



FINAL YEAR PROJECT REPORT

**TO AUTOMATE SECURITY TESTING OF WEB
APPLICATIONS BY USING MACHINE
LEARNING**

**In fulfillment of the requirement
For degree of
BS (COMPUTER SCIENCES)**

By

HAMZA SARWAR

51210 BSCS

USAMA AMJAD

51477 BSCS

MUHAMMAD AHRAR KHAN

53682 BSCS

SUPERVISED

BY

SIR NOMAN

BAHRIA UNIVERSITY (KARACHI CAMPUS)

SPRING-2021

DECLARATION

We hereby declare that this project report is based on our original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

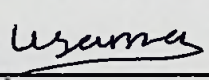
Name : HAMZA SARWAR

Reg No. : 02-134172-130

Signature :  _____

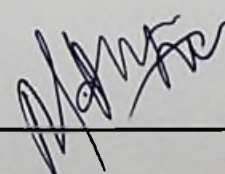
Name : USAMA AMJAD

Reg No. : 02-134172-135

Signature :  _____

Name : M AHRAR KHAN

Reg No. : 02-134172-158

Signature :  _____

Date : 29-MAY-2021

ACKNOWLEDGMENTS

The copyright of this report belongs to Bahria University according to the Intellectual Property Policy of Bahria University BUORIC-P15 amended on April 2019. Due acknowledgement shall always be made of the use of any material contained in, or derived from, this report.

ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express my gratitude to my research supervisor, Sir Noman for his invaluable advice, guidance and his/her enormous patience throughout the development of the research.

In addition, I/We would also like to express my gratitude to my/our loving parent and friends who had helped and given me encouragement.

TO AUTOMATE SECURITY TESTING OF WEB APPLICATIONS BY USING MACHINE LEARNING

ABSTRACT

To automate the security testing of the web applications just by using the Machine Learning tool in web application which assesses the security and vulnerabilities found in the web application and also produces group of some scanned results. Both the administrators and the scammers and the exploiters can also use some equivalent tool for the fixing or the exploiting of system, and administrators will really get to conduct scanned and the fixed problems before attacker does same scan and then exploit any vulnerability be found because of the web applications which are typically being developed with the hard time constraints which are often being deployed with some security vulnerabilities. The web scanners can also help in locating these vulnerabilities and their purpose to worry on appliance from attacker's view by issuing huge amount of interaction within it. The two widely dangerous vulnerabilities in the websites are the SQL injections being listed by the Open Web Application Security Project (OWASP) and the cross site scripting, in due of damage that they will cause to victim business and the located and also another vulnerability like the Cross site request forgery. In order to adapt to the difficulties, it is imperative to add security counter and measures in the website scanning, e.g, web crawler in order to diminish dangers of the vulnerabilities. The advance features which triggers use of the web application which are being given by the technologies and the architecture of the web applications with recognition of the forums, the web services and the blogging, the attackers also started about taking interest in the web applications. This joint effort of the researchers which is also utilized in the numerous speculation and layers is the establishment of the reason for the vulnerability in the websites. Numbers of the revealed website insecurities being expanded quickly. The loop holes and the bug also exists on online platforms which can also be misused by programmer and are referred to website vulnerability. Our project proposes method in order to evaluate web vulnerability scanners for the most used types of the online vulnerability are being injected in web application's code which then being checked by scanners.

TABLE OF CONTENTS

DECLARATION	II
APPROVAL FOR SUBMISSION	III
ACKNOWLEDGEMENTS	V
ABSTRACT	VI
TABLE OF CONTENT	VII
LIST OF TABLES	-
LIST OF SYMBOLS/ ABBREVIATION	-
LIST OF APPENDICES	-
REFERENCES	77

CHAPTER # 1

	INTRODUCTION	17
1.1	BACKGROUND	17
1.1.1	CROSS-SITE SCRIPTING (XSS)	17
1.1.2	SQL INJECTION	17
1.1.3	CODE INJECTION	17
1.1.4	BROKEN ACCESS CONTROL	17

1.1.5	WEB APPLICATION SCANNERS	17
1.1.6	WHAT IS VULNERABILITY SCANNER?	18
1.2	PROBLEM STATEMENT	18
1.3	AIMS AND OBJECTIVES	19
1.4	SCOPE OF PROEJCT	19

CHAPTER # 2

	LITRATURE REVIEW	20
2.1	WHY YOU NEED TO SECURE YOUR WEB APPLICATION.	20
2.1.1	WHY ARE WEB APPLICATION VULNERABLE?	20
2.1.2	THE NEED FOR AUTOMATED WEB APPLICATION SECURITY SCANNING	21
2.2	WEB VULNERABILITY SCANNER	22
2.3	-	
2.4	WEB APPLICATION VULNERABILITY	23
2.4.1	CROSS-SITE SCRIPTING	25
2.4.2	SQL INJECTION	25
2.4.3	AUTHENTICATION BYPASS	25

2.4.4	FORCEFUL BROWSING	25
2.4.5	COOKIE POISONING	25
2.4.6	CROSS SITE REQUEST FORGERY (CSRF)	25

CHAPTER # 3

	DESING AND METHODOLOGY	27
3.1	THE ARCHITECTURE OF VULNERABILITY SCANNER	27
3.2	HOW WEB VULNERABILITY SCANNER WORKS	27
3.3	PROJECT METHODOLOGY	28
3.3.1	CRAWLING MODULE	29
3.3.2	PARSING MODULE	29
3.3.3	ATTACK MODULE	29
3.3.4	ANALYSIS MODULE	29

CHAPTER # 4

	IMPLEMENTATION	31
4.1	COMPONENTS IN PROJECT	31
4.2	PROJECT INITIATION	31

4.3	PROJECT DESIGN	31
4.4	PROJECT WORKING	31
4.5	PROJECT FUNCTIONALITIES	31
4.6	CODING SCREEN SHOTS	33
4.6.1	MAIN PAGE	33
4.6.2	LOGIN PAGE	34
4.6.3	SIGN UP PAGE	35
4.6.4	PDF REPORT PAGE	36
4.6.5	PASSWORD RESET FORM	37
4.6.6	PASS RESET NOTIFICATION PAGE	37
4.6.7	NEW PASSWORD PAGE	38
4.6.8	PASS RESET COMPLETE PAGE	38
4.6.9	CRAWLING AND PARSING	39
4.6.10	ATTACKING AND ANALYSIS	40
4.6.11	REPORT	42
4.6.12	MAIN PAGE SCREEN SHOTS	43
4.6.13	DATABASE	47
4.6.14	LOGIN/SIGNUP	47

4.6.15	REGISTRATION SUCCESSFUL	48
4.6.16	RESET YOUR PASSWORD MESSAGE	49
4.6.17	PASSWORD RESET LINK	50
4.6.18	NEW PASSWORD MESSAGE	50
4.6.19	PASSWORD CHANGED MESSAGE	51
4.6.20	CRAWLING AND PARSING PROCESS	51
4.6.21	ATTACKING AND ANALYSIS PROCESS	55
4.6.22	PDF REPORT GENERATED PROCESS	57

CHAPTER # 5

	RESULT AND DISCUSSION	60
5.1	TESTING	60
5.1.1	DRUPAL METRICS DATASET	67
5.1.2	DRUPAL TOKEN DATASET	69
5.1.3	MOODLE METRICS DATASET	71
5.1.4	MOODLE TOKEN METRICS	73
5.1.5	PHP MYADMIN METRICS	76