Development of Semi-Automatic SQL Injection Exploitation Tool

**A Project Report**

**Presented At**

**Maharaja Surajmal Institute of Technology**

****

**By**

**Amit Sharma**

**0071312713**

**CSE (E)-- 4th yr.**

**PROJECT**

Development of Semi-Automatic SQL Injection Exploitation Tool

SUBMITTED IN PARTIAL FULFILLMENT OF THE DEGREE

OF

BACHELOR OF TECHNOLOGY

IN

“COMPUTER SCIENCE ENGINEERING”

By

Amit Sharma

To

**Maharaja Surajmal Insitute of Technology**

**Affiliated to Guru Gobind Singh Indraprastha University**

**Janakpuri, New Delhi-58**

**Certificate**

I hereby declare that this project report entitled “**Development of semi- automatic SQL injection tool**” by **Amit Sharma** enrolment number  **00713102713**, being submitted partial fulfilment of the requirements for the award of the degree of Bachelor of Technology (Computer Science Engineering)during academic year of 2015, is a bonafide record of my original work carried out under the guidance and supervision of **Mr. Yavar** and has not been presented elsewhere.

**Amit Sharma**

**00713102713**

**ACKNOWLEDGEMENT**

I hereby take this opportunity to thank all those people whose knowledge and experience helped me bring this report in its present form. It would have been a tough task for me to complete report without their help.

I would like to express my sincere gratitude to my project guide **Mr. Yavar**

for giving me the opportunity to work on this topic. It would never be possible for me to take this project to this level without his innovative ideas and his relentless support and encouragement.

I would like to express my gratitude to my group member, **Nishant Kumar Verma** for helping me in every aspect during the training phase as well as in carrying out the whole project.

Finally I would like to express my deep appreciation to my family and friends who have been a constant source of inspiration. I am internally grateful to them for always encouraging me wherever and whenever I needed them.

Amit Sharma

00713102713

|  |  |  |  |
| --- | --- | --- | --- |
| **Contents** | | | |
|  | | | **Page No.** |
| **Title** | | | |
| **Certificate** | | | |
| **Acknowledgement** | | | |
| **Abstract** | | | |
| **Chapter 1** | | **Introduction** | 8 |
| 1.1 | Python | | 9 |
| 1.2 | SQL Injection | | 10 |
| **Chapter 2** | | **Causes & Impacts** | 11 |
| 2.1 | | Causes | 12 |
| 2.2 | | Impacts | 12 |
| 2.3 | | Attack Vector | 13 |
| **Chapter 3** | | **System Requirements** | 17 |
| 3.1 | | Hardware Requirements | 18 |
| 3.2 | | Software Requirements | 18 |
| **Chapter 4** | | **Screenshots** | 19 |
| **Chapter 5** | | **Conclusion &Reference** | 28 |

# **ABSTRACT**

System administrators frequently rely on intrusion detection tools to protect their systems against SQL Injection, one of the most dangerous security threats in database-centric web applications. However, the real effectiveness of those tools is usually unknown until attacked by a hacker, which may lead administrators to put an unjustifiable level of trust in the tools they use. In this report, we present an experimental evaluation of the SQL Injection detection tool that we have prepared. To test the tool in a realistic scenario, Vulnerability and Attack Injection is applied in a setup based on two web applications of different sizes and complexities. Results show that the assessed tools have a very low effectiveness and only perform well under specific circumstances but still better than many of industrial standards, which highlight the limitations of current intrusion detection tools in detecting SQL Injection attacks. This tool which we have developed fills up the gap between the manual SQL injection and automated SQL injection. The main goal of the tools is to detect the SQL injection Vulnerability and exploitation of the same.