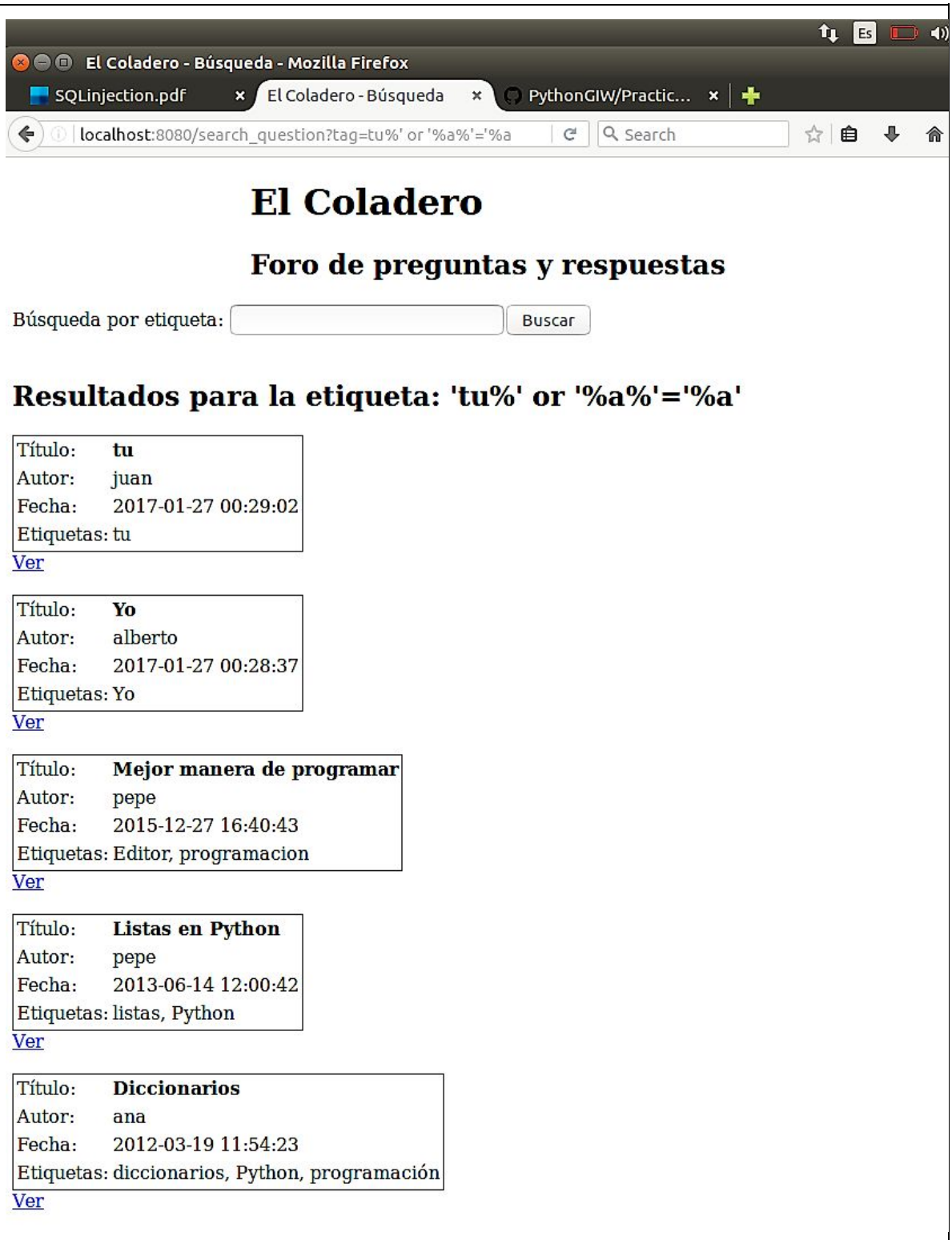
Autores:
Alberto Marquez
Álvaro Asenjo
Juan Jose Montiel
Declaramos que esta solución es fruto exclusivamente de nuestro trabajo personal. No hemos sido ayudados por ninguna otra persona ni hemos obtenido la solución de fuentes externas, y tampoco hemos compartido nuestra solución con nadie. Declaramos además que no hemos realizado de manera desho-nesta ninguna otra actividad que pueda mejorar nuestros resultados ni perjudicar los resultados de los demás.

