

Assessing and Measuring Security in Custom SAP Applications

*Sebastian Schinzel
IT-Security Consultant
Virtual Forge GmbH*

Agenda

- **Common Security Vulnerabilities**
- **Threat Modelling**
- **Measuring Security**
- **How can I improve my security performance?**

Common Security Vulnerabilities



XSS flaw makes PM say: "I want to suck your bl

http://www.zdnet.com.au/news/security/soa/XSS-f

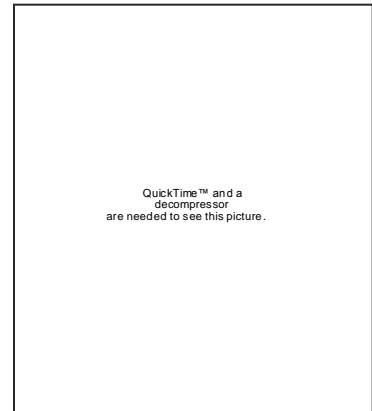
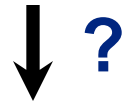
News > Security

XSS flaw makes PM say: "I want to suck your blood"

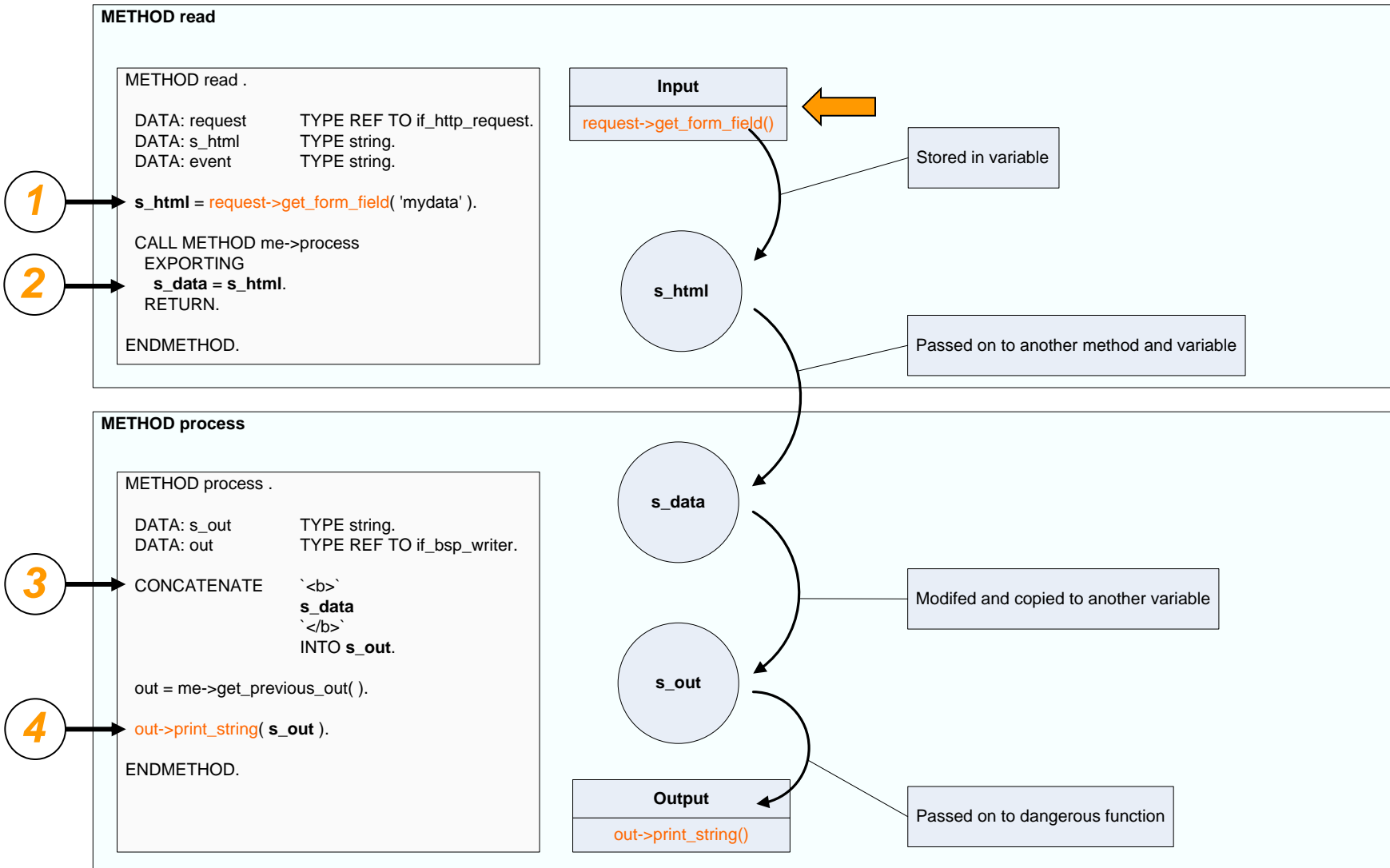
Liam Tung, ZDNet Australia
09 October 2007 04:52 PM
Tags: liberal, labor, cross-site scripting, xss, security, flaw, party, vulnerable

