How to start a software security initiative within your organization: a maturity based and metrics driven approach

OWASP Italy Day 2, 2008
March 31th, 2008
Marco.Morana@OWASP.ORG

OWASP

The OWASP Foundation
http://www.owasp.org

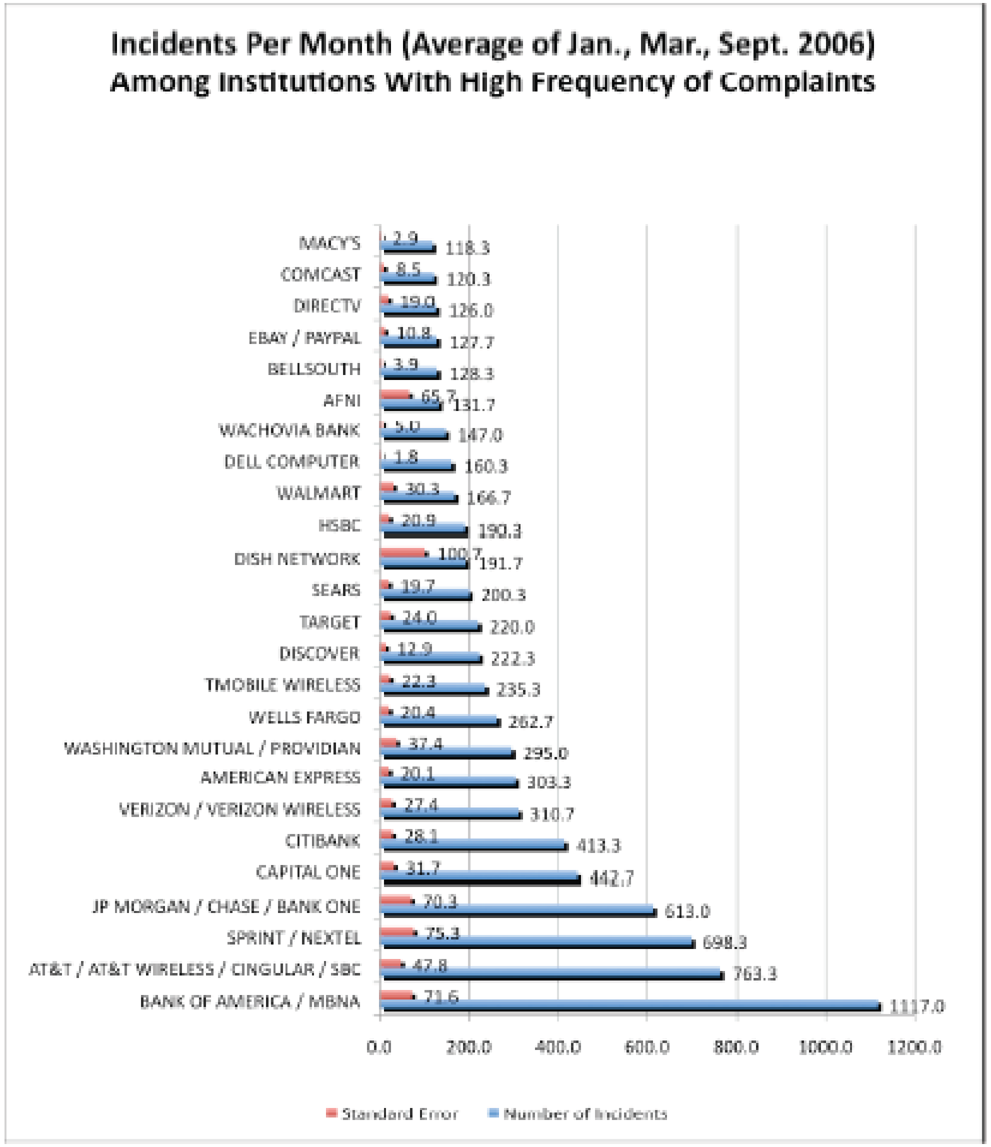
Agenda

1. Software Security Awareness
2. Tactical Responses
3. Software Security Strategy
4. Software Security Initiative
5. Questions & Answers

Software Security Awareness : Threats

- **On-line fraud overtakes viruses** as the greatest source of financial loss (Symantec)
- **93.8% of all phishing attacks in 2007 are targeting financial institutions** (Anti-Phishing Group)
- **Phishing attacks soar in 2007** (Gartner)
  - 3.6 Million victims, $ 3.2 Billion Loss (2007)
  - 2.3 Million victims, $ 0.5 Billion Loss (2006)

Software Security Awareness : Threats

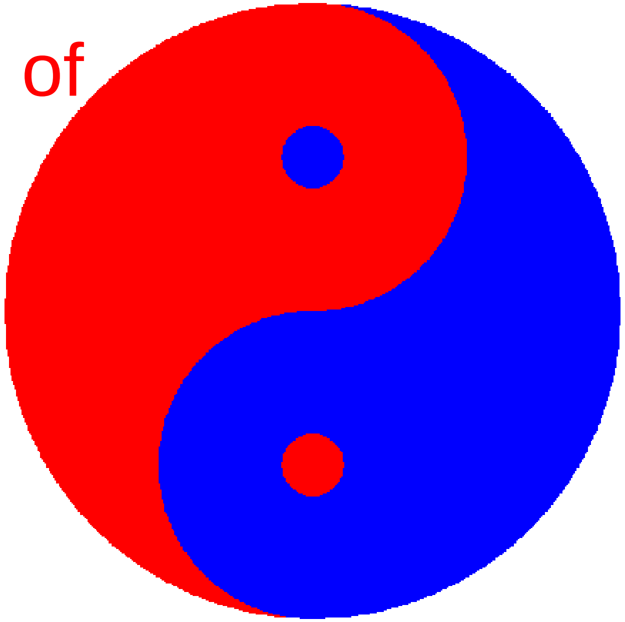


Software Security Awareness: Software Security Vs. Application Security

Security built into each phase of the SDLC

Look at root problem causes

Proactive, Threat Analysis, Risk Management



Security applied by catch and patches

Look at external symptoms

Reactive, Incident Response, Compliance

Agenda Update

1. Security Awareness
2. **Tactical Responses**
3. Software Security Strategy
4. Software Security Initiative
5. Questions & Answers

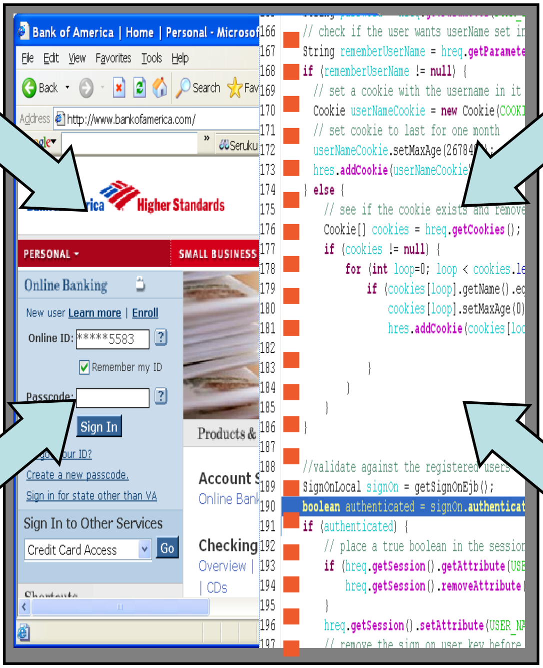
Tactical Responses: Initial Security Assessment

