

# SQL Injection Testing in Web Applications Using SQLmap

**Sabina-Daniela AXINTE**

EUROQUALROM, University POLITEHNICA of Bucharest, Romania  
axinte\_sabina@yahoo.com

## **Abstract**

*SQL Injection (SQLI) is a penetration technique used for unauthorized direct access data from the database server, throughout a Web Application which is authorized to connect. A malicious SQL code can be introduced in entry fields, and the database can reply with unapproved information such as usernames and passwords of clients. An analytical overview of this technique, methods, tools and prevention actions is presented. An example of a step-by-step SQL Injection implementation with results is developed in order to understand how to increase website applications security.*

**Index terms:** SQL Injection, penetration testing, SQLmap, security, vulnerability

## **References:**

- [1]. OWASP Top Ten Project, (2014, Sep. 10) [Online]. Available: [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- [2]. I.-C. Mihai, Information Security, Sitech Publishing, 2012.
- [3]. J. Clarke, K. Fowler, E. Oftedal, and R.M. Alvarez, “SQL Injection Attacks and Defense”, Second Edition, Syngress, USA, 2012.
- [4]. Understanding SQL Injection, (2014, Sep. 14) [Online]. Available: [http://www.cisco.com/web/about/security/intelligence/sql\\_injection.html](http://www.cisco.com/web/about/security/intelligence/sql_injection.html)
- [5]. SQL Injection, (2014, Sep. 20) [Online]. Available: <http://technet.microsoft.com/en-us/library/ms161953%28v=SQL.105%29.aspx>
- [6]. Damn Vulnerable Web Application, (2014, Sep. 23) [Online]. Available: <http://www.dvwa.co.uk/>
- [7]. R. Rankins, P. Bertucci, C. Gallelli, and A.T. Silverstein, “Microsoft SQL Server 2008 R2 Unleashed”, SAMS, Indiana, USA, 2012.
- [8]. SQLmap, (2014, Sep. 27) [Online]. Available: <https://github.com/sqlmapproject/sqlmap/wiki/Usage>