IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 3, April 2022

SQL Injection

Prof. P. S. Gawali[1], Sajid Shaikh[2], Pranav Pawar[3], Utkarsh Thakur[4]

Guide, Department of Computer Engineering[1]

Students, Department of Computer Engineering[1,2,3]

Singad Academy of Engineering Pune, Maharashtra, India

imsajidshaikh30@gmail.com[2], pranavpawar645@gmail.com[3], utkarshthakur414@gmail.com[4]

Abstract: *SQL Injection (SQLi) could also be a kind of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind an internet application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of an internet page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to feature, modify, and delete records within the database.*

Keywords: Cloud computing, SQL injection attack (SQLiA), Two fish encryption and decryption, Deep learning, code injection, intrusion detection, supervised learning, SQL injection, XSS, JAVA, JavaScript.

REFERENCES

[1]. S. Deering and R. Hinden, IETF RFC2460, Internet Protocol, Version 6, 1998, http://www.ietf.org/rfc/rfc2460.txt.

[2]. M. Boucadair, J. Grimault, P. Levis, A. Villefranque, and P. ´ Morand, “Anticipate IPv4 address exhaustion: a critical challenge for internet survival,” in Proceedings of the 1st International Conference on Evolving Internet (INTERNET ’09), pp. 27–32, Cannes La Bocca, France, August 2009.

[3]. M. Gunn, “War dialing,” 2002.

[4]. Wikipedia, “War dialing,” 2013, http://en.wikipedia.org/wiki/ War dialing.

[5]. R. Oppliger, “Security at the internet layer,” Computer, vol. 31, no. 9, pp. 43–47, 1998.

[6]. S. Weber and L. Cheng, “A survey of anycast in IPv6 networks,” IEEE Communications Magazine, vol. 42, no. 1, pp. 127–132, 2004.

[7]. E. Fong and V. Okun, “Web application scanners: definitions and functions,” in Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS ’07), Waikoloa, Hawaii, USA, January 2007

[8]. X. Fu, X. Lu, B. Peltsverger, S. Chen, K. Qian, and L. Tao, “A static analysis framework for detecting SQL injection vulnerabilities,” in Proceedings of the 31st Annual International Computer Software and Applications Conference (COMPSAC ’07), pp. 87–96, Beijing, China, July 2007.

[9]. J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, “State of the art: automated black-box web application vulnerability testing,” in Proceedings of the IEEE Symposium on Security and Privacy (SP ’10), pp. 332–345, Oakland, Calif, USA, May 2010.

[10]. G. Pant, P. Srinivasan, and F. Menczer, Crawling the Web, 2004.

[11]. A. Heydon and M. Najork, “Mercator: a scalable, extensible web crawler,” World Wide Web, vol. 2, no. 4, pp. 219–229, 1999 [12] HackTrix, “Stay away from malicious Facebook apps,” 2013 [Online]. Available: http://bit.ly/b6gWn5

[12]. H. Y. Kao, S. H. Lin, J. M. Ho, and M. S. Chen, “Mining web informative structures and contents based on entropy analysis,” IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 1, pp. 41–55, 2004.

[13]. I. S. Altingovde and O. Ulusoy, “Exploiting interclass rules for ¨ focused crawling,” IEEE Intelligent Systems, vol. 19, no. 6, pp. 66– 73, 2004.

DOI: 10.48175/IJARSCT-3292