OWASP

Open Web Application Security Project

DevSecOps落地之二三事

王文君

场景一：开发VS测试

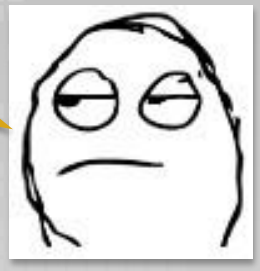
测试MM

别动我们测试的服务器，你们自己搭一个！

这个功能你们开发好了吗？在我们测试环境部署了吗？

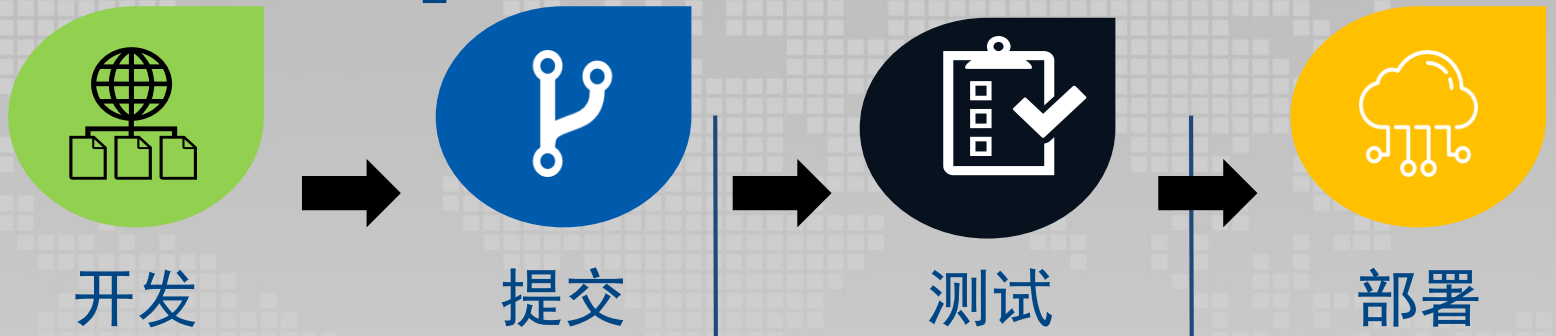
谁在用我们的账号？招呼都不打！我要用，赶紧退出来！

我电脑内存少，不用你的用谁的？



程序员

没有DevOps之前



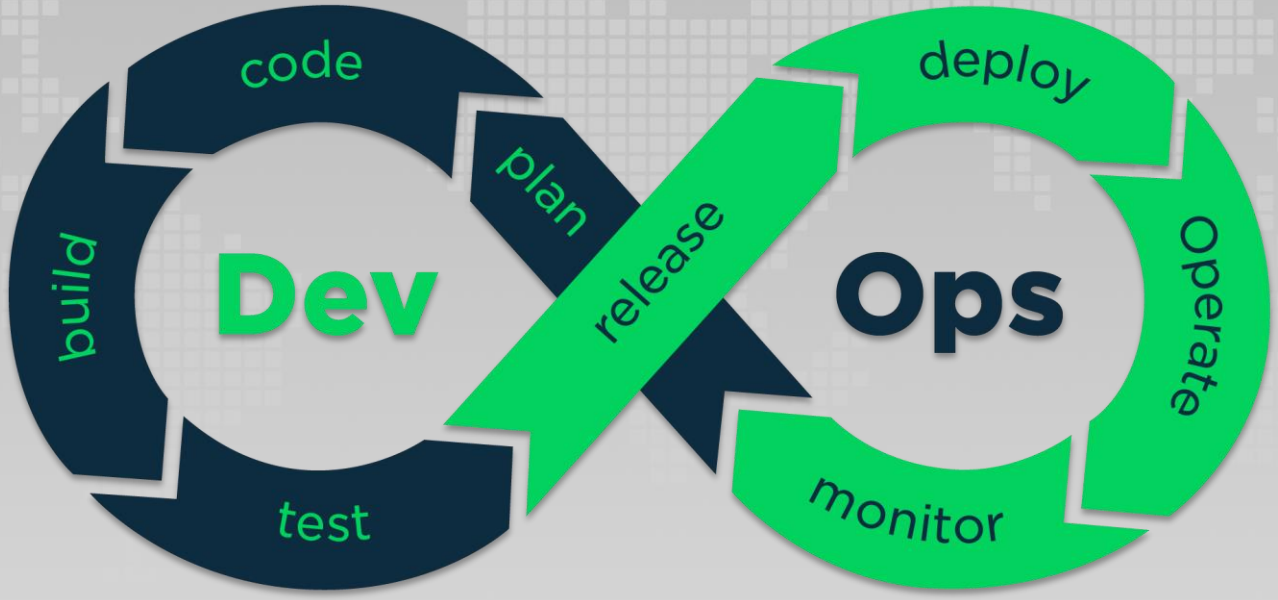
团队

Dev　QA　Ops

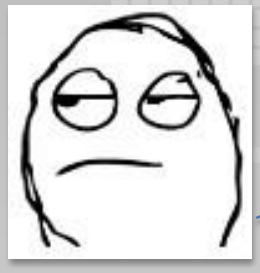
环境

Dev　Test　Test　Stage　Prod

DevOps


code
plan
build
Dev
test
release
deploy
