Practical pentesting of ERP’s and business applications

Alexander Polyakov
CTO in ERPScan
Alexey Tyurin
Director of consulting department in ERPScan
Alexander Polyakov

- CTO of ERPScan
- EBASS (OWASP-EAS) project leader
- Business application security expert
- R&D Professional of the year by Network Products Guide
- Organizer of ZeroNights conference

@sh2kerr
Alexey Tyurin

- Director of consulting in ERPScan
- XML/WEB/Network security fun
- Hacked a lot of online banking systems
- Co-Organizer of Defcon Russia Group
- Editor of “EasyHack” column for the “Xakep” magazine

@antyurin
• Developing software for SAP security monitoring
• Leader by the number of acknowledgements from SAP
• Invited to talk at more than 35 key security conferences worldwide (BlackHat, RSA, Defcon, HITB)
• First to develop software for NetWeaver J2EE assessment
• The only solution to assess all areas of SAP Security
• Multiple awards winner

Leading SAP AG partner in the field of discovering security vulnerabilities by the number of found vulnerabilities
Agenda

• Business applications
• EBASS (OWASP-EAS)
• ERP Pentesting approach
• Pentesting SAP NetWeaver JAVA
• Pentesting Oracle PeopleSoft
All business processes are generally contained in ERP systems. Any information an attacker, be it a cybercriminal, industrial spy or competitor, might want is stored in the company’s ERP. This information can include financial, customer or public relations, intellectual property, personally identifiable information and more. Industrial espionage, sabotage and fraud or insider embezzlement may be very effective if targeted at the victim’s ERP system and cause significant damage to the business.
Espionage

• Financial Data, Financial Planning (FI)
• HR Data, Personal, Contact Details (HR)
• Customer Lists
• Corporate Secrets (PLM)
• Supplier Tenders (SRM)
• Customer Lists (CRM)

Cyber criminals need only to gain access to one of the described systems to successfully steal critical information.
Sabotage

- Denial of service
  - Incurs huge costs
- Data modification to cause damage
  - Delete critical information
- SCADA connections
  - Common to see connections between ERP and SCADA
SAP security threats

Fraud

- Manipulate automated transaction systems
- Generate false payments
- Transfer money

Association of Certified Fraud Examiners estimates that corporations, on average, lose 7% of revenue to fraud
Business application security

- **Complexity**
  Complexity kills security. Many different vulnerabilities in all levels, from network to application

- **Customization**
  Cannot be installed out of the box. They have many (up to 50%) custom codes and business logic

- **Risky**
  Rarely updated because administrators are scared they can be broken during updates; also, it is downtime

- **Unknown**
  Mostly available inside the company (closed world)

ERP Pentesting Approach
EASSEC (OWASP-EAS)

- Enterprise Application Software Security project
- Founded in 2010 as OWASP-EAS
- Published concept and top 10 issues for different areas
- Rebranded to EASSEC in 2013 and updated
- Because it is much more than WEB
- Compliance for SAP NetWeaver ABAP planned for July 2013

Exists to provide guidance to people involved in the procurement, design, implementation or sign-off of large scale (i.e. 'Enterprise') applications.

[http://eas-sec.org](http://eas-sec.org)
• Network Implementation issues (EASSEC-NI-9-2013)
• OS Implementation issues (EASSEC-OI-9-2013)
• Database Implementation issues (EASSEC-NI-9-2013)
• Application Implementation issues (EASSEC-AI-9-2013)
• Frontend Implementation issues (EASSEC-CI-9-2013)
1 Insecurely configured Internet facing applications
2 Vulnerable or default configuration of routers
3 Lack of proper network filtration between EA and Corporate network
4 Lack or vulnerable encryption between corporate net and EA Network
5 Lack of frontend access filtration
6 Lack of encryption inside EA Network
7 Lack of separation between Test, Dev, and Prod systems
8 Insecure wireless communications
9 Lack or misconfigured network monitoring
1 Missing 3rd party software patches
2 Missing OS patches
3 Universal OS passwords
4 Unnecessary enabled services
5 Lack of password lockout/complexity checks
6 Unencrypted remote access
7 Insecure trust relations
8 Insecure internal access control
9 Lacking or misconfigured logging
1 Default passwords for DB access
2 Lack of DB patch management
3 Remotely enabled additional interfaces
4 Insecure trust relations
5 Unencrypted sensitive data transport
6 Lack of password lockout and complexity checks
7 Extensive user and group privileges
8 Unnecessary enabled DB features
9 Lacking or misconfigured audit
1. Lack of patch management
2. Default passwords
3. Unnecessary enabled functionality
4. Remotely enabled administrative services
5. Insecure configuration
6. Unencrypted communications
7. Internal access control and SoD
8. Insecure trust relations
9. Monitoring of security events
ERP pentesting features

