

CC3201-1

BASES DE DATOS

OTOÑO 2019

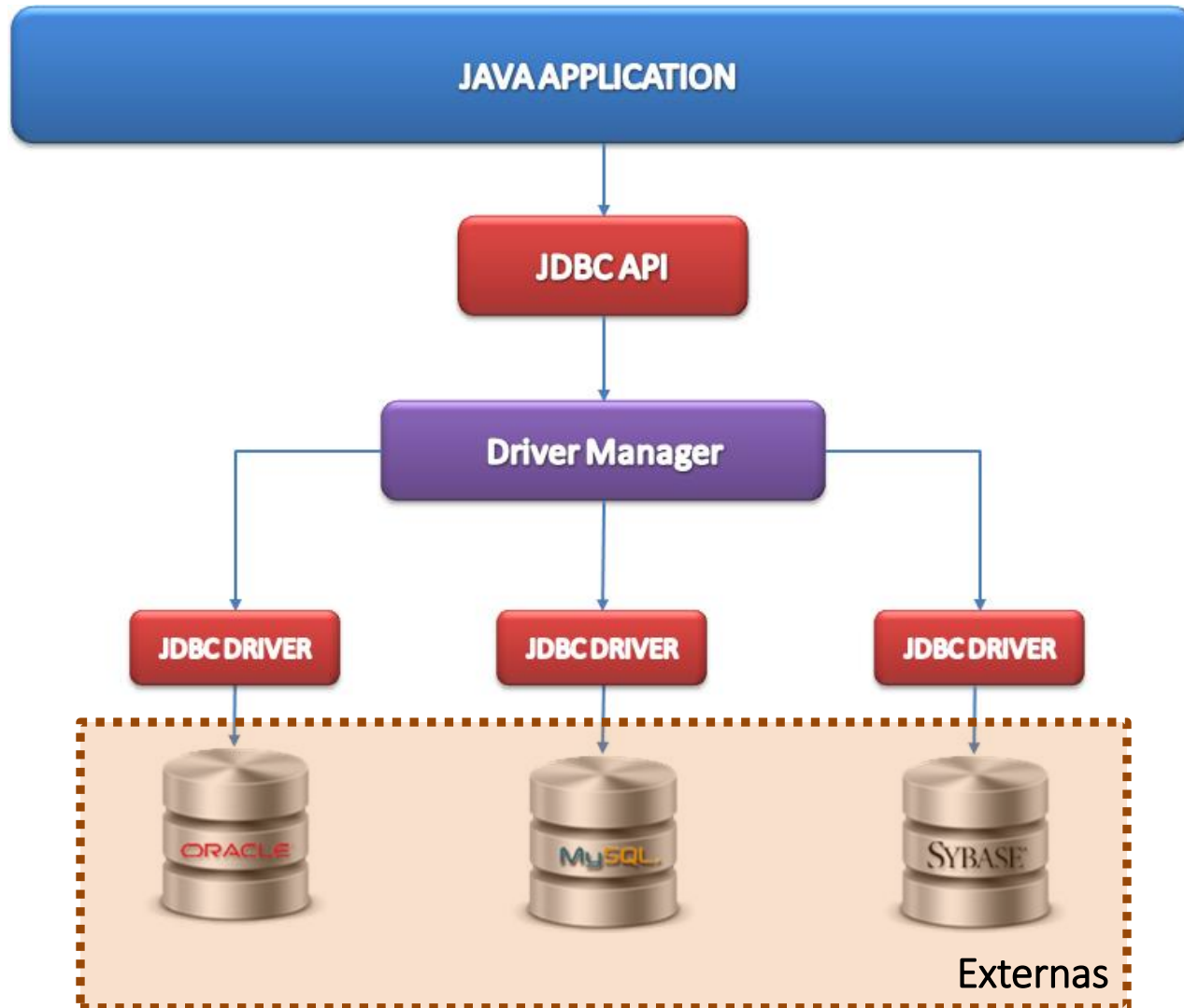
Clase 9: SQL: Acceso Programático,
Inyecciones, Seguridad

