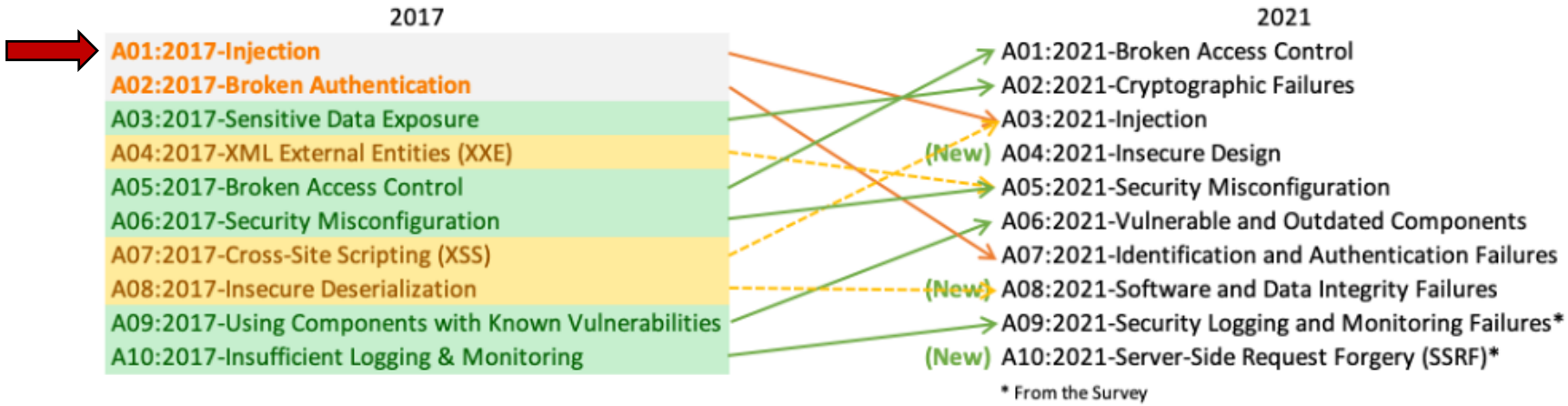
Introduction

Open Web Application Security Project



An ORM, or Object-Relational Mapping, is a software tool that maps object-oriented programming constructs to data stored in a relational database. It simplifies and automates database access by translating object read and write operations into SQL queries, allowing developers to work with data in a more intuitive manner.

ORM

=

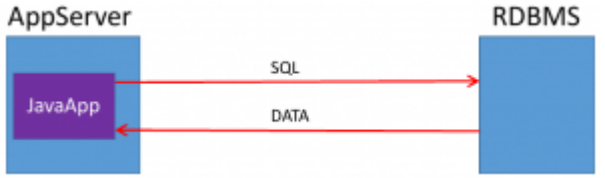
\+ Faster

\+ Flexible

\- Learn

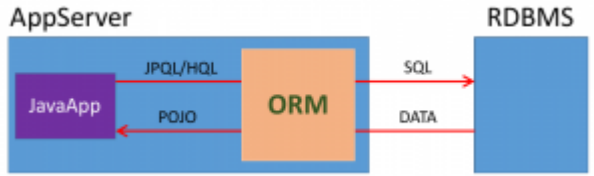
\- Setup

wo/ ORM



Java example:

w/ ORM



What is an ORM injection?

SQL injection

Definition

SQL injection occurs when an attacker inserts malicious SQL code into input fields or parameters to execute commands on the database.

Example

Username = **admin**
Password = **abc123**

> SELECT * FROM ‘users’ **WHERE** username = ‘admin’ AND password=‘abc123’
user = *name, email, address, username, password, credit card number, …*

Username = **’ OR 1=1--**
Password = **abc123**

> SELECT * FROM 'users' **WHERE** username = ‘’ OR 1=1-- ' AND password='whatever’
users = *user1 {}, user2 {}, … , userX{}*

ORM injection

Definition

ORM injection occurs when an attacker exploits input validation weaknesses in an ORM framework to execute malicious SQL commands.

Example

- Hibernate Single Quote Escaping attack

Hibernate:
> SELECT * FROM ‘users’ **WHERE** username = ‘admin\’’ OR 1=(select 1)--’

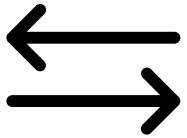
MySQL:
> SELECT * FROM ‘users’ **WHERE** username = ‘admin\’’ **OR** 1=(select 1)--’

ORMi impact

Modification

Suppression

Divulgation



Extraction

Corruption

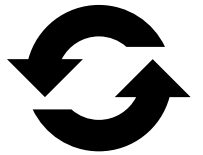
ORMi prevention

Input
validation

Prepared
Statements

Least Privilege
Access Control

Automated
Data Escaping



Regular
Updates

Questions?