



THE UNIVERSITY OF  
MELBOURNE

# Database Security and Backups

Database Systems & Information Modelling  
INFO90002

---

Week 11 – Database security  
Dr Tanya Linden  
David Eccles





# Lecture objectives

On completion of this lecture students should be able to discuss

- Technical safeguards
  - Types of access control
  - Firewall
- Data Safeguards
  - Encryption
  - Backups. Types of backups
- Reducing risk of data loss



# Technical Safeguards – Access Control

## Access Control Policy (People and Procedures)

- A high level set of rules to grant, revoke and or deny access to the database

## Access Control Model (Procedure)

- The model is the formalised policy of the rules

## Access Control Mechanism (Data and Technical)

- The mechanism is the means to enforce the policy



# Technical Safeguards - Access Control System

Policy content example: Only HR & Payroll managers should be able see the salary of employees. Only HR staff should be able to see an employee's date of birth

Model:

- Everybody who is a HR Manager or Payroll Manager will be able to see the employee table, all other job roles such as HR Staff, or Payroll Clerk will have to access the employee table via a view which omits the salary information. Only HR staff should be able to see an employees date of birth

Mechanism: Role Based AC

```
CREATE VIEW V_EMPLOYEE
AS
SELECT employeeid, firstname, lastname,
departmentid, bossid,dateofbirth
FROM employee;

GRANT select on V_EMPLOYEE to HRstaff;
```

Staff	Role	EmpID
Helen Jones	HR Manager	56
Van Nguyen	Payroll Manager	23
Cathy Bates	HR Staff	101
Wolfgang Tuck	Payroll Clerk	27

# Access Control Types

## Discretionary Access Control - DAC

- Based on the identity of the user requesting access
  - Explicitly states which user (subject) can perform which action (action) on which resource (object)
  - DAC mechanism controls are defined by user identification with supplied credentials during authentication
  - Data owners (or any users authorised to control data) can define access permissions for specific users or groups of users
- Authorisation is triple:
    - Subject (User)
    - Object (Table)
    - Action (DML, DDL, DQL)
  - Types of DAC
    - Authorisation Table
    - Access Control List
    - Capability (Owner determines access rights to the objects they own)

# Discretionary Access Control

DAC is used in UNIX, Windows, Linux, and many other network operating systems.

A user may give access to their file or directory to other users or groups. The user decides on the type of control (read/write/execute...)

Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Advanced

DBA (or sysadmin) could perform the following types of discretionary access control

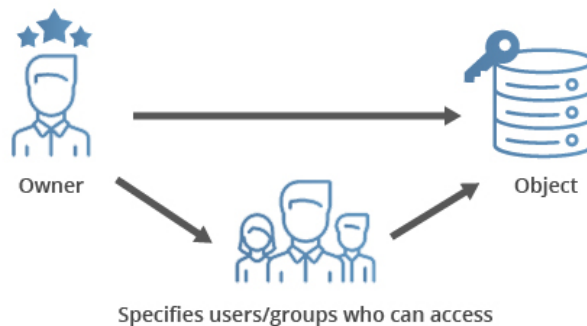
- Control who can create databases
- Prevent unauthorised users from registering user-defined routines

Example:

