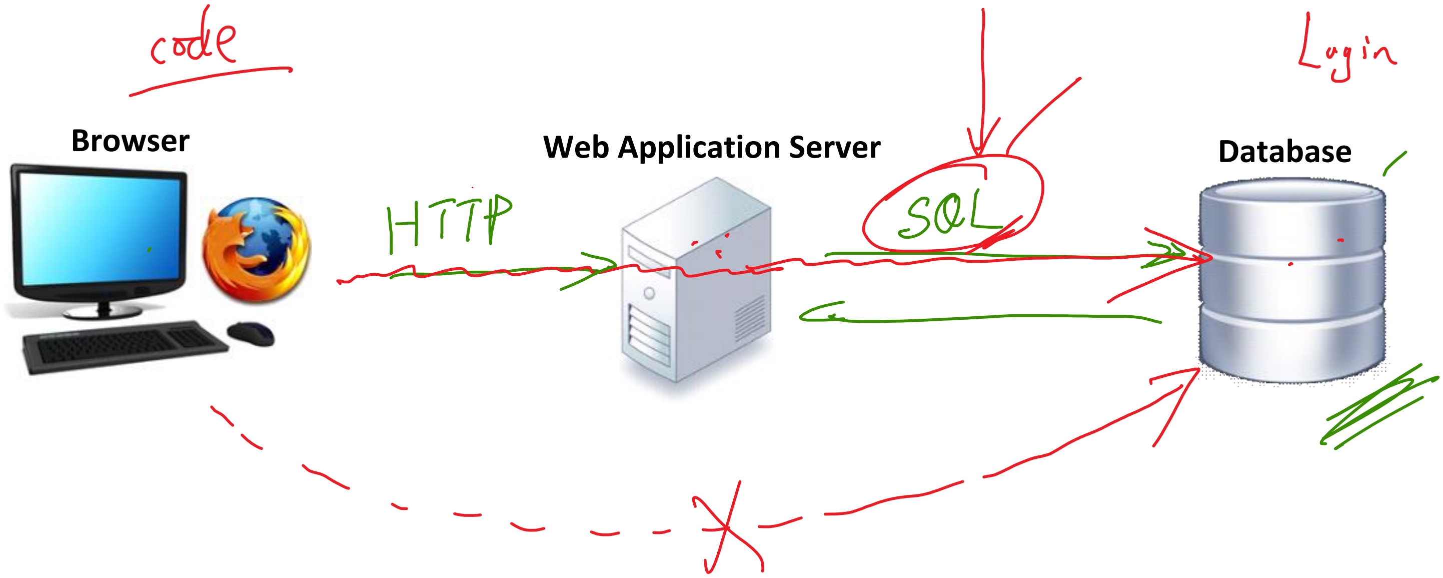
SQL Injection Attack

SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

SQL Tutorial

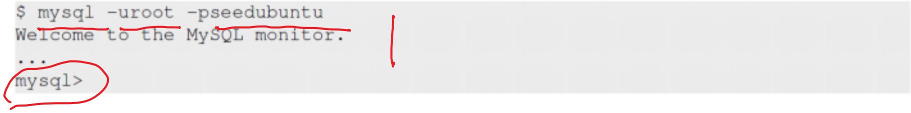
SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Web Application Architecture



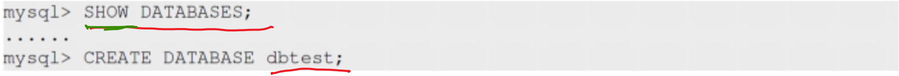
Database Setup

❖ Log into MySQL



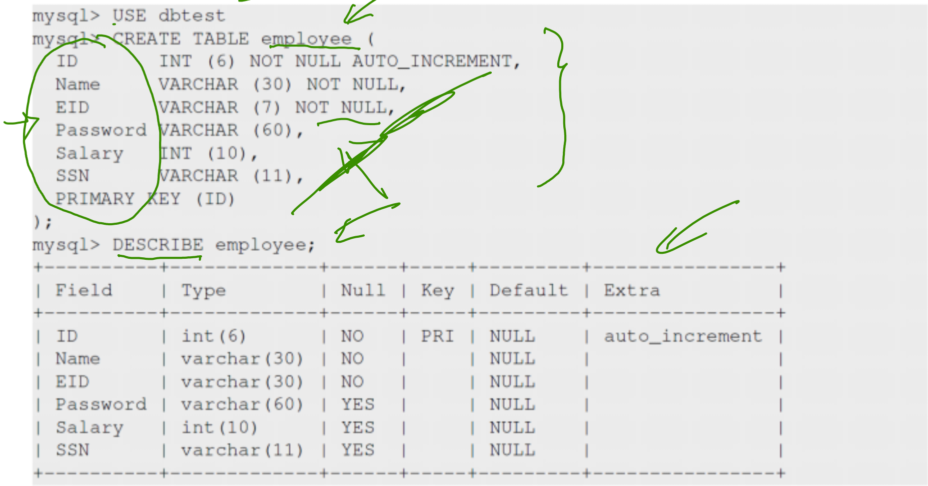
```
$ mysql -uroot -pseedubuntu
Welcome to the MySQL monitor.
...
mysql>
```

