

# References

- [1] MARKETSANDMARKETS. Application security market by component (software tools (SAST and DAST) and services), type (web application security and mobile application security), organization size, deployment mode, vertical (healthcare and BFSI), and region - global forecast to 2025. Online: <https://www.marketsandmarkets.com/Market-Reports/application-security-market-110170194.html>, accessed on 2021-04-09.
- [2] GitLab team. 2020 global DevSecOps survey - GitLab. Online: <https://about.gitlab.com/developer-survey/>, accessed on 2021-04-09.
- [3] H. Myrbakken and R. Colomo-Palacios, “DevSecOps: A multivocal literature review,” in *International Conference on Software Process Improvement and Capability Determination*. Springer, 09 2017. doi: 10.1007/978-3-319-67383-7\_2 pp. 17–29.
- [4] United Nations. United Nations sustainable development goals. Online: <https://sdgs.un.org/goals>, accessed on 2021-07-23.
- [5] Finnish advisory board on research integrity. (2012) Responsible conduct of research and procedures for handling allegations of misconduct in Finland. Online: [https://tenk.fi/sites/tenk.fi/files/HTK\\_ohje\\_2012.pdf](https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf).
- [6] Swedish research council. (2017) Ethics in research. Online: <https://www.vr.se/english/mandates/ethics/ethics-in-research.html>.
- [7] B. Potter and G. McGraw, “Software security testing,” *IEEE Security Privacy*, vol. 2, no. 5, pp. 81–85, 2004. doi: 10.1109/MSP.2004.84
- [8] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu, and A. Pretschner, “Chapter one — security testing: A survey,” ser. *Advances in Computers*, A. Memon, Ed. Elsevier, 2016, vol. 101. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0065245815000649>

- [9] N. Jovanovic, C. Kruegel, and E. Kirda, “Pixy: a static analysis tool for detecting web application vulnerabilities,” in *2006 IEEE Symposium on Security and Privacy (S&P’06)*. IEEE, 2006. doi: 10.1109/SP.2006.29
- [10] N. Jovanovic, C. Kruegel, and E. Kirda, “Precise alias analysis for static detection of web application vulnerabilities,” in *Proceedings of the 2006 Workshop on Programming Languages and Analysis for Security*, ser. PLAS ’06. New York, NY, USA: ACM, 2006. doi: 10.1145/1134744.1134751 p. 27–36.
- [11] J. Newsome, D. Song, J. Newsome, and D. Song, “Dynamic taint analysis: Automatic detection, analysis, and signature generation of exploit attacks on commodity software,” in *In Proceedings of the 12th Network and Distributed Systems Security Symposium*. Internet Society, 2005.
- [12] Synopsys. Black Duck software composition analysis. Online: <https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis.html>, accessed on 2021-04-16.
- [13] G. Tian-yang, S. Yin-sheng, and F. You-yuan, “Research on software security testing,” *International Journal of Computer and Information Engineering*. Publisher: World Academy of Science, Engineering and Technology, vol. 4, no. 9, pp. 1446 – 1450, 2010, <https://publications.waset.org/vol/45>.
- [14] K. Gos and W. Zabierowski, “The comparison of microservice and monolithic architecture,” in *2020 IEEE XVIth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH)*. IEEE, 2020. doi: 10.1109/MEMSTECH49584.2020.9109514 pp. 150–153.
- [15] M. Villamizar, O. Garcés, H. Castro, M. Verano, L. Salamanca, R. Casallas, and S. Gil, “Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud,” in *2015 10th Computing Colombian Conference (10CCC)*. IEEE, 2015. doi: 10.1109/ColumbianCC.2015.7333476 pp. 583–590.
- [16] C. Richardson. Microservice patterns. Online: <https://microservices.io>, accessed on 2021-04-23.
- [17] D. Namiot and M. Sneps-Snepe, “On micro-services architecture,” *International Journal of Open Information Technologies*. Publisher: Open Information Technologies Lab, vol. 2, no. 9, pp. 24–27, 2014.

- [18] V. Singh and S. K. Peddoju, “Container-based microservice architecture for cloud applications,” in *2017 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, 2017, pp. 847–852.
- [19] D. Taibi, V. Lenarduzzi, and C. Pahl, “Architectural patterns for microservices: A systematic mapping study,” in *8th International Conference on Cloud Computing and Services Science*. SCITEPRESS, 03 2018. doi: 10.5220/0006798302210232
- [20] Q. Abbas, H. Shafiq, I. Ahmad, and S. Tharanidharan, “Concurrency control in distributed database system,” in *2016 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2016. doi: 10.1109/ICCCI.2016.7479987 pp. 1–4.
- [21] M. Virmani, “Understanding DevOps bridging the gap from continuous integration to continuous delivery,” in *Fifth International Conference on the Innovative Computing Technology (INTECH 2015)*. IEEE, 2015. doi: 10.1109/INTECH.2015.7173368 pp. 78–82.
- [22] M. Artac, T. Borovssak, E. Di Nitto, M. Guerriero, and D. A. Tamburri, “DevOps: introducing infrastructure-as-code,” in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*. IEEE, 2017, pp. 497–498.
- [23] M. Shahin, M. Zahedi, M. Ali Babar, and L. Zhu, “An empirical study of architecting for continuous delivery and deployment,” *Empirical Software Engineering*. Publisher: Springer, vol. 24, 08 2018. doi: 10.1007/s10664-018-9651-4
- [24] V. Mohan and L. B. Othmane, “SecDevOps: Is it a marketing buzzword? — mapping research on security in DevOps,” in *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2016. doi: 10.1109/ARES.2016.92 pp. 542–547.
- [25] A. A. U. Rahman and L. Williams, “Software security in DevOps: Synthesizing practitioners’ perceptions and practices,” in *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED)*. IEEE, 2016. doi: 10.1109/CSED.2016.021 pp. 70–76.
- [26] C. Schneider, “Security DevOps-staying secure in agile projects,” *OWASP AppSec Europe*, 2015.

