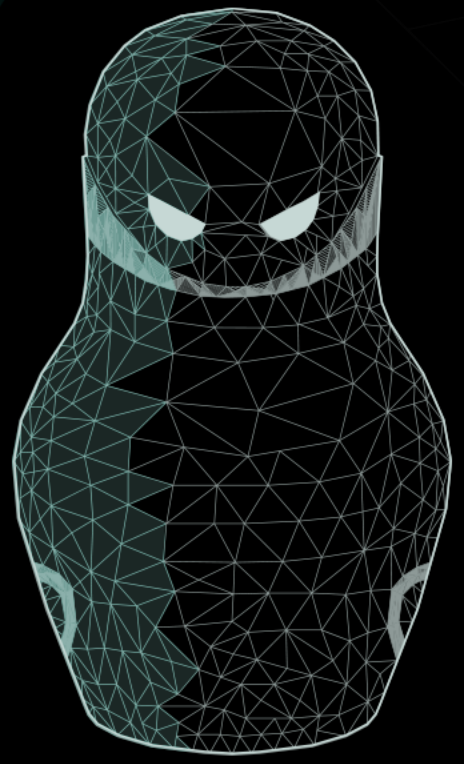


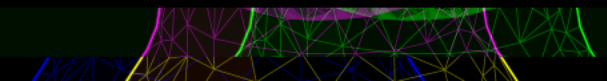
ZERO NIGHTS 2015

Enlarge your burp
or how not to be afraid of JavaDocs

Igor Bulatenko
Ivan Elkin

Sources

https://goo.gl/oYjBTg (python)



#whoami

- #videns
- Head of QIWI application security department
- Former security software developer
- CTF player and organizer (TechnoPandas)
- JBFC Member ☺

What is all about

- Why people (us) use burp
- Burp 101
  - Official info
  - Other presentations
- Internals
- Plugins

Is it good?

- #1 among web scanners *
- Crossplatform
- Good for manual vulnerabilities testing
- Can scan whole internet
- Has plugins
- Most popular vulnerability checks
- Gartner challengers for AST

