

**Digital Transformation Specialist** 

# Automated Security Scanning in Payment Industry

Michał Buczko





# Objectivity

### Michał Buczko

Test Consultant Public Speaker Security enthusiast

## Agenda

- 1.) Why security?
- 2.) How hard it is to start?
- 3.) How to run automated scanners?
- 4.) Alternative routes..
- 5.) Required investments?
- 6.) Main benefits?





## Why security is important?

Why Your team should focus around this topic inside project or product delivery?



Data integrity and management People give out their private data



Economnic impact of cybersecurity attacks is significant



IoT and digitalization of daily life





## Biggest challenges with starting security testing?



Domain klowledge if huge and We don't have expirience

## Experts costs are big



It costs a lot of time and money to start security testing





## Automated security scanners

Step by step guide how to enable security scanning inside Your existing test automation



Automated functional test i.e. Webdriver

## .000

Security intercepting proxy i.e. OWASP ZAProxy



Effective integration





## **OWASP ZAP**

- open-source web application security scanner
- fully internationalized into over 25 languages
- Used as a proxy server, it allows the user to manipulate all of the traffic that passes through it, including traffic using https.
- Cross-platform tool written in Java
- Some of the built in features include:
  - Intercepting proxy server,
  - Automated scanner,
  - Passive scanner,
- It has a plugin-based architecture and an online 'marketplace'.

Untitled Session - OWASP ZAP		-			
e Edit View Analyse Report Tools Online Help					
$ [Safe mode ] \bullet [1] \models \square \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \bullet \bullet$					
Sites Scripts	Break 🔄 Script Console				
🔻 🚳 🏴 Sites 🔺 📕 Header: Text 🔻 🖪 Body: Text 💌 📃 🗔					
▼          № http://localhost8082           ▶ GET:hackme         HTTP/1.1 200 0K					
Server: Apache-Coyote/1.1					
GET:login Cache-Control: private Expires: Thu, 01 Jan 1970 01:00:00 CET					
CSS X-Frame-Options: DENY					
▼ images X-Content-Type-Options: nosniff ▶ images X-Content-Type-Options: nosniff x-XSS-Protection: 1; mode=block					
▶					
CET:main_hg_1260 npg	Content-Language: en-US				
GET:note_add.png					
GET:lookingglass.png app.baseUrl = "http://localhost:8082	/hackme/";				
GET:picture.png					
L GE. Induite.prog ▶ ui "http://localhost:8082/hackme/scripts/app/application.js?version=1386267486599"×/scri					
<pre>POST:j_spring_security_cf <script src="&lt;/pre" type="text/javascript"></td><td></td><td></td></tr><tr><td colspan=4>GET.rit(page.page.search) Thttps://maps.googleapis.com/maps/api/js?key=AIzaSyBtsB_hMbkhLLzntmun6Ncs3ZR7USHZk8I&s</td></tr><tr><td><pre>v ann v =false" ></script></pre>					
<pre></pre>					
📝 Forced Browse 🛛 🍦 Fuzzer 🛛 🔄 Params 🛛 🤜 Http Sessions 🗍 🍪 Zest Results	WebSockets 🛛 💥 AJAX Spider				
🛗 History 🔍 Search 🔀 Break Points 🏴 Alerts 🕷		₩ Spic			
Cross-domain Java Script source file inclusion					
T 🕋 Alerts (4)         All URL:         http://localhost8082/hackme/					
Cross-domain JavaScript source file inclusion     Risk P     Low					
Content-Type-Options header missing (4)					
E Conversion Conference Academication (C)		Application Error Disclosure			
Alerts 🕅 0 🕅 0 🕅 3 🅅 1		This page contains an error/warning message that may disclose sensi launch further attacks against the web application. The alert could be a			
	URL	http://128.237.191.24:8080/docs/manager-howto.html			
	Parameter	N/A			
	Evidence	java.lang.NumberFormatException: For input string:			
	URL	http://128.237.191.24:8080/docs/jndi-resources-howto.html			
	Parameter	N/A			
	Evidence	JDBC Driver			
	URL	http://128.237.191.24:8080/docs/jndi-datasource-examples-howto.html			
		N/A			
	Parameter	JDBC Driver			