The Web sites of Australia's two major political parties contain cross-site scripting (XSS) flaws, which could be exploited to fraudulently acquire political donations, say security experts.

A short line of script developed by a security enthusiast, [Bsoric](#), causes the Liberal Party's Web site to read: "John Howard says: I want to suck your blood", while another script caused a window to pop up on the Labor Party's Web site, urging viewers to "Vote Liberal!"



Common Security Vulnerabilities



Common Security Vulnerabilities

```

<%@page language="abap" forceEncode="html" %>
<html>
  <body>
    <form>
      <% data: x type string.
        x = request->get_form_field( 'x' ).
      %>
      <input type=text name=x value="<%=x%>">
      <input type=submit>
    </form>
  </body>
</html>

```

You need to use `cl_http_utility=>escape_url`

Common Security Vulnerabilities

Cross Site Scripting is **not** limited to SAP technologies

- **Verisign** just had 6 XSS flaws, 1 still not fixed
- **McAfee** just had 9 XSS flaws, 2 still not fixed
- **Symantec** just had 17 XSS flaws, 7 still not fixed

[http://www.xssed.com/news/72/Verisign McAfee and Symantec sites can be used for phishing due to XSS](http://www.xssed.com/news/72/Verisign%20McAfee%20and%20Symantec%20sites%20can%20be%20used%20for%20phishing%20due%20to%20XSS)

Common Security Vulnerabilities



Porn and privacy: Big Brother's big bother



Technical glitches have plagued the launch of Big Brother.
Picture: Courtesy Channel Ten

