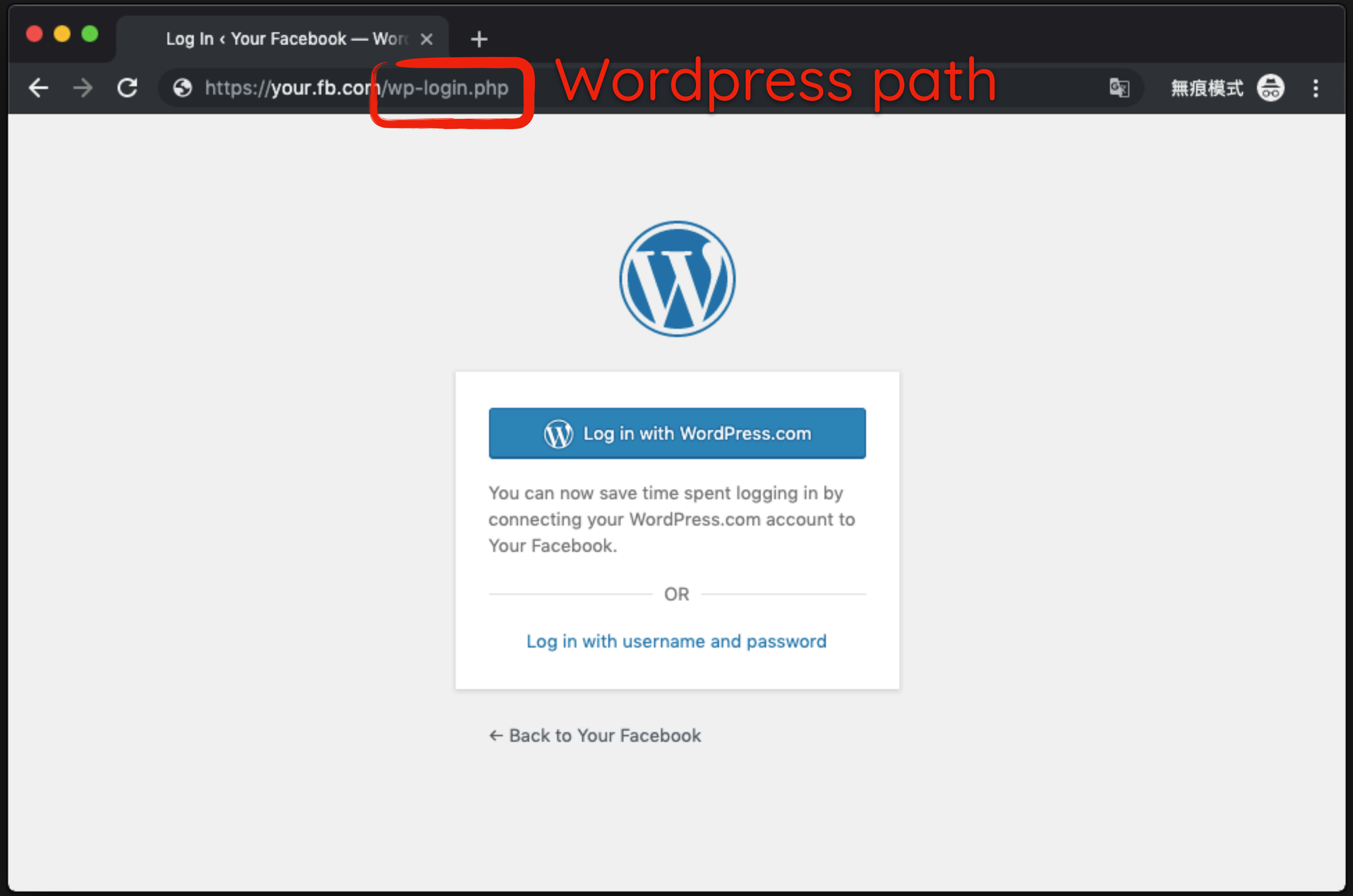
- 資訊偵查
- 針對目標搜集資訊
  - IP Range
  - Open Port (Service)
  - Sub Domain
  - Directory / Path Enumeration
  - Fingerprinting

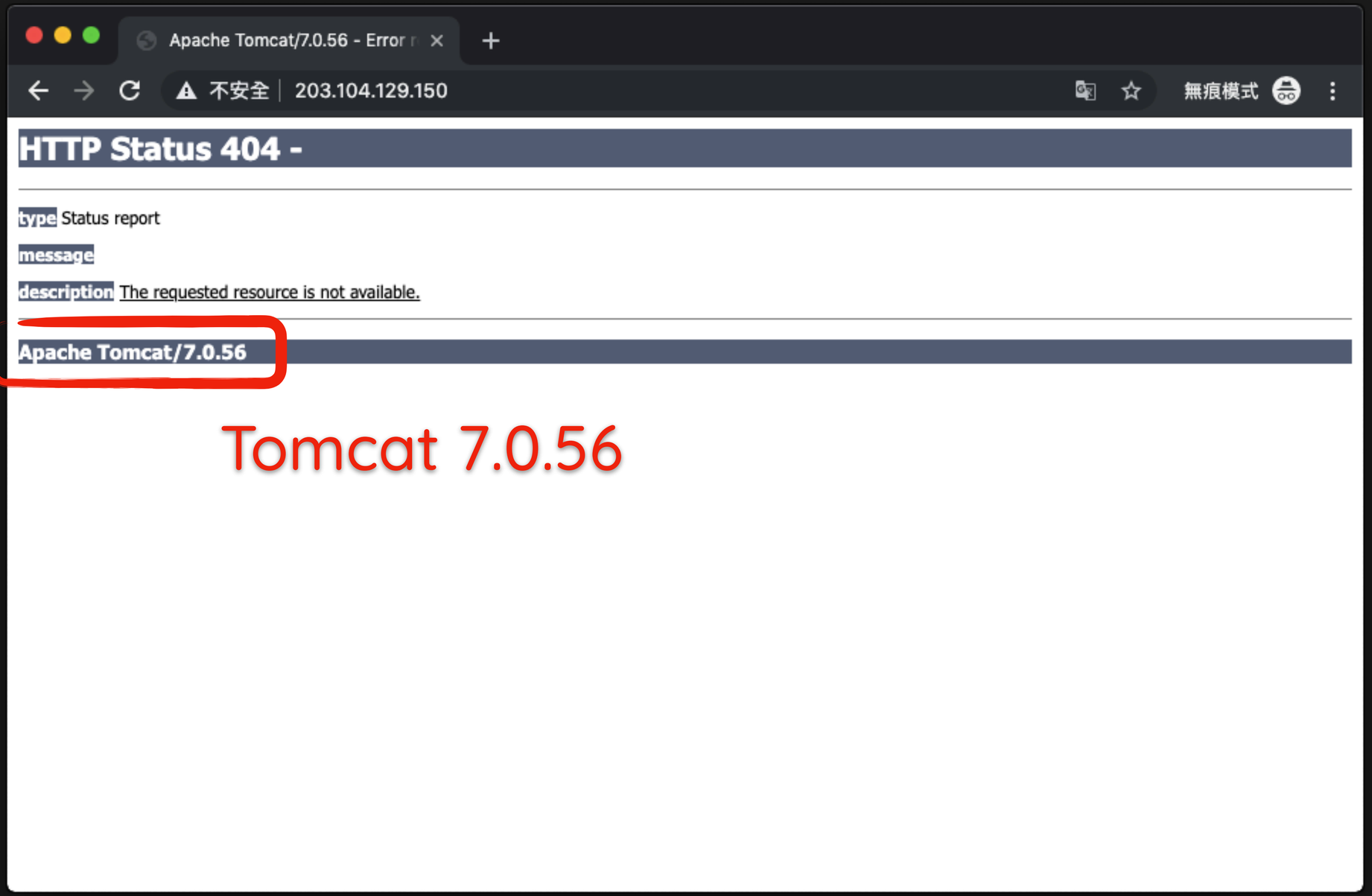
Recon (Reconnaissance)

- **指紋辨識**
  - Server Header
  - URL Route / Path
  - Error Message (HTTP 4xx / 5xx)
  - Cookie / Session ID
- Fingerprinting Tool : Wappalyzer



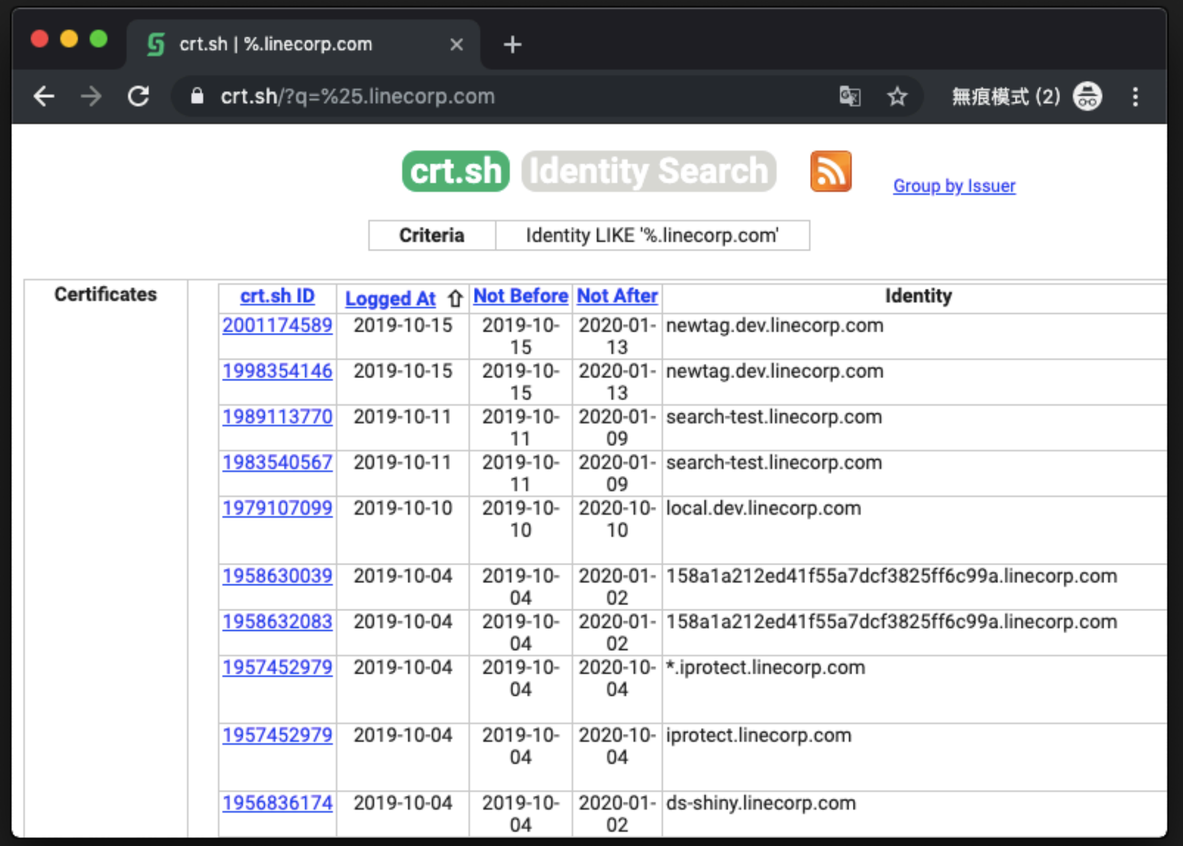

52.197.162.211
不安全 | 52.197.162.211
無痕模式
Buggy .Net
Here is the source for you: Default.txt
filename
Send
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
Preserve log
Disable cache
Online
20 ms
40 ms
60 ms
80 ms
100 ms
120 ms
140 ms
160 ms
Name
52.197.162.211
bootstrap.min.css
css?family=Neucha|Cabin+Sk...
QGYpz_kZZAGCONcK2A4bG...
q5uGsou0JOdh94bfvQlfKRZU...
Headers
Preview
Response
Timing
Response Headers
view source
Cache-Control: private
Content-Length: 1803
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Request Headers
view source
5 requests
2.0 KB transferred
Server: IIS 10.0
ASP.net: 4.0.30319

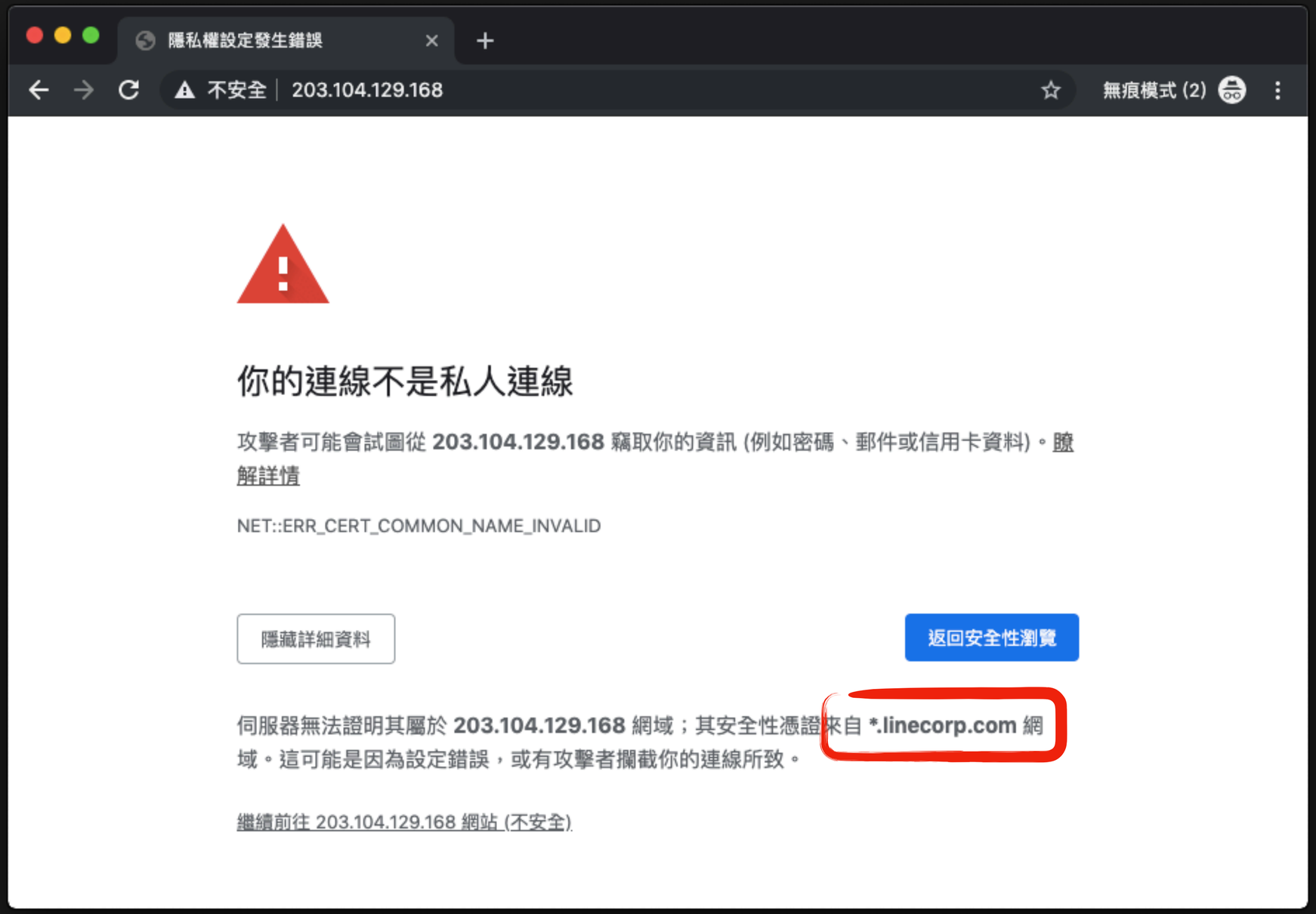

Log In ‹ Your Facebook — Wor
https://your.fb.com/wp-login.php
Wordpress path
無痕模式
Log in with WordPress.com
You can now save time spent logging in by connecting your WordPress.com account to Your Facebook.
OR
Log in with username and password
← Back to Your Facebook


