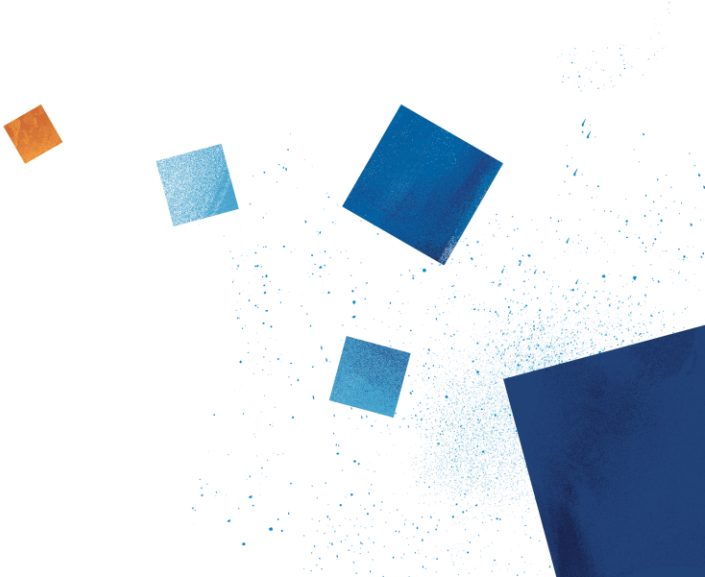
Objectivity

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

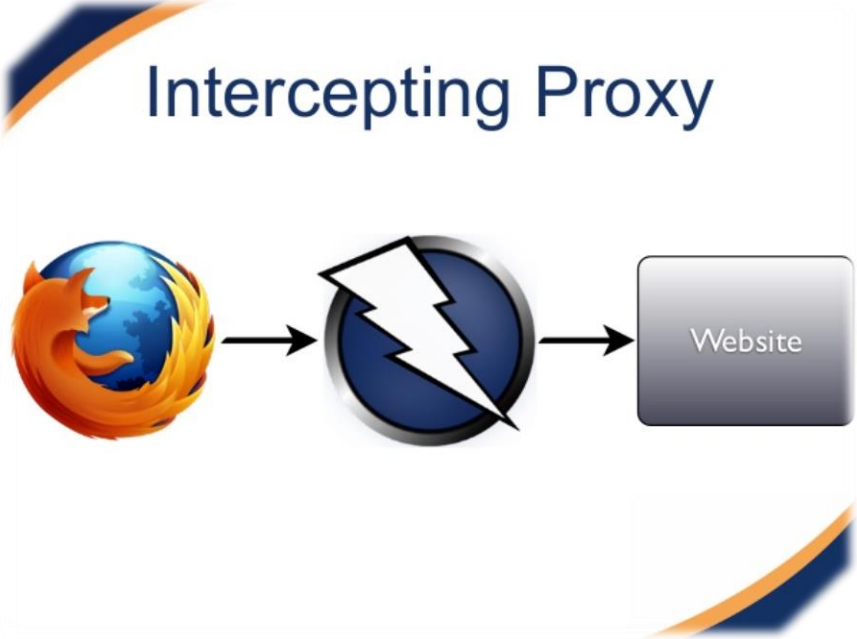
Automated security scanners

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

Automated functional test
i.e. Webdriver

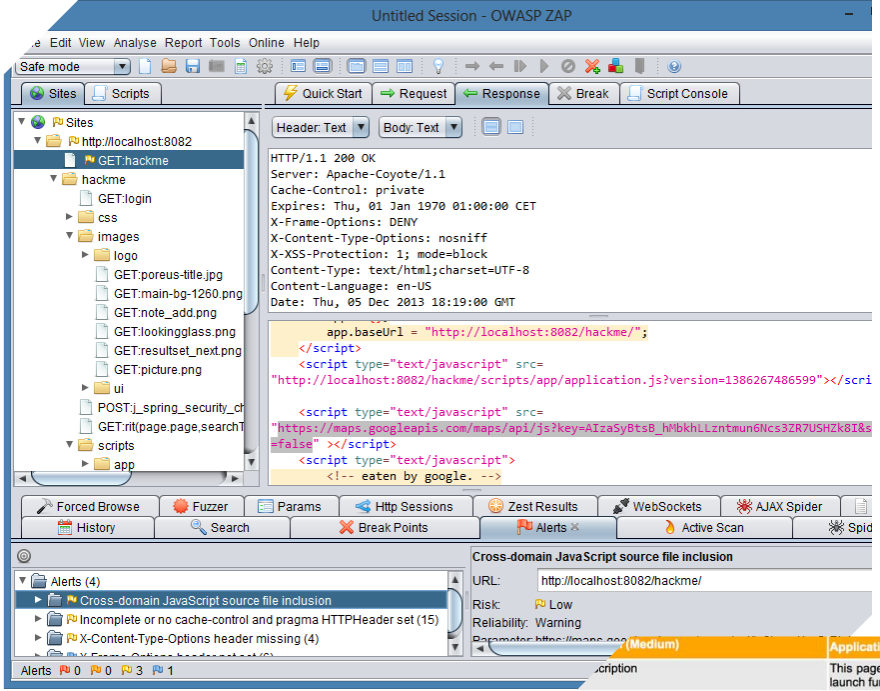
Security intercepting proxy
i.e. OWASP ZAProxy

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’.



