VELATEK
Your Confidence. Our Quality.

RISK MANAGEMENT IN SOFTWARE DEVELOPMENT: SECURITY & STABILITY

MSc. Pho Duc Giang, CISSP

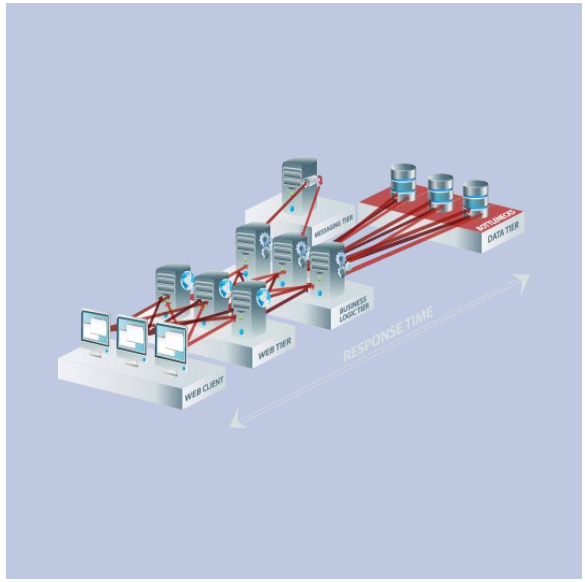

giang.pho@velatek.vn


84-986 727 355

Software ở khắp nơi!

Thách thức về an ninh **Cloud** –Code Space mới bị xâm nhập năm 2014!

Xu hướng sử dụng thiết bị di động thông minh (**Mobile**). Công nghệ mới, tạo thêm cửa ngõ mới cho kẻ tấn công xâm nhập hệ thống!



Websites và các ứng dụng web vẫn là kênh kết nối chủ đạo với KH. An ninh ứng dụng web ngày càng phức tạp!

Websites hacked (2012)

© 2012 WhiteHat Security, Inc.

Trong năm 2012-2013, Bộ Công an đã phát hiện gần 6.000 lượt cổng thông tin, trang tin điện tử của Việt Nam (trong đó có hơn 300 trang của cơ quan nhà nước) bị tấn công, chỉnh sửa nội dung và cài mã độc.

[220 website của Việt Nam đã bị "hacker Trung Quốc" tấn công]

Riêng năm 2014, Bộ Công an phát hiện gần 6.000 trang bị tấn công, chiếm quyền quản trị, chỉnh sửa nội dung (có 246 trang tên miền gov.vn). Đặc biệt, sau sự kiện giàn khoan HD 981 hạ đặt trái phép trong vùng đặc quyền kinh tế Việt Nam, tin tặc nước ngoài đã tấn công hơn 700 trang mạng Việt Nam và hơn 400 trang trong dịp Quốc khánh (2/9) để chèn các nội dung xuyên tạc chủ quyền của Việt Nam với quần đảo Hoàng Sa.

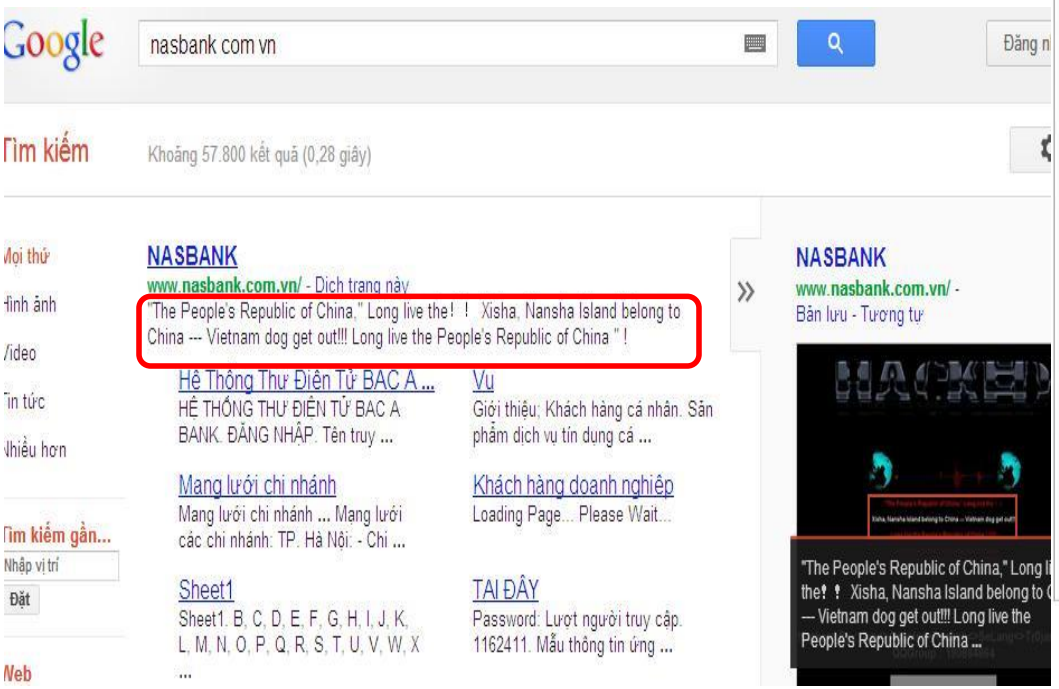
Trang web của Techcombank bị hack

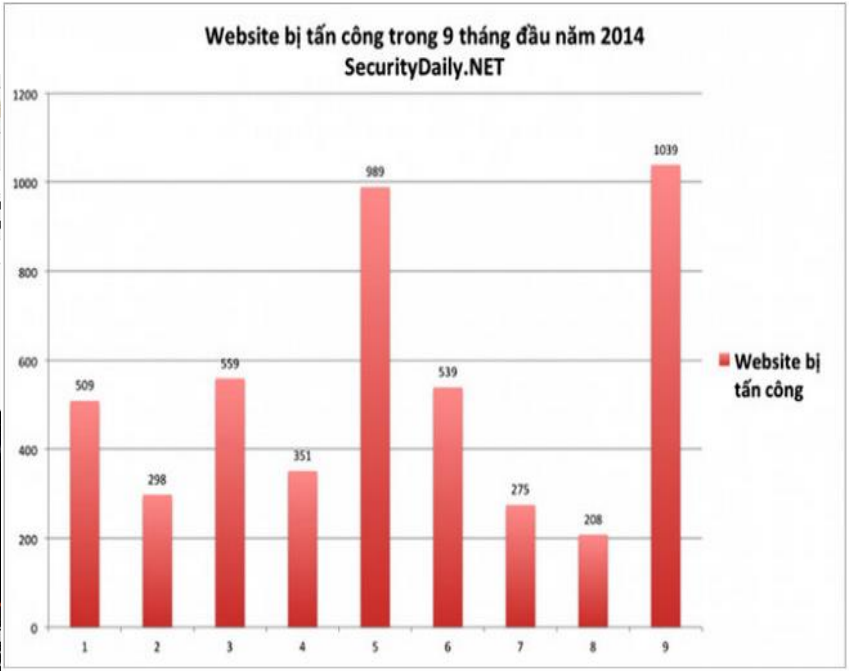
Cập nhật lúc 16:18, Thứ Sáu, 25/07/2008 (GMT+7)

- Tối ngày 24/7, trang Web của Ngân hàng Kỹ thương Việt Nam - Techcombank - tại địa chỉ http://techcombank.com.vn đã bị hacker tấn công và để lại thông điệp cảnh báo lỗi ở một trang web bên trong.

1.000 website Việt Nam bị tấn công trong 2 ngày cuối tháng 5

★ BẢO MẬT 21:20, 01/06/2015





Các CIO đang đối mặt với nhiều thách thức về an ninh mạng

BẢO MẬT 11:03, 25/03/2015

Thích Chia sẻ 21 g+1 0 Giúp ICTNEWS sửa lỗi

ICTnews - Theo Phó Tổng Cục trưởng Tổng Cục An ninh (Bộ Công an) Trần Văn Thành, trong bối cảnh an toàn, an ninh thông tin đã trở thành yếu tố vô cùng quan trọng thì thách thức dành cho các lãnh đạo CNTT (CIO) và lãnh đạo về an ninh thông tin thời gian tới hết sức nặng nề.

Số liệu từ VNCERT năm 2014

19.789 sự cố gồm các loại sự cố tấn công lừa đảo, tấn công thay đổi giao diện và tấn công cài mã độc lên website.... 1.458 sự cố tấn công lừa đảo, tăng 179% so với năm ngoái. VNCERT đã gửi yêu cầu điều phối và xử lý được 1.138 sự cố (tăng 145% so với năm 2013). 10.037 sự cố tấn công cài mã độc lên website, đã gửi yêu cầu điều phối và xử lý 5.976 sự cố, trong đó có 20 sự cố liên quan đến tên miền .gov.vn. 8.291 sự cố tấn công thay đổi giao diện (tăng 406% so với năm 2013), trong đó có 274 sự cố liên quan đến tên miền .gov.vn, đã gửi yêu cầu điều phối và xử lý 4.493 sự cố.