Apache Tomcat/7.0.56 - Error
不安全 | 203.104.129.150
無痕模式
HTTP Status 404 -
type Status report
message
description The requested resource is not available.
Apache Tomcat/7.0.56
Tomcat 7.0.56

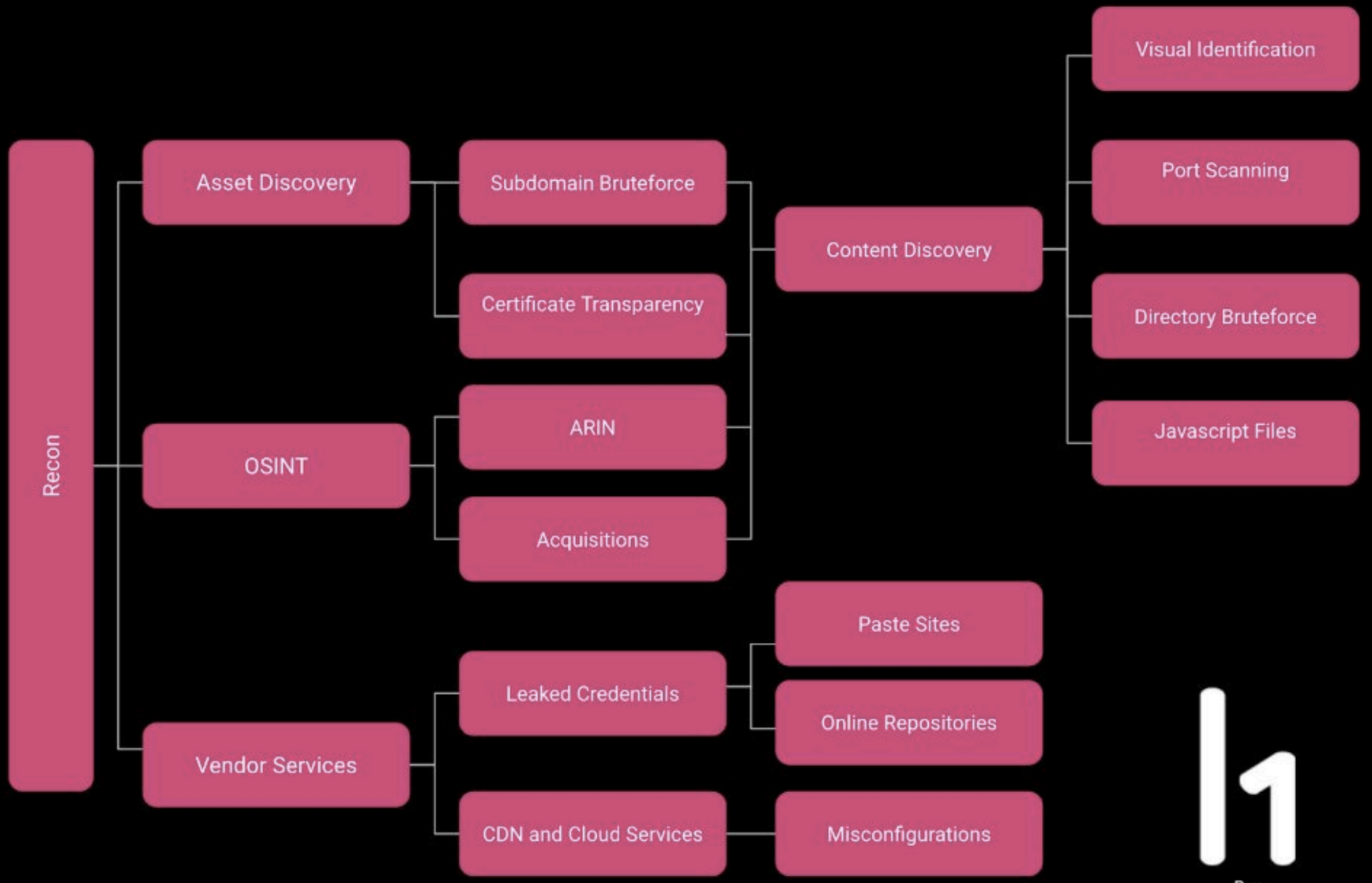
Certificate

- 憑證綁定域名
  - Domain Enumeration
  - crt.sh (憑證透明度查詢)




隱私權設定發生錯誤
不安全 | 203.104.129.168
無痕模式 (2)
你的連線不是私人連線
攻擊者可能會試圖從 203.104.129.168 竊取你的資訊 (例如密碼、郵件或信用卡資料)。瞭解詳情
NET::ERR_CERT_COMMON_NAME_INVALID
隱藏詳細資料
返回安全性瀏覽
伺服器無法證明其屬於 203.104.129.168 網域；其安全性憑證來自 *.linecorp.com 網域。這可能是因為設定錯誤，或有攻擊者攔截你的連線所致。
繼續前往 203.104.129.168 網站 (不安全)

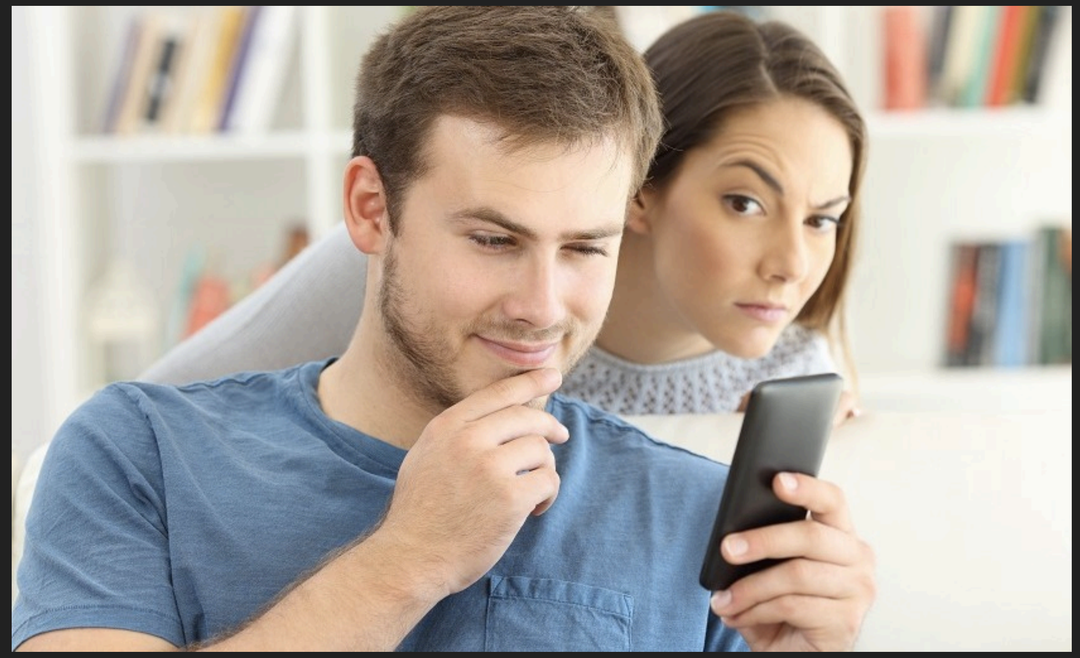
A Visual Guide to Recon



Ben
Sadeghipour
(@nahamsec)

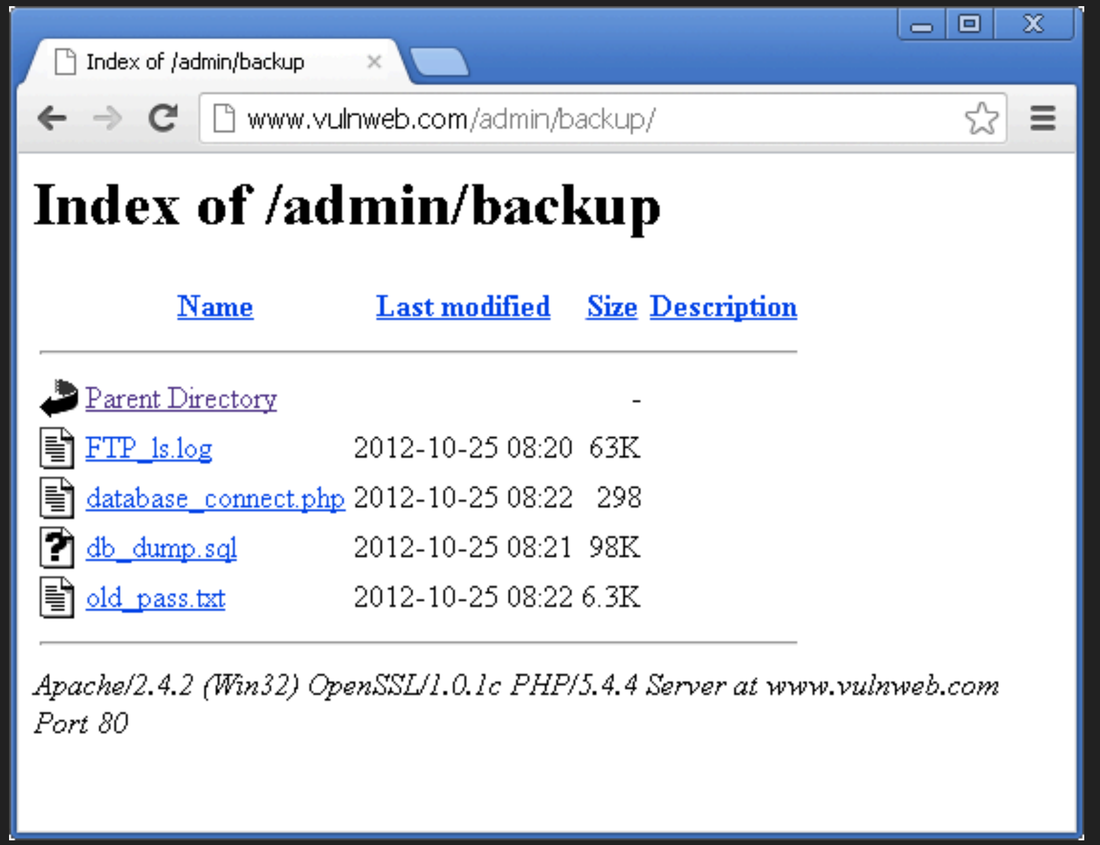
Information Leak

- Sensitive Information
  - Username / Password
  - Source Code
  - URL Route / File path
  - Config
  - . . . . . .



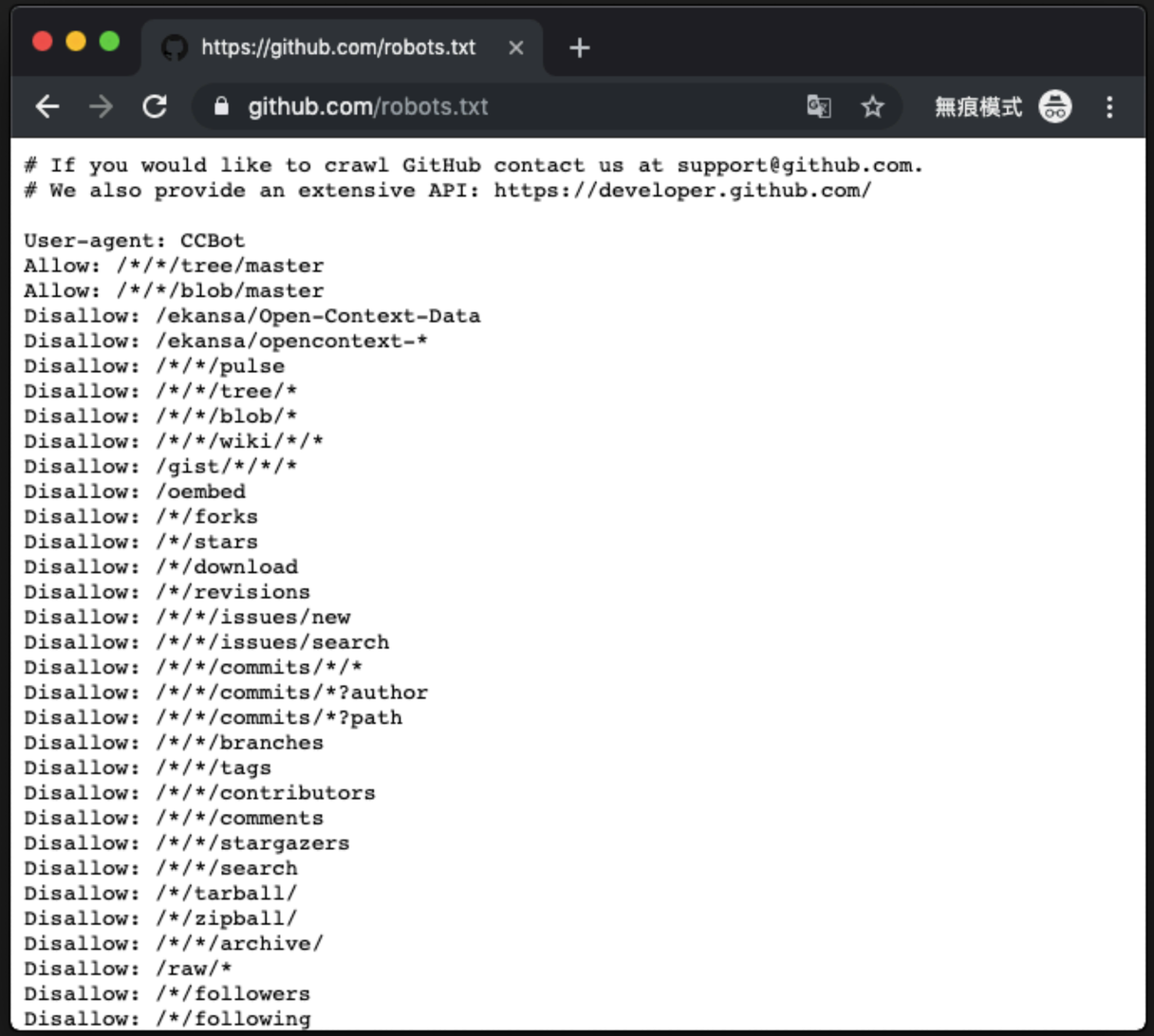
Why Leak?