Aidan Hogan

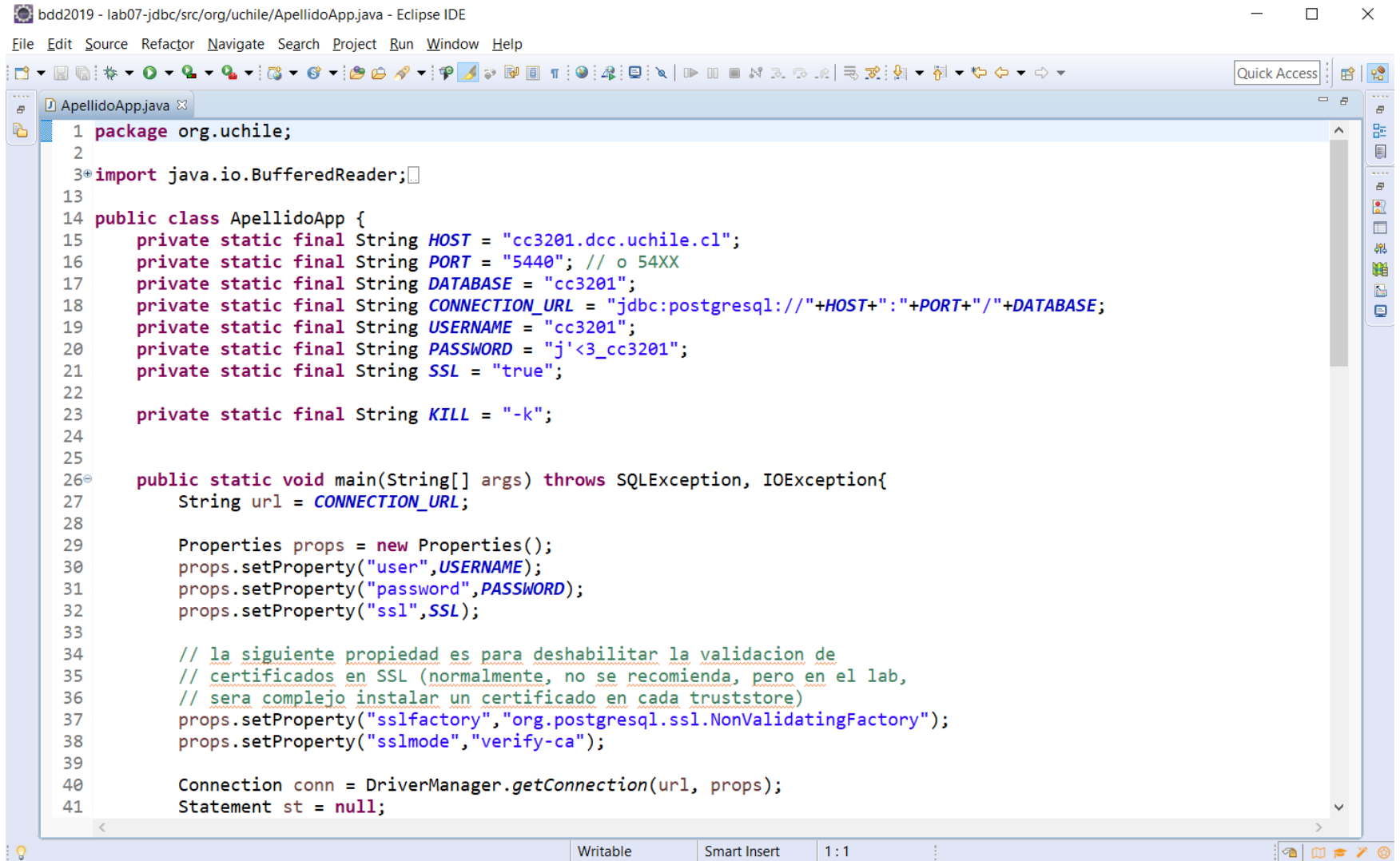
aidhog@gmail.com

ACCESO PROGRAMÁTICO (JAVA):
JAVA DATABASE CONNECTIVITY (JDBC)

Java Database Connectivity (JDBC)



Veremos el ejemplo ApellidoApp.java



```
bdd2019 - lab07-jdbc/src/org/uchile/ApellidoApp.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
ApellidoApp.java
1 package org.uchile;
2
3 import java.io.BufferedReader;
13
14 public class ApellidoApp {
15     private static final String HOST = "cc3201.dcc.uchile.cl";
16     private static final String PORT = "5440"; // o 54XX
17     private static final String DATABASE = "cc3201";
18     private static final String CONNECTION_URL = "jdbc:postgresql://" + HOST + ":" + PORT + "/" + DATABASE;
19     private static final String USERNAME = "cc3201";
20     private static final String PASSWORD = "j'<3_cc3201";
21     private static final String SSL = "true";
22
23     private static final String KILL = "-k";
24
25
26 public static void main(String[] args) throws SQLException, IOException{
27     String url = CONNECTION_URL;
28
29     Properties props = new Properties();
30     props.setProperty("user", USERNAME);
31     props.setProperty("password", PASSWORD);
32     props.setProperty("ssl", SSL);
33
34     // la siguiente propiedad es para deshabilitar la validacion de
35     // certificados en SSL (normalmente, no se recomienda, pero en el lab,
36     // sera complejo instalar un certificado en cada truststore)
37     props.setProperty("sslfactory", "org.postgresql.ssl.NonValidatingFactory");
38     props.setProperty("sslmode", "verify-ca");
39
40     Connection conn = DriverManager.getConnection(url, props);
41     Statement st = null;
```

Consulta vs. Actualización

- Para hacer consultas (SELECT):

```
String consulta = "SELECT ...";  
ResultSet rs = statement.executeQuery(consulta);
```

- Para hacer actualizaciones (INSERT; UPDATE, ...)

```
String actualizacion = "UPDATE ...";  
int tuplasAfectadas = statement.executeUpdate(actualizacion);
```

