Week 3

Help

Web Security

Now we will move away from low-level security and turn our attention to security on the worldwide web (WWW).

The web utilizes a variety of technologies, from HTTP (hypertext transfer protocol) and HTML (hypertext markup language) to SQL (standard query language) and the Javascript programming language. Unfortunately, these technologies can be used in ways that constitute significant vulnerabilities. We will examine several important kinds of vulnerabilities, see how they can be exploited, and explore how to defend against them.

Learning Objectives

After the completion of this week's material, you will be able to:

- Understand how **SQL injection** attacks affect web application back ends
- Understand how the web implements *session state*, using *cookies* and *hidden form fields*, and how improper implementations are subject to **Session hijacking** and **Cross-site Request Forgery (CSRF)** attacks
- Understand how popular, browser-executed *Javascript* programs can be used incorrectly by web sites, leading to **Cross-site Scripting (XSS)** vulnerabilities
- Avoid flaws and bugs that introduce these vulnerabilities, with a focus on employing **input validation** and **sanitization**

Video Lectures

- Security for the Web: Introduction (3:33)
- Web Basics (10:31)
- SQL Injection (10:35)
- SQL Injection Countermeasures (9:17)
- Web-based State Using Hidden Fields and Cookies (13:51)
- Session Hijacking (6:56)
- Cross-site Request Forgery (CSRF) (6:36)
- Web 2.0 (5:16)
- Cross-site Scripting (13:39)

Readings

No readings are required for this week, but you may find the following references helpful

- OWASP's guide to SQL injection - This is a good overview. You might find the linked page on Testing for SQL injection) to be useful for the project.
- SQL injection cheat sheet - This is a good reference for doing SQL injection
- OWASP's guide to cross-site scripting (XSS)) - Pay particular attention to the testing guide, for finding XSS vulnerabilities.
- OWASP's guide to session hijacking - Note that they give an example of stealing a session cookie via XSS, which is in play for the project.
- OWASP's guide to cross-site request forgery (CSRF))
- CWE/SANS top 25 most dangerous software errors - A little dated, but still relevant; here's the brief listing.

Quiz

The quiz for this week covers all of the material for this week. You must submit the quiz no later than the start of week 5. You will have three attempts to complete the quiz, at two hours per attempt. It consists of 16 questions, and if you are well versed in the

material it should take about 30 minutes (but longer if you have to go back and look things up, obviously).

Project

The second project tests your ability to exploit vulnerabilities in a web application called **BadStore**. It is due in three weeks, at the start of week 6. You will complete the work for the project on your own computer, and then take the on-line assessment to show that you've done so.

Created Wed 9 Apr 2014 6:16 AM PDT

Last Modified Sun 16 Nov 2014 6:56 PM PST