operate
Ops
monitor

场景二：(开发+测试)VS安全



程序员

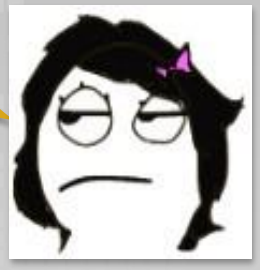
你知不知道产品明天就要发布了，你提的这个高危漏洞至少需要改2天！！

哎，开发改了，我又要做回归测试了…

测试MM

你能不能下次早点规划安全测试啊？？

早早早，环境没好，怎么安全测试？



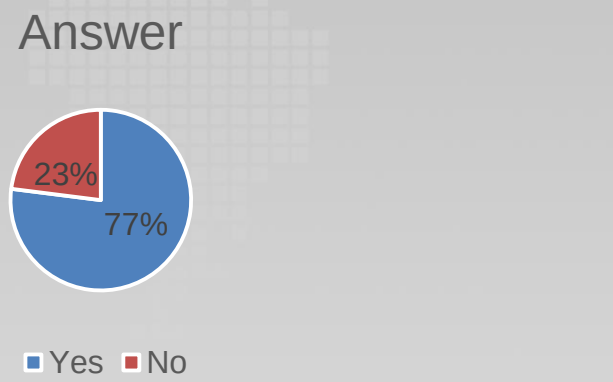
安全人员


DevOps打破了各部门之间沟通壁垒，
但Security团队往往还是被隔离着…

Gartner统计报告(Sep 2016)

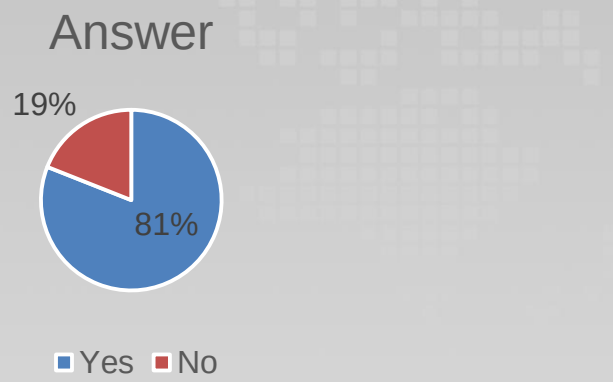
Information Security Professionals

Do You Believe Your Information Security Policies/Teams Are Slowing IT Down?



