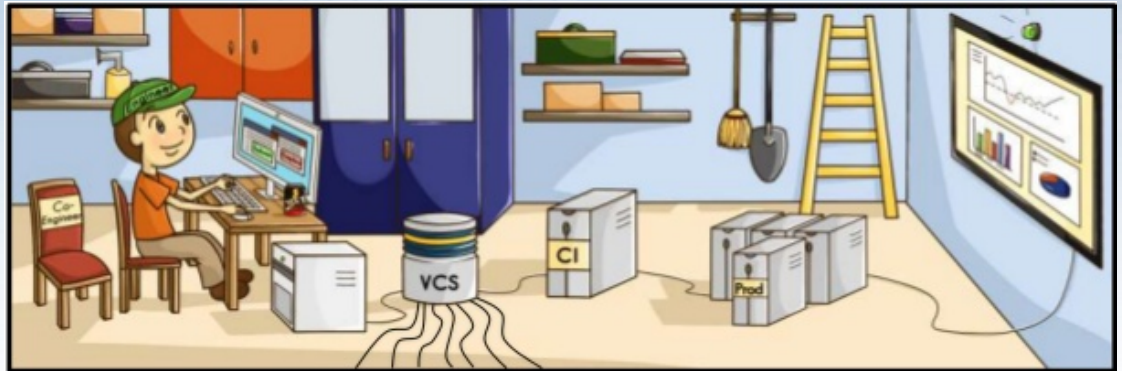




OWASP

Open Web Application
Security Project

Achieving Secure Continuous Delivery



Chris Rutter / Lucian Corlan

July 2016

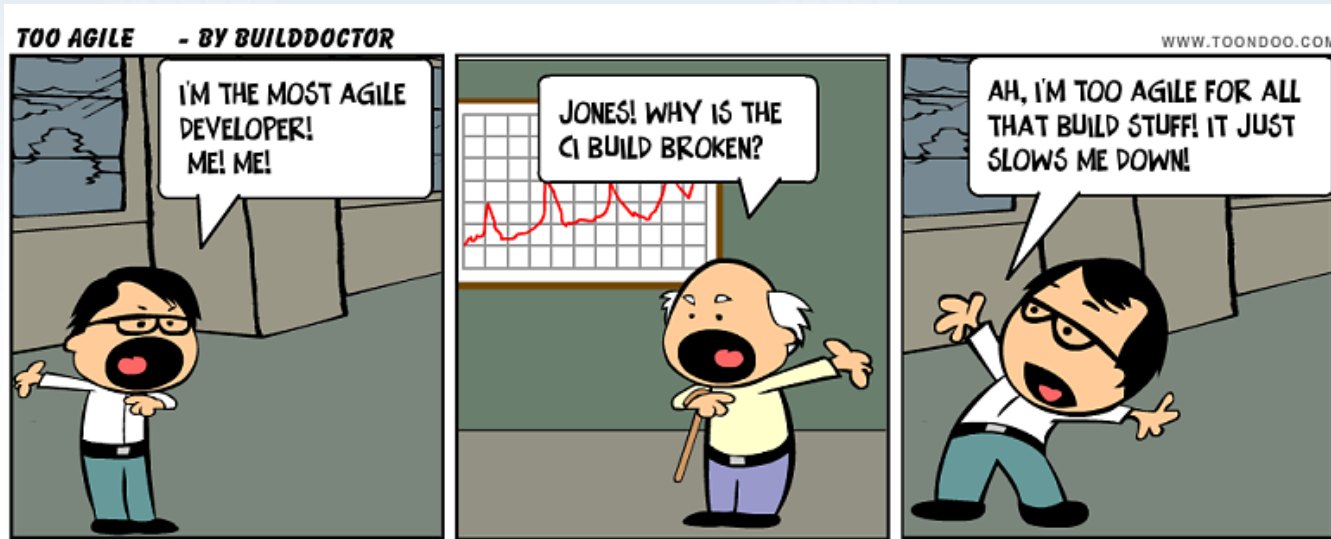
Problem statement - Security

- Difficult access to (uncorrelated) vulnerability data
- No clear view on the security risk of a specific build or release
- No real agreed security gate (no trigger threshold)
- Product has a Roadmap and Security is (always) not (always) part of it



Problem statement - Developers

- Security requirements appear when project is almost finished
- Security sign-off is a bottleneck
- When am I finally *secure enough*?



