

資安宣導

CSRF (Cross Site Request Forgery) 跨站請求偽造	1
File Upload.....	4
SQL Injection	8
Brute Force (暴力破解).....	11
資安意識	23

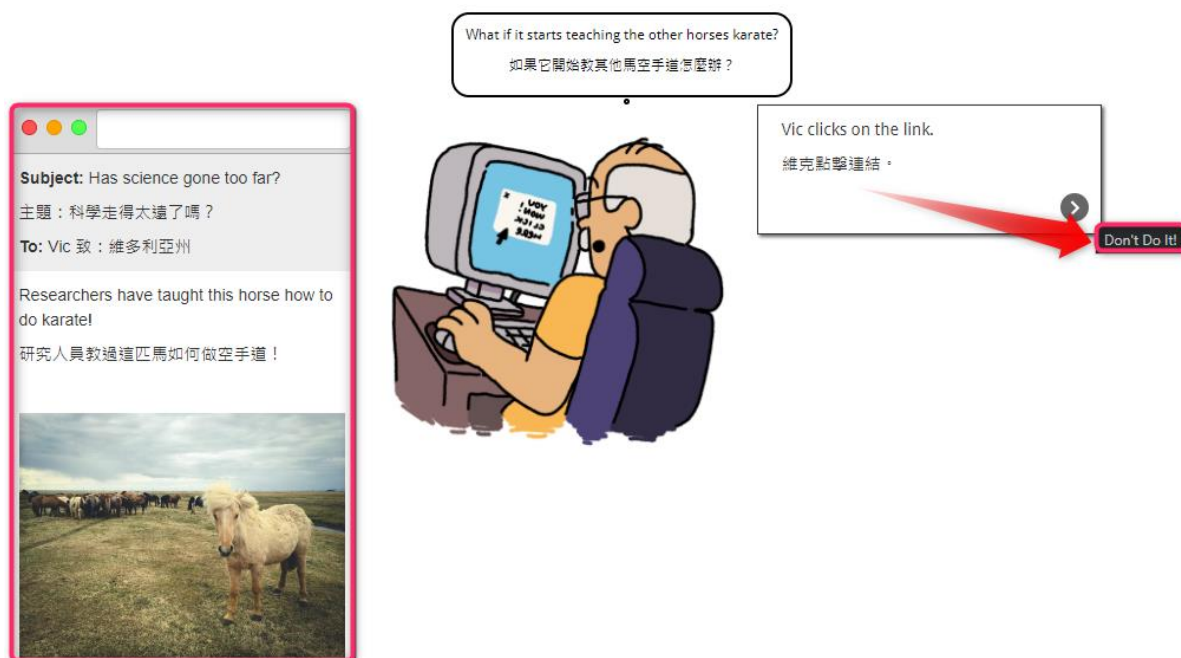
CSRF (Cross Site Request Forgery) 跨站請求偽造

CSRF：編制誤導使用者的連結，當點擊連結時會觸發 **GET** 請求，讓使用者對目標網站做出非預期的操作，主要是利用網站對使用者身分驗證不足的漏洞。

攻擊方法

攻擊者通常會在第三方網站上放置一個鏈接或圖片，其指向受害者要訪問的網站，當受害者點擊這個鏈接或圖片時，就會觸發攻擊

攻擊者可以利用這個漏洞，發送任意的 **HTTP** 請求，包括獲取敏感信息、修改用戶資料、發送郵件等等



我們來看看攻擊的範例，DVWA 是一個測試的網站。（DVWA（Damn Vulnerable Web Application）是一個用來進行弱點安全測試的網站系統，旨在為安全專業人員測試自己的專業技能和工具提供合法的環境，幫助 web 開發者更好的理解 web 應用安全防範的過程。）

在 Security Level 是 low 的情況下，是沒有任何防護的
這個頁面是修改密碼的頁面，在登入狀態下，使用者可以直接修改密碼，但是開發的人員是用 get 的方式來進行修改。

駭客攻擊方法

所以只要把想改的密碼設定好，變成縮短網址或是圖片影片連結誘騙使用者點開，密碼就被駭客修改了

 <https://blog.mitm.site/mod/resource/view.php?id=182>

medium 攻擊的範例，是開發人員發現了 CSRF 的漏洞之後，增加了 Referrer，若不是從網站密碼修改頁修改密碼的話，會被阻止

駭客攻擊方法

駭客透過攔截 Request 封包，加上 Referrer 欄位，還是可以攻擊成功

 <https://blog.mitm.site/mod/resource/view.php?id=183>

high 的程式，開發人員增加 user_token 的判斷，每次訪問頁面會得到一組參數值並驗證

駭客攻擊方法

利用 XSS 攻擊來取得使用者的 Token

將取到的 Token 搭配 CSRF

 <https://blog.mitm.site/mod/resource/view.php?id=184>

CSRF – Impossible

也就是防禦 CSRF 的方式

加入 Anti-CSRF token (<https://owasp.org/www-community/attacks/csrf>)

PHP 可以加入 PDO(PHP Data Objects) 防 SQL Injection

其它程式語言，可以參考(https://owasp.org/www-community/attacks/SQL_Injection)

改密碼前須要先輸入舊密碼，若不知道密碼就無法進行攻擊 遵守 REST 規範

GET：讀取資源

PUT：替換資源

DELETE：刪除資源

POST：新增資源

PATCH：更新資源部份內容

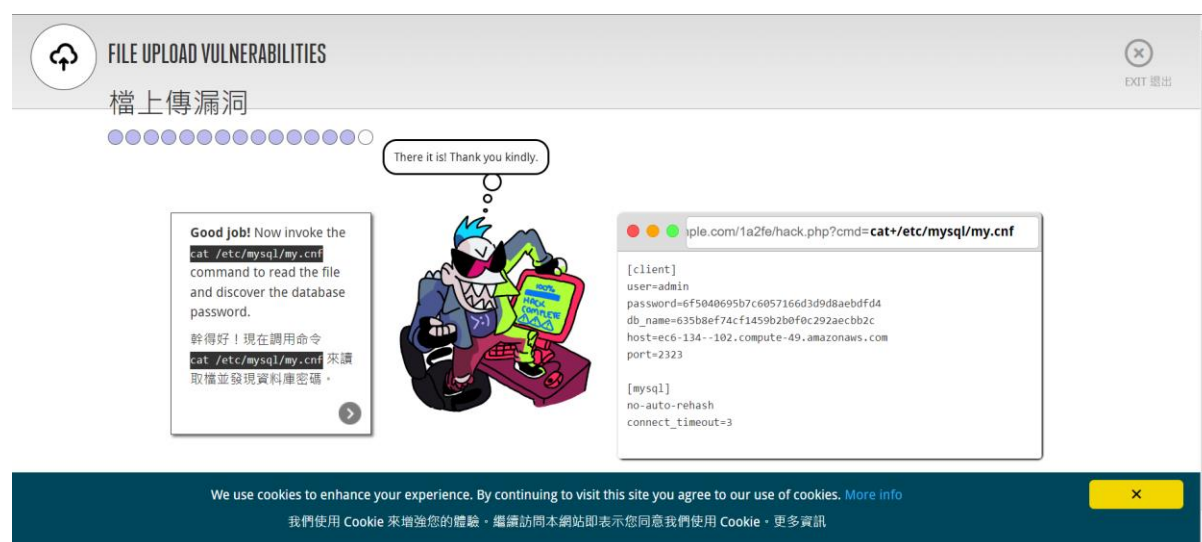
確保使用 SameSite Cookie 屬性發送 Cookie

在這個案例，若是增加圖型驗證碼或是原始密碼才能修改，也可以防止 CSRF

練習：<https://www.hacksplaining.com/exercises/csrf>

File Upload

OWASP Top 10 系列是網站開發時測試時最重要的安全基準，若是開發時沒有注意到就很有可能被駭，這次介紹的 **File Upload** 就是網站被駭客入侵的侵入點。



