INTEGRATING CROSS-SITE SCRIPTING (XSS) PREVENTION IN MOZILLA FIREFOX

By

Clenista, Allysa Mariel T.

Rosauro, Chrestine Joy V.

ATENEO DE DAVAO UNIVERSITY

COMPUTER STUDIES DIVISION

DAVAO CITY

SEPTEMBER, 2010

INTEGRATING CROSS-SITE SCRIPTING (XSS) PREVENTION IN MOZILLA FIREFOX

A Mini-Thesis

Presented to the

Undergraduate Faculty of the

Computer Studies Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

By

Clenista, Allysa Mariel T.

Rosauro, Chrestine Joy V.

ATENEO DE DAVAO UNIVERSITY

COMPUTER STUDIES DIVISION

SEPTEMBER, 2010

TABLE OF CONTENTS

ABSTRACT

Websites nowadays are more complex, containing a lot of dynamic content making the experience for the user more enjoyable. This dynamic content is achieved through the use of web applications which can convey different output to a user. Dynamic websites suffer from a threat called Cross-Site Scripting (also known as XSS) attack. There were number of studies which focus on creating a tool in detecting this XSS attack and some by avoiding such attack.

In this paper, the proponents discussed the development of XSS prevention that is integrated in the Firefox browser through an extension. The web page which is requested by the user is being processed through parsing algorithm first. The page then is checked against XSS attack strings. Pages that are vulnerable to XSS attacks are being marked. The marked outputs were returned to the user to prevent unintended execution of the scripts and a notification will be sent. The said outputs will be encoded which is then redirected to a safe page. The approach developed by the proponents which was named XSStopper, runs at varied time and evaluates one page at a time.

Keywords:

XSS, XSS attacks, Parsing, String Matching, Caching

Chapter 1

INTRODUCTION

1.1 Background of the Study

In the Internet World Stats, 28.7% of the world's population is being penetrated by internet usage. And many of the Web sites today add dynamic content to a web page making the experience of the user more enjoyable. This added dynamic content is a content-generated by some server processes, which when delivered can behave and display differently to the user depending on the user settings or needs. Dynamic Web sites had a threat that static do not had, this threat is called "cross-site scripting," also known as "XSS". A web page contains both text and HTML markup that is generated by the server and interpreted by the client browser. Web sites that generate dynamic pages did not have complete control over how their outputs are interpreted by the client. The heart of the issue is that if untrusted content can be introduced into a dynamic page, neither the Web sites nor the clients had enough information to recognize that this has happened and take protective actions.

1.2 Statement of the Problem

The main problem that the study has sought to answer is on how to develop an approach of prevention of XSS vulnerabilities that that will be integrated through an extension in Mozilla Firefox to address the problem directly in the browser.

The following are the sub problems of this study:

- What are the different XSS attacks?
- What are the existing approaches in preventing XSS attacks?

- What techniques should be used to develop a prevention mechanism for XSS attack?
- How are the contents of a target web page obtained?
- How is the developed approach integrated into Mozilla Firefox as an extension?

1.3 Objectives of the Study

The study aimed to answer the stated following problems above, as to develop an approach on prevention of XSS attack through an extension in a Mozilla Firefox browser and to provide XSS awareness to the user.

The following are the specific objectives:

- Know the different XSS attacks.
- Study how a XSS attack works in a dynamic page.
- Gather information and study the different techniques to detect XSS attacks and study the existing prevention approaches.
- Compare and contrast the existing detection and prevention techniques.
- Be able to get a reference to the content of the target web page.
- Explain how the developed approach of prevention of XSS works.
- Integrate the developed prevention mechanism into Mozilla Firefox plugin extension.

1.4 Significance of the Study

Websites nowadays tend to had dynamic content which makes the user enjoy more. As stated earlier, these dynamic contents can bring harm to the web page. Aside from the fact that a user can unknowingly execute malicious content while viewing dynamic pages, the attacker can take over the user session before it expires.

This study is significant to the people who use computers and visits dynamic web pages. A large number of individuals who visits dynamic web pages that is not educated on the possibilities of page vulnerabilities. Increasing the awareness of the people will be able to lessen the problem encountered while enjoying the web services. The extension that the proponents made will more likely prevent the risks that the executed malicious scripts may have. With this technology, the user will gain awareness before the attack is executed.

1.5 Scope and Limitations of the Study

The study focused on developing an approach to address the problem on XSS attack directly to the browser and not creating a standalone tool.

The scope of the study is to establish detection of XSS attacks and provide prevention mechanism before the attack is executed. This study will be through integrating the said approach into a plug-in extension for Mozilla Firefox.

The prototype is limited to evaluating one page at a time, so it cannot create session while there is a previous instance. The processing time of the page varies per page.

This study is limited to a Firefox browser with version 1.5 to 3.6.* family.

1.6 Definition of Terms

- XSS – is generally believed to be one of the most common application layer hacking techniques.
- XSS Vulnerability - is one of the most highly widespread flaws on the Internet and will occur anywhere a web application uses input from a user in the output it generates without validating it.
- Detection - the extraction of particular information from a larger stream of information without specific cooperation from or synchronization with the sender.
- JavaScript - the Netscape-developed object scripting language used in millions of web pages and server applications worldwide.
- Stored XSS Attack – an attack that embeds the malicious script permanently into the web application and therefore is executed every time any user visits the web page
- Reflective XSS Attack - this attack is carried out by using the GET parameter. The malicious user constructs a URL that embeds evil script as the value of the GET variable
- URL (Uniform Resource Locator) – the 'address' of a certain web page.
- web page - resource of information that is appropriate for the World Wide Web and can be accessed through a web browser.
- Web Server - a program (software) helps serve web pages to the web browsers and runs the HTTP.
- HTTP (Hypertext Transfer Protocol) - a request-response protocol standard for client-server computing which has web browser as a client and website as a server.
- GET – requests a representation of the specified resource.

- POST - submits data to be processed (e.g., from an HTML form) to the identified resource. The data is included in the body of the request. This may result in the creation of a new resource or the updates of existing resources or both.