- **The symptoms**: are the clues that lead to potential vulnerabilities and exploits
- **The root causes**: security design flaws, security bugs (coding errors), insecure-configuration
- **The risk factors**: how much damage can be done, how easy is to reproduce the exploits, how many users are exposed and how easy is to discover the vulnerabilities

Tactical Responses: Finding Vulnerabilities

Manual Penetration Testing

Manual Code Review



```
// check if the user wants userName set in
String rememberUserName = hreq.getParamete
if (rememberUserName != null) {
  // set a cookie with the username in it
  Cookie userNameCookie = new Cookie(COOKI
  // set cookie to last for one month
  userNameCookie.setMaxAge(26784[illegible]);
  hres.addCookie(userNameCookie
} else {
    // see if the cookie exists and remove
    Cookie[] cookies = hreq.getCookies();
    if (cookies != null) {
        for (int loop=0; loop < cookies.le
            if (cookies[loop].getName().eq
                cookies[loop].setMaxAge(0)
                hres.addCookie(cookies[loo

            }
        }
    }
}

//validate against the registered users
SignOnLocal signOn = getSignOnEjb();
boolean authenticated = signOn.authenticat
if (authenticated) {
    // place a true boolean in the session
    if (hreq.getSession().getAttribute(USE
        hreq.getSession().removeAttribute(
    }
    hreq.getSession().setAttribute(USER_NA
    // remove the sign on user key before
```

Automated Vulnerability Scanning

Automated Static Code Analysis

Tactical Responses: Risk Analysis

- **Risk terminology:**
  - Threat (e.g. the cause)
  - Vulnerability (e.g. the application weakness)
  - Impact (e.g. the loss of data)
  - Risk (e.g. The rating, likelihood x exposure)
- **Risk models:**
  - STRIDE/DREAD
  - Threat X Vulnerability X Impact (OWASP)
  - ALE = SLE X ARO

Agenda Update

1. Security Awareness
2. Tactical Responses
3. **Software Security Strategy**
4. Software Security Initiative
5. Questions & Answers

Software Security Strategy: First Approaches

- **Be Realistic**
  - Organization is **not yet ready** (e.g. mature)
  - Engineers are **not trained** in software security
  - There are **no tools available**
- **Make up strategy**
  - **Based upon your company strenghts**
  - **With stakeholders buy in** (CIOs, ISOs, PM, Developers, Architects)
  - **With achieveable goals**: reduce 30% of vulnerabilities found through ethical hacking via source code analysys

Software Security Strategy: Initial Business Cases

- **Not fixing security bugs early is expensive**:
  - $9,000 per defect after system tests (90X factor @ 100 dollars / hour x 1 hour= 9000 dollars) (NIST, Economic Impact of In-secure Testing)
  - $100,000 per security bulletin (M. Howard and D. LeBlanc in Writing Secure Software book)

Software Security Strategy: Create a Roadmap

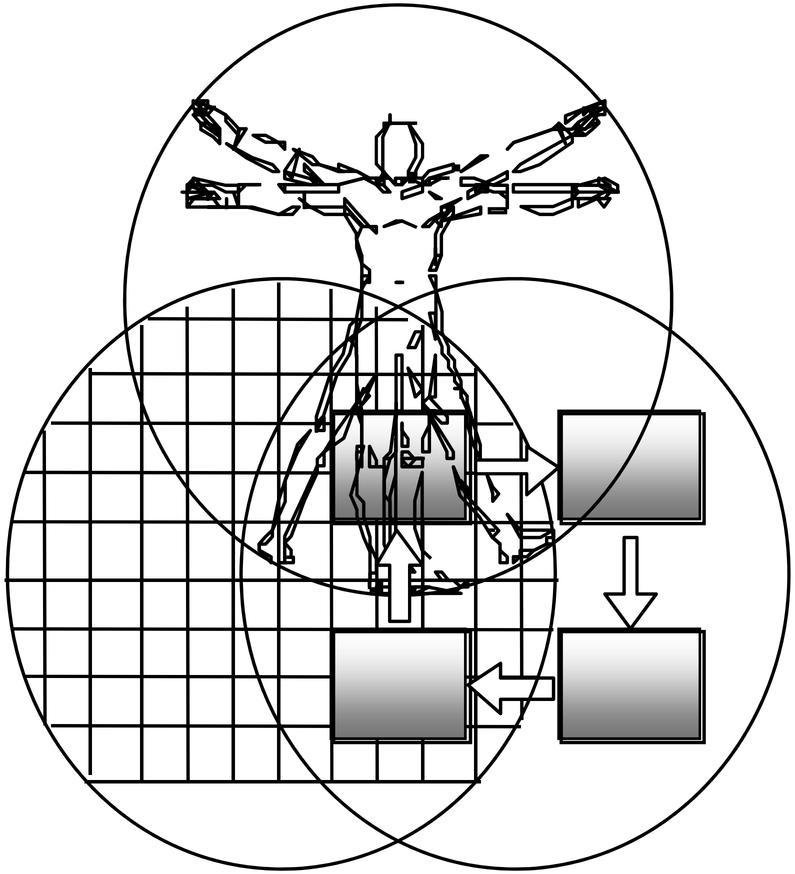
1. **Assess software maturity** of the organization software security development processes, people and tools
2. **Document the software security process:** security enhanced SDLCs and checkpoints
3. **Implement a framework:** software engineering and risk management processes
4. **Create business cases and set objectives**
5. **Collect metrics and measurements**
6. **Gain stakeholders commitments**

Agenda Update

1. Security Awareness
2. Tactical Responses
3. Software Security Strategy
4. **Software Security Initiative**
5. Questions & Answers

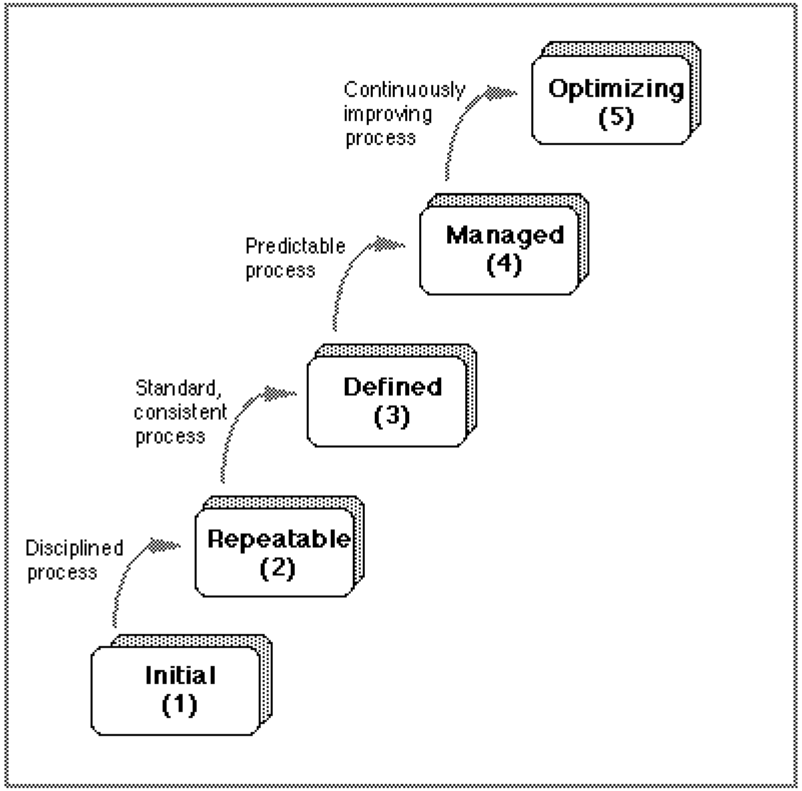
Software Security Initiative: People, Process, Technology