We've seen this before...

QA 5 years ago

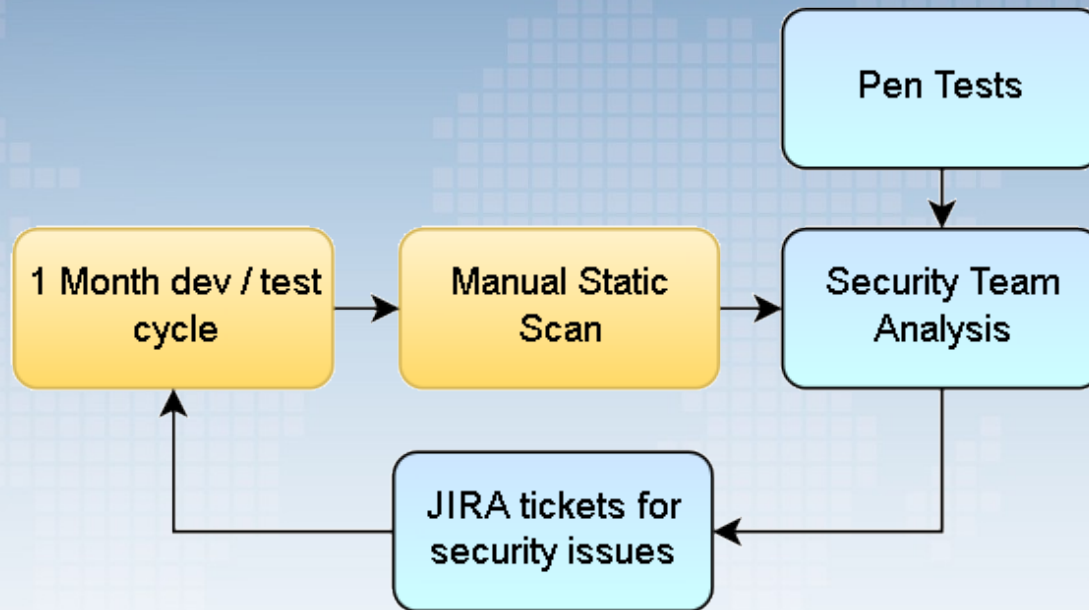
- QA manual, at the end of a project
- JIRA tickets passed around for small bugs
- Long dev / test cycles
- Key dependencies for sign-off
- Lack of overview of quality or risk

Our Goals

- Security requirements identified early
- Viewed as true non-functional requirements
- Easy to fix issues detected and fixed within a sprint
- Security quality part of definition of done each sprint
- Security policy defined and automatically applied
- Ability to measure and track all of the above



