References

[1] J. Oksanen, "Or as he's known "indiana jones of cyber security"," the tweet is in reference to Pontus Johnson's paper "Intrinsic Propensity for Vulnerability in Computers? Arbitrary Code Exection in the universal Turing Machine", found here: https://arxiv.org/abs/2105.02124. [Online]. Available: https://twitter.com/janne_oksanen/status/1391702951283118081?s=20 [Cited in section (document).]

[2] D. Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *Georgia Public Broadcasting*, 2021. [Online]. Available: https://www.gpb.org/news/2021/04/19/worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [Cited in sections 1.1, 7, and 6.3.]

[3] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. USA: Crown Publishing Group, 2014. ISBN 077043617X [Cited in section 1.1.]

[4] R. Duan, O. Alrawi, R. P. Kasturi, R. Elder, B. Saltaformaggio, and W. Lee, "Measuring and Preventing Supply Chain Attacks on Package Managers," *CoRR*, vol. abs/2002.01139, 2020. [Online]. Available: https://arxiv.org/abs/2002.01139 [Cited in section 1.1.]

[5] Q. Wu and K. Lu, "On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits," 2021. [Online]. Available: https://github.com/QiushiWu/qiushiwu.github.io/blob/main/papers/OpenSourceInsecurity.pdf [Cited in sections 1.1 and 8.]

[6] G. Kroah-Hartman, "[patch 000/190] revertion of all of the umn.edu commits," message to the Linux kernel mailing list. [Accessed on 2021-05-03]. [Online]. Available: https://lkml.org/lkml/2021/4/21/454 [Cited in section 8.]

[7] K. Lu, Q. Wu, and A. Pakki, “An Open Letter to the Linux Community,” [Accessed on 2021-05-03]. [Online]. Available: https://github.com/QiushiWu/qiushiwu.github.io/blob/main/OtherDocs/note_to_Linux.pdf [Cited in section 8.]

[8] L. Bass, I. Weber, and L. Zhu, *DevOps: A Software Architect’s Perspective*, 1st ed., ser. SEI Series in Software Engineering. Addison-Wesley Professional, 2015. ISBN 0134049845 [Cited in section 2.1.]

[9] J. Davis, *What Is DevOps?*, 1st ed. O’Reilly Media, 2018. ISBN 1-4920-3989-6 [Cited in section 2.1.]

[10] F. M. A. Erich, C. Amrit, and M. Daneva, “A qualitative study of devops usage in practice,” *Journal of Software: Evolution and Process*, vol. 29, no. 6, p. e1885, 2017. doi: https://doi.org/10.1002/smr.1885 E1885 smr.1885. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/smr.1885 [Cited in section 2.1.]

[11] M. Shahin, M. Ali Babar, and L. Zhu, “Continuous Integration, Delivery and Deployment: A Systematic Review on Approaches, Tools, Challenges and Practices,” *IEEE Access*, vol. 5, pp. 3909–3943, 2017. doi: 10.1109/ACCESS.2017.2685629 [Cited in section 12.]

[12] A. Capizzi, S. Distefano, L. J. P. Araújo, M. Mazzara, M. Ahmad, and E. Bobrov, “Anomaly Detection in DevOps Toolchain,” in *Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment*, J.-M. Bruel, M. Mazzara, and B. Meyer, Eds. Cham: Springer International Publishing, 2020. ISBN 978-3-030-39306-9 pp. 37–51. [Cited in section 2.1.1.]

[13] S. Chacon and B. Straub, *Pro Git (Second Edition)*, 2nd ed. Berkeley, CA: Apress, 2014. ISBN 9781484200773 [Cited in section 2.1.2.]

[14] A. Vladimirov, *Assessing Information Security Strategies, Tactics, Logic and Framewortk*, 2nd ed. Ely: IT Governance Ltd, 2015. ISBN 1-84928-600-0 [Cited in section 2.2.1.]

[15] G. Haff, *How Open Source Ate Software: Understand the Open Source Movement and So Much More*. Berkeley, CA: Apress L. P, 2018. ISBN 1484238931 [Cited in section 2.3.]

