Ruxcon Training
October 20-21, 2016
Melbourne, Australia

PENTERSTERLAB'S ADVANCED WEB HACKING

OVERVIEW

Do you want to know more about all these serialization bugs? You think there is more too life than Burp scanner? You went through PentesterLab's exercises and thought "I WANT MORE!!"? This training is for you!

This 2-day training will get you to the next level. We will look into CORS, WebSockets, the exploitation of vulnerabilities published in 2015/2016. This includes bugs in Spring, Jenkins... We will also get shells using serialisation in multiple languages and find vulnerabilities that you may have missed in the past.

After a quick overview of what you need to know to attack web applications, we will directly jump to the interesting stuff: Hands-on training and real attacks. The class is a succession of 10 minute explanations on what you need to know, followed by hands-on examples to really understand and exploit vulnerabilities. After the training, you go home with the course (slides based), the detailed version of the course (in-depth walk-through), and the systems to be able to play and refresh your memory!

This training also includes one-year access to PentesterLab Pro (https://pentesterlab.com/pro).

SYLLABUS

Key Learning Objectives

- Cross-origin resource sharing
- Struts RCE
- Multiple Serialisation attacks (PHP, Python, Java)
- Jboss web-console
- JWT
- Padding Oracle
- Outbound XML entities attacks

Day 1:

- Review of HTTP essentials
- Attacking JSON Web Token
- Attack on Electronic CodeBook
- Directory traversal and Tomcat Manager
- Heartbleed
- Outbound XML entities
- Attacks on Cipher Block Chaining
- Serialisation in Python
- Serialisation in Java

Day 2:

- Padding Oracle
- Struts Dev Mode
- Play Session Injection
- Cross-Origin Resource Sharing attacks
- Signature bypass using Bad Hash
- Serialization attacks in PHP
- Attacking JBoss console
- XSS and SQL injection to gain command execution
- Attacks against Gitlist

ABOUT THE TRAINERS

Louis Nyffenegger is an experienced and sought-after security consultant specialising in web penetration testing. He is a regular guest speaker at local security conferences including Ruxcon and Owasp, and has conducted a web application security training at both conferences. In his spare time Louis helps set up Ruxcon's Capture the Flag competition. In 2011, Louis started PentesterLab, a company specialising in security training. A free version of some of the PentesterLab exercises are available here. Recently, Louis published Bootcamp, a learning path for getting into penetration testing.

Luke Jahnke is the creator of Bitcoin CTF, one of the hardest CTF dedicated to web security. In 2014, he talked at Ruxcon on "Safe cracking on a budget".

RECOMMENDATIONS

This training is aimed at penetration testers and security professionals who want to improve their Web mojo.

The following skills/knowledge are required:

- Exposure to information security technologies
- The ability to use a web proxy like Burp Suite, Paros
- The ability to write basic scripts in Ruby, Python or Perl
- Blind XML entities attacks
- Heartbleed
- Tricky SQL injections.

Trainers	Louis Nyffenegger & Luke Jahnke
Dates	October 20-21, 2016
Level	Advanced (Web)

REGISTRATION FEES

Early Bird	$2,200	Ends July 31, 2016
Regular	$2,530	Ends August 31, 2016
Late	$2,860	Starts September 1, 2016

Prices include GST

For more information or to register click here
REGISTRATION WILL CLOSE ON OCTOBER 14, 2016