

OUTLINES:

1

1. Introduction
 - 1.1 Web application and SQL injection attacks
 - 1.1.1 Web application architecture
 - 1.1.2 An example of SQL injection attacks tautology
 - 1.1.3 Other kinds of SQL injection attacks

2. Related work
 - 2.1 Web framework
 - 2.2 Static analysis
 - 2.3 Dynamic Analysis
 - 2.4 Combined method of static and dynamic analysis
 - 2.5 Instruction-set randomization
 - 2.6 SQL query profiling
 - 2.7 Machine learning method

3. Implemented Method
 - 3.1 Implemented method
 - 3.2 Other examples applying implemented method

4. Experiment and evaluation
 - 4.1 Experiment method
 - 4.2 Experimental results analysis
 - 4.2.1 Detection/attack rate analysis
 - 4.2.2 Comparison of detection and prevention
 - 4.2.3 Comparison of additional detection factors

5. Conclusion

Acknowledgement

References

LIST OF FIGURES

| Figure No. | Title | Page No. |
|------------|--|----------|
| 1 | Web Application Architecture | 1 |
| 2 | Example of interaction between a user and a typical web application | 3 |
| 3 | SQL normal and SQL injection data flow | 5 |
| 4 | Structure of SANIA (Syntactic and Semantic analysis) | 6 |
| 5 | Schematic diagram for instruction-set randomization | 8 |
| 6 | Showing vulnerable input in web application | 10 |
| 7 | Showing ,get authorized with vulnerable input in web application | 11 |
| 8 | Taking vulnerable input into secure login and getting o/p as wrong user & password combination | 12 |

LIST OF TABLES

| Table No. | Title | Page No. |
|-----------|--|----------|
| 1 | Comparison of detection and prevention methods by attack types | 15 |
| 2 | Comparison of our detection method to other detection methods | 17 |

List of Abbreviation

| Symbols | Meaning |
|----------------|---|
| CGI | Common gateway interface |
| SQLIA | Structure Query Language injection attack |
| AMNESIA | Analysis & monitoring for neutralizing SQL injection attack |
| JDBC | Java database connectivity |
| OWASP | Open web application security Project |
| ZAP | Zed attack Proxy |
| JDC | JAVA database connectivity |