`## Grants for lindent@% ##`

`GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, SHUTDOWN, PROCESS, FILE, REFERENCES, SHOW DATABASES,`

## Discretionary Access Control (DAC)



# Access Control: Other types

## Mandatory Access Control (MAC)

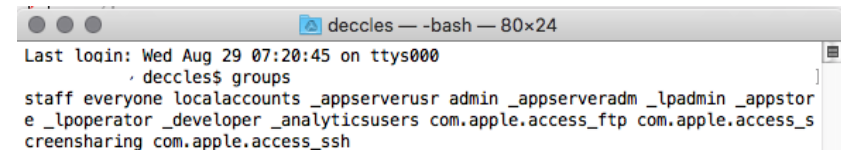
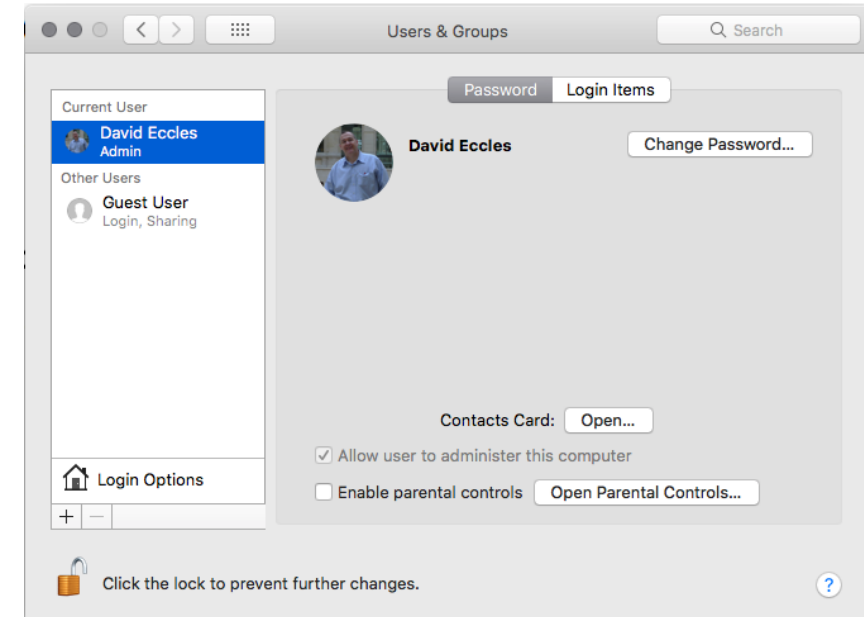
- Single Sign On
- Active Directory

## Role Based Access Control (RBAC)

- Unix / Linux / Mac Groups

## Examples (military systems)

- An individual data owner does not decide who has a top-secret clearance
- The owner of an object cannot change the classification of an object from top-secret to secret



# Technical Safeguard - Firewalls

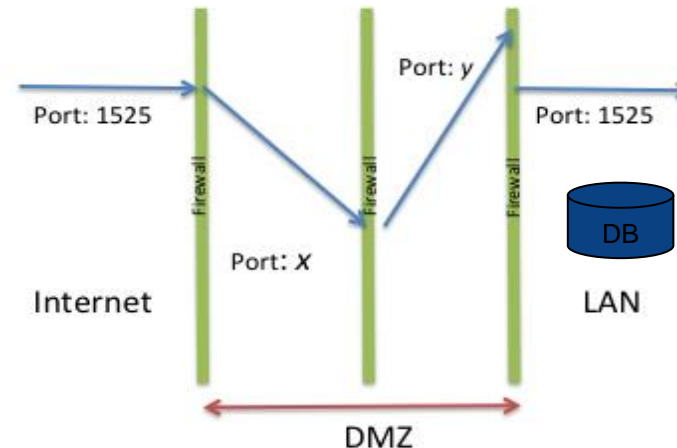
Protective layer between your LAN and the WAN / Internet

Software or dedicated hardware-software unit selectively blocks or allows data packets

