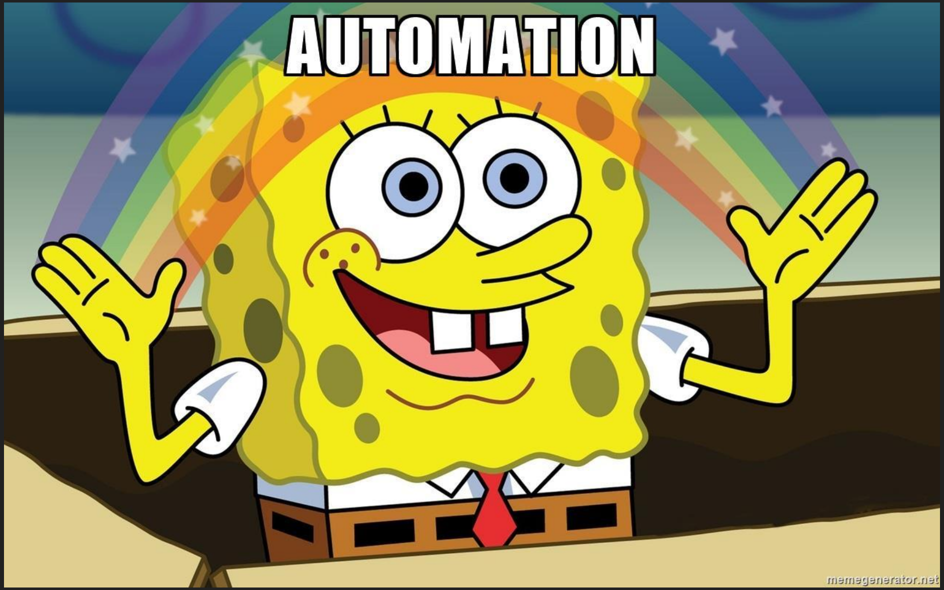
Automated Security Testing

OWASP Israel 2017 Chapter Meeting
3 April 2017

http://goo.gl/sphN9w

Demo: Building Security Testing from existing automation tests



http://goo.gl/sphN9w

Agenda

Approaches to Application Security Testing

Building Blocks

Live demo

Future plans

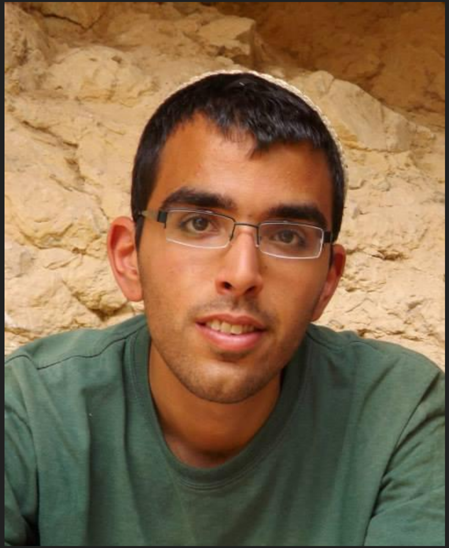
About me

Software Developer and Security Evangelist at Soluto

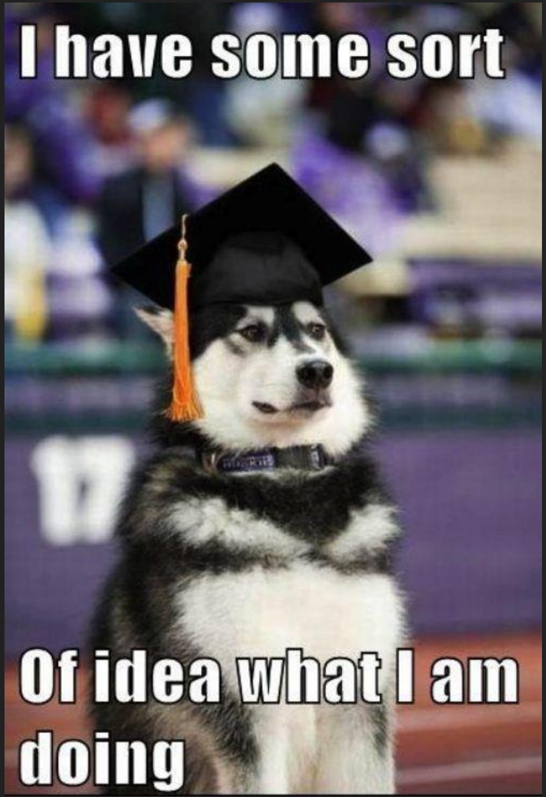
26yrs old

