



9 Database Security

David Eccles & Dr Greg Wadley

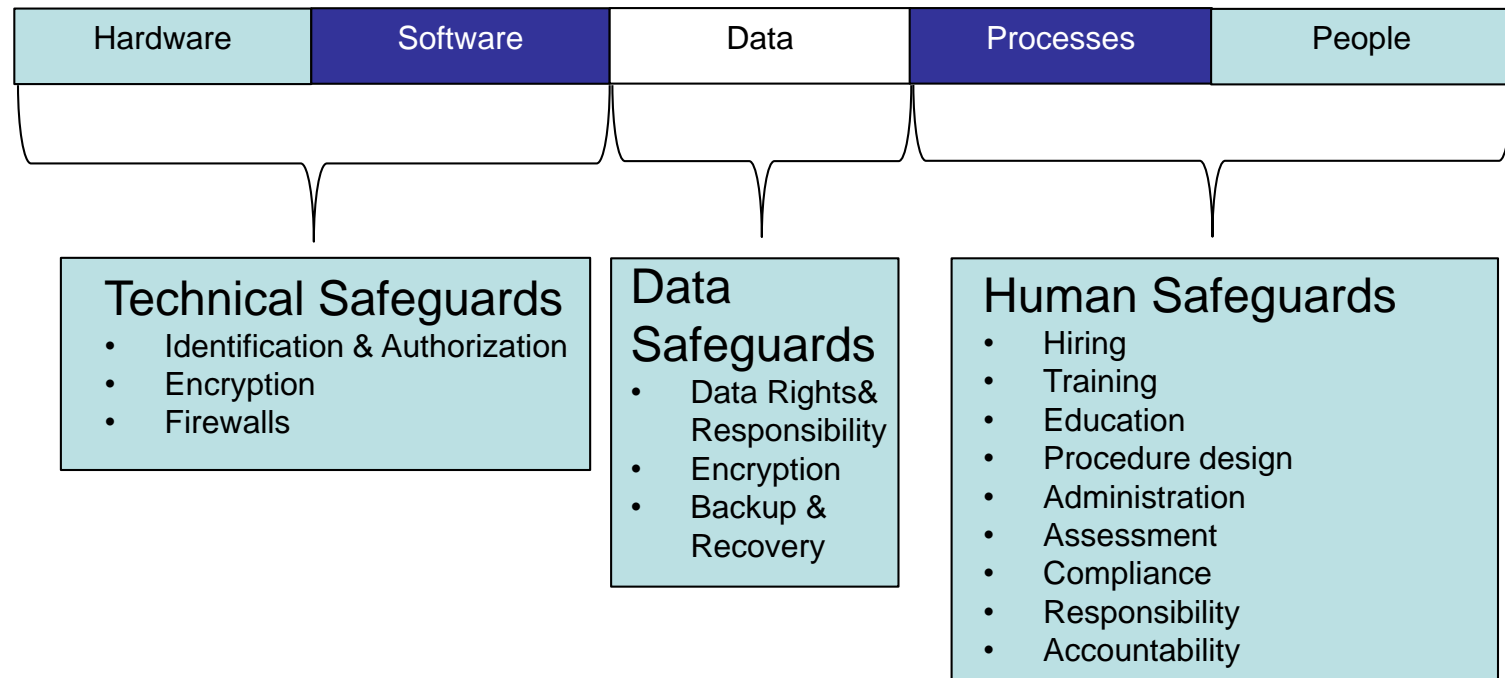
INFO90002

Database Systems &
Information Modelling



- Legal and Policy issues
- Ethics and Privacy issues
- Access and Control issues

- Five Component Framework (5CF) Approach:



- Professional Codes of Conduct
- Ethical & Moral considerations
- Privacy
- Legislative requirements
- Company Policy requirements



ACS CODE OF ETHICS

The ACS Code of Ethics is part of the ACS Constitution. As an ACS member you must uphold and advance the honour, dignity and effectiveness of being a professional. This entails, in addition to being a good citizen and acting within the law, your adherence to the following Society values:

1 The Primacy of the Public Interest

You will place the interests of the public above those of personal, business or sectional interests.

2 The Enhancement of Quality of Life

You will strive to enhance the quality of life of those affected by your work.

3 Honesty

You will be honest in your representation of skills, knowledge, services and products.

4 Competence

You will work competently and diligently for your stakeholders.

5 Professional Development

You will enhance your own professional development, and that of your colleagues and staff.

6 Professionalism

You will enhance the integrity of the Society and the respect of its members for each other.