All network traffic is quarantined and authenticated

Often several layers and types of firewall

DMZ – Demilitarized Zone





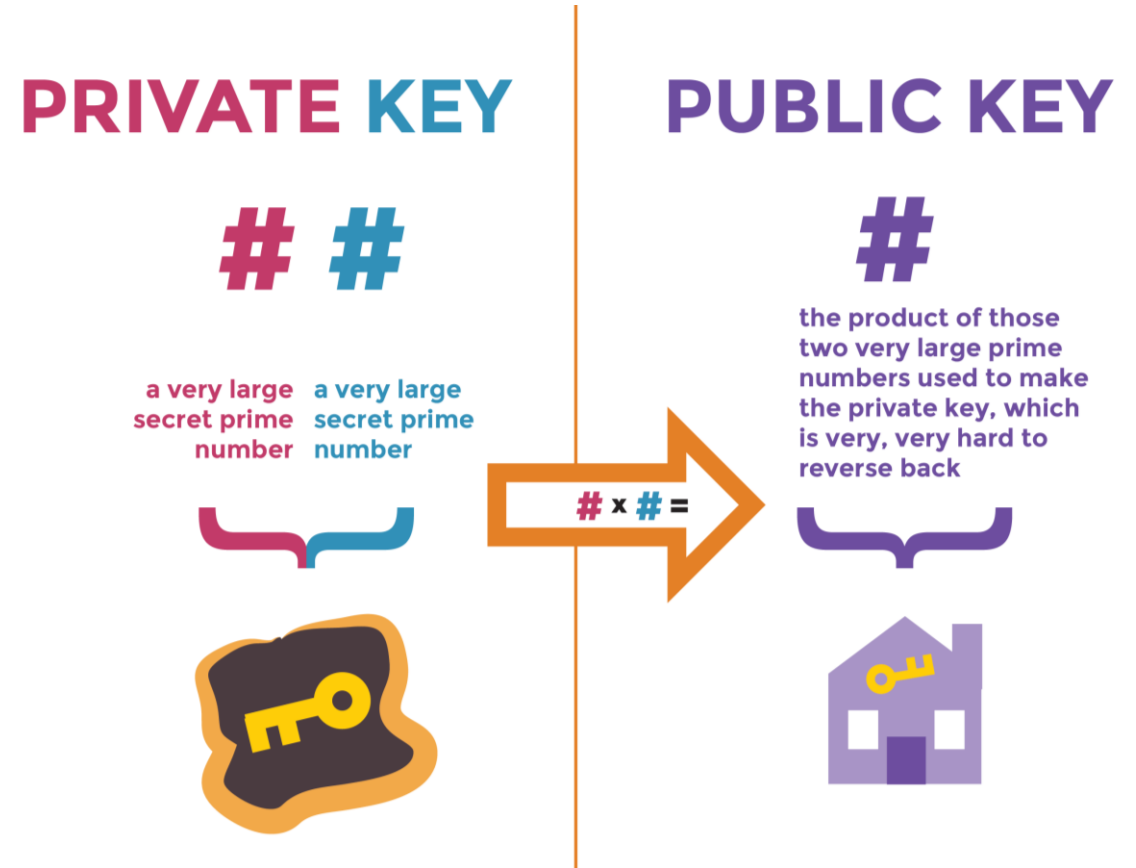
# Data Safeguard - Encryption

Encryption turns “clear text” into  
“\*k4#h2nsk7”

Involves very big prime number calculations  
used to scramble clear text

- Then “Salting” adding a byte or two to the encrypted string

Encryption *does not* hide data - it masks data



# Data Safeguard - Encryption

- Public Key and a Private Key
  - Public key is broadcast
  - Private key is required to unencrypt

(A encrypts sensitive information using B's **public key** and sends it across. B can only access that information and decrypt it using their corresponding **private key**)



# Data Safeguards – What is a Backup?

A backup is a copy of your data

- there are several types of backup

If data becomes corrupted or deleted or held to ransom it can be restored from the backup copy

A backup and recovery strategy is needed

- To plan how data is backed up
- To plan how it will be recovered



# Backups protect data from ...

## Human error

- e.g. accidental drop or delete
- example: <https://7news.com.au/business/banking/nab-blames-human-error-for-personal-data-breach-affecting-13000-customers-c-368105>



## Hardware or software malfunction

- bug in application
- hard drive (failure or corruption)
- CPU
- memory



# Back-ups protection

Backups could protect against

- malicious activity
  - security compromise
    - server, database, application
- natural or man made disasters
  - consider the *scale* of the damages

Backups help comply with


- government regulation
  - historical archiving rules
  - Metadata collection (AUS)
  - Privacy Rules

## Security

### Texas cops lose evidence going back eight years in ransomware attack

We have to get very, very tough on cyber and cyber warfare... and backups?

By Alexander J Martin 27 Jan 2017 at 16:57

36  SHARE ▼



♪ I hacked the sheriff, but I did not hack his deputy ♪

**Updated** Cockrell Hill, Texas has a population of just over 4,000 souls and a police force that managed to lose eight years of evidence when a departmental server was compromised by ransomware.

In a public statement, the department said the malware had been introduced to the department's systems through email. Specifically, it arrived "from a cloned email address imitating a department issued email address" and after taking root, requested 4 Bitcoin in ransom, worth about \$3,600 today, or "nearly \$4,000" as the department put it.





# Categories of Failure

Failures can be divided into the following categories:

## Statement failure

- Syntactically incorrect

## User Process failure

- The process doing the work fails (errors, dies)

## Network failure

- Network failure between the user and the database

## User error

- User accidentally drops the rows, table, database

## Memory failure

- Memory fails, becomes corrupt

## Media Failure

- Disk failure, corruption, deletion

```
SELECT employeeid, firstname, lastname, celery
FROM employee;
```

salary

A blue arrow points from the word 'salary' to the underlined word 'celery' in the SQL query, indicating a spelling correction.