Un problema ...

```
System.out.println("Ingrese un apellido paterno:");
String input = br.readLine().trim();
if(input.equals(KILL)) break;

// crear un statement en blanco
st = conn.createStatement();

// crear la consulta
String consulta =
    "SELECT * FROM uchile.transparencia "
    + "WHERE apellido_p='"+input+"' "
    + "ORDER BY total DESC LIMIT 10";
ResultSet rs = st.executeQuery(consulta);

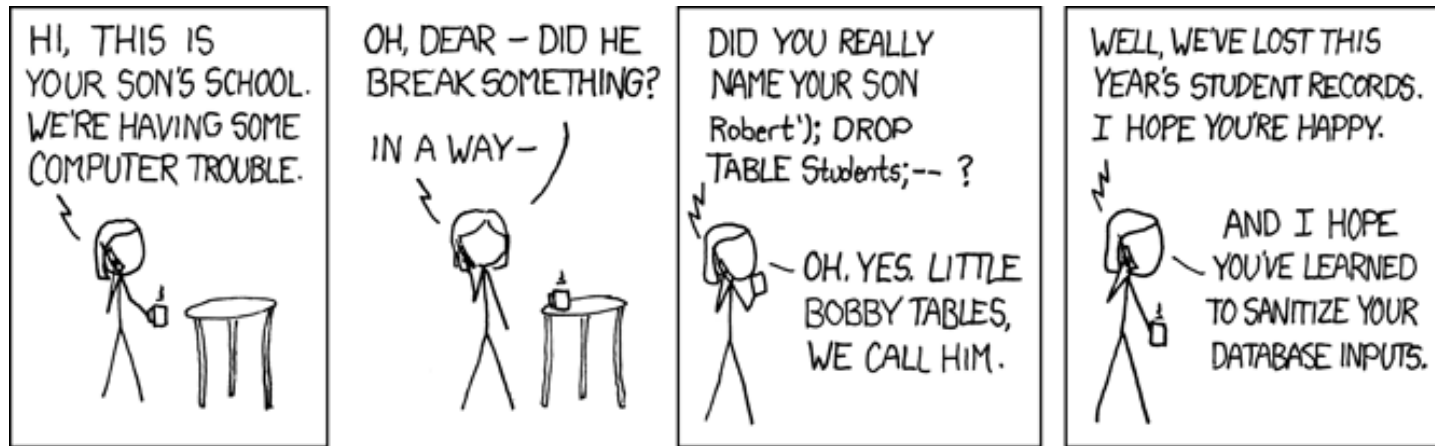
// ...
```

¿Hay algún problema aquí?

... no hemos "verificado" el input.

Inyección SQL

- Un usuario malintencionado puede ingresar un string de entrada para hacer algo inesperado



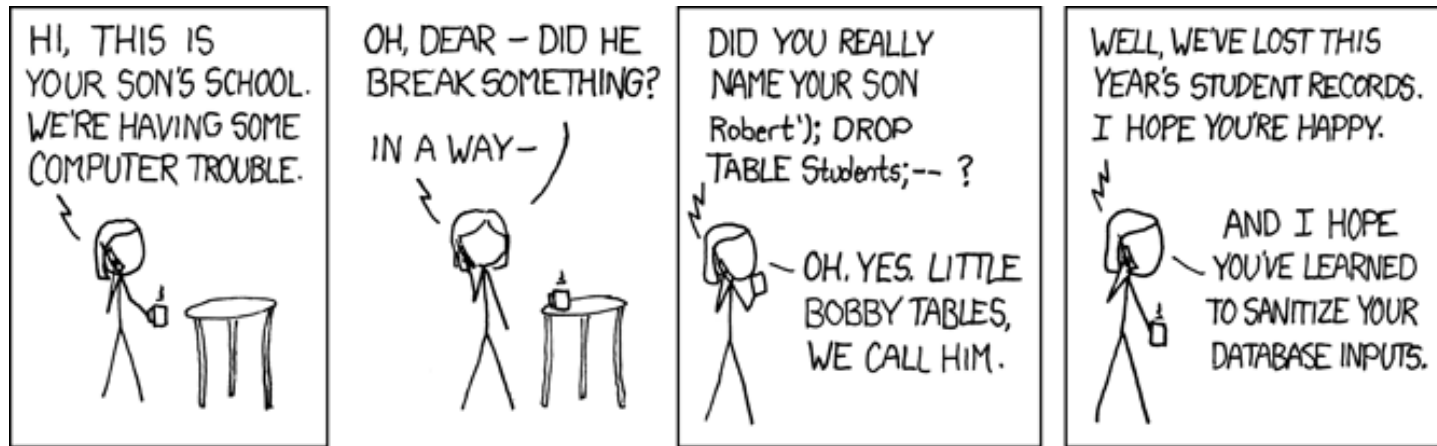
```
SELECT nota FROM Students WHERE name='"+input+"'
```

```
SELECT nota FROM Students WHERE name='Robert'); DROP TABLE Students; -- '
```