- People: Who manages software security risks
- Process: What where and how security can be build in the SDLC
- Tools: How processes can be automated



Security = Commitment *(People+Tools +Process^2)

Software Security Initiative :Maturity Levels



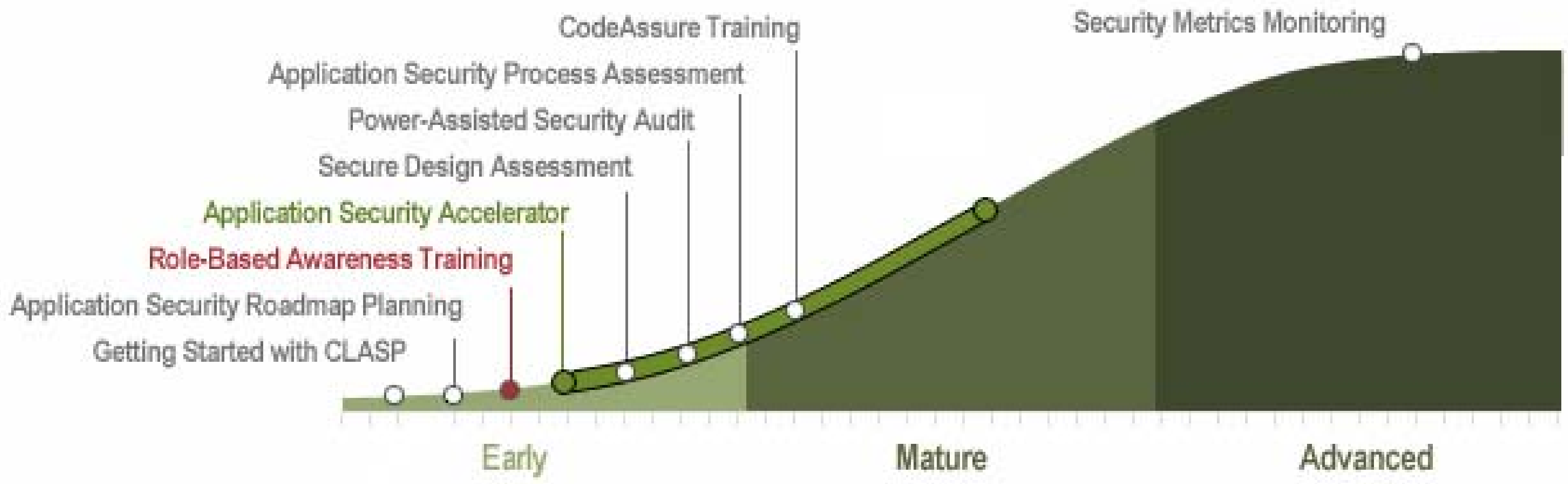
Software Security Initiative: Maturity Levels

- **Maturity Innocence (CMM 0-1)**
  - No formal security requirements
  - Issues addressed with penetration testing and incidents
  - Penetrate and patch and reactive approach
- **Maturity Awareness (CMM 2-3)**
  - All applications have penetration tests done before going into production
  - Secure coding standards are adopted as well as source code reviews

Software Security Initiative: Maturity Levels

- **Maturity Enlightenment (CCM 4-5)**
  - Threat analysis in each phase of the SDLC
  - Risk metrics and vulnerability measurements are used for security activity decision making (money for the bang)

Software Security Initiative: Maturity Adoption Curve (OWASP-CLASP)

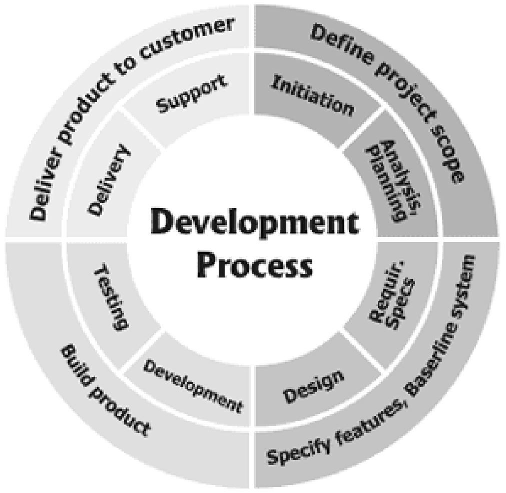


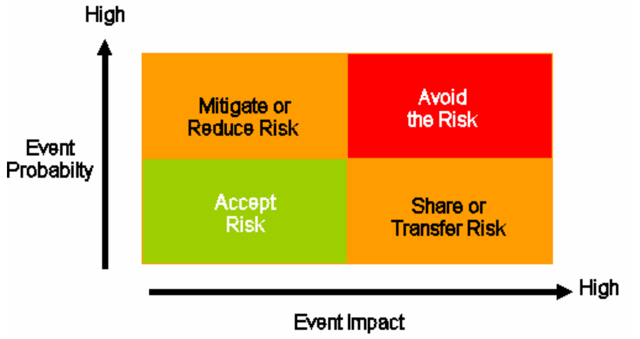
The area under the curve represents the cost for achieving maturity in terms of training, tools and activity implementation. The steeper the curve the highest the cost

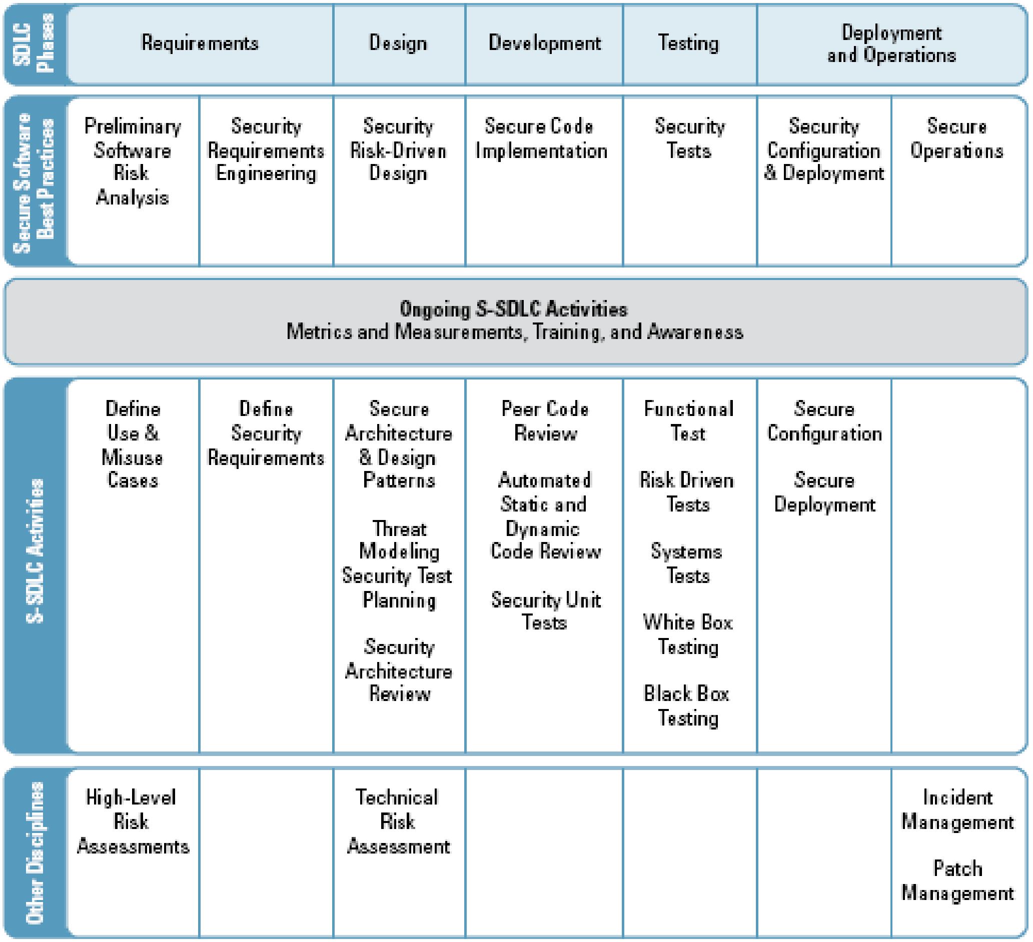
Software Security Initiative: People

- **What not to look for**:
  - Ethical hackers that cannot tell how to build applications securely
  - Security engineers with no experience in software engineering, design, coding
  - Information security professionals that only know how security auditing
- **What to look for**:
  - Security professionals that understand both coding and security
  - Software security consultants

