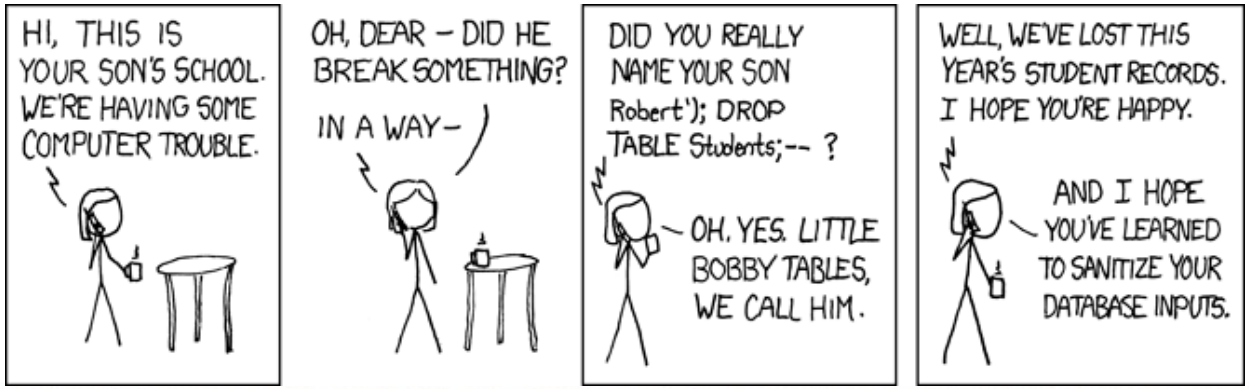

Proyecto Quiz

Inyección de Código

CORE 2015-2016

ver: 2016-04-13

¿Qué es la Inyección de Código?

- Es un problema de seguridad que aparece cuando generamos sentencias (para ejecutar) usando datos proporcionados por el usuario.
  - Los datos del usuario pueden contener fragmentos de sentencias SQL para borrar una base de datos, strings que al usarse en condiciones booleanas provocan una evaluación siempre verdadera, código javascript para inundar la pantalla de ventanas emergentes, etc.
- Hay que desconfiar siempre de los datos proporcionados por el usuario.
  - Estos datos pueden llegar al programa al rellenar los campos de un formulario, al recibir una petición HTTP, en una cookie, etc.
- Hay que validar siempre los datos recibidos antes de usarlos.

Inyección SQL

- Supongamos que ejecutamos el siguiente código para buscar en la base de datos un usuario con el **login** y el **password** introducidos en un formulario:

```
var login  = req.query.login;
var passwd = req.query.password;
var sql = "SELECT * FROM Users "+
                  "WHERE login='"+login+"' "+
                   " AND password='"+passwd+"';"
execute(sql, una_callback_cualquiera);
```

- Este programa busca el usuario y seguramente llamará a la callback especificada con el registro encontrado, o con un null.

- Si en el formulario se introdujo **pepe** y **1234**, la sentencia SQL ejecutada es:

```
SELECT * FROM Users WHERE login='pepe'
                      AND password='1234';
```

- Si existe el usuario **pepe**, y su password es **1234**, entonces se llama a la callback con el registro encontrado.

- **Ataque 1**: Vamos a introducir en el formulario los siguientes valores:

  login = **x**

  password = **x' OR '1=1**

  - En este caso la sentencia SQL ejecutada será:

```
SELECT * FROM Users WHERE login='x'
       AND password='x' OR '1=1';
```

  - Dado que **1=1** es siempre verdadero, entonces siempre se seleccionan todos los usuarios existentes,
    - y se llama a la callback dada.

- **Ataque 2**: ¿Piense qué pasaría si como valor del password se introduce el siguiente valor:

```
x'; DROP TABLE Users; --
```

Inyección Javascript

- Ejecute el servidor Quiz que estamos desarrollando, y cree un quiz introduciendo el siguiente texto como pregunta:

```
El ataque de la mujer de Thor <script>
document.body.style.backgroundImage =
"URL(http://www.ideal.es/multimedia/201502/11/media/
pataky/elsa-pataky-ahora.jpg)";
document.body.style.backgroundRepeat = "repeat"; </script>
```

  - Visualice en la aplicación (acción show) el quiz creado.
  - Modifique ahora el fichero **views/quizzes/show.ejs**, sustituyendo la línea:

```
<%= quiz.question %>
```

    - por esta otra:

```
<%- quiz.question %>
```

  - Visualice otra vez el quiz creado antes.

- **¿Nota alguna diferencia? Explique qué pasa.**