INFORME DE VULNERABILIDAD
Tipo de vulnerabilidad
Vulnerabilidad SQL Injection
Situaciones peligrosas o no deseadas que puede provocar
Se realizan consultas sin control y estas puede llegar a dañar la base de datos o acceder a datos no deseados.
Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)
En el siguiente ejemplo hemos ampliado la cabecera de la url para acceder a todos los valores de la búsqueda, sin que la pagina lo permitiese. Insertando a continuación de la url: /search_question?tag=tu% or ‘%a%’=’%a El resultado es este:



Medidas para mitigar la vulnerabilidad

hay que revisar todas las entradas para que no sea posible insertar código malicioso y asegurarnos de que el código que creamos está bien protegido ante estos ataques, ya que cualquier entrada es susceptible de sufrir un SQL Injection.

INFORME DE VULNERABILIDAD

Tipo de vulnerabilidad

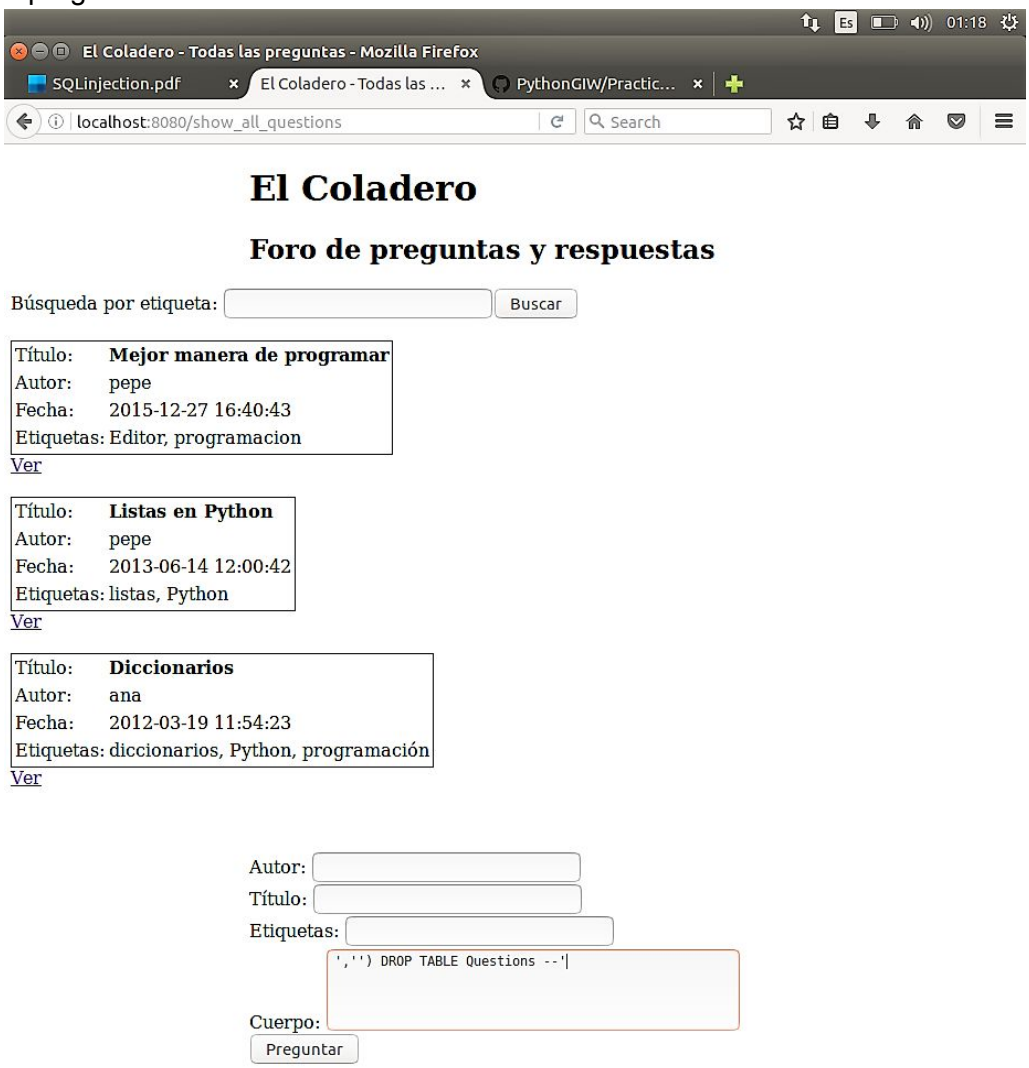
Vulnerabilidad SQL Injection.