Software Security Initiative: Frameworks

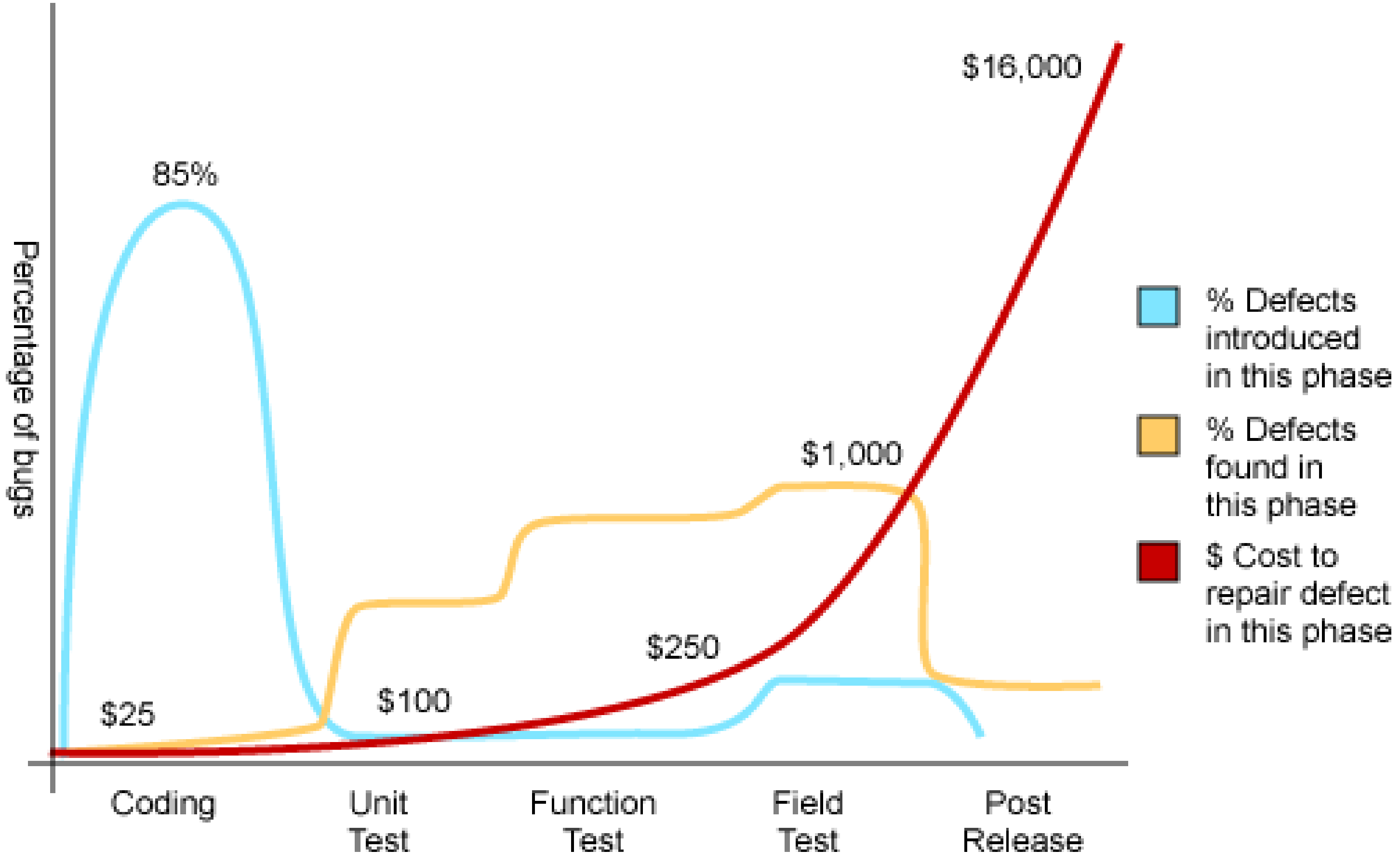






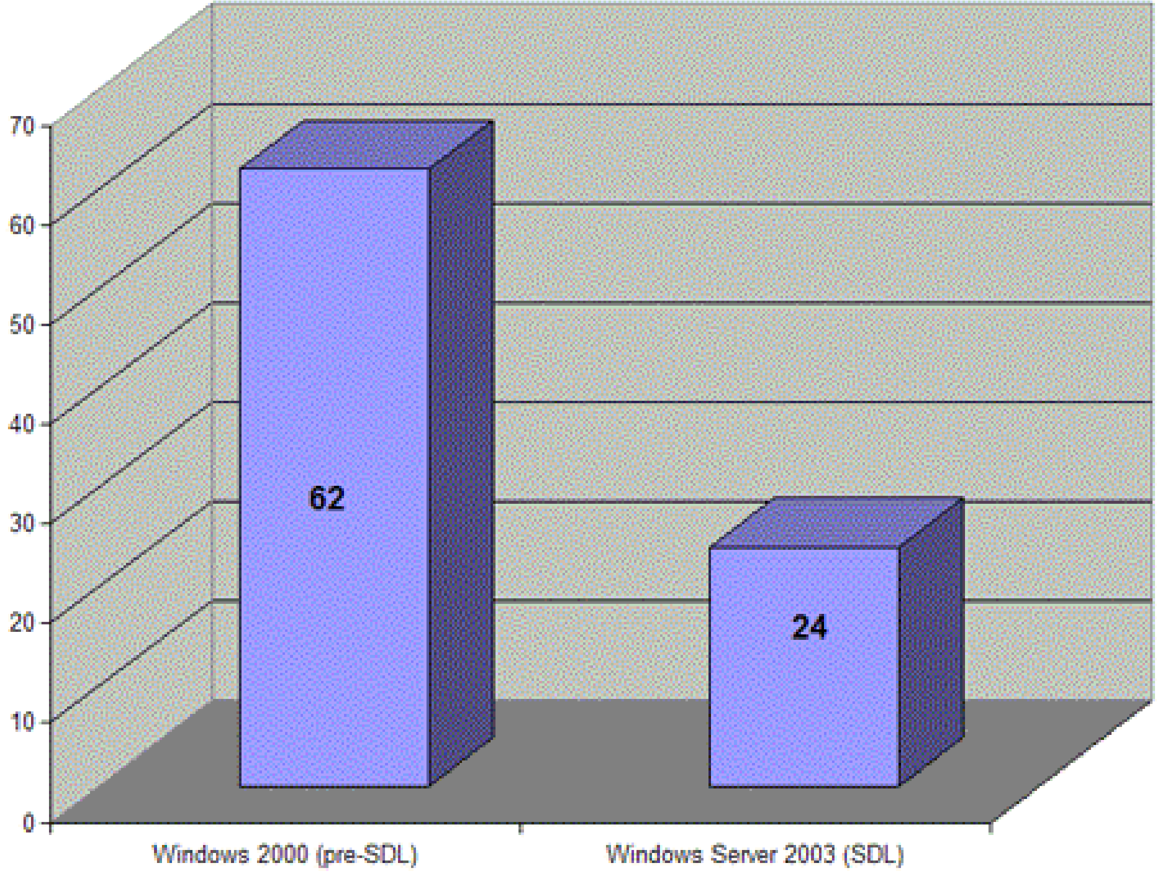
SDLC Phases	Requirements		Design	Development	Testing	Deployment and Operations	
Secure Software Best Practices	Preliminary Software Risk Analysis	Security Requirements Engineering	Security Risk-Driven Design	Secure Code Implementation	Security Tests	Security Configuration & Deployment	Secure Operations
Ongoing S-SDLC Activities Metrics and Measurements, Training, and Awareness							
S-SDLC Activities	Define Use & Misuse Cases	Define Security Requirements	Secure Architecture & Design Patterns Threat Modeling Security Test Planning Security Architecture Review	Peer Code Review Automated Static and Dynamic Code Review Security Unit Tests	Functional Test Risk Driven Tests Systems Tests White Box Testing Black Box Testing	Secure Configuration Secure Deployment	
Other Disciplines	High-Level Risk Assessments		Technical Risk Assessment				Incident Management Patch Management