## UI and Report examples

Reliability: Warni	ng	
acomotor https:	/mons.co/(Medium)	Application Error Disclosure
	cription	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
	URL	http://128.237.191.24:8080/docs/manager-howto.html
	Parameter	N/A
	Evidence	java.lang.NumberFormatException: For input string:
	URL	http://128.237.191.24:8080/docs/jndi-resources-howto.html
	Parameter	NA
	Evidence	JDBC Driver
	URL	http://128.237.191.24:8080/docs/jndi-datasource-examples-howto.html
	Parameter	NA
	Evidence	JDBC Driver
	URL	http://128.237.191.24:8080/docs/config/listeners.html
	Parameter	N/A
	Evidence	JDBC Driver



# Sounds easy, but how to start?

Where are the main investments in such solutions?



How to enable scanner in my automation?

### How to decode and test HTTPS traffic?



What is the impact on project schedule?



```
ic static WebDriver initBrowser(WebDriver driver, Strip
Browser WebApp = new Browser();
driver = WebApp.OpenBrowser(browser);
return driver;
```

```
ublic WebDriver OpenBrowser(String browser){
    if (browser == "firefox") {
        driver = new FirefoxDriver(new FirefoxProfile());
    }
}
```

```
else if (browser == "firefox-proxy") {
   FirefoxProfile profile = new FirefoxProfile();
   profile.setPreference("network.proxy.type", 1);
   profile.setPreference("network.proxy.http", "local
   profile.setPreference("network.proxy.http_port", 8
   profile.setPreference("network.proxy.ssl", "localh
   profile.setPreference("network.proxy.ssl_port", 80
   driver = new FirefoxDriver(profile);
```

# Driver with proxy Selenium 2.0

The simple way to:

- Set a manual proxy
- Accept all SSL Certs
- Run browser with proxy on all popups

```
ic static WebDriver initBrowser(WebDriver driver, String browser) {
  System.setProperty("webdriver.gecko.driver","C:\\...\geckodriver.exe");
  Browser WebApp = new Browser();
  driver = WebApp.OpenBrowser(browser);
  return driver;
```

```
public WebDriver OpenBrowser(String browser){
    if (browser == "firefox") {
        driver = new FirefoxDriver();
    }
    else if (browser == "firefox-proxy") {
}
```

}

```
DesiredCapabilities required = new DesiredCapabilities();
JsonObject json = new JsonObject();
json.addProperty("proxyType", "MANUAL");
json.addProperty("httpProxy", "localhost");
```

```
json.addProperty("httpProxyPort", Integer.valueOf("8080"));
json.addProperty("sslProxy", "localhost");
json.addProperty("sslProxyPort", Integer.valueOf("8080"));
```

```
required.setCapability("proxy", json);
required.setCapability(CapabilityType.ACCEPT_SSL_CERTS, true);
required.setJavascriptEnabled(true);
required.setCapability("marionette", true);
required.setCapability("acceptInsecureCerts", true);
driver = new FirefoxDriver(required);
```

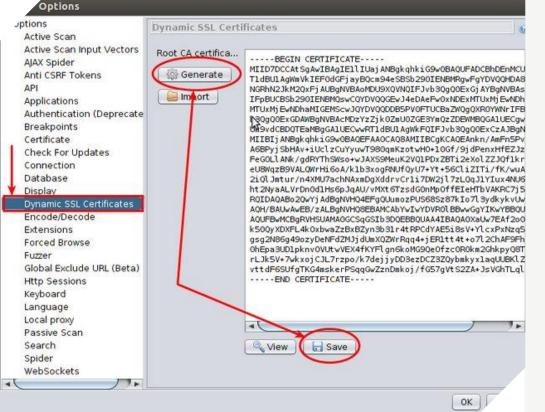
# Driver with Proxy Selenium 3.0

The simple way to:

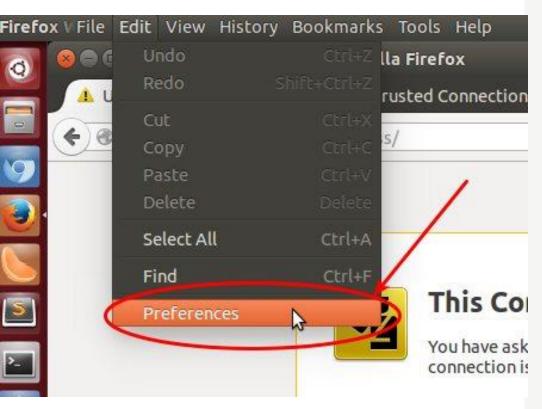
- Set a manual proxy
- Accept all SSL Certs
- Run browser with proxy on all popups