Writing code for the last 8 years

@omerlh: Github/Twitter



http://goo.gl/sphN9w



http://goo.gl/sphN9w

Approaches to Application Security Testing

Static: Code analysis - Checkmarx (our host :))

Dynamic: Live analysis

Integrated: Combination of Static and Dynamic

http://goo.gl/sphN9w

Building Blocks

http://goo.gl/sphN9w

ZAP - Zed Attack Proxy

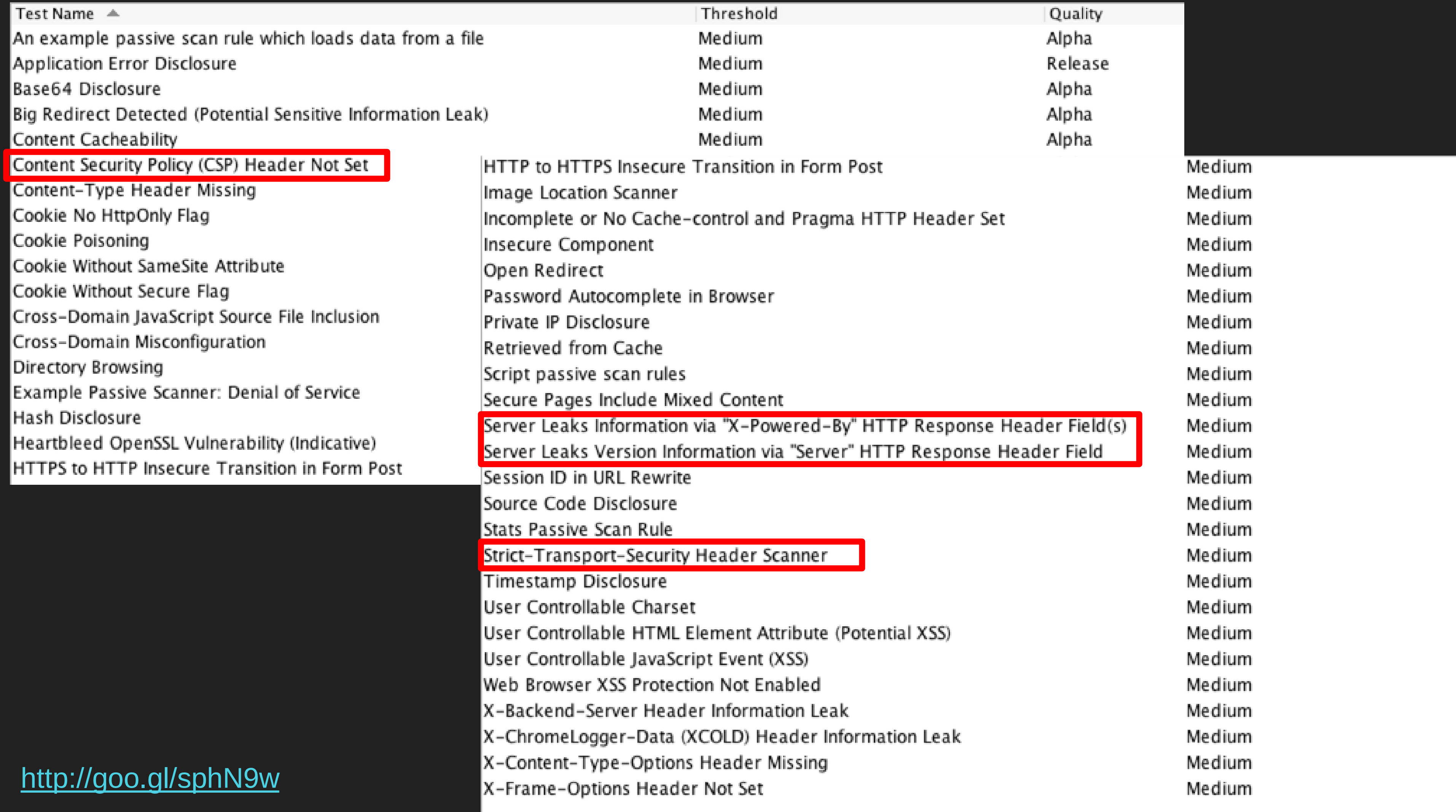
“The OWASP Zed Attack Proxy (ZAP) is one of the world’s most popular free security tools”

