IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, December 2023

Data Leaks Using SQL Injection

Tahseen Ali[1], Rohan Dipke[2], Vinayak Dhanshetti[4], Nikhil Gadepally[4]
Assistance Professor, Department of Computer Enggineering[1]
Students, Department of Computer Enggineering[2,3,4]
Gramin Technical & Management, Nanded, India

Abstract: *The security of digital data is paramount in today's interconnected world. Among the various cyber threats, SQL injection attacks represent a significant menace to the confidentiality, integrity, and availability of sensitive information stored within databases. SQL injection is a technique employed by malicious actors to exploit vulnerabilities in web applications that interact with databases, allowing unauthorized access to or manipulation of the data. This paper presents an in-depth analysis of SQL injection attacks, their mechanisms, and the potential risks they pose to organizational data. It examines various preventive measures and best practices to mitigate the vulnerabilities that lead to SQL injection. Techniques such as input validation, parameterized queries, and the use of prepared statements are explored as effective defences against these attacks*

Keywords: Parameterized Queries, Escaping Special Characters, Least Privilege Principle, Regular Security Audits, Use of ORM (Object-Relational Mapping) Libraries & Web Application Firewalls (WAFs)

REFERENCES

[1] Wei, K., Muthu Prasanna, M., & Suraj Kothari. (2006, April 18). Preventing SQL injection attacks in stored procedures. Software Engineering IEEE Conference. Retrieved November 2, 2007, from http://ieeexplore.ieee.org
[2] Thomas, Stephen, Williams, & Laurie. (2007, May 20). Using Automated Fix Generation to Secure SQL Statements. Software Engineering for Secure Systems IEEE CNF. Retrieved November 6, 2007, from http://ieeexplore.ieee.org
[3] Massachusetts Institute of Technology. Web Application Security MIT Security http://web.mit.edu/netsecurity/Camp/2003/clambert-slides.pdf
[4] Martin Bravenboer, Eelco Dolstra, Eelco Visser, Delft University of Technology The Netherlands. Preventing Injection Attacks with Syntax Embeddings A Host and Guest Language Independent Approach. Retrieved October 3, 2007, from http://portal.acm.org
[5] Yuji Kosuga, Kenji Kono, Miyuki Hanaoka Department of Information and Computer Science Keio University. Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection. Retrieved November 12, 2007, from IEEE Computer Society. http://ieeexplore.ieee.org
[6] Prithvi B, Madhusudan P, Venkatakrishnan VN (2010) CANDID: dynamic candidate evaluations for automatic prevention of SQL injection attacks. ACM Trans Inf System Security.
[7] Rahul J, Sharma P (2012) Survey on web application vulnerabilities (SQLIA,XSS) exploitation and security engine for SQL injection. In: Proceedings on CSNT 2012 IEEE international conference (978-0-7695-4692-6/1). IEEE, Washington, DC [8] Raju H, Cortesi A (2010) Obfuscation-based analysis of SQL injection attacks. In: ISCC '10 proceedings of the IEEE symposium on computers and communications, 931– 938. IEEE, Riccione