- Backup files / version control
  - www.tar.gz
  - .git / .svn
- Temporary files
  - .index.php.swp
  - index.php~
- Others
  - robots.txt
  - .DS_Store



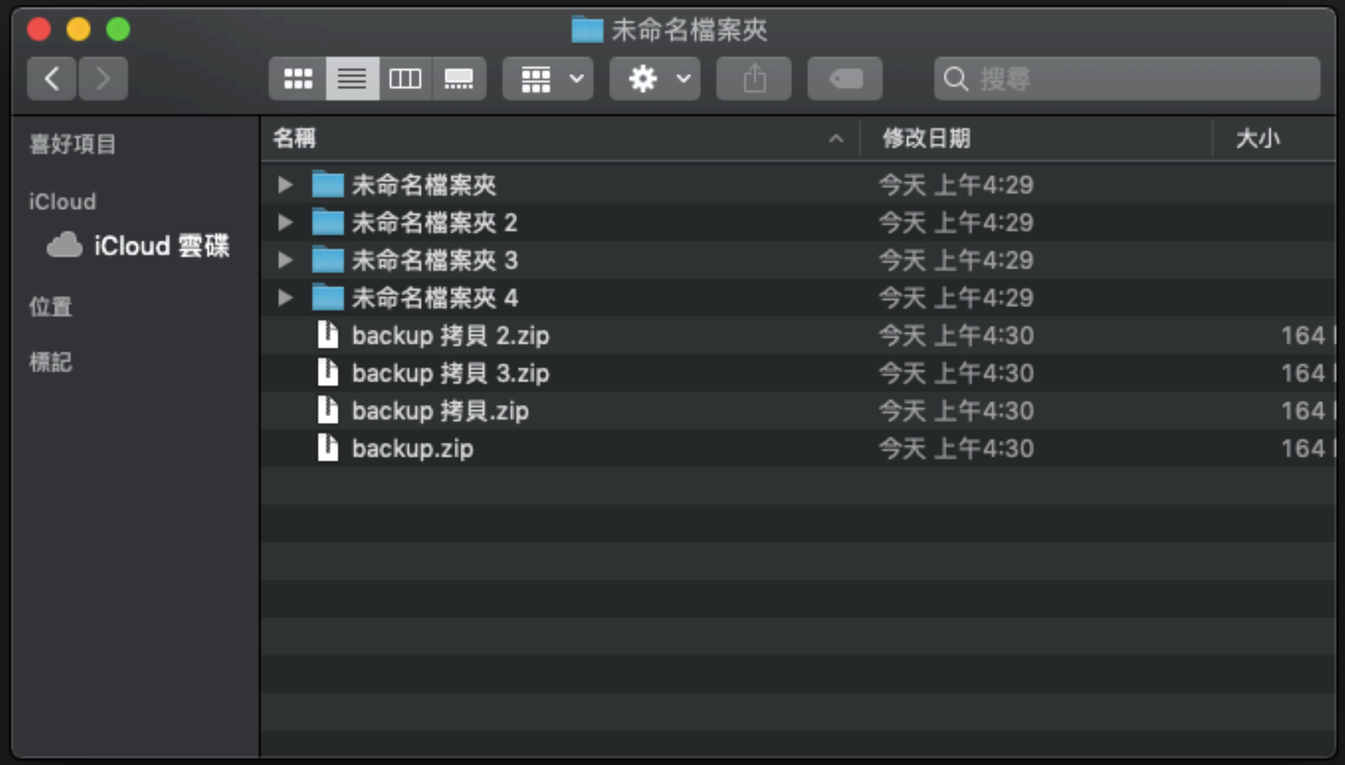
robots.txt

- 老梗
- 給搜尋引擎爬蟲看的
- 記錄不想被收錄的路徑
  - 網站後台
  - 敏感目錄



Backup files

- 週末下班前，順手備份
  - backup.zip
  - www.zip
  - www.tar.gz
  - index.php.bak

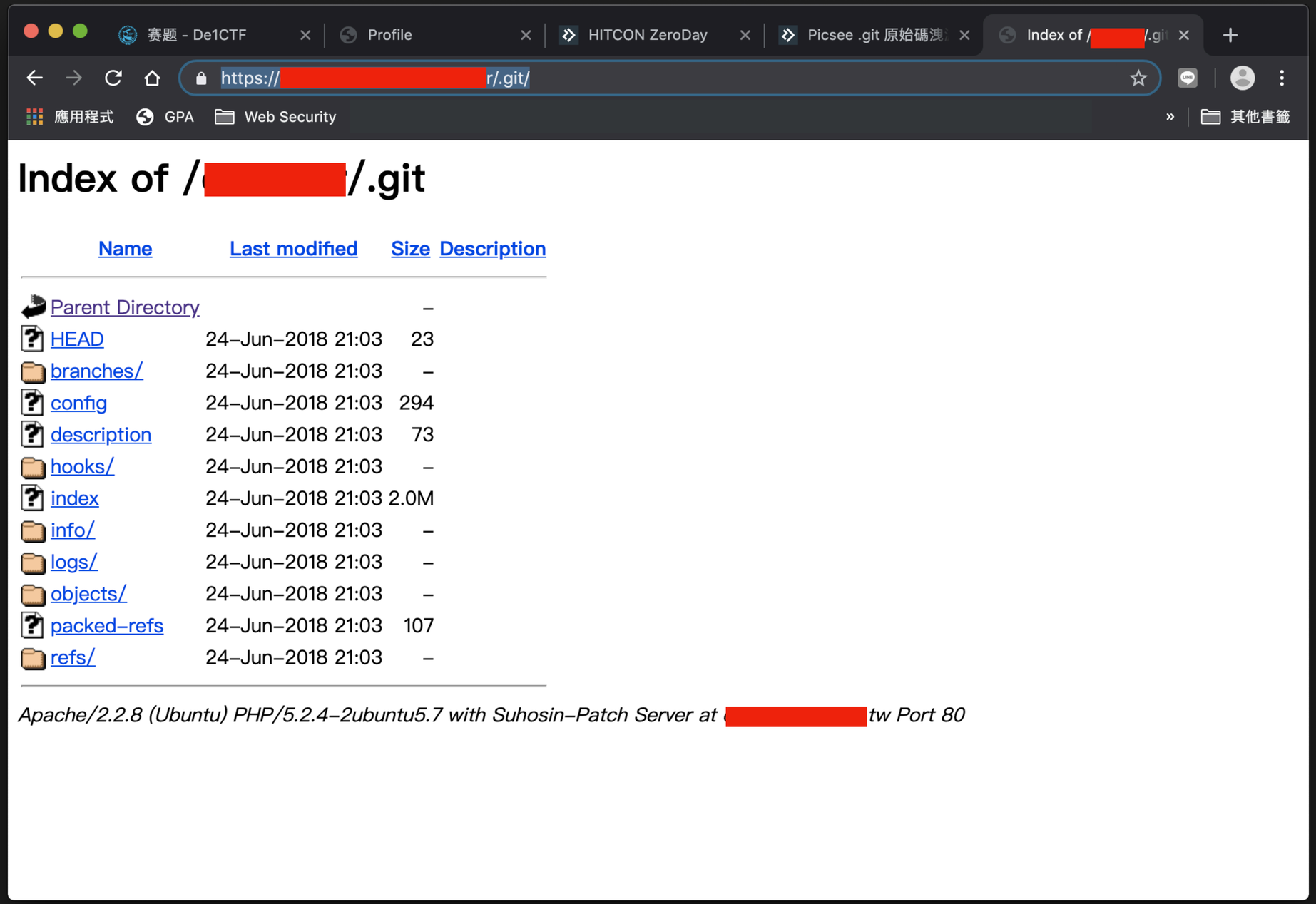


Temporary files

- 編輯器暫存檔
  - .index.php.swp
  - index.php~
  - #index.php#
- 可還原 Source Code

.git / .svn / .hg

- 版本管理系統
- 線上部署時未移除
- 可還原 Source Code
- Tool
  - github.com/denny0223/scrabble
  - github.com/lijiejie/GitHack

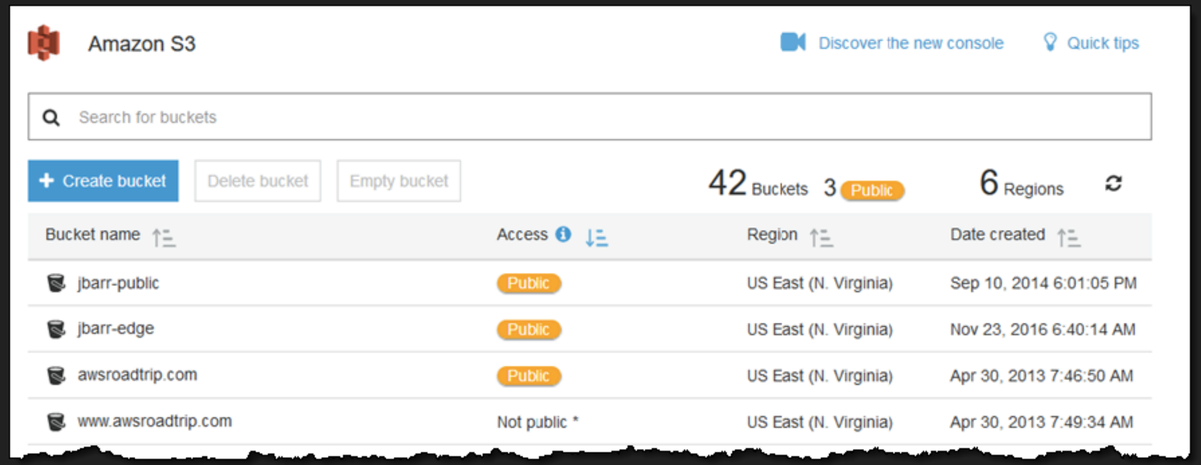

賽題 - De1CTF
Profile
HITCON ZeroDay
Picsee .git 原始碼洩
Index of /[redacted]/.git
https://[redacted]r/.git/
應用程式
GPA
Web Security
其他書籤
Index of /[redacted]/.git
Name
Last modified
Size
Description
Parent Directory -
HEAD 24-Jun-2018 21:03 23
branches/ 24-Jun-2018 21:03 -
config 24-Jun-2018 21:03 294
description 24-Jun-2018 21:03 73
hooks/ 24-Jun-2018 21:03 -
index 24-Jun-2018 21:03 2.0M
info/ 24-Jun-2018 21:03 -
logs/ 24-Jun-2018 21:03 -
objects/ 24-Jun-2018 21:03 -
packed-refs 24-Jun-2018 21:03 107
refs/ 24-Jun-2018 21:03 -
Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.7 with Suhosin-Patch Server at [redacted]tw Port 80

.DS_Store

- Mac 上的常見隱藏檔
- 記錄資料夾文件相關資訊
- 可以列舉資料夾內的檔案名稱
- Tool
  - github.com/lijiejie/ds_store_exp

AWS S3 Bucket

- AWS 雲端儲存服務
- 權限設定錯誤 (Public)
  - 枚舉 Bucket Name
  - buckets.grayhatwarfare.com
- Tool: github.com/sa7mon/S3Scanner



Case study: https://medium.com/@protector47/how-i-earned-1-500-in-just-15-mins-due-to-amazon-s3-bucket-misconfiguration-953b28242f95

