espion

intelligence

Practical Penetration Testing with Burp Suite

Presenter: Máirtín O'Sullivan, Consultancy Team Lead, Espion

espion
intelligence

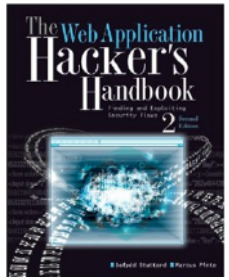
Agenda

- Burp Introduction
- Burp Free vs. Burp Pro
- Practical Demo
- Q & A

Credit: Bill Watterson, "Calvin & Hobbes"

Background

- Created in 2003 by Dafydd Stuttard
- One of the authors for the Web Application Hackers Handbook



- Started as a proxy… but evolved into a full web application penetration testing suite
- Constantly improving

- Two versions available – free and pro

Key Functionality

- Proxy
- Spider
- Intruder
- Repeater
- Scanner (Pro Only)

Burp Free vs. Burp Pro

- Pro version costs €210 for an annual, one user license

- Key features only in Pro
  - Save and restore session state
  - Scanner (Automated web application scanner)
  - Engagement Tools (Search request/responses,)

- Automated scanning capabilities improving with each release

Key Benefits For Inexperienced Pen Testers

- Easy to use
- Provides repeatability in testing
- Quick to run
- Scanner catches a lot (but not all!) of basic vulnerabilities
- Provides a basic level of assurance for very little money

Key Benefits For Experienced Pen Testers

- Designed around helping pen testers, rather than taking control away from them
- Reduced need for additional tools (Encoders, etc)
- Scanner can help with performing time consuming and repetitive tasks
- Allows testers to focus on the more complicated vulnerabilities
- Fuzzing parameters can be extended (FuzzDB)
- Can be extended using custom code

espion
intelligence

Demo

Questions?

Máirtín O'Sullivan

mairtin.osullivan@espiongroup.com