OWASP ZAP

open source intercepting proxy

27-June-2013
presenter: Adam Baso (@dr0ptp4kt)

Acronyms

OWASP: Open **W**eb **A**pplication **S**ecurity **P**roject

https://www.owasp.org

ZAP: Zed **A**ttack **P**roxy

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Download

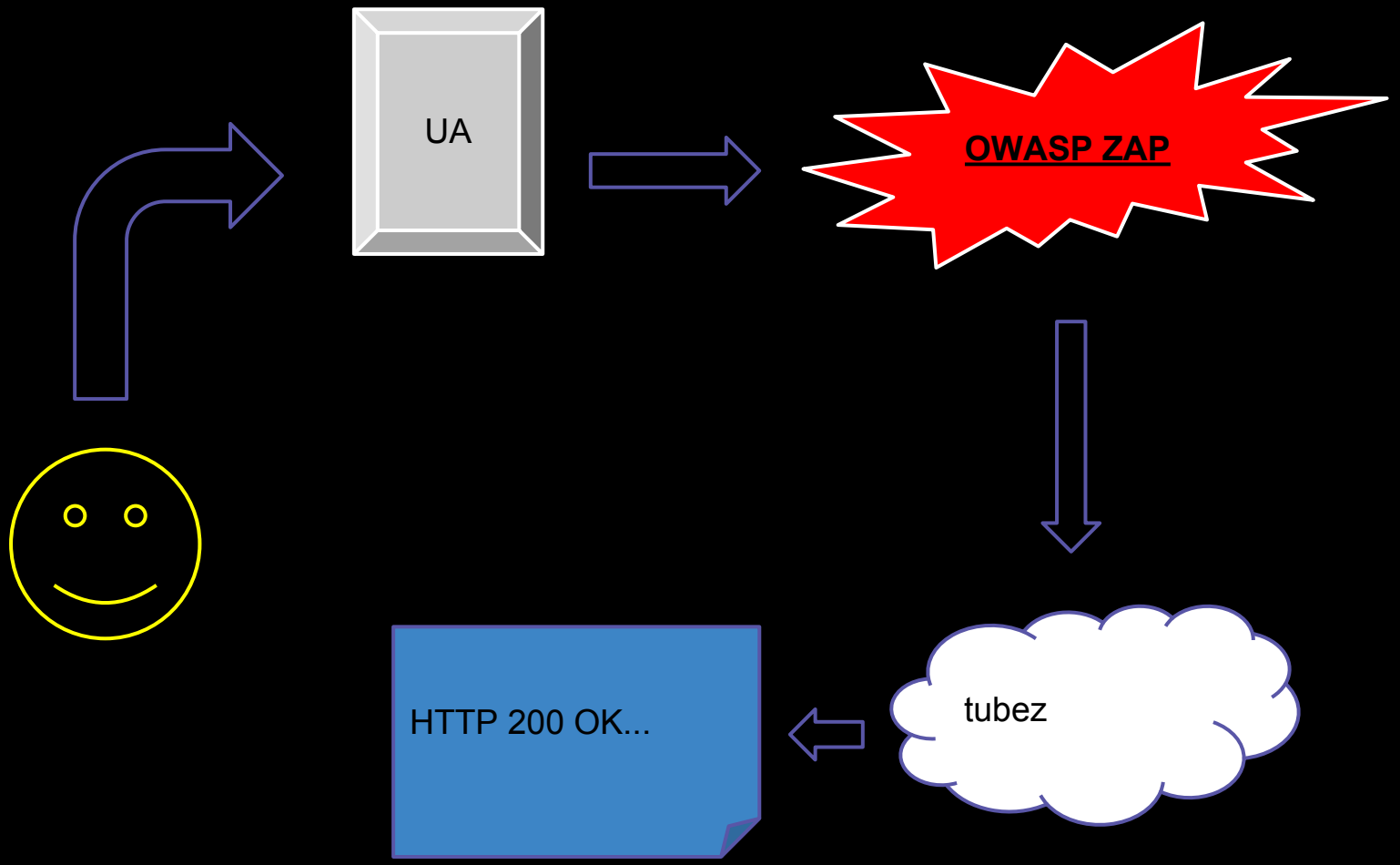
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Why?

Attackers have tools.

You should, too.

Intercepting proxy



Demo

Fingers crossed

Cucumber and Watir

```
$ vi features/support/env.rb
# look for browser_label and point stuff at ZAP

profile = Selenium::WebDriver::Firefox::Profile.new
profile.proxy = Selenium::WebDriver::Proxy.new :http => 'localhost:8085', :ssl => 'localhost:8085'
Watir::Browser.new browser_label, :profile => profile

# now run your browser test automation script
$ source ~/.rvm/scripts/rvm
$ gem update --system
# if necessary, $ gem install bundler
$ bundle install
$ bundle exec cucumber features/wikilove.feature
```

Be a good citizen

Shrink scan scope

Beware backend connections

Complementary Firefox tools

User Agent Switcher

Modify Headers

Web Developer Toolbar

Live HTTP Headers

FoxyProxy

THE END

OWASP ZAP
open source intercepting proxy

27-June-2013
presenter: Adam Baso (@dr0ptp4kt)