E-Mail Header Injections

An Analysis of the World Wide Web

by

Sai Prashanth Chandramouli

A Thesis Presented in Partial Fulfillment
of the Requirement for the Degree
Master of Science

Approved April 2016 by the
Graduate Supervisory Committee:

Dr. Adam Doupe, Chair
Dr. Gail-Joon Ahn
Dr. Ziming Zhao
\memberThree
\memberFour

ARIZONA STATE UNIVERSITY

May 2016

ABSTRACT

ACKNOWLEDGEMENTS

A project of this size is never easy to complete without the help and support of other people. I would like to take this opportunity to thank some of them.

This thesis would not have been possible without the help and guidance of my thesis advisor, and committee chair - the brilliant Dr. Adam Doupe. This project was his brainchild, and he held my hand through the entire project.

I would like to thank Dr. Gail-Joon Ahn, for being part of the committee, for all his help, and his valuable input on the changes to be made to make the project more impactful.

I would also like to thank Dr. Ziming Zhao, for being a part of my committee, and for the constant motivation.

I would like to thank the members of the SEFCOM, for their support, and would like to especially thank Mike Mabey, for helping set up the infrastructure for this project, and Marthony Taguinod, for helping me document this project.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

Chapter 1

INTRODUCTION

Franklin *et al.* (2007)

Chapter 2

E-MAIL HEADER INJECTION BACKGROUND

2.1 Problem Background

This section describes the background of the vulnerability.

2.2 History of E-Mail Injection

This section describes the history of the vulnerability.

2.3 Languages Affected

This section describes the popular languages which exhibit this type of vulnerability.

- PHP - Describe which functions/params are affected
- Java - Describe which functions/params are affected
- Python - Describe which functions/params are affected

2.4 Potential Impact

This section describes the impact of the vulnerability, and how wide/far-reaching the effects could be.

Chapter 3

SYSTEM DESIGN

3.1 Our Approach to the Problem

This section will describe the approach we have taken. Will discuss about blackbox testing, and why we chose it.

3.2 System Architecture

This will have a diagram of our architecture, including all 8 components.

3.3 System Components

This will discuss in detail about the components of the system, like the following:

3.3.1 Crawler

Describe the functionality of the Crawler

3.3.2 Form Parser

Describe the functionality of the Form Parser

3.3.3 E-Mail Field Checker

Describe the functionality of the E-Mail Field Checker

3.3.4 Fuzzer

Describe the functionality of the Fuzzer

Non-Malicious Payload

Malicious Payload

3.3.5 E-Mail Analyzer

Describe the functionality of the E-Mail Analyzer

3.3.6 Database

3.4 Design Issues

This section will describe the issues we might face with the approach that we have chosen, and the design decisions.

3.5 Assumptions

This discusses the assumptions that we have made while building the system, examples include:

1. Crawler is not blocked by the firewalls.

2. The Crawler feed is an ideal representation of the World Wide Web.

REFERENCES

Franklin, J., A. Perrig, V. Paxson and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants.", in "ACM conference on Computer and communications security", pp. 375–388 (2007).

Pietraszek, T. and C. V. Berghe, "Defending against injection attacks through context-sensitive string evaluation", in "Recent Advances in Intrusion Detection", pp. 124–145 (Springer, 2005).

Zanero, S., L. Carettoni and M. Zanchetta, "Automatic detection of web application security flaws", Black Hat Briefings (2005).

APPENDIX A

CODE SNIPPETS