❖ Create a database



```
mysql> SHOW DATABASES;
......
mysql> CREATE DATABASE dbtest;
```

❖ Create a table



```
mysql> USE dbtest
mysql> CREATE TABLE employee (
   ID       INT (6) NOT NULL AUTO_INCREMENT,
   Name     VARCHAR (30) NOT NULL,
   EID      VARCHAR (7) NOT NULL,
   Password VARCHAR (60),
   Salary   INT (10),
   SSN      VARCHAR (11),
   PRIMARY KEY (ID)
);
mysql> DESCRIBE employee;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| ID       | int(6)      | NO   | PRI | NULL    | auto_increment |
| Name     | varchar(30) | NO   |     | NULL    |                |
| EID      | varchar(30) | NO   |     | NULL    |                |
| Password | varchar(60) | YES  |     | NULL    |                |
| Salary   | int(10)     | YES  |     | NULL    |                |
| SSN      | varchar(11) | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
```

MySQL

↓

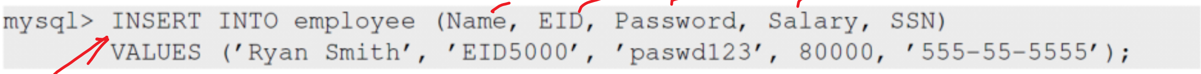
Databases

↓

Tables

Query and Update Database

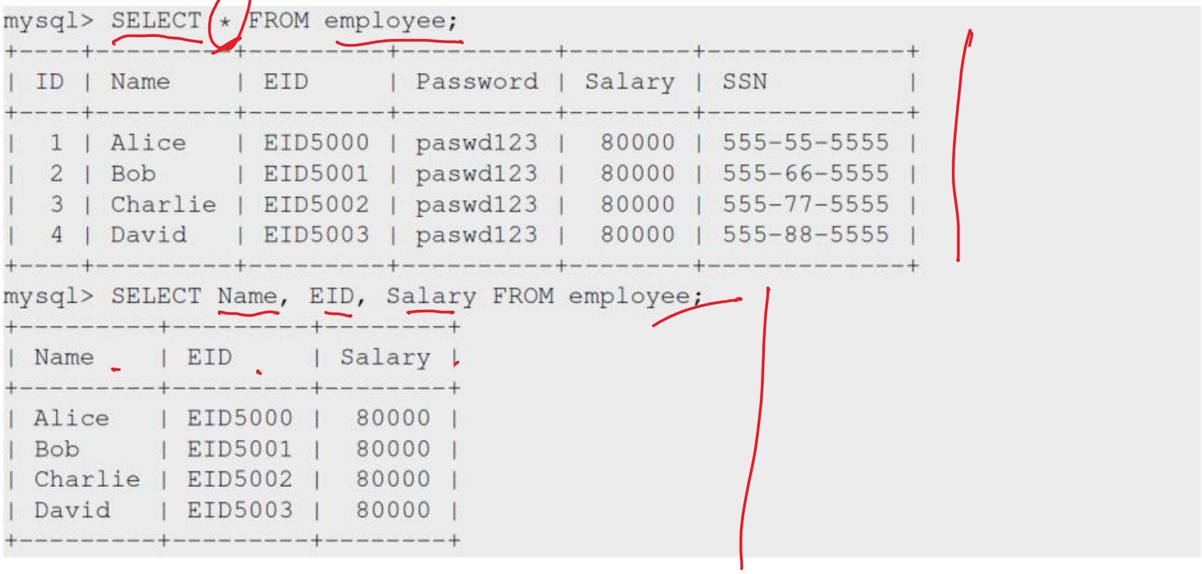
❖ Insert a record: "INSERT INTO" statement



```
mysql> INSERT INTO employee (Name, EID, Password, Salary, SSN)
    VALUES (’Ryan Smith’, ’EID5000’, ’paswd123’, 80000, ’555-55-5555’);
```