This Code of Ethics applies to all ACS members regardless of their role or specific area of expertise in the ICT industry.

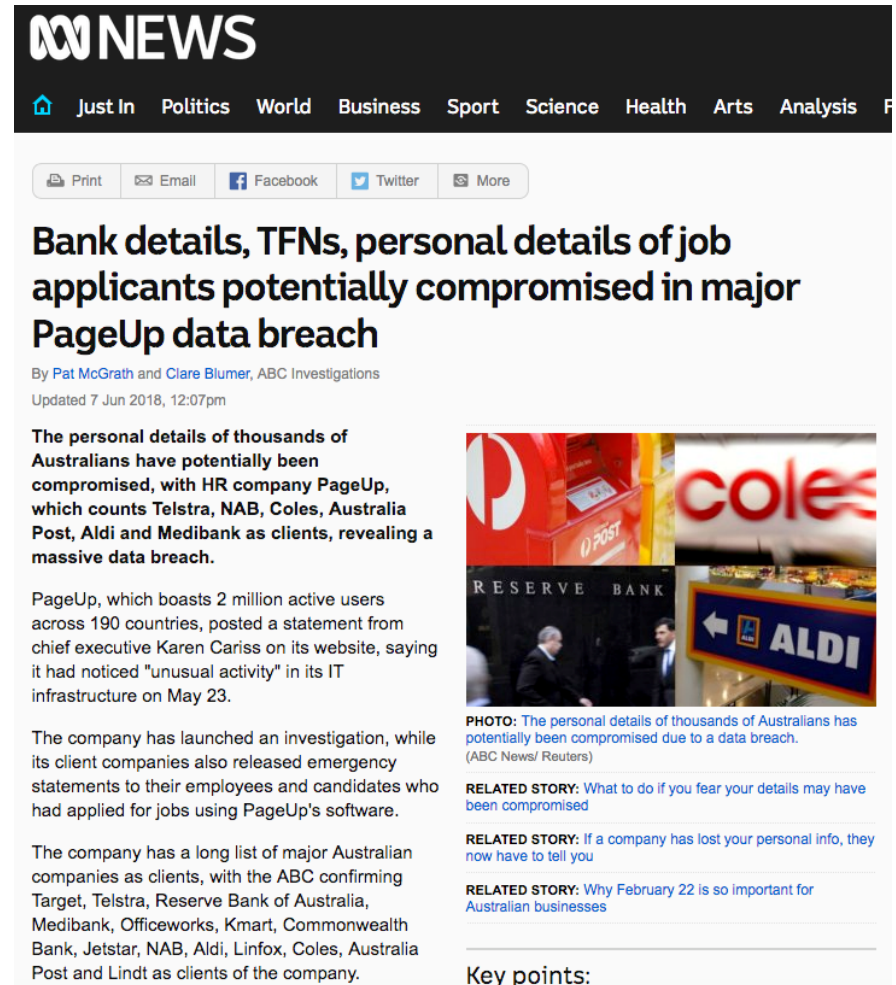
- Promises by professions to regulate themselves in the general interest of society
- Where we don't have clear laws we need ethical behaviours to ensure social harmony



- Do we always have the right to access information?
- You can apply ethical principles:
 - Immanuel Kant's Categorical Imperative
 - “If an action is not right for everyone to take then it is not right for anyone to take”
 - Risk aversion principle:
 - “Take the action that produces the least harm or incurs the least cost”

- Privacy and Data protection act 2014 (Vic Gov)
- Privacy Act 1988 (Commonwealth of Australia)
- Privacy Amendment (Private Sector) Act 2000
- Health Records Act 2001 (Vic Gov)
- Privacy Act of 1988 has been reformed to include larger fines for “repeated and serious breaches of privacy regulations”.
- University of Melbourne Privacy Policy:
Privacy Policy <http://policy.unimelb.edu.au/MPF1104>

- Page Up Data leak
- To apply for jobs
 - Proof of Australian Citizenship (Passport)
 - Proof have a current drivers license (Victorian Drivers License)
 - Date of Birth
- Job applicants have had sensitive private information leaked



ABC NEWS

Just In Politics World Business Sport Science Health Arts Analysis

Print Email Facebook Twitter More

Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach

By Pat McGrath and Clare Blumer, ABC Investigations
Updated 7 Jun 2018, 12:07pm

The personal details of thousands of Australians have potentially been compromised, with HR company PageUp, which counts Telstra, NAB, Coles, Australia Post, Aldi and Medibank as clients, revealing a massive data breach.