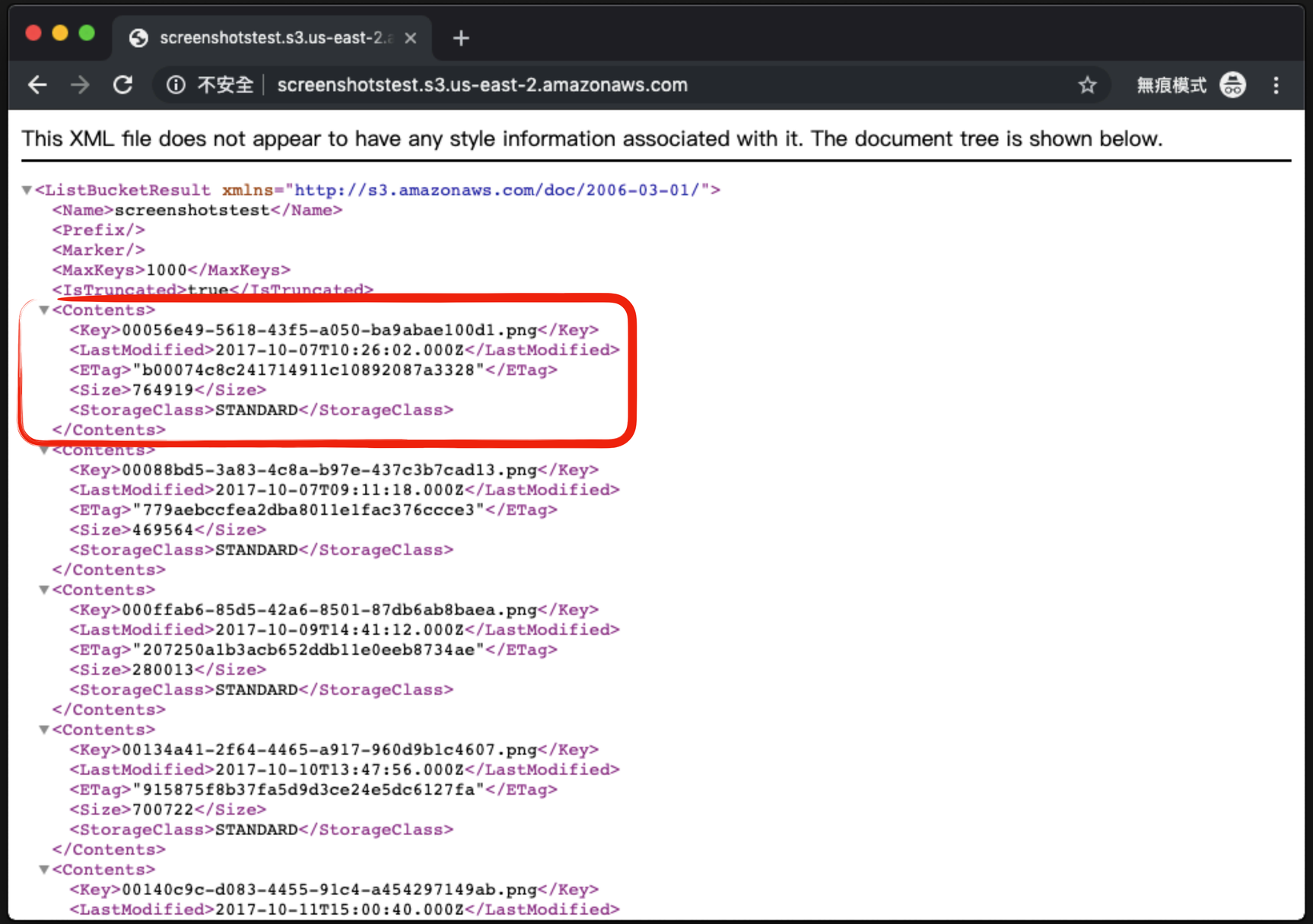
AWS S3 Bucket

- Bucket Name 是**全域唯一**的
- Endpoint format

  [bucket name].[region].amazonaws.com

  [region].amazonaws.com/[bucket name]　(2020廢除)