Software Security Initiative: SDLC Metrics



Source: Applied Software Measurement, Capers Jones, 1996

Software Security Initiative: Trailing Metrics



Software Security Initiative: Defending the case

- **Fight common misconceptions** that software security impacts:
  - performance
  - costs/budget
  - development
- **Make the case for each role**
  - Developers that are tired to rebuild software
  - Project managers that worry about missing deadlines
  - Information Security Officers worry about compliance
  - CIOs worry about budget,ROSI

Software Security Initiative: Commitment

- **Top Down**
  - Two months freeze on development
  - Every developer on training
  - SDL delivered across projects
- **Bottom up**
  - Project Managers commit resources to training and demand secure code reviews
  - Architects and engineering leads test and address security issues as early as are found in the source code and the application
  - CISO address compliance with information security policies as well secure coding standards

Concluding Remarks

Remember Rome was not build in a day!

You need time to mature you processes, train your employees and implement the right process, tools and technologies

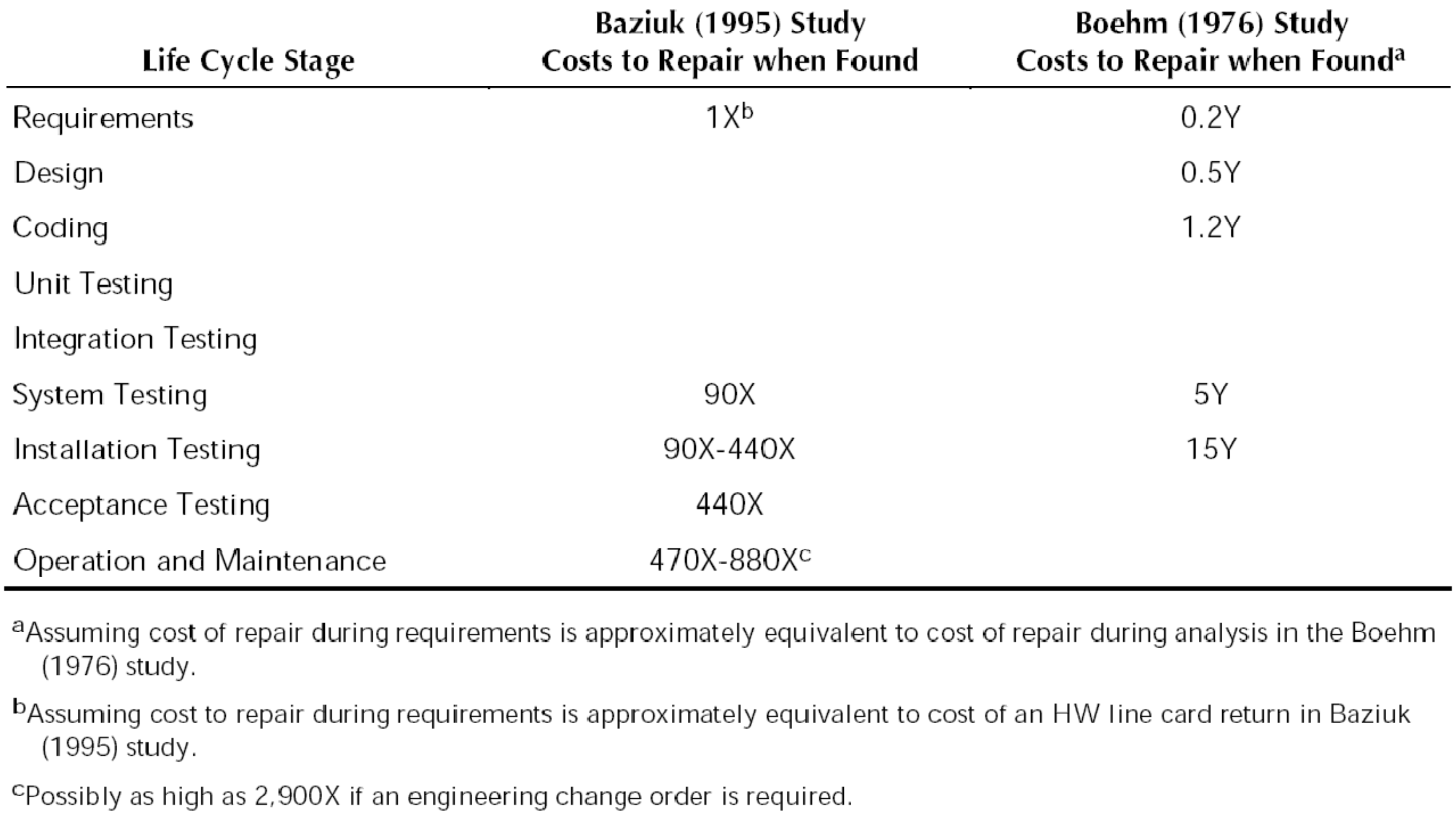
Agenda Update

1. Security Awareness
2. Tactical Responses
3. Software Security Strategy
4. Software Security Initiative
5. **Questions & Answers……..?**

Thanks for listening, further references

- Symantec threat report http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- Gartner study on phising: http://www.gartner.com/it/page.jsp?id=565125)
- UC Berkeley Center for Law and Technology on identity theft http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1045&context=bclt

