Contents

List of Figures 3

List of Tables 1

1 INTRODUCTION 2
- 1.1 Basics of XSS attack . . . 2
- 1.2 Attack vectors . . . 3
- 1.3 Scenarios . . . 5
  - 1.3.1 Scenario I . . . 6
  - 1.3.2 Scenario II . . . 7
  - 1.3.3 Scenario III . . . 8
- 1.4 Distinguishable characteristics for attack and benign script . . 9
- 1.5 Overview of existing approaches . . . 9
- 1.6 Motivation . . . 10
- 1.7 Objectives . . . 10
- 1.8 Report organization . . . 10

2 BACKGROUND 12
- 2.1 Classifiers . . . 12
- 2.2 Feature selection algorithms . . . 15
- 2.3 Malicious and benign scripts . . . 17
- 2.4 XSS attack and its types . . . 17
  - 2.4.1 Persistent or Stored XSS attack . . . 18
  - 2.4.2 Non-Persistent or Reflected XSS attack . . . 18
  - 2.4.3 DOM-based XSS attack . . . 18

3 LITURATURE SURVEY 20
- 3.1 An overview of the existing detection approaches . . . 20
- 3.2 Issues to be addressed . . . 22
- 3.3 Overview of existing prevention approaches . . . 22

4 DATASET PREPARATION 24
4.1 Data gathering 24
4.2 Feature extraction 25
4.3 C routines for dataset preparation 25
4.4 Increase in the population density of the dataset 28
4.5 Normalization of the dataset 28

5 ATTACK DETECTION FRAMEWORK 30
5.1 Proposed framework 31
5.2 Experimental results 38
5.2.1 Results 38
5.3 Comparison with other methods 39

6 ATTACK PREVENTION ARCHITECTURE 41
6.1 Background 41
6.2 Proposed framework 42
6.3 Issues to be addressed 44

7 CONCLUSION AND FUTURE WORK 45
7.1 Future work 45

Bibliography 46

List of Figures

1.1 Typical scenario of reflected XSS attack generated through mail. 6
1.2 Typical scenario of XSS attack through guestbook. 7
1.3 Typical scenario showing reflected XSS attack through specially crafted links in attacker's website. 8

2.1 An overview of XSS attack 17

4.1 Example of a benign JavaScript 24
4.2 Example of an attack script 25
4.3 A portion of the original dataset 29
4.4 A portion of the normalized dataset 29

5.1 Proposed framework for XSS attack detection 32
5.2 Optimal feature selection framework 37
5.3 Output of the rank aggregation algorithm with optimal feature subset 38
5.4 ROC curve 40

6.1 An XSS response system to mitigate XSS attacks 43

List of Tables

3.1 Summary of related works 21

4.1 Description of extracted features 26

5.1 Symbol table 31
5.2 Results obtained from various feature selection algorithms . . 37
5.3 Accuracy of the classes based on the feature subsets 40