



## The Skinny on SQL

Cybersecurity  
Web Vulnerabilities Day 3



# Today's Objectives

---

By the end of class, you will be able to:



Detect XSS with Burp Suite.



Identify and create CRUD queries with SQL.



Explain the syntax for and use WHERE clauses.



Explain the syntax and use conditional statements in SQL.

---

# Detecting XSS with Burp Suite

# Burp Intruder

---

## Using Intruder to Automate Testing for XSS Vulnerability:

01

Capture a request sent through a potentially vulnerable form.

02

Mark request data parameters for substitution.

03

Paste a set of XSS snippets as payloads.

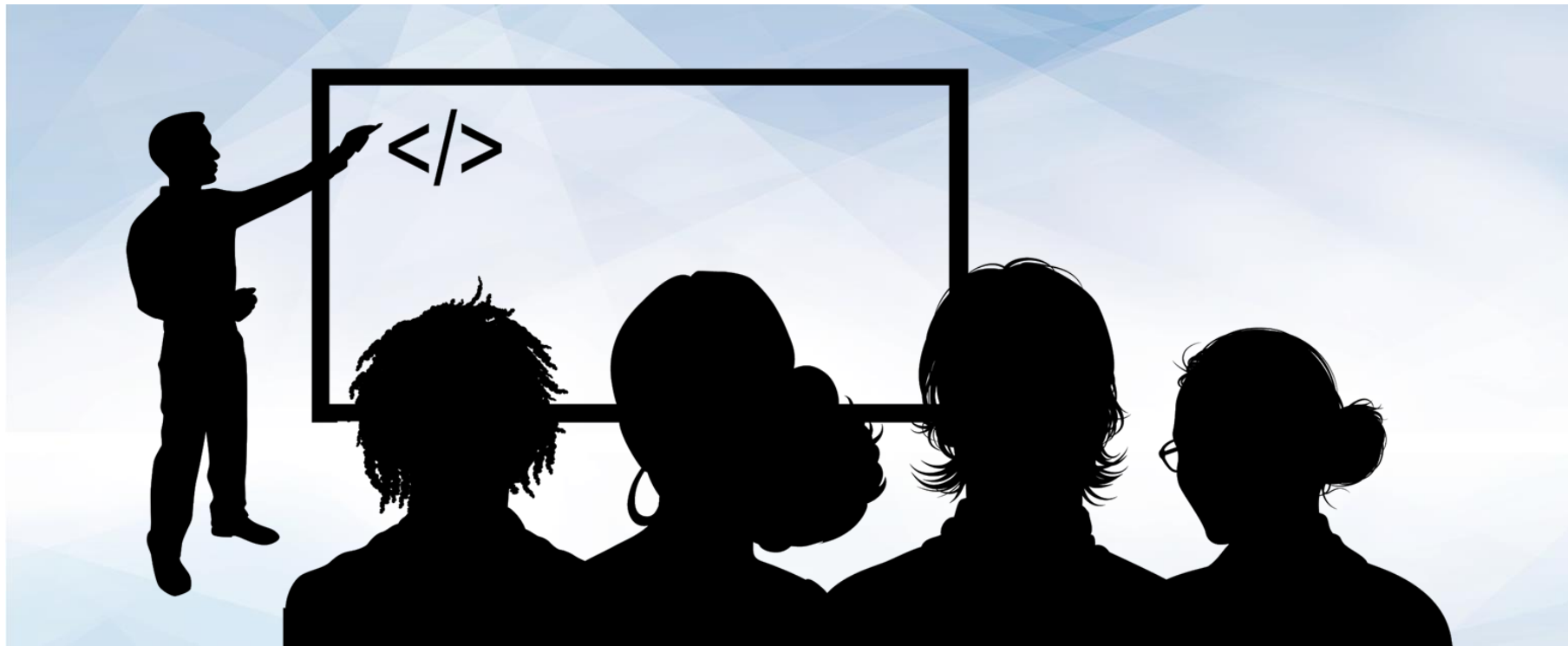
04

Run the attack.

05

Analyze response data for unsanitized ``script`` reflections, etc.

---



# Instructor Demonstration

XSS with Burp



## Activity: XSS Spraying

In this activity, you will use Burp Intruder to send XSS payloads to target a server *en masse*. Then, you'll inspect the responses to see which payloads succeeded.

[Activities/Stu\\_XSS\\_Spraying/README](#)

**Suggested Time:**  
15 Minutes



# Databases and SQL

# Databases

---

Databases are used to store large amounts of data, typically kept separate from serve machines.



Two popular databases are SQL and NoSQL. In class, we'll focus on SQL.

COLUMNS			
ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling

ROWS



# CRUD Operations

---

Once you've created a table, there are four main operations, or queries, used to interact with the data within it.