- Example: s3-us-east-2.amazonaws.com/kaibro/secret.txt

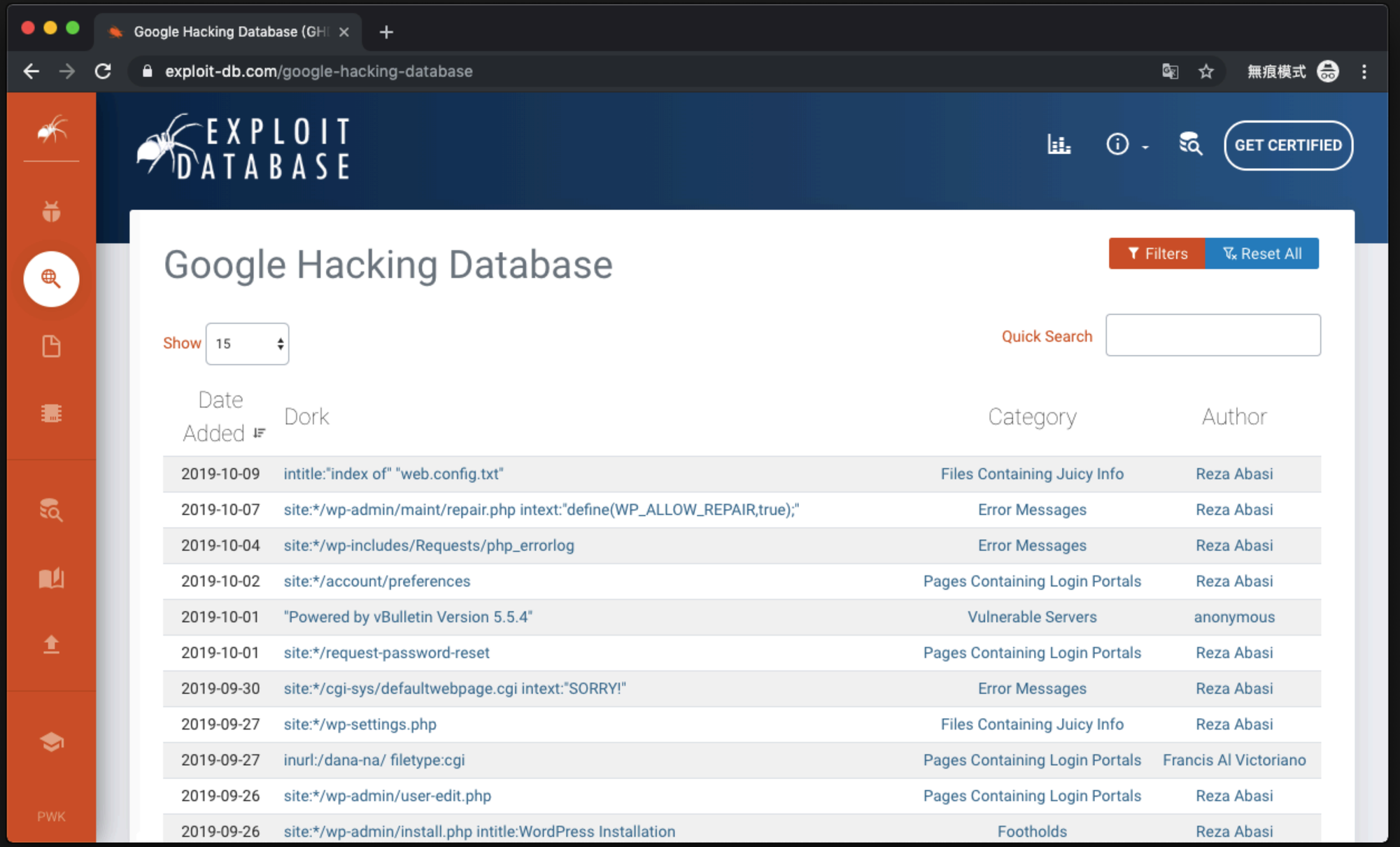


This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>screenshotstest</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>true</IsTruncated>
  <Contents>
    <Key>00056e49-5618-43f5-a050-ba9abae100d1.png</Key>
    <LastModified>2017-10-07T10:26:02.000Z</LastModified>
    <ETag>"b00074c8c241714911c10892087a3328"</ETag>
    <Size>764919</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>00088bd5-3a83-4c8a-b97e-437c3b7cad13.png</Key>
    <LastModified>2017-10-07T09:11:18.000Z</LastModified>
    <ETag>"779aebccfea2dba8011e1fac376ccce3"</ETag>
    <Size>469564</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>000ffab6-85d5-42a6-8501-87db6ab8baea.png</Key>
    <LastModified>2017-10-09T14:41:12.000Z</LastModified>
    <ETag>"207250a1b3acb652ddb11e0eeb8734ae"</ETag>
    <Size>280013</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>00134a41-2f64-4465-a917-960d9b1c4607.png</Key>
    <LastModified>2017-10-10T13:47:56.000Z</LastModified>
    <ETag>"915875f8b37fa5d9d3ce24e5dc6127fa"</ETag>
    <Size>700722</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <Contents>
    <Key>00140c9c-d083-4455-91c4-a454297149ab.png</Key>
    <LastModified>2017-10-11T15:00:40.000Z</LastModified>
```

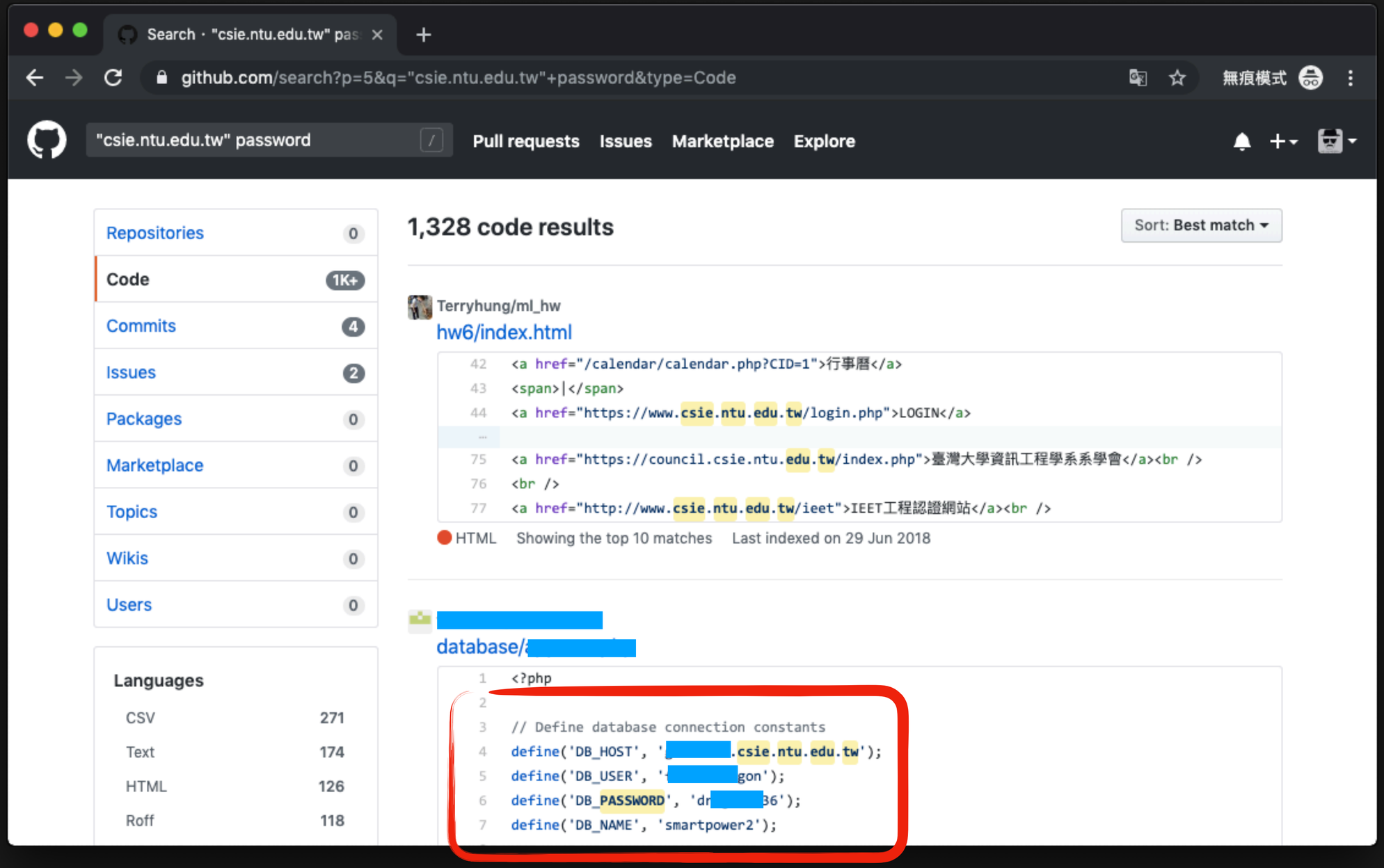
Google Hacking

- 用 Google 來打站
- 搜尋支援多種語法
  - site:ntu.edu.tw login
  - site:tw ext:sql password
  - . . . . . .

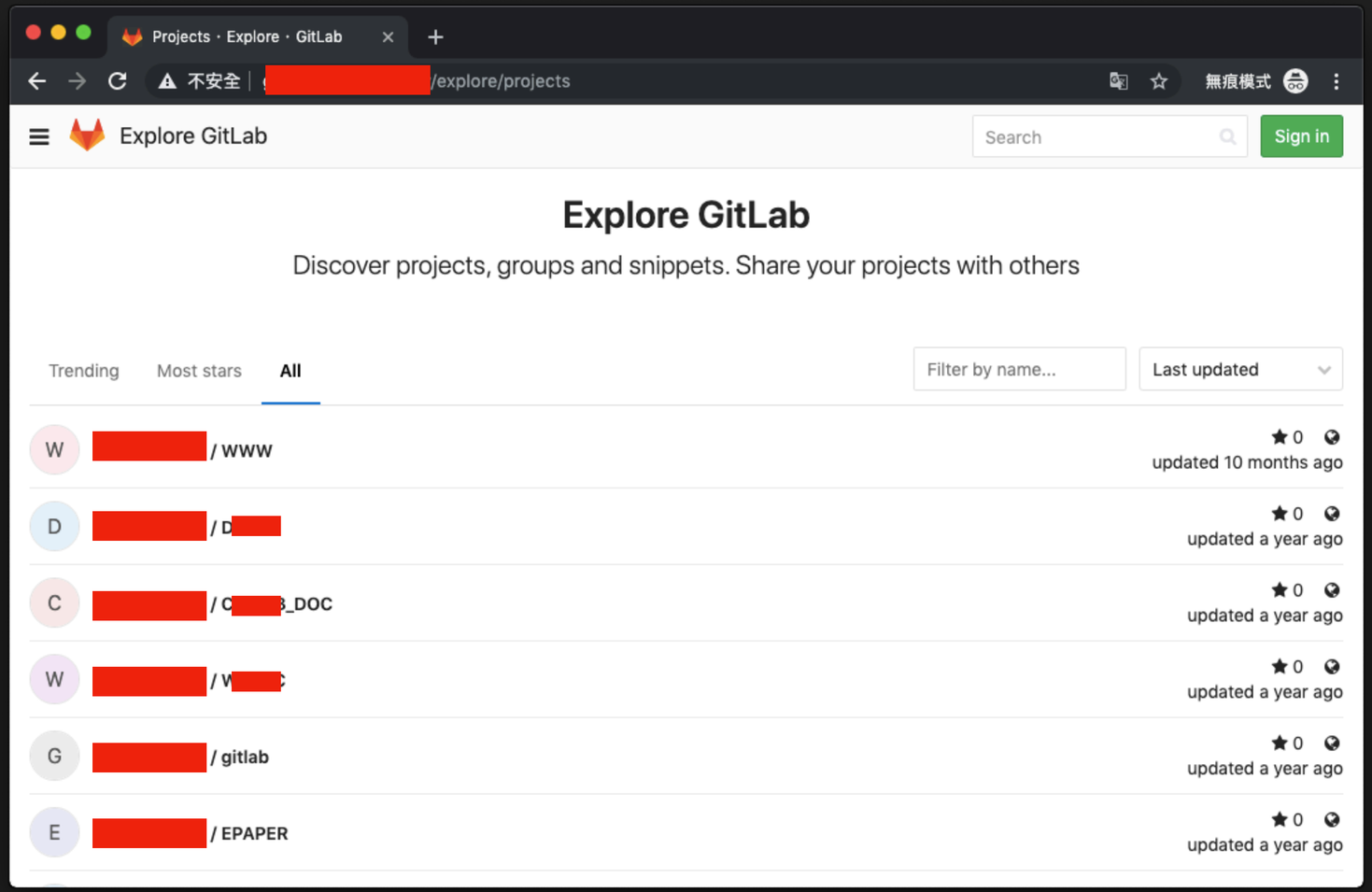

Google Hacking Database (GH
exploit-db.com/google-hacking-database
無痕模式
EXPLOIT DATABASE
GET CERTIFIED
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
Date Added
Dork
Category
Author
2019-10-09 intitle:"index of" "web.config.txt" Files Containing Juicy Info Reza Abasi
2019-10-07 site:*/wp-admin/maint/repair.php intext:"define(WP_ALLOW_REPAIR,true);" Error Messages Reza Abasi
2019-10-04 site:*/wp-includes/Requests/php_errorlog Error Messages Reza Abasi
2019-10-02 site:*/account/preferences Pages Containing Login Portals Reza Abasi
2019-10-01 "Powered by vBulletin Version 5.5.4" Vulnerable Servers anonymous
2019-10-01 site:*/request-password-reset Pages Containing Login Portals Reza Abasi
2019-09-30 site:*/cgi-sys/defaultwebpage.cgi intext:"SORRY!" Error Messages Reza Abasi
2019-09-27 site:*/wp-settings.php Files Containing Juicy Info Reza Abasi
2019-09-27 inurl:/dana-na/ filetype:cgi Pages Containing Login Portals Francis Al Victoriano
2019-09-26 site:*/wp-admin/user-edit.php Pages Containing Login Portals Reza Abasi
2019-09-26 site:*/wp-admin/install.php intitle:WordPress Installation Footholds Reza Abasi
PWK

GitHub Hacking

- GitHub： 全球最大男性交友平台
- 大家都喜歡上傳密碼、Secret Key
- 第三方套件白箱找洞洞

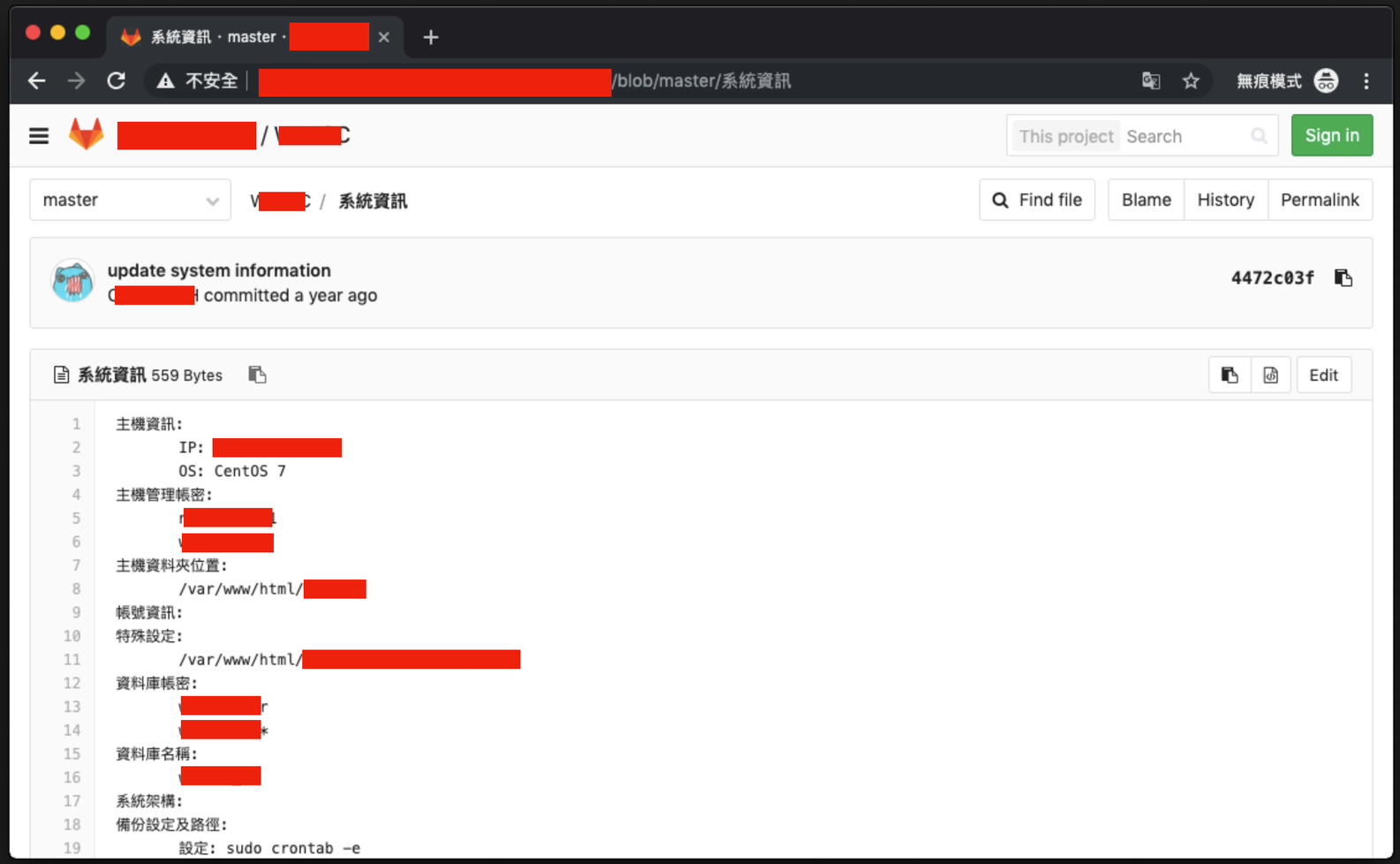

Search · "csie.ntu.edu.tw" pas
github.com/search?p=5&q="csie.ntu.edu.tw"+password&type=Code
無痕模式
"csie.ntu.edu.tw" password
Pull requests
Issues
Marketplace
Explore
Repositories 0
Code 1K+
Commits 4
Issues 2
Packages 0
Marketplace 0
Topics 0
Wikis 0
Users 0
Languages
CSV 271
Text 174
HTML 126
Roff 118
1,328 code results
Sort: Best match
Terryhung/ml_hw
hw6/index.html
42 行事曆
43 |
44 LOGIN
75 臺灣大學資訊工程學系系學會
76
77 IEET工程認證網站
HTML Showing the top 10 matches Last indexed on 29 Jun 2018
database/
1 <?php
3 // Define database connection constants
4 define('DB_HOST', '.csie.ntu.edu.tw');
5 define('DB_USER', 'gon');
6 define('DB_PASSWORD', 'dr36');
7 define('DB_NAME', 'smartpower2');

Case Study: GitLab Leak



Public Repo

Case Study: GitLab Leak



Common Tools

- Port Scan
  - NMAP
  - Masccan
- DNS Discovery
  - Sublist3r
  - Amass
- Directory / File Scan
  - dirseach
  - DirBuster
- Asset identification
  - Shodan
  - Censys

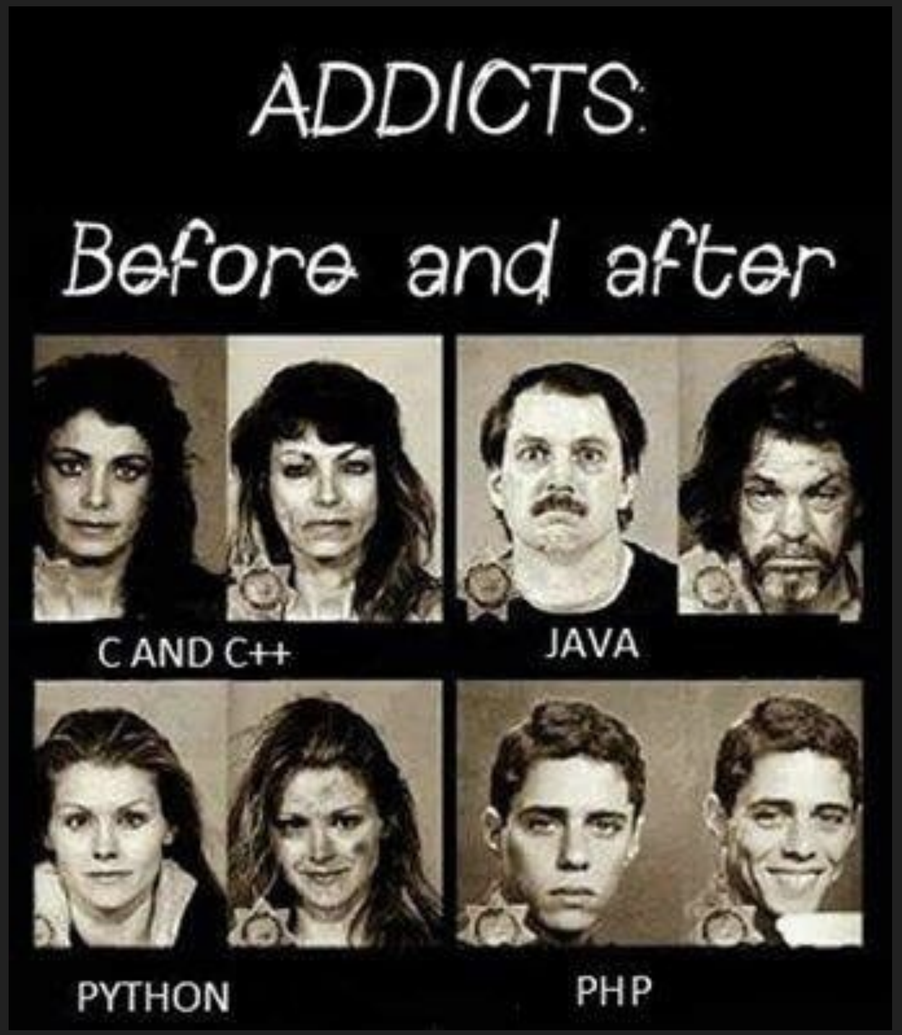

php

PHP是世界上最好的語言

胡適

Introduction

- Hacker Friendly
- 很多開發者常疏忽的黑魔法
- 到處都是 PHP 網站
  - 例如: 台科大、交大首頁
  - Wordpress, Drupal, Joomla



My First PHP Bug

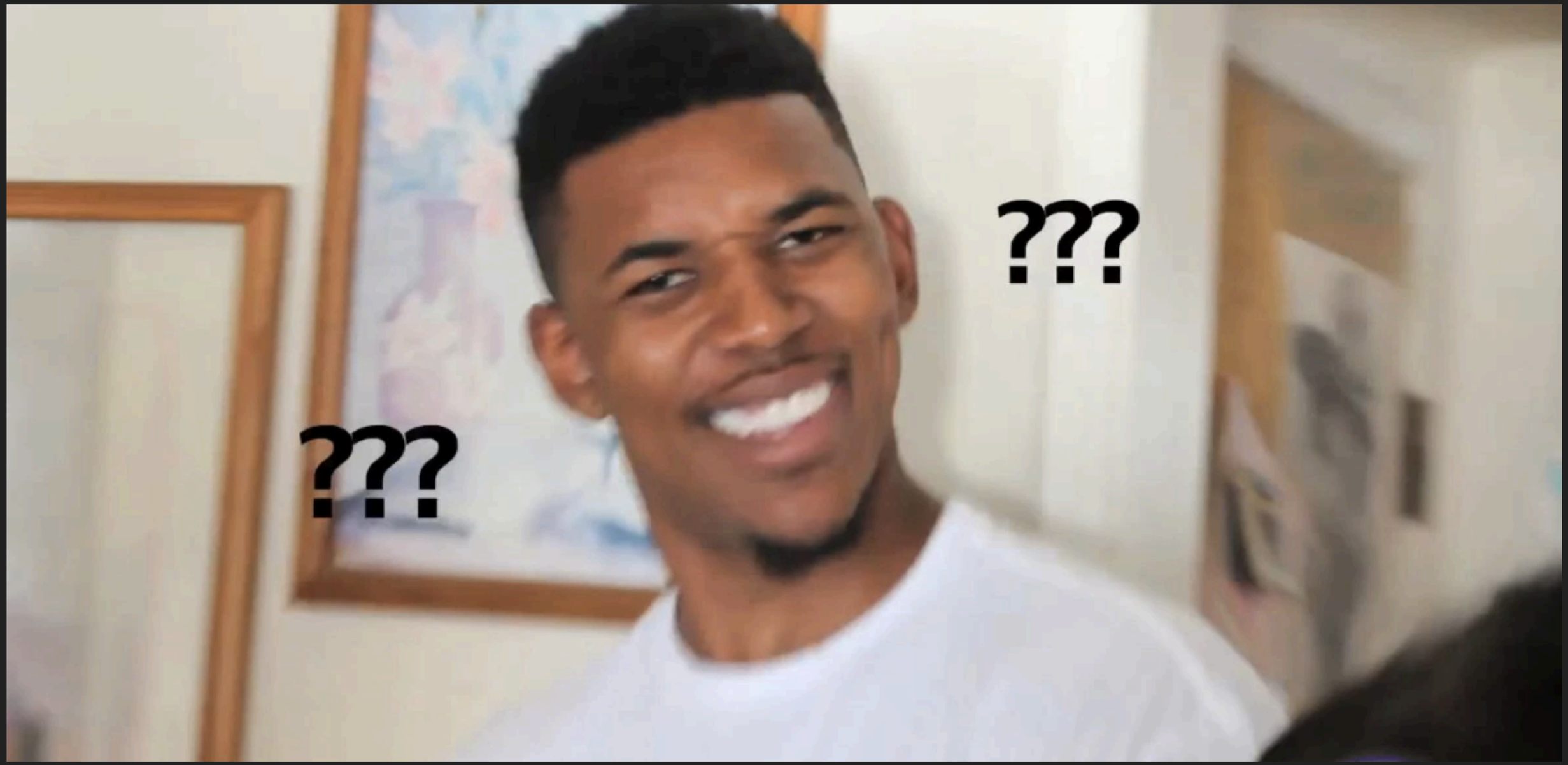
```
NULL == 0