An toàn thông tin 16:07 | 19/12/2014

Gắn kết chiến lược An toàn thông tin với các mục tiêu tăng trưởng và phát triển

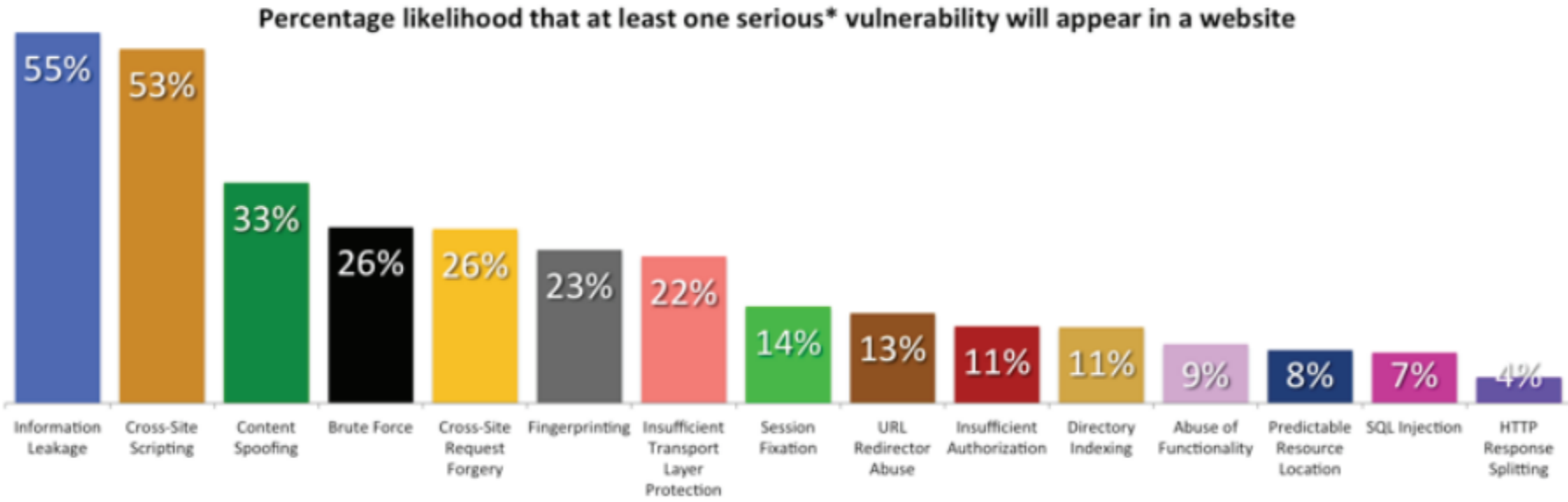
Những sự cố về mất an ninh thông tin vẫn có chiều hướng gia tăng và đi cùng với nó là các hệ lụy từ việc cơ sở dữ liệu và hạ tầng thông tin của doanh nghiệp bị tấn công. Việc đầu tư cho bảo mật thông tin đảm bảo tính hiệu quả, giúp doanh nghiệp phát triển luôn là câu hỏi khó đối với các nhà quản trị doanh nghiệp.

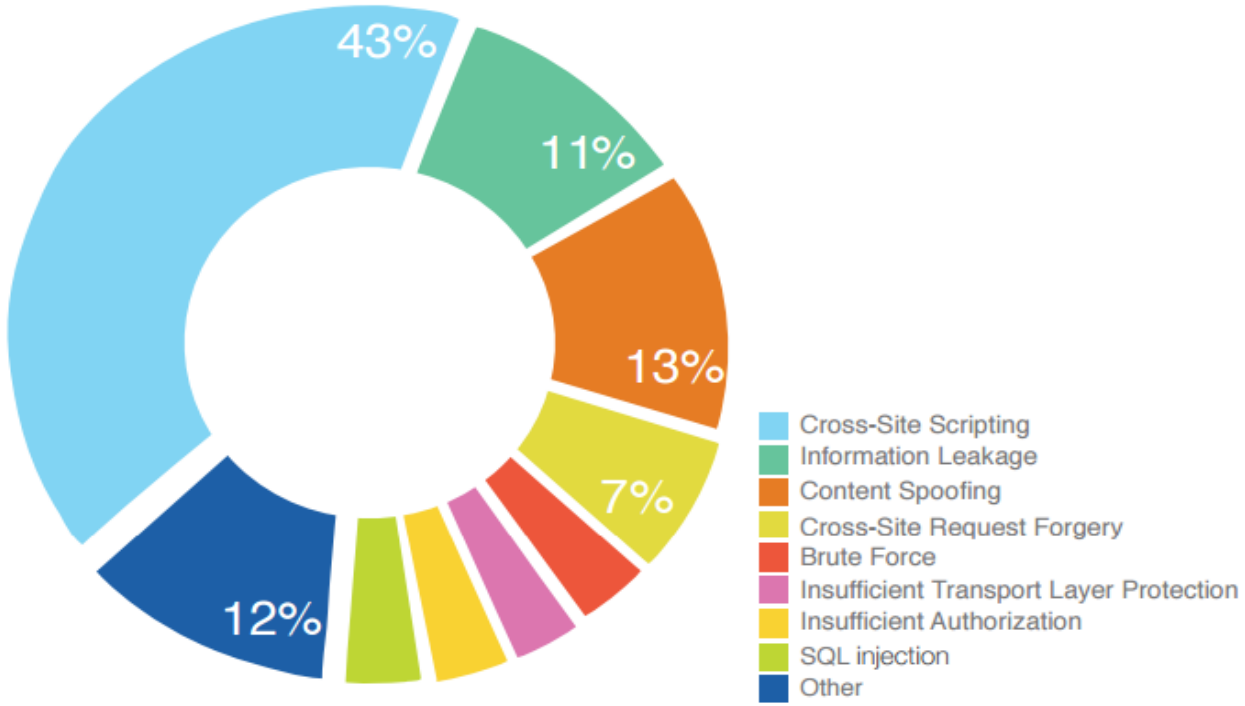
Total notifications: **27,826** of which **8,200** single ip and **19,626** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2015/06/12	PaWL		M				azwedding.vn/zxcbincx.php	Linux	mirror
2015/06/12	PaWL		M				neopham.com.vn/zxcbincx.php	Linux	mirror
2015/06/11	Index Php						vnglaw.vn/wp-admin/admin-ajax....	Linux	mirror
2015/06/11	Python	H	M				diaocinfo.vn	Linux	mirror
2015/06/11	Yheya Alshami			R		★	hungyenbusiness.gov.vn/Default...	Win 2003	mirror
2015/06/11	Yheya Alshami			R		★	qh-hdqna.gov.vn/Default.aspx?t...	Win 2008	mirror
2015/06/11	Zenvoz ID						www.saigoncc.com.vn/scc/	Unknown	mirror
2015/06/11	EvLaT_	H				★	dongvan.gov.vn	Linux	mirror
2015/06/11	Wisnu404		M	R		★	khuqldb7.gov.vn/nca.htm	Win 2003	mirror
2015/06/11	Index Php						www.nextbuild.vn/wp-admin/admi...	Linux	mirror
2015/06/11	Index Php						www.tachu.com.vn/indonesia.php	Linux	mirror
2015/06/11	Index Php						motorbiketoursvietnam.com.vn/i...	Win 2008	mirror
2015/06/10	SlayersHackTeam		M			★	tayho.hanoi.gov.vn/image/slaye...	Win 2008	mirror
2015/06/10	SlayersHackTeam		M			★	socson.hanoi.gov.vn/image/slay...	Win 2008	mirror
2015/06/10	SlayersHackTeam		M	R		★	tayho.gov.vn/image/slayers.txt	Win 2008	mirror
2015/06/10	SlayersHackTeam					★	sonnptnt.hanoi.gov.vn/image/sl...	Win 2008	mirror
2015/06/10	EvLaT_	H	M				trivietcenter.vn	Linux	mirror
2015/06/10	4ng3lz Team	H					ansinhviet.com.vn	Linux	mirror
2015/06/10	./MrJ		M				tophome.com.vn/owned-c3a226.html	Linux	mirror
2015/06/09	Phénoméne Dz	H	M				www.kimsonlau.vn	Linux	mirror
2015/06/09	Phénoméne Dz	H					www.maccoffee.vn	Linux	mirror
2015/06/09	Index Php						dogotruongthanh.com.vn/wp-admi...	Linux	mirror
2015/06/09	ZoRRoKiN		M				www.tienganhgiaotiep.vn/23_nis...	Linux	mirror
2015/06/09	ali attacker	H	M				music.mix.vn	Win 2003	mirror
2015/06/09	d3b~X		M				haihuonghotel.vn/wow.htm	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


Percentage likelihood that at least one serious* vulnerability will appear in a website
55%
53%
33%
26%
26%
23%
22%
14%
13%
11%
11%
9%
8%
7%
4%
Information Leakage
Cross-Site Scripting
Content Spoofing
Brute Force
Cross-Site Request Forgery
Fingerprinting
Insufficient Transport Layer Protection
Session Fixation
URL Redirector Abuse
Insufficient Authorization
Directory Indexing
Abuse of Functionality
Predictable Resource Location
SQL Injection
HTTP Response Splitting


43%
11%
13%
7%
12%
Cross-Site Scripting
Information Leakage
Content Spoofing
Cross-Site Request Forgery
Brute Force
Insufficient Transport Layer Protection
Insufficient Authorization
SQL injection
Other

