



SQL Injection

Session 1

Announcements

- Intern applications are due this Friday (10/19) @ 11:59pm: tinyurl.com/ACM-intern-app
- Attendance Code: **yaysql**



Before we start..

- 1. Introduction**
- 2. Questions**
- 3. A Message to Beginners**



Topic Overview

1. **Authentication Bypass SQL Injection**
2. **Error Based SQL Injection**
3. **Union Based SQL Injection**



What is SQL?

Structured Query Language

A standardized language used to interact with databases.

```
SELECT * FROM users WHERE username='aaron'  
AND password='test';
```



What is SQL Injection?



facebook®



NETFLIX





The Rainforest Puppy



“.. According to them [Microsoft],
what you are about to read is **not a
problem**, so don't worry about doing
anything to stop it.”



Authentication Bypass

SQL Injection



SQL Injection Demo



```
SELECT * FROM users WHERE username='aaron'  
AND password='test';
```

username

aaron

password

test

users

username	password
aaron	test
patty	yellow



SELECT * **FROM** users ← **select**
WHERE username='aaron' | ← **filter**
AND password='test';

users	
username	password
aaron	test
patty	yellow



SQL Select

```
SELECT column1, column2, ... FROM table;
```

Employee ID	FirstName	LastName	HireDate	City
1	Nancy	Davolio	1/5/1992	Seattle
2	Janet	Leverling	1/4/1992	Kirkland



SQL Select

```
SELECT * FROM Table1;
```

Employee ID	FirstName	LastName	HireDate	City
1	Nancy	Davolio	1/5/1992	Seattle
2	Janet	Leverling	1/4/1992	Kirkland



SQL Select Activity

Activity:

1. https://sqlbolt.com/lesson/select_queries_introduction
https://sqlbolt.com/lesson/select_queries_with_constraints
https://sqlbolt.com/lesson/select_queries_with_constraints_pt_2



SQL Select

```
SELECT FirstName FROM Table1;
```

Employee ID	FirstName	LastName	HireDate	City
1	Nancy	Davolio	1/5/1992	Seattle
2	Janet	Leverling	1/4/1992	Kirkland



SQL Select

```
SELECT FirstName, City FROM Table1;
```

Employee ID	FirstName	LastName	HireDate	City
1	Nancy	Davolio	1/5/1992	Seattle
2	Janet	Leverling	1/4/1992	Kirkland



SQL Select

```
SELECT FirstName, City FROM Table1  
WHERE FirstName='Nancy';
```

Employee ID	FirstName	LastName	HireDate	City
1	Nancy	Davolio	1/5/1992	Seattle
2	Janet	Leverling	1/4/1992	Kirkland



Activity 1: Select Queries 101

Find the **title** and **director** of each film:

```
SELECT title, director FROM movies;
```



Activity 2: Queries with Constraints (pt 1)

Find the movies **not** released in the years between **2000** and **2010**:

```
SELECT * FROM movies WHERE year NOT BETWEEN 2000 and 2010;
```