• Deeper knowledge of ERP than normal systems required
• ERP systems are mission critical and cannot be accidentally taken down (POC exploits are too dangerous)
• Gaining shell / command exec is not the goal
  – The goal is access to sensitive data or impact to business processes
Deeper knowledge

• Higher difficulty than standard pentests
• Required knowledge of:
  – Business processes
  – Business logic
  – Exploit testing impact risk assessment
  – High end databases
  – Numerous (sometimes esoteric) operating systems
  – Different hardware platforms
  – Common custom implementations

ERPScan — invest in security to secure investments
Exploitation

• Exploit code is not easily weaponized for ERP

• Payloads have to be adapted
  – Numerous hardware, OS, release version, and DB systems to generate payloads for
  – In some cases, up to 50 different shellcode variations

• Building a test environment is nearly impossible
  – Takes an expert a week to properly install each variation
  – A year to build a comprehensive test environment
• A better approach required with focus on
  – Architecture
  – Business logic
  – Configuration

  You will get administrator access to business data

• Rather than
  – Program or memory vulnerabilities

  You will probably gain access to OS and then need to obtain access to Application
<table>
<thead>
<tr>
<th>Program vulnerabilities:</th>
<th>Architecture flaws:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Can be patched quickly</td>
<td>+ Harder to patch and harder to re-design (old design – in production for 10 years)</td>
</tr>
<tr>
<td>- Need to write &amp; test numerous payloads</td>
<td>+ One vulnerability – one exploit</td>
</tr>
<tr>
<td>- After gaining OS shell you still need to access data</td>
<td>+ Direct access to application and API (mostly)</td>
</tr>
<tr>
<td>+ Easier to find</td>
<td>- Harder to find (deeper knowledge on the system required)</td>
</tr>
</tbody>
</table>
Architecture issues

- Information disclosure
- Authentication bypass
  - This is often provided non-privileged access
- Improper Access Control
  - This area is mostly covered by Segregation of Duties
- Undocumented Functionality
  - ERPs have many functions created for debug or left over from old versions
- Dangerous Functionality
  - Can be improperly restricted by user accounts with default passwords
- Insecure Trust Relations
  - It is very common to escalate privileges to another system
ERPScan's Pentesting Tool is a freeware tool that is intended for penetration of ERP systems using Black Box testing methods.

- Previous version 0.6 released in 2012 (41 module for SAP).
- Version 1.0 will be released after the BlackHat conference and will contain ~60 modules and tools for SAP and PeopleSoft.

Using ERPScan's SAP Pentesting Tool, you can:

- Obtain information using information disclosure vulnerabilities;
- Exploit potential vulnerabilities;
- Collect business critical data for reports;

* ERPScan's SAP Pentesting Tool is NOT a demo or part of the professional product called ERPScan Security Monitoring Suite. It is just a number of Perl scripts for penetration testers.
Pentesting SAP NetWeaver J2EE
• The most popular business application
• More than 120000 customers worldwide
• 74% of Forbes 500 companies run SAP
• Main system – ERP
• 3 platforms
  • NetWeaver ABAP
  • NetWeaver J2EE
  • BusinessObjects

INNOVATIVE COMPANIES LEAD THE CHARGE
“50 MOST INNOVATIVE COMPANIES”

- SONY
- JPMorganChase
- NIKE
- IBM
- Coca-Cola
- McDonald’s
- Nestle
- Johnson & Johnson
- Amazon
- P&G
- Samsung
- Walmart
- Southwest Airlines
- Volkswagen
- BMW
- Intel
- Apple
- 3M
- Shell
- Verizon
- AT&T
- ExxonMobil
- RIM

erpscann.com

ERPScan — invest in security to secure investments

26
• Additional platform
• Base platform for IT stuff. Like:
  • SAP Portal, SAP XI, SAP Solution Manager, SAP Mobile, SAP xMII
• Purpose: Integration of different systems
• If compromised:
  • Stopping of all connected business processes
  • Fraud
  • Industrial espionage
SAP for users

