# Tutorial Blind SQL Injection by SkillmaX

Tenemos la web ahora agregamos el valor "1=1" después del numero:
**?idnot=25 and 1=1**

De momento no estamos agregando un valor FALSE por que el 1=1 es un valor TRUE por entonces la web no debe de mostrar ningún cambio y debe de salir igual que al principio.

Ahora probaremos si la web es vulnerable, por que le agregaremos un valor FALSE
La web se quedaría así:
**?idnot=25 and 1=2**

Si al pulsarle intro la web se sigue cargando igual significa que acepta el valor FALSE por lo tanto la web es vulnerable.

Ahora después de saber si la web es vulnerable añadiéndole "1=2" deberemos de saber su versión de Mysql, debemos de saber que hay dos tipos de versiones la versión MYSQL "4" y la versión MYSQL "5"

Pondríamos esto:
**?idnot=25 and substring(@@version,1,1)=4**

Para la versión "4"
Si la web se sigue mostrando igual nos quedamos hay, por que sabemos que es esa la versión MYSQL.

Y si nos da algun error o texto o algo raro, cambiamos el numero "4" por el "5" para probar la versión "5"

Ahora como si fuera SQL injection deberemos de averiguar las tablas que hay:
**?idnot=25 and (select+1+from+admin+limit+0,1)=1**

Ahora si la tabla admin funciona, es que es TRUE entonces nos quedaremos hay estancados.
Ahora probaremos un nombre de una columna a ver si existe, si existe somos dioses:
**?idnot=25 and (select substring(concat(1,password),1,1)**

Si la columna password no existe nos dará un error, y debemos probar con otra. Como contraseña, pass, etc..
Bueno, ya luego tocaría extraer los datos de los usuarios y pass, pero como ya sabéis extraer los datos por que sabéis SQL, no hace falta explicarlo, y hasta aquí todo.

Espero que os haya gustado a todos.

By SkillmaX
Fuente: Indetectables.net