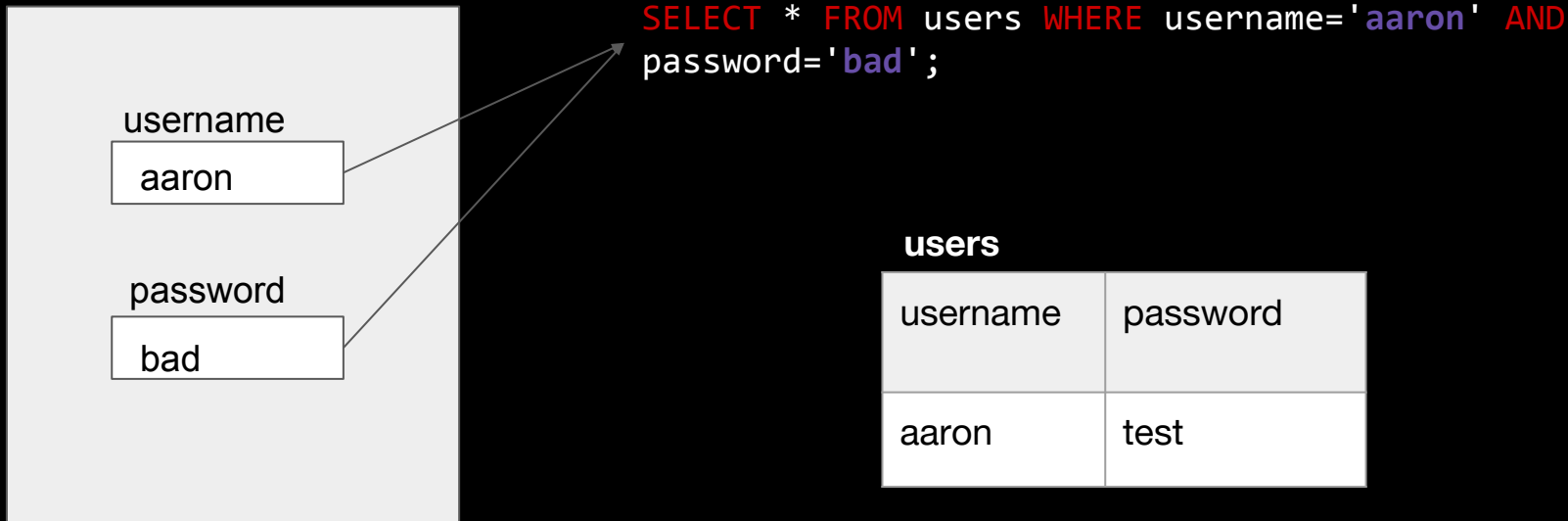
Activity 3: Queries with Constraints (pt 2)

Find all the movies directed by John Lasseter:

```
SELECT * FROM movies WHERE director='John Lasseter'
```



How does SQL Injection work?



How does SQL Injection work?

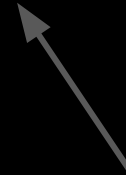
```
$result = $exec_query($query);
```

```
if($result_count == 1)
```

```
    //grant access
```

```
else
```