API/cli

Active Scan Mode (spider)

Passive Scan Mode

http://goo.gl/sphN9w



Test Name	Threshold	Quality
An example passive scan rule which loads data from a file	Medium	Alpha
Application Error Disclosure	Medium	Release
Base64 Disclosure	Medium	Alpha
Big Redirect Detected (Potential Sensitive Information Leak)	Medium	Alpha
Content Cacheability	Medium	Alpha
Content Security Policy (CSP) Header Not Set		
Content-Type Header Missing		
Cookie No HttpOnly Flag		
Cookie Poisoning		
Cookie Without SameSite Attribute		
Cookie Without Secure Flag		
Cross-Domain JavaScript Source File Inclusion		
Cross-Domain Misconfiguration		
Directory Browsing		
Example Passive Scanner: Denial of Service		
Hash Disclosure		
Heartbleed OpenSSL Vulnerability (Indicative)		
HTTPS to HTTP Insecure Transition in Form Post		

HTTP to HTTPS Insecure Transition in Form Post	Medium
Image Location Scanner	Medium
Incomplete or No Cache-control and Pragma HTTP Header Set	Medium
Insecure Component	Medium
Open Redirect	Medium
Password Autocomplete in Browser	Medium
Private IP Disclosure	Medium
Retrieved from Cache	Medium
Script passive scan rules	Medium
Secure Pages Include Mixed Content	Medium
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Medium
Server Leaks Version Information via "Server" HTTP Response Header Field	Medium
Session ID in URL Rewrite	Medium
Source Code Disclosure	Medium
Stats Passive Scan Rule	Medium
Strict-Transport-Security Header Scanner	Medium
Timestamp Disclosure	Medium
User Controllable Charset	Medium
User Controllable HTML Element Attribute (Potential XSS)	Medium
User Controllable JavaScript Event (XSS)	Medium
Web Browser XSS Protection Not Enabled	Medium
X-Backend-Server Header Information Leak	Medium
X-ChromeLogger-Data (XCOLD) Header Information Leak	Medium
X-Content-Type-Options Header Missing	Medium
X-Frame-Options Header Not Set	Medium