WhiteHat SECURITY

Banking Industry Scorecard

April 2013

AT A GLANCE

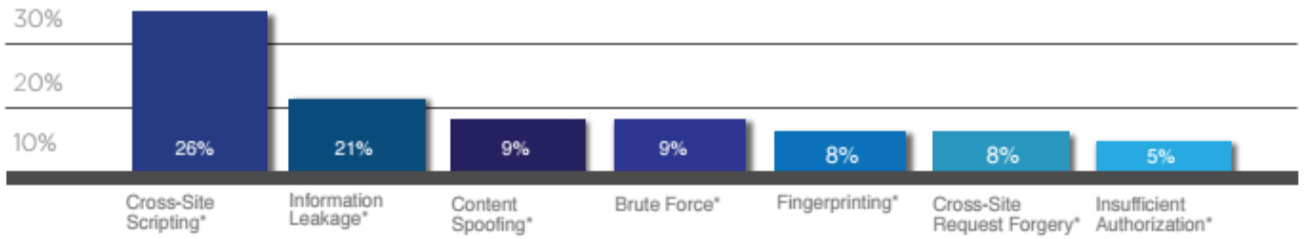
THE CURRENT STATE OF WEBSITE SECURITY

PERCENT OF ANALYZED SITES WITH A SERIOUS* VULNERABILITY	AVERAGE NUMBER OF SERIOUS* VULNERABILITIES PER SITE PER YEAR	PERCENT OF SERIOUS* VULNERABILITIES THAT HAVE BEEN FIXED	AVERAGE TIME TO FIX
81%	11	54%	107 DAYS

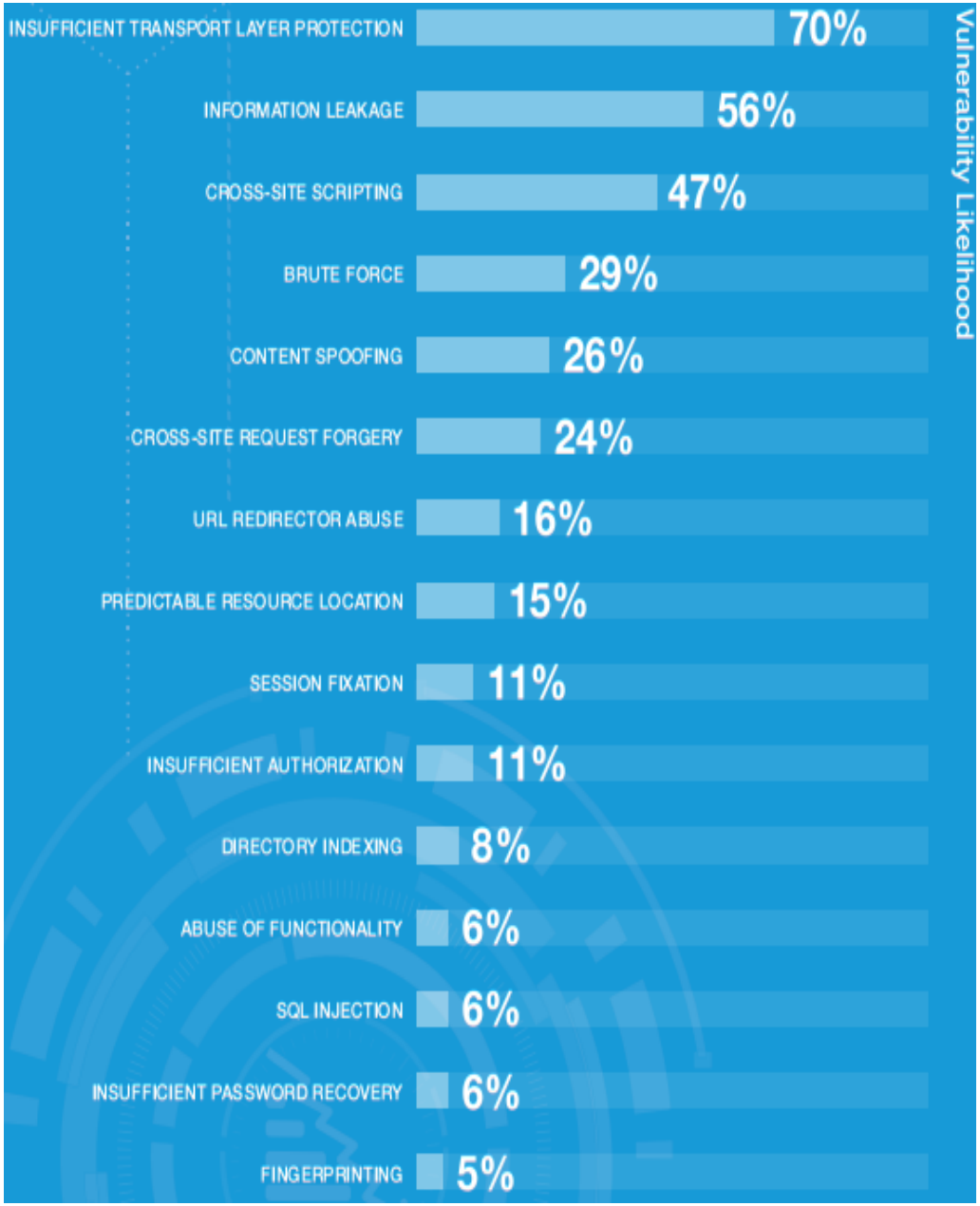
*Serious vulnerabilities are defined as those in which an attacker could take control over all, or a part, of a website, compromise user accounts, access sensitive data or violate compliance requirements.

MOST COMMON VULNERABILITIES

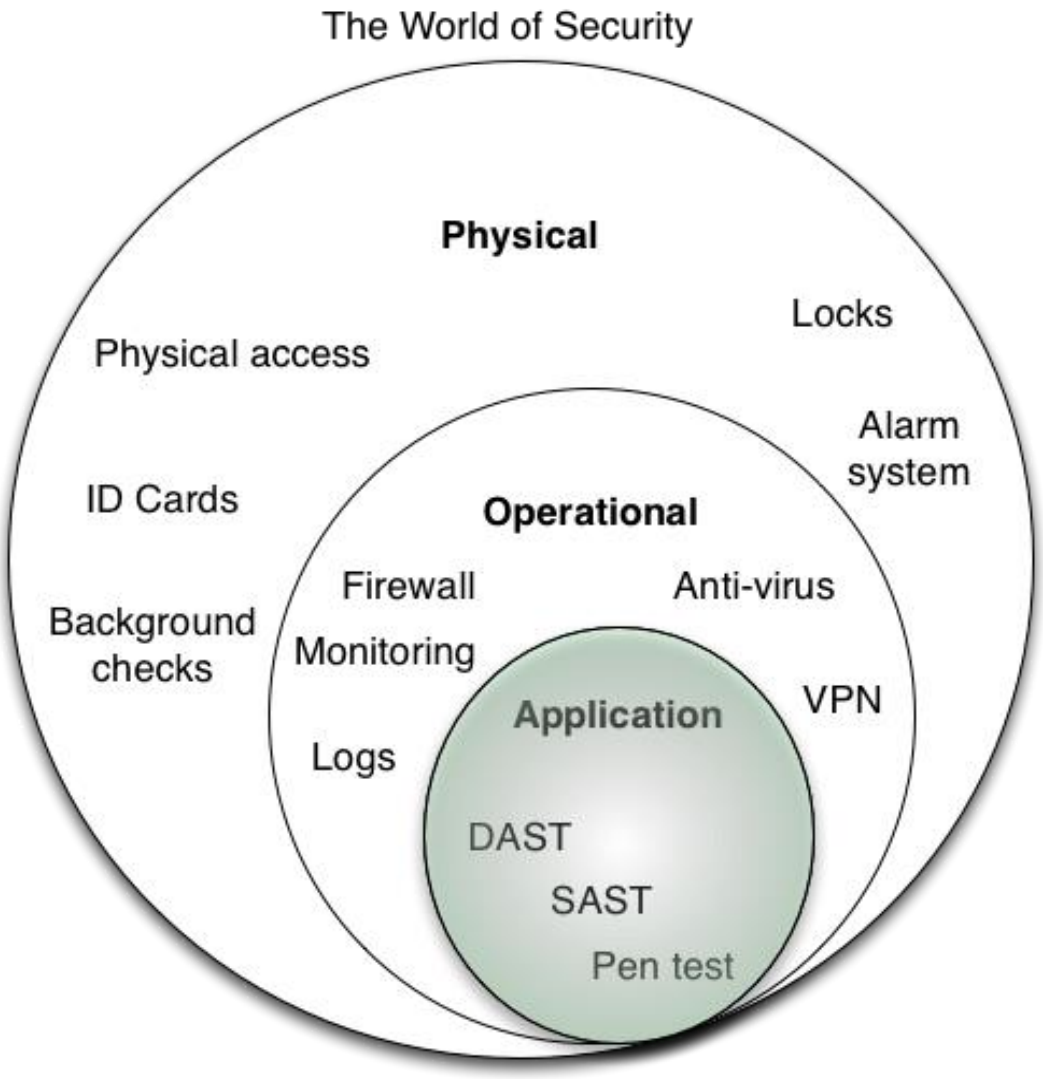
TOP SEVEN VULNERABILITY CLASSES



*The percent of sites that had at least one example of...