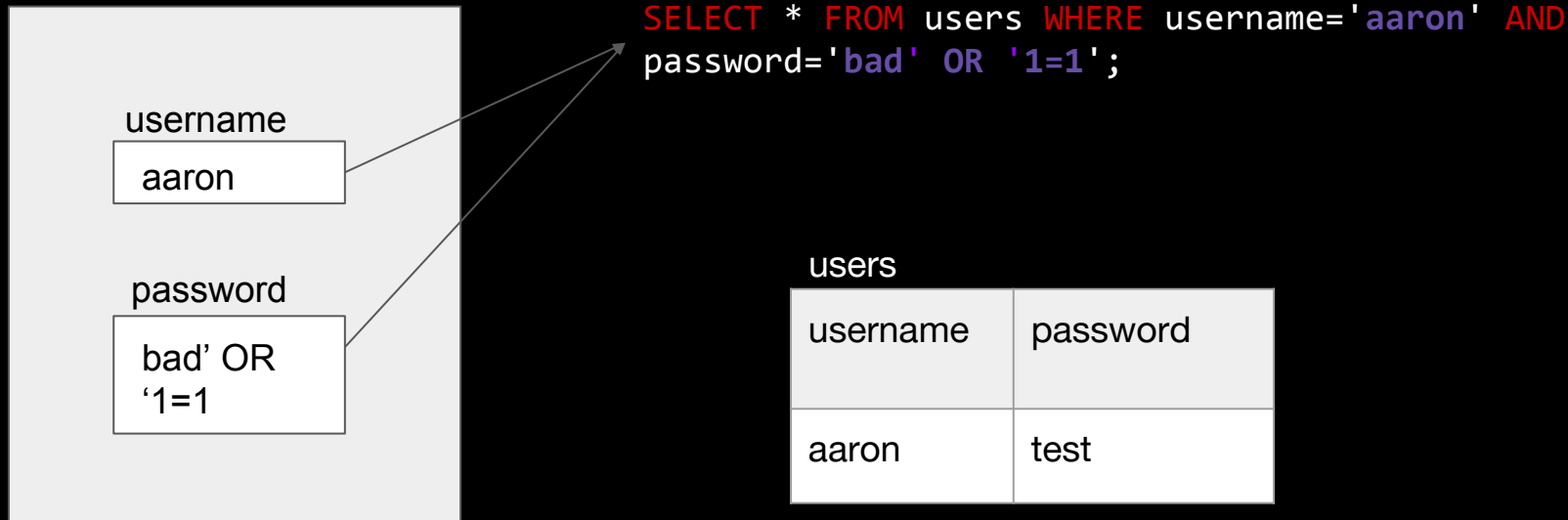
```
    //deny access
```



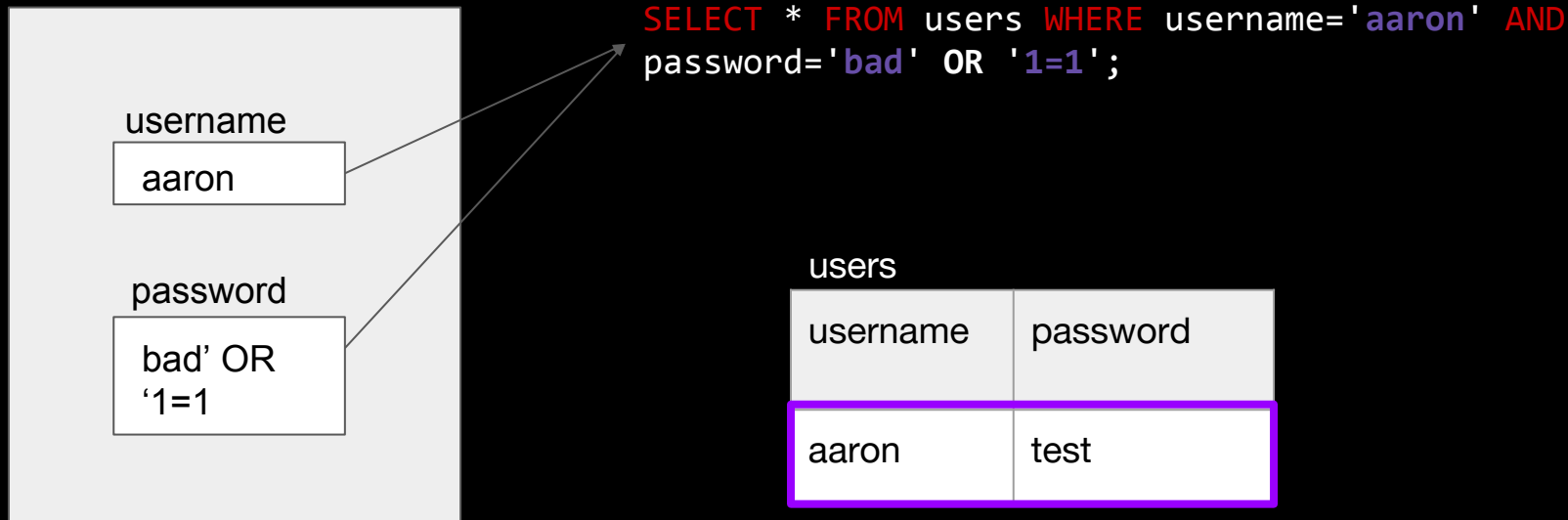
SQL Query



How does SQL Injection work?



How does SQL Injection work?