NULL <  -1
```

My First PHP Bug

NULL == 0 ⟶ bool(true)

NULL < -1 ⟶ bool(true)



Weak Type

- Auto Type Casting

```
"1" + "2"          ⟶  int(3)
"5" + 5.5          ⟶  float(10.5)
"30cm" == 30       ⟶  bool(true)
false == NULL      ⟶  bool(true)
```

經典例子


```php
$hash = "0e666666666666666666666666666666";
if(md5($_GET['secret']) == $hash)
    echo "YOU WIN!";
```

經典例子

```php
$hash = "0e666666666666666666666666666666";
if(md5($_GET['secret']) == $hash)
    echo "YOU WIN!";
```

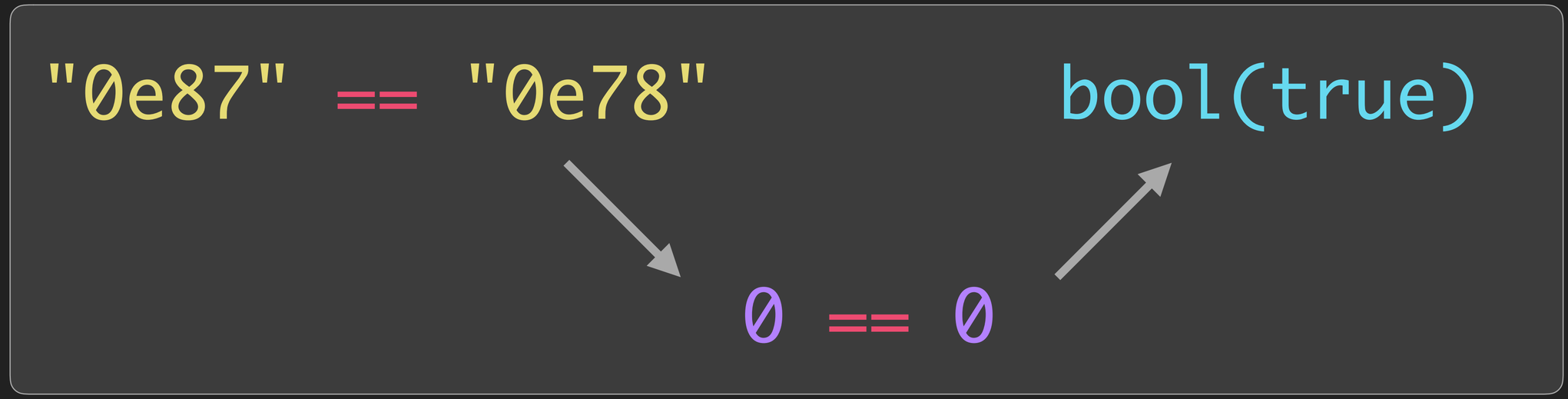
Solution: /?secret=240610708

```
md5("240610708")
```

```
"0e462097431906509019562988736854"
```

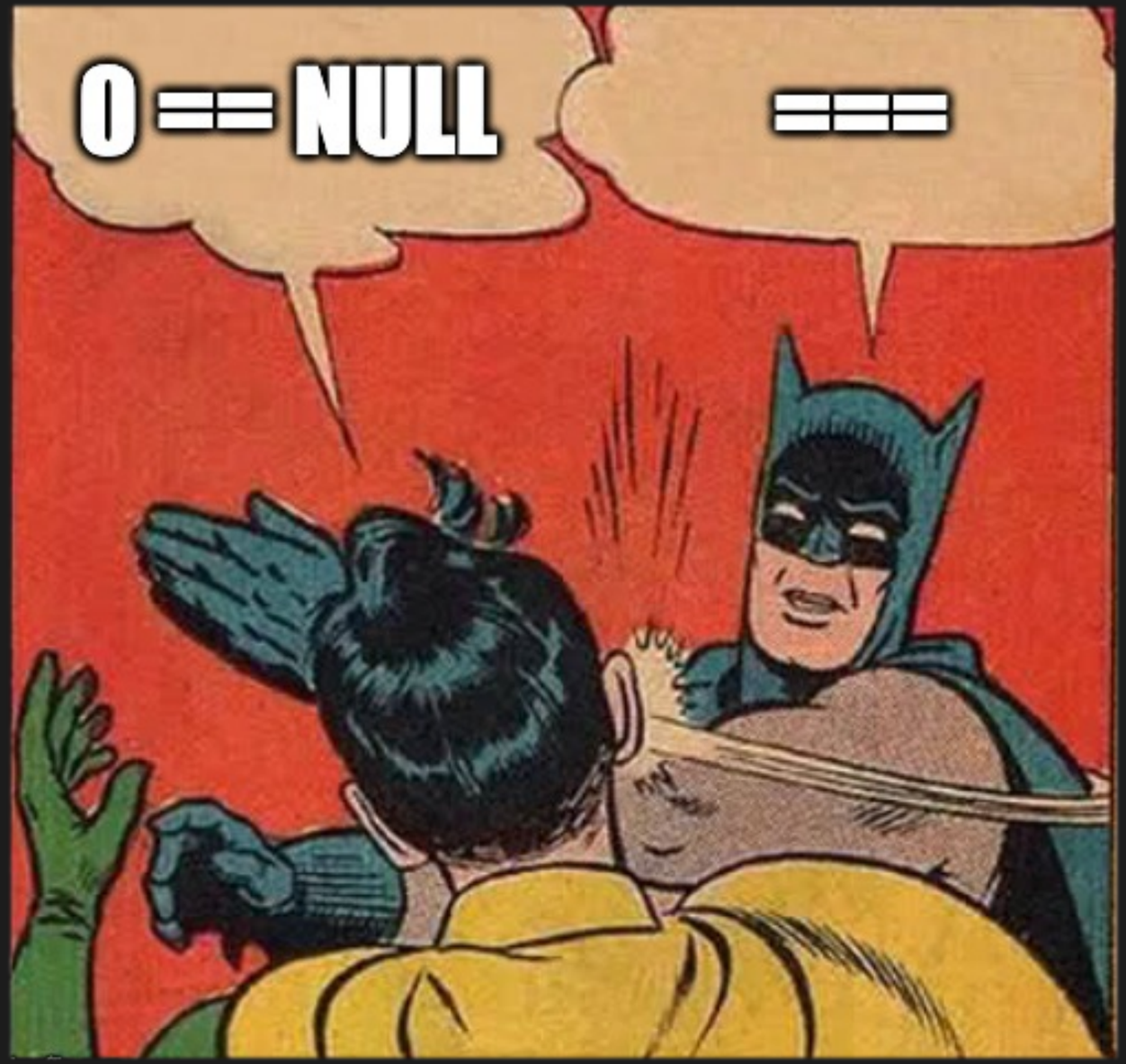
Why?

- (number) e (number)
  - 科學記號



Loose comparisons with ==

	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
-1	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
"1"	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
"0"	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
"-1"	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
NULL	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE
array()	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
"php"	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
""	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE


0 == NULL
===

More Magic !

- `md5([]) == NULL`
- `strcmp([], []) == NULL`
- `strlen([]) == NULL`
- `file_put_contents("a.php", ["<?","php", " phpinfo();"])`
  - 先拼接，再寫入
  - `<?php phpinfo();`

經典例子


```php
$pass = $_GET['pass'];
if( strcmp($pass, $secret) == 0 )
    echo "YOU WIN!";
```

經典例子


```php
$pass = $_GET['pass'];
if( strcmp($pass, $secret) == 0 )
    echo "YOU WIN!";
```

Solution: /?pass[]=x

經典例子 again


```php
$name = $_POST['name'];
$r = $db->find($name);
if($r->pass === md5($_POST['pass']))
    echo "Login success";
```

How to bypass?

經典例子 again


```php
$name = $_POST['name'];
$r = $db->find($name);
if($r->pass === md5($_POST['pass']))
    echo "Login success";
```

如果用戶不存在 . . .

經典例子 again


```php
$name = $_POST['name'];
$r = $db->find($name);
if($r->pass === md5($_POST['pass']))
    echo "Login success";
```

$r->pass ⟶ NULL

經典例子 again