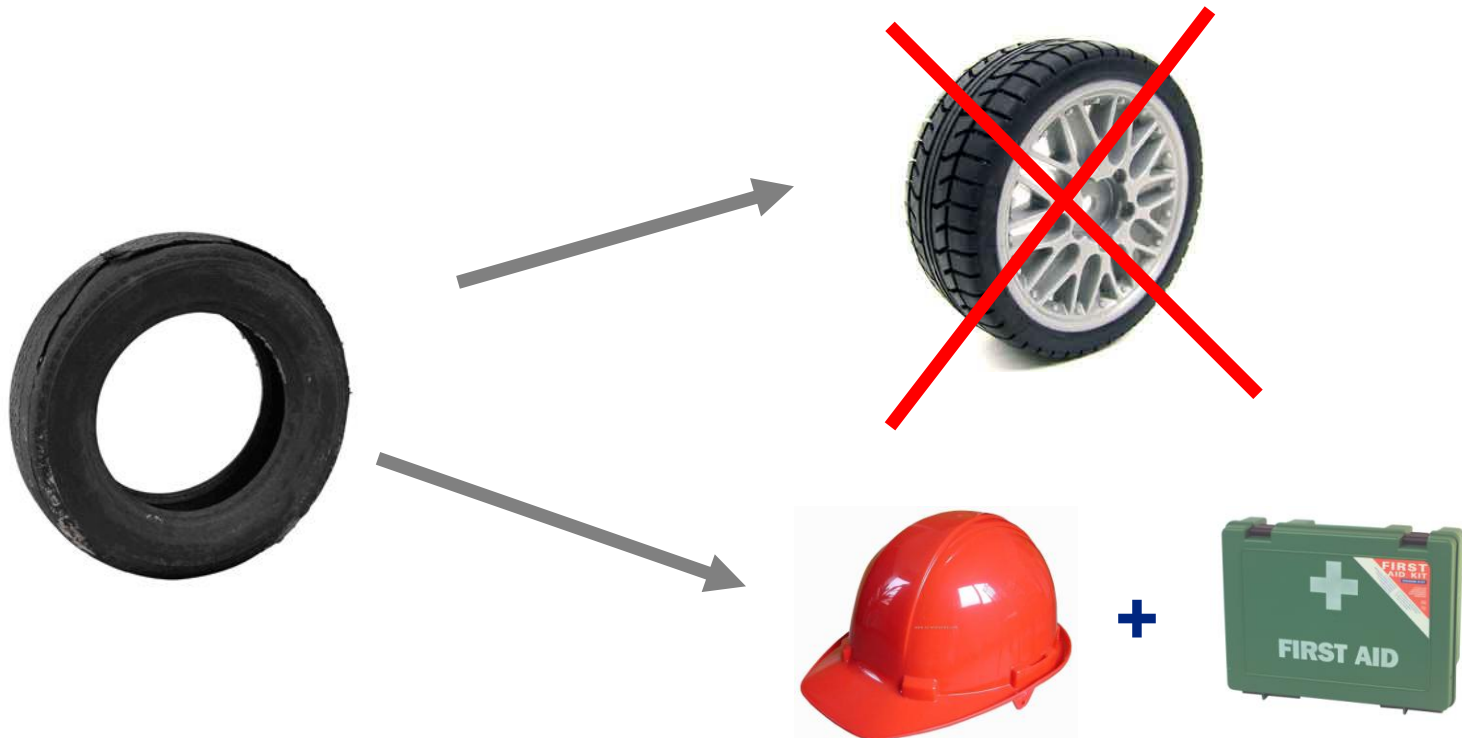
<http://www.theage.com.au/news/tv--radio/porn-privacy-glitches-hit-big-bro/2007/04/23/1177180548617.html>