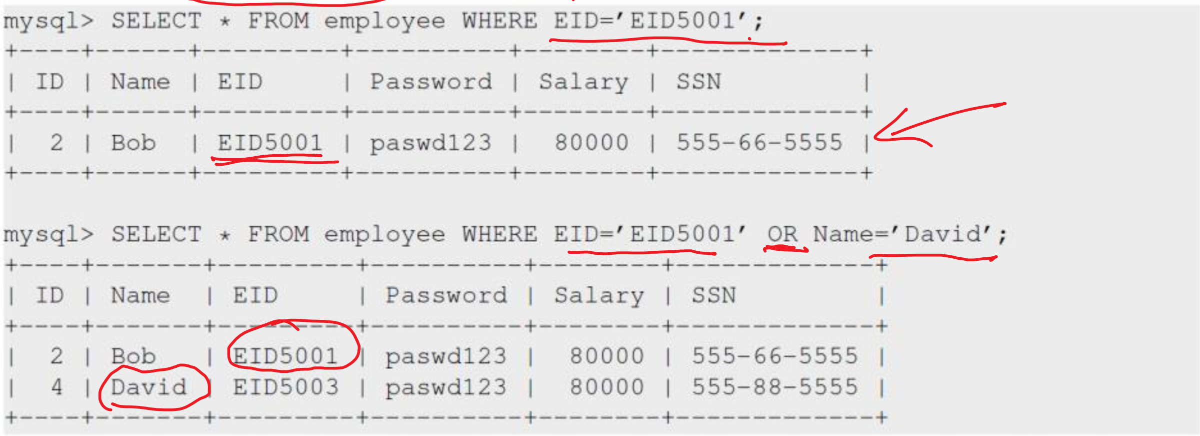
❖ Query a database: SELECT statement

Cdl



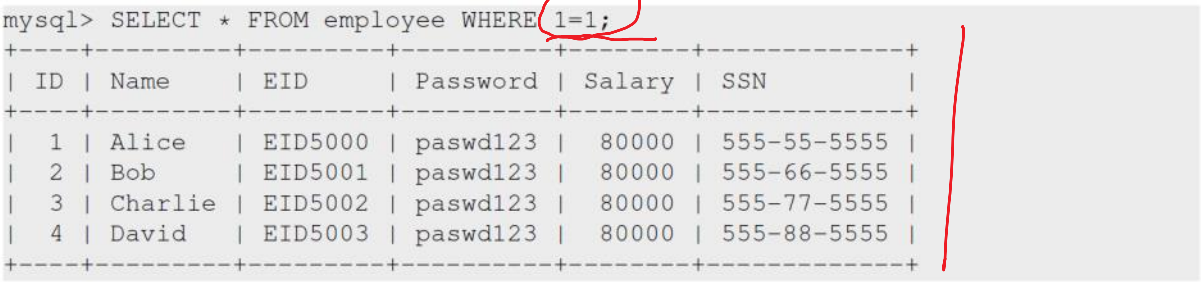
```
mysql> SELECT * FROM employee;
+----+---------+---------+----------+--------+-------------+
| ID | Name    | EID     | Password | Salary | SSN         |
+----+---------+---------+----------+--------+-------------+
|  1 | Alice   | EID5000 | paswd123 |  80000 | 555-55-5555 |
|  2 | Bob     | EID5001 | paswd123 |  80000 | 555-66-5555 |
|  3 | Charlie | EID5002 | paswd123 |  80000 | 555-77-5555 |
|  4 | David   | EID5003 | paswd123 |  80000 | 555-88-5555 |
+----+---------+---------+----------+--------+-------------+
mysql> SELECT Name, EID, Salary FROM employee;
+---------+---------+--------+
| Name    | EID     | Salary |
+---------+---------+--------+
| Alice   | EID5000 |  80000 |
| Bob     | EID5001 |  80000 |
| Charlie | EID5002 |  80000 |
| David   | EID5003 |  80000 |
+---------+---------+--------+
```

❖ Conditions: WHERE clause



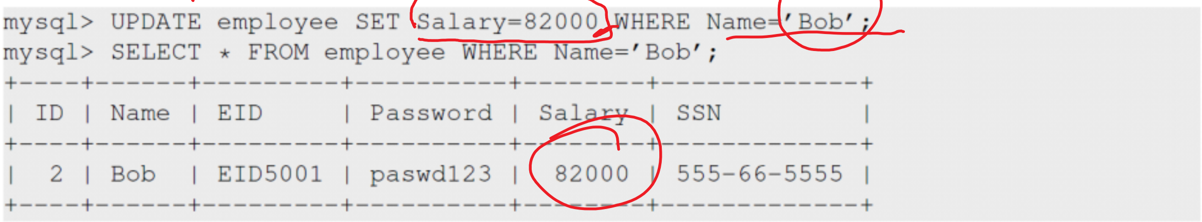
```
mysql> SELECT * FROM employee WHERE EID=’EID5001’;
+----+------+---------+----------+--------+-------------+
| ID | Name | EID     | Password | Salary | SSN         |
+----+------+---------+----------+--------+-------------+
|  2 | Bob  | EID5001 | paswd123 |  80000 | 555-66-5555 |
+----+------+---------+----------+--------+-------------+

mysql> SELECT * FROM employee WHERE EID=’EID5001’ OR Name=’David’;
+----+-------+---------+----------+--------+-------------+
| ID | Name  | EID     | Password | Salary | SSN         |
+----+-------+---------+----------+--------+-------------+
|  2 | Bob   | EID5001 | paswd123 |  80000 | 555-66-5555 |
|  4 | David | EID5003 | paswd123 |  80000 | 555-88-5555 |
+----+-------+---------+----------+--------+-------------+
```

❖ A special condition



```
mysql> SELECT * FROM employee WHERE 1=1;
+----+---------+---------+----------+--------+-------------+
| ID | Name    | EID     | Password | Salary | SSN         |
+----+---------+---------+----------+--------+-------------+
|  1 | Alice   | EID5000 | paswd123 |  80000 | 555-55-5555 |
|  2 | Bob     | EID5001 | paswd123 |  80000 | 555-66-5555 |
|  3 | Charlie | EID5002 | paswd123 |  80000 | 555-77-5555 |
|  4 | David   | EID5003 | paswd123 |  80000 | 555-88-5555 |
+----+---------+---------+----------+--------+-------------+
```

