

سبر 1213  
Network Defense

Lecture #7 Part 2  
Protecting Against Advanced Attacks

## DNS Attacks

- **Domain reputation**
  - helps ISPs determine an email is being sent by a legitimate organization
- **DNS sinkhole**
  - DNS server that gives incorrect results for one or more domain names
- **DNS log files**
  - record DNS quer

## Network Attacks

- **Replay attacks/ session replays**
  - **capture data in a session to impersonate one of the parties in the session**
  - **can occur on both wired and wireless networks**

## Secure Coding Concepts

- **OWASP**
  - **Open Web Application Security Project**
  - **focused on improving the security of software**
- **Code reuse**
  - **saves time and helps prevent the introduction of new bugs**
- **Dead code**
  - **code that is never executed or used**

# Input Validation

- Verifies validity of data before using it
  - Verifies proper characters
  - Uses boundary and/or range checking
  - Blocks HTML code
  - Prevents the use of certain characters
- Client-side vs server-side
  - Server-side is more secure (many sites use both)
- Input validation prevents
  - Buffer overflow, SQL injection, command injection, and cross-site scripting attacks

# Error and Exception Handling

- Catch errors and provides feedback
  - Prevent improper input from crashing an application providing information to attackers
  - Errors to users should be general
  - Logged information should be detailed

# Secure Coding Concepts

- **Third-party libraries**
- **Software Development Kits (SDKs)**
  - Provide software tools easy to reuse
- **Code obfuscation**
  - Camouflage code

## Secure Coding Concepts

- **Avoid race conditions**
  - **Occur when two modules attempt to access the same resource**
  - **First module to complete the process wins**
  - **Database locks prevent race conditions**



# Software Diversity

- Outsourced Code Development
- Data exposure
- HTTP headers
  - HTTP Strict-Transport-Security
  - Content-Security-Policy
  - X-Frame-Options
- Secure cookie
- Code signing

# Common Methods of Testing Code

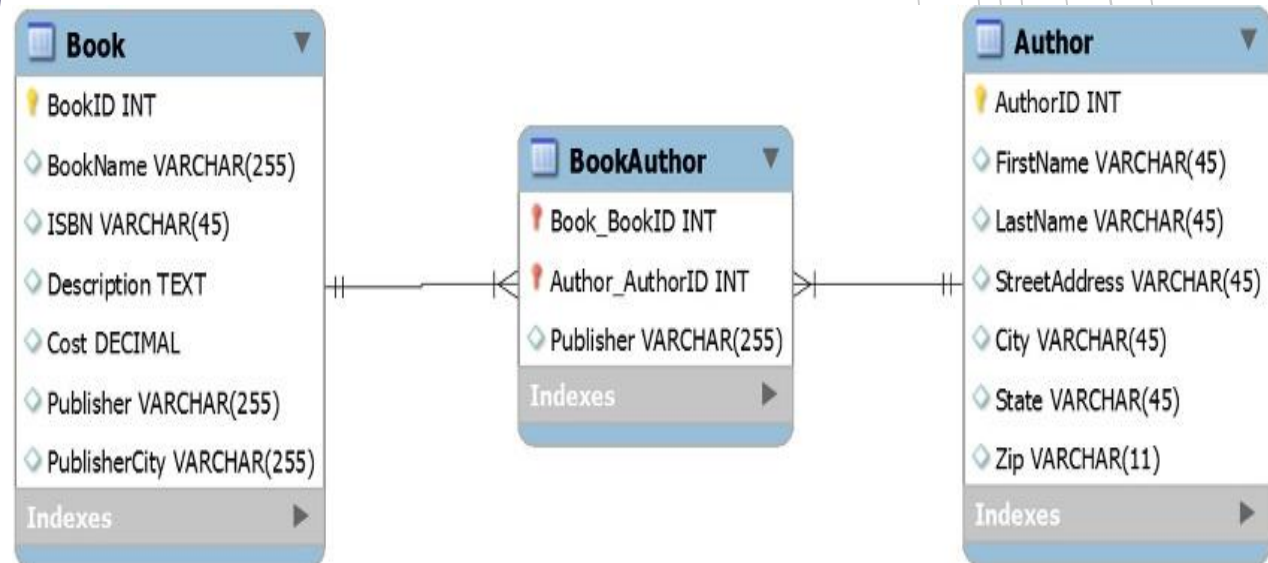
- **Static code analysis**
  - examines the code without executing it
- **Manual code review**
  - static code analysis where someone goes through the code line by line
- **Dynamic code analysis**
  - checks the code as it is running
- **Sandboxing**
  - used to test applications within an isolated area