Create



Read

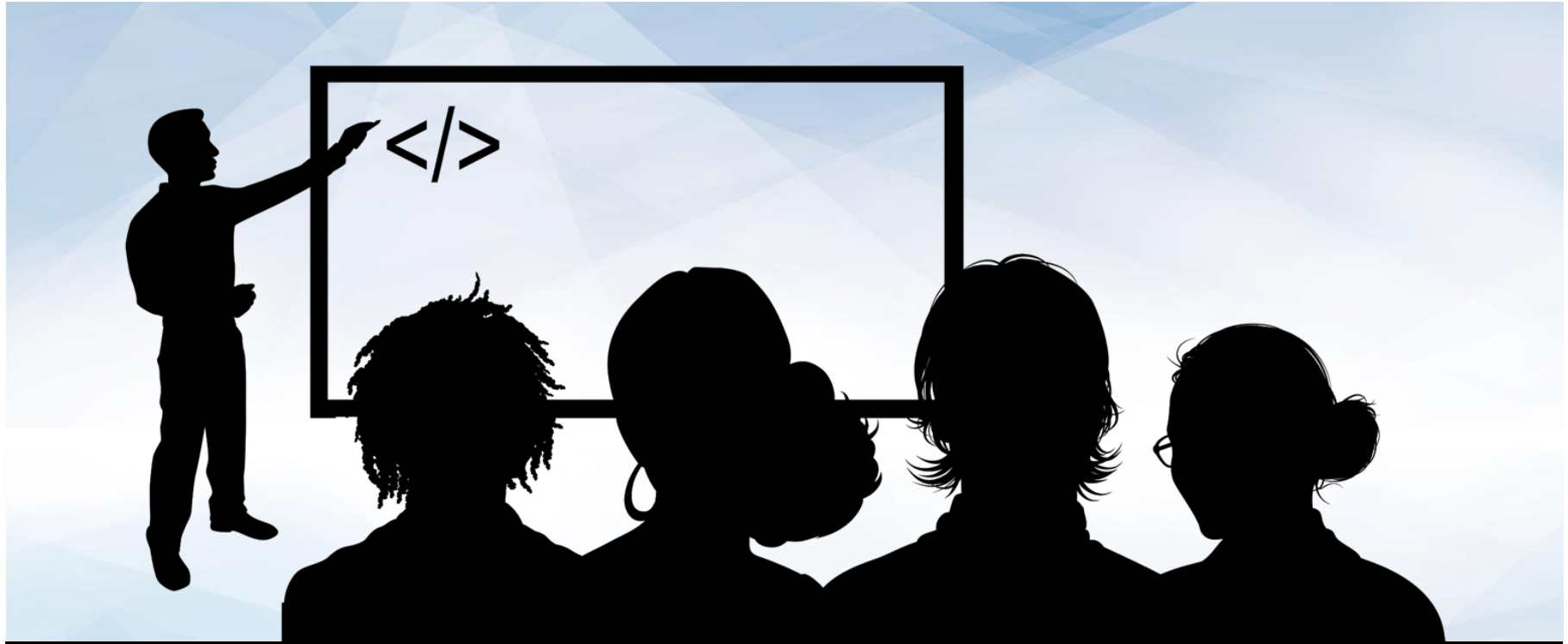


Update



Delete

---



# Instructor Demonstration

SQL

10



## Activity: Reading SQL

In this activity, you will read SQL that created databases and tables, adds data to the tables, and retrieves all records in the database.

Activities/Stu\_Reading\_SQL/README

**Suggested Time:**  
15 Minutes



# Take a Break!

---



# Where Clauses

# SELECT WHERE

---

Where allows you to specify a property to search for:

```
SELECT first, last  
FROM users  
WHERE first='Jane';
```



ID	First Name	Last Name	Department
1	Jane	Doe	Security



ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling

---

# DELETE

---

Specify a table to delete a record from, specify a search condition that allows us to find a record to delete.

```
DELETE FROM users  
WHERE first='Jane';
```



ID	First Name	Last Name	Department
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling



ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling

# UPDATE

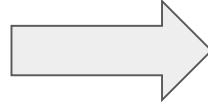
---

1. Specify a table to update, 2. target column and new value to insert, 3. the search condition which finds record to update

Update users

SET= last = 'Fonda'

WHERE first='Jane';



ID	First Name	Last Name	Department
1	Jane	Fonda	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling

ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling





## Activity: First Steps with SQL

In this activity, you will write SQL queries to manually insert records into a database.

`Activities/Stu_First_Steps_with_SQL/README`

**Suggested Time:**  
15 Minutes



18

# Conditional Statements

# OR

Allows you to specify a property to search for with the widen scope of conditionals :

```
SELECT first, last
```

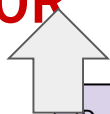
```
FROM users
```

```
WHERE first='Jane'
```

```
OR last= `Competent` ;
```



1	Jane	Doe	Security
2	Bob	Competent	Marketing



ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling

# AND

Allows you to specify a property to search for with the wider scope of conditionals :

**SELECT** first, last

**FROM** users

**WHERE** first='Jane'

**AND** last= `Doe` ;



1	Jane	Doe	Security
---	------	-----	----------



ID	First Name	Last Name	Department
1	Jane	Doe	Security
2	Bob	Competent	Marketing
3	Jon	Rolls	Modeling



## Activity: Conditionals

In this activity, you will write conditional SQL with OR and AND.

[Activities/Stu\\_Conditional\\_Statements/README](#)

**Suggested Time:**

23



# Today's Objectives

---

By the end of class, you will be able to:



Detect XSS with Burp Suite.



Identify and create CRUD queries with SQL.



Explain the syntax for and use WHERE clauses.



Explain the syntax and use conditional statements in SQL.

---