Web Security Vulnerabilities: Challenges and Solutions

A Tutorial Proposal for ACM SAC 2018

by

Dr. Hossain Shahriar
Department of Information Technology
Kennesaw State University
Kennesaw, GA 30144, USA
Email: hshahria@kennesaw.edu

1. Title: Web Security Vulnerabilities: Challenges and Solutions

2. Duration: Half day, 3 hours

3. Abstract

We rely on web applications to perform many useful activities. Despite the awareness over the past decade on secure programming practices and tools on vulnerability discovery in the implementation, we still observe the presence of known vulnerabilities. Both the client sides and server sides are responsible to let attackers exploiting vulnerabilities with malicious inputs. Web services are used as integral part of web applications and they remain vulnerable when not implemented securely. Given that an understanding of the common vulnerabilities for applications and services are essential for practitioners to tame the unsecured web.

In this tutorial, we will provide an overview of common vulnerabilities for web applications and web services, followed by common techniques useful to combat against security threats. In particular, we will discuss implementation level vulnerabilities for applications (e.g., code injection, object injection, clickjacking) along with a popular mitigation approach known as security testing. We also focus on web service security vulnerabilities and exploitation techniques followed by best practices.

4. Motivation, target audience, and interest for the SAC community

Most of reported security breaches reported (*e.g.*, OWASP) have shown to be related to implementation level vulnerabilities. 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 *software designers and developers*, *security testers*, *academic 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 2018. 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, Object Injection, Clickjacking, Denial of Service) can lead to many unwanted behaviors such as login bypassing.

In the second part, we introduce the vulnerability mitigation process based on security testing, static analysis, and intrusion detection system. 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*, and *vulnerability coverage*. We discuss some of test case generation techniques in details followed by open issues.

In the third part, we discuss the common vulnerabilities for web services with a taxonomy followed by example of mitigation approaches from the literature and available tools.

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
- **Application vulnerabilities (Part 1: 40 min)**
  - SQL Injection
  - Cross-Site Scripting
  - Object Injection
  - Clickjacking
  - Denial of Service
- **Mitigation approaches (Part 2: 40 min)**
  - Taxonomy of security testing
  - Static analysis based security testing
  - Intrusion Detection System
- **Service Vulnerabilities and Mitigation (Part 3: 30 min)**
  - Taxonomy of web service vulnerabilities
  - Prevention and solution
- **Summary (10 min)**

References

1. R Bronte, H Shahriar, HM Haddad, "Mitigating distributed denial of service attacks at the application layer," *Proceedings of the 32nd Symposium on Applied Computing (SAC)*, April 2017, Marrakech, Morocco, pp. 693-696.
2. R Bronte, H Shahriar, HM Haddad, "A signature-based intrusion detection system for web applications based on genetic algorithm," *Proceedings of the 9th International Conference on Security of Information and Networks (SIN)*, July 2016, Newark, NJ, USA, pp. 32-39.
3. R Bronte, H Shahriar, H Haddad, "Information Theoretic Anomaly Detection Framework for Web Application," *Proceedings of the 40th IEEE Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, USA, June 2016, pp. 394-399.
4. H Shahriar, HM Haddad, P Bulusu, "OCL Fault Injection-Based Detection of LDAP Query Injection Vulnerabilities," *Proceedings of the 40th IEEE Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, USA, June 2016, pp. 455-460.
5. H Shahriar, HM Haddad, "Object injection vulnerability discovery based on latent semantic indexing," *Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC)*, Pisa, Italy, April 2016, pp. 801-807.

6. H Shahriar, HM Haddad, VK Devendran, "Request and Response Analysis Framework for Mitigating Clickjacking Attacks," *International Journal of Secure Software Engineering (IJSSE)*, Vol. 6, Issue 3, 2015, pp. 1-25.
7. H Shahriar, HM Haddad, "Security assessment of clickjacking risks in web applications: metrics based approach," *Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC)*, Geyonju, South Korea, March 2014, pp. 791-797.

6. Specific goals and learning objectives

After completing the tutorial, the participants will be able to

- Identify the cause of web application and web service security vulnerabilities and demonstrate the consequence of vulnerabilities with attack payloads
- Describe various security testing approaches including static analysis, test case generation with genetic algorithms, intrusion detection-based defense
- Apply some secure programming principles to prevent vulnerabilities

7. Expected background of the audience

Participants are expected to have some familiarity with web application development using PHP/JSP. Knowledge of SQL, JavaScript, and XML will be helpful.

8. Presenter bios

Dr. Hossain Shahriar is an Assistant Professor of Information Technology at Kennesaw State University, Georgia, USA since Fall 2012. He received his PhD in Computing from Queen's University, Canada in 2012. His research interests include cyber security, particularly application (web, mobile) security vulnerabilities and mitigation approaches, risk assessment techniques, and metric-based attack detection. He also teaches cyber security courses such as Ethical Hacking. Dr. Shahriar has published more than 70 peer reviewed research articles on various topics within cyber security in International Journals, Conferences, and Book Chapters including ACM SAC, ACM SIN, IEEE HASE, IEEE COMPSAC, Computer & Security, and ACM Computing Survey. He has been a reviewer for many international journals and PC member of international conferences on software, computer, and application security. He served as Fast Abstract Chair in IEEE COMPSAC 2015-2017, Program Chair in ACM SIN 2016, Publicity Chair in IEEE COMPSAC 2017, Publication Chair in ACM SAC 2017 and 2018, and Student Research Competition Chair in ACM SAC 2016. Currently, he is also a Co-PI of a funded research project from National Science Foundation on Secure Mobile Application Development aiming to develop open source labware resources. Dr. Shahriar is a professional member of 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

1. Secure and Reliable Mobile Applications: Challenges and Approaches, In ACM SAC 2016, Pisa, Italy.
2. Security of Web Applications and Browsers: Challenges and Solutions, In ACM SAC 2015, Salamanca, Spain.
3. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2014, Gyeongju, South Korea.
4. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In IEEE ISSRE 2012, Dallas, TX, USA.
5. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2011, Taichung, Taiwan.

b) Academic courses

1. Ethical Hacking and Networking Defense (IT4843), Kennesaw State University, USA.
2. Information Security Administration (IT6823), Kennesaw State University, USA.
3. Health Information Security and Privacy (IT6533), Kennesaw State University, GA, USA.
4. Computing Security (CS6040), Kennesaw State University, GA, USA.
5. Theory of Networking & Security (CS3550), Kennesaw State University, GA, USA.
6. Secure Software Development (CS4550), Kennesaw State University, GA, USA.