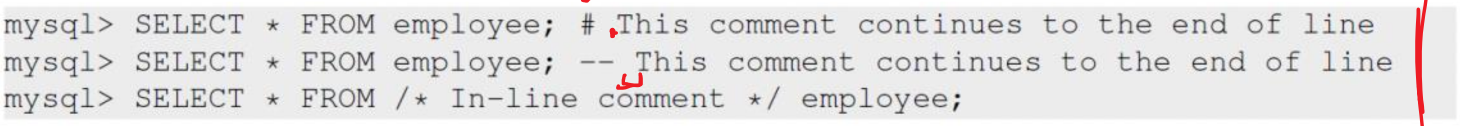
❖ Update an existing record: UPDATE statement



```
mysql> UPDATE employee SET Salary=82000 WHERE Name=’Bob’;
mysql> SELECT * FROM employee WHERE Name=’Bob’;
+----+------+---------+----------+--------+-------------+
| ID | Name | EID     | Password | Salary | SSN         |
+----+------+---------+----------+--------+-------------+
|  2 | Bob  | EID5001 | paswd123 |  82000 | 555-66-5555 |
+----+------+---------+----------+--------+-------------+
```

Comments

❖ Comments in SQL statement

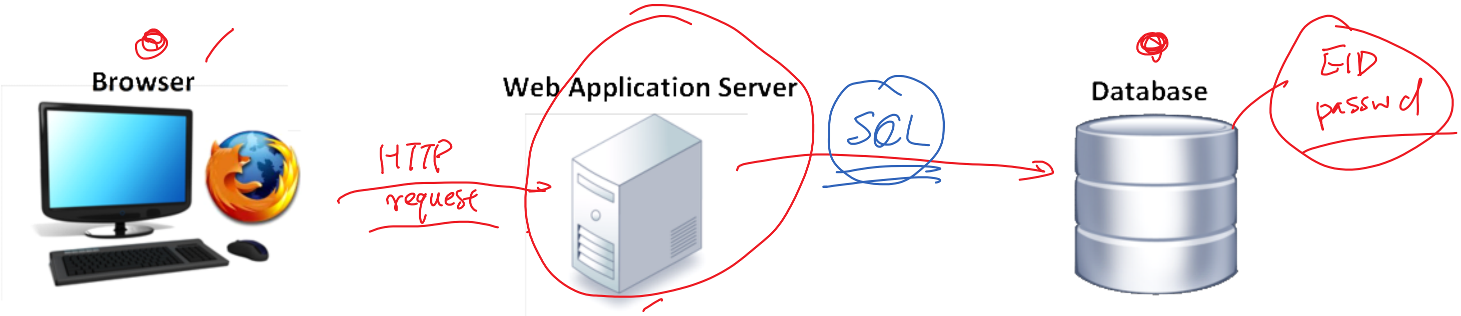


```
mysql> SELECT * FROM employee; # This comment continues to the end of line
mysql> SELECT * FROM employee; -- This comment continues to the end of line
mysql> SELECT * FROM /* In-line comment */ employee;
```

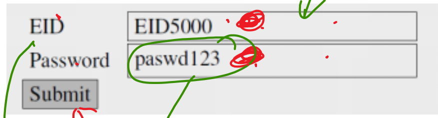
How Web Applications Interact With a Database

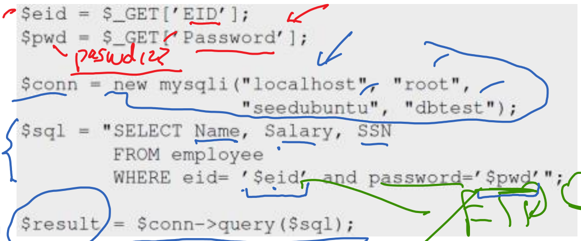
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Programming Involved



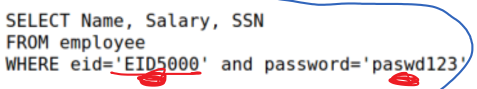
EID5000





```
$eid = $_GET['EID'];
$pwd = $_GET['Password'];
$conn = new mysqli("localhost", "root",
                   "seedubuntu", "dbtest");
$sql = "SELECT Name, Salary, SSN
        FROM employee
        WHERE eid= '$eid' and password='$pwd'";
$result = $conn->query($sql);
```

paswd123



```
SELECT Name, Salary, SSN
FROM employee
WHERE eid='EID5000' and password='paswd123'
```

hash( )

EID (/* */0

hash ($pwd)

curl

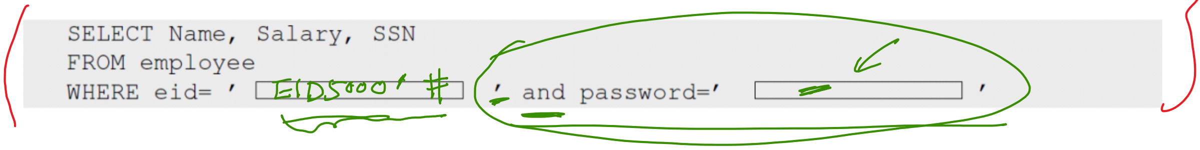
curl http:// - - - / .php? EID= & password =

