Australian
National
University

Database Security – Part 3

A Survey

- A survey by GreenSQL (http://www.greensql.com, released on April 3, 2012) shows that **the most critical database security concerns** are:

	database administrator errors, and dat privileged internal users
18%	**Regulatory compliance**

- Surveyed more than six thousand users – IT administrators, DBAs, data security professionals and consultants.

SQL Injection

- SQL injection is mostly known as an attack for **web applications** (considered as **one of the top 10 web application vulnerabilities** of 2007 a

- S

- Web applications often access a database by

1. Connect to the database;
2. Send SQL statements and data to the datab n!
3. Fetch the result and display data from the database;
4. Close the connection.

What is SQL Injection?

- In **SQL injection attacks**, hackers inject a string input through the Web a

- It c

  -
  - retrieve sensitive data in the database like c

  - execute system level commands that ma service to the application,
  - ...

What is SQL Injection?

- In **SQL injection attacks**, hackers inject a string input through the Web application which changes the SQL statement to their advantages.
- It c
  -
  -
  -
    service to the application,
  - ...

A credit card payment processing company cal CardSystems had an SQL injection att in which 263,000 credit card numbers were stolen from its database. CardSystems lost large amounts of business and its assets were acquired by another company.

SQL Injection – Example

- T

s

SQL Injection – Example

- The following query is issued by a simplistic authentication procedure:

```
S
```

- T

```
SELECT * FROM users WHERE name=‘jake’
                   AND password=‘p’ OR ‘x
```

```
SELECT * FROM users WHERE name=‘jake’
                   AND password=‘p’; DROP TABLE users; --;’;
```

SQL Injection – Example

- The following query is issued by a simplistic authentication procedure:

```
SELECT * FROM users WHERE name=‘jake’ and password=‘passwd’;
```

- T

```
S
                  AND password=‘p’ OR ‘x
```

```
SELECT * FROM users WHERE name=‘jake’
                  AND password=‘p’; DROP TABLE users; --;’;
```

- Because the query here is constructed from strings, the use of quotes has turned the original WHERE condition into a condition **that is always true**.

SQL Injection – Another Example

link to this comic: http://xkcd.com/327/

SQL Injection – Protection Techniques

- Protection against SQL injection attacks can be achieved by applying certain rules to all Web-accessible procedures and functions.
  - **Parameterized queries** is used to improve security by preventing SQL

```
[illegible]
    [illegible]
stmt.setString(1, user_name);
stmt.setString(2, user_passwd
```

  - **Input validation** is used to remove or esc strings. For example,

```
"SELECT * FROM users WHERE name = '" + escape(user_name) +
      "' and password= '" +escape(user_passwd) +"'"
```

In this case, user_name can't be `p' OR 'x'='x`.

Summary

- Database security is critical.
  - Ensure that only authenticated users can access the system (i.e.,
  -

- S
  avoiding SQL injection vulnerabilities is much ea

  - SQL Injection (http://www.w3scho n.asp)
  - Testing for SQL Injection (https:// Testing_for_SQL_Injection_(OTG-INPVAL-005)
  - SQL Injection Prevention Cheat Sheet (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)
  - "**Foundations of Security: What Every Programmer Needs To Know**" by Neil Daswani, Christoph Kern, and Anita Kesavan