IT Operations Professionals

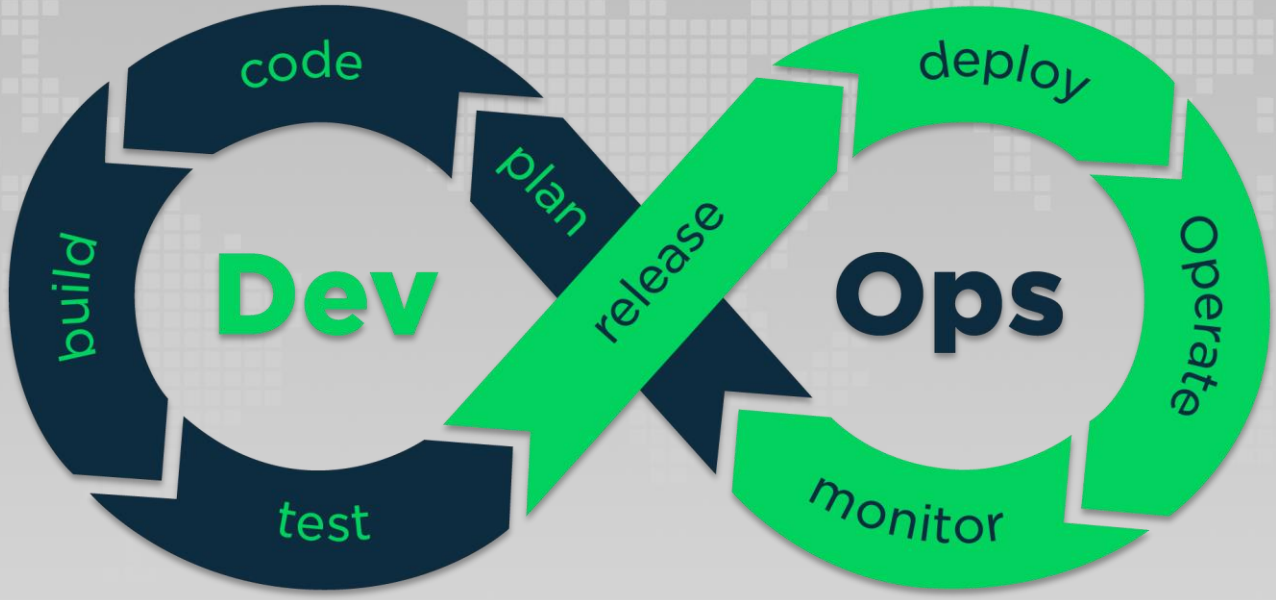
Do You Believe Your Information Security Policies/Teams Are Slowing IT Down?



来源：https://cdn2.hubspot.net/hubfs/1958393/White_Papers/devsecops_how_to_seamlessly__315283.pdf