http://goo.gl/sphN9w

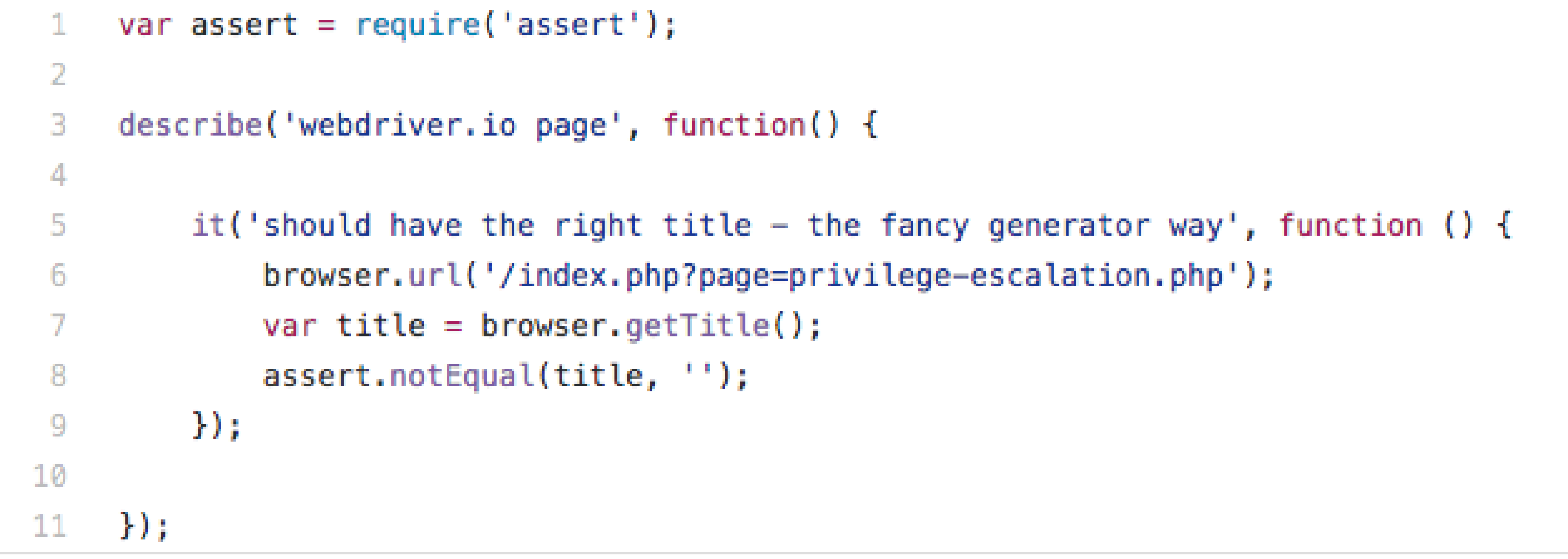
Webdriver.io

“WebdriverIO lets you control a browser or a mobile application with just a few lines of code.”

Simple Selenium binding for JS

Very popular framework for automation testing

http://goo.gl/sphN9w



```
var assert = require('assert');

describe('webdriver.io page', function() {

    it('should have the right title - the fancy generator way', function () {
        browser.url('/index.php?page=privilege-escalation.php');
        var title = browser.getTitle();
        assert.notEqual(title, '');
    });

});
```