Common Security Vulnerabilities

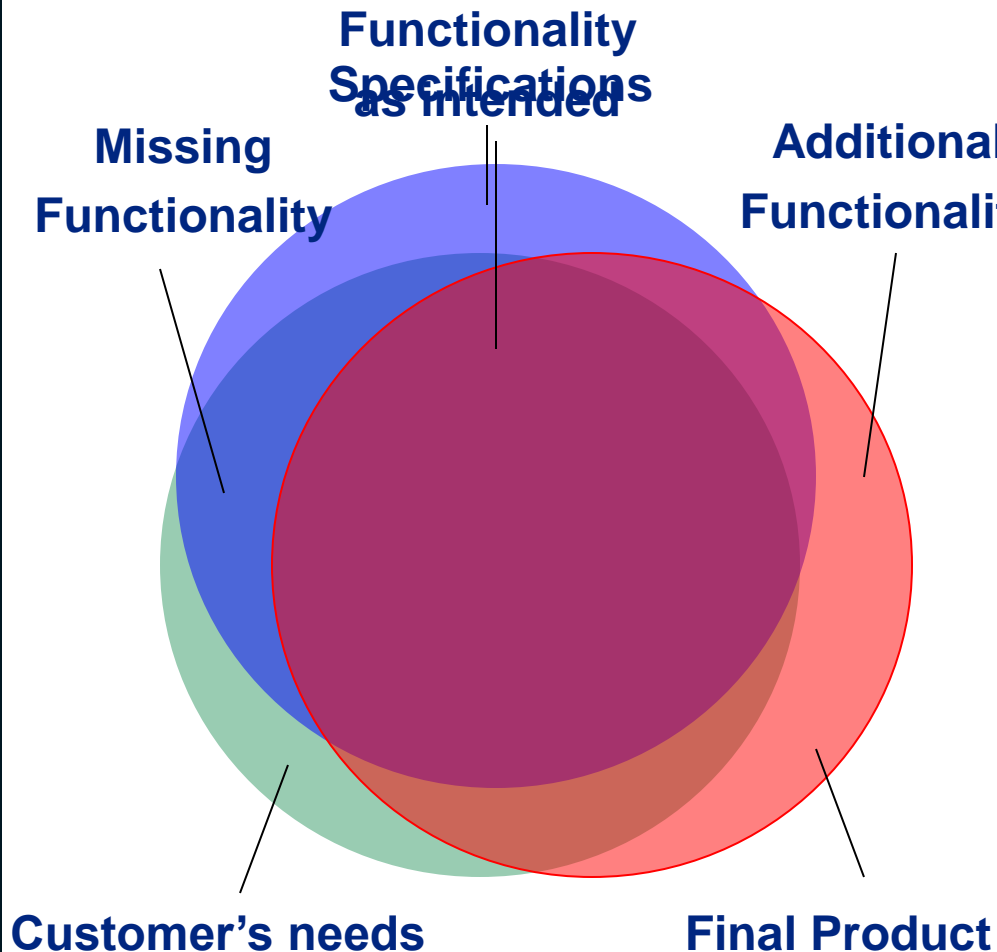
- **Vulnerabilities in handling of user session IDs**
 - ◆ Small pool of available session IDs
 - ◆ Pool got exhausted with many concurrent users
 - ◆ Users were falsely logged in as another already logged in user
- **Small pool of session IDs = predictable session IDs**
 - ◆ Easy to find and exploit for an attacker
 - ◆ Attack easy to automate
 - ◆ Possibility of getting caught is low

Common Security Vulnerabilities

Fighting symptoms, not root causes...