UI and Report examples

(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	N/A
Evidence	JDBC Driver
URL	http://128.237.191.24:8080/docs/jndi-datasource-examples-howto.html
Parameter	N/A
Evidence	JDBC Driver
URL	http://128.237.191.24:8080/docs/config/listeners.html
Parameter	N/A
Evidence	JDBC Driver

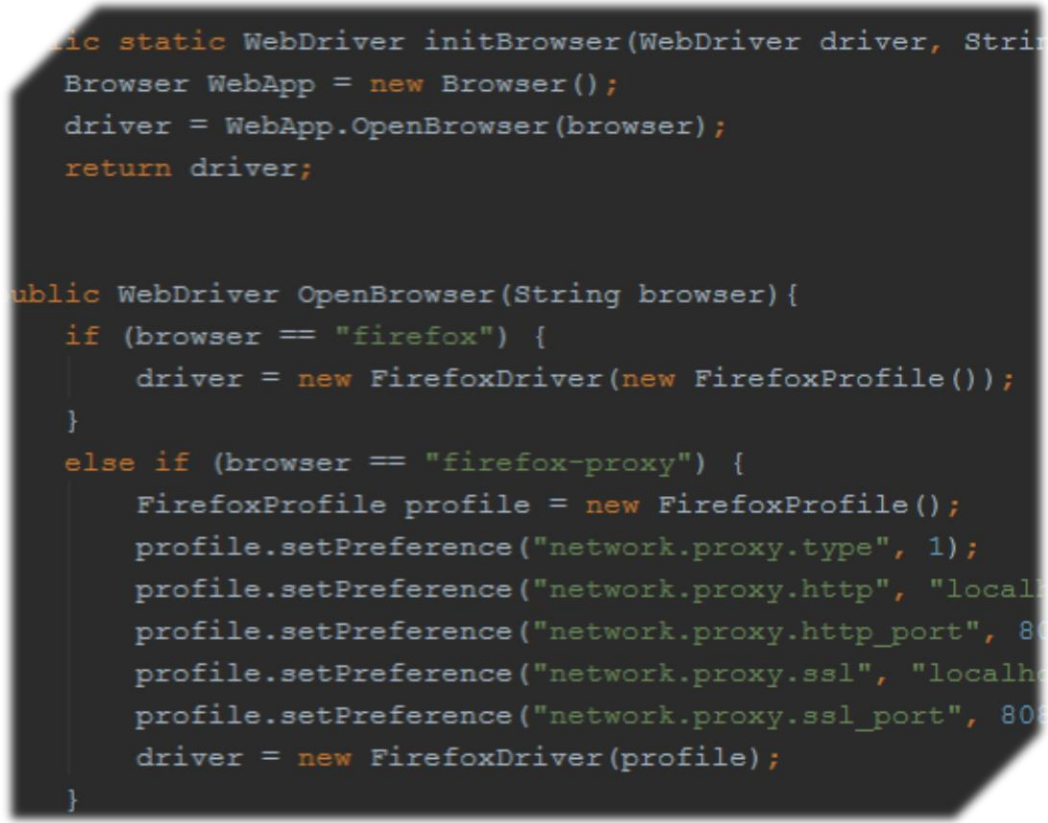
Sounds easy, but how to start?

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?