- Client-server application  SAP-GUI with proprietary DIAG protocol
- Main functions:
  - transactions executed in SAPGUI
  - calling special background functions (RFC) remotely
  - modifying code of transactions or RFC functions using ABAP language
  - using web interfaces like Web Dynpro or BSP in some applications, like SRM
By May 2013, 2600 notes
J2EE platform architecture
## J2EE platform services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port Number</th>
<th>Default Value</th>
<th>Range (min-max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enqueue server</td>
<td>32NN</td>
<td>3201</td>
<td>3200-3299</td>
</tr>
<tr>
<td>HTTP</td>
<td>5NN00</td>
<td>50000</td>
<td>50000-59900</td>
</tr>
<tr>
<td>HTTP over SSL</td>
<td>5NN01</td>
<td>50001</td>
<td>50001-59901</td>
</tr>
<tr>
<td>IIOP</td>
<td>5NN07</td>
<td>50007</td>
<td>50007-59907</td>
</tr>
<tr>
<td>IIOP Initial Context</td>
<td>5NN02</td>
<td>50002</td>
<td>50002-59902</td>
</tr>
<tr>
<td>IIOP over SSL</td>
<td>5NN03</td>
<td>50003</td>
<td>50003-59903</td>
</tr>
<tr>
<td>P4</td>
<td>5NN04</td>
<td>50004</td>
<td>50004-59904</td>
</tr>
<tr>
<td>P4 over HTTP</td>
<td>5NN05</td>
<td>50005</td>
<td>50005-59905</td>
</tr>
<tr>
<td>P4 over SSL</td>
<td>5NN06</td>
<td>50006</td>
<td>50006-59906</td>
</tr>
<tr>
<td>Telnet</td>
<td>5NN08</td>
<td>50008</td>
<td>50008-59908</td>
</tr>
<tr>
<td>Log Viewer control</td>
<td>5NN09</td>
<td>50009</td>
<td>50009-59909</td>
</tr>
<tr>
<td>JMS</td>
<td>5NN10</td>
<td>50010</td>
<td>50010-59910</td>
</tr>
</tbody>
</table>
Prevention:

- Deny access to open ports from users subnet (except 5NN00). Only administrators must have access.
- Disable unnecessary services
• **UME: User management engine.** Using UME, you can manage all user data through web interface:  
   [http://server:port/useradmin](http://server:port/useradmin)

• **SPML: Service Provisioning Markup Language (SPML).** A new unified interface for managing UME:  
   [http://server:port/spml/spmlservice](http://server:port/spml/spmlservice)
Authentication

- **Declarative authentication:**
  - The Web container (J2EE Engine) handles authentication
  - Example: J2EE Web applications

- **Programmatic authentication.**
  - Components running on the J2EE Engine authenticate directly against User Management Engine (UME) using the UME API.
  - Example: Web Dynpro, Portal iViews
J2EE Engine services

- SAP NetWeaver HTTP (webserver)
- SAP Visual Admin (P4)
- SAP J2EE Telnet
- SAP Log Viewer
- SAP Portal
- SAP SDM
SAP HTTP Services can be easily found on the Internet:

- `inurl:/irj/portal`
- `inurl:/IciEventService sap`
- `inurl:/IciEventService/IciEventConf`
- `inurl:/wsnavigator/jsp/test.jsp`
- `inurl:/irj/go/km/docs/`
A lot of results

ERPScan — invest in security to secure investments
Vulnerabilities

• Information disclose
• SMBRelay
• XSS
• CSRF
• Auth bypass Verb Tampering
• Auth bypass Invoker Servlet
• XXE/SSRF
SAP NetWeaver web server

• Application service with J2EE support
• It is like Apache Tomcat but 100 times more complex
• Supports different SAP web service types:
  • Web Dynpros
  • JSPs
  • J2EE web applications
  • Java Beans
  • SOAP web services
  • Portal iViews
• By default, a lot of test applications installed
Demonstration of attacks by ERPScan Pentesting Tool

- Information disclosure
- CTC web service auth bypass
- Log Viewer attacks
- P4 password decryption
- Breaking connected ABAP systems
Information disclosure

- Kernel or application release and SP version.
  DSECRG-11-023, DSECRG-11-027, DSECRG-00208

- Application logs and traces
  DSECRG-00191, DSECRG-11-034

- Username
  DSECRG-12-028

- Internal port scanning, Internal user bruteforce
  DSECRG-11-032, DSECRG-00175
**Software Build information of DM0 - REPOSITORY**

