CSE 484 / CSE M 584
Computer Security: SQL, Wireshark, and Policy

TA: Thomas Crosley
tcrosley@cs
SQL Review

• Structured Query Language (SQL) used to communicate with databases
• Standard SQL commands SELECT, INSERT, UPDATE, DROP
More important SQL Commands

• **SELECT** - extracts data from a database
• **UPDATE** - updates data in a database
• **DELETE** - deletes data from a database
• **INSERT INTO** - inserts new data into a database
• **CREATE TABLE** - creates a new table
• **ALTER TABLE** - modifies a table
• **DROP TABLE** - deletes a table
Select

• Used to select (read) data from a database

• SELECT column_name, column_name
  FROM table_name
  WHERE column_name operator value;
Insert

• Insert new records in a table
  
  INSERT INTO *table_name*
  VALUES (value1,value2,value3,...);

• INSERT
  INTO *table_name* (column1,column2,...)
  VALUES (value1,value2,...);
SQL Injection

- SQL Injection allows the attacker to insert malicious SQL statements
- Usually caused by incorrect filtering or escaping of user input
Forms of SQL Injection

- 1=1
  - SELECT * FROM Users WHERE UserId = 105 or 1=1
- ‘’=‘’
  - SELECT * FROM Users WHERE Name = ‘’ or ‘’=‘’
  - SELECT * FROM Users WHERE Pass = ‘’ or ‘’=‘’
- Batched SQL Statements
  - SELECT * FROM Users; DROP TABLE Suppliers
Preventing SQL Injection

• “Sanitizing” input data
  – Can be hard to do well/completely
  – Removing SQL commands, etc.

• Escaping strings often works better
  – Each DBMS has their own version
  – Ex: mysqli_real_escape_string in MySql
SQL Injection

Hi, this is your son’s school. We’re having some computer trouble.

Oh, dear – did he break something? In a way –

DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?

Oh, yes. Little Bobby tables, we call him.

Well, we’ve lost this year’s student records. I hope you’re happy.

And I hope you’ve learned to sanitize your database inputs.

HTTP://XKCD.COM/327/
Helpful resources

• SQL Injection – OWASP
  https://www.owasp.org/index.php/SQL_Injection

• Cross-site Scripting (XSS)
  https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
Tech Policy

• Talk to your neighbors
• Write down 2 or more concerns you have about security
• Write down 2 or more security related policy issues you think would be hard to come up with a policy for
Wireshark

• Free tool to inspect incoming and outgoing packets on HTTP/TCP/Ethernet/etc.

• Notice
  – Massive streams of data to load a single website
  – How many requests are being made to 3rd parties
  – Most content (including cookies) are sent in plaintext

https://www.wireshark.org/