**7ET023 Dissertation Artefact Design**

* Create database structure and test data for MySQL, Oracle and Microsoft SQL Server database management systems (DBMS)
* Insert test data and begin testing security with various forms of SQL Injection Attack (SQLIA) and any available tools
* Collate data gained into graph form to compare standard SQLIA protection
* Employ various detection and prevention methods found in the literature research that are available
* Collate data gained into graph form to compare SQLIA protection
* Formulate answer to research question based on results

Database design and development

Database SQLIA testing

Answer research question

Database enhanced testing result collation

Database testing result collation

Enhanced database SQLIA testing

Microsoft SQL Server test database design -

CREATE TABLE USERS

(USERNAME VARCHAR(50),

PASSWORD VARCHAR(50)

);

Oracle test database design -

CREATE TABLE "OPS$1007022"."SQLI"

( "USERNAME" VARCHAR2(10 BYTE),

"PASSWORD" VARCHAR2(10 BYTE)

) SEGMENT CREATION IMMEDIATE

PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255

NOCOMPRESS LOGGING

STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645

PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1

BUFFER\_POOL DEFAULT FLASH\_CACHE DEFAULT CELL\_FLASH\_CACHE DEFAULT)

TABLESPACE "USERS" ;

MySQL test database design -

CREATE TABLE IF NOT EXISTS `SQLI` (

`user\_id` int(11) NOT NULL AUTO\_INCREMENT,

`User` varchar(10) NOT NULL,

`Pass` varchar(10) NOT NULL,

PRIMARY KEY (`user\_id`)

) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO\_INCREMENT=10391 ;

* Defensive coding
  + Manual defensive coding practices
  + SQL DOM
  + Parameterized query insertion
* SQLIV detection
  + SQLUnitGen
  + MUSIC
  + Vulnerability and attack injection
  + SUSHI
  + Ardilla
  + String analyser
  + PhpMinerI
  + idMAS-SQL
  + IDS-6300
* Runtime SQLIA prevention
  + SQLrand
  + AMNESIA
  + SQLCheck
  + WASP
  + SQLProb
  + CANDID
  + <http://www.greensql.com/company/about-us>
  + <http://www.modsecurity.org/about.html>
* Misc
  + SQLGuard, CSSE, IDS, Java Dynamic Tainting, Tautology-checker, Web App. Hardening, JDBC-Checker, Java Static Tainting, Safe Query Objects, Security gateway, SecuriFly, WAVES, WebSSARI, Acunetix Web Vulnerability Scanner, aidSQL, Gamja, Grabber, Crypto Servers, CryptDB, Netsparker, WebCruiser, SQLIPA, DIWeDa, WAMID,