<table>
<thead>
<tr>
<th>Name of property</th>
<th>Value of property</th>
</tr>
</thead>
<tbody>
<tr>
<td>make.rel</td>
<td>NW04S_06_REL</td>
</tr>
<tr>
<td>SP-Number</td>
<td>06</td>
</tr>
<tr>
<td>jdk.version</td>
<td>1.3</td>
</tr>
<tr>
<td>latest.change</td>
<td>10491</td>
</tr>
<tr>
<td>sync.time</td>
<td>2006-03-04 20:19</td>
</tr>
<tr>
<td>build.date</td>
<td>2006-03-04 20:19</td>
</tr>
</tbody>
</table>
**Business Communication Broker - System Information**

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCB/ICI version</td>
<td>3.00.64507</td>
</tr>
<tr>
<td>SAP J2EE Engine</td>
<td>SAP J2EE Engine/7.00 PatchLevel with 2 cluster elements (1 dispatcher and 1 servers)</td>
</tr>
<tr>
<td>1. connection</td>
<td>SAP Contact Center Simulator 3.00.64507</td>
</tr>
</tbody>
</table>
Prevention

• Install SAP notes: 1503856, 1548548, 581525, 1503856, 1740130, 948851, 1619539, 1545883
• Update the latest SAP notes every month
• Disable unnecessary applications
WEB.XML file is stored in WEB-INF directory of application root.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Restrictedaccess</web-resource-name>
    <url-pattern>/admin/**</url-pattern>
    <http-method>DELETE</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>admin</role-name>
  </auth-constraint>
</security-constraint>
```
CTC authentication bypass

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>RestrictedAccess</web-resource-name>
    <url-pattern>/admin/*</url-pattern>
    <http-method>GET</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>admin</role-name>
  </auth-constraint>
</security-constraint>
```

What if we use HEAD instead of GET?
CTC authentication bypass

• Must use the security control that lists HTTP verbs (DONE)
• Security control fails to block verbs that are not listed (DONE)
• GET functionality will be executed with an HEAD verb (DONE)
• SAP NetWeaver J2EE engine has all these features!!!
CTC authentication bypass

- Administrative interface for managing J2EE engine (CTC)
- Can be accessed remotely
- Can run user management actions
  - Create new users
  - Assign any roles to them
  - Execute OS commands on the server side
  - Create RFC destinations
  - Read RFC destinations info
DEMO
Prevention:

- Install SAP notes 1503579, 1616259, 1589525, 1624450
- Scan applications using ERPScan WEB.XML check tool or manually
- Secure WEB.XML by deleting all `<http-method>`
- Disable application that are not necessary
• SAP Visual Admin: a remote tool for controlling J2EE Engine
• Uses the P4 protocol – SAP’s proprietary
• By default, all data transmitted in cleartext
• P4 can be configured to use SSL to prevent MitM
• Passwords transmitted in some sort of encryption
• In reality, it is some sort of Base64 transform with known key
/* 87 */ char mask = 43690;
/* 88 */ char check = 21845;
/* 89 */ char[] result = new char[data.length + 1];
/* */
/* 91 */ for (int i = 0; i < data.length; ++i) {
/* 92 */ mask = (char)(mask ^ data[i]);
/* 93 */ result[i] = mask;
/* */
/* 95 */ result[data.length] = (char)(mask ^ check);
/* */
/* 97 */ return result;
DEMO
Prevention:

- Use SSL for securing all data transmitting in server-server and server-client connections

http://help.sap.com/saphelp_nwpi71/helpdata/de/14/ef2940cbf2195de100000000a1550b0/content.htm
• LogViewer: a special service which can be manually enabled in an SAP system.
• If LogViewer-standalone is installed on SAP server, attacker can try to remotely register a log file by console command `register_log.bat`
• No authentication needed
• This option can be used for SMBRelay attack
• Port address can be 50109 or 5465 or any custom
DEMO
Prevention:

- Install SAP note 1685106
- Disable applications that are not necessary
Breaking connected ABAP systems

- Major part of penetration testing is post-exploitation
- NetWeaver J2EE connected with ABAP stack of other systems by RFC protocol
- Authentication data for those connections are stored in J2EE Engine and can be obtained by using API
- To do that, you need to upload a special service which will call internal functions for obtaining access to RFC connections.
- In most cases, those connections are configured with privileged users