Unable to connect to info90002db.eng.unimelb.edu.au

```
-- What does this do?
DROP table employee;
Rollback;
```



# Types of Backups

Physical vs. Logical

Online vs. Offline

Full vs. Incremental

Onsite vs. Offsite



# Backups – Physical vs. Logical

## Physical

Raw copies of files and directories

Suitable for large databases that need fast recovery

Database is preferably offline (“cold” backup) when backup occurs

- MySQL Enterprise automatically handles *file* locking, so database is not wholly offline

Backup = exact copies of the database directories and files

Backup should include logs

Backup is only portable to machines with a similar configuration

To restore

- shut down DBMS
- copy backup over current structure on disk

## Logical

Backup completed through SQL queries

Slower than physical

- SQL SELECTs rather than OS copy

Output is larger than physical

Doesn't include log or config files

Machine independent

Server is available during the backup

In MySQL can use the backup using

- Mysqldump
- SELECT ... INTO OUTFILE

To restore

- use mysqlimport, or LOAD DATA INFILE within the mysql client





# Backups Offline vs. Online

## Online (LIVE) or HOT

Backups occur when the database is “live”

Clients don’t realise a backup is in progress

Need to have appropriate locking to ensure integrity of data

No downtime or outage

Physical and Logical backups

## Offline (Shutdown) COLD

Backups occur when the database is stopped

Simpler to perform

Offline backup is preferable, but not available in all situations, e.g. applications without downtime

Physical backups only

# Backups Full vs. Incremental

## Full backup

A full backup is where the complete database is backed up

- Physical (online or offline)
- Logical (online)

It includes everything you need to get the database operational in the event of a failure

## Incremental Backup

Only the changes since last backup are backed up

For most databases this means only backup log files

To restore:

1. stop the database,
2. copy backed up log files to disk,
3. start the database,
4. tell it to redo the log files

# Backup Strategy

Backup strategy is usually a combination of full and incremental backups

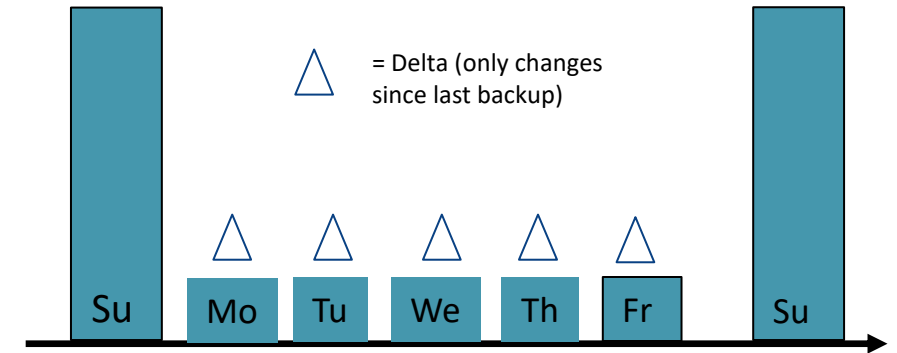
For example:

- weekly full backup
- weekday incremental backup

Conduct backups when database load is low

If you replicate the database, use the mirror database for backups to negate any performance concerns with the main database

**TEST** your backup before you **NEED** your backup!



# Offsite Backup

Motivation: hackers could still potentially get into your backups if they're connected to your network

Offsite means company backups are not stored in the organisation's building

Enables disaster recovery and business continuity

- Must be at remote site (e.g. ASIC require 100 km away)

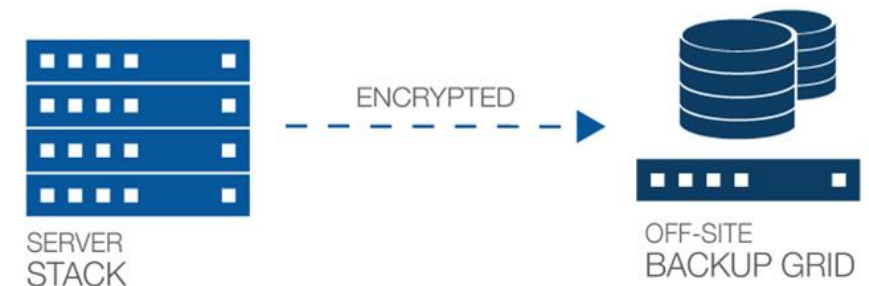
Backup tapes transported to underground vault

- NAB Knox City vault (15 feet silicon wall)

Remote mirror database maintained via replication

- Telstra Data Centres (Melbourne and Sydney)