Situaciones peligrosas o no deseadas que puede provocar

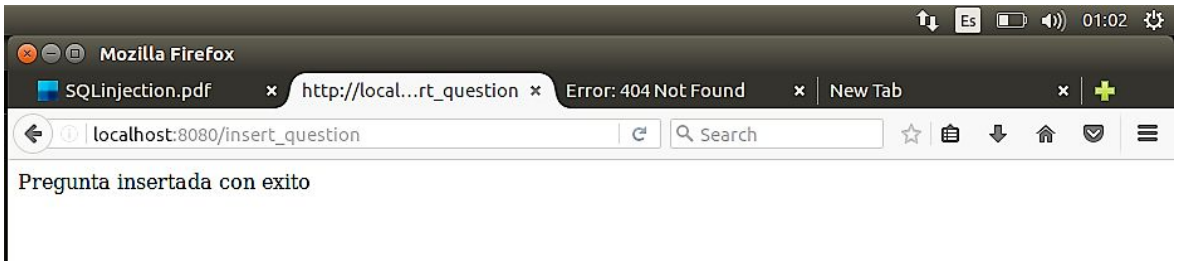
Se realizan consultas sin control y estas puede llegar a dañar la base de datos como en el ejemplo siguiente.

Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)

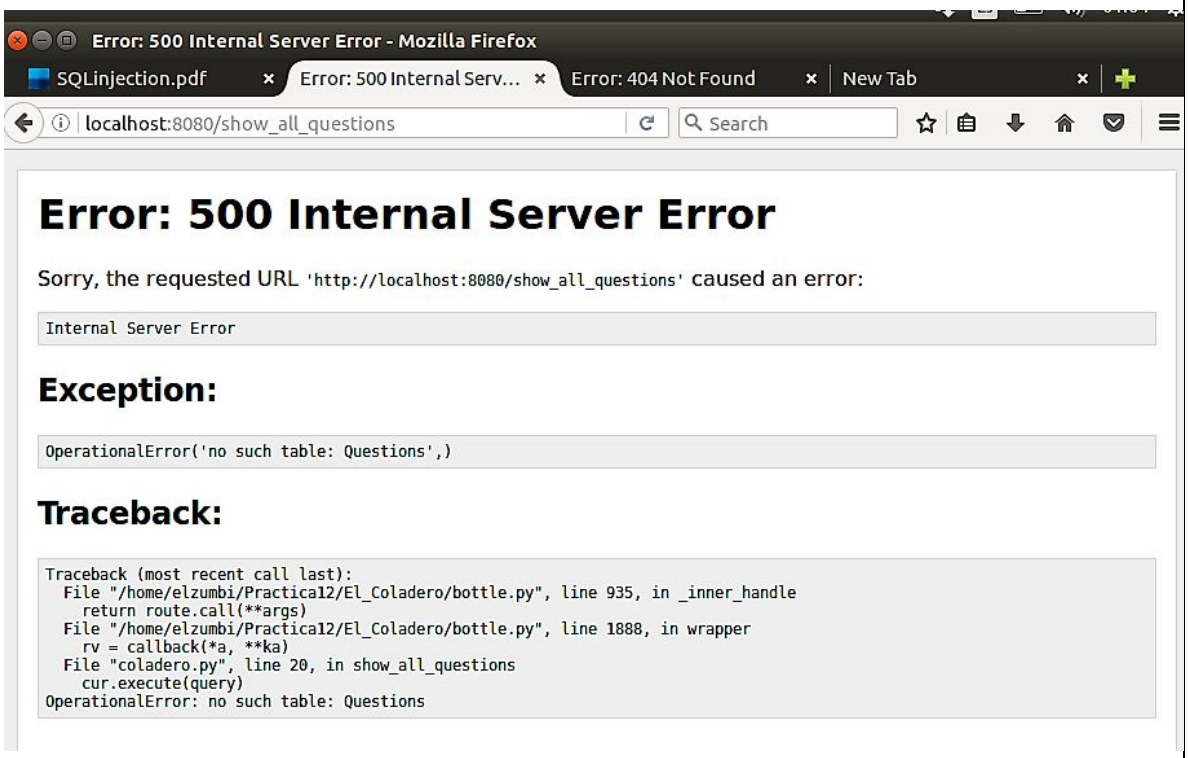
Introducimos una consulta en el campo etiquetas, que pretende borrar una tabla de la base de datos.