Vulnerability Likelihood
INSUFFICIENT TRANSPORT LAYER PROTECTION 70%
INFORMATION LEAKAGE 56%
CROSS-SITE SCRIPTING 47%
BRUTE FORCE 29%
CONTENT SPOOFING 26%
CROSS-SITE REQUEST FORGERY 24%
URL REDIRECTOR ABUSE 16%
PREDICTABLE RESOURCE LOCATION 15%
SESSION FIXATION 11%
INSUFFICIENT AUTHORIZATION 11%
DIRECTORY INDEXING 8%
ABUSE OF FUNCTIONALITY 6%
SQL INJECTION 6%
INSUFFICIENT PASSWORD RECOVERY 6%
FINGERPRINTING 5%

An ninh ứng dụng



Sự cần thiết an ninh ứng dụng

- Chi phí liên quan lỗ hổng an ninh phần mềm
  - Chi phí kiểm tra, đánh giá, đào tạo;
  - Chi phí phát triển bản vá lỗi;
  - Chi phí quản lý, kiểm thử, đóng gói bản vá lỗi;
  - Chi phí thông báo vá lỗi và hỗ trợ bảo hành;
  - Chi phí về hình ảnh, danh tiếng.
- **76%** trong **200** ngân hàng được khảo sát đều có ít nhất 1 ứng dụng tồn tại lỗ hổng an ninh (ĐH Michigan, Hoa Kỳ)
- Chi phí để phát hiện và khắc phục lỗ hổng an ninh ứng dụng ngay trong giai đoạn phát triển (design & development) rẻ hơn **7 lần** trước khi đưa vào triển khai (implementation) và rẻ hơn **100 lần** khi golive (IBM System Sciences Institute)

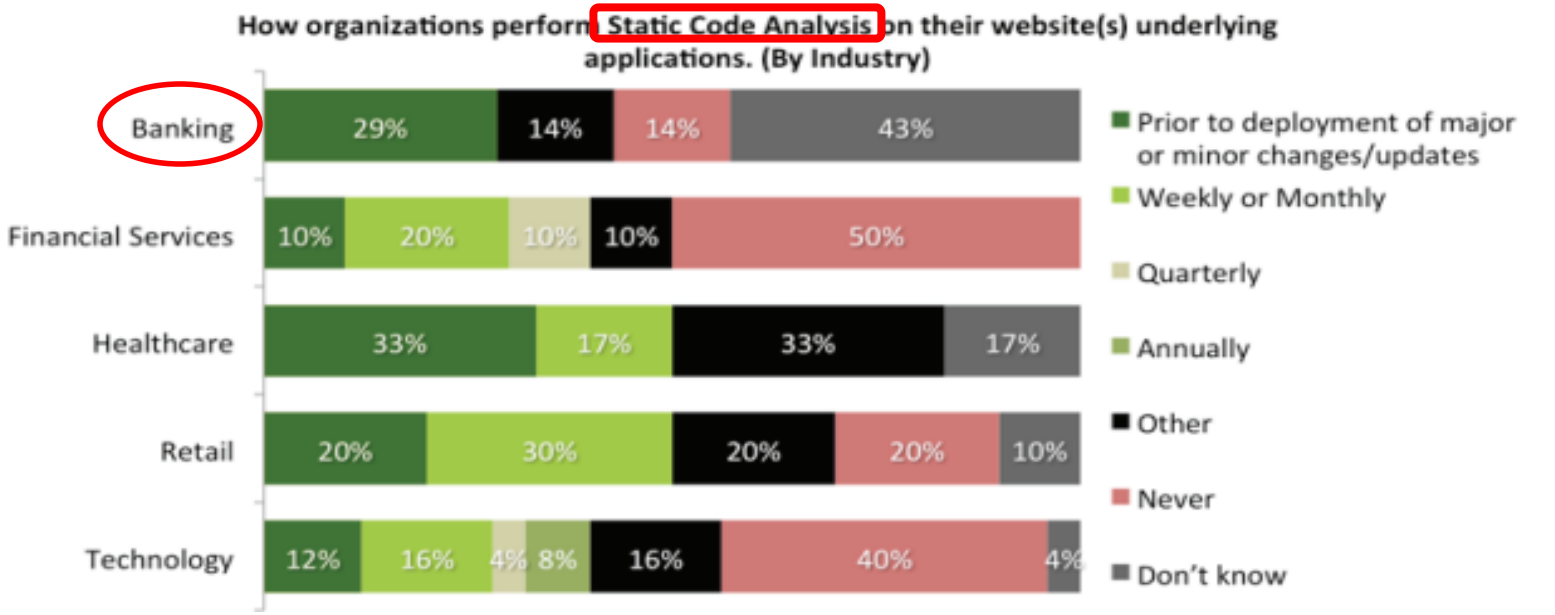
Sự cần thiết an ninh ứng dụng

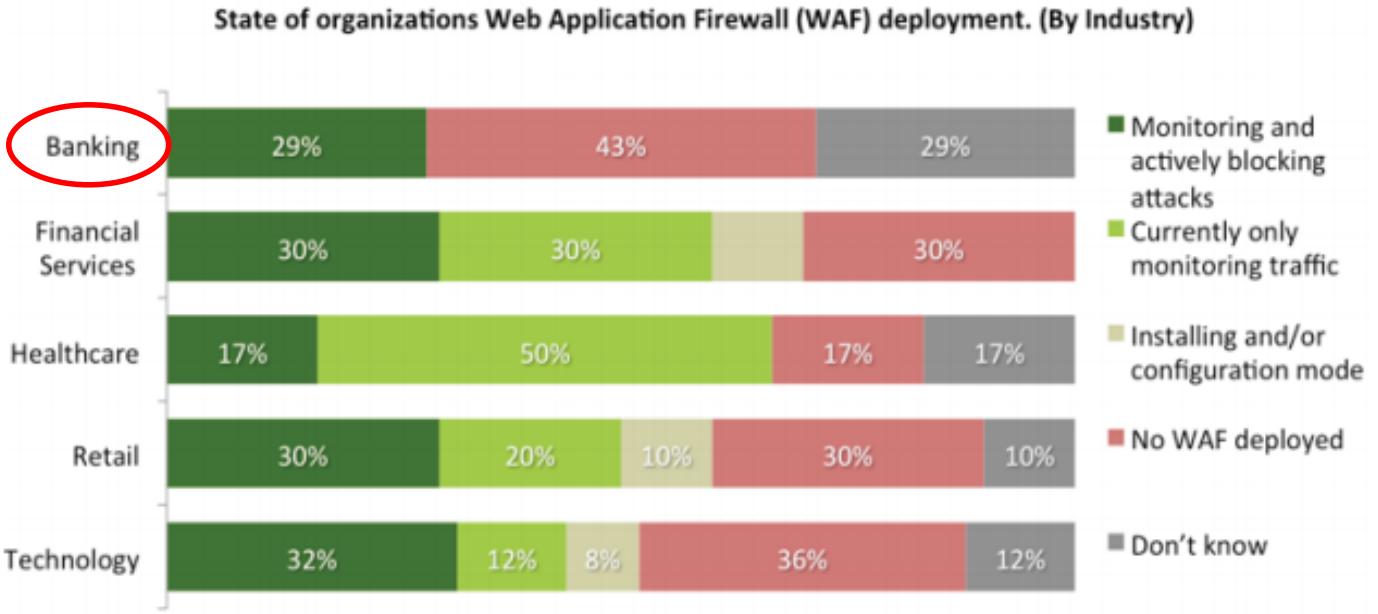
"If only 50 percent of software vulnerabilities were removed prior to production … costs would be reduced by 75 percent"
- *Gartner "Security at the Application Level"*

"64 percent of developers are not confident in their ability to write secure applications" - *Microsoft Developer Research*