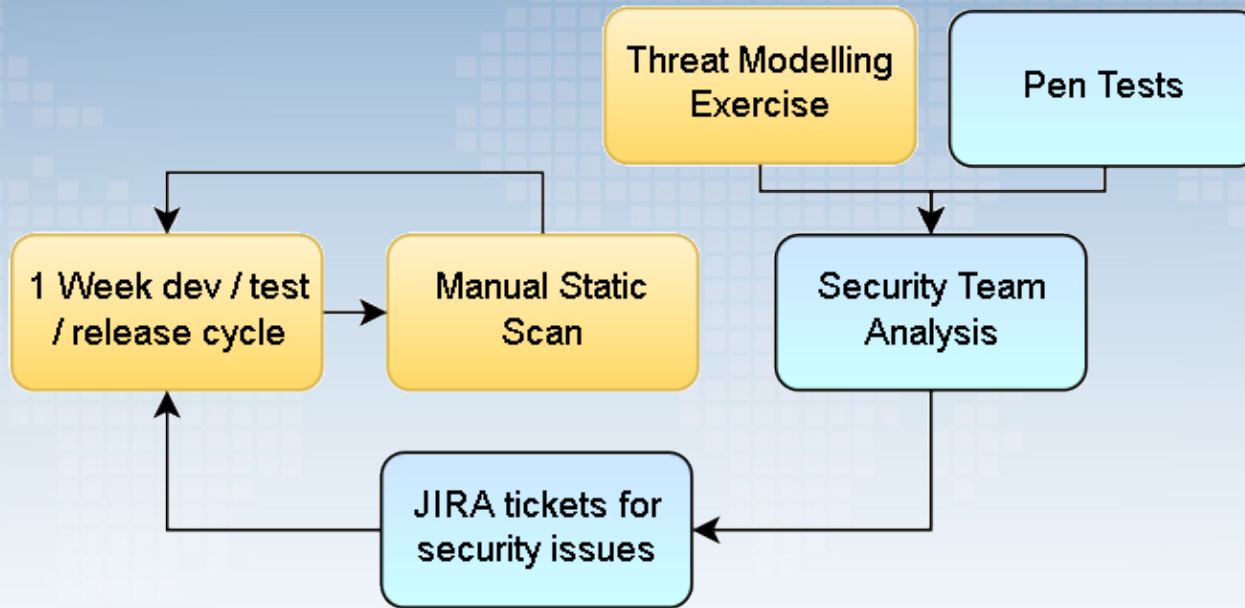
On the grid



- Pros: Security team have visibility and quality control of all testing
- Cons: Bottlenecks, Key dependencies, 1 monthly cycle, time cost, unclear sign-off criteria, manual reports / metrics



20mph

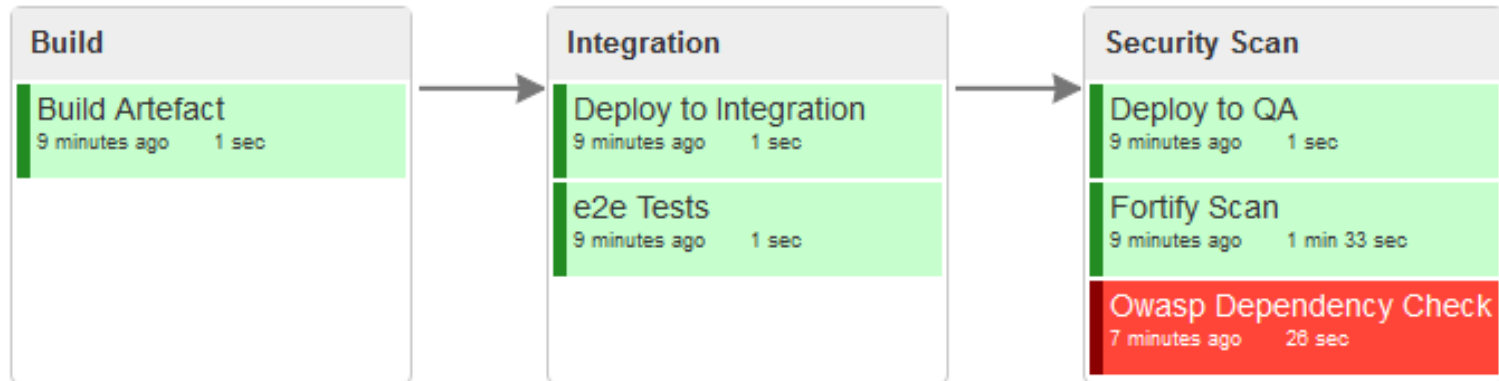


- Pros: Bottleneck reduced, High value threat modelling, shorter time to fix
- Cons: Reliance on static analysis, time consuming manual process, issues highlighted at end of sprint