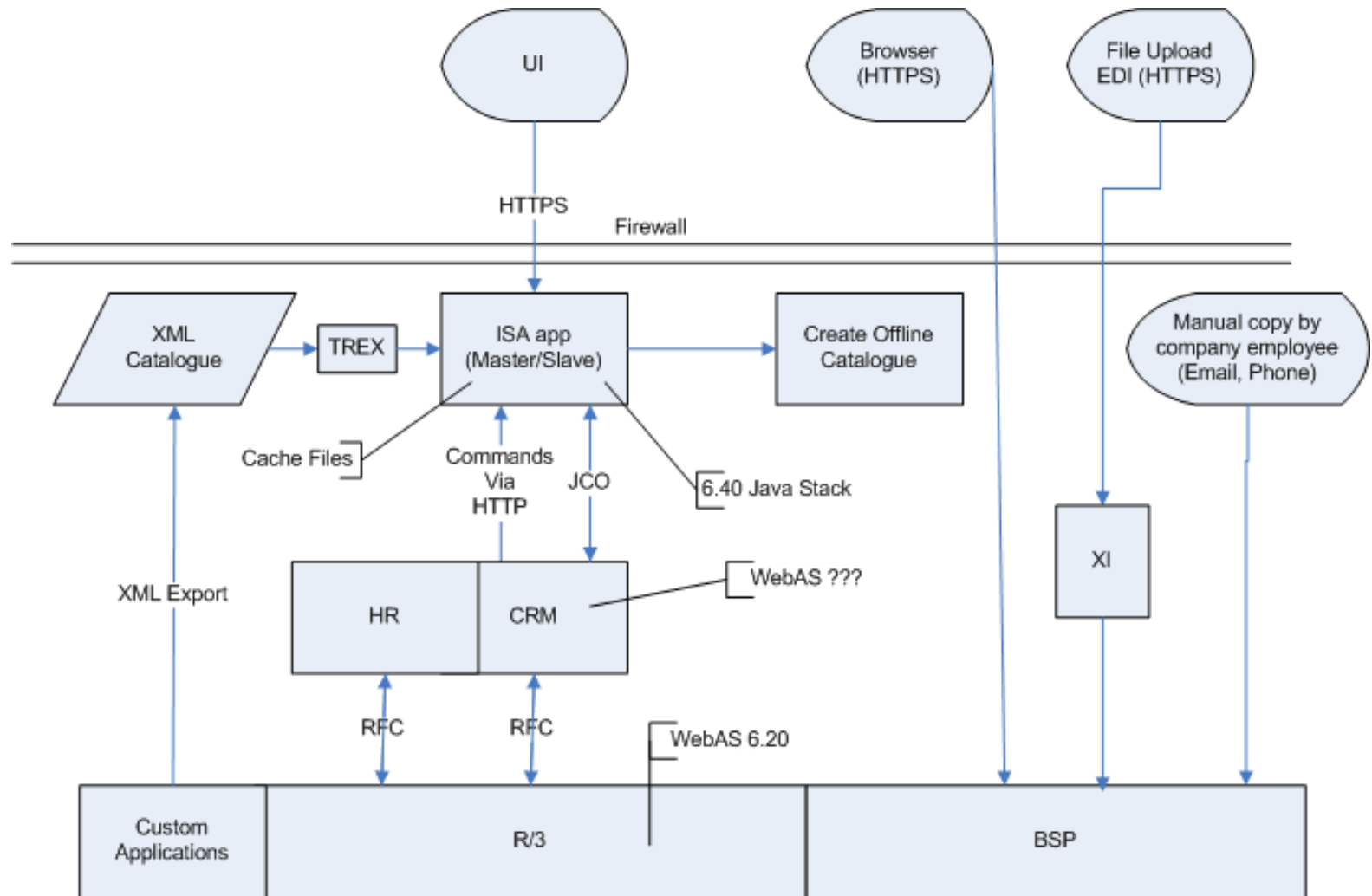
Common Security Vulnerabilities



Additional functionality:

- Unknown functionality
- Not documented
- Hard to discover
- Don't show up during normal usage
- Surprising effects

Common Security Vulnerabilities



Common Security Vulnerabilities

Problems:

- **SAP architectures very complex**
- **You had no security incidents because...**
 - ◆ ... your application landscape is secure?
 - ◆ ... the hacker covered the tracks?
 - ◆ ... nobody bothered so far to look for vulnerabilities?

→ How can you reasonably protect your business data?

Agenda

- Common Security Vulnerabilities
- **Threat Modelling**
- Measuring security
- How can I improve my security performance?

Threat Modelling

**XSS... XSRF...
Input Validation...**

**ROI...
Revenue**



**Governance...
Risk...
Compliance...**



Threat Modelling

- **Threat Modelling creates a common language for security experts and business people**
- **Find business impact of security vulnerabilities**
- **Prioritise applications by criticality**

Threat Modelling

- **Cost-Benefit analysis from an attacker viewpoint**

Cost
Time needed for attack
Skill needed for attack
Probability of getting caught

Benefit
Industrial espionage
Blackmail
Repudiation

Targets are interesting for an attacker if
Cost of attack << Benefit of successful attack

Threat Modelling

Analysis from the viewpoint of companies

- **Focus on applications that**
 - ♦ **have a large attack surface**
 - ♦ **process critical business data**
- **Intranet applications are as exposed as Internet applications!**

Threat Modelling

- **Determine threats your applications face**
 - List the *assets* of your company
 - How are these assets *processed* digitally by your applications? (→ Processes)
 - *Who* uses the applications to work with the company's assets? (→ Actors)

Threat Modelling

- **Assets**
 - ◆ Employee data (e.g. SSN)
 - ◆ Customer data (e.g. Credit Card Data)
- **Process**
 - ◆ Online Recruiting
 - ◆ Online shop (order form, edit customer data)
- **Actors**
 - ◆ HR Department
 - ◆ Customers, shipping department

Threat Modelling

Example:

- **Asset:** Private data of customers (e.g. *CC data*)
- **Process:** *A registered user edits the private data in the web form*
- **Threats**
 - *A registered user views private data of other customers by tampering with the form's request*
 - *A registered user edits private data of other customers*
 - *An attacker may steal credentials or sessions of logged on users*

Agenda

- Common Security Vulnerabilities
- Threat Modelling
- **Measuring security**
- How can I improve my security performance?