SQL Injection:

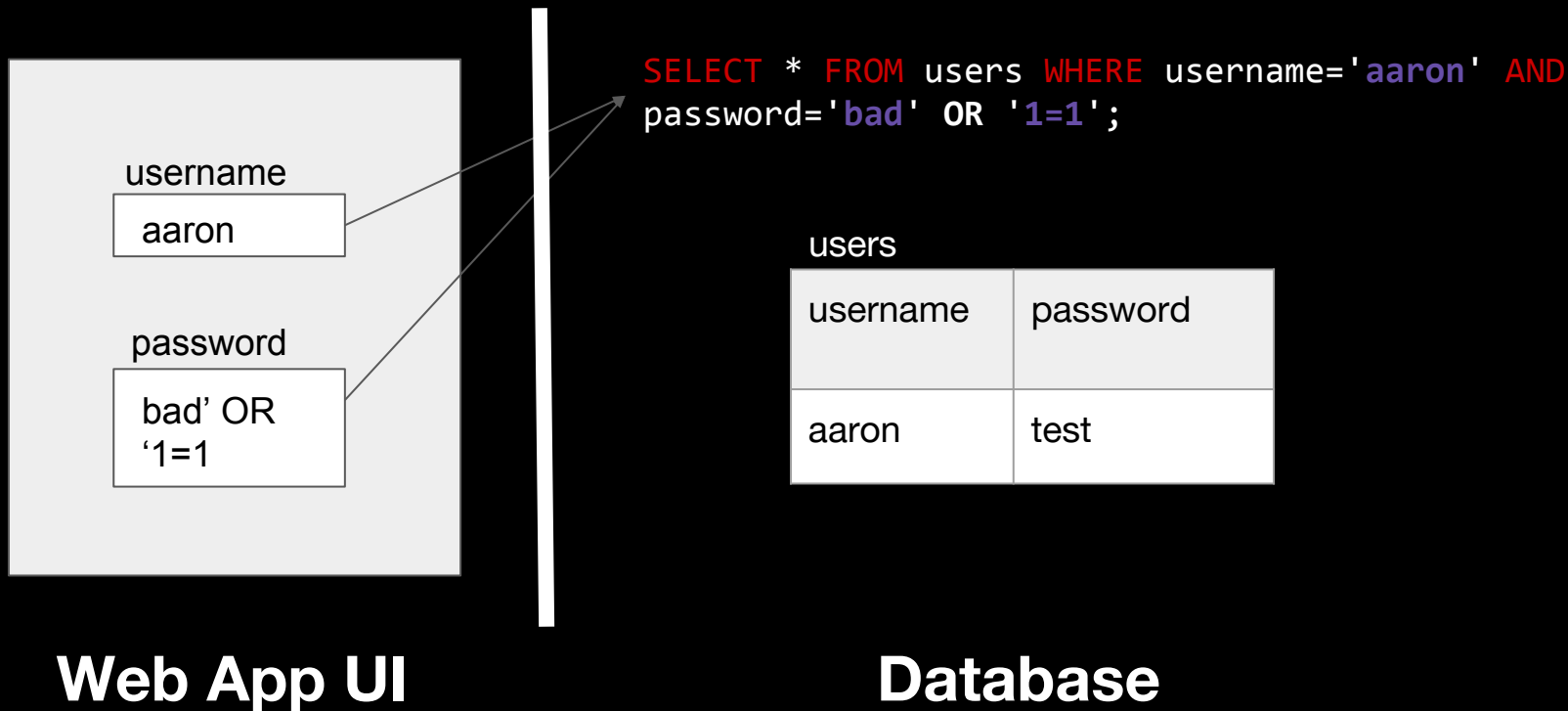
A code injection technique in which **sneaky** SQL statements are inserted into a query to manipulate the SQL database or bypass authentication.



Sometimes you have to **guess what an SQL query might look like to perform SQL injection.**



How does SQL Injection work?