Backup to Cloud





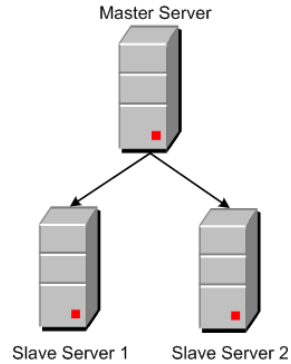
THE UNIVERSITY OF  
MELBOURNE

# Other ways to reduce risk of data loss



# Other ways to reduce risk of data loss

Server replication



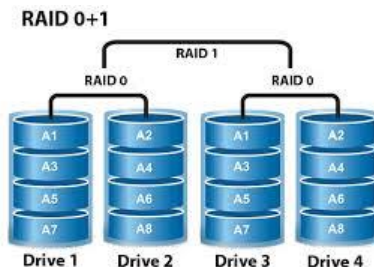
Problem	Protection?
accidental drop or delete	data loss!
server failure	protected
security compromise	limited protection

Server cluster



Problem	Protection?
accidental drop or delete	data loss!
server failure	protected
security compromise	limited protection

RAID



Problem	Protection?
accidental drop or delete	data loss!
server failure	data may be lost!
security compromise	all data compromised!



# Database Hardening - checklist

## DB Physical Hardening

- harder to get to the server room

## Firewalls for DB Servers

## Database Software; App / Web Server and App Code

- regularly patched, constant checking for vulnerabilities

## Client Workstations / Browsers

- least privilege rule

Admin SU (Super User) accounts, permissions and passwords

User roles, permissions, passwords and reporting

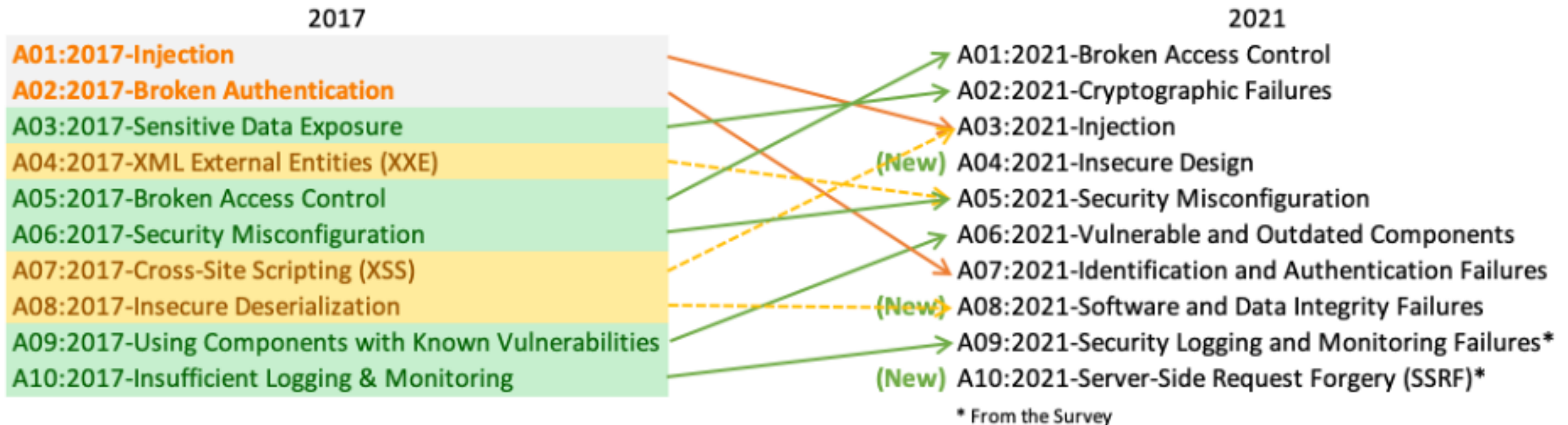
Change Management

Auditing

Backup and Recovery

# Web security

## OWASP top ten web app vulnerabilities



<https://owasp.org/www-project-top-ten/>

OWASP = Open Web Application Security Project



# Web security

## OWASP Top Ten web app vulnerabilities

- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.

# Protecting against SQL injection

## SQL Injection attacks

- a technique used to exploit web applications that use *user input within database queries*
- malicious code is entered into a data entry field in such a way that it becomes part of SQL commands that are run against the database
- How to prevent:
  - sanitize user inputs
  - pass inputs as parameters to a stored procedure, rather than directly building the SQL string in the code