PageUp, which boasts 2 million active users across 190 countries, posted a statement from chief executive Karen Cariss on its website, saying it had noticed "unusual activity" in its IT infrastructure on May 23.

The company has launched an investigation, while its client companies also released emergency statements to their employees and candidates who had applied for jobs using PageUp's software.

The company has a long list of major Australian companies as clients, with the ABC confirming Target, Telstra, Reserve Bank of Australia, Medibank, Officeworks, Kmart, Commonwealth Bank, Jetstar, NAB, Aldi, Linfox, Coles, Australia Post and Lindt as clients of the company.

PHOTO: The personal details of thousands of Australians has potentially been compromised due to a data breach. (ABC News/ Reuters)

RELATED STORY: What to do if you fear your details may have been compromised

RELATED STORY: If a company has lost your personal info, they now have to tell you

RELATED STORY: Why February 22 is so important for Australian businesses

Key points:



- Hiring – Hire the right people
- Training – Train them
- Education – Educate them (SQL Injection; ransomware, trojans, worms)
- Procedures – How to prevent, what to do when (*not if*) it happens
- Administration – Not Set & Forget – active monitoring and enforcement
- Compliance – Privacy, Data Laws and Company policy
- Accountability – Someone is *responsible* and will be *accountable* if something goes wrong

- Access Control
- Access Control Policy (People & 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 & Technical)
 - The mechanism is the means to enforce the policy