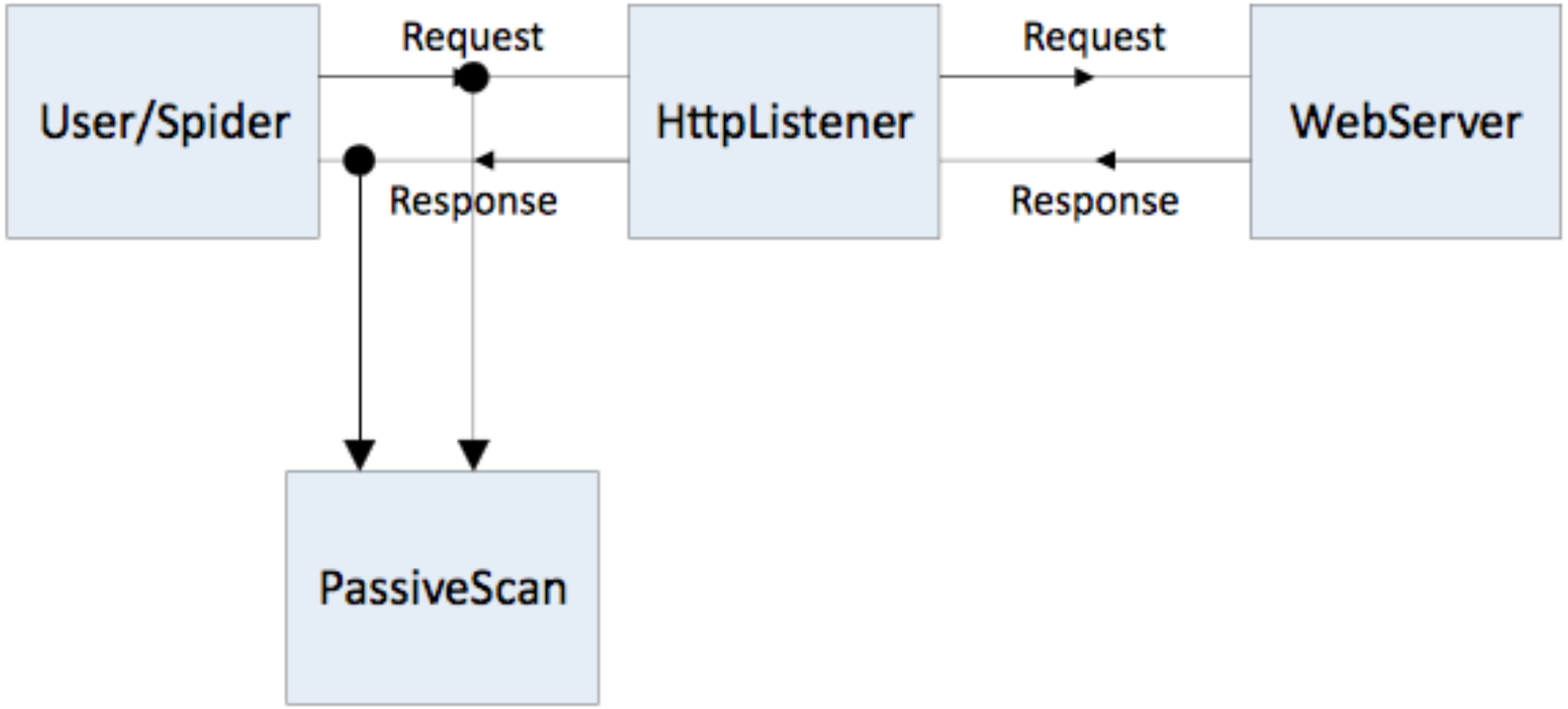
Unofficial infos

http://www.slideshare.net/jasonhaddix/bsides-final
http://www.slideshare.net/AugustDetlefsen/burp-extensions
http://www.slideshare.net/marcwickenden/burp-plugin-development-for-java-n00bs-44-con
http://www.agarri.fr/docs/HiP2k13-Burp_Pro_Tips_and_Tricks.pdf
http://www.youtube.com/watch?v=Q2WK5LpDbxw
http://www.youtube.com/watch?v=N-IKHmGjf2c
https://twitter.com/everythingburp
http://www.slideshare.net/AugustDetlefsen/appsec-usa-2015-customizing-burp-suite

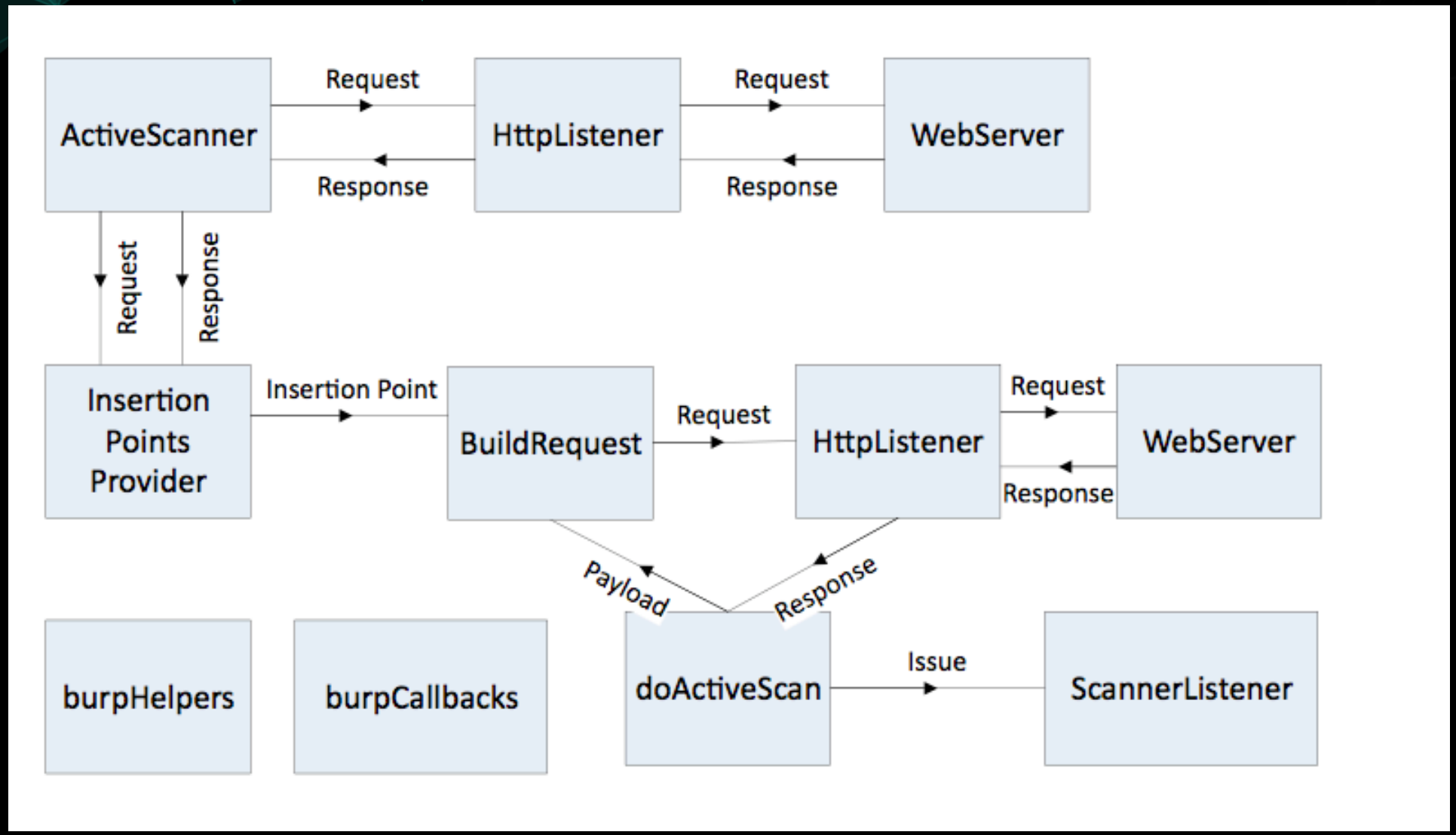
Why improve it?