‘,’’) DROP TABLE Questions --’
Y preguntamos.



Esta consulta es inyectada en la base de datos y se nos confirma que se ha realizado correctamente.



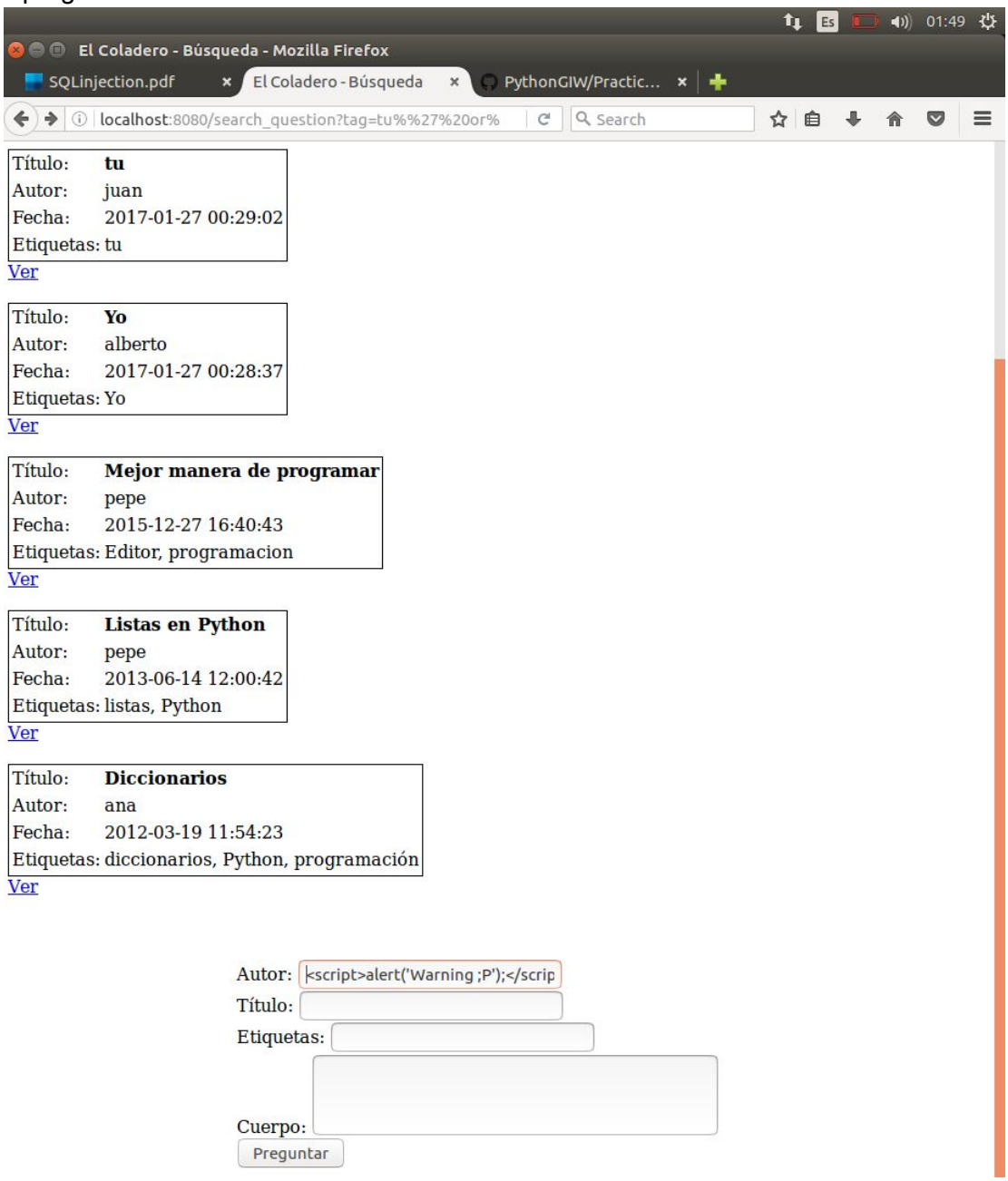
Al volver a la página show_all_questions nos encontramos que no se puede acceder a la tabla Questions, porque esta ha sido borrada.