('--' empieza un comentario)

Inyección SQL

- Un usuario malintencionado puede ingresar un string de entrada para hacer algo inesperado



```
SELECT nota FROM Students WHERE name=''+input+''
```

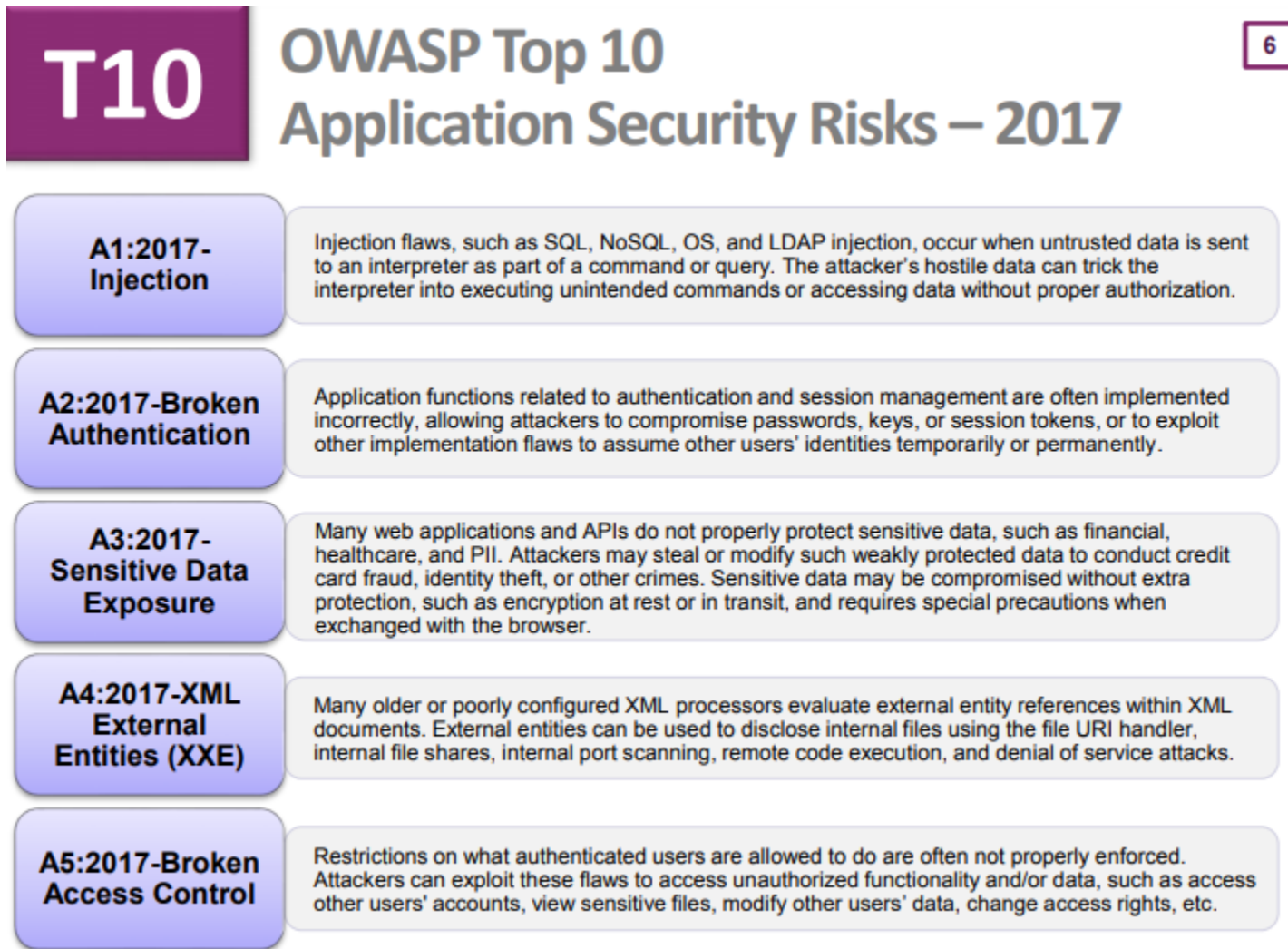
```
SELECT nota FROM Students WHERE name='Robert' OR 1=1 --'
```

¿Qué hace el ejemplo?

¡Devolverá toda la tabla!

Parece estúpido pero ...

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf



T10 **OWASP Top 10** 6
Application Security Risks – 2017

A1:2017-Injection Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE) Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Parece estúpido pero (por ejemplo) ...



The header of the ICO website features the logo 'ico.' in white on a dark blue background, with 'Information Commissioner's Office' written below it. To the right, a white text block states: 'The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.' Below this is a navigation menu with links: 'Home', 'For the public', 'For organisations', 'Report a concern', 'Action we've taken', and 'About the ICO' (which is highlighted with a light blue underline).

