www.example.com

Browser

HTTP Request
HTTP Response

Application
Server

Burpsuite (Web
Proxy tool)

Windows 10

Intercept
Repeater
Intruder

Analyse all the HTTP Request and Responses

Submit and test multuple payloads to Application server for verifying multiple vulnerabilits
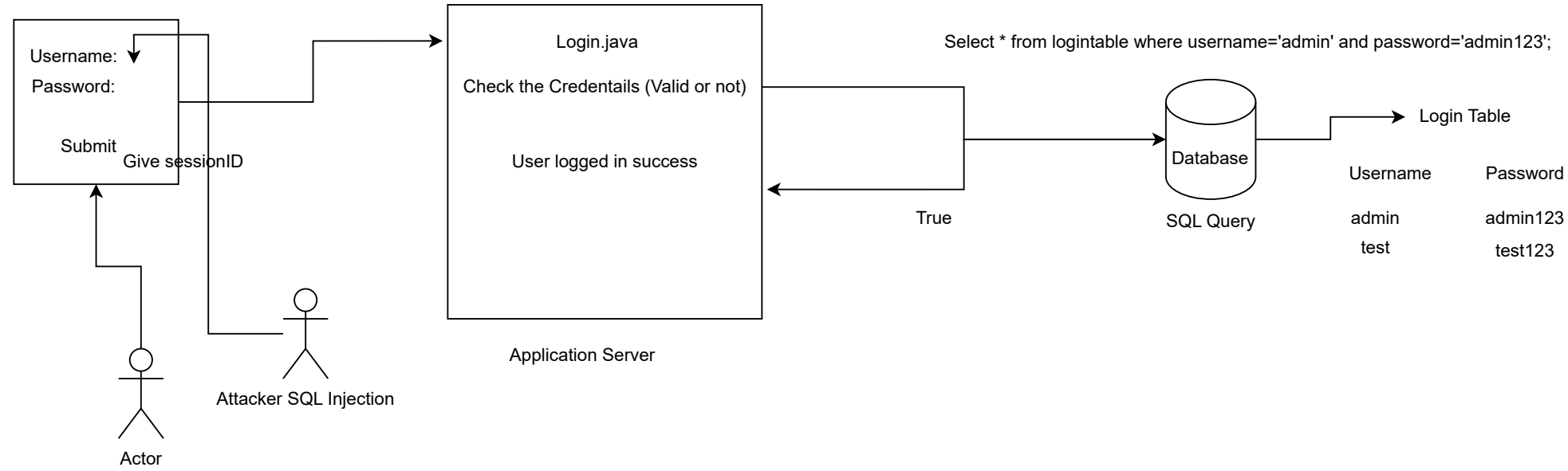
OWASP ZAP

Actor

dummy' or 1=1 --

Boolean based SQL Injection Attack

Select * from logintable where username ='**dummy' or 1=1--** and password='admin123';

Select * from logintable where username='admin' and password='admin123';

Username:

Password:

Submit

Give sessionID

Login.java

Check the Credentails (Valid or not)

User logged in success

Login Table

Database

SQL Query

True

Username   Password

admin   admin123

test   test123

Attacker SQL Injection

Application Server

Actor

SQL injection will occur when user supplied input taken as SQL query and executed in database

ViewmyTransaction

Select tdate,ttime,type from transaction where transactionuserid=test' or 1=1--