- Policy: 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;
```

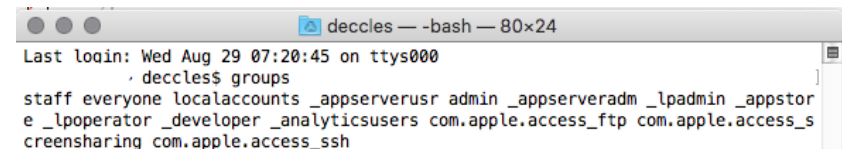
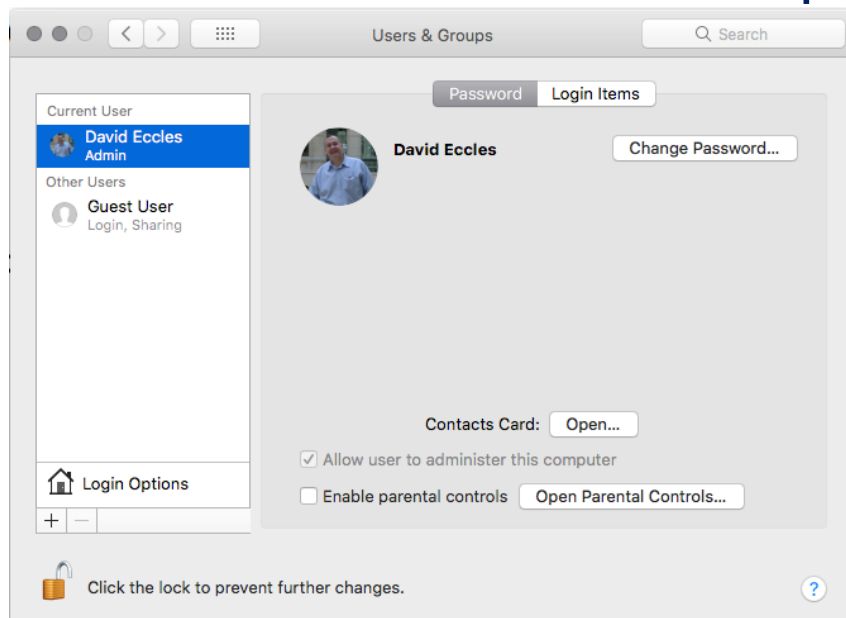
Staff	Role	EmpID
Helen Jones	HR Manager	56
Van Nguyen	Payroll Manager	23
Cathy Bates	HR Staff	101
Wolfgang Tuck	Payroll Clerk	27



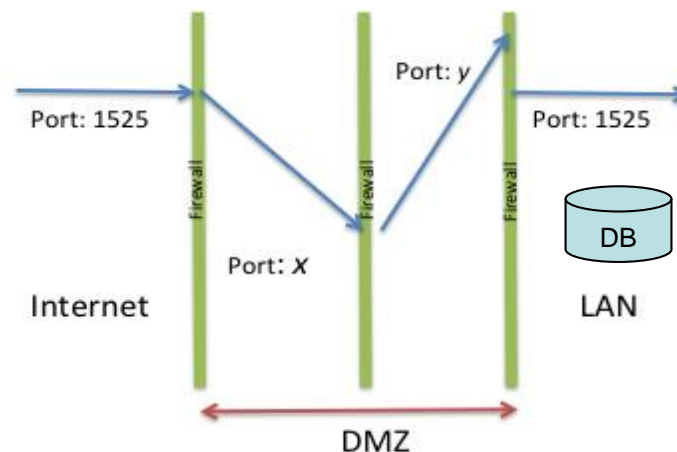
- DAC Discretionary Access Control
 - Based on the identity of the user requesting access
 - Explicitly states which user (subject) can perform which action (action) on which resource (object)
 - Authorization is triple:
 - Subject (User)
 - Object (Table)
 - Action (DML, DDL, DQL)
- Types of DAC
 - Authorization Table
 - Access Control List
 - Capability



- Mandatory Access Control
 - Single Sign On
 - Active Directory
- Role Based Access Control
 - Unix / Linux / Mac Groups



- Protective layer between your LAN and the WAN / Internet
- All network traffic is quarantined and authenticated
- Often several layers and types of firewall
- DMZ – Demilitarized Zone





- 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
 - Public Key and a Private Key
 - Public key is broadcast
 - Private key is required to unencrypt
 - (Your PIN on your ATM card is a Private Key)
- Encryption *does not* hide data - it masks data
 - Delays the data being revealed
 - (may be hours/weeks/years/centuries/millennia)

- A backup is a copy of your data
 - however 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:
<http://www.theaustralian.com.au/australian-it/human-error-triggered-nab-software-corruption/story-e6frgakx-1225962953523>
- hardware or software malfunction
 - bug in application
 - hard drive (failure or corruption)
 - CPU
 - memory




- malicious activity
 - security compromise
 - server, database, application
- natural or man made disasters
 - consider the *scale* of the damage
- government regulation