SQL Injection: Steal Information

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

SQL Injection: Step 1

❖ User input



```
SELECT Name, Salary, SSN
FROM employee
WHERE eid= ' [EID5000' #] ' and password=' [        ] '
```

→ Database

❖ Question

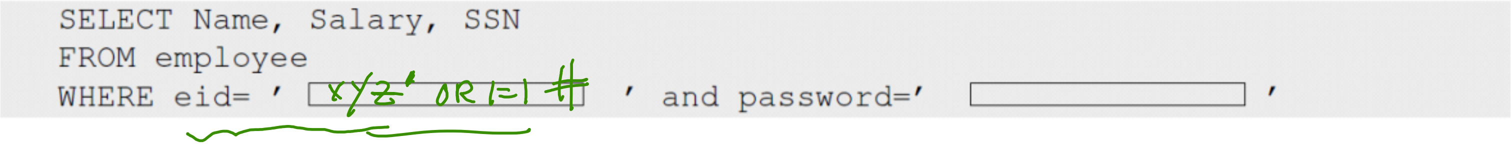
If you know an eid, but you don't know the password, can you get the database to return the data for the eid?

EID5000

← use comment
- #
- -- ␣

SQL Injection: Step 2

❖ User input



```
SELECT Name, Salary, SSN
FROM employee
WHERE eid= ' xyz' OR 1=1 #  ' and password=' □ '
```

❖ Question

If you don't know an eid or password, can you get the database to return the information for a record?

SQL Injection: Modify Database

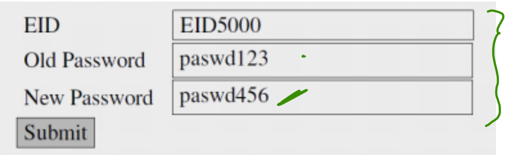
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Change Your Own Salary

❖ Attack objective

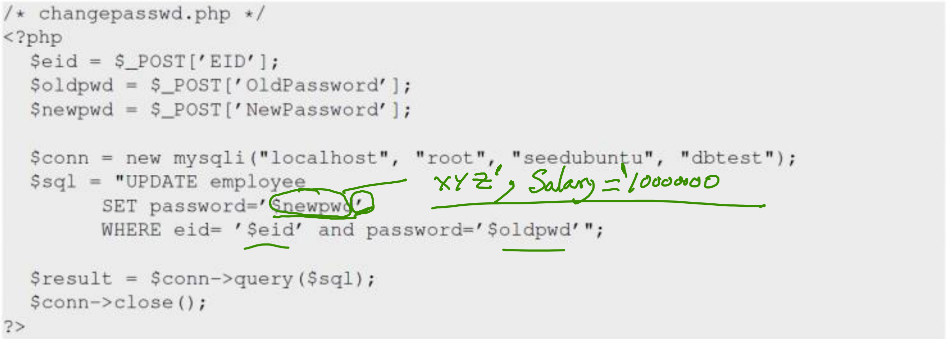
You are not happy with the salary that you get. Can you use the vulnerability to change your salary?

❖ Change-password form



EID	EID5000
Old Password	paswd123
New Password	paswd456

❖ Change-password script



```
/* changepasswd.php */
<?php
  $eid = $_POST['EID'];
  $oldpwd = $_POST['OldPassword'];
  $newpwd = $_POST['NewPassword'];

  $conn = new mysqli("localhost", "root", "seedubuntu", "dbtest");
  $sql = "UPDATE employee
        SET password='$newpwd'
        WHERE eid= '$eid' and password='$oldpwd'";

  $result = $conn->query($sql);
  $conn->close();
?>
```

xyz', Salary='1000000

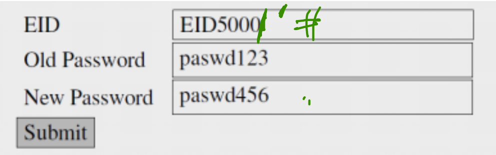
Hint: Updat table SET field1='_', field2='_', ...

Change Your Boss's Salary

❖ Attack objective

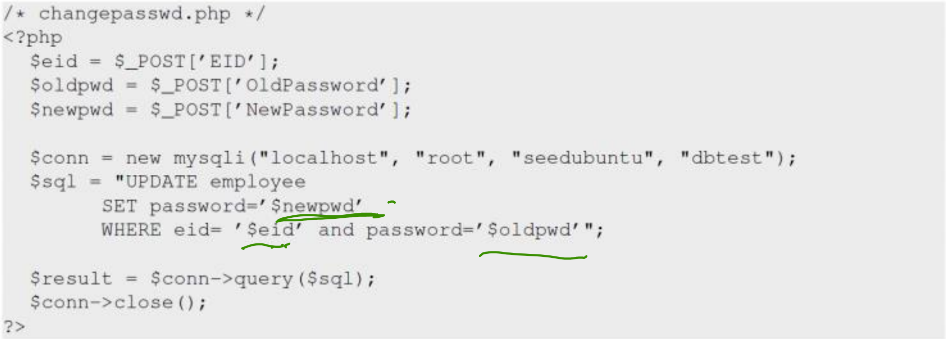
You hate your boss (EID5001). Can you use the vulnerability to change his/her salary?

