Cybersecurity Essentials: Detecting & Preventing Vulnerabilities & Malwares

April 09, 2025

Hello!

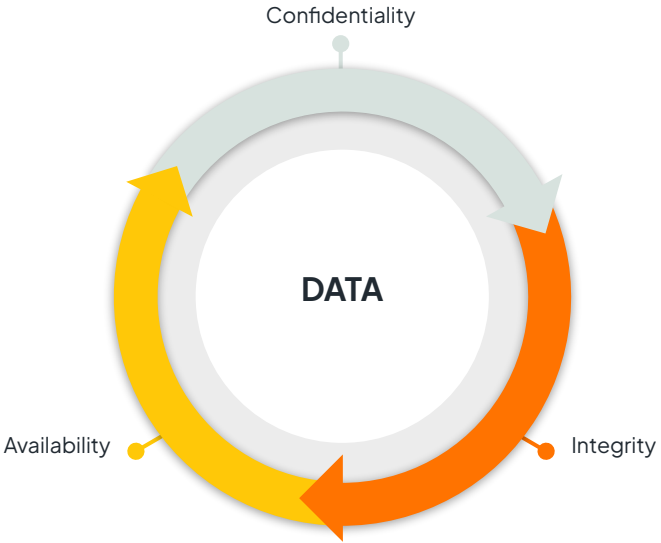
Chamupathi Gigara Hettige

Associate Technical Lead

chamupathi@wso2.com

Introduction to Cybersecurity

CIA Triad – Core Principles of Cybersecurity

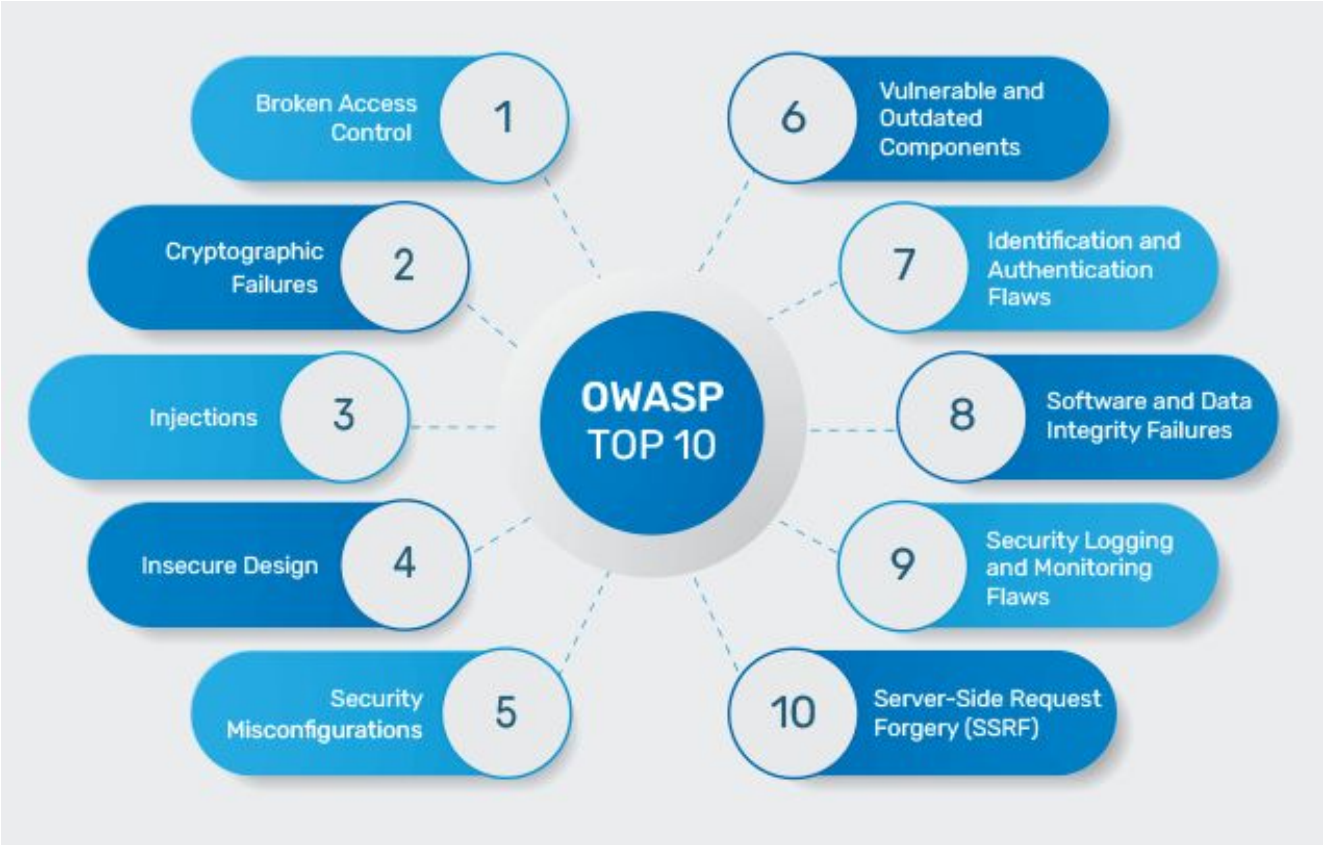


Vulnerabilities, Threats, and Risks

Vulnerability

Categories of Vulnerabilities and Examples	
Category	**Examples**
Software Vulnerabilities	Buffer overflows, SQL injection, Cross-site scripting (XSS), Unpatched software, Misconfigurations
Network Vulnerabilities	Open ports, Weak encryption protocols, Default passwords, Improper firewall rules
Physical Vulnerabilities	Unlocked server rooms, Lack of surveillance, Unprotected hardware
Human Vulnerabilities	Lack of training, Social engineering susceptibility, Weak passwords