RFC is an SAP interface protocol, which simplifies the programming of communication processes between systems
public void getUsers(String _file)
   throws Exception
{
    ClassLoader origClassLoader = Thread.currentThread().getContextClassLoader();
    Thread.currentThread().setContextClassLoader(getClass().getClassLoader());

    InitialContext ctx = new InitialContext();

    Object obj = ctx.lookup("rfcengine");
    RFCRuntimeInterface runtime = (RFCRuntimeInterface)ctx.lookup("rfcengine");
    BundleConfiguration bundle = new BundleConfiguration();
    String text = "Users: \n\n";
    BundleConfiguration[] bundles = runtime.getConfigurations();
    for (int i = 0; i < bundles.length; i++)
    {
        text = text + "LogonUser \t" + bundles[i].getLogonUser() + "\n";
        text = text + "LogonPassword \t" + bundles[i].getLogonPassword() + "\n";
        text = text + "SystemNumber \t" + bundles[i].getSystemNumber() + "\n";
        text = text + "LogonClient \t" + bundles[i].getLogonClient() + "\n\n";
    }
    save(text, _file);
    Thread.currentThread().setContextClassLoader(origClassLoader);
}
DEMO
Prevention:

• Install SAP notes 1503579, 1616259
• Disable applications that are not necessary
• Don’t store critical accounts in RFC destinations, especially from less critical systems to more critical
Pentesting Oracle Peoplesoft
Agenda

- Introduction to Oracle PeopleSoft
- PeopleSoft Internet Architecture
- Introduction to PeopleSoft Security
- Assessing PeopleSoft using EBASS (OWASP-EAS)
- A lot of DEMOs...
What is it?

- Oracle PeopleSoft Apps: HRMS, FMS, SCM, CRM, EPM
- Can work as one big portal or separately
- Many implementations

DID YOU KNOW?

- 20M+ Employees served by PeopleSoft worldwide
- 6K+ Customers in 54 countries and in 18 languages use PeopleSoft
- 57% Of the Fortune 100 run on PeopleSoft

ERPScan — invest in security to secure investments
• Many applications, but they have one architecture:
• PeopleSoft Internet Architecture
  – Internet oriented since version 8
• Based on several special core technologies.
PeopleTools:

• Technology
• Developer tools
• Framework
• PeopleCode

All of the applications are created using PeopleTools.
PeopleCode:

- object-oriented proprietary (case-insensitive) language
- used to express business logic for PeopleSoft applications.
- PeopleCode syntax resembles other programming languages.
- fundamentals of objects and classes are the same as in Java
PeopleSoft Internet Architecture

- External System
- Web Server
- Application Server
- RDBMS
- Developers 2-Tier
- Developers 3-Tier

Connections:
- HTTP
- JCLT
- SQL
Components:

- Web browser
- Web server
- Application server
- Batch server
- Database server
PeopleSoft Internet Architecture

ERPScan — invest in security to secure investments
PeopleSoft Internet Architecture

- **Web server**
  - WebLogic/WebSphere
  - PS Servlets
  - Forwards request from a browser to an App Server

- **Application server**
  - PS Services + Tuxedo + Jolt
  - Business logic, SQL transaction management, Transport

- **Database server**
  - System Tables, PeopleTools metadata, PeopleSoft application data

ERPScan — invest in security to secure investments

erpscan.com
Another view:

- Weblogic
- Tuxedo
- PeopleSoft Application (HCM, CRM, etc)
- PeopleTools
- DB with Data
• **Users (web browser)**
  - All common web technologies
  - A single escalation point for common and administrative goals

• **Developers (PeopleTools)**
  - 2-Tier – direct connection to DBMS
  - 3-Tier – connection through Application Server. Special ports WSH, WSL.
  Essentially, basic SQL requests which are forwarded to DBMS by Application Server

• **External systems**
  - Different web services (SOAP, XML) for a cross-system integration
PeopleSoft Internet Architecture
Basic role model:

- **Permission Lists**
  - *Permission lists* are the building blocks of user security authorization

- **Roles**
  - A *role* is a collection of permission lists

- **User Profile**
  - The user profile specifies a number of user attributes, including one or more assigned roles
Authentication process and terms:

- User logs in with his User ID and password
- Application Server uses Connect ID to connect to DBMS.
  - This account has limited rights in DBMS. It is used to retrieve the \( u= \)User ID and password, which are then compared to the user’s input
- If successful, the system takes Symbolic ID (associated with) User ID.
- The system uses Symbolic ID to find in PSACCESSPRFL the necessary Access ID and the password. This account is privileged.
- The system reconnects to DBMS using Access ID.