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

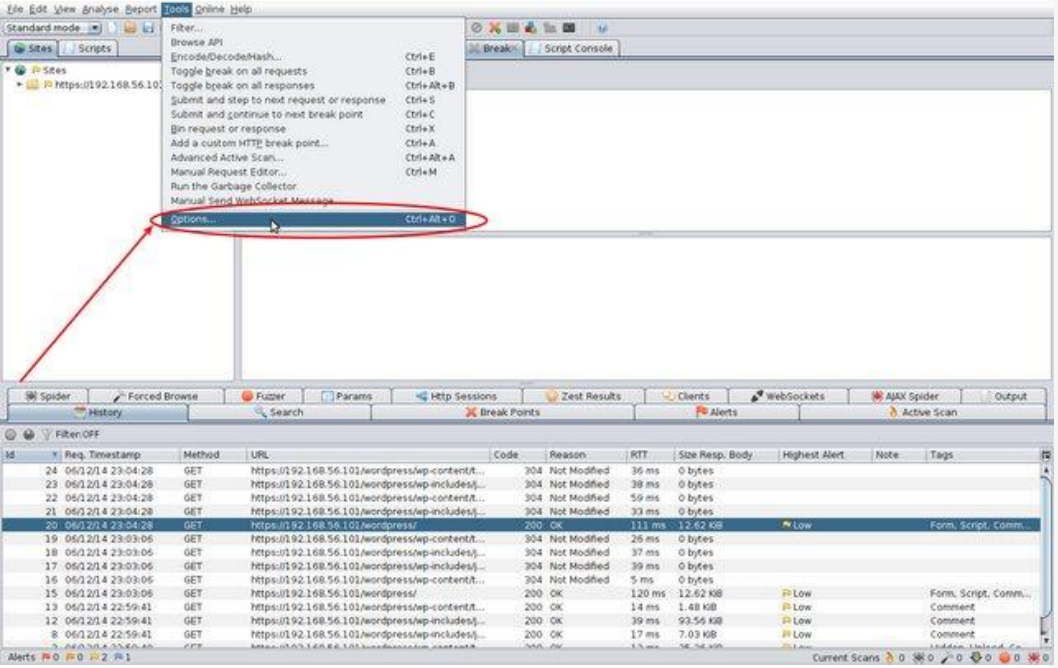
```
ıic static WebDriver initBrowser(WebDriver driver, String browser) {
    System.setProperty("webdriver.gecko.driver","C:\\...\\geckodriver.exe");
    Browser WebApp = new Browser();
    driver = WebApp.OpenBrowser(browser);
    return driver;
}