[About the ICO](#) / [News and events](#) / [News and blogs](#) /

TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

Date **05 October 2016**

Type **News**

Telecoms company TalkTalk has been [issued with a record £400,000 fine](#) by the ICO for security failings that allowed a cyber attacker to access customer data "with ease".

The [ICO's in-depth investigation](#) found that an attack on the company last October could have been prevented if TalkTalk had taken basic steps to protect customers' information.

ICO investigators found that the cyber attack between 15 and 21 October 2015 took advantage of technical weaknesses in TalkTalk's systems. The attacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.

Más ejemplos ...

https://en.wikipedia.org/wiki/SQL_injection

Examples [edit source]

- In February 2002, Jeremiah Jacks discovered that Guess.com was vulnerable to an SQL injection attack, permitting anyone able to construct a properly-crafted URL to pull down 200,000+ names, credit card numbers and expiration dates in the site's customer database.^[23]
- On November 1, 2005, a teenage hacker used SQL injection to break into the site of a Taiwanese information security magazine from the Tech Target group and steal customers' information.^[24]
- On January 13, 2006, Russian computer criminals broke into a Rhode Island government website and allegedly stole credit card data from individuals who have done business online with state agencies.^[25]
- On March 29, 2006, a hacker discovered an SQL injection flaw in an official Indian government's tourism site.^[26]
- On June 29, 2007, a computer criminal defaced the Microsoft UK website using SQL injection.^{[27][28]} UK website *The Register* quoted a Microsoft spokesperson acknowledging the problem.
- In January 2008, tens of thousands of PCs were infected by an automated SQL injection attack that exploited a vulnerability in application code that uses Microsoft SQL Server as the database store.^[29]
- In July 2008, Kaspersky's Malaysian site was hacked by a Turkish hacker going by the handle of "m0sted", who said to have used an SQL injection.
- In February 2013, a group of Maldivian hackers, hacked the website "UN-Maldives" using SQL Injection.
- In May 28, 2009 *Anti-U.S. Hackers Infiltrate Army Servers* Investigators believe the hackers used a technique called SQL injection to exploit a security vulnerability in Microsoft's SQL Server database to gain entry to the Web servers. "m0sted" is known to have carried out similar attacks on a number of other websites in the past—including against a site maintained by Internet security company Kaspersky Lab.
- On April 13, 2008, the Sexual and Violent Offender Registry of Oklahoma shut down its website for "routine maintenance" after being informed that 10,597 Social Security numbers belonging to sex offenders had been downloaded via an SQL injection attack.^[30]
- In May 2008, a server farm inside China used automated queries to Google's search engine to identify SQL server websites which were vulnerable to the attack of an automated SQL injection tool.^{[29][31]}
- In 2008, at least April through August, a sweep of attacks began exploiting the SQL injection vulnerabilities of Microsoft's IIS web server and SQL Server database server. The attack does not require guessing the name of a table or column, and corrupts all text columns in all tables in a single request.^[32] A HTML string that references a malware JavaScript file is appended to each value. When that database value is later displayed to a website visitor, the script attempts several approaches at gaining control over a visitor's system. The number of exploited web pages is estimated at 500,000.^[33]
- On August 17, 2009, the United States Department of Justice charged an American citizen, Albert Gonzalez, and two unnamed Russians with the theft of 130 million credit card numbers using an SQL injection attack. In reportedly "the biggest case of identity theft in American history", the man stole cards from a number of corporate victims after researching their payment processing systems. Among the companies hit were credit card processor Heartland Payment Systems, convenience store chain 7-Eleven, and supermarket chain Hannaford Brothers.^[34]
- In December 2009, an attacker breached a RockYou plaintext database containing the unencrypted usernames and passwords of about 32 million users using an SQL injection attack.^[35]
- On July 2010, a South American security researcher who goes by the handle "Ch Russo" obtained sensitive user information from popular BitTorrent site The Pirate Bay. He gained access to the site's administrative control panel and exploited a SQL injection vulnerability that enabled him to collect user account information, including IP addresses, MD5 password hashes and records of which torrents individual users have uploaded.^[36]
- From July 24 to 26, 2010, attackers from Japan and China used an SQL injection to gain access to customers' credit card data from Neo Beat, an Osaka-based company that runs a large online supermarket site. The attack also affected seven business partners including supermarket chains Izumiya Co, Maruetsu Inc, and Ryukyuu Jusco Co. The theft of data affected 100,000 customers. As of August 14, 2010 it was reported that there have been more than 300 cases of credit card information being used by third parties to purchase goods and services in China.
- On September 19 during the 2010 Swedish general election a voter at the Swedish Election Authority used writing SQL commands as part of a write-in vote.^[37]
- On November 8, 2010 the British Royal Navy website was compromised by a hacker named TinKode using SQL injection.^{[38][39]}
- On February 5, 2011 HBGary, a technology security firm, was breached by a hacker who used SQL injection in their CMS-driven website.^[40]
- On March 27, 2011, mysql.com®, the official homepage for MySQL, was hacked by a hacker using SQL blind injection.^[41]
- On April 11, 2011, Barracuda Networks was compromised by a hacker who used SQL injection to steal names and usernames of employees were among the information obtained.^[42]
- Over a period of 4 hours on April 27, 2011, an automated SQL injection tool used by a hacker to Reports website that was able to extract 8% of the username/password pairs: 8,000 random accounts of the 9,000 active and 90,000 old or inactive accounts.^{[43][44][45]}
- On June 1, 2011, "hacktivists" of the group LulzSec were able to download keys, and passwords that were stored in plaintext on Sony's website, accessing the personal information of a million users.^{[46][47]}
- In June 2011, PBS was hacked, mostly likely through use of a SQL injection. The hackers to execute SQL injections was described in this Imperva® blog.^[48]
- In May 2012, the website for *Wynn Casino*, a massively multiplayer online game, was hacked by a hacker from an SQL injection while the site was being updated.^[49]
- In July 2012 a hacker group called the logs were stored in plain text and were allegedly taken from a Yahoo! subdomain, Yahoo! Voices. The group breached Yahoo's security by using a "union-based SQL injection technique".^{[50][51]}
- On October 1, 2012, a hacker group of students, faculty, employees, and alumni from 53 universities including Harvard, Princeton, Stanford, Cornell, Johns Hopkins, and the University of Zurich on pastebin.com. The hackers claimed that they were trying to change education laws in Europe and increase tuition in the United States.^[52]
- On June 27, 2012, a hacker group they've been able to erase people's debts to water, gas, Internet, electricity, and telephone companies. Additionally, they published admin user name and password for other citizens to log in and clear their debts.^[53]
- On June 27, 2012, a hacker group using an SQL injection attack on the Chinese Chamber of International Commerce. The leaked data was posted publicly in cooperation with Anonymous.^[54]
- On June 27, 2012, a hacker group the hackers arrested for reporting the security vulnerability. 70,000 user details were exposed over this conflict.^[55]
- On June 27, 2012, a hacker group some victim to an SQL injection attack carried out by an Anonymous hacker named "Hooky" and aligned with hacktivist group "RaptorSwag". The hackers compromised information from nearly 420,000 websites through SQL injections.^[56] *The New York Times* confirmed this finding by hiring a security expert to check the claim.^[57]
- On June 27, 2012, a hacker group communications company Talk Talk's servers, exploiting a vulnerability in a legacy web portal.^[58]