The screenshot shows a web application interface for 'FILE UPLOAD VULNERABILITIES'. At the top, there's a title bar with a cloud icon and an 'EXIT 退出' button. Below the title, a progress bar shows 10 steps, with the first 9 being blue and the 10th being white. A cartoon character with a speech bubble saying 'There it is! Thank you kindly.' is positioned in the center. To the left, a text box says: 'Good job! Now invoke the `cat /etc/mysql/my.cnf` command to read the file and discover the database password. 幹得好！現在調用命令 `cat /etc/mysql/my.cnf` 來讀取檔並發現資料庫密碼。'. To the right, a terminal window shows the command `cat /etc/mysql/my.cnf` being executed, resulting in the following output:

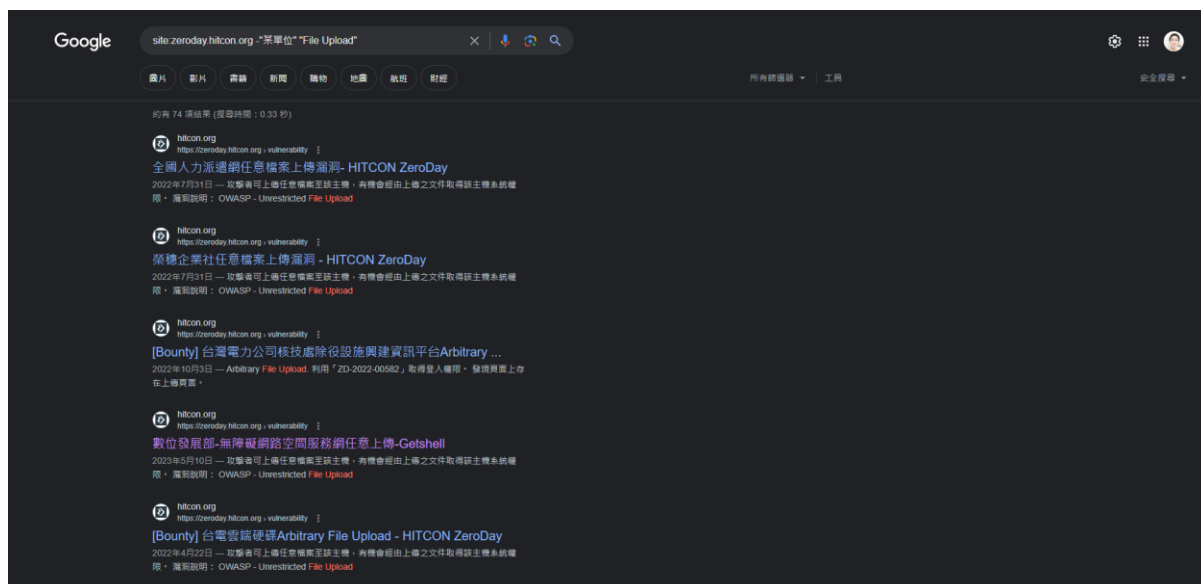
```
[client]
user=admin
password=6f9040695b7c6057166d3d9d8aebfd4
db_name=635b8ef74cf1459b2b0f0c292aebbb2c
host=ec6-134--102.compute-49.amazonaws.com
port=2323

[mysql]
no-auto-rehash
connect_timeout=3
```

File Upload 攻擊通常發生在開發人員對客戶文件上傳的控制不足或處理上有漏洞，導致用戶可以越過本身的權限，向伺服器上傳可執行的動態腳本，上傳的文件可以是木馬、病毒、惡意腳本或 **WebShell** 等，一句話木馬就可以屠城

google search keywords **site:zeroday.hitcon.org - "某單位" "File Upload"**

可以看到雖然是已知的開發弱點，仍然還是有許多開發人員在開發網站時忽略



Low 無判斷

Low 攻擊方法

嘗試可上傳檔案的類型，發現可以上傳 **php** 格式的檔案

建構一句話木馬直接上傳文件，並可以藉由此腳本在伺服器上執行系統指令



<https://blog.mitm.site/mod/resource/view.php?id=185>

Medium 加上判斷

限制上傳的檔案類型和大小

檔案類型必須是 **jpeg** 和 **png**

大小不能超過 **100 KB**

Medium 攻擊方法

上傳 **php** 檔後使用 **Burp Suite** 攔截封包，並修改

Content-Type 的值為 **image/jpeg**



<https://blog.mitm.site/mod/resource/view.php?id=186>

High 加上判斷

限制 **jpeg** 和 **png** 類型的檔案

使用 **getimagesize** 函式讀取圖片的 **header**、長寬等資訊，若發現格式不對就會報錯

High 攻擊方法

使用 **Exiftool** 修改圖片的資訊

將 **Comment** 參數改成 **php** 腳本



<https://blog.mitm.site/mod/resource/view.php?id=187>

Impossible

加入 **Anti-CSRF token**

將上傳的檔名使用 **md5** 編碼重新命名

使用 **imagecreatefromjpeg** 開啟文件，創建一個新圖像

防範方法：

1. 檢查檔案類型：限制上傳檔案的類型，例如只允許上傳圖片、影片、音樂等特定類型的檔案，避免上傳可執行檔或其他危險檔案。
2. 檢查檔案大小：限制上傳檔案的大小，避免攻擊者上傳大型檔案佔據系統資源。
3. 檢查檔案內容：使用防毒軟體檢查上傳的檔案是否包含惡意程式碼。

4. 檢查檔案名稱：避免使用者上傳具有攻擊性的檔案名稱，例如包含特殊字元或系統保留字的檔案名稱。
5. 檢查權限設定：限制使用者上傳檔案的權限，例如只允許管理員上傳檔案，避免普通使用者上傳危險檔案。
6. 更新軟體版本：定期更新網站上傳檔案功能的軟體版本，避免漏洞被攻擊者利用。

補充：

<https://www.hacksplaining.com/prevention/file-upload>

The screenshot displays the Hacksplaining website's 'PROTECTING YOUR FILE UPLOADS' guide. The page features a clean, modern design with a light gray background and a white central content area. The title 'PROTECTING YOUR FILE UPLOADS' is prominently displayed in bold, uppercase letters, followed by its Chinese translation '保護您的文件上傳'. Below the title, a paragraph explains that file uploads are a common attack vector for injecting malicious code and emphasizes the need for secure uploads. A section titled 'RISKS/風險' (Risks/Risks) follows, containing three orange boxes with icons and text: 'PREVALENCE: COMMON 常見患病率' (Prevalence: Common / 常見患病率) with a gear icon, 'EXPLOITABILITY: MODERATE 可利用性中等' (Exploitability: Moderate / 可利用性中等) with a wrench icon, and 'IMPACT: HARMFUL 衝擊有害' (Impact: Harmful / 衝擊有害) with a skull and crossbones icon. A concluding paragraph states that sophisticated hackers often exploit a combination of vulnerabilities, with uploading malicious code being the first step. At the bottom, a dark blue footer contains a cookie consent message in English and Chinese, with a 'More info' link and a close button.

HACKSPLAINING FEATURES LESSONS ENTERPRISE OWASP TOP 10 PCI COMPLIANCE THE BOOK LOGIN SIGNUP

PROTECTING YOUR FILE UPLOADS

保護您的文件上傳

File uploads represent an easy way for an attacker to inject malicious code into your application. You need to ensure uploaded files are kept at arm's length until they are fully secured, or else you risk creating an easy route to having your systems compromised.