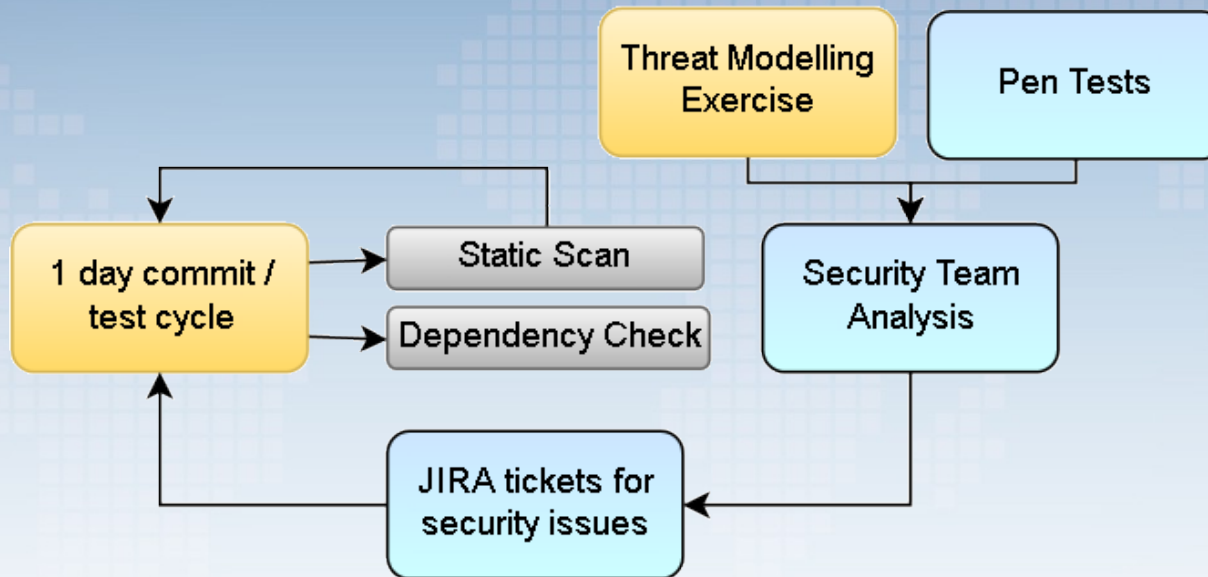


#6 triggered by user Chris Rutter started 9 minutes ago

Total build time: 2 min 5 sec



40mph



- Pros: Issues highlighted quickly, multiple types of scan, defined policy under version control.
- Cons: Custom policy effort and maintenance, difficulty analysing risk from separate reports



OWASP
Open Web Application
Security Project

Demo

LX12 Jenkins template-renderer pip... Scan History

Jenkins search Chris Rutter log out

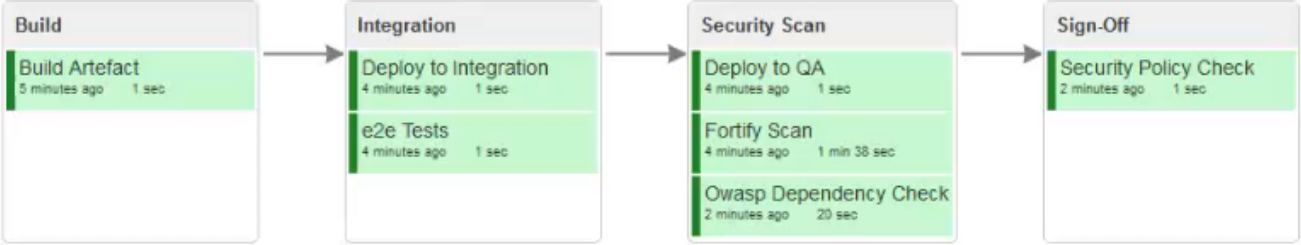
Jenkins > Auto-Security-Pipeline > [ENABLE AUTO REFRESH](#) [add description](#)

Active All **Auto-Security-Pipeline** Fortify-indigo-team Threadfix fortify test +

Auto-Security-Pipeline

#14 triggered by user Chris Rutter started 5 minutes ago

Total build time: 2 min 6 sec



```
graph LR; Build[Build] --> Integration[Integration]; Integration --> SecurityScan[Security Scan]; SecurityScan --> SignOff[Sign-Off];
```

Stage	Task	Time
Build	Build Artefact	3 minutes ago 1 sec
Integration	Deploy to Integration	4 minutes ago 1 sec
	e2e Tests	4 minutes ago 1 sec
Security Scan	Deploy to QA	4 minutes ago 1 sec
	Fortify Scan	4 minutes ago 1 min 38 sec
	Owasp Dependency Check	2 minutes ago 20 sec
Sign-Off	Security Policy Check	2 minutes ago 1 sec