Más ejemplos ...

https://en.wikipedia.org/wiki/SQL_injection

Examples [\[edit source\]](#)



- On June 1, 2011, "hacktivists" of the group LulzSec were accused of using SQLi to steal coupons, download keys, and passwords that were stored in plaintext on Sony's website, accessing the personal i
- In June 2011, PBS was hack
- In May 2012, the website for
- In July 2012 a hacker group
- On October 1, 2012, a hacker they were trying to "raise awa
- On June 27, 2013, hacker gr and clear their debts early m
- On November 4, 2013, hacke
- On February 2, 2014, AVS T
- On February 21, 2014, Unites
- On February 21, 2014, Hacke
- On March 7, 2014, officials a personal details of 878 stud
- In August 2014, Milwaukee-based computer security company Hold Security disclosed that it uncovered a theft of confidential information from nearly 420
- In October 2015, an SQL injection attack was used to steal the personal details of 156,959 customers from British telecommunications company Talk Talk's servers, exploiting a vulnerability in a legacy web porta

The 7-Eleven logo, featuring a white number "7" with a red and orange shape above it, and the word "ELEVEN" in green below it, all on a white background with a green border.The Royal Navy logo, featuring a white Union Jack flag on a blue background with the words "ROYAL NAVY" in white, bold, sans-serif capital letters below it.The HBGary logo, featuring the text "HBGary" in a large, bold, black sans-serif font, with "Detecting Tomorrow's Threats Today" in a smaller blue font below it, and "Part of ManTech International Corporation" in a red font at the bottom.

El Jefe de HBGary ...



aaronbarr

Today we taught everyone a lesson. When we actually decide to bite back against those who try to bring us down, we bite back hard. #gameover

23 minutes ago via web

<http://vocaroo.com/?media=vY7n2sXJaoPZVTHGq> Aaron's new resumé amirite #hurrhurr

about 1 hour ago via web

Spot the edit: <http://www.linkedin.com/in/tedvera> you Ted Vera, you're not getting away either! Nom nom nom, who's next? Penny? #hbgary

about 1 hour ago via web

Here's my address: [REDACTED]