檔上傳是攻擊者將惡意代碼注入應用程式的一種簡單方法。您需要確保上傳的檔案將與您保持距離，直到它們完全安全為止，否則您可能創建一條簡單的路徑來破壞您的系統。

RISKS/風險

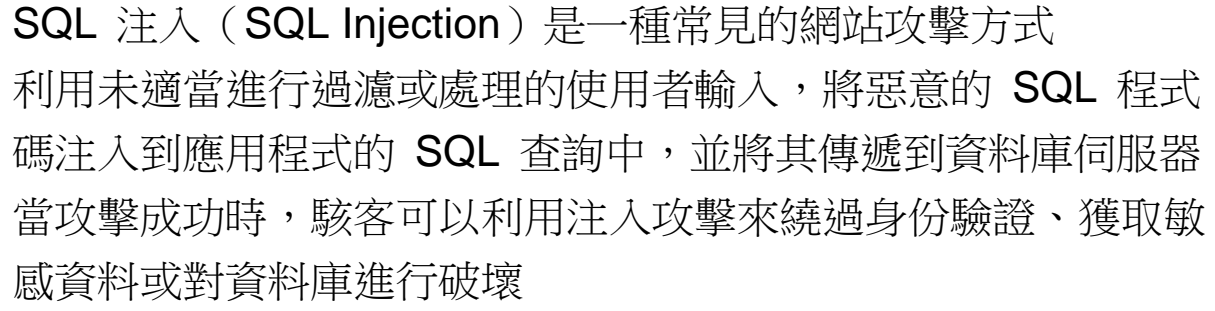
PREVALENCE: COMMON 常見患病率	EXPLOITABILITY: MODERATE 可利用性中等	IMPACT: HARMFUL 衝擊有害
--------------------------	---------------------------------	----------------------

Sophisticated hackers typically exploit a combination of vulnerabilities when attacking your site - uploading malicious code to a server is step one in the hacker playbook. The next step is finding a way to execute the malicious code.

進練的攻擊者在攻擊您的網站時通常會利用一系列漏洞——將惡意代碼上傳到伺服器是攻擊者手冊中的第一步，下一步是找到執行惡意代碼的方法。

We use cookies to enhance your experience. By continuing to visit this site you agree to our use of cookies. [More info](#)

我們使用 Cookie 來增強您的體驗。繼續訪問本網站即表示您同意我們使用 Cookie。更多資訊



正常情況

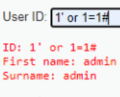
- 輸入 user id: 1
- 返回結果 user id 為 1 的使用者資訊

- The screenshot shows a web application interface with a login form and its output. The form has a label "User ID:" followed by a text input field and a "Submit" button. Below the form, the output is displayed in a monospaced font, showing the results of three different input attempts:

```
User ID:  Submit  
ID: 1  
First name: admin  
Surname: admin  
  
ID: 1' or 1=1#  
First name: Gordon  
Surname: Brown  
  
ID: 1' or 1=1#  
First name: Hack  
Surname: Me  
  
ID: 1' or 1=1#  
First name: Pablo  
Surname: Picasso  
  
ID: 1' or 1=1#  
First name: Bob  
Surname: Smith
```

- 輸入 user id: 1' or 1=1#
- 返回結果 繞過查詢機制，返回所有使用者的資訊

- 輸入 user id: 1' or 1=1#
- 返回結果 繞過查詢機制，返回所有使用者的資訊



User ID:

ID: 1' or 1=1#
First name: admin
Surname: admin

ID: 1' or 1=1#
First name: Gordon
Surname: Brown

ID: 1' or 1=1#
First name: Hack
Surname: Me

ID: 1' or 1=1#
First name: Pablo
Surname: Picasso

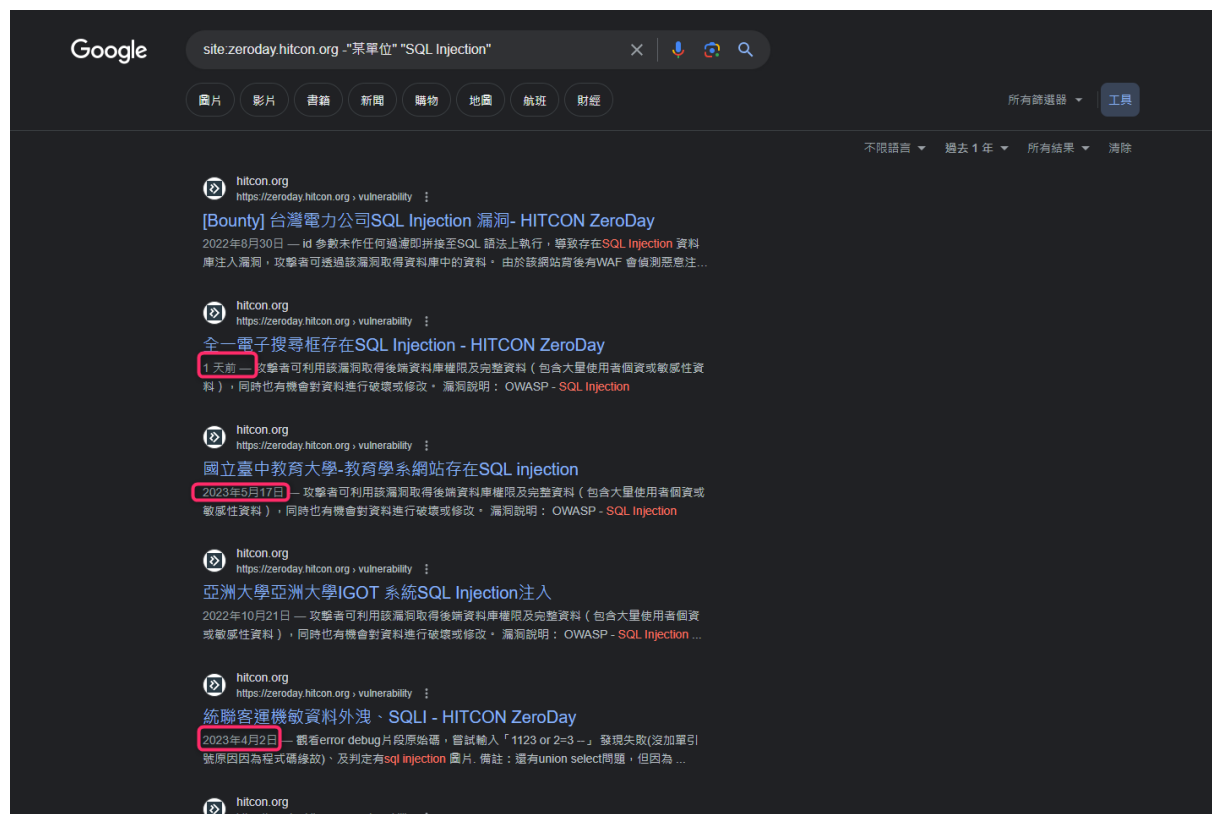
ID: 1' or 1=1#
First name: Bob
Surname: Smith

How to Attack?

- 攻擊者通常會透過網頁表單、URL 參數或供使用者輸入的任何地方輸入惡意的 SQL 程式碼



site:zeroday.hitcon.org -"某單位" "SQL Injection" 可以看到許多大型網站開發，仍然持續發生



真實案例

- 國立新營高工 SQL injection
- 用 guest 登入後退回登入畫面，帳號密碼皆利用 'or' a '=' a 以最高權限登入，可檢視、編輯所有使用者的帳號密碼

The screenshot shows a web application interface with a table of user accounts. The table has columns for time slots (15:00-16:00, 16:00-17:00, 17:00-18:00, 18:00-19:00) and user names. Below the table is a search bar with a dropdown menu for 'Search by' and a 'Search' button. The interface is in Chinese.

The screenshot shows a web application interface with a table of user accounts. The table has columns for user ID, username, password, and role. The user IDs range from 999 to 1. The usernames are mostly in Chinese. The passwords are mostly in English. The roles are mostly 'admin' or 'user'. The interface is in Chinese.

