# DAFTAR PUSTAKA


Rui, Liu, Yan Danfeng, Lin Fan, and Yang Fangchun. 2009. "Optimization of Hierarchical Vulnerability Assessment Method." *Proceedings of 2009 2nd IEEE International Conference on Broadband Network and Multimedia Technology, IEEE IC-BNMT2009* (1):458–62. doi: 10.1109/ICBNMT.2009.5348535.

Riadi, Imam, Anton Yudhana, and Yunanri W. 2020. "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment." *Jurnal Teknologi Informasi Dan Ilmu Komputer* 7(4):853. doi: 10.25126/jtiik.2020701928.

Rahalkar, Sagar. 2021. *Guide to Burp Suite*. Pune: Apress.

Qu, Guangzhi, J. Rudraraju, and R. Modukuri. 2002. "A Framework for Network Vulnerability Analysis." *Communications, ...* 2(4):1–6.

Chazar, Chalifa. 2017. "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005." *Jurnal Informasi* VII(2):48–57.

Li, Huan Chung, Po Huei Liang, Jiann Min Yang, and Shiang Jiun Chen. 2010. "Analysis on Cloud-Based Security Vulnerability Assessment." *Proceedings - IEEE International Conference on E-Business Engineering, ICEBE 2010* 490–94. doi: 10.1109/ICEBE.2010.77.

Backdoors, About, Trojan Horses, and Embedding Backdoors. 2001. "Backdoors and Trojan Horses." *Information Security Technical Report* 6(4):31–57. doi: 10.1016/s1363-4127(01)00405-8.

Goel, Jai Narayan, and B. M. Mehtre. 2015. "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology." *Procedia Computer Science* 57:710–15. doi: 10.1016/j.procs.2015.07.458.

Ermawelis, Ermawelis. 2018. "Teknologi Informasi Untuk Perpustakaan, Pusat Dokumentasi Dan Informasi." *AL MUNIR : Jurnal Komunikasi Dan Penyiaran Islam* (1):11–18. doi: 10.15548/amj-kpi.v0i1.5.

2018 .צפקיאל. "Mengenal Dan Memahami Information Disclosure Vulnerability." *LinuxSec* 1. Retrieved (https://www.linuxsec.org/2018/04/mengenal-dan-memahami-information.html).

RSI Security. 2021. "7 TYPES OF VULNERABILITY SCANNERS." *RSI Security* 1. Retrieved (https://blog.rsisecurity.com/7-types-of-vulnerability-scanners/).

Kranch, Michael, and Joseph Bonneau. 2015. “Upgrading HTTPS in Mid-Air: An Empirical Study of Strict Transport Security and Key Pinning.” (February):8–11. doi: 10.14722/ndss.2015.23162.

Cwe.mitre.org. 2021. “CWE-327: Use of a Broken or Risky Cryptographic Algorithm.” *Cwe.Mitre.Org*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/327.html).

Plover. 2006. “CWE - CWE-326: Inadequate Encryption Strength (4.5).” *2006-07-19*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/326.html).

CWE Content Team. 2018. “CWE - CWE-1104: Use of Unmaintained Third Party Components (4.8).” *Common Weakness Enumerations* 1. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/1104.html).

CWE Content Team. 2017. “CWE - CWE-699: Software Development (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/699.html).

CWE Content Team. 2021. “CWE - CWE-693: Protection Mechanism Failure (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/693.html).

Anonymous Tool Vendor (under NDA). 2020. “CWE - CWE-615: Inclusion of Sensitive Information in Source Code Comments (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/615.html).

MITRE. 2022. “CWE - CWE-614: Sensitive Cookie in HTTPS Session Without ‘Secure’ Attribute (4.4).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/614.html).

Anonymous Tool Vendor (under NDA). 2021. “CWE - CWE-541: Inclusion of Sensitive Information in an Include File (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/541.html).

Anonymous Tool Vendor (under NDA). 2021. “CWE - CWE-540: Inclusion of Sensitive Information in Source Code (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/540.html).

Anonymous Tool Vendor (under NDA). 2021. “CWE - CWE-525: Use of Web Browser Cache Containing Sensitive Information (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/525.html).

Anonymous Tool Vendor (under NDA). 2020. “CWE - CWE-524: Use of Cache Containing Sensitive Information (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/524.html).

Anonymous Tool Vendor (under NDA). 2021. “CWE - CWE-523: Unprotected Transport of Credentials (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/523.html).

7 Pernicious Kingdoms. 2020. “CWE - CWE-388: 7PK - Errors (4.8).” *Common Weakness Enumerations*. Retrieved July 1, 2022 (https://cwe.mitre.org/data/definitions/388.html).

OWASP. 2017. “OWASP Top Ten 2017 | A9:2017-Using Components with Known Vulnerabilities | OWASP Foundation.” *OWASP Top Ten 2017*. Retrieved July 1, 2022 (https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities).

CAPEC Content Team. 2022. “CAPEC - CAPEC-153: Input Data Manipulation (Version 3.7).” *Common Attack Pattern Enumeration and Classification*. Retrieved July 1, 2022 (https://capec.mitre.org/data/definitions/153.html).

CAPEC Content Team. 2022. “CAPEC - CAPEC-37: Retrieve Embedded Sensitive Data (Version 3.7).” *Common Attack Pattern Enumeration and Classification*. Retrieved July 1, 2022 (https://capec.mitre.org/data/definitions/37.html).

CAPEC Content Team. 2020. “CAPEC - CAPEC-103: Clickjacking (Version 3.7).” *Common Attack Pattern Enumeration and Classification*. Retrieved July 1, 2022 (https://capec.mitre.org/data/definitions/103.html).

CAPEC Content Team. 2022. “CAPEC - CAPEC-94: Adversary in the Middle (AiTM) (Version 3.7).” *Common Attack Pattern Enumeration and Classification*. Retrieved July 1, 2022 (https://capec.mitre.org/data/definitions/94.html).

CAPEC Content Team. 2022. “CAPEC - CAPEC-157: Sniffing Attacks (Version 2.10).” *Common Attack Pattern Enumeration and Classification*. Retrieved July 1, 2022 (https://capec.mitre.org/data/definitions/157.html).

MITRE. 2021. “CWE-295: Improper Certificate Validation.” *Common Weakness Enumerations2* 1. Retrieved (https://cwe.mitre.org/data/definitions/295.html).

PLOVER. 2022. “CWE-200: Exposure of Sensitive Information to an Unauthorized Actor.” *Common Weakness Enumerations* 1.

PLOVER. 2022. “CWE-159: Improper Handling of Invalid Use of Special Elements.” *Common Weakness Enumerations* 1. Retrieved (https://cwe.mitre.org/data/definitions/159.html).

MITRE-CVE. 2022. “CWE-116: Improper Encoding or Escaping of Output.” *Common Weakness Enumerations* 1. Retrieved (https://cwe.mitre.org/data/definitions/116.html).

Enumeration, Commons Weakness. 2016. “CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-Site Scripting’).” *2016* 1. Retrieved (http://cwe.mitre.org/data/definitions/79.html).

Landwehr. 2022. “CWE CATEGORY: DEPRECATED: Source Code.” *Common Weakness Enumerations* 1. Retrieved (https://cwe.mitre.org/data/definitions/18.html).