Server-Side Protection of Web Application Against Cross-Site Scripting Attack

Dissertation

Submitted To:

Central Department of Computer Science and Information Technology

Institute of Science and Technology

Tribhuvan University

In Partial Fulfillment of the Requirements for the Degree of

Master of Science
In
Computer Science and Information Technology

By:
Tek Raj Subedi

March, 2009
Kirtipur, Nepal

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date: ……..

LETTER OF RECOMMENDATION

Mr. ***Tek Raj Subedi*** has carried out this thesis work in title "**SERVER-SIDE PROTECTION OF WEB APPLICATION AGAINST CROSS-SITE SCRIPTING ATTACK**" under my supervision and guidance. In my best knowledge this dissertation/thesis successfully completed with fulfills the requirements for the aware of the Degree of Master's in computer science and information technology, therefore I recommended for further evaluation.

……..
Dr. Subarna Shakya
(Associate Professor)
Department of Electronics and Computer Engineering
Pulchowk Campus, Pulchowk
(Supervisor)

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

We certify that we have read this dissertation work and in our opinion it is satisfactory in the scope and quality as a dissertation as the partial fulfillment of the requirement of Master in Computer Science and Information Technology from Tribhuvan University, Nepal.

Evaluation Committee

Dr. Tanka Nath Dhamala **Head, Central Department of Computer Science and Information Technology** **Tribhuvan University, Kirtipur**	**Dr. Subarna Shakya** **(Associate Professor)** **Department Electronics and Computer Engineering** **Pulchowk Campus, Pulchowk** **(Supervisor)**
(External Examiner)	**(Internal Examiner)**

Date: …….

Acknowledgement

This dissertation/thesis work would not exist without help, advice and encouragement of many people. I thank my supervisor, Dr. Subarna Shakya (Associate Professor), who taught me about research methodology. His knowledge and suggestion always brought a curiosity, interest and labor of study during the most challenging time of research. I want to thank Mr. Dinesh Bajracharya, Central Department of Computer Science and Information Technology, as my co-supervisor for his continuous support and suggestion throughout my thesis work.

I am grateful to the Prof. Dr. Shashidhar Ram Joshi, Prof. Sudarshan Karanjeet, Mr. Min Bahadur Khati, Mr. Sammujjwal Bhandari, Mr. Bishnu Gautum, Mr. Jagadish Bhatta, Mr. Arjun Singh Saud, Central Department of Computer Science and Information Technology while not being directly involved in my dissertation work, nevertheless influenced me greatly. I am especially grateful to Dr. Tankanath Dhamala, Head, Central Department of Computer Science and Information Technology, who has been a positive and encouraging on my research work.

I am also thankful to my friends Mr. Rabin Shrestha, Mr. Madhav Dhakal. Finally, I am thankful to my parents, my wife who were ultimately the people, who prepared me for this endeavor.

Tek Raj Subedi
M. Sc. (Computer)
CDCSIT, T.U., Kirtipur

Abstract

Web applications are accessed using the Internet and face risks associated with usage of the Internet. There are different attacking techniques against clients while using Web application. The attack using XSS attack technique is frequent. XSS attack is an attack on the privacy of client, by injecting malicious code to vulnerable Web site and forcing the client to click it. Cross-Site Scripting (XSS) is one of the most common application level attacks that attackers use to sneak into the Web applications today. The goal of the XSS attack is to steal the client cookies, or any other sensitive information, which can identify the client with the Web site. With the token of the legitimate user at hand, the attacker can proceed to act as the user in his/her interaction with the site-specifically impersonate the user. In this dissertation/thesis work, the study of different attacking techniques through XSS on the Web application has been shown and addressed some of the prevention techniques, which is related with the filtration (input and output) mechanism through server-side. XSS attack is the attack against Web application and that harms the user or client. Depending on the position of the provided solution for the client in the Web application, solutions are divided into three classes: client-side solution, server-side solution, and third party application fire-wall. Solution has been given through server-side for the client. Different formats for the filtration have defined using regular expression. It has been analyzed to which condition which provided filtering formats are when appropriate. The comparisons have shown among the defined formats within the server-side solution. The comparison is not about the execution efficiency but it's about the malicious input format filtering situation. If the same domain is used any number of attacking messages according to defined format can be filtered. Since XSS attack is vague subject, it covers some specified condition following the research view.

Abbreviations

ASP	Active Server Pages
CERT	Computer Emergency Response Team
CSS	Cross-Site Scripting
CVE	Common Vulnerabilities and Exposures
DFA	Definite Finite Automata
DBMS	Database Management System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
H/W	Hardware
IDS	Intrusion Detection System
JSP	Java Server Pages
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security project
PHP	Hypertext Preprocessor
RE	Regular Expression
S/W	Software
SSL	Secure Socket Layer
URL	Uniform Resource Locator
WWW	World Wide Web
XSS	Cross-Site Scripting

Contents

List of tables

List of figures