#### Elle Edit View Analyse Beport Tools Online Help Standard mode 💌 👌 🔛 🖬 Filter.. OX HALLON U Browse APS Break Script Console Sites Scripts Encode/Hash Ctrl+E G PStes Toggle break on all requests Ctrl+B \* 10 https://192.168.56.101 Togole break on all responses Ctrl+Alt+B Ctrl+S Submit and step to next request or response. Ctrie C Submit and continue to next break point Bin request or response Ctrl+X Add a custom HTTP break point ... Ctrl+A. Advanced Active Scan. Ctrl+Alt+A Manual Request Editor. Ctrl+M Run the Garbage Collector Manual Send WebCocket Meter Ski Spider Forced Browse G Fuzzer Params Ktp Sessions Zest Results Clients A webSockets MAAX Spider Output Search X Break Points PD Alerts Active Scan History Filten OFF Y Reg. Timestamp Method URL Code Reason Size Resp. Bod Note Tags 24 05/12/14 23:04:28 GET https://j92.168.56.101/wordpress/wp.content/t. 304 Not Modified 26 ms 0 hites 23 06/12/14 23:04:28 GET https://192.168.56.101/wordpress/wp-includes/j. 304 Not Modified 38 ms 0 bytes 22 06/12/14 23:04:28 6ET https://192.168.56.101/wordpress/wp-content/t. 304 Not Modified 59 ms 0 bytes 21 06/12/14 22:04:28 GET https://192.168.56.103/wordpress/wp-includes/L 203 Not Modified () hotes 33 mis 20 05120423:0428 19 06/12/14 23:03:06 GET https://192.168.56.101/wordpress/wp-content/t. 304 Not Modified 26 ms 0 hites 18 05/12/14 23:03:05 6ET https://192.168.56.101/wordpress/wp-includes/j. 304 Not Modified 37 ms 0 bytes 17 06/12/14 23:03:06 GET https://192.168.56.101/wordpress/wp-includes/j. 304 Not Modified 39 ms 0 bytes 16 06/12/14 23:03:05 304 Not Modified GÉT. https://192.168.56.101/wordpress/wp-content/t... S ms 0 bytes 15 06/12/14 23:03:06 GET. https://192.168.56.101/wordpress/ 200 06 120 ms 12.62 KB PLOW Form, Script, Comm 13 05/12/14 22:59:41 GET. https://192.168.56.101/wordpress/wp-content/t. 200 OK 14 ms 1.48 KB P Low Comment 12 06/12/14 22:59:41 GET https://192168.56.101/wordpress/wp-includes/j. 200 OK 39 ms 93.56 KB PLow Commerci 8 06/12/14 22:59:41 GET https://192.168.56.101/wordpress/wp-includes/j. 200. OK 17 ms 7.03 KiB Low Comment nenne mene here of the lange 1 of the descent of the sector of Charles . 10.14.1 addam 1 Alerts #0 #0 #2 #1 Current Scans 👌 0 🛞 0 🎤 0 🤤 0

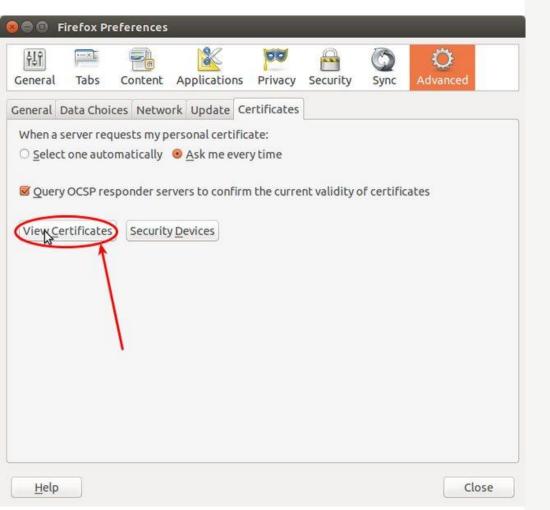
- ▶ Open up OWASP ZAP
- go to Tools -> Options
- ▶ In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.