Measuring Security

People thinking about security

- “Yes, others have issues, we read that in the news – but not here.” → How do you know?
- “We haven’t been attacked so far.” → How can you tell?
- “We use a firewall and IDS.” → Is that enough?
- “This is a feature, not a defect!” → What is the impact?
- “This is the responsibility of the development consultants” → How secure is your code?

Measuring Security

Why measure security?

- Find your strengths and weaknesses
- Measure improvement in secure development
- Benchmark subcontractors
- Compare your values to market averages (“What security league are you playing in?”)
- Motivate for secure development

Measuring Security



There is an 80% risk that a child hit by a car driving at 40 mph hour will be killed

There is an 80% chance that a child hit by a car driving at 30 mph would survive

People now drive slower as a result

Smoking ban reduces likelihood of heart attacks ...

After the smoking ban in all public places in Scotland in 2006, hospital admissions due to heart attacks are down a whopping 17%.

- That's how security metrics should be ←
- *shaping behaviour and not just being interesting!* ←

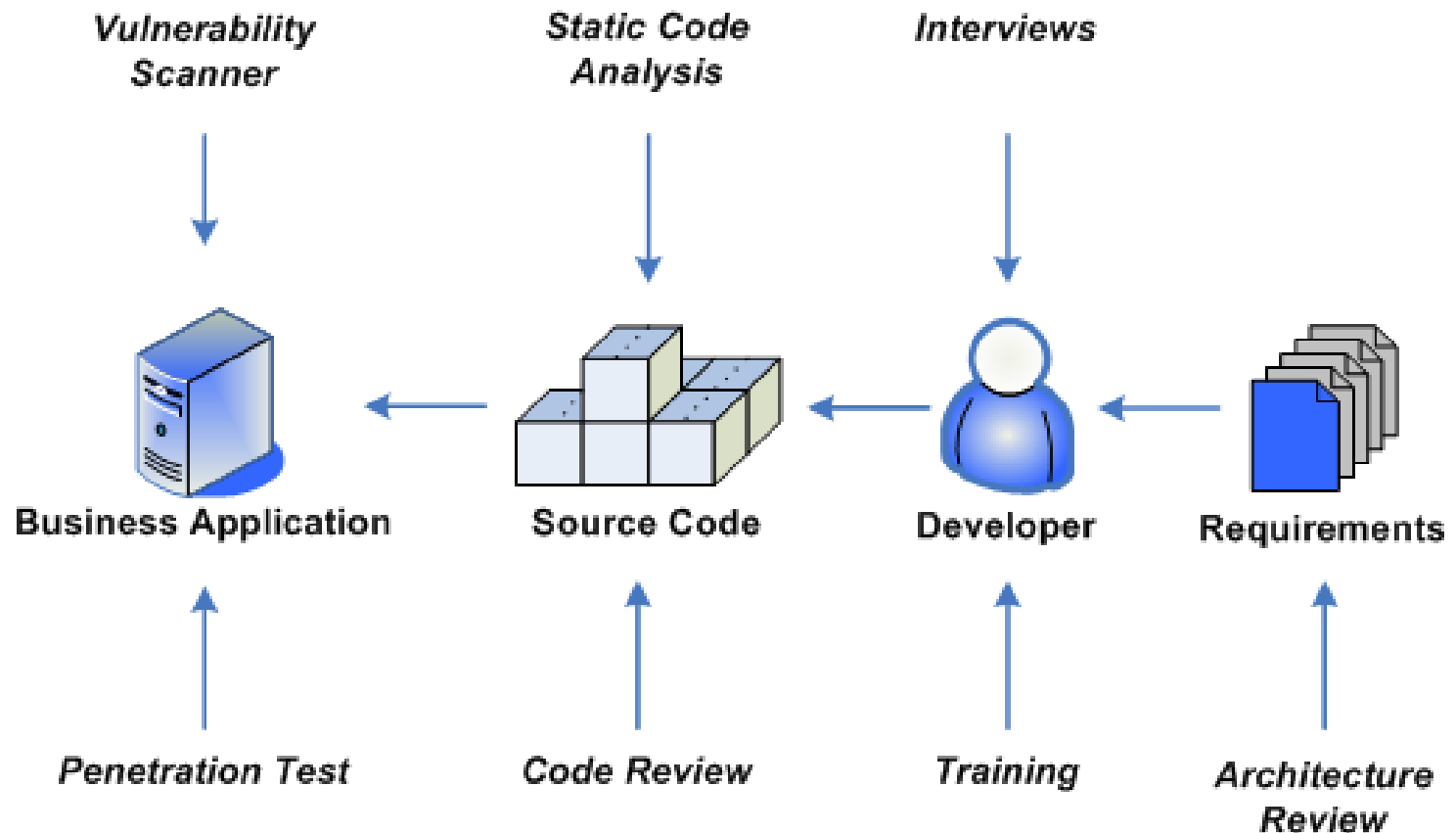
Measuring Security

Recall

- **Secure code is the *real* line of defence**
- **Metrics should change behaviour**
- **Software Security Metrics should lead to secure software!**
- **Change behaviour of**
 - **Customers**
 - **Vendors**
 - **Consultants**
 - **Developers, ...**

Measuring Security

Different levels of measurement



Agenda

- Common Security Vulnerabilities
- Threat Modelling
- Measuring security
- **How can I improve my security performance?**

How Can I Improve My Security Performance

- **Rank entries in threat model**
 - Determine the most critical threats to your business assets
 - Determine threats that are easy to mitigate (easy wins)
- **Perform a security assessment (external security experts)**
 - Peer reviews are not efficient
 - Find security vulnerabilities in applications that are involved with critical threats