❖Change-password form



EID	EID50001' #
Old Password	paswd123
New Password	paswd456

❖Change-password script



```
/* changepasswd.php */
<?php
  $eid = $_POST['EID'];
  $oldpwd = $_POST['OldPassword'];
  $newpwd = $_POST['NewPassword'];

  $conn = new mysqli("localhost", "root", "seedubuntu", "dbtest");
  $sql = "UPDATE employee
        SET password='$newpwd'
        WHERE eid= '$eid' and password='$oldpwd'";

  $result = $conn->query($sql);
  $conn->close();
?>
```

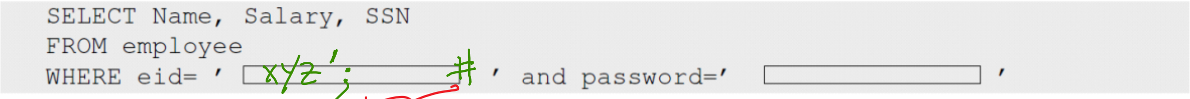
Turn One SQL Statement Into Multiple Statements

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Run an Arbitrary SQL Statement

MySQL

❖ User input



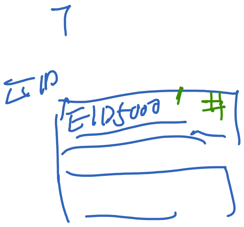
```
SELECT Name, Salary, SSN
FROM employee
WHERE eid= ' [xyz';          #] ' and password=' [                    ] '
```

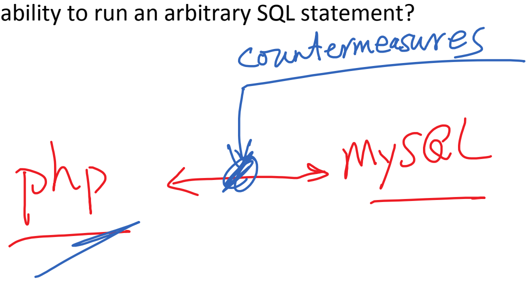
new command

❖ Question

Can you use this SQL injection vulnerability to run an arbitrary SQL statement?

system(cmd)