SQL Injection Activity

```
SELECT * FROM users WHERE password = '$password' AND  
        username = '$username';
```

<https://junkaiong11.000webhostapp.com/index.php>



Error Based SQL Injection



<http://hack-yourself-first.com/>



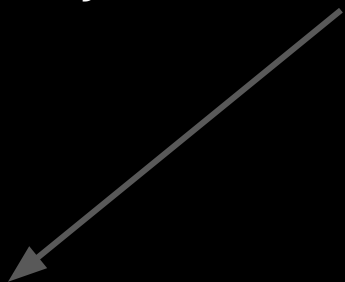
Error Based SQL Injection

URL:

`http://hack-yourself-first.com/CarsByCylinders?Cylinders=V6`

SQL Query:

`SELECT name, id FROM cars WHERE cylinders='V6'`



Error Based SQL Injection

URL:

`http://hack-yourself-first.com/CarsByCylinders?Cylinders=V6'`

SQL Query:

`SELECT name, id FROM cars WHERE cylinders='V6'`



ERROR!



Union Based SQL Injection



Union Based SQL Injection

Combine the results of two or more select statements

1. Columns must have similar data types
2. Columns in select must be in the same order



Union Based SQL Injection

```
SELECT City FROM Table1  
      UNION ALL  
SELECT FirstName FROM Table2;
```



Union Operator

SQL Statement:

```
SELECT City FROM Customers
UNION
SELECT FirstName FROM Employees
ORDER BY City;
```

Edit the SQL Statement, and click "Run SQL" to see the result.

Run SQL »

Result:

Number of Records: 79

City
Aachen
Adam
Albuquerque
Anchorage
Andrew
Anne
Barcelona
Barquisimeto
Bergamo

Tablename	Records
Customers	91
Categories	8
Employees	10
OrderDetails	518
Orders	196
Products	77
Shippers	3
Suppliers	29

Restore Database



Union Based Demo (sort of)



Defense?

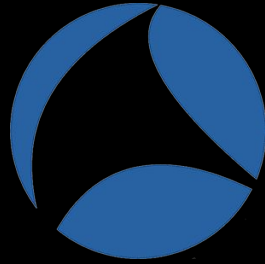


Thank You For Listening!



- 1. Feedback Form**
- 2. ACM Intern Applications**
- 3. Next Week's Track**





Wireshark Demo



How to get away with **cybercrime...**



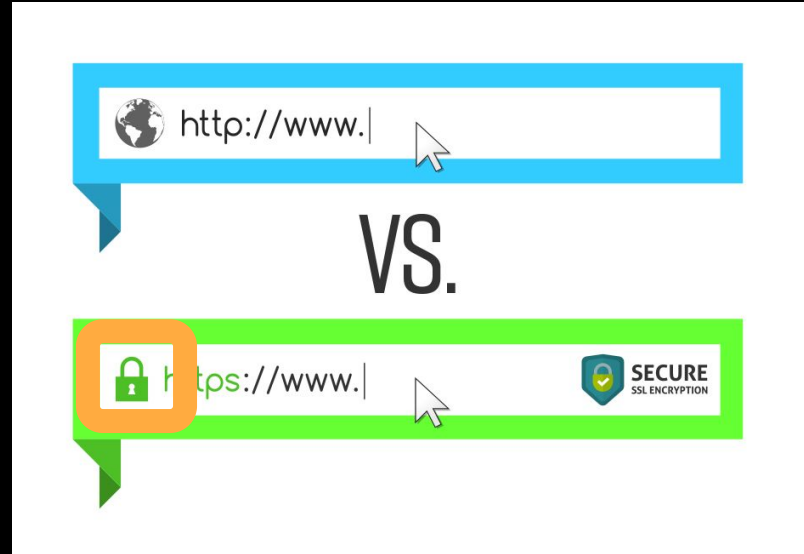
Don't let other people see you...