Configuration Vulnerabilities	Incorrect access controls, Overly permissive roles, Lack of multi-factor authentication
Supply Chain Vulnerabilities	Compromised third-party software, Tampered hardware, Dependency on unverified vendors

Common Vulnerabilities – OWASP Top 10



Access Control with Ballerina

Cryptographic Failures

Cryptographic Failures in Modern Web Apps

01 Sensitive data exposure due to insecure transmission or storage.

02 Encryption not enforced

03 Improper use of cryptographic algorithms and protocols.

04 Insecure deserialization of user input.

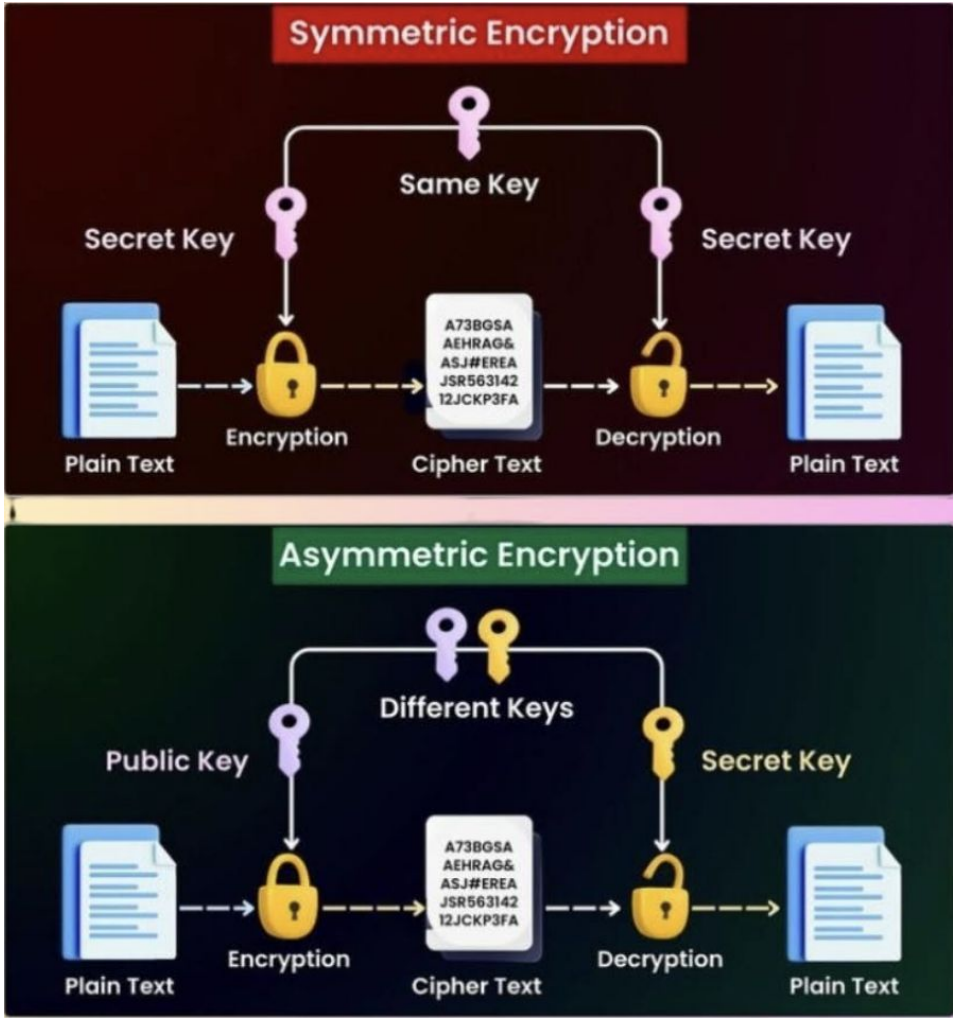
This is one example for content slide

You can use one or two paragraphs. But remember not to overload your slides with content. Your audience will listen to you or read the content, but won’t do both. Mmm.. anything else?