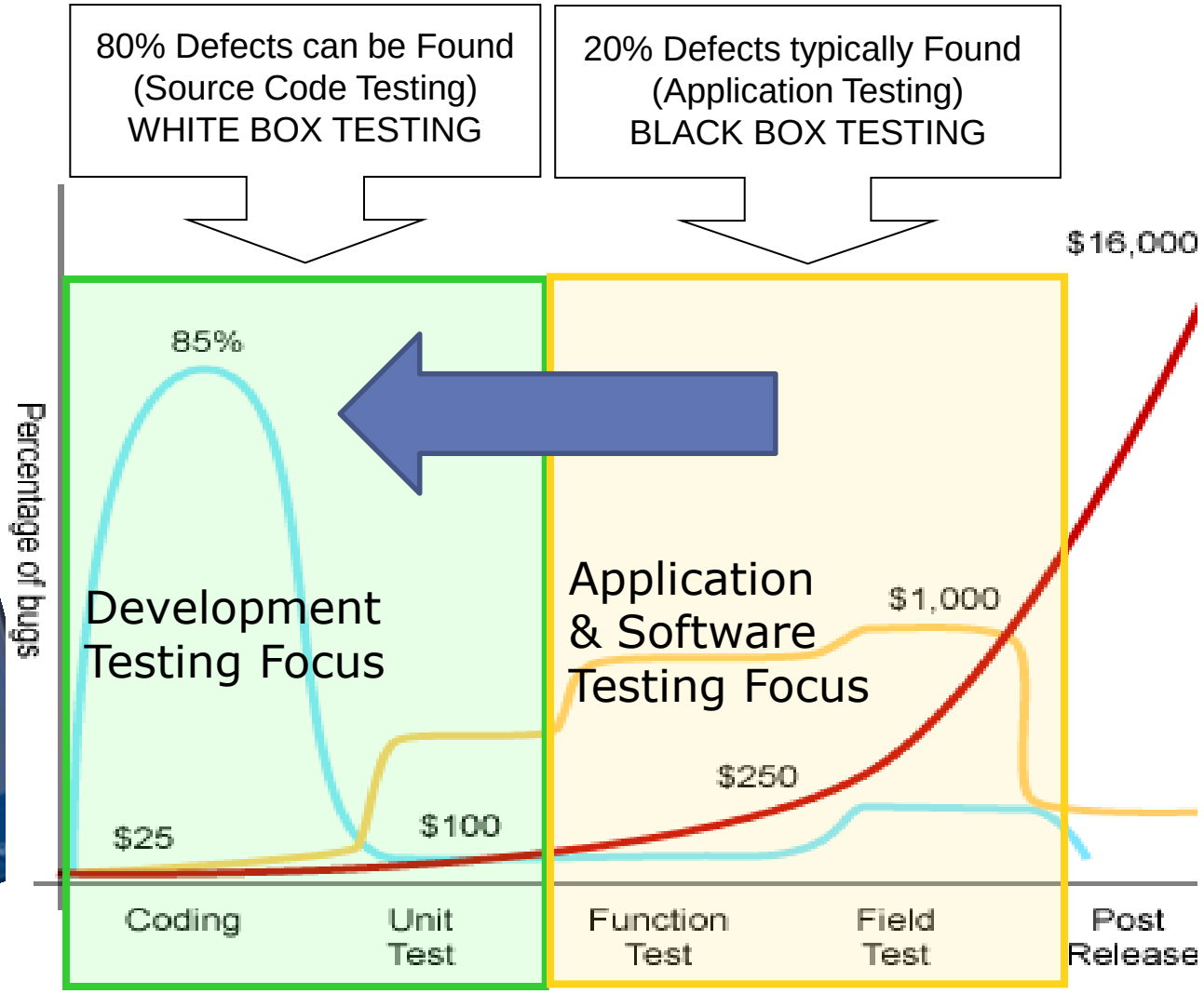
Developers are under pressure to launch applications faster so code integrity is sometimes sacrificed. Very few companies have a thorough secure development life cycle to regularly check for security flaws [VeraCode]

"The biggest mistake people make is that they underestimate the threat," [Moss – Def Con Founder]


How organizations perform Static Code Analysis on their website(s) underlying applications. (By Industry)
Banking
Financial Services
Healthcare
Retail
Technology
29%
14%
14%
43%
10%
20%
10%
10%
50%
33%
17%
33%
17%
20%
30%
20%
20%
10%
12%
16%
4%
8%
16%
40%
4%
Prior to deployment of major or minor changes/updates
Weekly or Monthly
Quarterly
Annually
Other
Never
Don't know


State of organizations Web Application Firewall (WAF) deployment. (By Industry)
Banking
Financial Services
Healthcare
Retail
Technology
29%
43%
29%
30%
30%
30%
17%
50%
17%
17%
30%
20%
10%
30%
10%
32%
12%
8%
36%
12%
Monitoring and actively blocking attacks
Currently only monitoring traffic
Installing and/or configuration mode
No WAF deployed
Don't know

Quản lý rủi ro trong phát triển phần mềm



Source: Applied Software Measurement, Capers Jones, 1996

Giảm thiểu rủi ro

Governance

Coding Guidelines, Security Test Requirements, ALM (App Lifecyce Management)

Monitoring

Requirements Management, Code Analysis & Review, Functional & Load Testing

Compliance

Industry, Company, Project

Enforcement

Carrot or Stick?

Chuẩn mực lập trình an toàn!