```php
$name = $_POST['name'];
$r = $db->find($name);
if($r->pass === md5($_POST['pass']))
    echo "Login success";
```

Solution: name=nonexist&pass[]=x

More Magic !

- Array Bracket
    - `$array[87] === $array{87}`
- Double Quote Evaluation
    - `$msg = "Hello, $name"`
    - `$msg = "${@phpinfo()}"`
- Case Insensitive
    - `<?pHP sYStEm(ls);`


GIVE ME MORE!


RTFM
https://php.net/manual/

How to find bugs?

- Garbage In, Garbage Out
- 由上到下: 從使用者輸入往下追到危險函數
- 由下到上: 從危險函數往上追到使用者輸入

How to find bugs?

- Input
  - $_GET / $_POST / $_REQUEST
  - $_COOKIE / $_SESSION
  - $_SERVER
  - $_FILES
  - $_ENV
  - ……

How to find bugs?

- Dangerous functions
  - system
  - shell_exec / exec
  - popen / proc_open
  - assert
  - passthru
  - create_function
  - *_replace
  - include / include_once
  - requre / require_once
  - ……

How to find bugs?

- Dangerous functions
  - system
  - shell_exec / exec
  - popen / proc_open
  - assert
  - passthru
  - create_function
  - *_replace
  - include / include_once
  - requre / require_once
  - ……

p.s. eval 不是 function

Lab 0x01 - Sushi 🍣

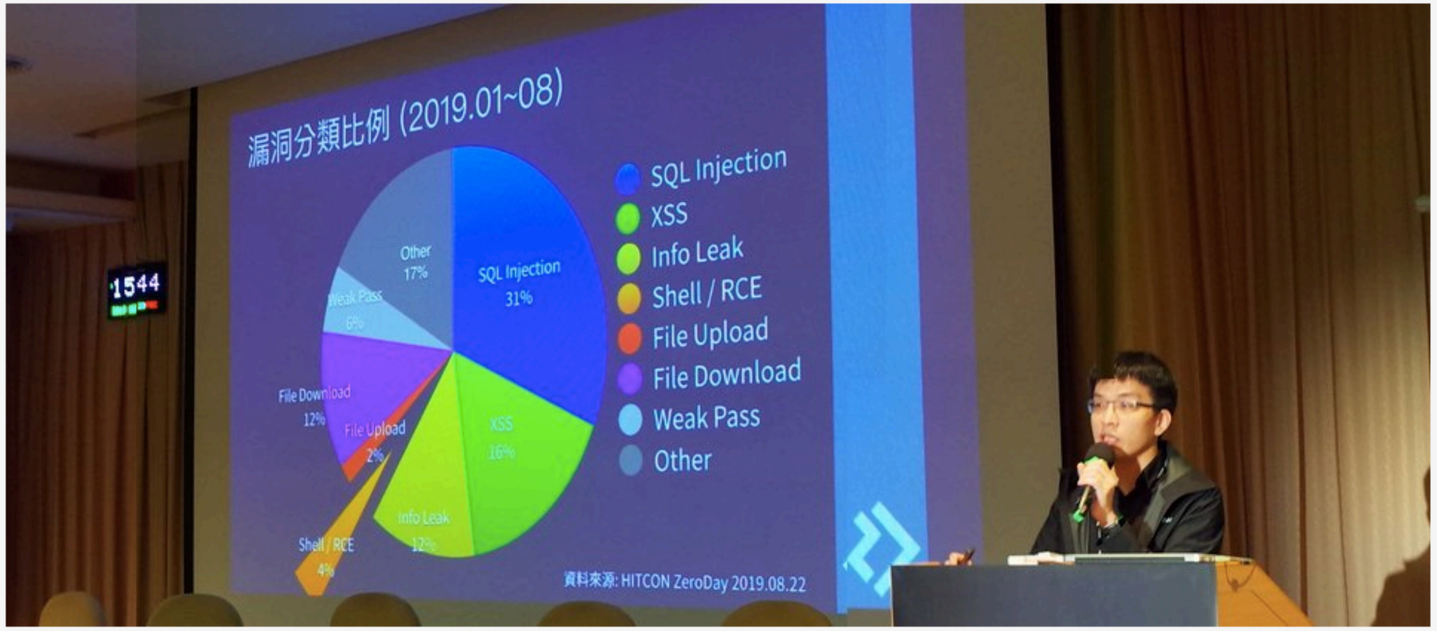
Common Vulnerabilities

Weak Password

2019年HITCON ZeroDay漏洞通報現況，弱密碼問題通報數量增，平臺新增人才媒合功能

最新臺灣漏洞通報趨勢出爐！並宣布推出人才媒合功能。在今年HITCON ZeroDay漏洞通報的分類中，多年來常見SQL Injection、XSS漏洞仍然最多，而弱密碼問題是今年需要關注的新焦點。

文/ 羅正漢 | 2019-08-24 發表



第11屆iT邦幫忙鐵人賽熱門文章

- 到日本當軟體工程師的入門指南 – 去日本一定要滑雪啊啊啊!!
- 開源暴力攻擊防禦工具：IPBan
- 開源登入事件分析工具：LogonTracer
- Day25: [Misc] 我從來沒想過我會害怕寫code

Weak Password

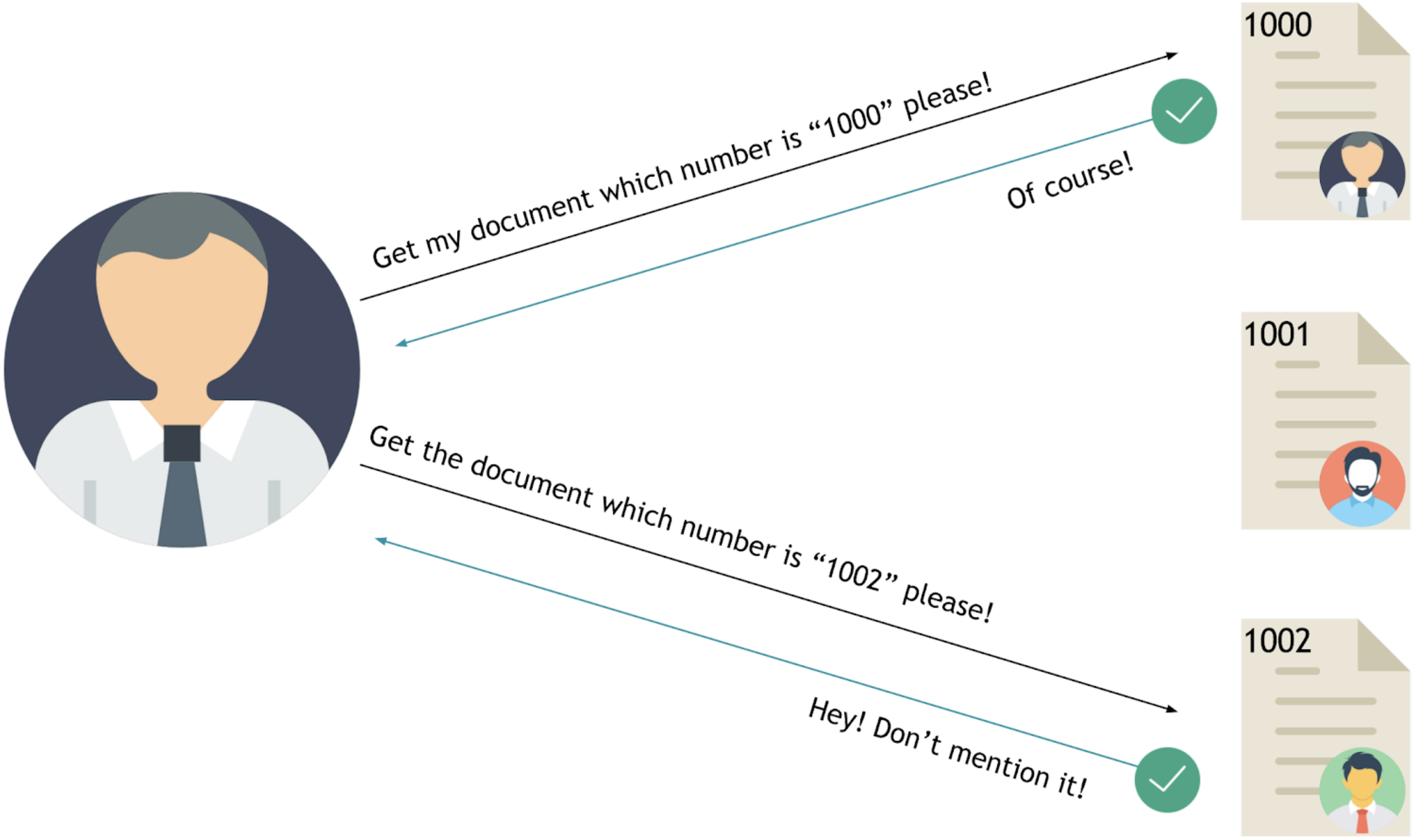
- 系統預設密碼未更改
  - admin / admin
  - tomcat / s3cret
- 密碼過於簡單
  - admin / 123456
  - root / hello123

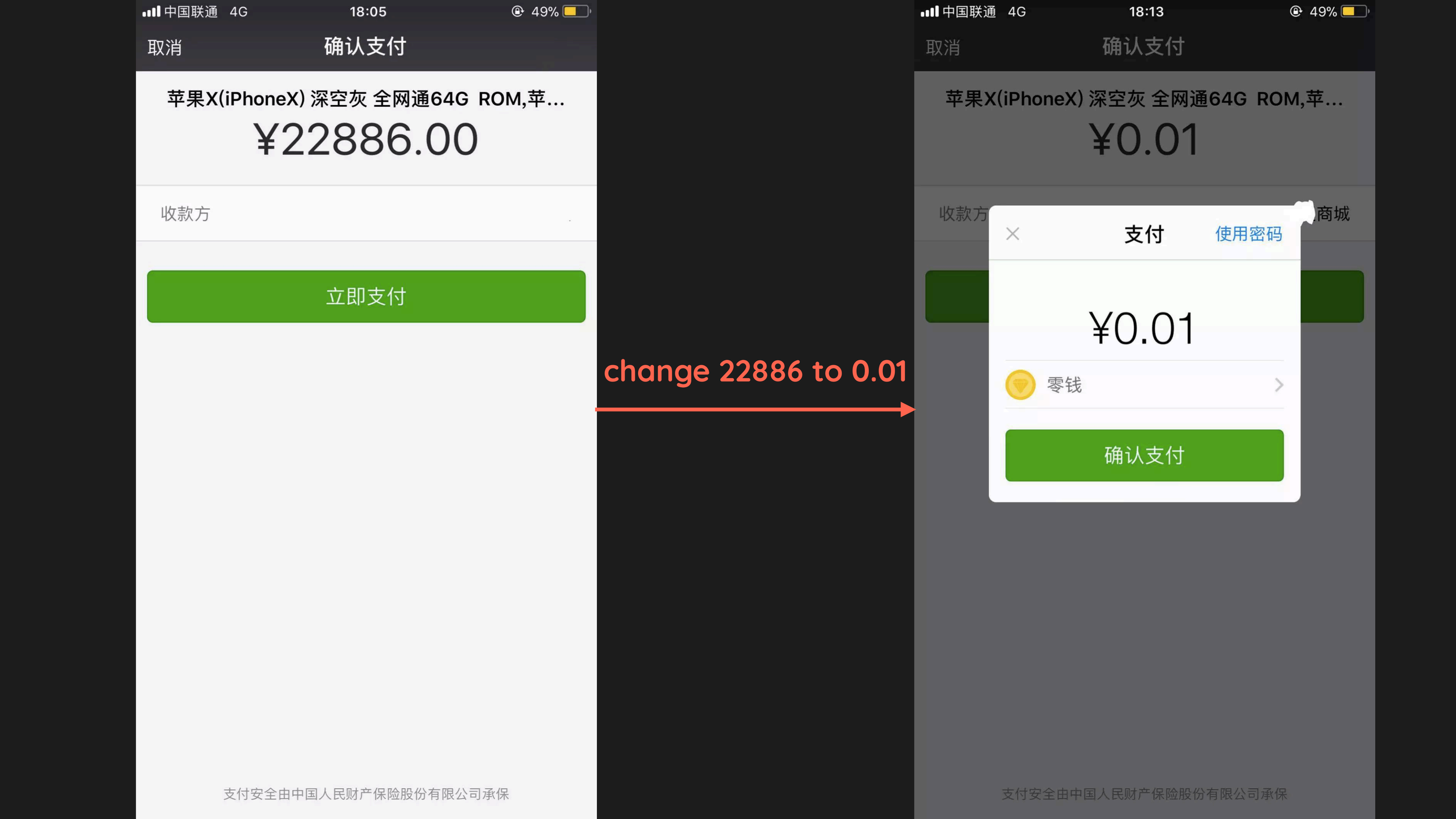

Mark Zuckerberg @finkd
Hey, @finkd You were in Linkedin Database with the password "dadada" ! DM for proof..
Hacked By OurMine Team - Read
@zuck
ZUCK GET PWNED!

「dadada」

Insecure Direct Object References

- 平行權限管控不當
  - /user/1001/changePassword
  - /user/1002/changePassword
- 垂直權限管控不當
  - /user/getAccount
  - /admin/getAccount


1000
Get my document which number is “1000” please!
Of course!
1001
Get the document which number is “1002” please!
Hey! Don’t mention it!
1002


中国联通 4G
18:05
49%
取消
确认支付
苹果X(iPhoneX) 深空灰 全网通64G ROM,苹...
¥22886.00
收款方
立即支付
支付安全由中国人民财产保险股份有限公司承保
change 22886 to 0.01
中国联通 4G
18:13
49%
取消
确认支付
苹果X(iPhoneX) 深空灰 全网通64G ROM,苹...
¥0.01
收款方
商城
支付
使用密码
¥0.01
零钱
确认支付
支付安全由中国人民财产保险股份有限公司承保


眼鏡
手錶
2015.09.16
中天快點TV
中時電子報 HD
最新
3D列印狼現蹤
簽約租屋 房仲報警
台中
知名駭客_張[redacted]元
中天新聞
改成負一 那1千減掉999元
cti 中天新聞

Injection

- **輸入被拼接到指令、查詢語句，導致非預期行為**
  - Command Injection
  - CRLF Injection
  - SQL Injection / NoSQL Injection
  - XPath Injection
  - Template Injection
  - ……

Command Injection

- 執行的系統指令部分可控


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

Command Injection

- 執行的系統指令部分可控


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

✓ 正常輸入: 8.8.8.8

Command Injection

- 執行的系統指令部分可控


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

✗ 不正常輸入: 8.8.8.8 ;ls -al

Command Injection

- 執行的系統指令部分可控


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

✗ 不正常輸入: 8.8.8.8 ;ls -al 任意執行指令！

常見玩法

- `ping 8.8.8.8 ; ls`
- `ping 8.8.8.8 | ls`
- `ping 8.8.8.8 && ls`
- `ping 8.8.8.8 $(sleep 5)`
- ping 8.8.8.8 `` `sleep 5` ``

Bypass Space

- `cat${ISF}/etc/passwd`
- `cat</etc/passwd`
- `{cat,/etc/passwd}`
- ....

Bypass Keyword

- String Concat
    - A=fl;B=ag; cat AB;
- Empty Variable
    - cat f${x}ag
- Environment Variable
    - $PATH => "/usr/local/..."
    - ${PATH:0:1} => '/'

Lab 0x02 - me0w 

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
Content-Length: 31\r\n
Connection: close\r\n
Location: http://kaibro.tw\r\n
\r\n
<html><body>Hello</body></html>
```

回憶一下 HTTP Response

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
Content-Length: 31\r\n
Connection: close\r\n
Location: [可控]\r\n
\r\n
<html><body>Hello</body></html>
```

如果某個 Response header 可控 . . .

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
Content-Length: 31\r\n
Connection: close\r\n
Location: a\r\n
Set-Cookie: JSESSIONID=kaibro\r\n
\r\n
<html><body>Hello</body></html>
```

寫入 a%0d%0aSet-Cookie: JSESSIONID=kaibro

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.
C
                                    \r\n
                                    \r\n
<html><body>Hello</body></html>
```

Session Fixation

寫入 a%0d%0aSet-Cookie: JSESSIONID=kaibro

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
Content-Length: 31\r\n
Connection: close\r\n
Location: a\r\n
\r\n
<script>alert(1)</script>\r\n\r\n
<html><body>Hello</body></html>
```

寫入 a%0d%0a%0d%0a<script>alert(1)</script>

CRLF Injection

```
HTTP/1.1 302 Moved Temporarily\r\n
Server: Apache/2.4.29 (Ubuntu)\r\n
Content-Length: 31\r\n
Connection: close\r\n
Location: a\r\n
\r\n
<script>alert(1)</script>\r\n\r\n
<html><body>Hello</body></html>
```

Header

Body

寫入 a%0d%0a%0d%0a<script>alert(1)</script>

CRLF Injection

```
HTTP/1.1 302 Moved Temporaril
Server: Apache/
C
                    /script>\r\n\r\n
<html><body>Hello</body></html>
```