SQL Injection - Low 未進行防禦

傳送的參數沒有經過任何過濾和檢查直接進行 SQL 查詢

攻擊方式：直接輸入 SQL 語句注入

SQL Injection - Low 未進行防禦

傳送的參數沒有經過任何過濾和檢查直接進行 SQL 查詢

攻擊方式：直接輸入 SQL 語句注入

 <https://blog.mitm.site/mod/resource/view.php?id=188>

SQL Injection - Medium

使用 POST 方法傳遞參數

使用 `mysql_real_escape_string` 函式對特殊字元轉義

使用下拉式選單，因此攻擊方式改用 Burp Suite 攔截封包

 <https://blog.mitm.site/mod/resource/view.php?id=189>

SQL Injection - High

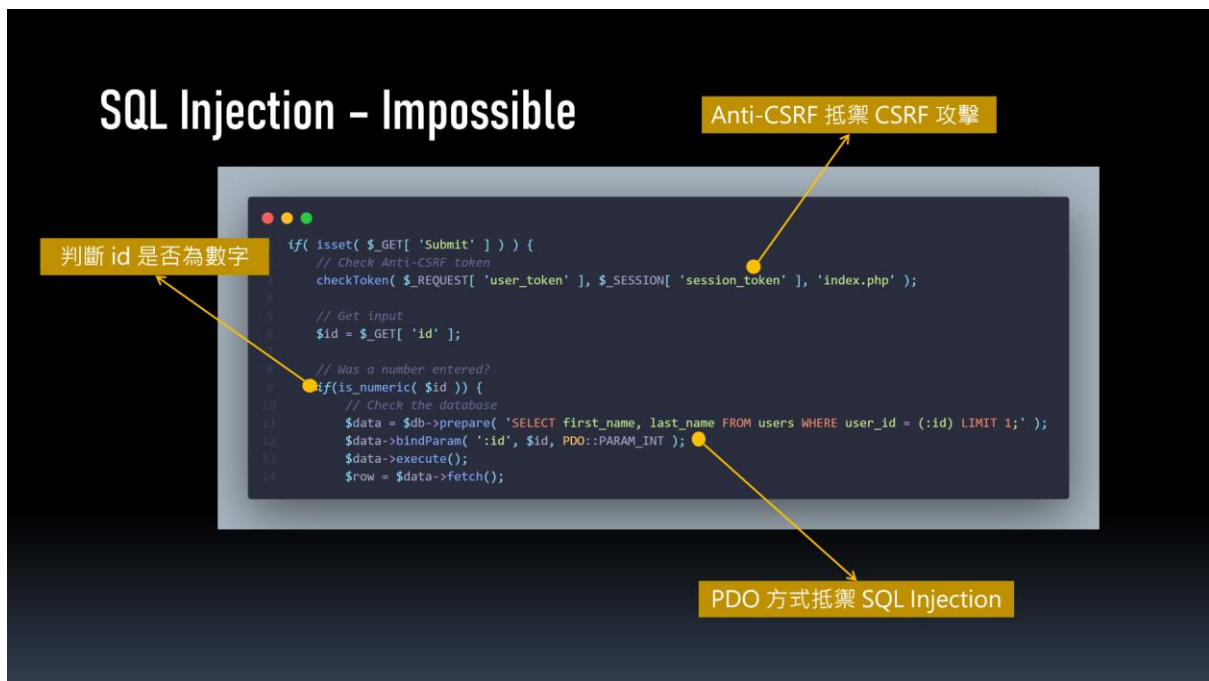
SQL 語句中增加 `Limit 1`

使用彈出視窗

攻擊方式與 Low 相同

SQL Injection - Impossible

SQL Injection – Impossible



如何防範

- 1.使用參數化查詢（**Prepared Statements**）或存儲過程，而不是直接將用戶輸入插入到 **SQL** 語句中。
- 2.進行嚴格的用戶輸入驗證和過濾，移除或轉義潛在的 **SQL** 關鍵字和特殊字符。
- 3.限制數據庫用戶的權限，僅提供應用程序所需的最小權限。
- 4.定期更新和修補應用程序和數據庫的漏洞，確保使用的是最新的安全補丁。
- 5.進行安全測試和代碼審查，以發現和修復應用程序中的漏洞。

<https://www.hacksplaining.com/prevention/sql-injection>

保護數位安全，共創無憂未來！

Brute Force (暴力破解)

Brute Force (暴力破解)：使用密碼字典，窮舉的方式破解

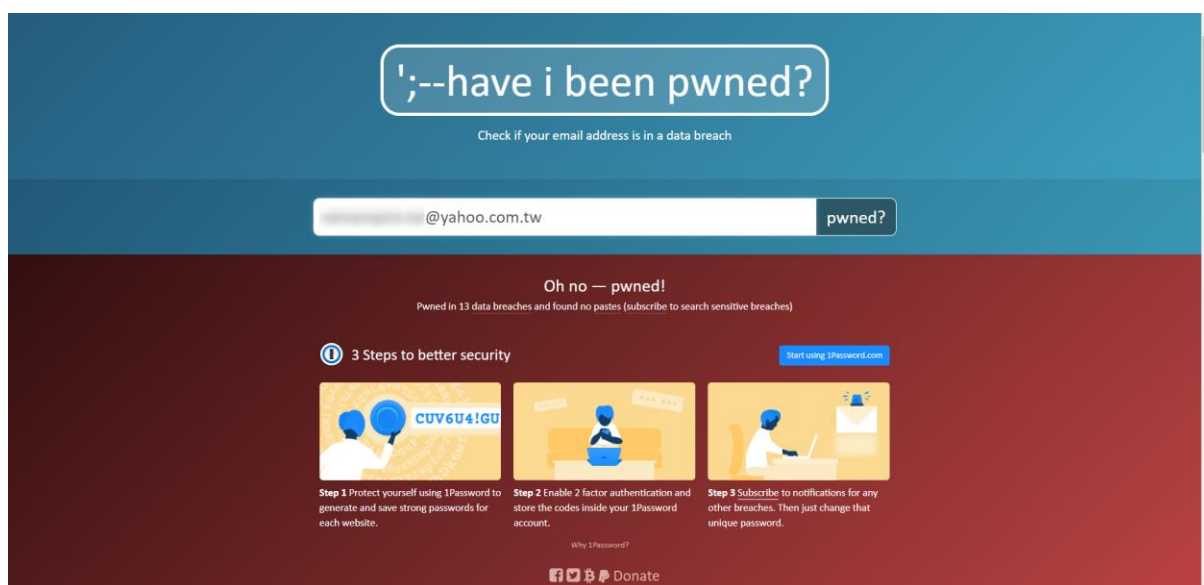
大家常常聽到字典攻擊，但是想到的是英文字典，但是攻擊用的字典，是常用的帳號名和密碼，也是駭客常常用來猜登入，最近常常聽到有人的 facebook 帳號被盜，可以參考