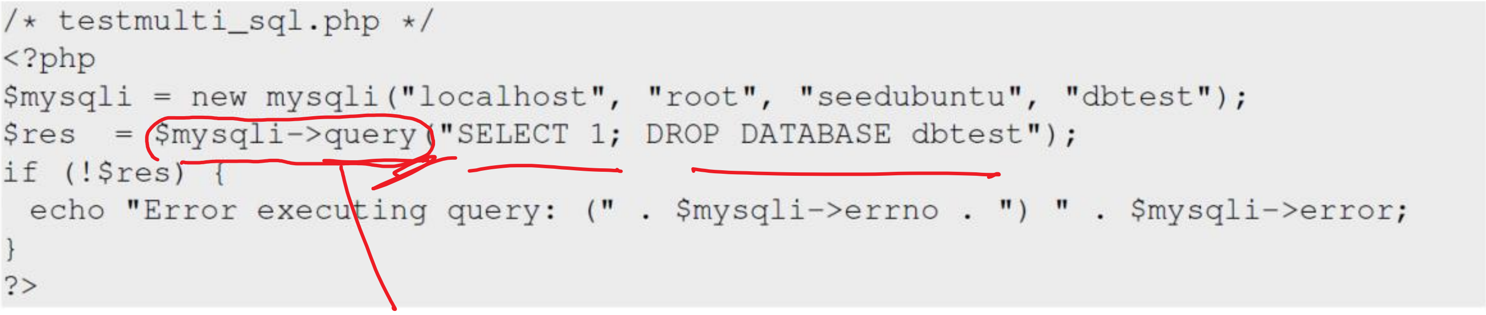




cmd; cmd

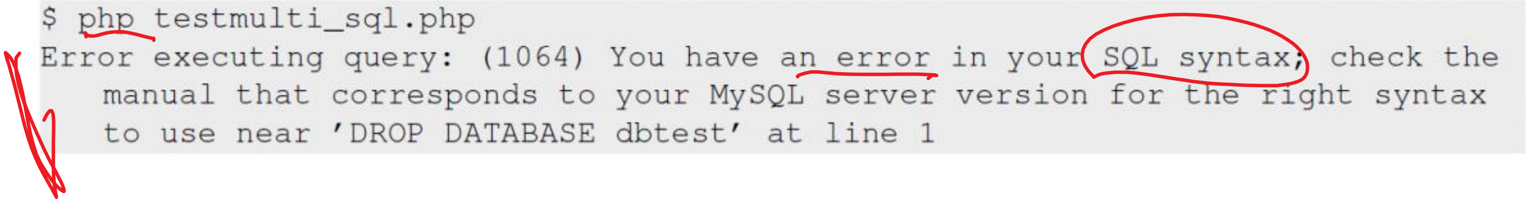
Experiment

❖ Run multiple SQL statements



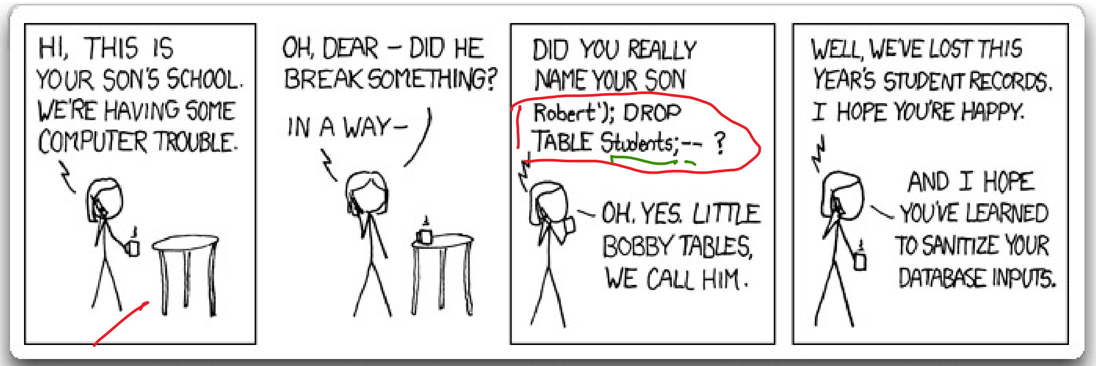
```
/* testmulti_sql.php */
<?php
$mysqli = new mysqli("localhost", "root", "seedubuntu", "dbtest");
$res   = $mysqli->query("SELECT 1; DROP DATABASE dbtest");
if (!$res) {
  echo "Error executing query: (" . $mysqli->errno . ") " . $mysqli->error;
}
?>
```

❖ Error message



```
$ php testmulti_sql.php
Error executing query: (1064) You have an error in your SQL syntax; check the
    manual that corresponds to your MySQL server version for the right syntax
    to use near 'DROP DATABASE dbtest' at line 1
```

SQL Injection Comic Strip


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.

(Source: https://xkcd.com/327/)

Robert');

Name '

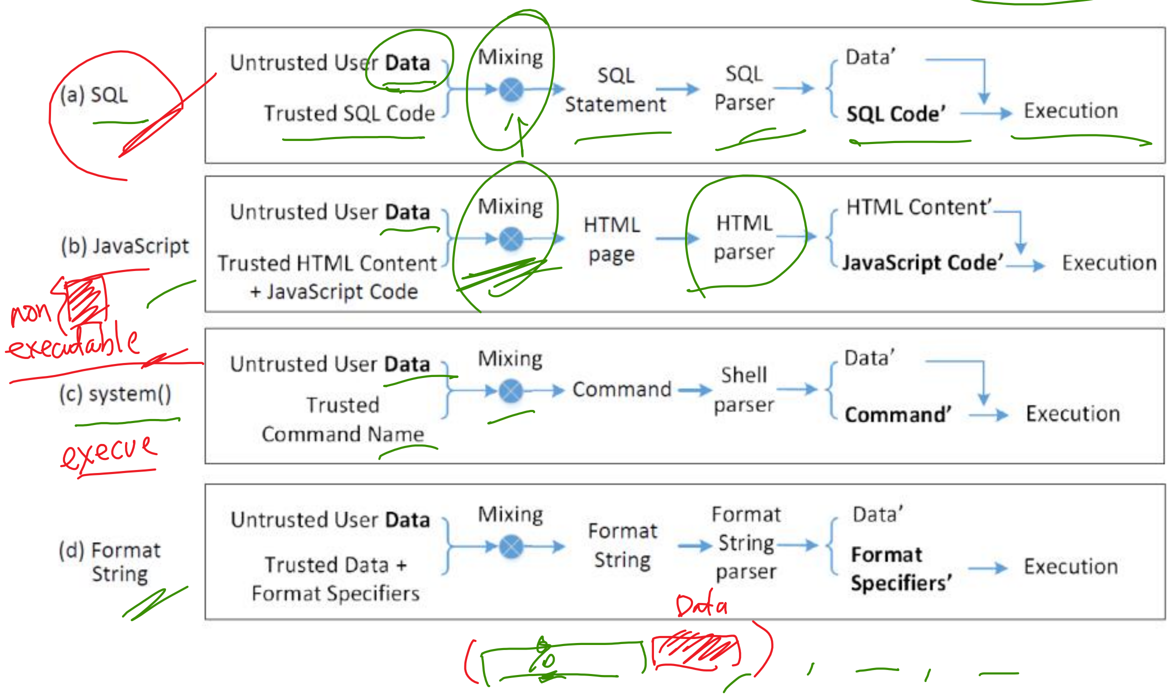
passwd

The Fundamental Cause

SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Similarity Among Code-Injection Attacks

' # OR =



SQL

XSS

cmd = "/bin/cat file"

; cmd

"code"