 - historical archiving rules
 - Metadata collection (AUS)
 - GDP (EU) HIPPA (US)
 - 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.





Failures can be divided into the following categories:

- Statement failure
 - Syntactically incorrect

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

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

MySQL Workbench has stopped working

- Network failure
 - Network failure between the user and the database

Unable to connect to info20003db.eng.unimelb.edu.au

- User error
 - User accidentally drops the rows, table, database

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

- Memory failure
 - Memory fails, becomes corrupt

- Media Failure
 - Disk failure, corruption, deletion



- Physical vs. Logical
- Online vs. Offline
- Full vs. Incremental
- Onsite vs. Offsite



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 off line
- 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

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 & 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

Logical backups only

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

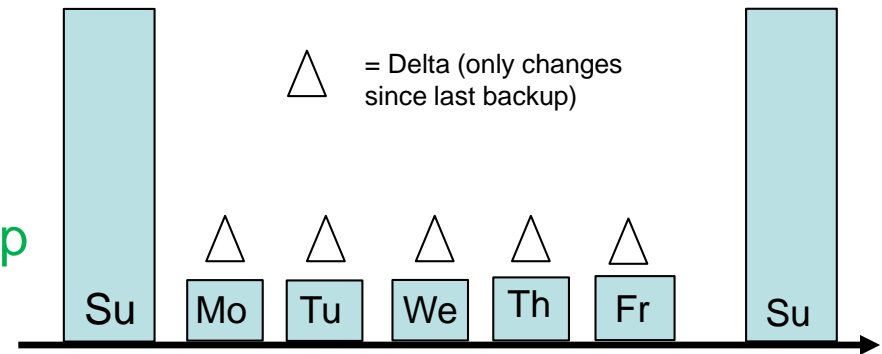
Incremental Backup

- only the changes since last backup are backed up
- for most databases this means only backup log files
- to restore:
 - stop the database, copy backed up log files to disk
 - start the database and tell it to redo the log files

- 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!

- enables disaster recovery & business continuity
 - 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 & Sydney)
- backup to Cloud

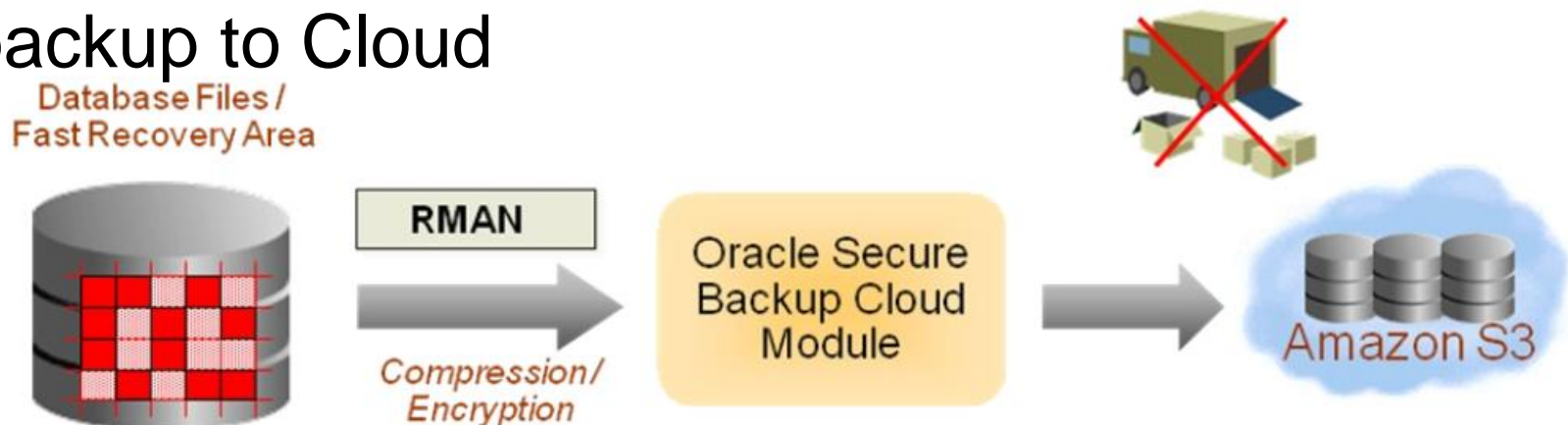
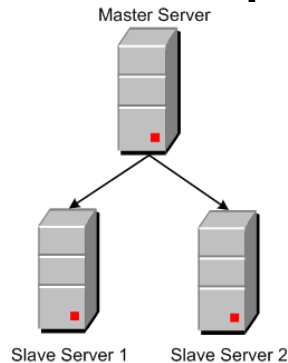


Figure 1. Oracle Database backup in the Cloud

- Server replication



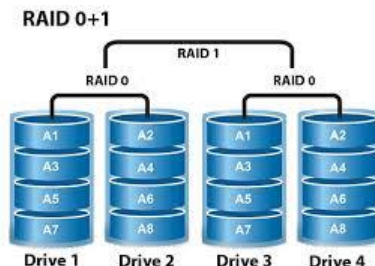
Problem	Protection?
