

Final Year Project Report

Web Application Security Risk Assessment



Bahira University Islamabad

Supervisor

Dr. Waqas Aman

Group Members

Alina Khalid (01-134141-009)

Sidra Khalid (01-134141-120)

Computer Science Department

A report submitted in the partial fulfilment of degree of BS(CS)

Abstract

In today's software industry web development is the most essential and emerging field. Websites are used to provide information to the users about any specific area of interest. There are numerous websites and web applications that are available online for users. Information is readily available due to the advancements in the technology, but it's not a safe world today. One cannot simply forget the concerns that are raised with respect to the security and safety to the intellectual property of an individual or an organization. As everything good has a bad side too it so is the case here as your information can also be used against you, hackers can forge the information on your website and can also make your application unavailable to the legitimate user which can lead to a great loss in terms of revenue in an organization. IT companies and corporate businesses spend millions of dollars to safeguard their websites and online systems from hackers intrusion and damaging the organizations reputation. The sole objective of our project is to safeguard an online system or a website by informing the organizations about the vulnerabilities and loop holes which can be exploited in future and cause harm to their business. This will help the web developers in better understanding of the weakness and making their application more secure in future. This project is related to the domain of information security and will help web developers in testing of their websites and hence in development of a secure system which will guard-off the system against web attacks and related vulnerabilities.

Contents

1	Introduction	1
1.1	Problem Statement	1
1.2	Project Objectives	2
1.3	Project Motivation	2
1.4	Methodology	2
1.5	Summary	3
2	Literature Review	4
2.1	Introduction	4
2.2	OWASP RRM	4
2.3	MITRE CWRAF	5
2.3.1	Challenge	5
2.3.2	Solution	5
2.4	MITRE CWSS	5
2.4.1	Problem	5
2.4.2	Solution	6
2.5	OSSTMM	6
2.5.1	Challenge	6
2.5.2	Solution	6
2.6	OWASP ASVS	7
2.6.1	Challenge	7
2.6.2	Solution	7
3	Requirement Specification	8
3.1	Overview	8
3.2	Introduction	8
3.3	Application System Environment	9
3.4	Functionality	9
3.5	Functional Requirements	10
3.5.1	Login/Signup	10
3.5.2	Url Validation	10
3.5.3	Scan Project	10
3.5.4	Report Generation	10
3.5.5	Download Report	10

3.5.6	Upload Report	10
3.5.7	Id Extraction	11
3.5.8	Comparing Id's With CWE-list	11
3.5.9	Fetching data from CWE-list	11
3.5.10	Impact Scorecard	11
3.5.11	Risk Analysis Report	11
3.6	Non-Functional Requirements	11
3.6.1	Performance	11
3.6.2	Portability	11
3.6.3	Security	11
3.6.4	Price	11
3.6.5	Backup	12
3.7	Use Cases	12
3.7.1	System Use Case	12
3.7.2	Use Case 01: Scan for vulnerabilities	13
3.7.3	Use Case 02: Id extraction through parsing	14
3.7.4	Use Case 03:Generation of Impact Score Card	15
3.7.5	Use Case 04:Risk analysis is performed	16
3.7.6	Use Case 05:Generation of Risk Assessment Report	17
4	Design	18
4.1	System Architecture	18
4.2	Data Flow Diagram	19
4.2.1	Level 0 DFD	19
4.2.2	Level 1 DFD	19
4.2.3	Level 2 DFD	20
5	System Implementation	22
5.1	Strategy	22
5.2	Tools And Techniques	22
5.2.1	Arachni-1.5.1	22
5.2.2	Sublime Text Editor	22
5.2.3	Risk Analysis	25
5.2.4	Impact Score Card	25
5.2.5	Risk Assessment Report	25
5.2.6	CWRAF	26
5.3	Development Environment	26
5.3.1	Encryption Library	26
5.3.2	File Uploading Class	27
5.3.3	Form Validation	27
5.3.4	Session Library	27
5.3.5	Database Configuration	27
5.3.6	Connecting to Database	27
5.4	Steps of Implementation	27
5.4.1	Insertion of URL of Any Live Website	27
5.4.2	Scanning of Website	28

5.4.3	Report of Vulnerabilities	28
5.4.4	Download Report in Jason Format	30
5.4.5	Import Report and Vulnerability Details Extraction	32
5.4.6	Input Details in Formula for Risk Analysis	32
5.4.7	Import Jason Report on Website	32
5.4.8	File Upload	36
5.4.9	Parsing the Report	37
5.4.10	Comparison of CVE-db-xml and Json Report	38
5.4.11	Computation of Risk Analysis	39
6	System Testing and Evaluation	41
6.1	Software Testing Techniques	41
6.2	Test Cases	41
6.2.1	Test Case 01: URL validation	42
6.2.2	Test Case 02: URL Format	42
6.2.3	Test Case 03: Report Generation	42
6.2.4	Test Case 04: Report Parsing	43
6.2.5	Test Case 05: ID Comparing	43
6.2.6	Test Case 06: Score Card	43
7	Conclusion	44
7.1	Our Work	44
7.2	Future Work	45

List of Figures

1.1	Methodology	3
3.1	System Environment	9
3.2	System Use Case Diagram	12
3.3	scanning vulnerabilities of project	13
3.4	Id extraction through parsing	14
3.5	Generation of Impact Score Card	15
3.6	Risk analysis is performed	16
3.7	Generation of Risk Assessment Report	17
4.1	Application Architecture	19
4.2	LEVEL 0 Generating XML or JASON File	19
4.3	LEVEL 1	20
4.4	LEVEL 2	21
5.1	displays the user guide of sublime text editor	24
5.2	displays the working of MVC framework	25
5.3	Interaction Amongst the CWE CWRAF and CWSS	26
5.4	Arachni Interface	28
5.5	Provide URL	28
5.6	Enlisting The Vulnerabilities Categorized as High, Medium and Low	29
5.7	Vulnerabilities Rated As Medium Risk To The System	29
5.8	Vulnerabilities That Rated As Low Risk To The System	30
5.9	Vulnerabilities Rated as Informational Risk To The System	30
5.10	Format for Downloading Vulnerability Report	31
5.11	Screenshot For Report Generated in .Jason Format	33
5.12	Screenshot of Login Page	34
5.13	Screenshot of Signup Page	35
5.14	User Panel	36
5.15	Screenshot of Jason File Upload	37
5.16	Parsing the File	38
5.17	Depicts Comparison Between CVE-db and Jason File	39
5.18	Output Displayed to User	40

List of Tables

3.1	Scan for vulnerabilities	13
3.2	Id extraction through parsing	14
3.3	Generation of Impact Score Card	15
3.4	Risk analysis is performed	16
3.5	Generation of Risk Assessment Report	17
6.1	URL validation	42
6.2	URL Format	42
6.3	Report Generation	42
6.4	Report Parsing	43
6.5	ID comparing	43
6.6	Score card	43