<https://www.facebook.com/help/1216349518398524>

，但是沒有點擊過任何連結或開啟郵件執行程式，就有可能是別的地方資料流出，

根據被盜的朋友反饋，用 facebook 的 email，都是在

<https://haveibeenpwned.com/> 出現 Oh no- pwned! 記得每個月一次檢查 email



Security Level : low

破解步驟

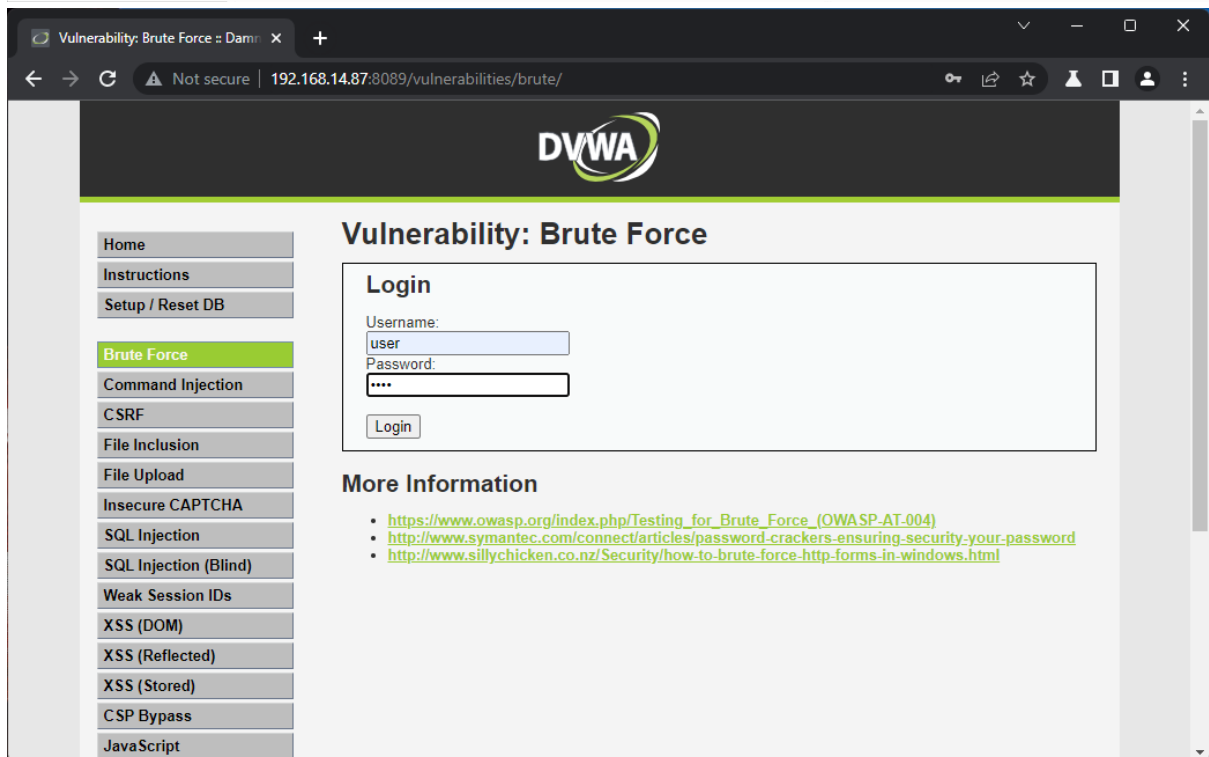
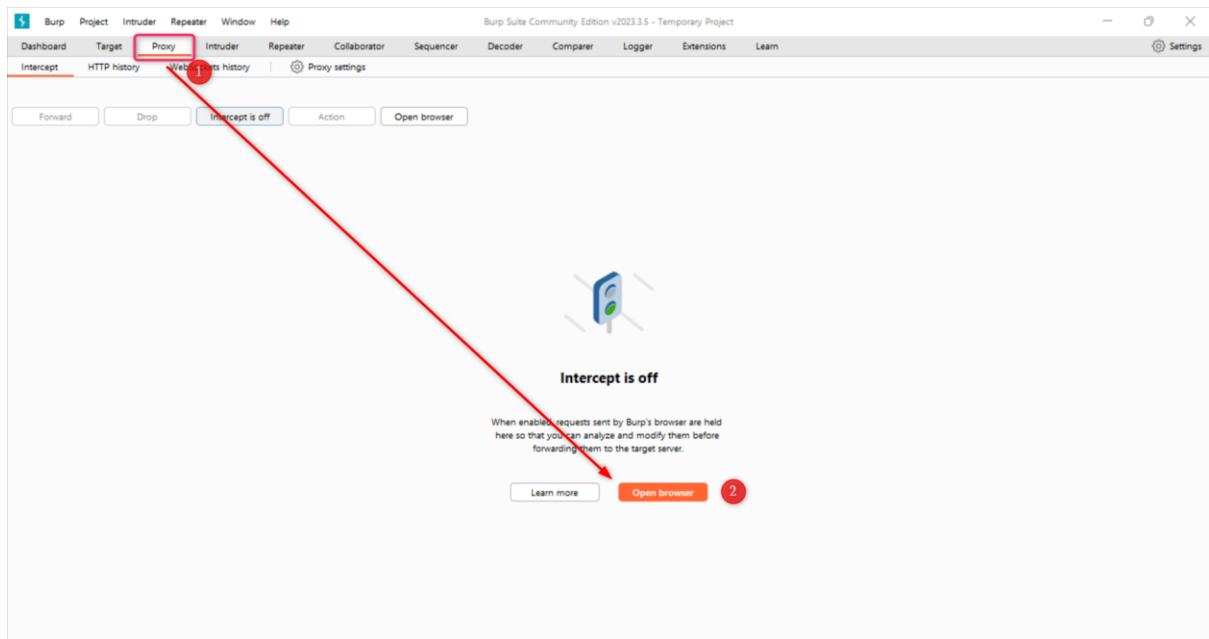
使用 Burp Suite 攔截 request

發送到 Intruder

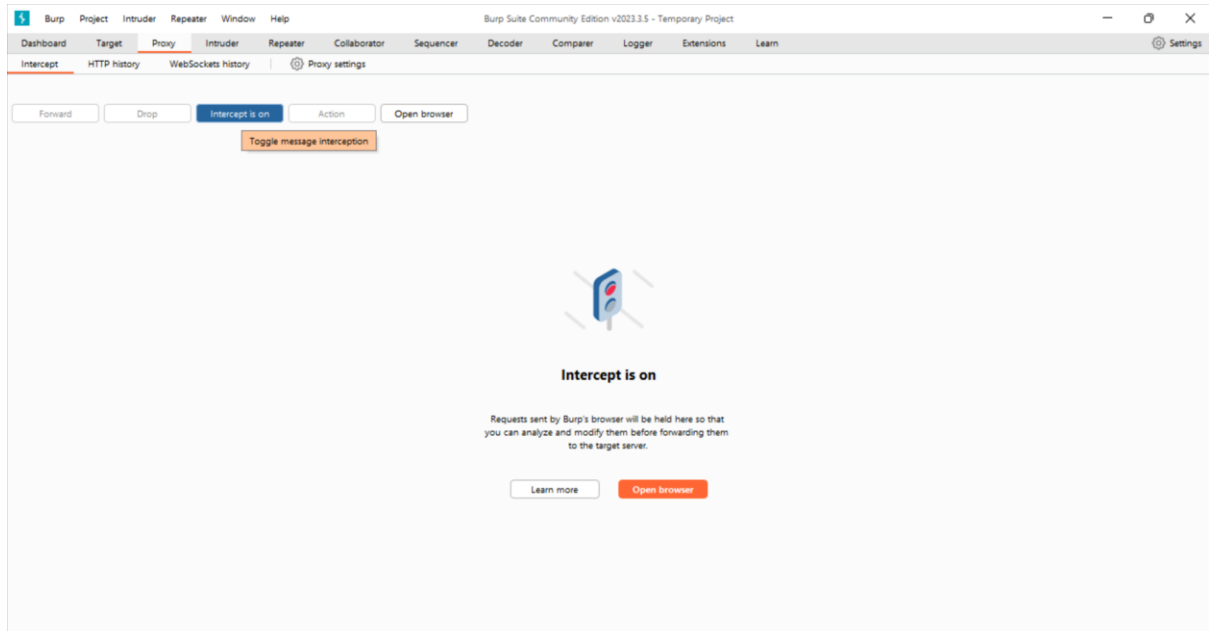
進行字典暴力攻擊

也可以使用 SQL Injection 攻擊，帳號輸入: admin 'or '1 = 1

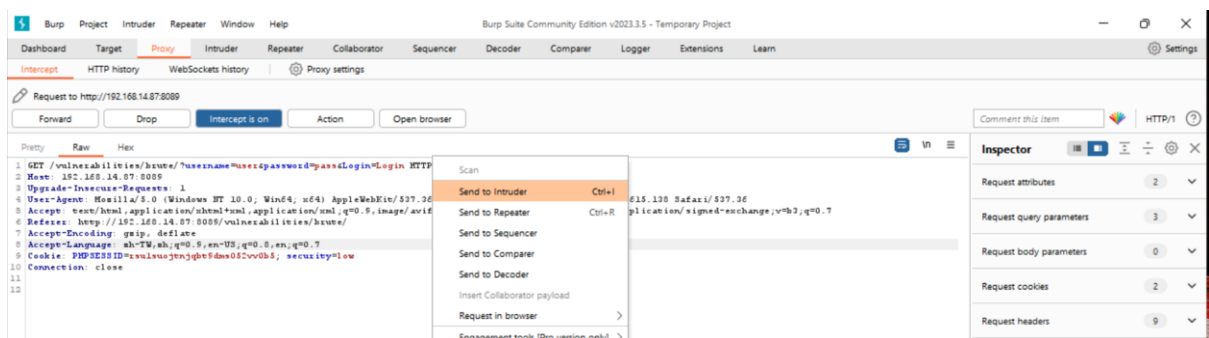
<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt>