accidental drop or delete	data loss!
server failure	protected
security compromise	limited protection

- 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!



- ☐ DB Physical Hardening
 - ☐ (harder to get to the server room)
- ☐ Firewalls for DB Servers
- ☐ Database Software; App / Web Server & App Code
 - ☐ (regularly patched, constant checking for vulnerabilities)
- ☐ Client Workstations / Browsers
 - ☐ least privilege rule
- ☐ Admin SU (Super User) accounts, permissions & passwords
- ☐ User roles, permissions, passwords & reporting
- ☐ Change Management
- ☐ Auditing
- ☐ Backup & Recovery



OWASP top ten web app vulnerabilities

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

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



OWASP Top Ten web app vulnerabilities

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)

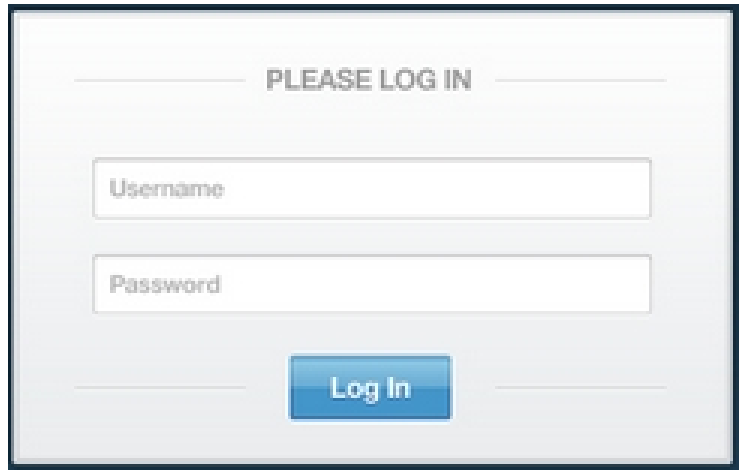
Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.



- 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

Login

- user inputs are used to form an SQL statement



PLEASE LOG IN

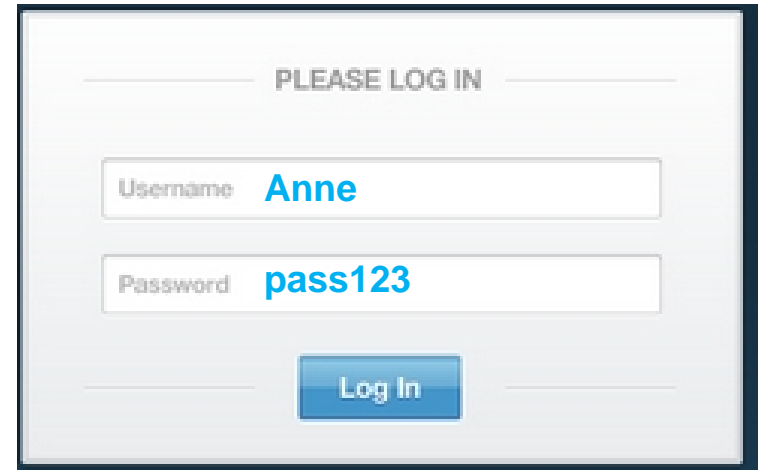
Username

Password

Log In

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

Programmer wants:



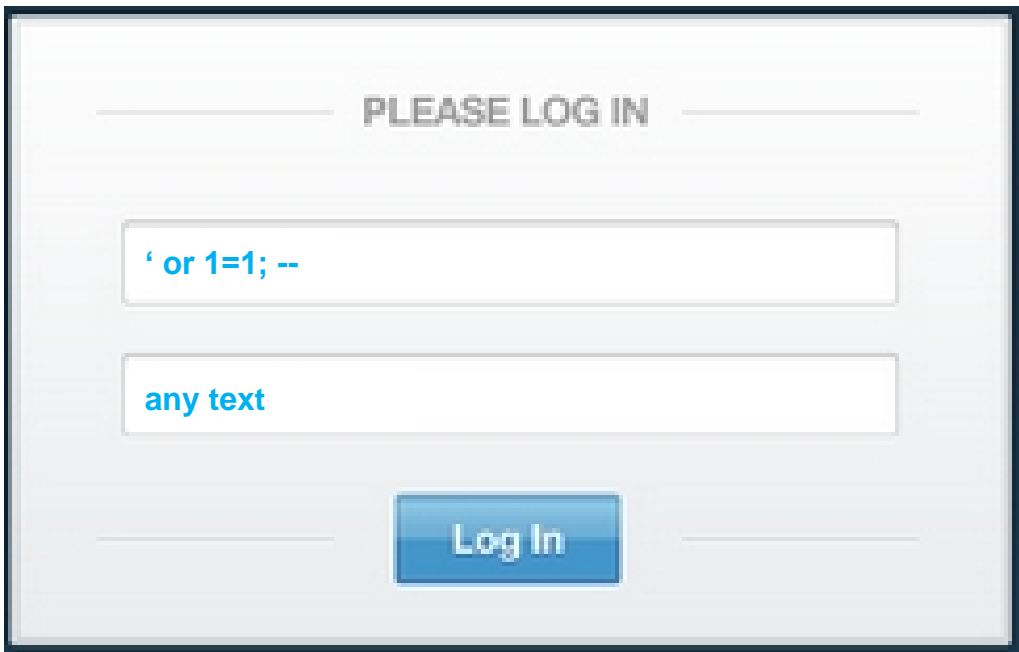
PLEASE LOG IN

Username Anne

Password pass123

Log In

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



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 neutralize the rest of the SQL

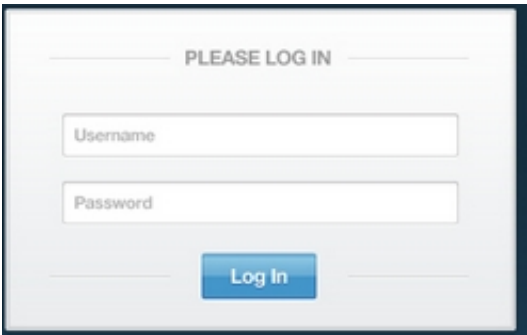
SELECT *

FROM User

WHERE username = ' ' or 1=1; -- ' '

and password = 'any text';

- Primary defences:
 - Prepared Statements (parameterized 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



THE UNIVERSITY OF
MELBOURNE

9 Database Security, Ethics and Privacy

David Eccles

INFO90002 Database Systems
& Information Modelling