- Not correct use of API
- Scan fullness
- Time for implementing new techniques

How it works (spidering)



How its works (active scan)



Demo 01

- Simplest Plugin
  - Show logging functionality (stdout, stderr)
  - Log InsertionPoints info
- Nested InsertionPoint
- DoActiveScan
- How to debug in python (jython)

Demo 02

- DoActiveScan
  - Building request for attack
  - How requests are counted (scanner tab)
  - Send requests via callbacks or via jython
- Highlighting in request/responses

Demo 03

- Error message check (http://virvales.blogspot.ru/2015/08/burp-stacktrace-sniffer.html)
- HttpListener
- Manual adding scan issue

You're doing it wrong

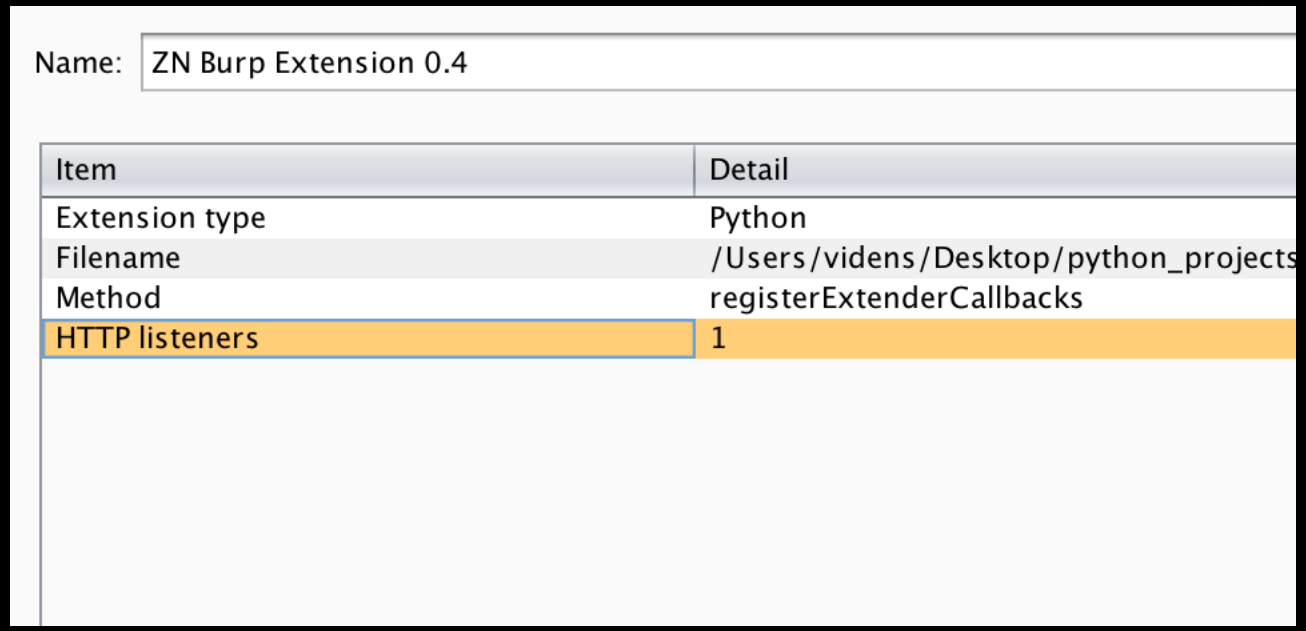
Item	Detail
Extension type	Java
Filename	bapps/4f01db4b668c4126a68e4673df79
Method	registerExtenderCallbacks
Scanner checks	1

Building a Passive Scanner

Passive Scanning – Room for Improvement

- Error Messages
- Software Version Numbers

Right way


Name: ZN Burp Extension 0.4
Item
Detail
Extension type
Python
Filename
/Users/videns/Desktop/python_projects
Method
registerExtenderCallbacks
HTTP listeners
1

Demo 04

Insertion Point Provider
Custom Insertion Point, necessary methods
Logging payloads

The end (part 1)