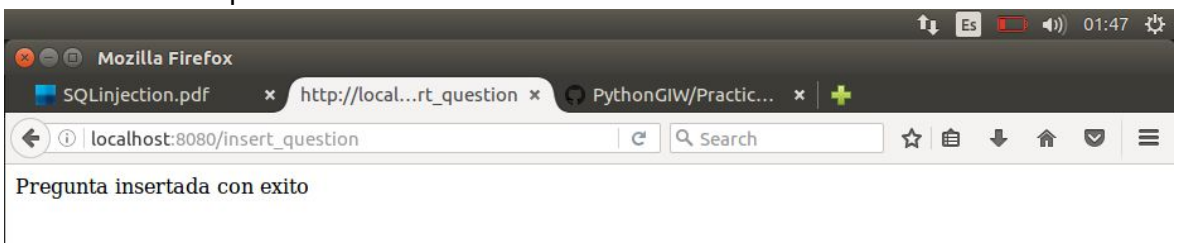
Medidas para mitigar la vulnerabilidad

-Deberíamos de limitar los permisos a la base de datos.
-Comprobar en el código que ataques como este no son posibles, mediante su corrección.
-Cambiar los tipos de las variables también podría ayudar.

INFORME DE VULNERABILIDAD
Tipo de vulnerabilidad
XSS persistente
Situaciones peligrosas o no deseadas que puede provocar
Cuando mostramos los datos, estos no se validan, y si un usuario ha insertado un script malicioso cuando vayamos a esta ruta nos aparecerá dicho script.
Ejemplo paso a paso de cómo explotar la vulnerabilidad (con capturas de pantalla)
Insertamos el scrip<scrip>alert(Warning ;P);</scrip></text> por el campo autor y le damos a preguntar.



Insertamos el script con éxito.



Cuando volvemos a la página show_all_questions nos encontramos con el script insertado.

Medidas para mitigar la vulnerabilidad

Deberían revisar los datos ya que están aceptando datos incorrectos. Esto se podría solucionar si cuando insertamos preguntas revisamos todas he impedimos la inserción código malicioso evitando este tipo de ataque.