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:

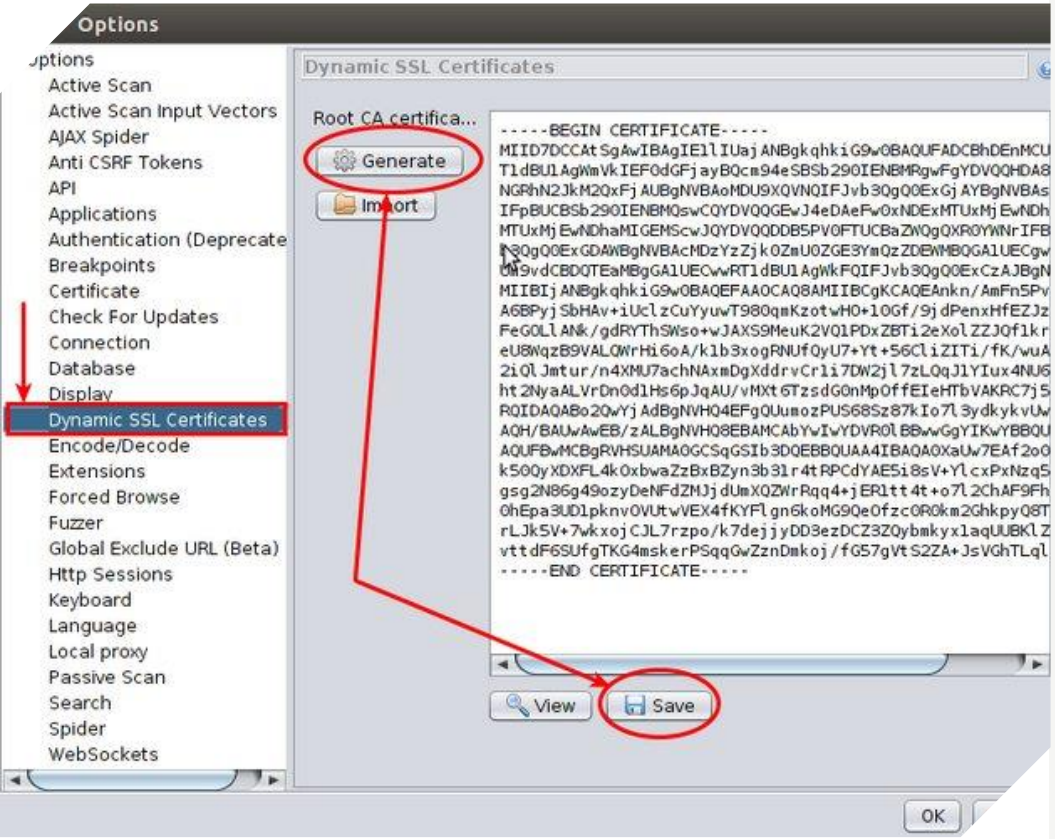
- Set a manual proxy
- Accept all SSL Certs
- Run browser with proxy on all popups

ZAP SSL certificate in Firefox



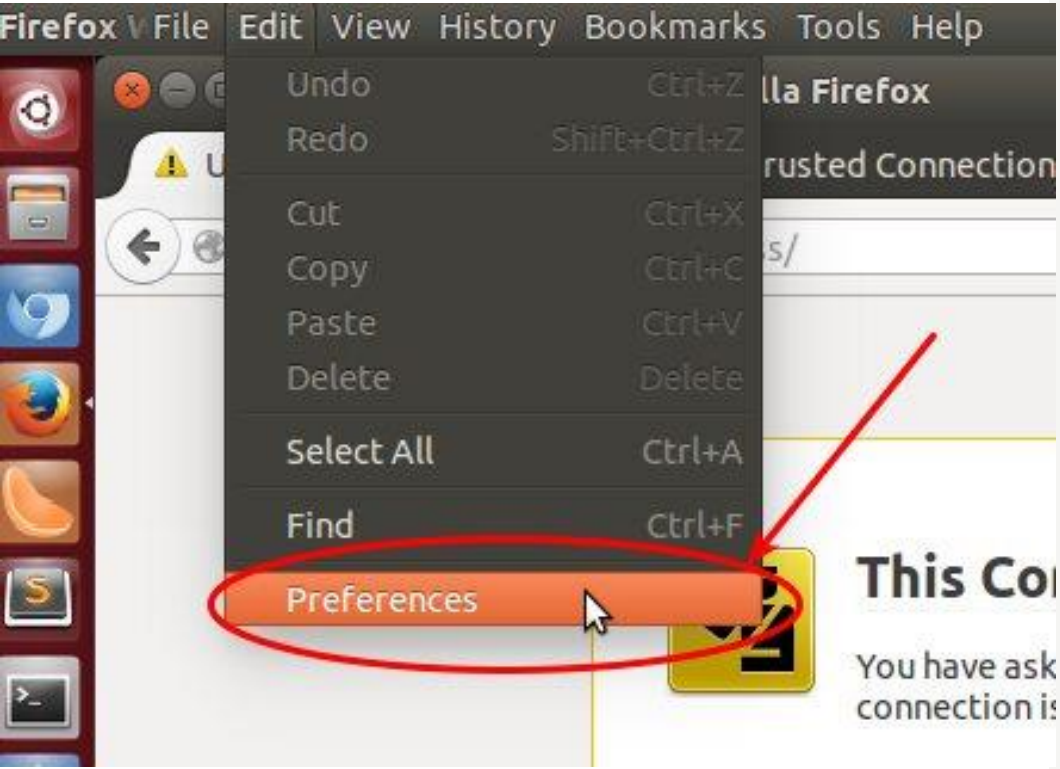
- Open up OWASP ZAP
- go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab 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.