 - Determine root causes of vulnerabilities (faulty input validation, faulty output encoding, faults in application design, misuse of frameworks and libraries)
- **Map found vulnerabilities to threats in the threat model**
 - E.g.: XSS --> *“An attacker may steal credentials or sessions of logged on users”*

How Can I Improve My Security Performance

The aftermath:

- **Rank the vulnerabilities that were found during the assessment**
 - ◊ What are the most critical vulnerabilities?
 - ◊ What vulnerabilities are easy to fix (quick wins)
- **What are the root causes of the vulnerabilities?**
 - ◊ Coding flaws
 - ◊ Architecture design flaws
 - ◊ Flaws in business logic
 - ◊ ...

How Can I Improve My Security Performance

The aftermath (cont):

- **Fix it!**
 - **Fix easy wins immediately**
 - **Create plan about how to mitigate the most critical threats as soon as possible**
- **Create road map for Security Assurance**
 - **Train software architects for secure software application design**
 - **Train developers for security development guidelines and best practices**
 - **Include regular security assessments in your development lifecycle**
 - **Incorporate managed security services (e.g. regular scans of coding for trivial security vulnerabilities)**

Conclusion

- **Security incidents happen regularly**
- **SAP application landscapes are very complex, thus difficult to build securely**
- **Use Threat Modelling to find the risks to your assets**
- **Measure security to improve security**
- **Create a road map for security assurance**

3 Key Points to Take Home

“Complexity is the worst enemy of security” (Schneier)

Measure security to improve security

Security can only be successful when it is an ongoing process. One-time efforts are not effective.

QUESTIONS?

Sebastian Schinzel

Sebastian.Schinzel@virtualforge.de

Threat Modelling

- **Add further information to the threats**
 - ◆ **Business impact of**
 - ◆ **Level of exposure**
 - ◆ **Affected users**
 - ◆ **Damage potential**
 - ◆ **Exploitability**