[16] R. T. Fielding, “REST: architectural styles and the design of network-based software architectures,” Doctoral dissertation, University of

California, Irvine, 2000, there are two pdf's available. Our page numbers are referencing the single-column version intended for screen use. [Online]. Available: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm [Cited in sections 2.4, 2.4.1, 4, and 2.4.1.]

[17] C. Pautasso, E. Wilde, and R. Alarcon, Eds., *REST: Advanced Research Topics and Practical Applications*, 1st ed. Springer, 2014. ISBN 1-4614-9299-8 [Cited in section 2.4.1.]

[18] R. T. Fielding, "Rest apis must be hypertext-driven," Untangled: musings of Roy T. Fielding, 2008. [Online]. Available: https://roy.gbiv.com/untangled/2008/rest-apis-must-be-hypertext-driven [Cited in sections 2.4.1 and 18.]

[19] S. Buna, *GraphQL in Action*. Manning Publications, 2021. ISBN 9781617295683 [Cited in sections 19 and 2.4.2.]

[20] E. Porcello and A. Banks, *Learning GraphQL: Declarative Data Fetching for Modern Web Apps*. Sebastopol: O'Reilly Media, Incorporated, 2018. ISBN 9781492030713 [Cited in section 20.]

[21] N. Thomas. Create Deep Dive 3: GraphQL. GitLab Youtube Channel. Nick Thomas was at the time of the recording Staff Backend Engineer at GitLab's Create team. The url directs to a second or two before the quote, but the talk is recommended for anyone interested in GraphQL in general, and GitLab's implementation in particular. [Online]. Available: https://youtu.be/-9L_1MWrjkg?t=787 [Cited in section 2.4.2.]

[22] O. Hartig and J. Pérez, "Semantics and Complexity of GraphQL," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2018. doi: 10.1145/3178876.3186014. ISBN 9781450356398 p. 1155–1164. [Online]. Available: https://doi.org/10.1145/3178876.3186014 [Cited in section 2.4.2.]

[23] A. Shostack, *Threat modeling: designing for security*. Indianapolis, IN: Wiley, 2014. ISBN 9781118809990 OCLC: ocn855043351. [Cited in sections 3.2 and 3.3.]

[24] M. Howard and S. Lipner, *The security development lifecycle: SDL, a process for developing demonstrably more secure software*, ser. Secure

software development series. Redmond, Wash: Microsoft Press, 2006. ISBN 9780735622142 OCLC: ocm70211570. [Cited in section 3.3.]

[25] "WSTG - Latest OWASP," library Catalog: owasp.org. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/ [Cited in sections 3.4 and 3.5.]

[26] "Owasp cheat sheet series: Graphql cheat sheet," accessed on: 2021-06-24, 23:22. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html [Cited in section 3.4.]

[27] W. 'vakzz' Bowling, "devcraft.io: Ctf write ups by vakzz," accessed on: 2021-06-24, 23:24. [Online]. Available: https://devcraft.io [Cited in section 3.4.]

[28] Portswigger, "Web security academy," accessed on: 2021-06-24, 23:24. [Online]. Available: https://portswigger.net/web-security [Cited in section 3.4.]

[29] D. Stuttard, *The web application hacker's handbook : finding and exploiting security flaws*, 2nd ed. Wiley, 2011. ISBN 9781118175224 [Cited in section 3.4.]

[30] HackerOne, "Hacker101," accessed on: 2021-06-24, 23:24. [Online]. Available: https://www.hacker101.com [Cited in section 3.4.]

[31] A. Borg and C. A. Francke, "Iot Pentesting: Obtaining the Firmware of a Smart Lock," Master's thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2020. [Cited in section 5.1.]

[32] M. Berner, "Where's My Car? Ehtical Hacking of a Smart Garage," Master's thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2020. [Cited in section 5.1.]

[33] D. Freimanis, "Vulnerability assessment of authentication methods in a large-scale computer system," Master's thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2019. [Cited in section 5.1.]

[34] D. Skeppstedt, "Identification and exploitation of vulnerabilities in a large-scale itsystem," Master's thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2019. [Cited in section 5.1.]

[35] “GitLab Values.” [Online]. Available: https://about.gitlab.com/handbook/values/ [Cited in section 5.2.]