ZAP SSL certificate in Firefox

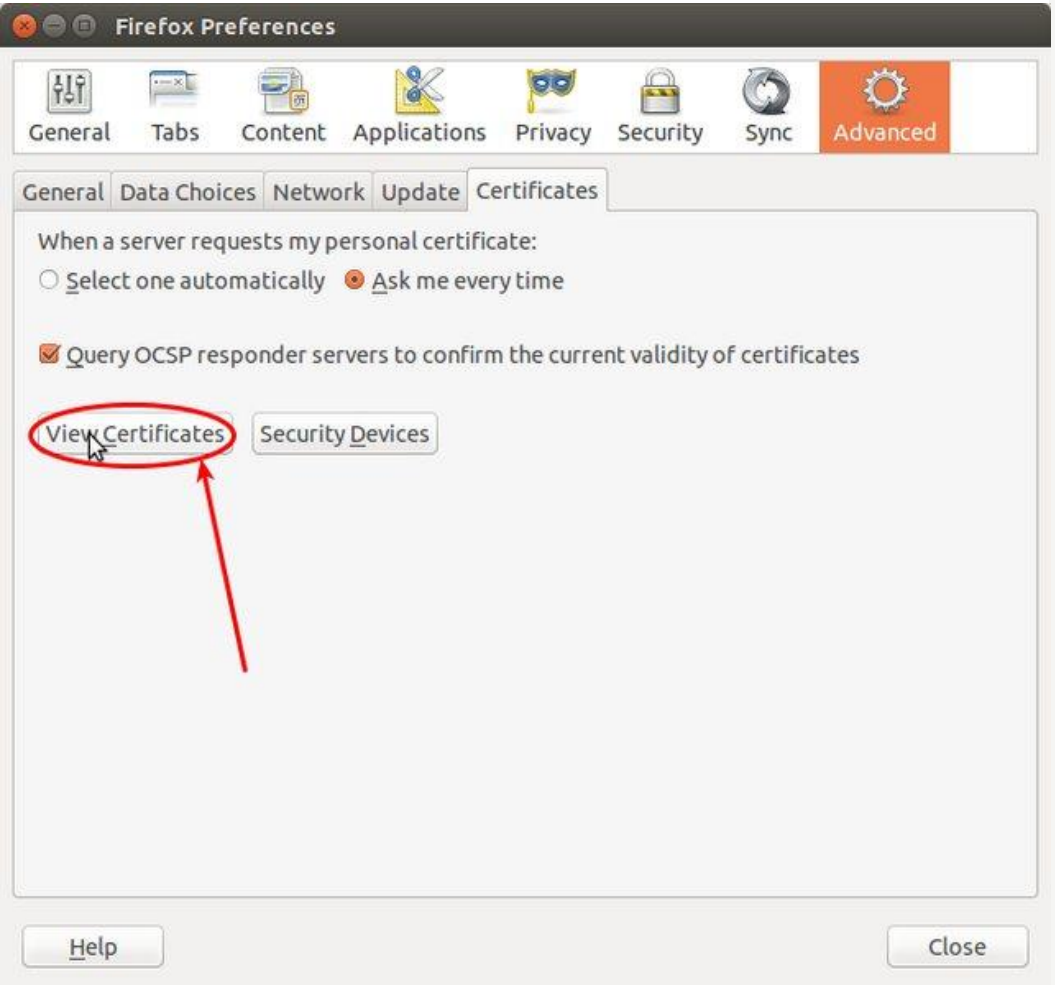


- Open up OWASP ZAP
- go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab 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.

ZAP SSL certificate in Firefox



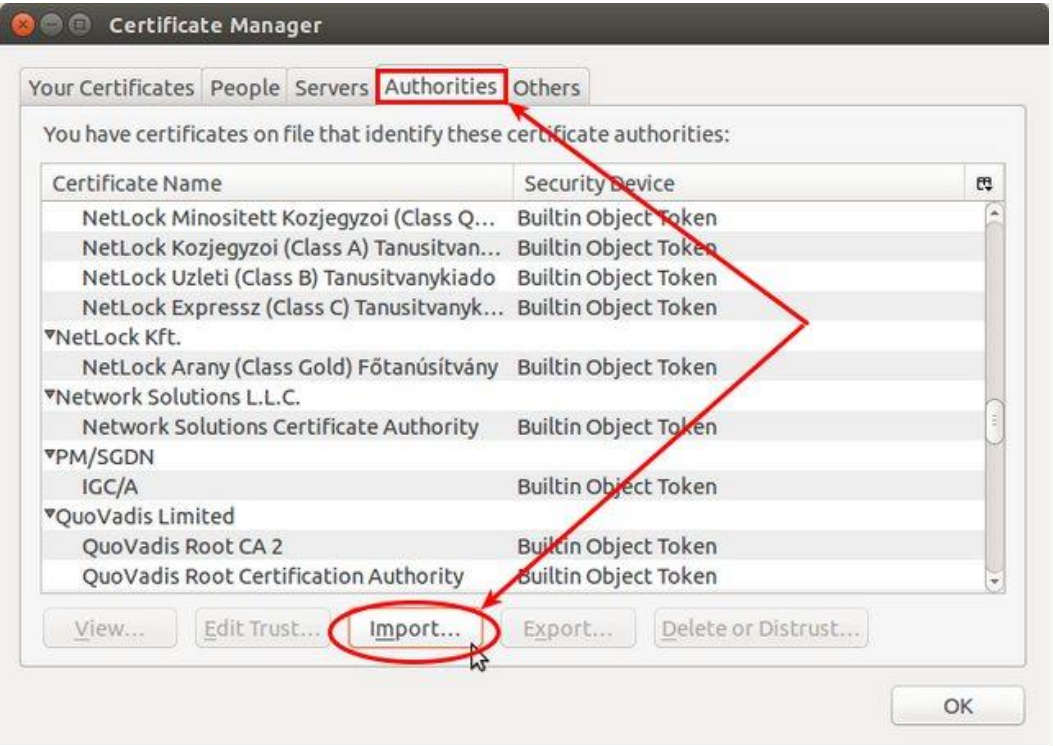
- Open up OWASP ZAP
- go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab 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.