PCI DSS

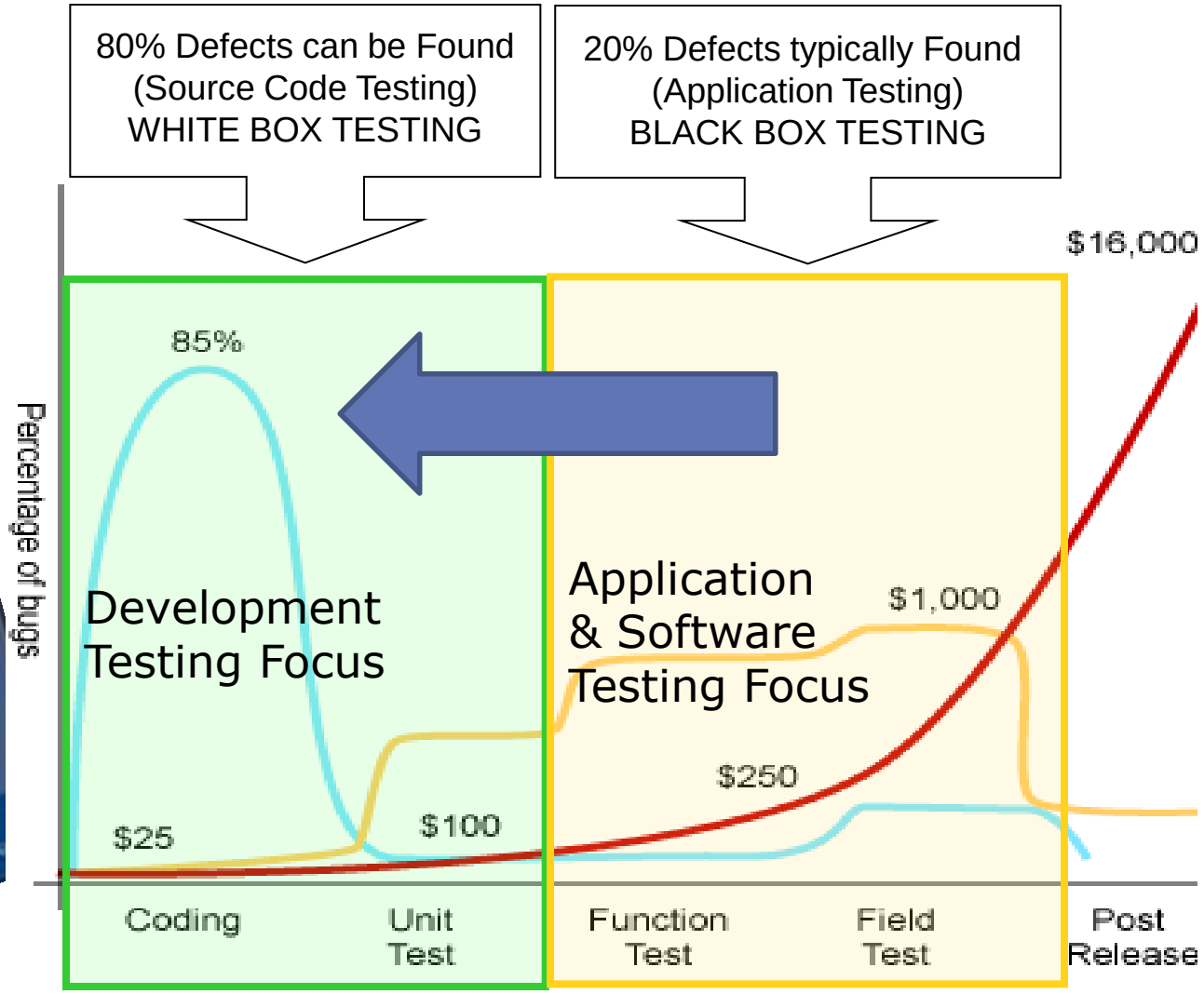
OWASP

CWE/SANS

NIST SAMATE

Customize/Company Security Rules

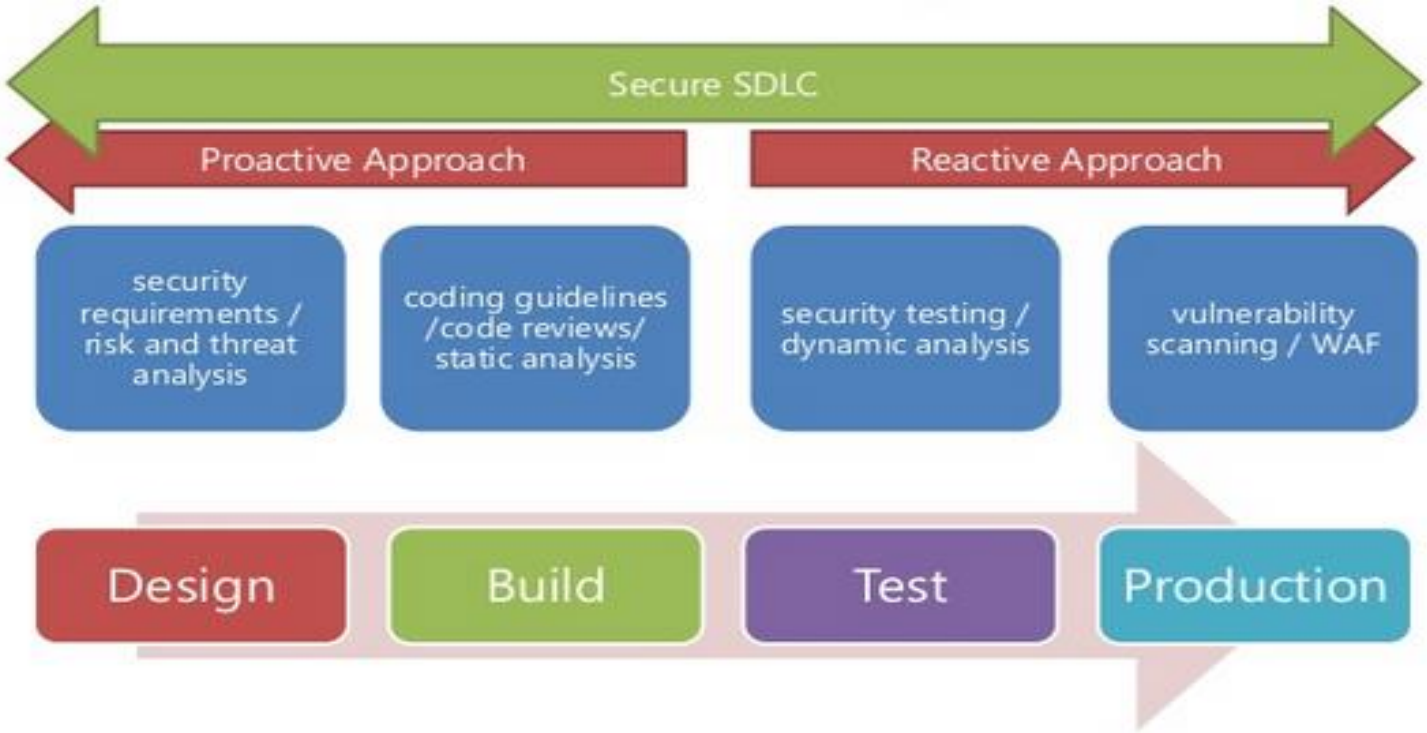
Quản lý rủi ro trong phát triển phần mềm

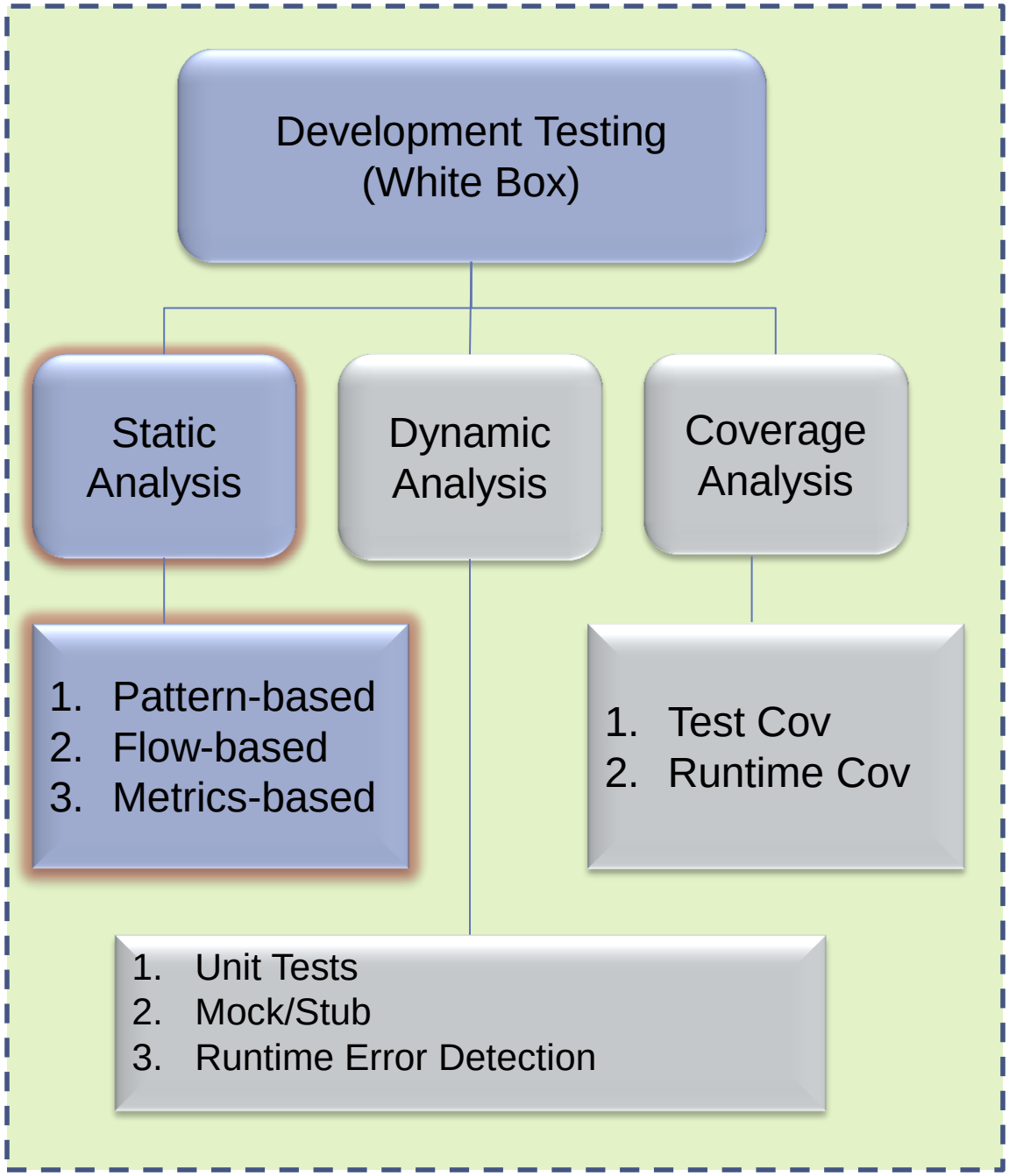


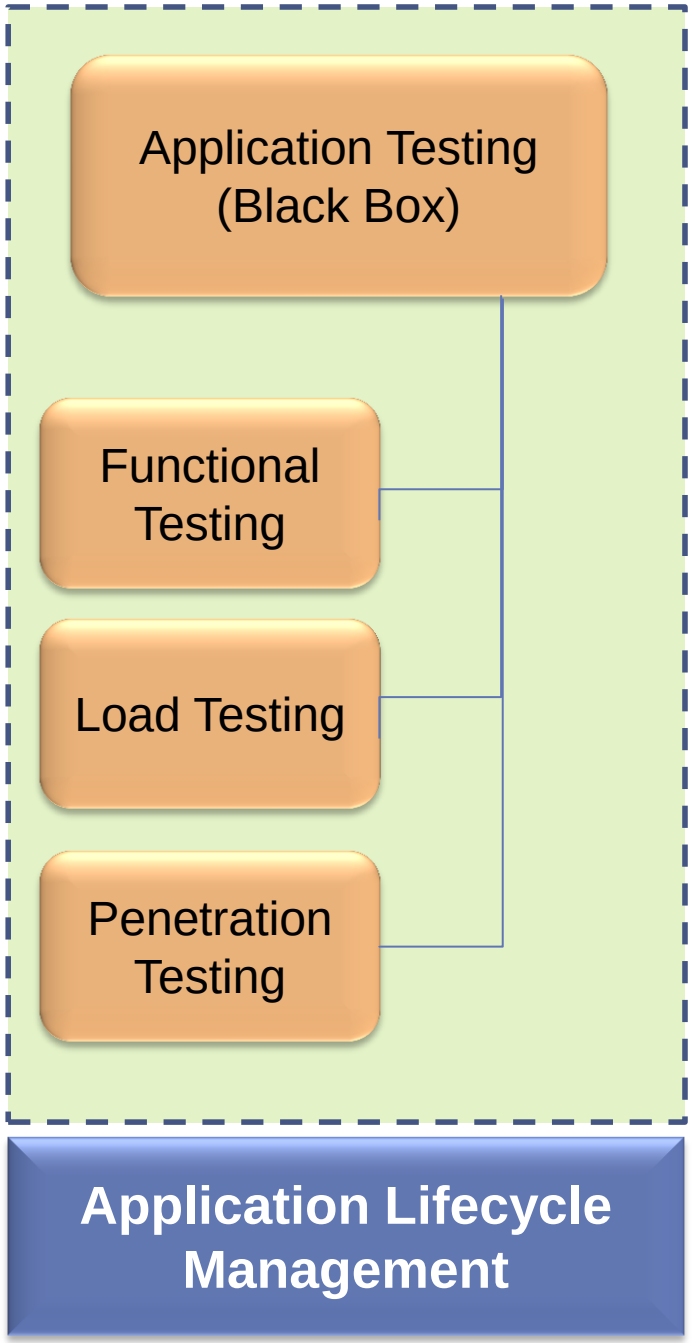
Source: Applied Software Measurement, Capers Jones, 1996

Quản lý rủi ro trong phát triển phần mềm

- Quy trình đề xuất (Secure Software Development Life Cycle)




Development Testing
(White Box)
Static
Analysis
Dynamic
Analysis
Coverage
Analysis
1. Pattern-based
2. Flow-based
3. Metrics-based
1. Test Cov
2. Runtime Cov
1. Unit Tests
2. Mock/Stub
3. Runtime Error Detection


Application Testing
(Black Box)
Functional
Testing
Load Testing
Penetration
Testing
Application Lifecycle
Management

Lợi ích

- Thiết lập được sự kỳ vọng của BLĐ
  - Lập trình viên hiểu được cần phải làm gì và được yêu cầu phải làm gì để góp phần gia tăng sự an toàn cho các phần mềm.
- Nâng cao kiến thức
  - Lập trình viên có thể cải thiện chất lượng và tính an toàn ổn định cho các phần mềm thông qua hoạt động hàng ngày.
- Nâng cao tính tuân thủ chuẩn mực lập trình an toàn
- Nâng cao sự tin cậy, tín nhiệm trong nội bộ và bên ngoài
  - Nội bộ: các ứng dụng tin cậy và an toàn hơn.
  - Bên ngoài: đối tác, khách hàng hài lòng hơn về chất lượng sản phẩm dịch vụ cung cấp.