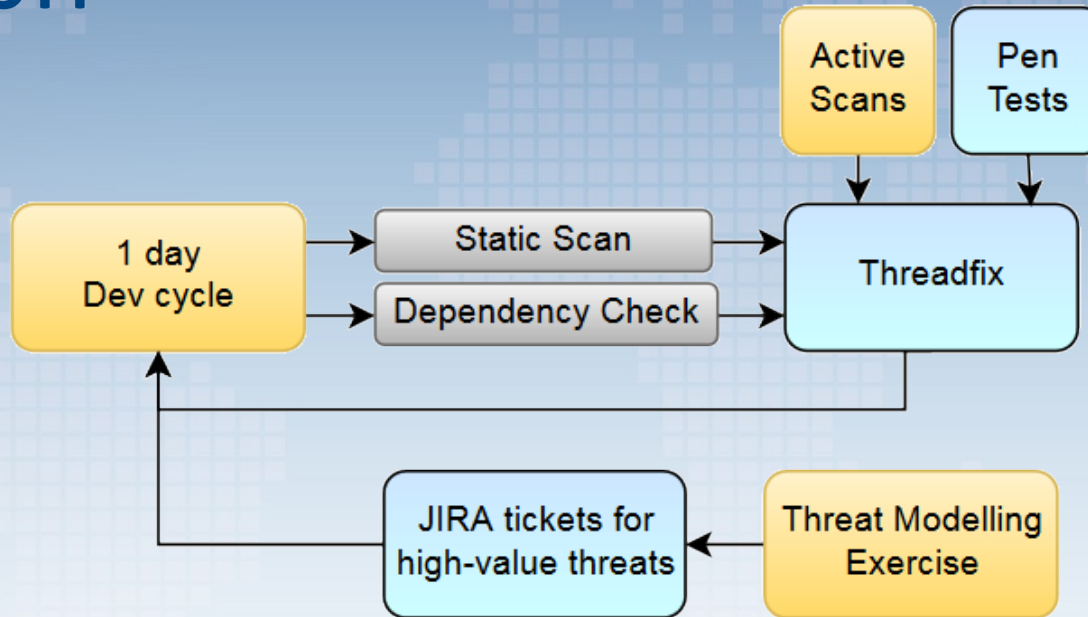
Build Queue —
No builds in the queue.

Build Executor Status —

master

- 1 Idle
- 2 Idle
- 3 Idle

60mph



- Pros: All scans & tests normalised in one place, mitigations and suppressions tracked, metrics available, devs / testers performing active scans.
- Cons: Dynamic scans manual or passive, lack of custom app attributes



YOU MAY BE COOL

**BUT YOU'LL NEVER BE LEOPARD FUR COVERED
MOTORCYCLE WITH MATCHING LEOPARD FUR
ACCENTED LEATHER JACKET COOL**

88mph

Automated dynamic scanning

- Donatello proxies e2e tests through ZAP for active scan mapping without crawling

Contextual risk policies – application passports

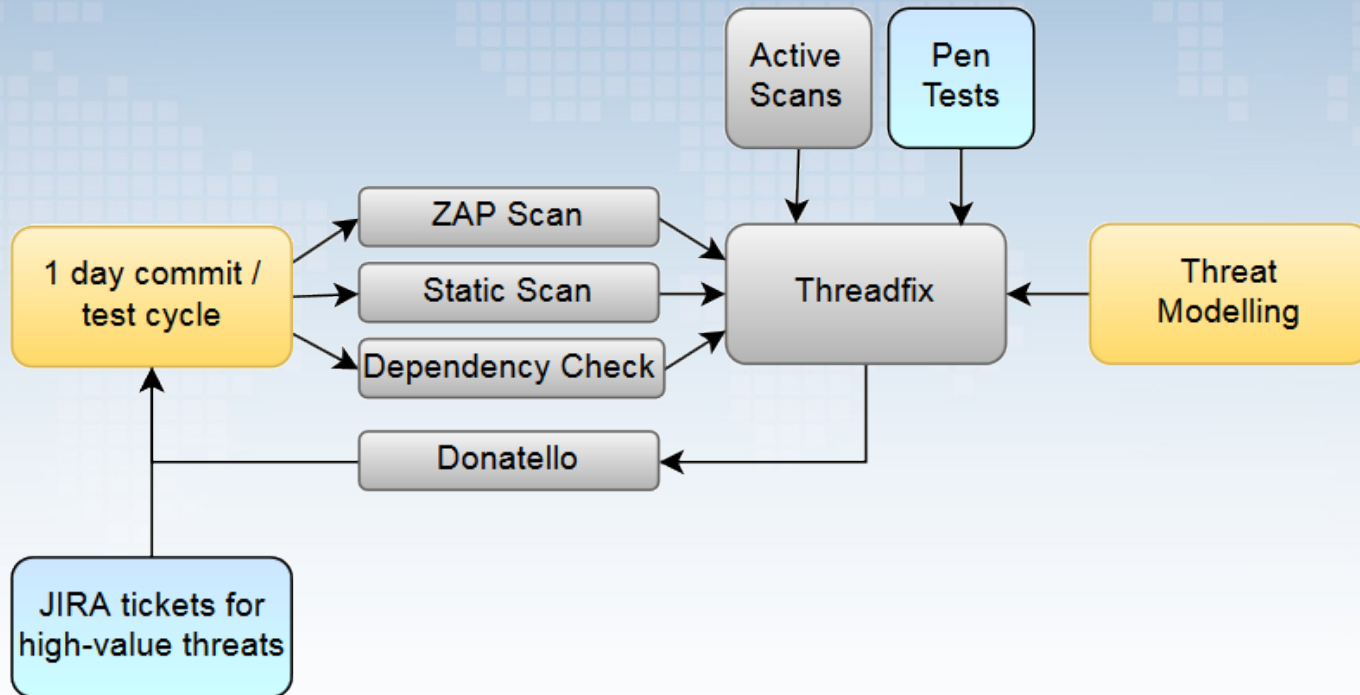
- Static & dynamic risk indicators based on Threat Modelling exercises and OWASP Top 10 and assign weight to risk indicators
- Integration with GRC tool