ZAP SSL certificate in Firefox

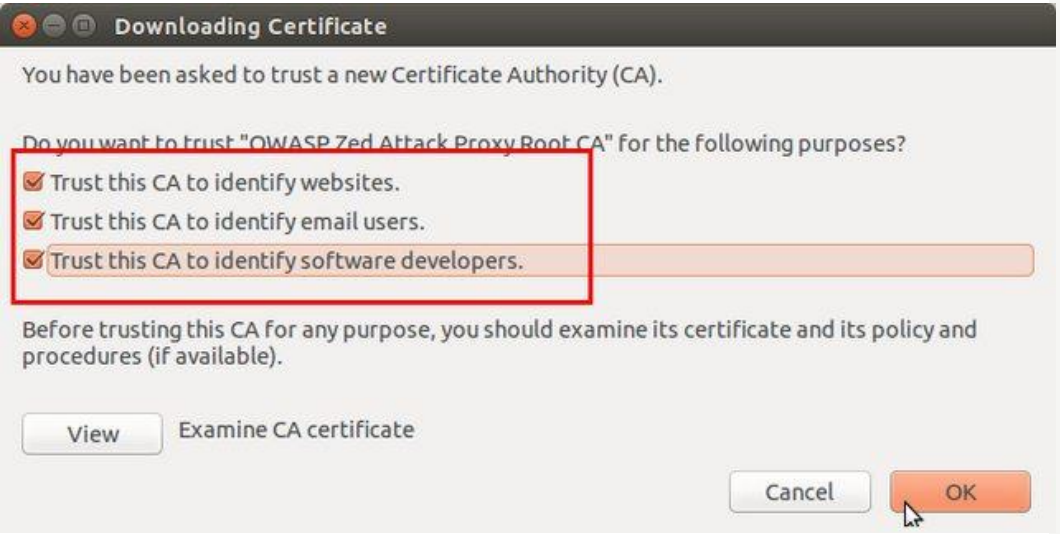
- Open up OWASP ZAP
- go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab 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.

