# Trabajo de inyección ciega de SQL

## Descripción

Poner en marcha WebGoat, e ir al subapartado "Blind String SQL Injection" dentro del apartado "Injection Flaws". En este subapartado, intentamos obtener el nombre del propietario de una cuenta inyectando una cadena SQL de forma ciega. De esta forma, en lugar de '101' (El código pedido), inyectamos lo siguiente:

'101 AND (SUBSTRING(SELECT name FROM pins WHERE cc_number='4321432143214321'),1,1) < 'H');'

Y así, letra a letra, extraemos el nombre (name) asociado a la cuenta dada (cc_number='4321…') en la tabla dada (pins).

Se pide hacer lo mismo con los siguientes datos:

| **Alumno** | **name** | **pins** | **cc_number='4321432143214321'** |
|---|---|---|---|
| Arnau Navarro, Maria | password | user_system_data | userid='101' |
| Arzola Pérez, José David | password | user_system_data | userid='102' |
| Baron Rubio, Alba | password | user_system_data | userid='103' |
| Capdevila Fabregat, Jose Vicente | password | user_system_data | userid='104' |
| Flores Figueredo, Alberto Daniel | password | user_system_data | userid='105' |
| Grau López, David | user_name | user_system_data | userid='101' |
| Jimenez Muñoz, Maria Jose | user_name | user_system_data | userid='102' |
| Perez Mullor, Alex | user_name | user_system_data | userid='103' |
| Pla Climent, Josep | user_name | user_system_data | userid='104' |
| Torres García, Yailén | user_name | user_system_data | userid='105' |
| Zhuo, Runchen | password | user_system_data | user_name='dave' |

De esta forma, cada uno de vosotros entregará un archivo txt con la secuencia de inyecciones SQL necesaria para extraer el password o el user_name (según corresponda en la tabla anterior), los resultados de cada una, y un breve texto explicando cómo se decide cada nueva inyección sql a partir del resultado de la anterior.

Obviamente, añadir al final cuál es el password o user_name obtenido, y explicar cómo habéis detectado el final de palabra (es decir, cómo estáis seguros de que la última letra de la palabra obtenida es de verdad la última).

## Forma de entrega

Tanto el apartado 1 como el apartado 2 se realizarán en un archivo de texto que se entregará en una tarea de aulavirtual puesta al efecto. Debe ser todo texto plano, pues yo copiaré y pegaré vuestras trazas para comprobar que funcionan, y el fragmento de código que propongáis, lo copiaré en el lugar correspondiente para compilarlo y probarlo.