XSS

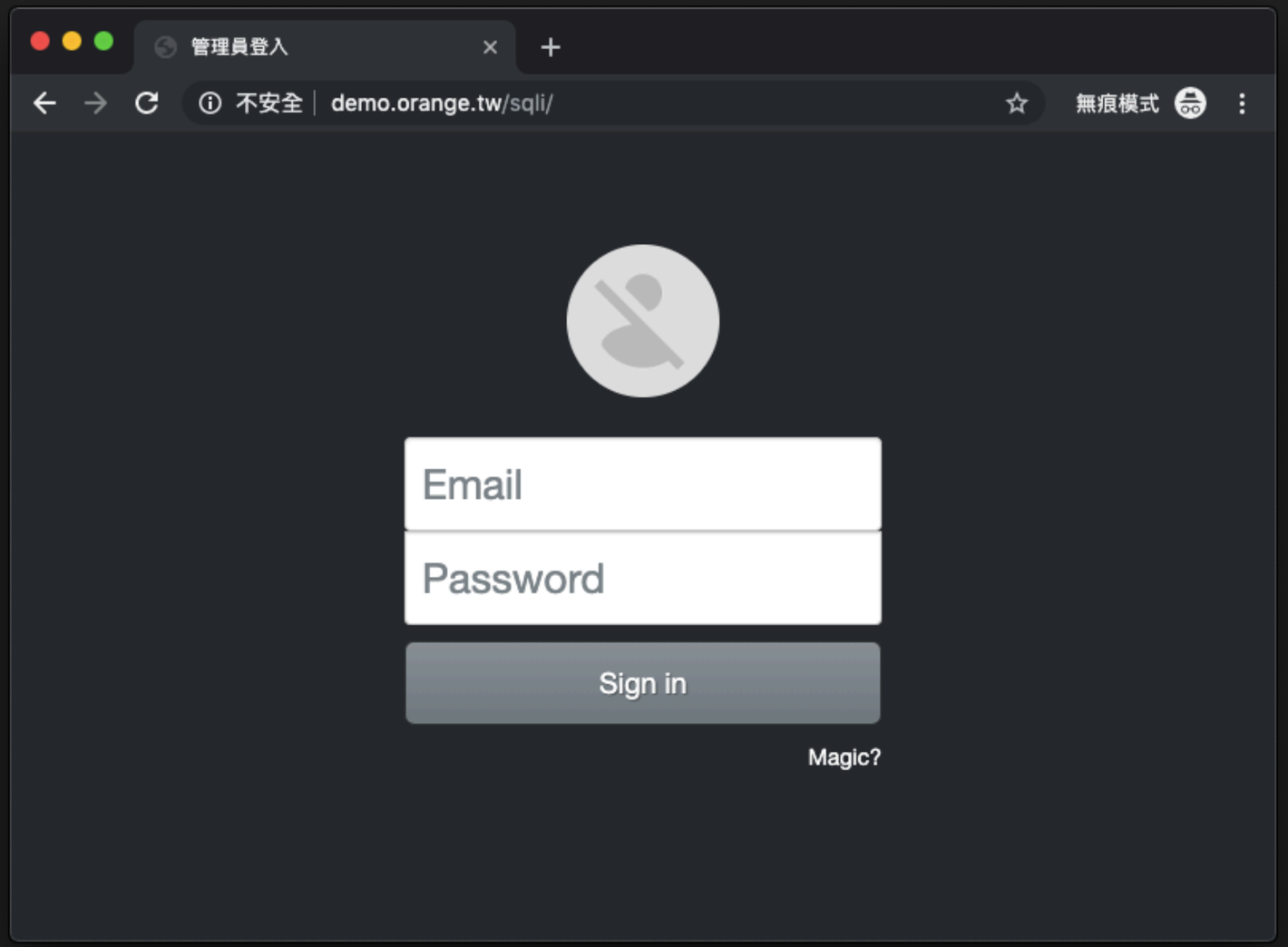
Body

寫入 a%0d%0a%0d%0a<script>alert(1)</script>

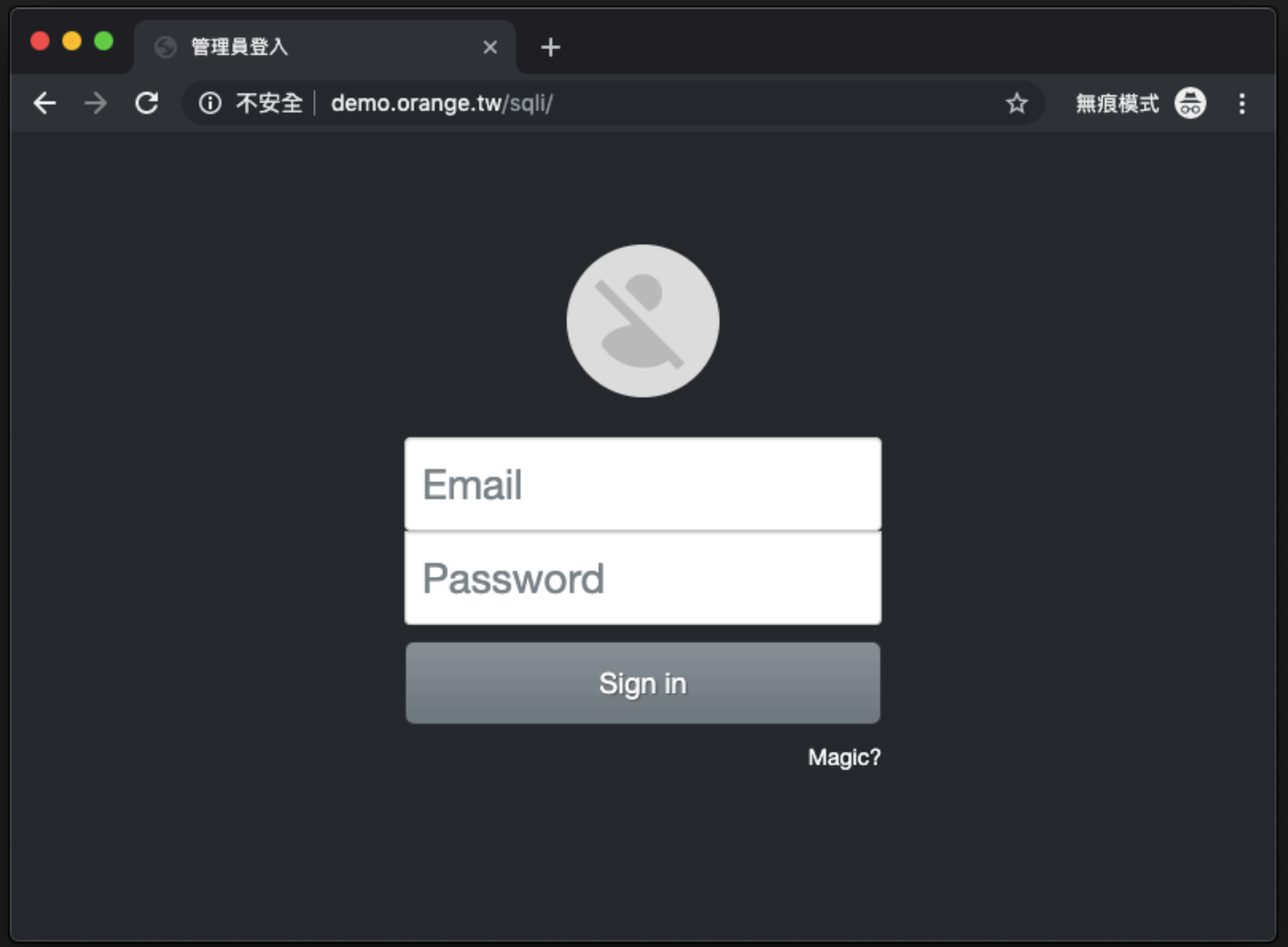
SQL Injection Basic

- Structured Query Language
- 存取、修改關連式資料庫 (realation dataase) 中的資料
  - e.g. MySQL, MSSQL, Oracle, PostgreSQL, . . .

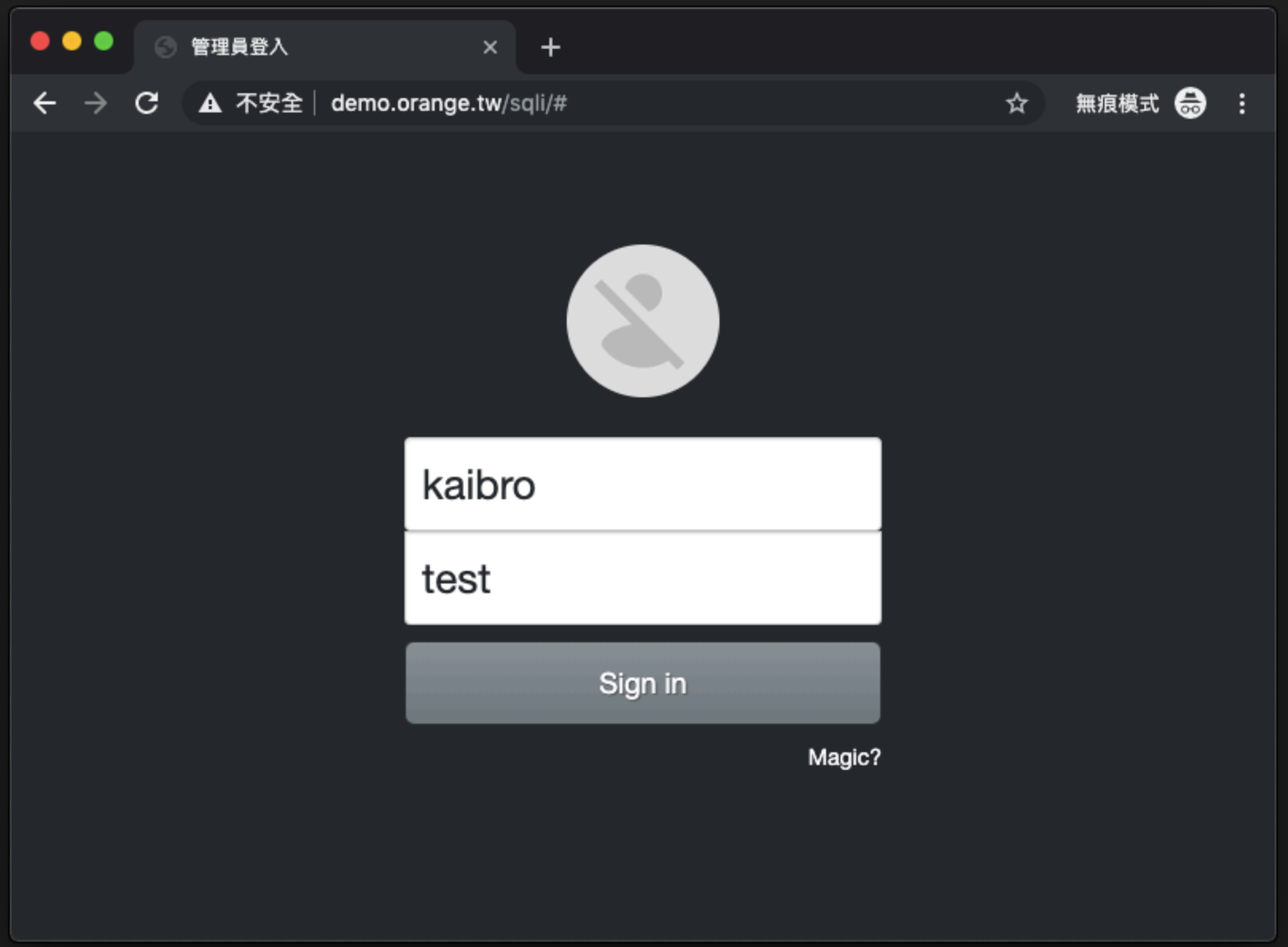

ZU 0666', 0, 0); DROP DATABASE TABLICE;


管理員登入
不安全 | demo.orange.tw/sqli/
無痕模式
Email
Password
Sign in
Magic?

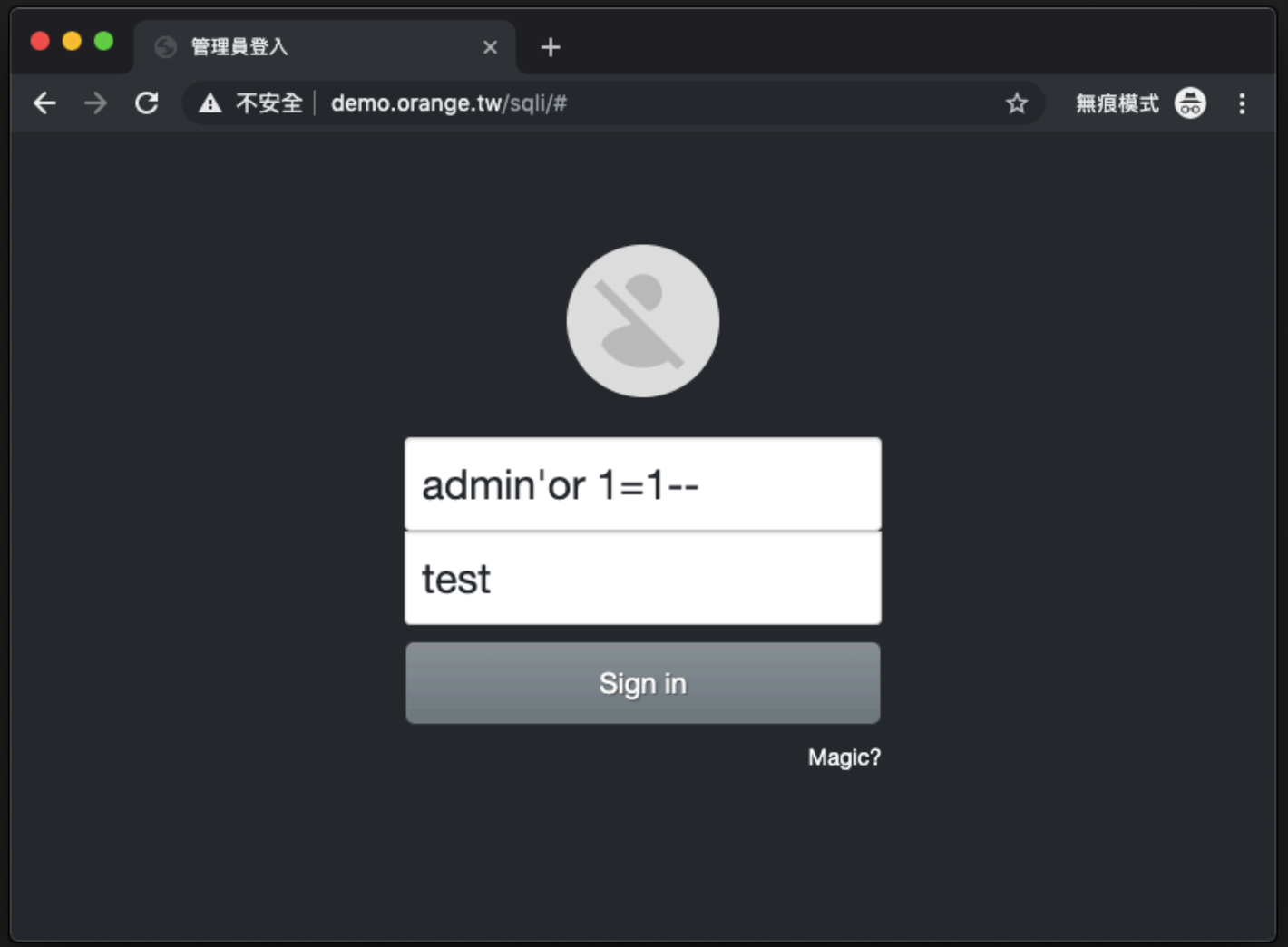
背後可能怎麼實作?



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



SELECT * FROM admin
WHERE username = 'kaibro' AND password = 'test'

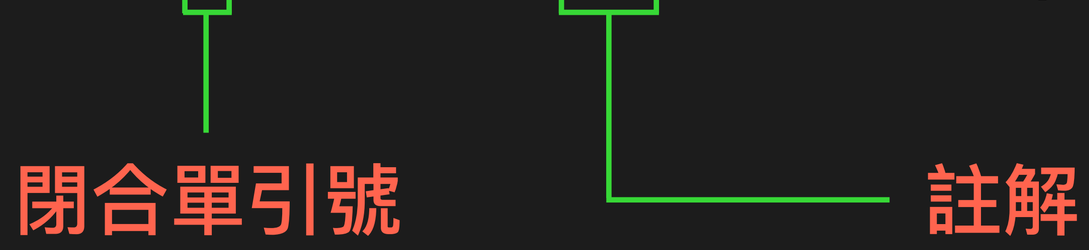


SELECT * FROM admin

WHERE username = 'admin'or 1=1-- ' AND password = 'test'


管理員登入
不安全 | demo.orange.tw/sqli/#
無痕模式
登入成功
歡迎你：)

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



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

Lab 0x03 - No Password

HW 0x01 - Unexploitable

HW 0x02 - Safe R/W

HW 0x03
預習SQL

Q & A