ZAP SSL certificate in Firefox



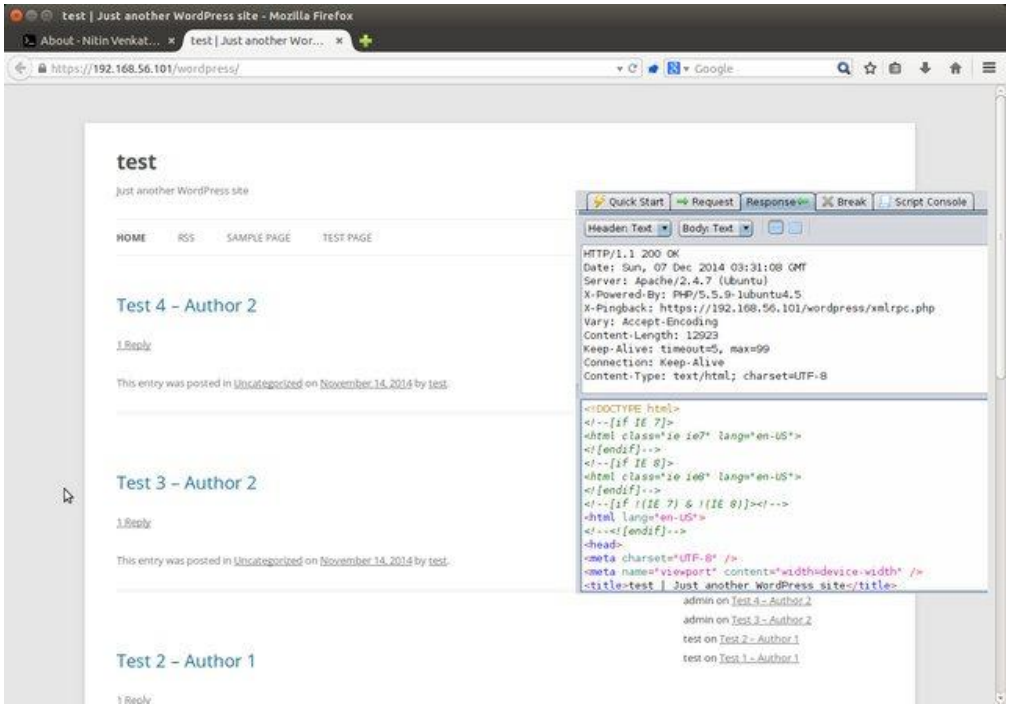
- Open up OWASP ZAP
- go to Tools -> Options
- In the Certificates section, click on Generate
- Save the certificate in some location
- Navigate to the Preferences of your browser
- Click on the Advanced tab, navigate to the Certificates tab and click on View Certificates
- Select the Authorities tab 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.

ZAP SSL certificate in Firefox



- 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.

ZAP SSL certificate in Firefox



- 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:

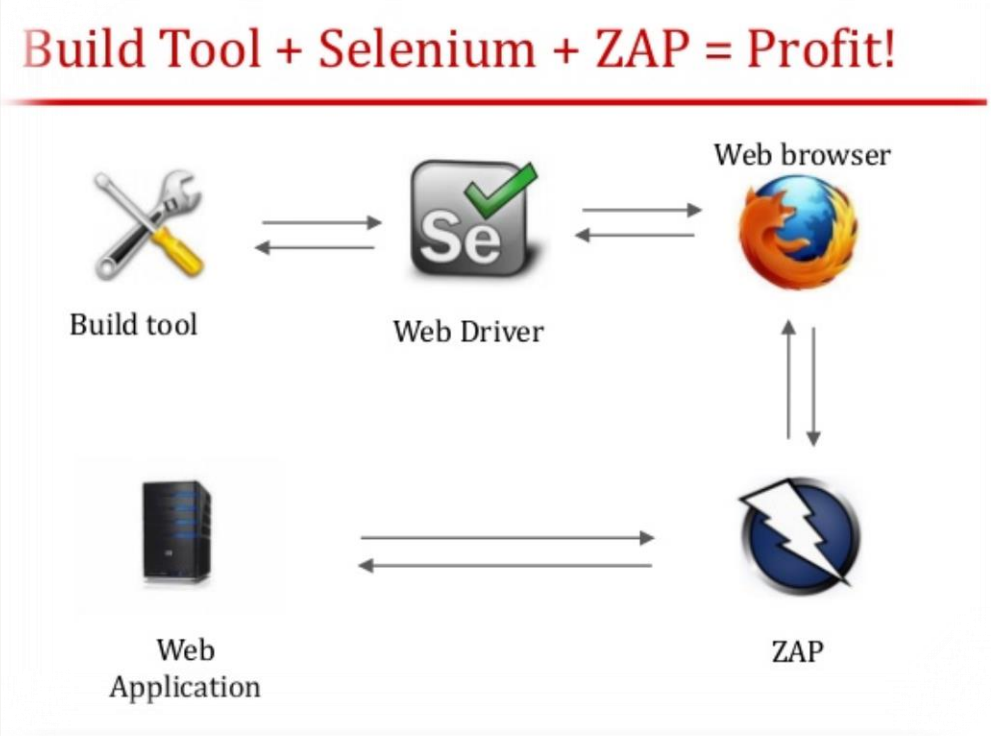
- Team
- Project
- Product
- Company

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?



Does any alternatives exist?

How to enable simillar results via other market available solutions?

Objectivity Test Framework

Features

- Multiple integrated tools and solutions
- Free to use and adapt to Your needs
- Constant developement 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
- CI 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

- 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

Any questions ?

Thanks !!