Contextual risk profiles

- Enhance Application criticality from ThreadFix
- static attributes
 - PCI data involved
 - PII data involved
 - Exposure
 - New service?
 - User story review
 - Input filtering
 - Output encoding
 - 3rd party integration
 - Actively maintained
 - Transported data encryption
 - Non-repudiation or IP whitelisting
 - Security meter Defcon
 - Authentication
 - Randomness level
- Dynamic attributes
 - Number of user stories since last release
 - Number of user stories since last manual pentest
 - Number of Security User Stories (outcome of Threat Modeling)



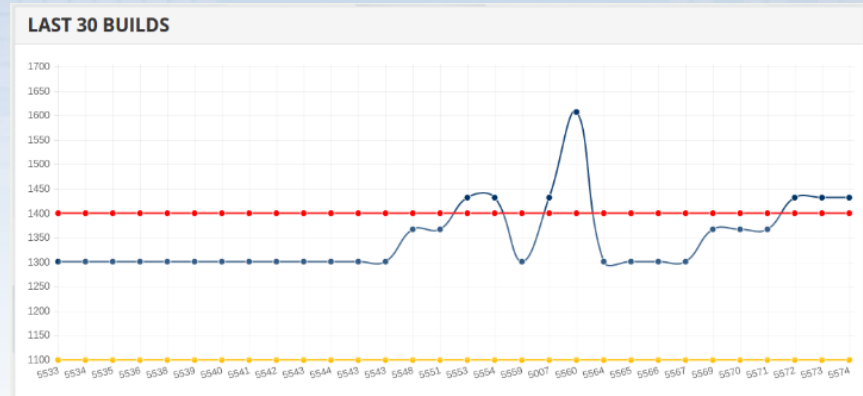
Donatello / Threadfix



Sources of inspiration

- Betfair Security solution & DevSecCon
- Proprietary API (python or node.js) hooking into all the tools, plus static attributes and interpretation of results per application in Gitlab
- Job in the continuous delivery tool to run the calculation (per build)
- Dashboard for metrics

COMMIT	QA_DEPLOY	QA_TEST	NXT	SECURITY	COMMENTS
BUILD: 5360 27 Jan, 21:18:29 SCR: US99161 - Improved logging (updated mediation version)	21:21:58	21:32:18		PASS: 864 0 0	Ok
BUILD: 5359 27 Jan, 18:41:30 SCR: n/a fixing component tests	18:46:50	19:30:59		PASS: 864 0 0	Ok
BUILD: 5358 27 Jan, 14:51:30 SCR: US99326 - Added default value (false) on bean definition for isStorageNode property.	14:56:54	18:11:49		PASS: 864 0 0	Error: http://jenkins-QA/279/
BUILD: 5357 27 Jan, 14:36:31 SCR: US99326 added support for null values	14:42:00			PASS: 864	Ok



#	Application	Inherent-Risk-Score	Avoidable-Risk-Score	Risk Score	Risk-Threshold-Warning	Risk-Threshold-Error
7		625	996	1621	1400	1700
1		292	597	889	700	900
5		209	1223	1432	1100	1400
6		115	747	862	600	800
3		34	843	877	600	800
2		10	578	578	450	550
4		10	210	210	300	450



Q



OWASP
Open Web Application
Security Project