[36] “GitLab’s HackerOne Bug Bounty Program is public today.” [Online]. Available: https://about.gitlab.com/blog/2018/12/12/gitlab-hackerone-bug-bounty-program-is-public-today/ [Cited in section 5.2.]

[37] “GitLab disclosed on HackerOne: Unauthorized user is able to access...” [Online]. Available: https://hackerone.com/reports/962462 [Cited in section 5.2.]

[38] “GitLab disclosed on HackerOne: Graphql query namespace leaks data.” [Online]. Available: https://hackerone.com/reports/614355 [Cited in section 5.2.]

[39] “Rce via unsafe inline Kramdown options when rendering certain Wiki pages.” [Online]. Available: https://hackerone.com/reports/1125425 [Cited in sections 5.2 and 6.5.]

[40] “Bypass of GitLab CI runner slash fix in YAML validation.” [Online]. Available: https://hackerone.com/reports/409395 [Cited in section 5.2.]

[41] “Remote hacker can download all the files of master branch in public projects where everything is members only.” [Online]. Available: https://hackerone.com/reports/1043480 [Cited in section 6.5.]

[42] “Todos are not redacted when membership changes - access to (confidential) issues and merge requests.” [Online]. Available: https://hackerone.com/reports/880863 [Cited in section 6.5.]

[43] “Gitlab-runner on windows docker_auth_config container host command injection.” [Online]. Available: https://hackerone.com/reports/955016 [Cited in section 6.5.]

[44] “Privilege escalation from any user (including external) to gitlab admin when admin impersonates you.” [Online]. Available: https://hackerone.com/reports/493324 [Cited in sections 6.5.1 and 7.2.2.]

[45] “Sql injection in milestonefinder order method.” [Online]. Available: https://hackerone.com/reports/298176 [Cited in sections 43 and 7.3.5.]

[46] “Local files could be overwritten in gitlab, leading to remote command execution.” [Online]. Available: https://hackerone.com/reports/587854 [Cited in sections 44 and 7.3.5.]

[47] “Insufficient type check on graphql leading to maintainer delete repository.” [Online]. Available: https://hackerone.com/reports/858671 [Cited in sections 6.6 and 7.4.3.]

[48] “Able to leak private email of any user given his/her username via graphql.” [Online]. Available: https://hackerone.com/reports/972355 [Cited in sections 6.6 and 7.4.1.]

[49] “Cve-2021-22209.” [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22209 [Cited in section 7.1.1.]

[50] R. T. Fielding and J. Reschke, “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content,” RFC 7231, Jun. 2014. [Online]. Available: https://rfc-editor.org/rfc/rfc7231.txt [Cited in section 7.1.2.]

[51] “Project access tokens GitLab.” [Online]. Available: https://docs.gitlab.com/ee/user/project/settings/project_access_tokens.html [Cited in sections 7.2.1 and 7.2.4.]

[52] “Session hijacking attack Software Attack.” [Online]. Available: https://owasp.org/www-community/attacks/Session_hijacking_attack [Cited in section 7.2.2.]

[53] “Business logic vulnerabilities Web Security Academy.” [Online]. Available: https://portswigger.net/web-security/logic-flaws [Cited in section 7.2.3.]

[54] “View the starred projects in a private profile.” [Online]. Available: https://hackerone.com/reports/703894 [Cited in section 7.4.2.]

[55] “Importing gitlab project archives can replace uploads of other users.” [Online]. Available: https://hackerone.com/reports/534794 [Cited in section 7.4.2.]

[56] “The 2021 Hacker Report.” [Online]. Available: https://www.hackerone.com/resources/reporting/the-2021-hacker-report [Cited in section 7.4.6.]

Appendix A

Authentication script

```
import requests
import sys
import json

# Usage
# Run the script with an argument containing the file with tokens. The token file needs to be
# in the format "tokenname scope token" and not contain trailing line breakes.

file_name = sys.argv[1]
server = ’https://gitlab.domain.com’

# GraphQL queries
query_read = """
query {
    currentUser {
        id
    }
}
"""
query_mutate = """
mutation {
  createIssue(input:{
    title: "test"
    projectPath: "root/open01"
  }){
    errors
  }
}
"""
```