## Contents

1. Introduction ........................................................................................................................................... 3
2. Research Problem and Significance of research work............................................................................. 4
3. Current Research Status .......................................................................................................................... 4
4. Methodology ........................................................................................................................................... 6
5. Objectives of Research ........................................................................................................................... 6
6. Chapter Planning ................................................................................................................................... 7
7. Survey of Literature ............................................................................................................................... 8
8. References ............................................................................................................................................. 11
1. Introduction

In the last two decades, the usage of Internet has grown many folds. Web applications have become one of the most important and critical interfaces for many enterprises. The use of web-based services (such as e-commerce, online banking and web-based emails, to name just a few) has become a wide-spread routine in today’s economic and social life. Countless applications are running on millions of servers world-wide, and their numbers are constantly increasing.

Because of huge growth in the internet usage, it became target to attackers and hackers for the attacks. It is easy to target less secure machines. It is evident, attacking less secure applications are easier to target the system. The complexity and extensibility of Web applications make these applications an easy prey by exploiting software vulnerabilities and defects. It is important for all enterprises, in order to maintain their reputation and keep their products valuable for users, to improve and secure their applications.

With more than 20 percent of all web vulnerabilities being attributed to SQL injections, this is the second most common software vulnerability attack on web applications. Therefore, having the ability to find and prevent SQL injection should be top of mind for web developers and security personnel.

According to numerous studies, the preferred method for attacking businesses’ online assets is via their Web applications. According to a study released in year 2014 by HP, 69% of Web applications scanned by the company had at least one SQL injection error, and 42% contained a cross-site scripting vulnerability. For every known Web application, seven times out of 10 there is at least one and usually, more than just one--SQL injection flaw just waiting to be discovered by an enterprising hacker.