

HACK YOUR
OWN
WEBAPP



Belastingdienst

LUUK BUIT



@lwkbuit



github.com/lwkbuit/javaone2017



THEORY
PRACTICE
IMPROVE

PART ONE

THEORY

VULNERABILITIES

TECHNOLOGY
+ ASSETS

THREATS

CONTROLS

VERIFY



APPLICATION
SECURITY
VERIFICATION
STANDARD

PART TWO

PRACTICE

OWASP ZAP
CODEREVIEW
DEPENDENCYCHECK
AUTOMATION

ZAP



BROWSER



ZAP



WEB APPLICATION

CODEREVIEW

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

XSS & 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

PART THREE

IMPROVE

IMPROVE

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



W A H H





fsociety

DISCUSSION & QUESTIONS