Advanced Burp Pro 100% hands-on

Insomni'Hack 2014
Nicolas Grégoire (@Agarri_FR)

The training

Nicolas presented last year at HackInParis and OWASP AppSec about advanced usage of Burp Suite, based on his 8 years of experience. This "Burp Pro real-life tips and tricks" talk was very well received. All modesty aside, the author of Burp himself published on Twitter "Serioulsy cool presentation - excellent work!". This talk was a compilation based on a 3-days hands-on Burp training proposed by Nicolas to his customers.

A compact 1-day version is now proposed at Insomni'Hack 2014!

Why should you attend?

Mastering Burp Suite allows a penetration tester to get the most of a tool where he usually spend countless hours. His work is then faster, less error-prone and more reproducible. Last but not least, more time and brain power are available to the tester, who can focus on identifying and exploiting complex and creative vulnerabilities. Possible targets are classical web applications (of course) but also thick clients, mobile applications, internal networks or complex cloud deployments.

Proposed plan

Introducing Burp (GUI, tools, audit workflow)
Using a personalized configuration
Advanced usage of Intruder, Repeater, Proxy and Sequencer, ...
Tons of tips and tricks (cf. my HackInParis'13 talk for an excerpt)
Extensions: useful on-the-shelf ones, basic templates for common needs, coding your own
And much more!

The training is based on dozens of micro-challenges replicating real-life scenarios: complex brute-force, data extraction, thick clients, ACL, cryptography, home-made encoding, CSRF tokens, sessions and macros, …

Note: this plan may be modified depending on the audience skills/expectations or the trainer's mood.

Prerequisites

Laptop with an Ethernet/RJ45 connector
OS Linux (including Kali) or Windows or Mac
Recent JVM (preferably from Oracle)
Burp Pro license (if needed, a temporary one can be provided on prior request)
Basic knowledge of Burp Suite (UI navigation, traffic interception and replay)
Text editor + browser

The trainer

Nicolas Gregoire has more than 13 years of experience in penetration testing and auditing of networks and (mostly Web) applications. He founded Agarri, a small company where he finds security bugs for customers and for fun. His research was presented at numerous conferences around the world (Hack in the Box, HackInParis, ZeroNights, ...) and he was publicly thanked by some well known vendors (Microsoft, Adobe, Mozilla, Google, Apple, VMware, ...) for responsibly disclosing vulnerabilities in their products. He also participates in bug bounties and won (twice) the highest Prezi reward ever offered.