This is sample text only. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean auctor convallis elit, at lobortis libero rutrum id. Suspendisse pretium, purus eget placerat suscipit, erat velit efficitur sapien.

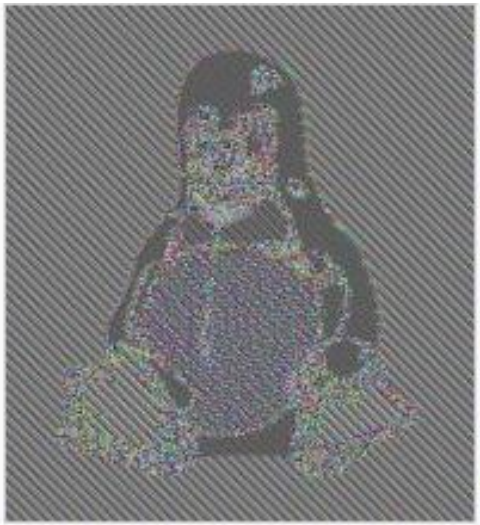
Symmetric vs. Asymmetric Encryption

- Symmetric algorithms: use the same key for both encryption and decryption.
- Asymmetric algorithms: use a public key for encryption and a private key for decryption.
- Symmetric algorithms are generally faster than asymmetric algorithms.
- Asymmetric algorithms are more secure for key exchange and digital signatures.
- Examples of symmetric algorithms: AES, DES, 3DES.
- Examples of asymmetric algorithms: RSA, ECC.

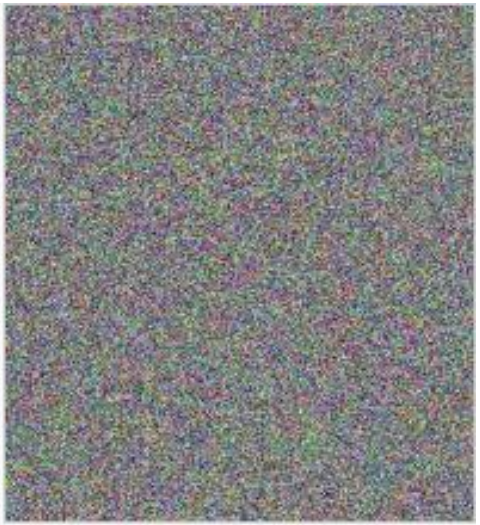


ECB VS CBC

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

SQL Injection

Raw queries

```
`SELECT * FROM users where name = ${username}`;
```

```
string username = "xxx";
sql:ParameterizedQuery queryString = `SELECT * FROM users where name = ${username}`;
```

Detection & Prevention

Types of Malware

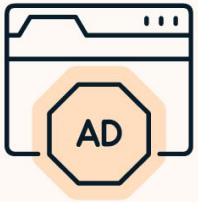
RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE



Spams you with ads

WORMS

Spread
across computers

TROJANS

Sneak malware
onto your PC

BOTNETS

Turn your PC
into a zombie

Detection

Static Analysis: Review code/binaries without executing

Dynamic Analysis: Observe behavior

Hybrid methods are often used

How AI Helps?

Student engagement community

- Ballerina is an open source project (https://github.com/ballerina-platform/ballerina-lang/)
- Seeking open source contributors
  - Ballerina is available for hacktoberfest
  - Community contributions and rewards
- Research Collaborations to explore new tech applications offering students the opportunity to engage in high-impact research projects.

https://ballerina.io/community/

https://ballerina.io/community/student-program/

https://ballerina.io/community/ambassadors/

Find out more…

- Ballerina documentation
  - Ballerina by example
    - ballerina.io/learn/by-example/
  - API Documentation
    - https://lib.ballerina.io/
  - Static analysis
    - https://ballerina.io/learn/scan-tool/

- Join the Ballerina community

Discord
ballerinalang

COLLECTIVES™ on stackoverflow
WSO2 Collective

@ballerinalang

GitHub
ballerina-lang

Resources

- Ballerina installation
  - Download the latest version
    - https://ballerina.io/downloads/
  - Ballerina Visual Studio Code plugin
    - https://marketplace.visualstudio.com/items?itemName=WSO2.ballerina
- Example source code
  - https://github.com/nureka-rodrigo/Ballerina-JWT-Auth-API
- Ballerina static analysis tool
  - https://ballerina.io/learn/scan-tool/
- Report vulnerabilities

Question Time!

Thanks!

wso2.com