about 1 hour ago via web

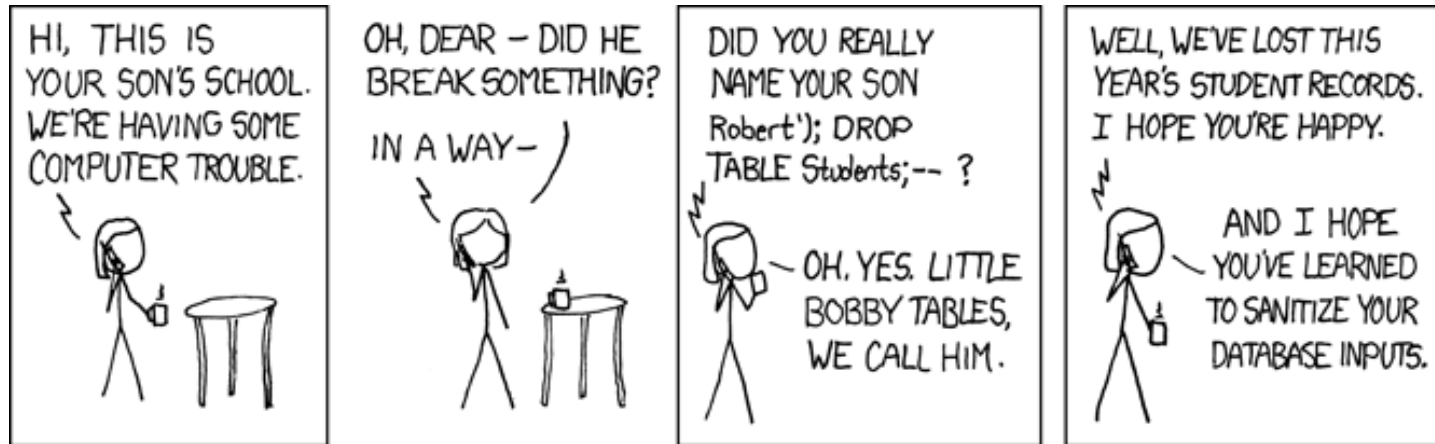
Here's my social security number: [REDACTED]

about 1 hour ago via web



HBGary
Detecting Tomorrow's Threats Today
Part of ManTech International Corporation

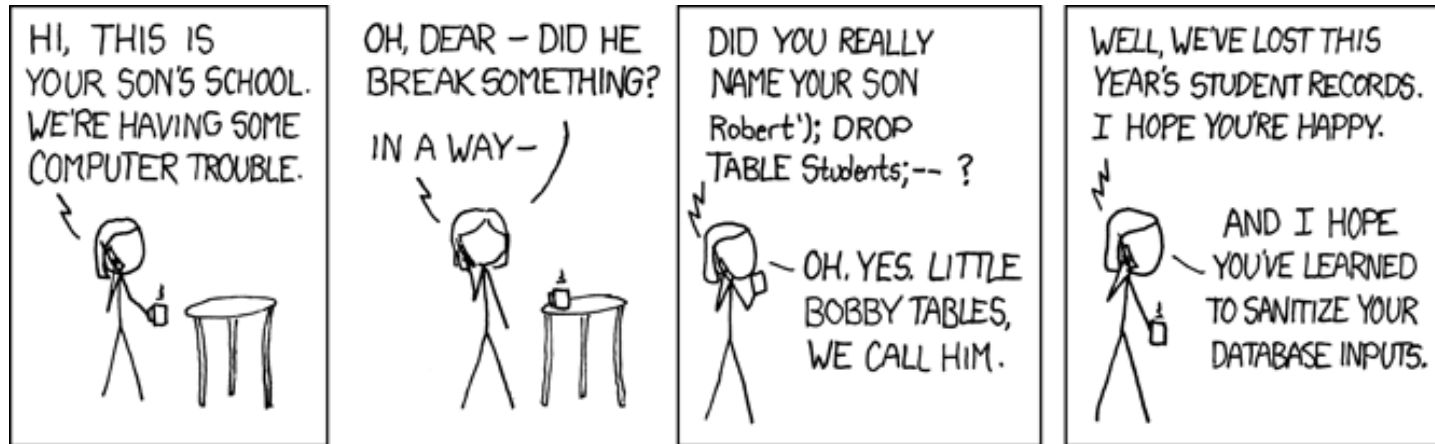
Inyección SQL



```
String consulta = "SELECT nota FROM Students WHERE name='"+input+"'";  
ResultSet rs = statement.executeQuery(consulta);
```

¿Cómo podemos resolver el problema?

Inyección SQL: ¿*escapar* los strings?