%s %n %x

Countermeasures

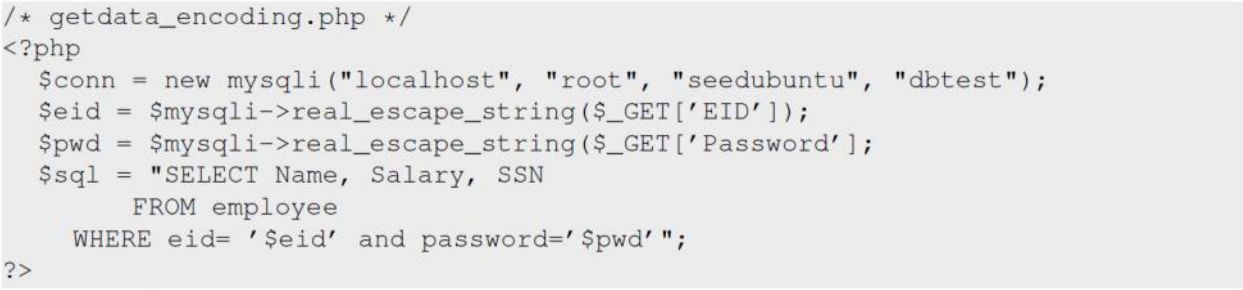
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Encoding Special Characters

❖ **Apache's configuration**

"`magic_quotes_gpc = On`" in php.ini

❖ **PHP's solution: `mysqli::real_escape_string()`**



```
/* getdata_encoding.php */
<?php
  $conn = new mysqli("localhost", "root", "seedubuntu", "dbtest");
  $eid = $mysqli->real_escape_string($_GET['EID']);
  $pwd = $mysqli->real_escape_string($_GET['Password'];
  $sql = "SELECT Name, Salary, SSN
        FROM employee
    WHERE eid= '$eid' and password='$pwd'";
?>
```

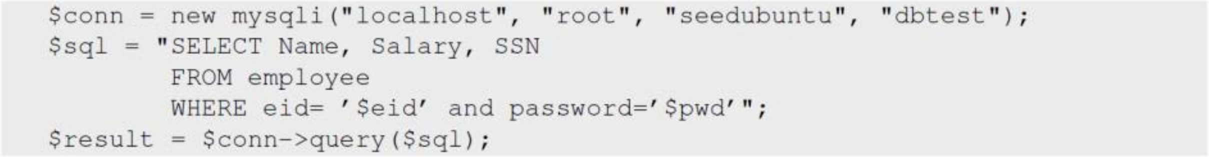
Solving the Fundamental Problem

Review: How do we defend against the attack on system()?

How Prepared Statements Work

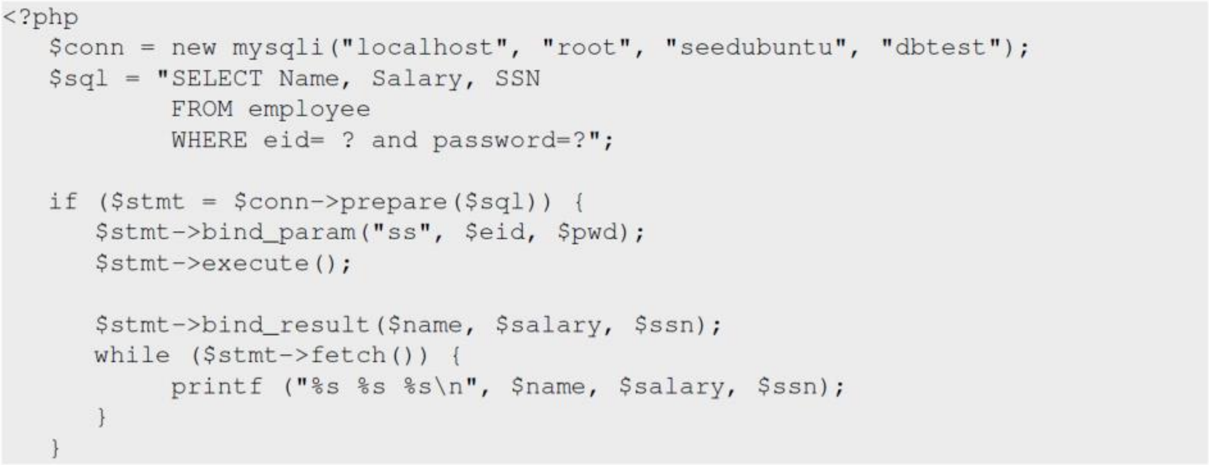
Prepared Statement: Example

❖ The vulnerable approach



```
   $conn = new mysqli("localhost", "root", "seedubuntu", "dbtest");
   $sql = "SELECT Name, Salary, SSN
           FROM employee
           WHERE eid= ’$eid’ and password=’$pwd’";
   $result = $conn->query($sql);
```

❖ Using prepared statement



```
<?php
   $conn = new mysqli("localhost", "root", "seedubuntu", "dbtest");
   $sql = "SELECT Name, Salary, SSN
           FROM employee
           WHERE eid= ? and password=?";

   if ($stmt = $conn->prepare($sql)) {
      $stmt->bind_param("ss", $eid, $pwd);
      $stmt->execute();

      $stmt->bind_result($name, $salary, $ssn);
      while ($stmt->fetch()) {
            printf ("%s %s %s\n", $name, $salary, $ssn);
      }
   }
```

Questions

- **Question 1: What do SQL injection and attacks on the `system()` function have in common?**

- **Question 2: What do their countermeasures have in common?**

Summary

- SQL statement
- SQL injection
- Countermeasures