Injection 們的簡介

SQL和cmd

Database 基礎架構

- 最大的是database

Database 中包含table(表)

table(表)中有column(欄位)

SQL (structed query language)

- 有很多種 MySQL MSDB 巴拉巴拉
- 語法幾乎就是自然語言
- 寫不好你的DB(Database)就完蛋了 會被打爆
- 總之很重要
- HOHOHOHO

SQL基本語法

Select * from table name where column name = ‘column name’ 反正就是英文

分號; 是一行的結束

然後--或#

兩個減號或井號是單行註解(很好用

/* */是全部註解

壞掉的SQL寫法

- var sql = "select * from users where username = '" + username + "‘

  and password = '" + password + "’’’;

上述例子的SQL是用組合的方式構成的, 但是這樣就出了一些問題

就是呢 如果username 輸入的是 ‘; drop table users -- 這個時候 users這個table(表單)就被惡意刪除了

然後如果是輸入 admin‘ – 诶 這樣你就變成admin登入了

或者輸入了‘ or 1=1– 你就會是以第一個帳號登入

所以呢 通常會用黑名單的方式過濾特殊字元 (白名單就很麻煩了

但是就是有方法可以繞過去

範例題

- https://hackme.inndy.tw/login0/

好用的tool

- SQLmap

SQLmap 實作

- CTFlearn :injection time

CMDi (command injection)

- 在了解CMDi之前先了解CMD指令和LINUX系統