DevSecOps

Security



DevSecOps实施面临的困难

Dev

缺乏安全意识

市场压力

ITOps

注重边界保护

那是安全团队的事情

Security

缺乏应用安全专才

安全与DevOps集成困难

三因素帮助企业实现DevSecOps

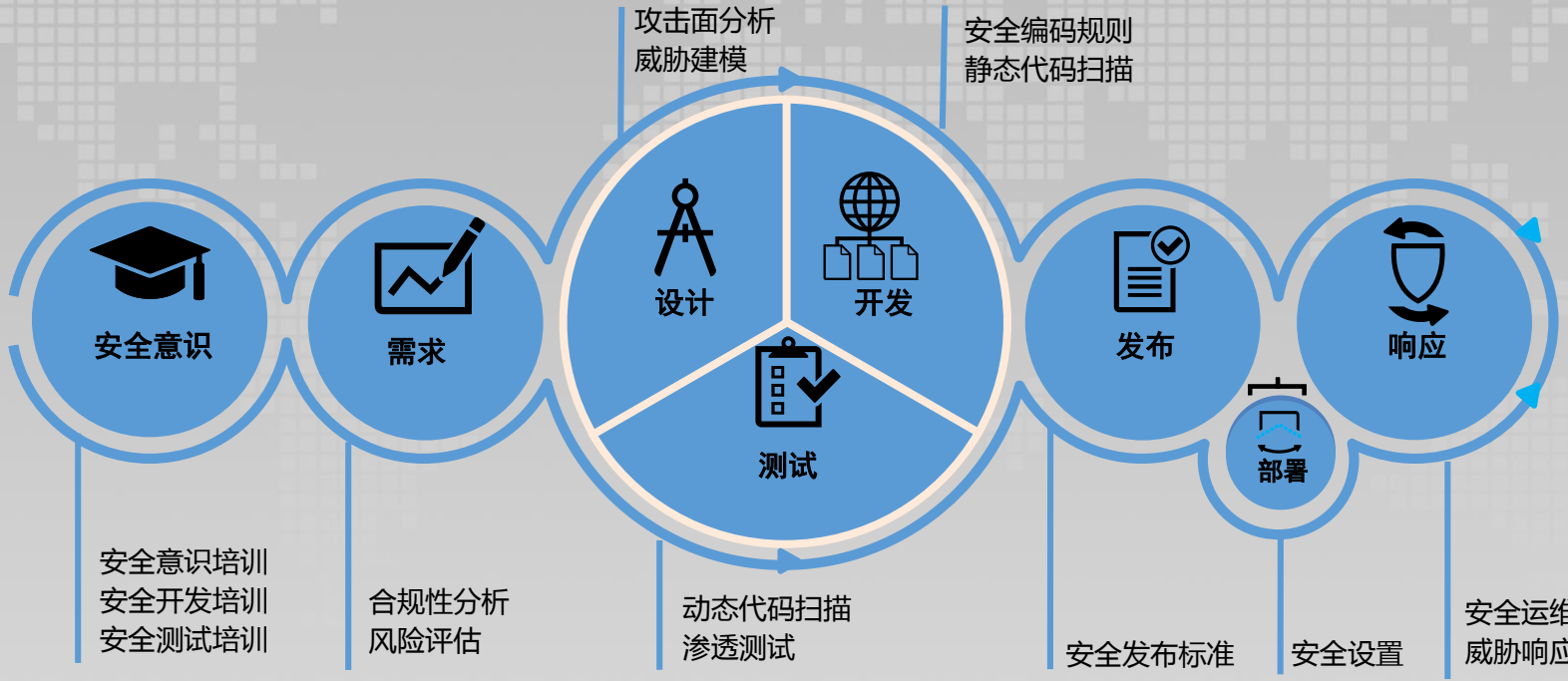
文化

风险量化+dashboard

安全人员融入开发团队

自动化

流程 – Security Shift Left



技术-DevSecOps工具箱

开发IDE

需求管理

代码仓库

构建服务器

配置自动化

团队协作

应用安全

安全运维

OWASP提供的工具

安全意识

- Top 10
- Snakes & Ladders
- Shepherd

需求

- ASVS

设计

- Cornucopia

开发

- Dependency Check
- Proactive Controls
- Cheat Sheets

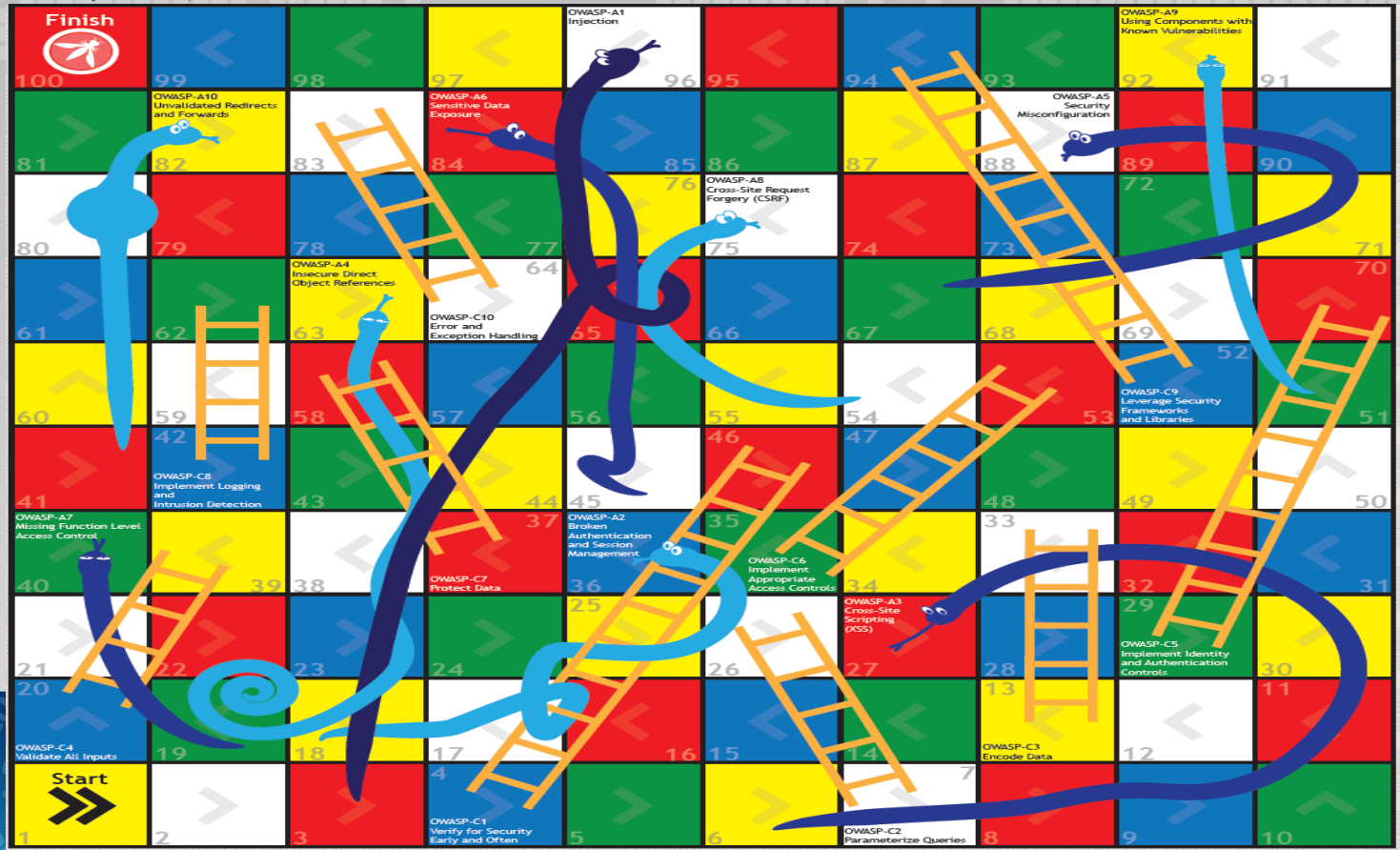