Appendix: Cost of Defects, NIST Study



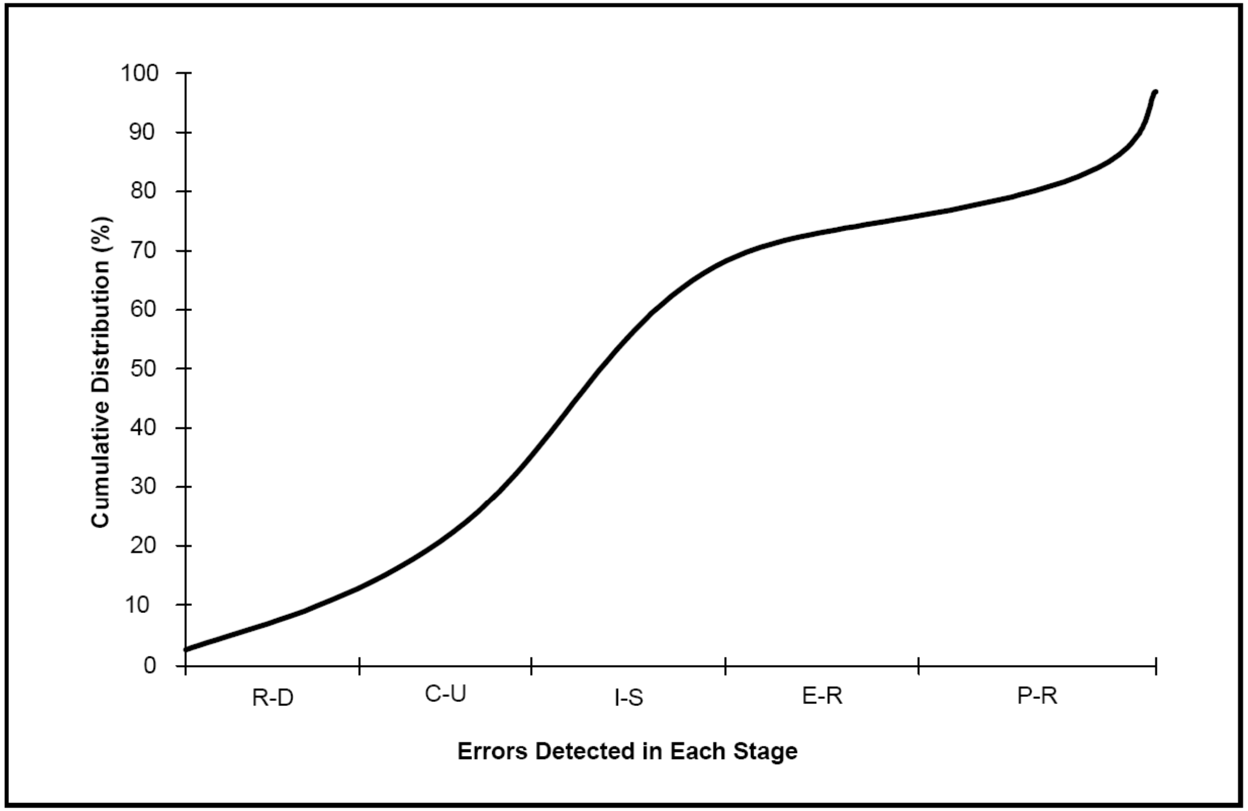
Life Cycle Stage	Baziuk (1995) Study Costs to Repair when Found	Boehm (1976) Study Costs to Repair when Found[a]
Requirements	1X[b]	0.2Y
Design		0.5Y
Coding		1.2Y
Unit Testing		
Integration Testing		
System Testing	90X	5Y
Installation Testing	90X-440X	15Y
Acceptance Testing	440X	
Operation and Maintenance	470X-880X[c]	

[a] Assuming cost of repair during requirements is approximately equivalent to cost of repair during analysis in the Boehm (1976) study.

[b] Assuming cost to repair during requirements is approximately equivalent to cost of an HW line card return in Baziuk (1995) study.

[c] Possibly as high as 2,900X if an engineering change order is required.

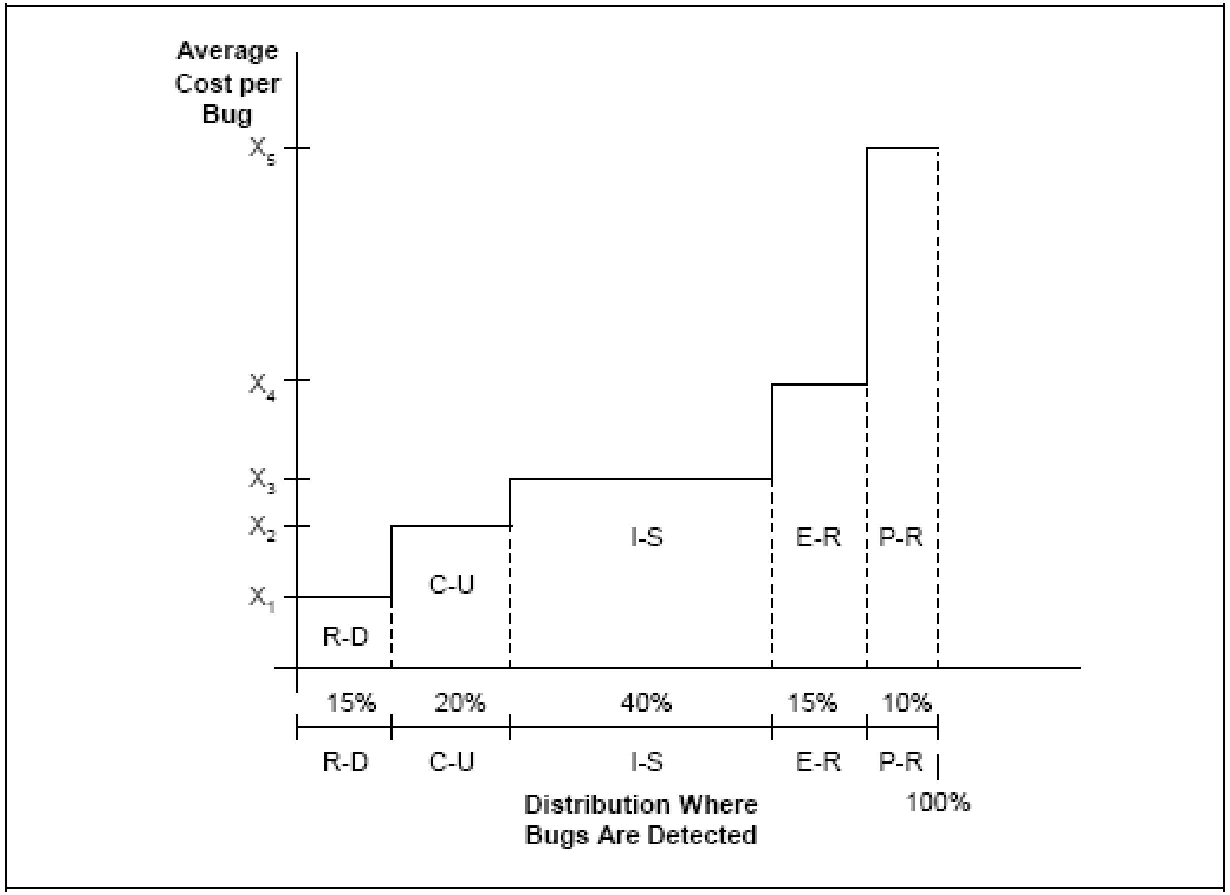
Appendix: Location of Defects



Legend:

R-D: Requirements Gathering and Analysis/Architectural Design
C-U: Coding/Unit Test
I-S: Integration and Component/RAISE System Test
E-R: Early Customer Feedback/Beta Test Programs
P-R: Post-product Release