- [27] J. Han, H. E. G. Le, and J. Du, "Survey on NoSQL database," in *2011 6th International Conference on Pervasive Computing and Applications*. IEEE, 2011. doi: 10.1109/ICPCA.2011.6106531 pp. 363–366.
- [28] E. Shmueli, R. Vaisenberg, Y. Elovici, and C. Glezer, "Database encryption — an overview of contemporary challenges and design considerations," *SIGMOD Record. Publisher: ACM*, vol. 38, pp. 29–34, 09 2009.
- [29] M. Amaral, J. Polo, D. Carrera, I. Mohomed, M. Unuvar, and M. Steinder, "Performance evaluation of microservices architectures using containers," in *2015 IEEE 14th International Symposium on Network Computing and Applications*. IEEE, 2015. doi: 10.1109/NCA.2015.49 pp. 27–34.
- [30] The Pallets Projects. Python Flask module. Online: <https://palletsprojects.com/p/flask/>, accessed on 2021-05-05.
- [31] D. Spinellis, "Version control systems," *IEEE Software*, vol. 22, no. 5, pp. 108–109, 2005. doi: 10.1109/MS.2005.140
- [32] Gogs team. Gogs - a painless self-hosted Git service. Online: <https://gogs.io>, accessed on 2021-05-06.
- [33] Gogs team . Gogs REST API v1 usage. Online: <https://github.com/gogs/docs-api>, accessed on 2021-05-06.
- [34] V. Radha and D. H. Reddy, "A survey on single sign-on techniques," *Procedia Technology. Elsevier*, vol. 4, pp. 134–139, 2012.
- [35] Microsoft. Microsoft identity platform and OpenID Connect protocol. Accessed date: 2021-05-08. [Online]. Available: <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-protocols-oidc>
- [36] S. Lee, J.-Y. Jo, and Y. Kim, "Method for secure RESTful web service," in *2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS)*. IEEE, 2015. doi: 10.1109/ICIS.2015.7166573 pp. 77–81.
- [37] Network Working Group. HTTP authentication: Basic and digest access authentication. RFC2617. IETF, 1999. Online: <https://tools.ietf.org/html/rfc2617>.
- [38] R. Sandhu, E. Coyne, and C. Y. Feinstein, HL, "Access control models," *IEEE computer*, vol. 29, no. 2, pp. 38–47, 2013.

- [39] National Institute of Standards and Technology. (2001, 11) FIPS 197 - advanced encryption standard (AES). Online: <https://csrc.nist.gov/publications/detail/fips/197/final>.
- [40] Docker Inc. Develop with Docker Engine API. Online: <https://docs.docker.com/engine/api/>, accessed on 2021-05-11.
- [41] Docker Inc. Docker SDK for Python. Online: <https://docker-py.readthedocs.io/>, accessed on 2021-05-11.
- [42] RabbitMQ team. RabbitMQ message broker. Online: <https://www.rabbitmq.com/>, accessed on 2021-05-17.
- [43] D. Shadija, M. Rezai, and R. Hill, "Towards an understanding of microservices," in *2017 23rd International Conference on Automation and Computing (ICAC)*. IEEE, 2017. doi: 10.23919/ICoNAC.2017.8082018 pp. 1–6.
- [44] RabbitMQ team. Message reliability in RabbitMQ. Online: <https://www.rabbitmq.com/reliability.html>, accessed on 2021-05-17.
- [45] OWASP project. OWASP damn vulnerable serverless application project. Available: <https://github.com/OWASP/DVSA>, accessed on 2021-06-7.
- [46] Foreseeti AB. The missing piece in DevSecOps. Online: <https://foreseeti.com/missing-piece-devsecops/>, accessed on 2021-06-14.

# For DIVA

```
{
  "Author1": {
    "Last name": "Le",
    "First name": "Duc Quang",
    "Local User Id": "u100001",
    "E-mail": "dqle@kth.se",
    "ORCID": "0000-0002-00001-1234",
    "organisation": {"L1": "School of Electrical Engineering and Computer Science ",
                    }
  },
  "Degree": {"Educational program": ""},
  "Title": {
    "Main title": "A framework to unify application security testing in DevOps environment",
    "Language": "eng" },
  "Alternative title": {
    "Main title": "Ett ramverk för enhetlig testning av applikationssäkerhet i DevOps-miljöer",
    "Language": "swe"
  },
  "Supervisor1": {
    "Last name": "Aura",
    "First name": "Tuomas",
    "E-mail": "tuomas.aura@aalto.fi",
    "Other organisation": "Aalto University, School of Science, Department of Computer Science"
  },
  "Examiner1": {
    "Last name": "Robert",
    "First name": "Lagerström",
    "E-mail": "robertl@kth.se",
    "organisation": {"L1": " ",
                    "L2": "Division of network and systems engineering" }
  },
  "Cooperation": {"Partner_name": "KONE Corporation, Finland"},
  "Other information": {
    "Year": "2021", "Number of pages": "vii,??"
  }
}
```