测试

- ASVS
- Testing Guide

响应

- Defect Dojo

工具1 – Snake&Ladder



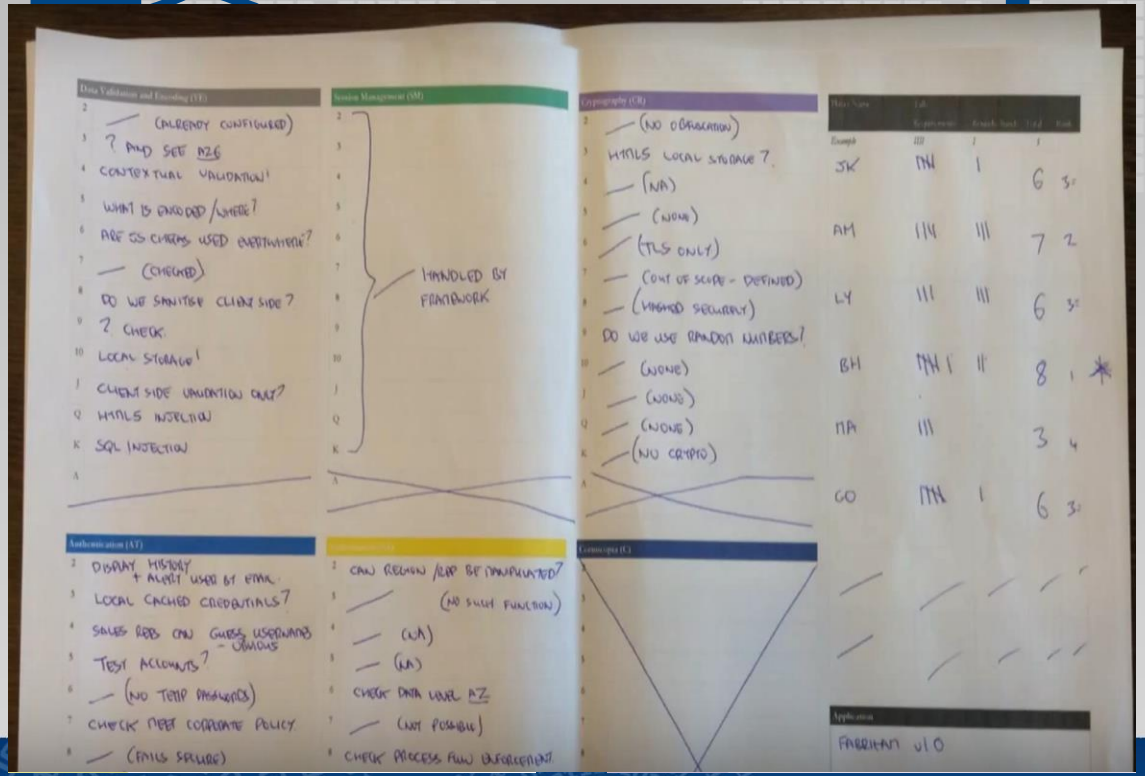
OWASP
Open Web Application Security Project

工具2 - ASVS

		1	2	3
V9.1	Verify that all forms containing sensitive information have disabled client side caching, including autocomplete features.	✔	✔	✔
V9.2	Verify that the list of sensitive data processed by this application is identified, and that there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). Verify that this policy is properly enforced.			✔
V9.3	Verify that all sensitive data is sent to the server in the HTTP message body (i.e., URL parameters are never used to send sensitive data).	✔	✔	✔
V9.4	Verify that all cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		✔	✔
V9.5	Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.		✔	✔
V9.6	Verify that there is a method to remove each type of sensitive data from the application at the end of its required retention period.			✔