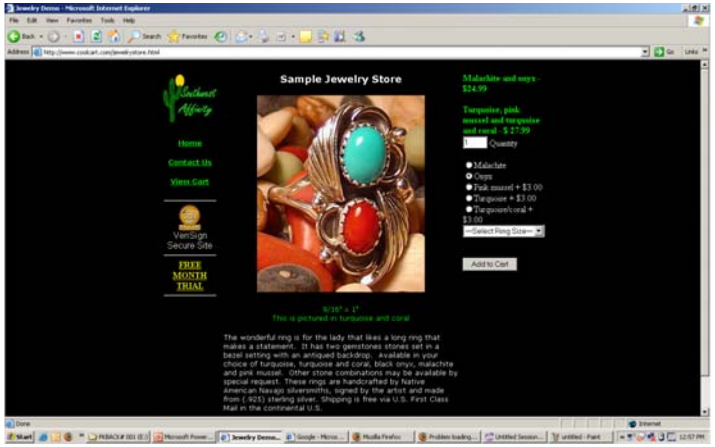
Appendix: Location of Defects



Legend:
- R-D: Requirements Gathering and Analysis/Architectural Design
- C-U: Coding/Unit Test
- I-S: Integration and Component/RAISE System Test
- E-R: Early Customer Feedback/Beta Test Programs
- P-R: Post-product Release

Appendix: Insecure Shopping Cart

http://www.coolcart.com/jewelrystore.html



Jewelry Demo - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.coolcart.com/jewelrystore.html
Southwest Affinity
Home
Contact Us
View Cart
VeriSign Secure Site
FREE MONTH TRIAL

Sample Jewelry Store

Malachite and onyx - $24.99

Turquoise, pink mussel and turquoise and coral - $ 27.99

1 Quantity

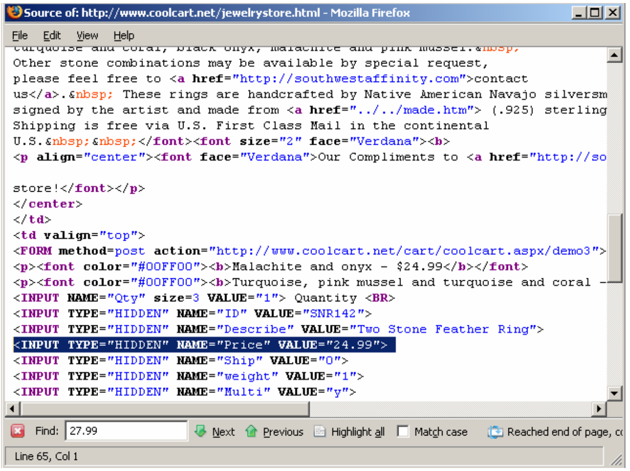
○ Malachite
● Onyx
○ Pink mussel + $3.00
○ Turquoise + $3.00
○ Turquoise/coral + $3.00

--Select Ring Size--

Add to Cart

9/16" x 1"
This is pictured in turquoise and coral

The wonderful ring is for the lady that likes a long ring that makes a statement. It has two gemstones stones set in a bezel setting with an antiqued backdrop. Available in your choice of turquoise, turquoise and coral, black onyx, malachite and pink mussel. Other stone combinations may be available by special request. These rings are handcrafted by Native American Navajo silversmiths, signed by the artist and made from (.925) sterling silver. Shipping is free via U.S. First Class Mail in the continental U.S.



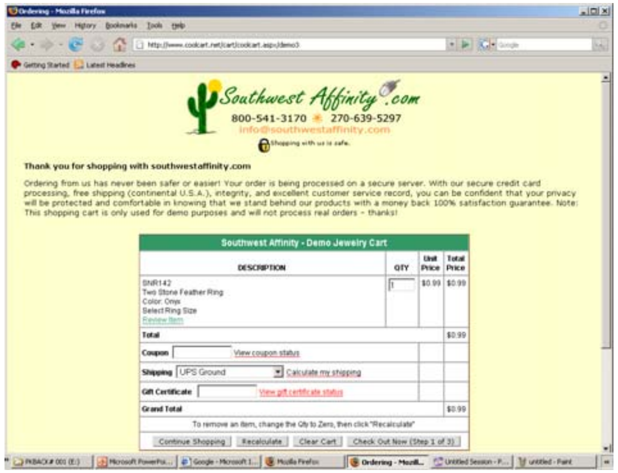
Source of: http://www.coolcart.net/jewelrystore.html - Mozilla Firefox
File Edit View Help

```
turquoise and coral, black onyx, malachite and pink mussel.&nbsp;
Other stone combinations may be available by special request,
please feel free to <a href="http://southwestaffinity.com">contact
us</a>.&nbsp; These rings are handcrafted by Native American Navajo silversm
signed by the artist and made from <a href="../../made.htm"> (.925) sterling
Shipping is free via U.S. First Class Mail in the continental
U.S.&nbsp;&nbsp;</font><font size="2" face="Verdana"><b>
<p align="center"><font face="Verdana">Our Compliments to <a href="http://so

store!</font></p>
</center>
</td>
<td valign="top">
<FORM method=post action="http://www.coolcart.net/cart/coolcart.aspx/demo3">
<p><font color="#00FF00"><b>Malachite and onyx - $24.99</b></font>
<p><font color="#00FF00"><b>Turquoise, pink mussel and turquoise and coral -
<INPUT NAME="Qty" size=3 VALUE="1"> Quantity <BR>
<INPUT TYPE="HIDDEN" NAME="ID" VALUE="SNR142">
<INPUT TYPE="HIDDEN" NAME="Describe" VALUE="Two Stone Feather Ring">
<INPUT TYPE="HIDDEN" NAME="Price" VALUE="24.99">
<INPUT TYPE="HIDDEN" NAME="Ship" VALUE="0">
<INPUT TYPE="HIDDEN" NAME="weight" VALUE="1">
<INPUT TYPE="HIDDEN" NAME="Multi" VALUE="y">
```

Find: 27.99 Next Previous Highlight all □ Match case Reached end of page, c

Line 65, Col 1



Ordering - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.coolcart.net/cart/coolcart.aspx/demo3
Getting Started Latest Headlines
Southwest Affinity.com

800-541-3170 270-639-5297
info@southwestaffinity.com
Shopping with us is safe.

Thank you for shopping with southwestaffinity.com

Ordering from us has never been safer or easier! Your order is being processed on a secure server. With our secure credit card processing, free shipping (continental U.S.A.), integrity, and excellent customer service record, you can be confident that your privacy will be protected and comfortable in knowing that we stand behind our products with a money back 100% satisfaction guarantee. Note: This shopping cart is only used for demo purposes and will not process real orders - thanks!