# SQL injection

User inputs are used to form an SQL statement

Login



PLEASE LOG IN

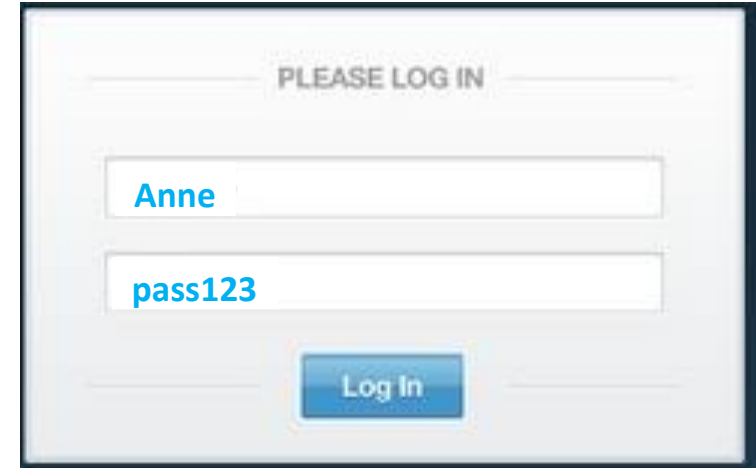
Username

Password

Log In

```
SELECT *  
FROM User  
WHERE username = ' @name '  
and password = ' @pw ' ;
```

Programmer wants:



PLEASE LOG IN

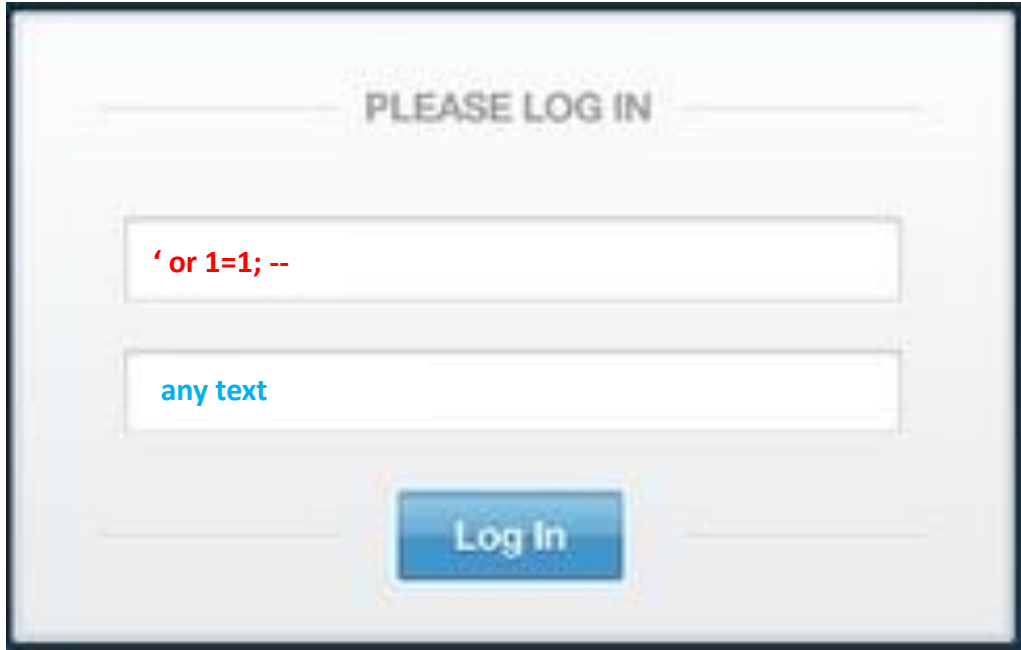
Anne

pass123

Log In

```
SELECT *  
FROM User  
WHERE username = 'Anne'  
and password = 'pass123' ;
```

# SQL injection: malicious input



PLEASE LOG IN

`' or 1=1; --`

`any text`

Log In

- Text entered in @name string now
- closes the string
  - adds a condition that is always true
  - ends the SQL statement
  - begins a comment with ' - - ' to neutralise the rest of the SQL

```
SELECT *  
FROM User  
WHERE username = ' ' or 1=1; --
```

# SQL injection: prevention

## Primary defences:

- Prepared Statements  
(parameterised queries)
- Stored Procedures
  - (both mean SQL is no longer 'dynamic')
- i.e. “escape” all user input
  - turns SQL special characters like ' ; -- into ordinary characters

## Additional defences:

- Principle of Least Privilege
  - don't give application accounts DBA privileges
- White List input validation
  - check input is from a list of acceptable values



PLEASE LOG IN

Username

Password

Log In



# What's examinable

- Access control
- Technical safeguards
- Data safeguards
- Types of back-ups
- Reducing risk of data loss



THE UNIVERSITY OF  
MELBOURNE

# Thank you