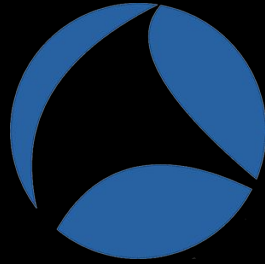


... so use **encryption!**



HTTP vs. HTTPS





Wireshark Demo





HTTP



HTTPS




Don't let other people track you down



IP Addresses (IPv4)

216.58.193.206

IP Address	Country	Region	City
216.58.193.206	United States 	California	Mountain View
ISP	Organization	Latitude	Longitude
Google LLC	Not Available	37.4060	-122.0785



IP Addresses (IPv6)

2605:e000:1313:c142:99be:f65e:599a:54cf

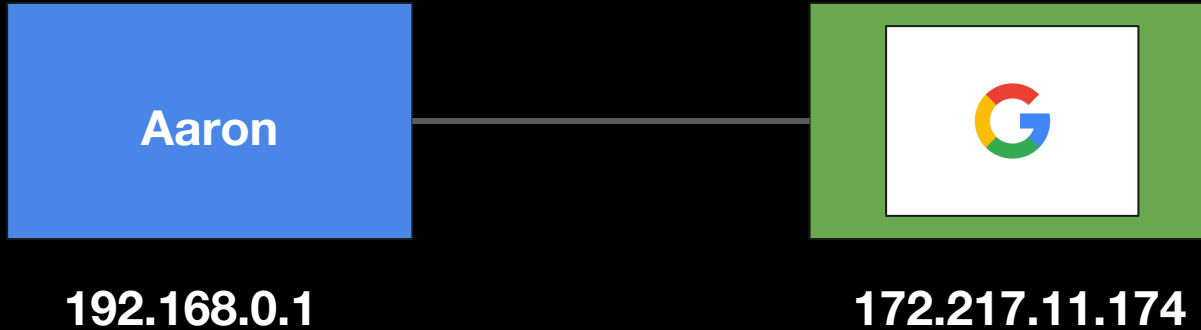
Your public IP address



[Learn more about IP addresses](#)

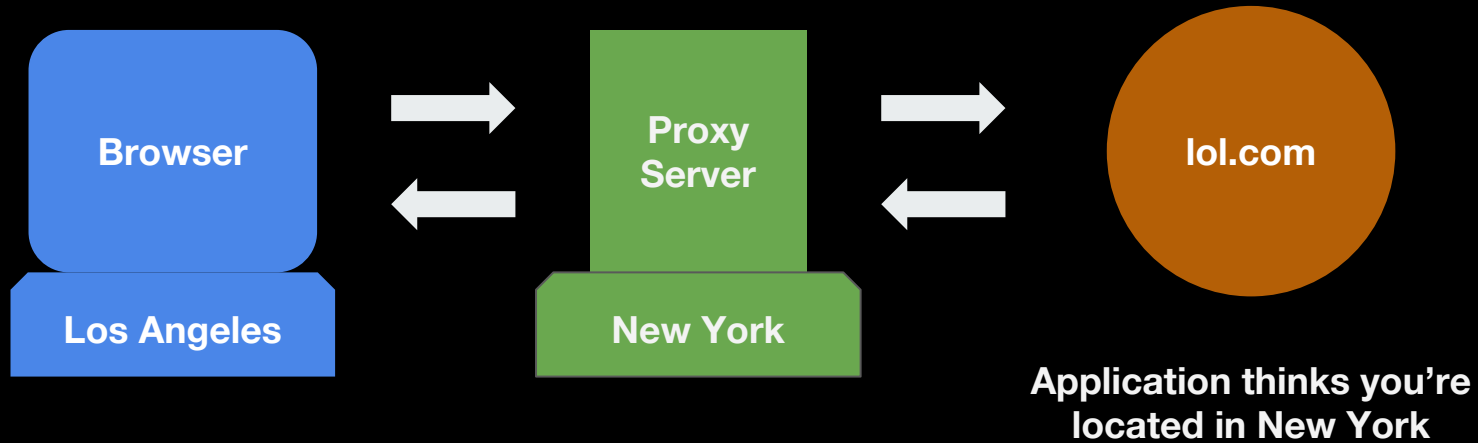


IP Addresses (IPv4)



Proxy

Intermediary endpoint between device and server.



Proxy Demo



Feedback Form