登入 DVWA 調整 security level low 到 brute force 帳密亂打 送出前把 intercept is 改成 on

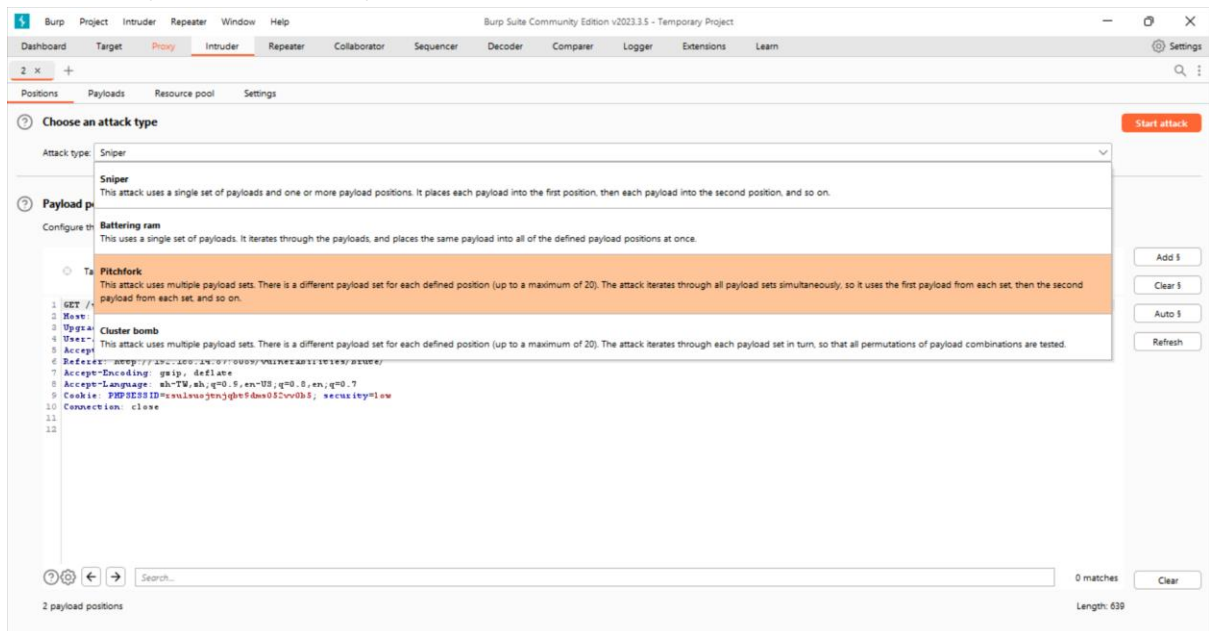


mouse right 或是 Ctrl+I 到 intruder

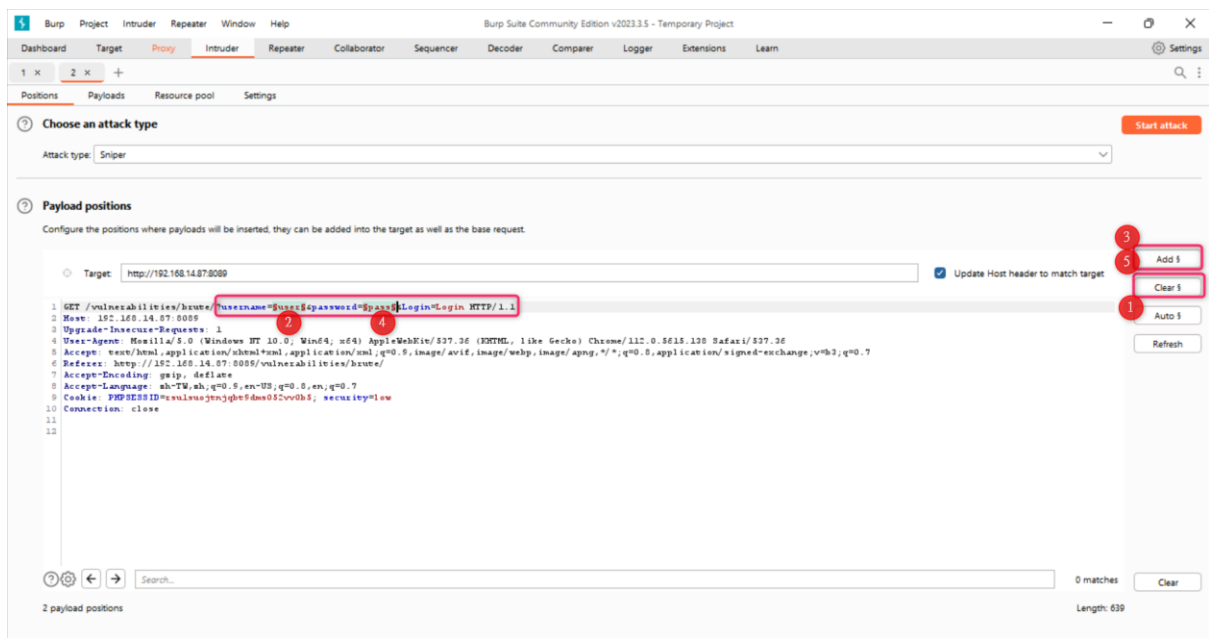


四種攻擊方式

<https://hackercat.org/burp-suite-tutorial/burp-suite-intruder-attack-type-and-payloads>



先 clear\$ all，payload 只選 username password Add\$



攻擊模式選 cluster bomb

測試資料

administrator

sysadmin

user

root

superuser

admin

123456

111111

000000

1qaz@WSX

toor

tiger

password





Payload sets

You can define one or more payload sets. The number of payload sets depends on the

Payload set: 1

Payload count: 6

Payload type: Simple list

Request count: 0



Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

administrator

sysadmin

user

root

superuser

admin

Positions

Payloads

Resource pool

Settings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the

Payload set:

2

▼

Payload count: 7

Payload type:

Simple list

▼

Request count: 42

?

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

123456

111111

000000

1qaz@WSX

toor

tigger

password

找回應結果長度不同的就有可能會是正確的

Attack Save Columns

2. Intruder attack of http://192.168.14.87:8089 - Temp

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
42	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4704	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
1	administrator	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
2	sysadmin	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
3	user	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
4	root	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
5	superuser	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
6	admin	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
7	administrator	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
8	sysadmin	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
9	user	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
10	root	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
11	superuser	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
12	admin	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
13	administrator	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
14	sysadmin	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
15	user	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
16	root	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
17	superuser	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
18	admin	000000	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
19	administrator	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
20	sysadmin	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
21	user	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
22	root	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
23	superuser	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
24	admin	1qaz@WSX	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
25	administrator	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
26	sysadmin	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
27	user	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
28	root	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
29	superuser	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	
30	admin	toor	200	<input type="checkbox"/>	<input type="checkbox"/>	4666	

Security Level : medium

增加字串特殊符號判斷

e.g. \n, \r, ' , "

防止了 SQL Injection 攻擊

增加 sleep(2) 函式，破解需花費較多時間

破解方法與 Low 相同

無法使用 SQL Injection 攻擊破解

```
// Login failed
sleep( 2 );
echo "<pre><br />Username and/or password incorrect.</pre>";
```