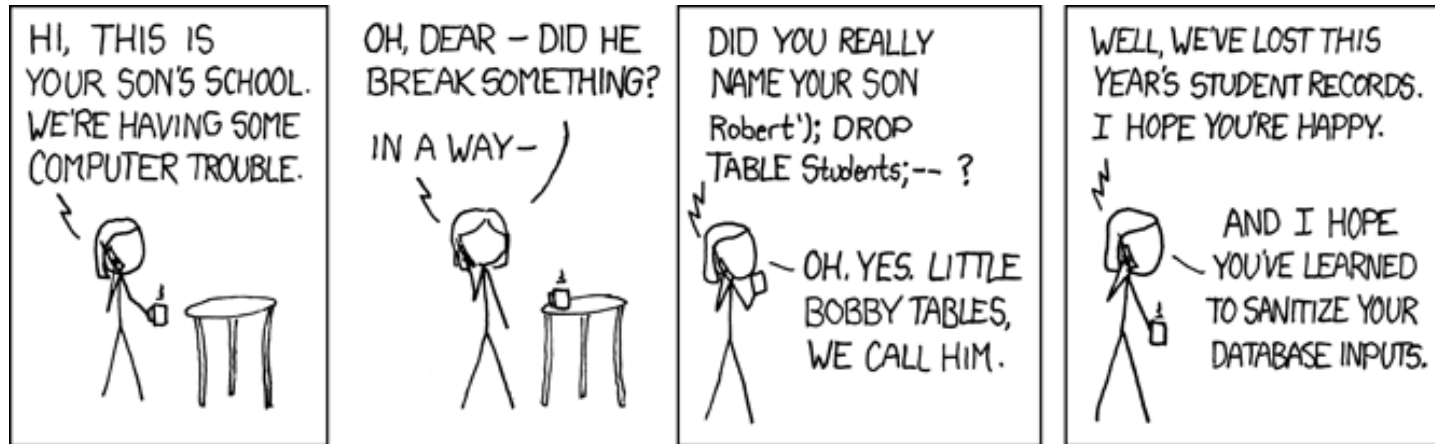
```
String consulta = "SELECT nota FROM Students WHERE name='"+input+"'";  
ResultSet rs = statement.executeQuery(consulta);
```

¿Cómo podemos resolver el problema?

```
String consulta = "SELECT nota FROM Students WHERE name='"+escapar(input)+"'";  
ResultSet rs = statement.executeQuery(consulta);
```

Mejor, pero sería complicado implementar la función *escapar* en un lenguaje de programación general y garantizar que prevenga cada tipo de inyección en cada versión (futura) de cada sistema de BdB dado cualquier tipo de consulta y entrada!

Inyección SQL: *¡sentencias pre-compiladas!*



```
String consulta = "SELECT nota FROM Students WHERE name='?'";  
// donde ? es un parámetro que reemplazaremos con la entrada del usuario  
PreparedStatement ps = conn.prepareStatement(consulta);  
ps.setString(1, input);  
ResultSet rs = ps.executeQuery();
```

Mandamos la consulta al sistema de bases de datos y después se reemplazarán los parámetros con la entrada del usuario

Inyección SQL: *¡sentencias pre-compiladas!*

```
String consulta = "SELECT nota FROM Students WHERE name=?";  
  
PreparedStatement ps = conn.prepareStatement(consulta);           // 1  
ps.setString(1, input);                                         // 2  
ResultSet rs = ps.executeQuery();                               // 3
```

// 1 : El sistema de bases de datos compila la sentencia

```
SELECT nota FROM Students WHERE name=?
```

QUERY PLAN

Seq Scan on Students (cost=0.00..9654.67 rows=57 width=132)

Filter: ((name)::text = ?::text)

El sistema de base de datos

*La consulta es compilada por el sistema **sin** la entrada*

Inyección SQL: *¡sentencias pre-compiladas!*

```
String consulta = "SELECT nota FROM Students WHERE name=?";  
  
PreparedStatement ps = conn.prepareStatement(consulta);           // 1  
ps.setString(1, input);                                         // 2  
ResultSet rs = ps.executeQuery();                               // 3
```

// 2 : El sistema de bases de datos reemplaza el parametro en el plan

```
SELECT nota FROM Students WHERE name=?
```

QUERY PLAN

Seq Scan on Students (cost=0.00..9654.67 rows=57 width=132)

Filter: ((name)::text = 'Robert'::text)

El sistema de base de datos

*Se reemplaza el parámetro en la sentencia pre-compilada
(que es un plan en memoria, no un string)*

Inyección SQL: *isentencias pre-compiladas!*

```
String consulta = "SELECT nota FROM Students WHERE name=?";  
  
PreparedStatement ps = conn.prepareStatement(consulta);           // 1  
ps.setString(1, input);                                         // 2  
ResultSet rs = ps.executeQuery();                               // 3
```

// 3 : El sistema de bases de datos ejecuta el plan

```
SELECT nota FROM Students WHERE name=?
```

QUERY PLAN

Seq Scan on Students (cost=0.00..9654.67 rows=57 width=132)

Filter: ((name)::text = 'Robert'::text)

El sistema de base de datos

nota

3,7

Sentencias pre-compiladas

```
String consulta = "SELECT nota FROM Students WHERE name=? AND year=?";
```

```
PreparedStatement ps = conn.prepareStatement(consulta);  
for(String[] input:inputs){  
    ps.setString(1, input[1]);  
    ps.setInt(2, Integer.parseInt(input[2]));  
    ResultSet rs = ps.executeQuery();  
    ...  
}
```

Se puede reutilizar el PreparedStatement varias veces
(es más eficiente también: se compila la sentencia sólo una vez)

Se puede tener varios parámetros con varios tipos

Preguntas?



CATS : ALL YOUR BASE ARE BELONG
TO US.