

CONTENTS

INTRODUCTION GENERAL	1
INTRODUCTION GENERAL	2
CHAPITRE I - WEB SECURITY	3
1. Introduction	4
1.1. What is security.....	5
1.2. The foundations of security.....	6
1.3. Threats, vulnerabilities, and attacks defined.....	7
1.4. How to implement safety assessment	7
1.4.1. Asset Classification	8
1.4.2. Threat analysis.....	10
1.4.3. Risk analysis	10
1.4.4. Design of security programs	13
2. Web security.....	13
2.1. Targets and impacts of web attacks	13
2.2. The web application	14
2.3. 96% of Tested Applications Have Vulnerabilities (Report of CENZIC).....	14
2.4. Top 10 OWASP	15
2.5. Understanding the dangers of insecure web applications	16
2.6. Rise of web security	18
2.7. Improving Security in Web Applications	19
2.8. Web application security lifecycle (S-SDLC).....	19
2.8.1. Secure development.....	20
2.8.2. Secure deployment.....	20
2.8.3. Secure operation	21
2.9. Common detectable application vulnerabilities.....	21
3. Conclusion	22
CHAPITRE II - SQL INJECTION	23
1. Introduction	24
2-Understanding SQL Injection	24
3-Understanding How It Happens	27
3.1. Example of Incorrectly Handled Escape Characters.....	27
4 - Finding SQL Injection	28
4.1. Testing by Inference	28

4.2. Identifying data entry	29
4.3. GET Requests	29
4.4. POST Requests	30
4.5. Browser modification extensions	30
4.6. Proxy servers	31
4.7. Workflow of Web request and Web response.....	31
4.8. Database Errors	32
5. Differentiating Numbers and Strings	33
5.1. Example:	33
6. Inline SQL Injection.....	33
6.1. Injecting Strings Inline	34
6.2. Injecting Numeric Values Inline	35
7. Terminating SQL Injection	35
7.1. Database Comment Syntax.....	36
7.2. How Using Comments to terminate SQL statements	36
8. Conclusion	38
CHAPITRE III - THE APPROACH PROPOSED	39
1. Introduction	40
2. Definition of SQLIA	40
3. SQL Injection Attacks (SQLIA) Process	40
4. Types of SQLIA.....	41
4.1. Tautologies	41
4.2. Piggy-backed Query	41
4.3. Logically Incorrect.....	42
4.4. Union query	42
4.5. Stored Procedure.....	43
4.6. Inference	43
4.7. Alternate Encodings.....	44
5. The proposed approach	45
6. The method – (Method Detector)	45
6.1. Example	46
6.2. Queries	46
6.3. Links.....	46
6.4. Results of the test	47
6.5. Analyze of the results.....	47
7. Related work	47

7.1. SWADDLER	47
7.2. SQL Prevent.....	47
7.3. SQL Lrand.....	48
7.4. SAFELI	48
7.5. SQLIPA	48
7.6. SQLCheck	48
7.7. IDS (Intrusion Detection Systems)	49
7.8. Detection based on removing SQL query attribute values	49
7.9. DIWeDa.....	49
7.10. Context Sensitive String Evaluation (CSSE)	50
7.11. CANDID	50
7.12. Automated Approaches.....	50
7.13. AMNESIA.....	51
8. Comparison of SQL Injection detection techniques with respect to attack types	51
9. Percentage of SQL Injection Detection Techniques.....	52
10. Conclusion	53
CHAPTER IV ANALYSIS, RESULTS AND EXPERIMENTAL	54
1. Introduction	55
2. Platform.....	55
2.1. Visual Studio	55
2.2. C#.....	55
2.3. XAMPP	55
2.4. PHP	56
2.5. MySQL	56
3. Experimentation	56
4. The Sites of experimentation	56
4.1. The BTS Lab	56
4.1.1. Presentation	56
4.1.2. Architecture.....	57
4.2. TEST Site.....	57
4.2.1. Presentation	57
4.2.2. Architecture.....	57
4.3. Buggy Web Application (bWAPP)	58
4.3.1. Presentation	58
4.3.2. Architecture.....	58
5. The scanners used in the experiment.....	58

5.1. Netsparker	58
5.2. OWASP ZAP 2.4.2	58
6. Experiment of the Method	59
6.1. bWAPP	59
6.1.1. Queries	59
6.1.2. Links (bWAPP)	59
6.1.3. Method	59
6.1.4. Test method with queries.....	59
6.1.5. Bwapp – SQL Injection – Bypass Authentication.....	60
6.1.5.1 Queries	60
6.1.5.2 Links	60
6.1.5.3 Method	60
6.1.5.4 Test method with queries	60
6.1.6 Bwapp – SQL Injection – Blind – Boolean- Based.....	61
6.1.6.1 Queries	61
6.1.6.2 Links	61
6.1.6.3 Method	61
6.1.6.4 Test method with queries	61
6.2. BTS Lab Site	62
6.2.1 Queries	62
6.2.2 Links	62
6.2.3 Method	62
6.2.4 Test method with queries	62
7. Comparison the method with different scanner	63
7.1. List of the URL (TEST Site)	63
7.2. Low Security	63
7.3. Medium Security.....	64
7.4. High Security	65
7.5 The result of the vulnerability (12 page vulnerable).....	66
7.6 The result of False positive/the vulnerability (12 page vulnerable).....	66
8. Conclusion	67
CONCLUSION GENERAL.....	68
CONCLUSION GENERAL	69
REFERENCES	70