但是依然可以執行工具

Security Level : high

增加 user_token

驗證帳號密碼前，會先驗證 token，每次登入都需要提交 token

訪問頁面時，token 會自動生成

破解步驟

攔截 request，並發送到 Intruder

設定 password 和 user_token 為變量，攻擊類型為

Pitchfork，可使用多組 Payload 集合

取得 Response 中 user_token 的位置，每次攻擊會自動取 token 的值

設定 Payload : password 參數為密碼字典 (Simple list)，

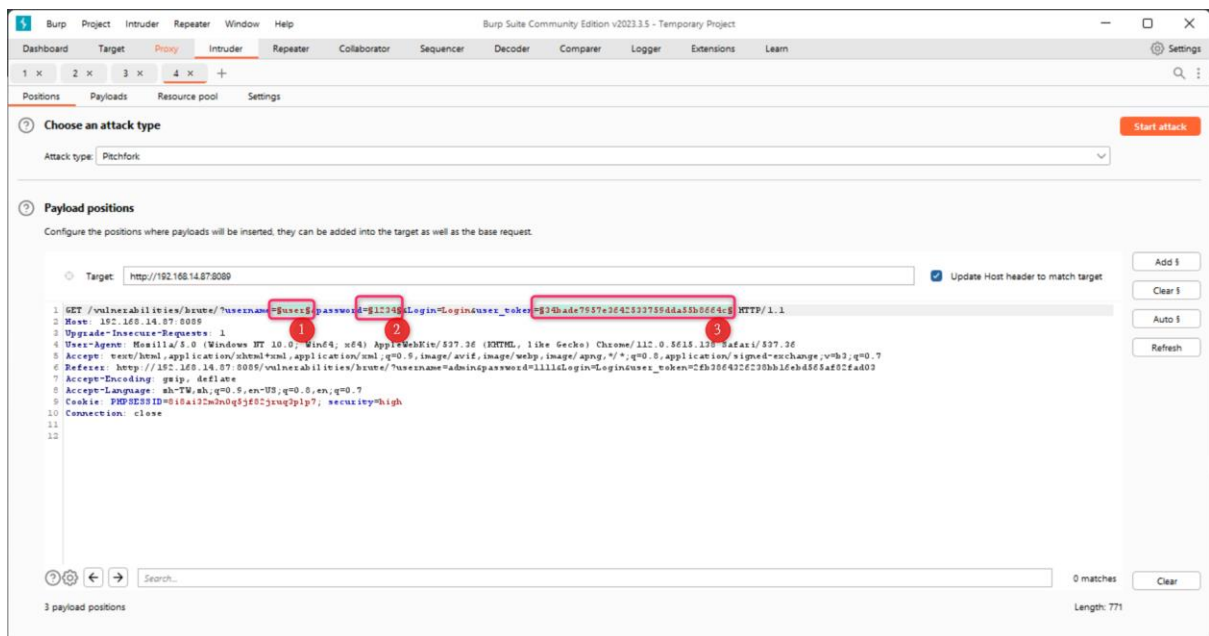
user_token 參數為自動取得的 token (Recursive)

Thread 設置成 1，開始攻擊

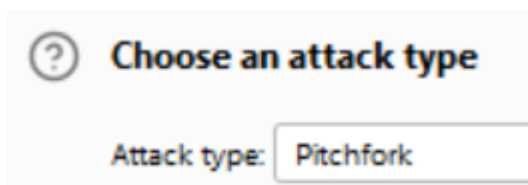
失敗時等候時間是 random，加上 anti-csrf

```
// Login failed  
sleep( rand( 0, 3 ) );
```

```
// Generate Anti-CSRF token  
generateSessionToken();
```



攻擊模式選 Pitchfork ，只有選擇 Pitchfork 和 cluster bomb 才可以針對不同的 payload 給不同的設定值



這個主要的防範是檢查 token，所以我們的 payload 設成三個，帳號、密碼和 token

token 要利用網頁產生的才會被接受，所以 payload set 3 的 payload type 設定 Recursive grep



Resource pool 的 maximum concurrent requests 要設成 1，否則會無法進行測試，防呆的設計，因為 token 是一對一，concurrent 會產生不同的 token 會對應不了，檢查不通過

Security Level : Impossible

對登入次數有限制，失敗 3 次將帳號鎖定 15 分鐘

DashboardTargetProxyIntruderRepeaterCollaborator

1 x2 x3 x4 x+

PositionsPayloadsResource poolSettings

☒ Create new resource pool

Name: Custom resource pool 1

☒ Maximum concurrent requests:1

☐ Delay between requests:

☒ Fixed

☐ With random variations

☐ Increase delay in increments of milliseconds

milliseconds

☒ Automatic backoff

The screenshot displays the Burp Suite Community Edition v2023.3.5 interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Extensions, and Learn. The 'Target' tab is active, showing a list of positions (1x, 2x, 3x, 4x, +) and a resource pool. The 'Settings' button is highlighted with a red circle 1. Below the resource pool, the 'Match type' is set to 'Simple string', and 'Exclude HTTP headers' is checked. The 'Grep - Extract' section is visible, with the text 'These settings can be used to extract useful information from responses into the' and a list of items to extract from responses. The 'Add' button is highlighted with a red circle 2. The 'Maximum capture length' is set to 100. The 'Define extract grep item' dialog is open, showing the 'Define start and end' section. The 'Start after expression' is set to 'value=' and the 'End at delimiter' is set to '>/\n'. The 'Extract from regex group' section is also visible, with the 'value=.*?>/\n' pattern and the 'Case sensitive' checkbox checked. The 'Refetch response' button is highlighted with a red circle 3. The dialog shows the selected item in the response panel, with the 'value=' and '>/\n' delimiters highlighted by red circles 4 and 5 respectively. The 'OK' button is highlighted with a red circle 6.

回到設定 payloads 的 tab，把剛剛複製的 token，貼到 initial payload for first request

② **Payload settings [Recursive grep]**

This payload type lets you extract each payload from the response to the previous request in the attack. It is useful in some situations where you need to work recursively to extract useful data or deliver an exploit. Extract grep items can be defined in the Options tab.

Select the "extract grep" item from which to derive payloads:

From [value=] to [/>\n\r\n09\r\n09</form>]

Initial payload for first request: Sf8aec0fdbbe824a0de438bdefa2e68c

☐ Stop if duplicate payload found

找出長度不同的就有可能是結果

The screenshot shows the Burp Suite interface. The top part displays the 'Results' tab for an 'Intruder attack of http://192.168.14.87:8089 - Temporary attack - Not saved to project file'. A table lists the results of the attack, with the last row highlighted in red:

Request	Payload 1	Payload 2	Status	Error	Redirect...	Timeout	Length	value=	Comment
0			200		1		4783	dc55345d38dec289e3...	
1	123456	fc637e3de4d89c5e9d0b3a22...	200		1		4783	d88763139c0552beec5...	
2	111111	cd8763139c0552beec5a705a...	200		0		4754	5d5f3ab45ca955dc1c...	
3	000000	5d5f3ab45ca955dc1ca7bd69...	200		0		4754	a2c388c499e98b4196e...	
4	1qaz@WSX	a2c388c499e98b4196e1e751...	200		0		4754	9c70b5281eb135fe11f8...	
5	toor	9c70b5281eb135fe11f806a7b6...	200		0		4754	5d53606641cfd79ecd...	
6	tgjher	5d53606641cfd79ecd8d105...	200		0		4754	8f6ea618973503dc650f...	
7	password	8f6ea618973503dc650fcd0c...	200		0		4792	f0837128af22c504baef...	

The bottom part shows the 'Response' tab, which is rendered. It displays a login form with a 'PASSWORD:' field and a 'Login' button. Below the form, it says 'Welcome to the password protected area admin' and shows a small image of a person. A 'More Information' section at the bottom provides a link to a security resource: [https://www.owasp.org/index.php/Testing_for_Brute_Force_\(OWASP_AT_004\)](https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP_AT_004)).