Southwest Affinity - Demo Jewelry Cart

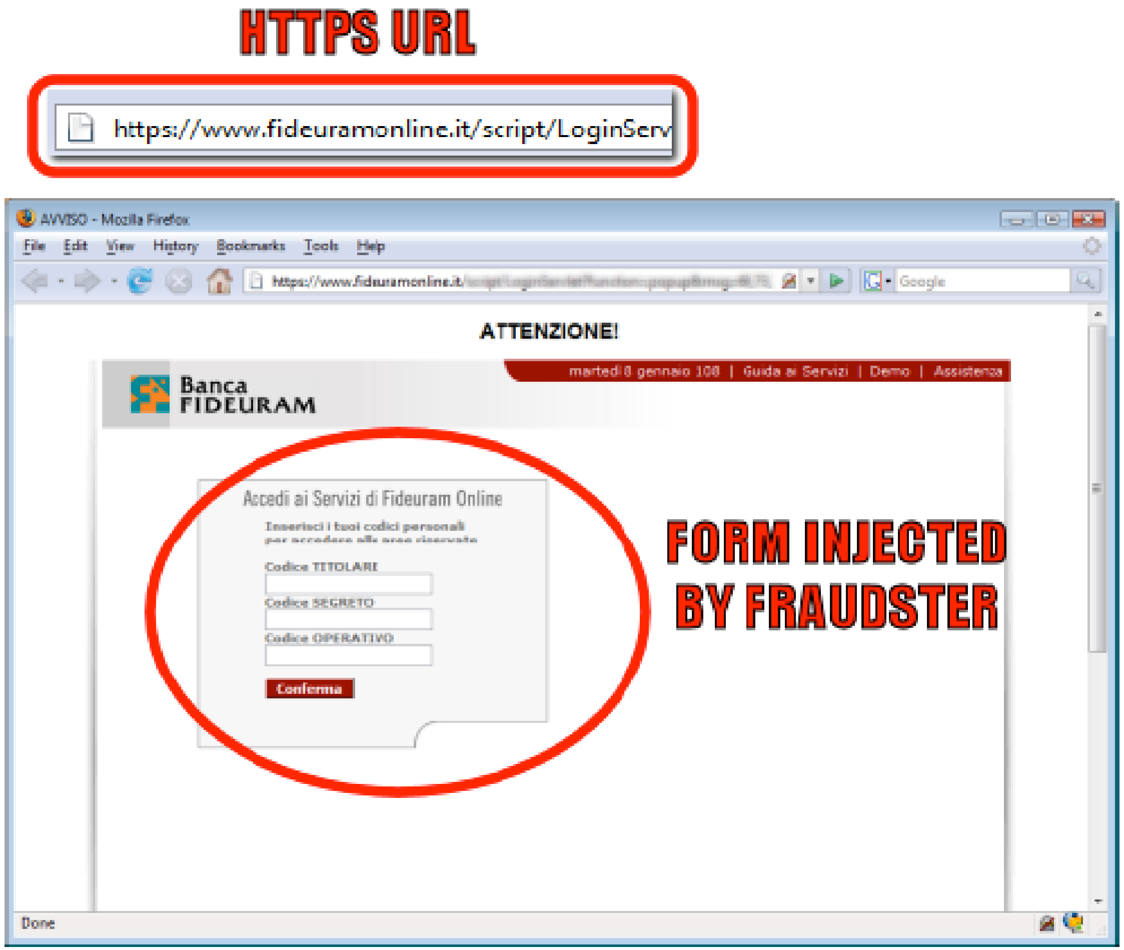
DESCRIPTION	QTY	Unit Price	Total Price
SNR142 Two Stone Feather Ring Color: Onyx Select Ring Size Review Item	1	$0.99	$0.99
Total			$0.99
Coupon View coupon status			
Shipping UPS Ground Calculate my shipping			
Gift Certificate View gift certificate status			
Grand Total			$0.99

To remove an item, change the Qty to Zero, then click "Recalculate"

Continue Shopping | Recalculate | Clear Cart | Check Out Now (Step 1 of 3)

The price charged for the "Two Stone Feather Ring" is now 99 cents

Appendix: XFS Vulnerabilities



HTTPS URL

https://www.fideuramonline.it/script/LoginServ

AVVISO - Mozilla Firefox

https://www.fideuramonline.it/[redacted]

ATTENZIONE!

martedì 8 gennaio 108 | Guida ai Servizi | Demo | Assistenza

Banca FIDEURAM

Accedi ai Servizi di Fideuram Online

Inserisci i tuoi codici personali
per accedere alle aree riservate

Codice TITOLARE

Codice SEGRETO

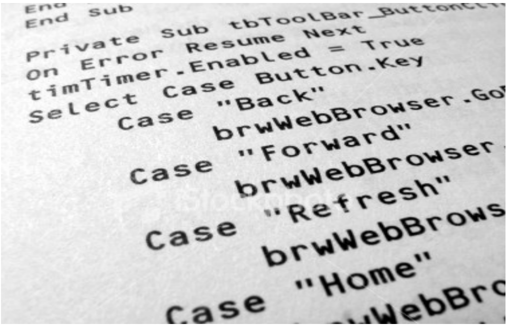
Codice OPERATIVO

Conferma

FORM INJECTED BY FRAUDSTER

Done

Appendix: Reactive Approach



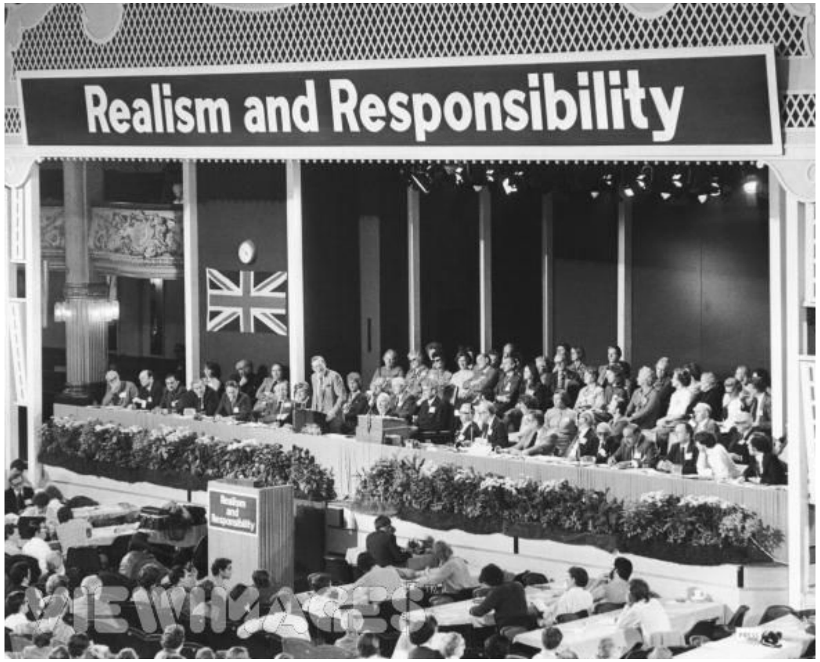
```
End
End  Sub
Private Sub tbToolBar_ButtonCl
On Error Resume Next
timTimer.Enabled = True
Select Case Button.Key
    Case "Back"
        brwWebBrowser.Go
    Case "Forward"
        brwWebBrowser
    Case "Refresh"
        brwWebBrows
    Case "Home"
        WebBr
```

Go Fix Security Bugs!

Appendix: Tie Attacks To Vulnerabilities

- Phishing
  - A1, A4, A7, A10
- Privacy violations
  - A2, A4, A6, A7, A10
- Identity theft
  - A3, A7, A8, A9, A10
- System compromise, data alteration or data destruction
  - A2, A3
- Financial loss
  - A4, A5, A7, A10
- Reputation loss
  - A1, A2, A3, A4, A5, A6 ,A7, A8, A9, A10

Appendix: The Motto



*“If your software security practices are **not yet mature be pragmatic and start making software security a responsibility** for who builds software in your organization*

Appendix: About Me

- Graduated from University of Padua, Italy in 1987 (Dr. Ing, Laurea Ingegneria Meccanica)
- Worked as Aerospace engineer in Italy between 1990-1994
- Got a Master in Computer System Engineering from Northwestern Polytechnic University in 1996
- Worked as Software Eng. in silicon valley between 1996-1998
- While working at NASA as Sterling Software contractor, developed the first e-mail S/MIME and got a patent in 1997
- Founded CerbTech LLC in 2003 and I worked at a security project for VISA
- Developed commercial security tools/products for ISS (Safesuite Decisions) and Sybase (Security Manager) (1998-2004)
- As Sr. Security Consultant with Foundstone/McAfee (2004-2006) and consulted for major banks and telco in USA
- Joined Citigroup in 2006 as Technology Information Security Officer (Sr. Director/VP)
- Founded the OWASP Cincinnati USA chapter in 2007