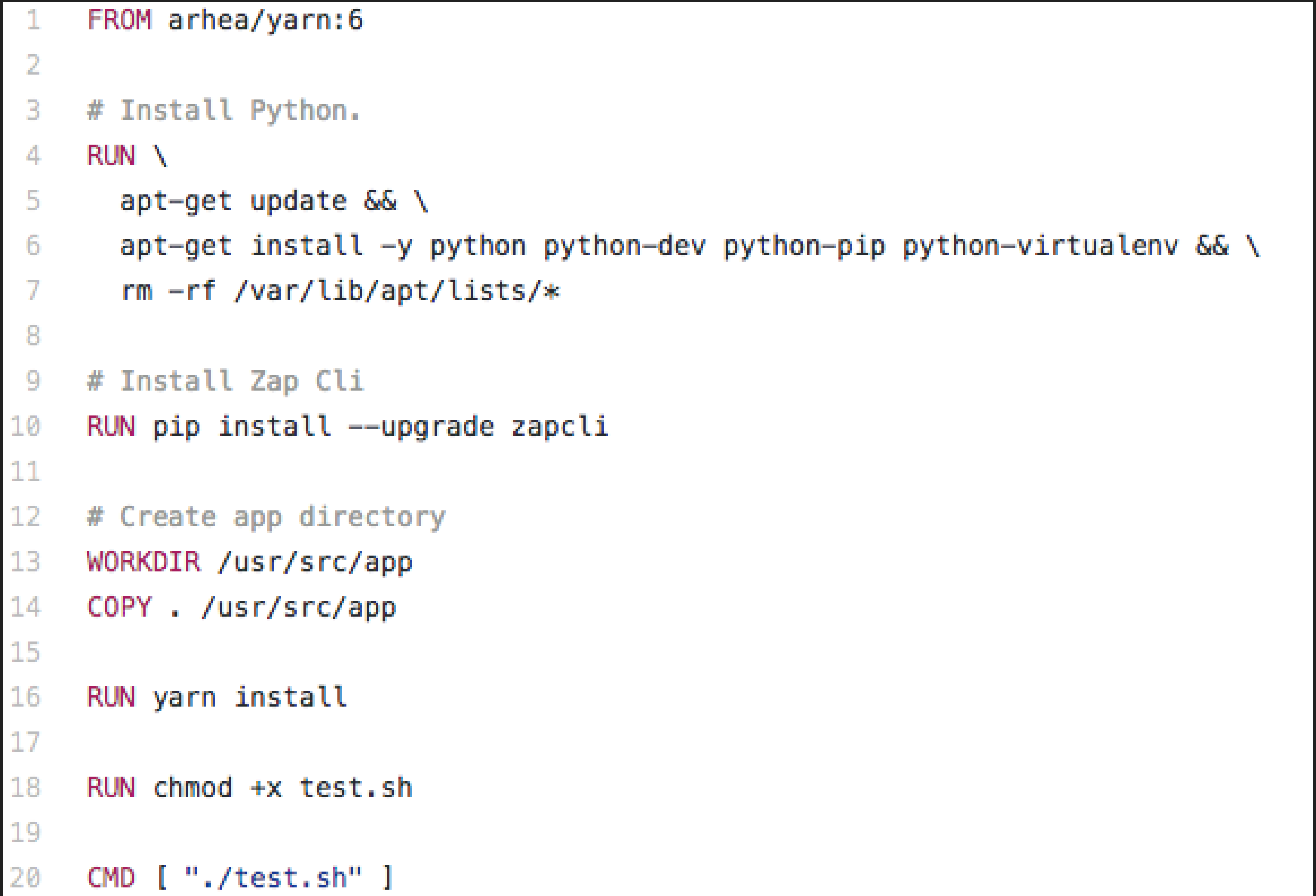
http://goo.gl/sphN9w

Docker

“Docker is the world’s leading software container platform”

“Using containers, everything required to make a piece of software run is packaged into isolated containers”

http://goo.gl/sphN9w



```
FROM arhea/yarn:6

# Install Python.
RUN \
  apt-get update && \
  apt-get install -y python python-dev python-pip python-virtualenv && \
  rm -rf /var/lib/apt/lists/*

# Install Zap Cli
RUN pip install --upgrade zapcli

# Create app directory
WORKDIR /usr/src/app
COPY . /usr/src/app

RUN yarn install

RUN chmod +x test.sh

CMD [ "./test.sh" ]
```

http://goo.gl/sphN9w

OWASP Mutillidae

“free, open source, deliberately vulnerable web-application”

Used to demonstrate ZAP Capabilities

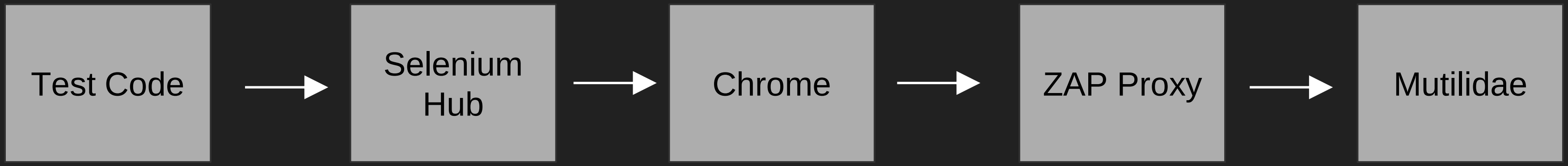
Docker image

http://goo.gl/sphN9w

Putting it all together...

http://goo.gl/sphN9w

Demo Setup



http://goo.gl/sphN9w

Live Demo

All the code is available at Github

http://goo.gl/sphN9w

Comparison with Zap Active Scan

Better coverage of the tested app

Take advantage of existing tests

No additional setup - baseline scan

Mixed tests types - automation and security

Future Plans

Alerts processing - see this issue

Use Jenkins plugin? (we are using TeamCity)

Dedicated security tests

Integrate Active Scan (XSS Dom plugin)

SSL/HSTS

Mobile/Certificate pinning override

Questions?

We are hiring!
Checkout our blog

http://goo.gl/sphN9w