## HACK YOUR WEBAPP

#### LUUK BUIT



github.com/lwkbuit/javaone2017

## PRACTICE MPROVE

## PARTONE

## THEORY

#### VULNERABILITIES



THREATS

CONTROLS



VERIFY

## APPLICATION SECURITY VERIFICATION STANDARD

## PARTTUO

## PRACTICE

#### OWASP ZAP CODEREVIEW DEPENDENYCHECK AUTOMATION

#### ZAP



#### CODEREVIEW

- Missing authentication/authorization
- Input validation
- SQL Injection
- Cross Site Scripting

#### **KSS & FRAMEWORKS**

```
JSP
<%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
<c:out value="${myName}"/>
Wicket
add(new Label("markup", "<h1>Hello!</h1>")
  .setEscapeModelStrings(false));
```

#### DEPENDENCY CHECK

\$ brew install dependency-check

```
$ dependency-check \
   --scan {dir} \
   --project {name}
```



http://jeremylong.github.io/DependencyCheck/

#### AUTOMATION

- Static code analysis
- Passive/active scanner
- Security acceptance tests
  - Selenium
  - BrowserMob Proxy

## PARTTHREE

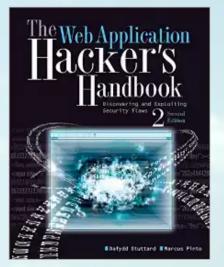
## IMPROVE

#### IMPROVE

- Playgrounds
  - Security shepherd, Webgoat, Bodgeit
- OWASP Conferences
- Web Security Fundamentals | edX
  - Philippe De Ryck



#### 



# DISCUSSION & QUESTIONS

fsociety