# Secure Coding Concepts

- **Software version control**
- **Secure development environment**
  - **includes multiple stages**
    - **Development**
    - **Test**
    - **Staging**
    - **Production**
    - **Quality assurance**

# Database concepts

- Tables related to each other with keys
- Database schema



# Database concepts

## Tables

- Rows (also called records or tuples)
- Columns (also called attributes)
- Cells hold individual values (such as “Lisa”) are cells

Column



AuthorID	FirstName	LastName	StreetAddress	City	State	
1	Lisa	Simpson	742 Evergreen Terrace	Springfield	IDK	← Row
2	Moe	Szylak	1313 Walnut Street	Springfield	IDK	← Row
3	Ned	Flanders	744 Evergreen Terrace	Springfield	IDK	← Row

# Database concepts

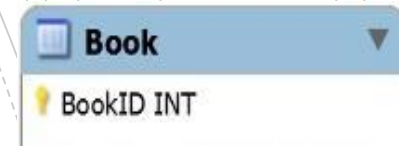
## Normalization

- Organizing tables and columns to reduce redundant data and improve performance
- First normal form (1NF)
- Second normal form (2NF)
- Third normal form (3NF)

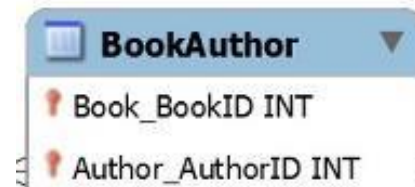
# Database concepts

## 1NF

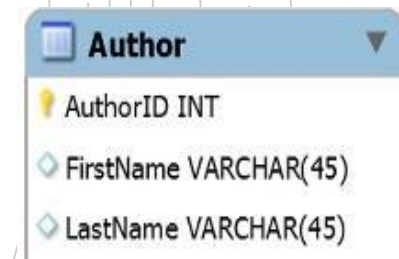
- Each row within a table is unique and identified with a primary key
- Related data is contained in a separate table
- None of the columns include repeating groups



Book
BookID INT



BookAuthor
Book_BookID INT
Author_AuthorID INT



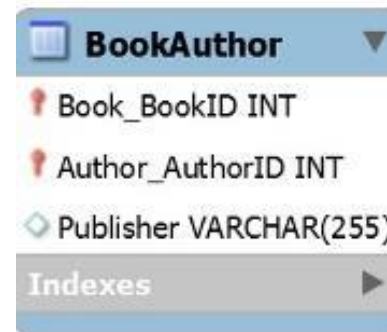
Author
AuthorID INT
FirstName VARCHAR(45)
LastName VARCHAR(45)

# Database concepts

2NF (must be in 1NF)

- Non-primary key attributes are completely dependent on the composite primary key

Composite  
key



The screenshot shows a table named 'BookAuthor' with three columns: 'Book\_BookID INT', 'Author\_AuthorID INT', and 'Publisher VARCHAR(255)'. The first two columns are marked with a red key icon, indicating they form a composite primary key. The 'Publisher' column is marked with a diamond icon, indicating it is a non-primary key attribute. Below the columns is an 'Indexes' section with a right-pointing arrow.

Column Name	Data Type	Key Type
Book_BookID	INT	Primary Key
Author_AuthorID	INT	Primary Key
Publisher	VARCHAR(255)	Non-Primary Key

Publisher  
column in  
this table  
violates this  
rule