

manos zalokostas

# 2011-2012

SQL Injection

Information &  
Networking Security  
Engineering



## Table of Contents

Introduction .....	4
What is SQL injection? .....	5
SQL Injection on a Web Application Login Input .....	5
SQL Injection on a Web Application URL input.....	6
SQL Injection Implementations.....	7
Common SQL Injection .....	7
Blind SQL Injection .....	8
Defensive Techniques Against SQL Injection .....	10
Encode critical data with hashing techniques .....	10
Restrain outputting articulate error messages.....	10
Escape Malicious Characters .....	11
Stored Procedures .....	12
Restrain Database Privileges.....	13
Prepared Statements .....	13
White List Maps .....	14
Conclusions .....	16
Bibliography .....	17

## Introduction

The aim of this report is to explore one of the most popular and hazardous application security attacks that is closely related to databases and SQL coding implementations; SQL Injection.

Initializing the report we will make a brief reference on some of the most appropriate attack's characteristics, and the techniques that are used to intervene on system's routines and take control of their function.

An enumeration of distinct best practices that could be recruited will follow along accompanied with short examples, all the way to qualify over and defend an SQL Injection attack. Also some of the most common drawbacks will be discussed for each.