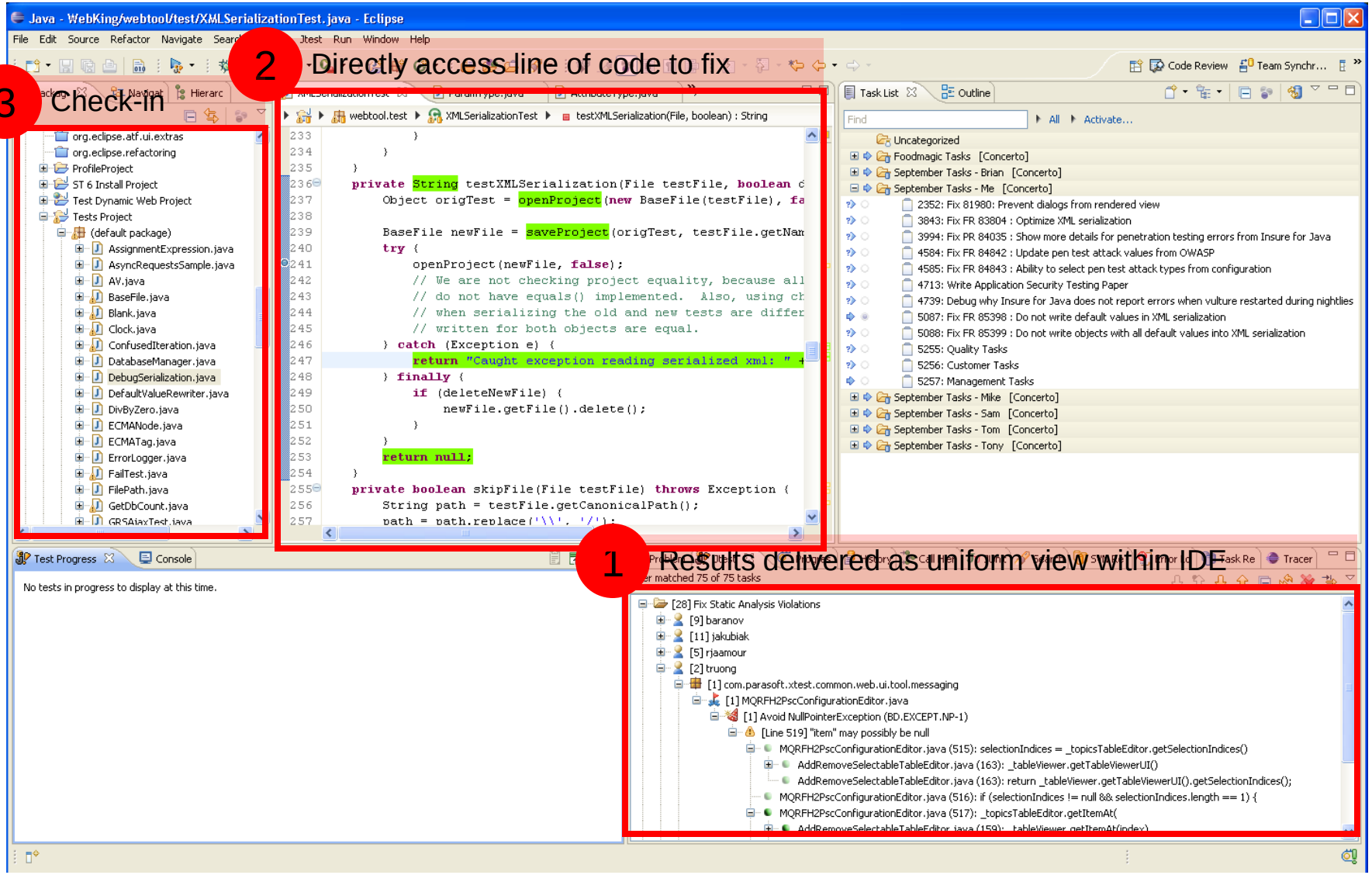
Các giải pháp kiểm soát an ninh mã nguồn

Microsoft .net

C/C++

Java

Kết quả trực quan trên IDE



PARASOFT. Jtest® Report

11/27/13 18:47:21	Results from: **PCI Data Security Standard (Server Configuration)**

STATIC ANALYSIS

Project Name	Tasks				Files		Lines	
	suppressed	qfix	total	per 10,000 lines	checked	total	checked	total
.jsp.test.project.Jtest Example	0	0	0	0	0	2	0	0
Jtest Example	0	17	137	202	125	125	6768	6768
Total [0:01:36]	**0**	**17**	**137**	**202**	**125**	**127**	**6768**	**6768**

All Tasks by Category

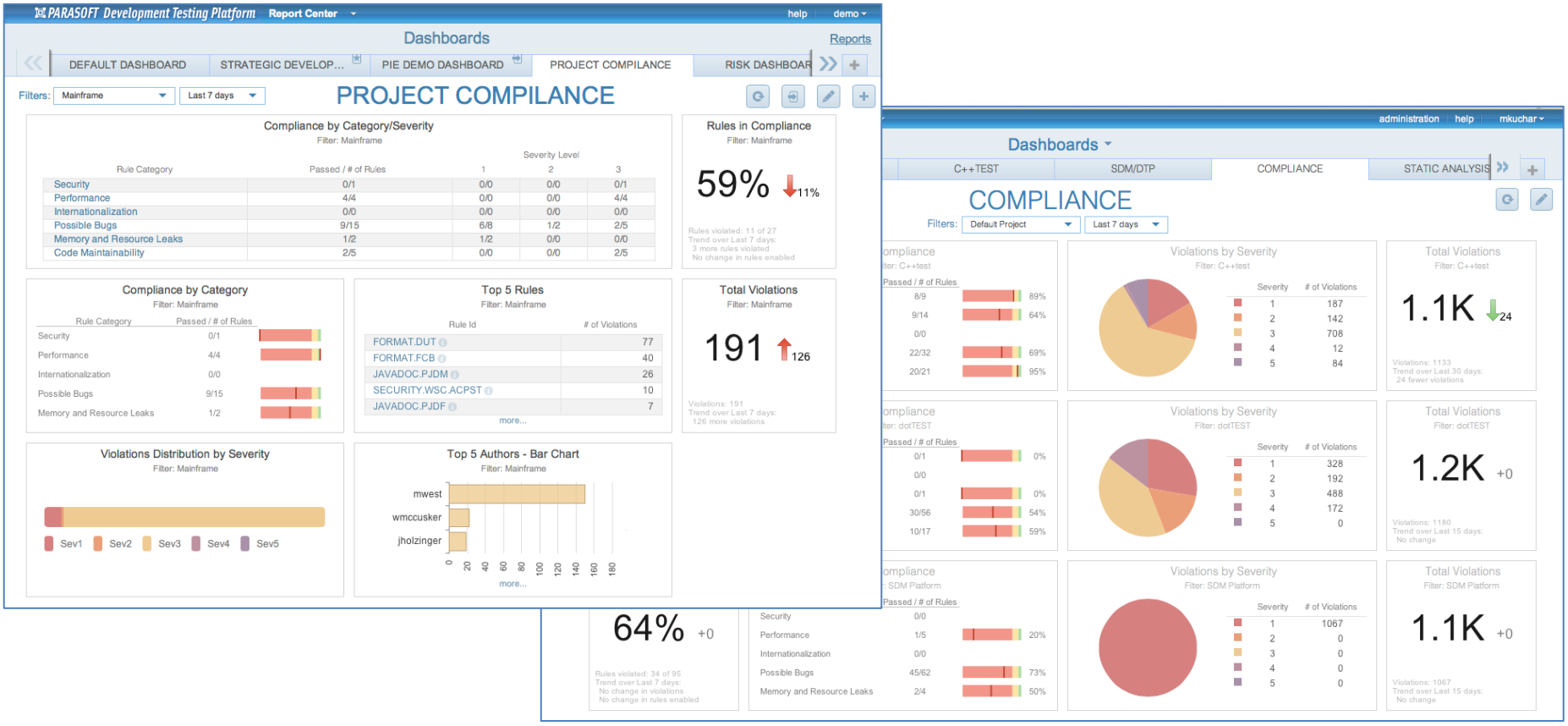
[18] Security (BD.SECURITY)
- **[1]** Protect against Command injection (BD.SECURITY.TDCMD-1)
- **[1]** Protect against Environment injection (BD.SECURITY.TDENV-1)
- **[1]** Protect against File contents injection (BD.SECURITY.TDFILES-1)
- **[1]** Protect against File names injection (BD.SECURITY.TDFNAMES-1)
- **[1]** Protect against Library injection (BD.SECURITY.TDLIB-1)
- **[1]** Protect against Reflection injection (BD.SECURITY.TDRFL-1)
- **[4]** Protect against SQL injection (BD.SECURITY.TDSQL-1)
- **[4]** Protect against XML data injection (BD.SECURITY.TDXML-1)
- **[4]** Protect against XSS vulnerabilities (BD.SECURITY.TDXSS-1)