1. 开发者可用来做指导
2. 安全人员可以用来检查
3. 外包作为验收标准

工具3 - Cornucopias

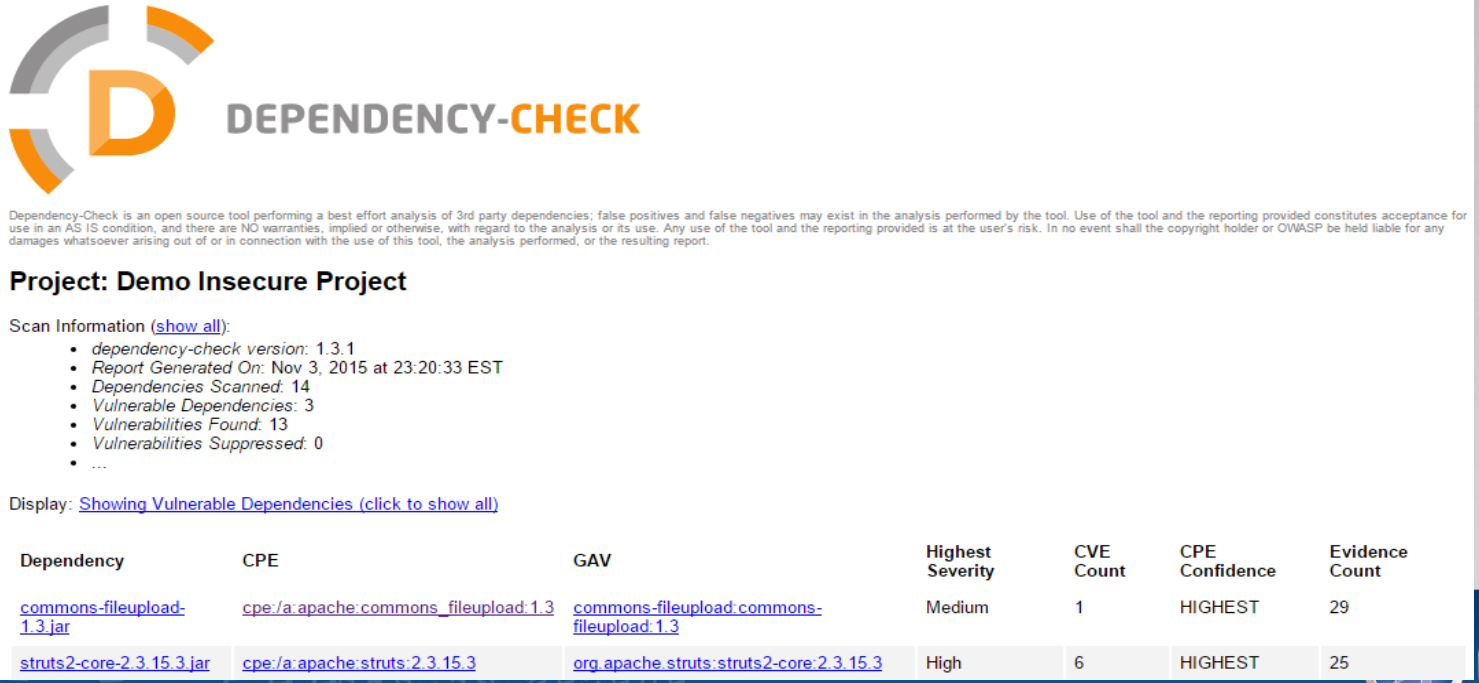


1. Gamification
2. OWASP SCP/ASVS/Testing guide
3. 6 suites * 13 cards
   - Data validation and encoding
   - Authentication
   - Session management
   - Authorization
   - Cryptography
   - Cornucopia

https://www.youtube.com/watch?v=i5Y0akWj31k

工具4 - OWASP Dependency

Collect all dependencies → Identify CPE → Search vulnerabilities from NVD → CVE Report



DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

Project: Demo Insecure Project

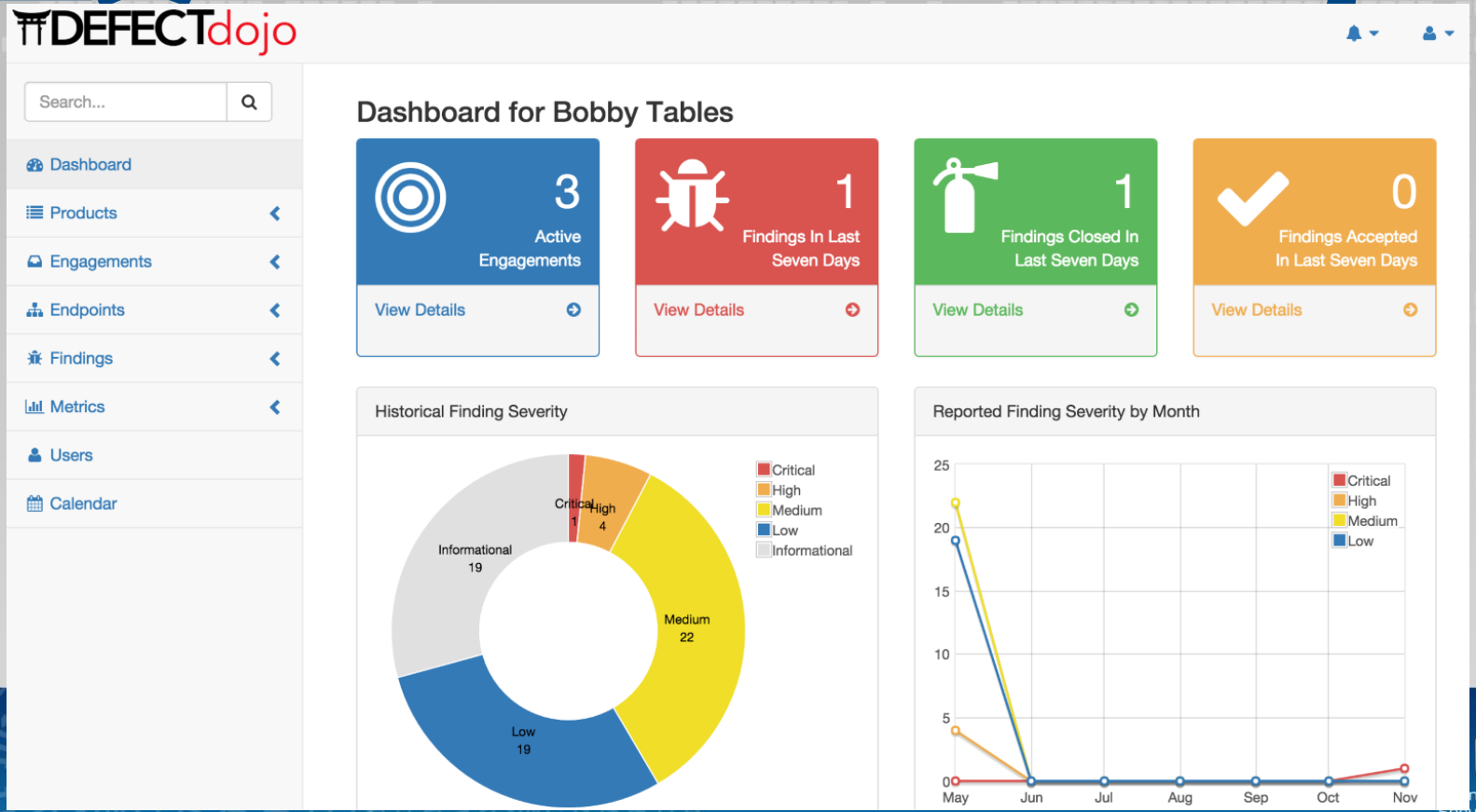
Scan Information (show all):

- *dependency-check version*: 1.3.1
- *Report Generated On*: Nov 3, 2015 at 23:20:33 EST
- *Dependencies Scanned*: 14
- *Vulnerable Dependencies*: 3
- *Vulnerabilities Found*: 13
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-fileupload-1.3.jar	cpe:/a:apache:commons_fileupload:1.3	commons-fileupload:commons-fileupload:1.3	Medium	1	HIGHEST	29
struts2-core-2.3.15.3.jar	cpe:/a:apache:struts:2.3.15.3	org.apache.struts:struts2-core:2.3.15.3	High	6	HIGHEST	25

工具5 - OWASP Defect Dojo



应用今天所学的

3 天

- 改变意识，拥抱DevSecOps

3 周

- 精心专研DevSecOps用的各种工具和技术

3 月

- 将Security引入到DevOps中去

Perfect or Progress? 记住：重在改善，而不是追求完美。