- ▶ Open up OWASP ZAP
- go to Tools -> Options
- ▶ In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.

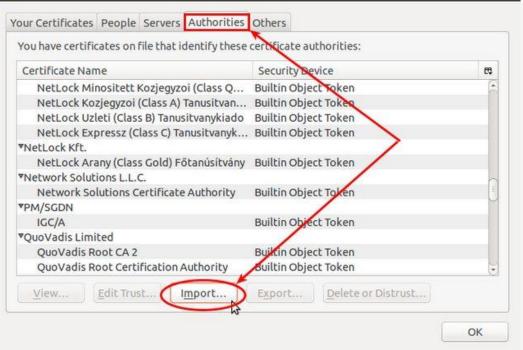


- Open up OWASP ZAP
- ▶ go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.



- Open up OWASP ZAP
- ▶ go to Tools -> Options
- ▶ In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.

#### 😑 😑 Certificate Manager



- Open up OWASP ZAP
- ▶ go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.

#### 😣 🗐 🕕 Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "OWASP Zed Attack Proxy Root CA" for the following purposes?

Trust this CA to identify websites.

Trust this CA to identify email users.

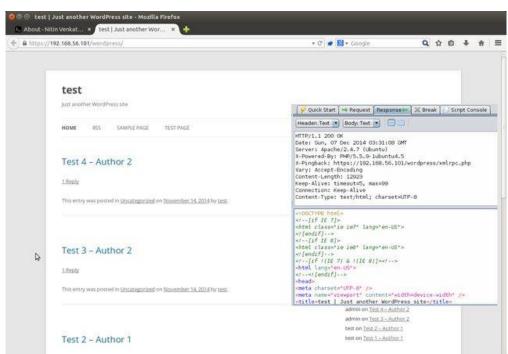
Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate



- Open up OWASP ZAP
- go to Tools -> Options
- ▶ In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.



1 Reply

- Open up OWASP ZAP
- ▶ go to Tools -> Options
- ▶ In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab and click on Import and choose the OWASP ZAP Root Certificate
- Check all the boxes
- Browse sites with HTTPS enabled. You're no longer prompted with the SSL Security Exception Error message.



## What can I get from this?

### What is the benefit for my:

- Team
- Project
- Product
- Company



Easy start with building image about security of your system



Starting point for learning, excercising, upskilling anyone interested in security

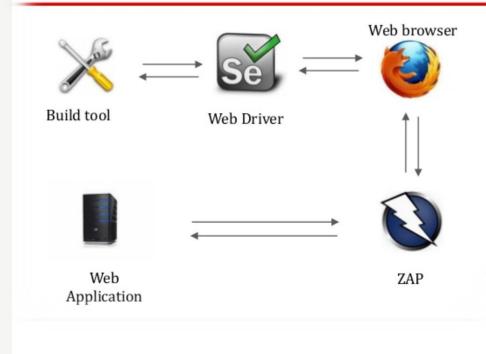


Security related pipeline inside Your CI/CD systems without investing in additional costly licences



## How to maximize the benefits?

### Build Tool + Selenium + ZAP = Profit!





## Does any alternatives exist?

How to enable similar results via other market available solutions?

### Objectivity Test Framework

### Features



- Multiple integrated tools and solutions
- Free to use and adapt to Your needs
- Constant development make by Objectivity

### Risks



- Require technical knowledge to start integration
- Its a tool-set to re-use not box solution

### **Benefits**



- Freedom of usage and adaptation
- Open-source
- Not limited by technology stack or business objective



## F-Secure Mittn BDD Security

### Features

- Open source on github
- BDD test enhancement without technical skills requirement
- Cl integrated

### Risks

- BDD tests are not easily owned inside organizations
  - Another layer on top of tool-set i.e. ZAP
  - No proven market value I heard

### **Benefits**



0

- BDD in good setup can work very well Few alternative routes to use
- Less technical requirements to enable such solutions



### Qualys Web Scanner

#### Features



- Standalone scanning solution
- Do not require technical knowledge
- Push URL and wait for results

### Risks



- No control over the scanning scope Not cheap solution – costly licences
- Sometimes to big for the problem

### **Benefits**



- Easy to understand visualisation
- Well documented results
- Catalog feature, if applied on multiple projects





### **Digital Transformation Specialist**

## Any questions ?

Thanks !!

