Security of Web Applications and Browsers: Challenges and Solutions

A Tutorial Proposal for ACM SAC 2015 By

Dr. Hossain Shahriar
Department of Computer Science
Kennesaw State University
Kennesaw, GA 30144, USA
Email: hshahria@kennesaw.edu
1. Title: Security of Web Applications and Browsers: Challenges and Solutions

2. Duration: Half day, 3 hours

3. Abstract
We rely on web applications to perform many useful activities. Despite the awareness have raised since the past decade on vulnerabilities commonly discovered in the implementation of web applications, we still observe the presence of known vulnerabilities today. Worse that the browser platforms are posing extra challenges through extended functionalities or light weight extension applications that can not only access data from visited webpages and local machines, but also transfer them to remote hosts controlled by hackers. Given that a solid understanding of both application and browser platform security is essential to tame the unsecured web.

In this tutorial we will provide an overview of some common vulnerabilities for web applications and browsers, followed by some common techniques useful to combat against security threats. In particular, we will discuss some well-known implementation level vulnerabilities (e.g., SQL Injection, Cross-Site Scripting, Clickjacking) along with a popular mitigation approach known as security testing. We then focus our discussion on the browser platform and explore some of its supported features for extension applications with their capabilities. We will highlight vulnerabilities arise from extensions followed by exploring malware extensions. Finally, we discuss some practices to securely implementing browser extensions and combat against malware extensions.

4. Motivation, target audience, and interest for the SAC community
Most of discovered security breaches reported in various surveys (e.g., OWASP) have been shown to be related to implementation level weakness and some of the supported features of the underlying browser. The consequence of vulnerabilities could result in unwanted consequences such as bypassing of legitimate login procedure, hijacking of session information, deletion or alteration of sensitive data, execution of arbitrary code supplied by hackers, and passing of sensitive information to unwanted third parties. Given that this tutorial is intended to raise awareness and guide practitioners to prevent the consequences.

The tutorial is intended for application designers and developers, security testers, security researchers, scientists, and graduate students. As the tutorial is addressing one of the most emerging and crucial issues in security and quality assurance, it demonstrates an extremely high degree of relevance and addresses a broad spectrum of potential attendees of ACM SAC 2015. The tutorial will benefit related stakeholders to understand the most common program security vulnerabilities. Moreover, it will allow relevant professionals to apply appropriate vulnerability mitigation techniques.

5. Outline of the tutorial
The tutorial consists of three major parts. In the first part, we briefly discuss some of the most common vulnerabilities that are widely discovered in programs. We provide an idea on how the exploitations of four commonly discovered web security vulnerabilities (SQL injection, Cross-site scripting, Cross-site request forgery, clickjacking) can lead to many unwanted behaviors such as login bypassing.
In the second part, we introduce the vulnerability detection process based on testing approach. We explore both black box and white box approaches. In particular, our discussion will focus on some key aspects to conduct the testing process such as test case generation method, source of test case, test case granularity, and vulnerability coverage. We discuss some of test case generation techniques in details followed by open issues.

In the third part, we discuss the browser structure, particularly focusing on Mozilla, an open source browser widely used today. We provide an introduction of browser extension concept, outlining structure, with supporting application examples. We discuss vulnerabilities that may arise in extensions and show how they can be exploited. We then discuss malware extensions that can perform unwanted activities without the knowledge of the uses. Finally, we discuss some common programming practices that can be applied to prevent vulnerabilities in extensions as well as approaches to detect and prevent malware extensions.

For each of the part, we provide estimated duration, subtopics as below in structure of contents followed by a list of the most relevant literatures.

Structure of Contents

- **Introduction (10 min)**
  - Motivation and background

- **Web application vulnerabilities (Part 1: 45 min)**
  - SQL Injection
  - Cross-Site Scripting
  - Cross-Site Request Forgery
  - Clickjacking

- **Security testing (Part 2: 40 min)**
  - Taxonomy of web security testing
  - Test case generation technique
  - Static analysis based security testing

- **Browser Vulnerabilities (Part 3: 45 min)**
  - Browser security model and extension
  - Vulnerable and malware extension
  - Prevention and solutions

- **Summary (10 min)**

References


6. **Specific goals and learning objectives**

After completing the tutorial, the participants are expected to do the followings:

- Explain the cause of web application security vulnerabilities and demonstrate the consequence of vulnerabilities with attack payloads, and generate new attack payloads
- Explain various features of browsers and extension, and develop small extensions having vulnerabilities, followed by exploiting them with suitable test cases
- Follow some secure programming principles to prevent vulnerabilities
- Choose appropriate defense techniques to detect vulnerabilities in applications and malware extensions
- Follow the best practices for deploying web applications and configuring browsers

7. **Expected background of the audience**

Participants are expected to have some familiarity with languages for web application development including HTML, JavaScript, PHP, JSP, and XML.

8. **Presenter bios**

Dr. Hossain Shahriar is currently an Assistant Professor of Computer Science at Kennesaw State University, Georgia, USA. His research interests include software security, web application security, software testing, mobile application security, and malware analysis. Dr. Shahriar is an expert on application security testing with extensive publications and industry experience. His research has attracted a number of awards including *IEEE DASC 2011 Best Paper Award*, *Outstanding PhD Research Achievement Award 2011*, and *IEEE Kingston Section Research Excellence Award 2008*. Dr. Shahriar presented tutorials in ACM SAC 2011 and IEEE ISSRE 2012, and has been invited to present a tutorial on web application security issues in ACM/SIGSAC SIN 2013. He has served as PC member in various international conferences related to computer and software security such as ACM SAC 2014 (Computer Security Track),
ACM/SIGSAC SIN 2014, and IEEE ITNG 2014. He is also serving as an associate editor of the International Journal of Secure Software Engineering. Dr. Shahriar is currently a member of the ACM, ACM SIGAPP, and IEEE.

9. Audio Visual equipment needed for the presentation

Projector for power point slide show would be sufficient.

10. Teaching materials on the topic by the presenter

a. Tutorial in International Conference

3. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In IEEE ISSRE 2012, Dallas, TX, USA.

b) Invited talk/Guest speaker seminar

1. Web Application Security Vulnerability: Mitigation Approaches and Challenges, CIISE, Concordia University, Quebec, Canada, February 2013.
3. Web Security, School of Computing (Guest Lecture Seminar), Queen’s University, Canada, November 2010.

c) Academic courses

1. Computing Security (CS6040), Kennesaw State University, GA, USA.
2. Theory of Networking & Security (CS3550), Kennesaw State University, GA, USA.
3. Secure Software Development (CS4550), Kennesaw State University, GA, USA.