A02:2021 | Cryptographic Failures

OWASP Top 10 - Series

Presenter – Jalaj
@ Null-meet, Delhi Chapter
eSec Forte® Technologies, Gurugram
October 8th, 2022

LibreOffice

>_ whoami

- Tech Enthusiast

- Cyber security geek

- Ex-Suzuki, Ex-Dcm Hyundai (Mech.)

- Codes in C++ and Python.

- CTF Player

- CRAC research group : CVE Analysis and Cloud Security

- Learning about Cloud security and Malware analysis

- Practising Red Teaming

- Bikes, MMA

01 Introduction to OWASP Top 10

02 A02:2021 Cryptographic Failure

03 Attack Vectors With Examples

04 QnA

OWASP Top 10

The OWASP Top 10 is a de facto industry standard that provides a list of the 10 Most Critical Web Application Security Risks

- Broken Access Control
- Cryptographic Failure
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)

Illustrations by Pixeltrue on icons8

Cryptographic Failures

Shifting up one position to #2, previously known as Sensitive Data Exposure, which is more of a broad symptom rather than a root cause, the focus is on failures related to cryptography (or lack thereof). Which often lead to exposure of sensitive data.

Notable Common Weakness Enumerations (CWEs) included are CWE-259: Use of Hard-coded Password, CWE-327: Broken or Risky Crypto Algorithm, and CWE-331 Insufficient Entropy. The 29 *Common Weakness Enumerations (CWEs)* mapped to Cryptographic Failures with maximum incidence rate of 46.44% .

List of Mapped CWEs

CWE-261 Weak Encoding for Password

CWE-296 Improper Following of a Certificate's Chain of Trust

CWE-310 Cryptographic Issues

CWE-319 Cleartext Transmission of Sensitive Information

CWE-321 Use of Hard-coded Cryptographic Key

CWE-322 Key Exchange without Entity Authentication

CWE-323 Reusing a Nonce, Key Pair in Encryption

CWE-324 Use of a Key Past its Expiration Date

CWE-325 Missing Required Cryptographic Step

CWE-326 Inadequate Encryption Strength

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CWE-328 Reversible One-Way Hash

CWE-329 Not Using a Random IV with CBC Mode

CWE-330 Use of Insufficiently Random Values

CWE-331 Insufficient Entropy

CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')

CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere

CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory

CWE-540 Inclusion of Sensitive Information in Source Code

CWE-548 Exposure of Information Through Directory Listing

CWE-552 Files or Directories Accessible to External Parties

CWE-566 Authorization Bypass Through User-Controlled SQL Primary Key

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CWE-639 Authorization Bypass Through User-Controlled Key

CWE-651 Exposure of WSDL File Containing Sensitive Information

CWE-668 Exposure of Resource to Wrong Sphere

CWE-706 Use of Incorrectly-Resolved Name or Reference

CWE-862 Missing Authorization

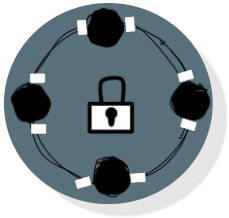
CWE-863 Incorrect Authorization

CWE-913 Improper Control of Dynamically-Managed Code Resources

CWE-922 Insecure Storage of Sensitive Information

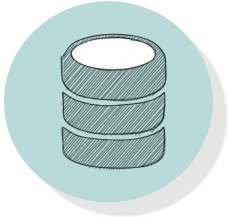
CWE-1275 Sensitive Cookie with Improper SameSite Attribute

Securing Data



Data in Transit

- TLS vs insecure communication
- Old TLS versions, vuln. To SWEET32



Data at Rest

- Hard Coded Credentials/Cryptographic Keys
- Weak/No Encryption of Database

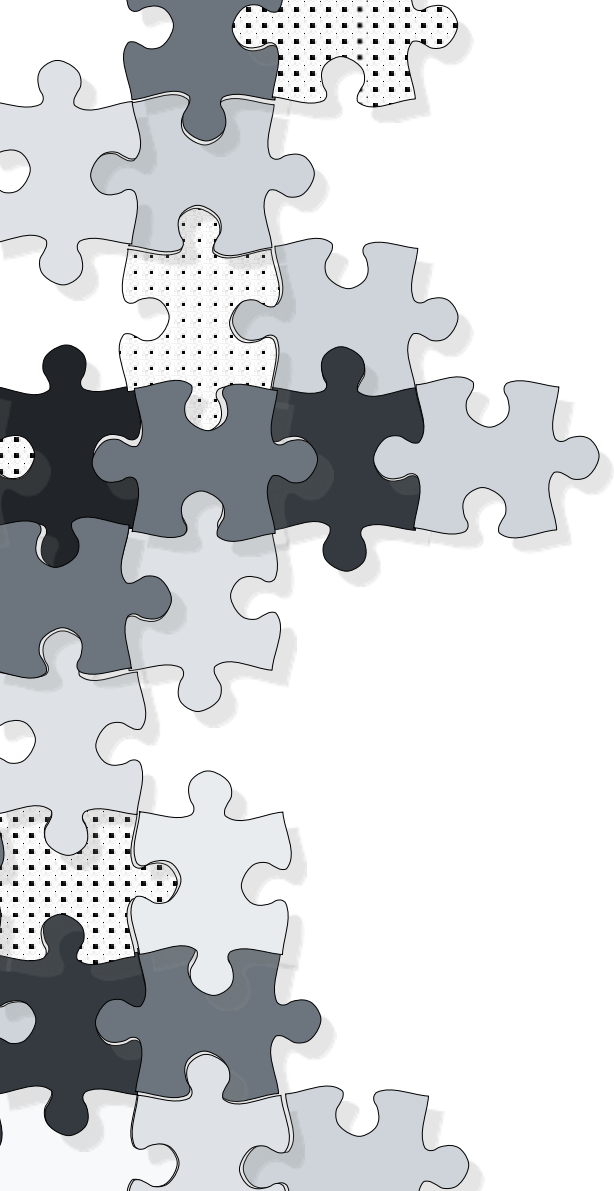
Example: Data in Transit
TLS vs Lack of TLS connection

Example: Data at Rest
Hard Coded credentials without hashing

Example: Data at Rest Unencrypted Database

Mitigation for Cryptographic failure

- Use TLS everywhere, Don’t accept plain text communication.
- Don't store sensitive data unnecessarily. Discard it as soon as possible
- Make sure to encrypt all sensitive data at rest.
- Store passwords using strong adaptive and salted hashing functions with a work factor, such as Argon2, scrypt, bcrypt or PBKDF2.
- Avoid deprecated cryptographic functions and padding schemes, such as MD5, SHA1, PKCS number 1 v1.5
- Do not use legacy protocols such as FTP and SMTP for transporting sensitive data



Further reading resources

Scan :

Thanks!

Any Questions ?