[45] Unsafe Error Handling and Logging (SECURITY.UEHL)
- **[45]** Ensure all exceptions are either logged with a standard logger or rethrown (SECURITY.UEHL.LGE-3)

[5] Weak Security Controls (SECURITY.WSC)

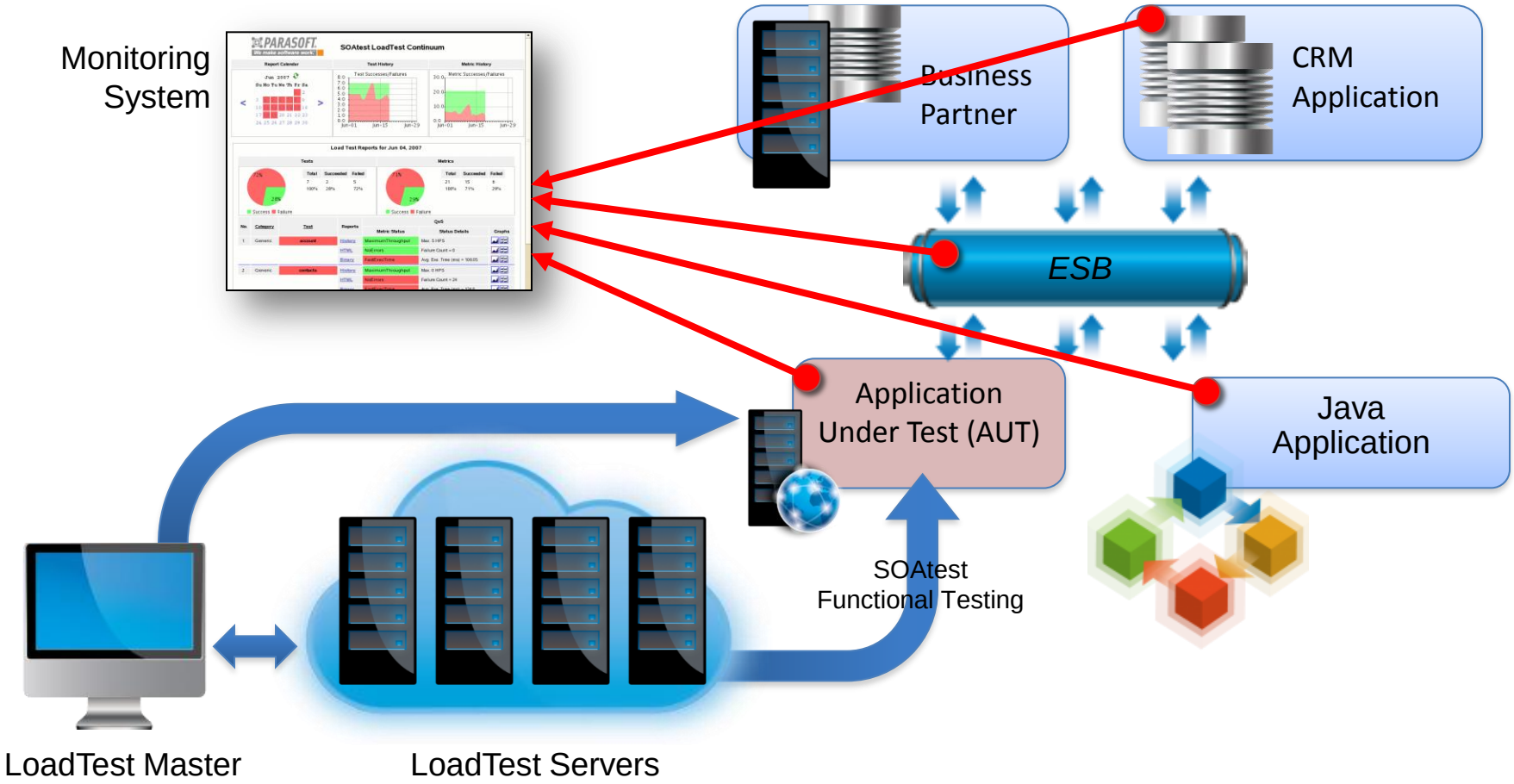
Quản lý trực quan!

- Cung cấp các phản hồi theo thời gian thực mức độ tuân thủ các tiêu chuẩn lập trình (PCI-DSS, OWASP, SANS) trong quá trình triển khai phần mềm/ứng dụng.

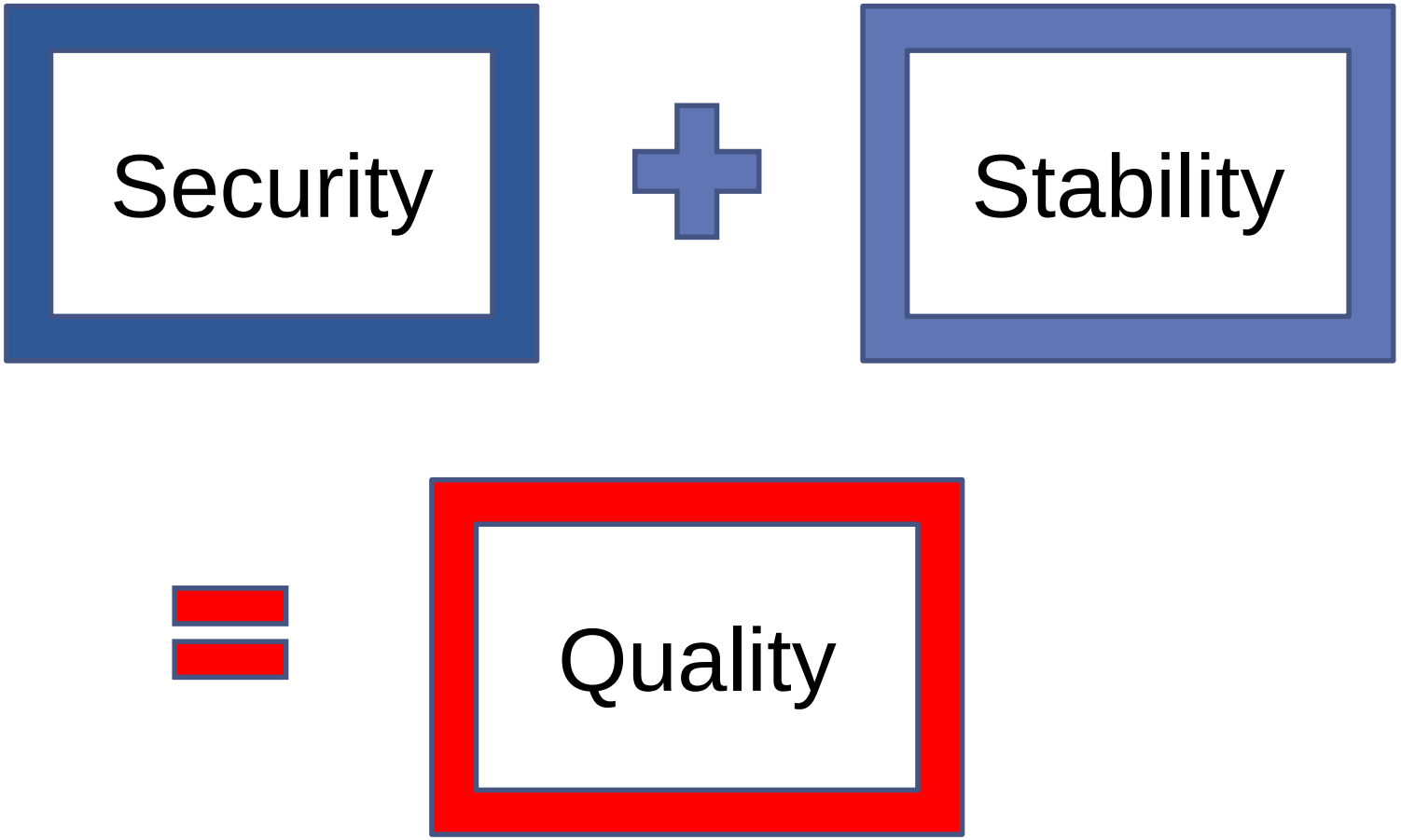


Kiểm thử hiệu năng (Load test)

- **Record and Replay** – Browser-based & API/Protocol Testing
- Có thể tái sử dụng các functional tests được tạo dựng từ trước
- Tuỳ biến số lượng virtual end-users



Công thức chất lượng phần mềm



Trên 10,000 KH toàn cầu

Tóm tắt

And they drew hope again
from their schoolfellow's teaching lesson

TORSTEN ZELGER

http://www.simply-the-test.blogspot.sg

Trân trọng cảm ơn!

VELATEK
Your Confidence. Our Quality.

- #10, Pham Van Hai, Tan Binh Dist., HCMC.
- +84-8-3844 3627
- info@velatek.vn
- www.velatek.vn