用 python 程式測試的方式，可以參考

<https://stackzero.net/brute-force-dvwa-python/>

資安意識

第一次登入電腦系統，

請務必變更預設密碼。

請務必變更預設密碼。

請務必變更預設密碼。

登入電腦：網域帳號：英文名字.英文姓氏 (Ex：gary.tsai)

網域密碼：“新人報到單上”

※輸入錯誤 3 次 帳號將會鎖定

變更密碼：

1. 登入電腦後按下 **Ctrl + Alt + Del**，選擇“變更密碼”

2. 輸入原密碼

3. 輸入新密碼 (須遵守密碼原則)

密碼原則：

(1)英文大小寫 (A-Z / a-z)

(2)數字 (0-9)

(3)特殊符號 (Ex：!, @, #, \$, %)

(4)至少 12 碼

(5)勿與帳號相似 (Ex: 帳號為 gary.tsai，新密碼設定 Gary@1234)

公司公告

請閱讀所有資訊安全宣導

請閱讀所有資訊安全宣導

請閱讀所有資訊安全宣導

公司公告			hide...
日期	主題	觀看人數	
2023-09-12	20230912【資訊安全宣導】	38 / 40	
2023-08-08	20230808【資訊安全宣導】	38 / 40	
2023-07-17	20230717【資訊安全宣導】	37 / 40	
2023-06-08	20230608【資訊安全宣導】	37 / 40	
2023-05-08	20230508【資訊安全宣導】	38 / 40	
2023-04-10	20230410【資訊安全宣導】	38 / 40	
2023-03-13	20230313【資訊安全宣導】	38 / 40	
2023-02-07	20230207【資訊安全宣導】	38 / 40	
2023-01-19	20230119【資訊安全宣導】	38 / 40	
2023-01-12	2023/1/12晚宴安全宣導	38 / 40	

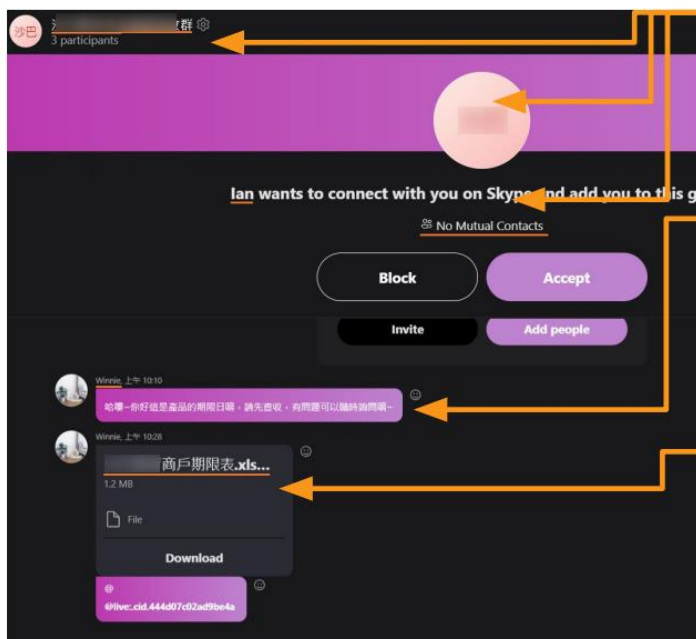
資安事件 案例分享

認識冒名詐騙



衍伸事件—Skype 惡意檔案

透過Skype顯示名稱、大頭貼騙取目標信任，再傳送惡意檔案。



識別訊息的真實性

- * 偽裝熟悉的群組名稱，常與職務 內容相關
- * 發起訊息群組的是誰？
- * 為何沒有共同聯絡人？

訊息內容

- * 訊息內容可能與職務內容有關，有時則會是時事新聞等題材，目的就是為了讓你降低戒心。
- * 傳送的檔案通常都是含有惡意程式的常見文件，如：Word, Excel, PDF...等。

巧妙偽裝的惡意文件

- * 檔案名稱長度經過設計，讓 Skype 僅顯示了部分檔名，實際為：[redacted] 商戶期限.xls D.com的巨集型惡意文件。

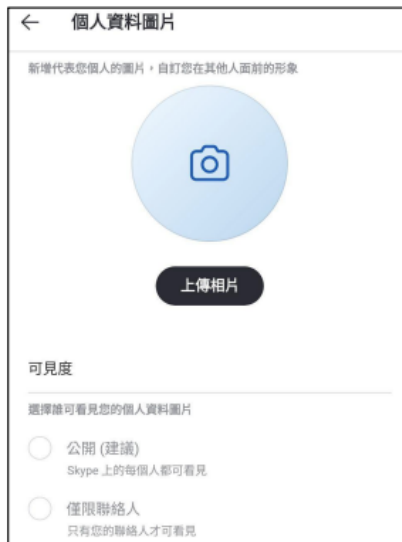
- 強化 Skype 帳號的安全性設定

強化 Skype 帳號的安全性設定

1. Skype → 設定 → 聯絡人 → 隱私權 → 關閉 "出現在搜尋結果中"



2. Skype → 設定 → 帳戶與個人資料 → 個人資料圖片 → 勾選"僅限聯絡人"

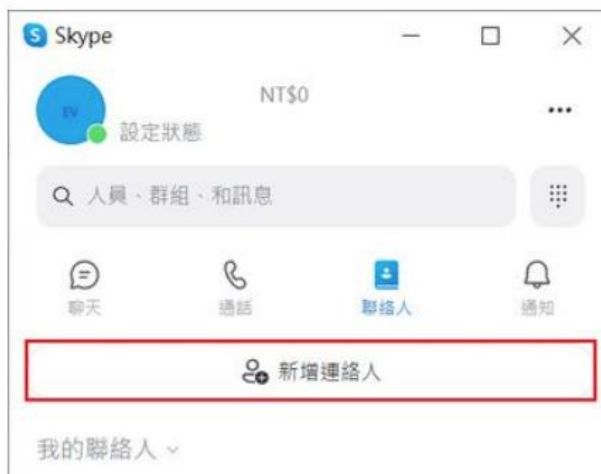


● 三種安全的方式新增 Skype 聯絡人

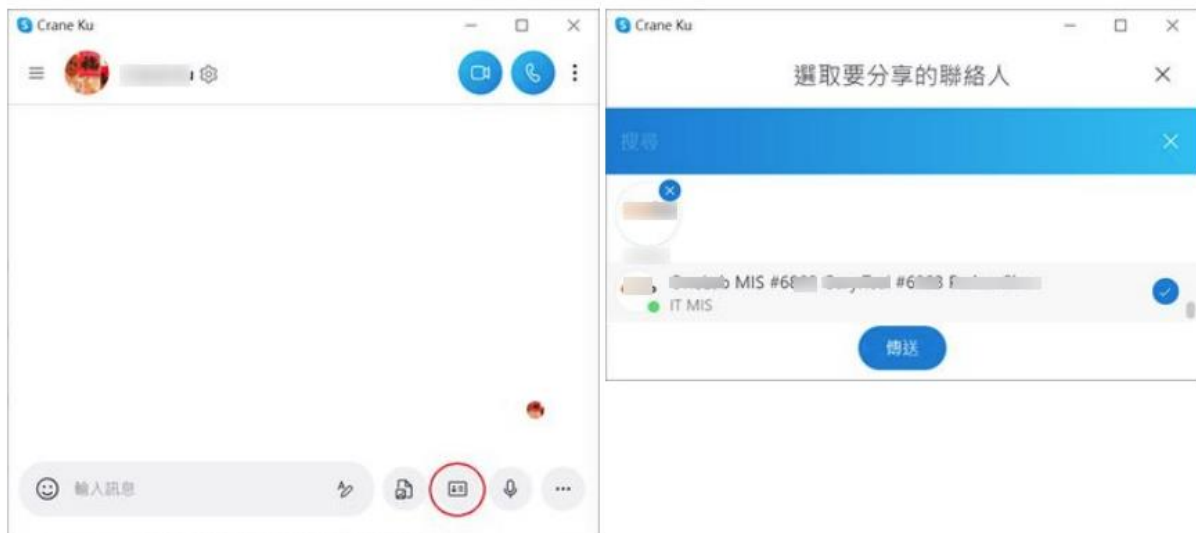
請勿使用搜尋方式新增聯絡人，請同仁使用下列三種方式進行“安全的新增聯絡人”：

1. 透過第二管道交換：Skype 產生的連結或 QRCode，以 EMail/Letstalk...交換。

Skype → 設定 → 聯絡人 → 新增聯絡人 → 邀請對方使用 Skype，手機版更有 QRCode 方式。



2. 透過中間人交換：透過共同聯絡人，協助傳送你或對方的聯絡人名片。 Skype → 聊天 → 聯絡人 → 將聯絡人傳送到此聊天 → 透過聯絡人名片添加好友。



3. 從既有公司群組中尋找聯絡人：透過有許多公司同仁的大群中新增。 Skype → 聊天 → 群組 → 群組設定(群組名稱後的齒輪) → 透過群組內的聯絡人名片添加好友。

