Tables of content

Chapter 1 : **Introduction**

1.1 Motivation 3

1.2 Web Vulnerability Attacks 4

Chapter 2 : **Cross Site Scripting**

2.1 Actors in an XSS attack 6

2.1.1 The website 6

2.1.2 The victim. 6

2.1.3 The attacke 6

2.2 Types of Xss attacks 7

2.2.1 Persistent Attack 8

2.2.2 Non-persistent attack 9

2.2.3 DOM based attack 10

2.3 Dangers of XSS vulnerabilities 11

Chapter 3 : **Present XSS detection technique**

3.1 Current browser security mechanisms and their limitations 13

3.1.1 Zone security 13

3.1.2 XSS Filter 13

3.1.3 Disabling JavaScript 13

3.2 Server side defenses against XSS attacks 14

3.2.1 Writing safe code 14

3.2.2 Adding double quotes around all tag properties 14

3.3 Adding double quotes around all tag properties 15

3.3.1 Code-rewriting (Browser Shield, Core Script) 15

3.2.2 Anomaly detection approaches 15

Chapter 4 : **Observation and Problem Selection**

4.1 Problem Selection 17

4.1.1 Client-side URL XSS attack 17

4.1.2 Client-side Input field attack 17

4.1.3 Server-side XSS attack 17

4.2 Proposed Model for Defense against XSS attack 18

4.2.1 Differentiating defense mechanism via Input Validation 18

4.2.2 Differentiating defense mechanism via Escaping and Sanitizing 18

4.3 Choice of Algorithm 21

4.3.1 Regular Expression 22

4.3.2 Regular expressions in JavaScript 22

4.4 Current Limitations 24

Chapter 5 : **Results and Discussion** 26

Chapter 6 : **Conclusion and Future Scope** 32

References

Appendix

List of tables

Table No	Title	Page No
Table 5.1	Summary of test results	29
Table 5.2	Malicious string testing results.	29
Table 5.3	XSS attack testing results on the designed model.	30

LIST OF FIGURES

No	Title	Page No
Figure2.1	History of XSS attack	7
Figure2.2	Sequence diagram of Persistent attack	8
Figure2.3	Sequence diagram of Non Persistent attack	9
Figure3.1	Current solution to set security policies for websites in I E 6 and 7	10
Figure5.1	XSS attack before implementation of deigned mode	26
Figure5.2	XSS attack after implementation of designed model.	27
Figure5.3	Attackers Add an Attack Code in Question Field and Submits the Form.	27
Figure5.4	When Someone Views This Question, an Alert Pops-Up, as Script Executes in Browser	28
Figure5.5	Web Application Integrated With Our Framework (Secured) Web Applications Protected by Proposed Approach.	28