Course Abstract

Title: Web Application Hacking with Burp Suite

Workshop length: 2 parts – each 1 day; split to be stand alone
Day 1 – Beginner and foundational materials
Day 2 – More advanced topics and techniques

This course can be expanded beyond 2 days if desired. In particular, an additional day+ of advanced training on Burp Suite features is under development, contact us for details.

Hands-on Web App Hacking with Burp Suite – Day 1

Who should attend: People who are auditing web application security, developing web applications, or managing the development of web applications. Some essentials of HTTP will be covered in the course to assist those with limited prior experience.

Hands-on Exercises: The workshop will cover a single day and include live demos by the instructor as well as lab exercises to be performed by the students.

Each student will be given a virtual machine containing tools, documentation, and web application targets for a fully self-containing web app security testing environment. Training will take place in the open-source "Web Application Security Dojo" (https://dojo.mavensecurity.com) centered around the commercial tool Burp. A two week license for Burp Suite Pro will be provided to students, which can be used outside of class..

Students are expected to bring a laptop computer so that they can run the virtual machine image supplied by the instructor. Student system requirements are simple:

- Any operating system that can run the latest stable version of VirtualBox (free from https://www.virtualbox.org/). Currently supported operating systems include Windows, Mac, and Linux.
- 5 GB of free HD storage
- 2 GB of RAM
- USB port or DVD drive
- Wi-Fi networking capability

*** **Before the first day of class students must install** the latest stable version of VirtualBox. Also install the latest version of "Oracle VM VirtualBox Extension Pack". Both are free and found here: https://www.virtualbox.org/wiki/Downloads.

Course Abstract

The proliferation of web-based applications has increased the enterprise's exposure to a variety of threats. There are steps that can and should be taken at various steps in the application's lifecycle to prevent or mitigate these threats, such as implementing secure design and coding practices, performing source code audits, and maintaining proper audit trails to detect unauthorized use.

+1-877-MAVEN-HQ (1-877-628-3647) phone ❖ www.MavenSecurity.com

Course Abstract

Title: Web Application Hacking with Burp Suite

This workshop, through hands-on demos and labs, will introduce the student to the techniques needed to remotely detect and validate the presence of common vulnerabilities in web-based applications using Burp Suite, the industries' most popular toolkit. Testing will be conducted from the perspective of the end user (as opposed to a source code audit). Security testing helps to fulfill industry best practices and validate implementation. Remote security testing is especially useful since it can be done at various phases within the application's lifecycle (e.g. during development), or when source code is not available for review.

Due to time constraints of only one day, this workshop will focus on the most popular and critical threats (based on the industry standard OWASP "Top Ten" – see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). For example, cross-site scripting (XSS) and SQL injection. The foundation learned in this class will enable the student to go beyond the top ten via self-directed learning using other industry resources, such as the OWASP Testing Guide (https://www.owasp.org/index.php/OWASP_Testing_Project) or Web Application Hacker's Handbook.

Course Objectives:

- Understand the most popular security threats facing web applications.
- Introduction and hands-on use of the tools and techniques to remotely validate a web application's security.
- Enhance secure programming practices by raising awareness and giving developers and auditors the tools & knowledge needed to test their web application's security from the user's perspective.

Course Topics:

Day 1:
Web Primer (HTML, HTTP, Cookies, the basics)
Introduction to Burp Suite
Threat Classification Systems (OWASP Top Ten & WASC Threat Classes)
Vulnerability Category: A1: Injection (SQL, XML entity, etc)
Vulnerability Category: A3: Cross-Site Scripting (XSS)
Vulnerability Category: A2: Broken Authentication and Session Management
Vulnerability Category: A5: Security Misconfiguration
Vulnerability Category: A9: Using Components with Known Vulnerabilities
Overall Testing Advice & Strategies – Real-world advice from the trenches

+1-877-MAVEN-HQ (1-877-628-3647) phone ❖ www.MavenSecurity.com

Hands-on Web App Hacking with Burp Suite – Day 2

Who should attend: People who are auditing web application security, developing web applications, or managing the development of web applications. Prior hands-on experience with HTTP and man-in-the-middle fuzzing techniques is required. If in doubt, attend Part 1.

Hands-on Exercises: The workshop will cover a single day and include live demos by the instructor as well as lab exercises to be performed by the students.

Each student will be given a virtual machine containing tools, documentation, and web application targets for a fully self-containing web app security testing environment. Training will take place in the open-source "Web Application Security Dojo" (https://dojo.mavensecurity.com) centered around the commercial tool Burp. A two week license for Burp Suite Pro will be provided to students, which can be used outside of class.

Students are expected to bring a laptop computer so that they can run the virtual machine image supplied by the instructor. Student system requirements are simple:

- Any operating system that can run the latest stable version of VirtualBox (free from https://www.virtualbox.org/). Currently supported operating systems include Windows, Mac, and Linux.
- 5 GB of free HD storage
- 2 GB of RAM
- USB port or DVD drive
- Wi-Fi networking capability

*** **Before the first day of class students must install** the latest stable version of VirtualBox. Also install the latest version of "Oracle VM VirtualBox Extension Pack". Both are free and found here: https://www.virtualbox.org/wiki/Downloads.

Course Abstract

The proliferation of web-based applications has increased the enterprise's exposure to a variety of threats. There are steps that can and should be taken at various steps in the application's lifecycle to prevent or mitigate these threats, such as implementing secure design and coding practices, performing source code audits, and maintaining proper audit trails to detect unauthorized use.

This workshop, through hands-on demos and labs, will introduce the student to the techniques needed to remotely detect and validate the presence of common vulnerabilities in web-based applications using Burp Suite, the industries' most popular toolkit. Testing will be conducted from the perspective of the end user (as opposed to a source code audit). Security testing helps to fulfill industry best practices and validate implementation. Remote security testing is especially useful since it can be done at

various phases within the application's lifecycle (e.g. during development), or when source code is not available for review.

This workshop will focus on some more advanced or subtle security threats (based on the industry standard OWASP "Top Ten" – see http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). For example, cross-site request forgery (CSRF). The foundation learned in this class will enable the student to go beyond the top ten via self-directed learning using other industry resources, such as the OWASP Testing Guide (https://www.owasp.org/index.php/OWASP_Testing_Project) or Web Application Hacker's Handbook.

Course Objectives:

- Understand the popular security threats facing web applications.
- Gain proficiency with the tools and techniques needed to remotely validate a web application's security via hands-on use.
- Enhance secure programming practices by raising awareness and giving developers and auditors the tools & knowledge needed to test their web application's security from the user's perspective.

Day 2:
Burp Suite Redux
Vulnerability Category: A4: Insecure Direct Object References
Vulnerability Category: A8: Cross-Site Request Forgery (CSRF)
Vulnerability Category: A7: Missing Function Level Access Control
Vulnerability Category: A6: Sensitive Data Exposure
Vulnerability Category: A10: Unvalidated Redirects and Forwards
Leveraging Automated Tools – Speed, Safety, Accuracy, and Limitations
Burp automation: Session handling tools and extensions
Overall Testing Advice & Strategies – Real-world advice from the trenches