* Passwords are encrypted.
1. Lack of patch management
2. Default passwords
3. Unnecessary enabled functionality
4. Remotely enabled administrative services
5. Insecure configuration
6. Unencrypted communications
7. Internal access control and SOD
8. Insecure trust relations
9. Monitoring of security events
1. Lack of patch management
PeopleSoft Vulns

Some vulns every year, but no info for pentesting...

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Publish Date</th>
<th>Update Date</th>
<th>Score</th>
<th>Gained Access Level</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2013-2410</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>4.0</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise HRMS component in Oracle PeopleSoft Products 9.1.0 allows remote authentication related to Absence Management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-2408</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>4.3</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 also related to PIA Core Technology and use of Internet Explorer 6.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-2404</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>4.3</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all vectors related to Portal.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-2402</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>4.3</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all vectors related to WorkCenter.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-2401</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>3.5</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all unknown vectors related to Portal.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2013-2374</td>
<td>2013-04-17</td>
<td>2013-04-18</td>
<td>4.0</td>
<td>None</td>
<td>Remote</td>
</tr>
<tr>
<td>Unspecific vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all unknown vectors related to Rich Text Editor.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- Old research
- buffer overflow in login process!!!
- we can control the return address
- but stack cookie... so only DoS

* Do you think it is secure Java? No, there are too many crashes 😊
+ a lot of 0-days after our last research *wait until show time*...
A strange finding:
Apache Axis 1.4 is from 2006. Is it not too old?

What about CVE **CVE-2012-5785** or CVE-**2012-4418**, which exist in Axis 2?

Needs deeper testing...
2. Default passwords for application access
Some of them:

• PS:PS – super PS user (also VP1:VP1)
• “password” for many web services
• “dayoff” for a Portal servlet

Ex: psp/[site]/?cmd=viewconfig&pwd=dayoff – to see configs

Different way: non-standard Weblogic accounts:

• system: Passw0rd (password) – main administrator
• operator: password – operator role
• monitor: password – monitor role

* The password of “system” is often changed to that of “PS”
3. Unnecessary enabled application features
Some of PS:
- Business Interlinks
- Integration Gateway
- PeopleSoft Online Library
- PeopleSoft Reporting

Some of WebLogic:
- UDDI Explorer
- WebLogic web services
But much more when we look closely (some of them):
4. Open remote management interfaces
Debug commands for the Portal sevlet:

- `?cmd=viewconfig&pwd=dayoff`
- `?cmd=reloadconfig&pwd=dayoff`
- `?cmd=viewsprop&pwd=dayoff`
- `?cmd=debugCache&pwd=dayoff`
- `?cmd=purge&pwd=dayoff`
- `?cmd=resettimeout&pwd=dayoff`
- `?cmd=resetlog&pwd=dayoff`
- `?cmd=manifestCache&pwd=dayoff`
WebLogic

- WebLogic admin “/console”
- on the same port with PeopleSoft application by default.
- Anyone can try to access the inside with default accounts
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands

wls:/offline> connect('weblogic','***',localhost:7001')
Connecting to t3://localhost:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'web _domain'.
Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

wls:/web_domain/serverConfig> deploy('helloWorld','C:/123.war')
Deploying application from C:\123.war to targets (upload=false) ...
<28.06.2013 13:15:40 MSD> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating deploy operation for application, helloWorld [archive: C:\123.war], to AdminServ er >
.Completed the deployment of Application with status completed
Current Status of your Deployment:

And what about the T3 protocol? remote management interfaces
• Non-default is fine too
• information from SNMP “public”
5. Insecure options
Accounts

- Large enterprise systems.
- There are a lot of accounts which we can bruteforce...
Encryption of password in config files:

- Some passwords of PeopleSoft are stored in plaintext
- Some – 3DES
- Some – AES
Encryption

3DES
- The key for 3DES is standard by default.
- You can check it. The string “{V1.1}” before an encrypted password shows the key is default.
- After each key regeneration, the number is changed (1.2, 1.3...)
- Do you regenerate it?

AES
- If you want to decrypt with AES, you need SerializedSystemIni.dat
- You can understand that it is AES by the “{AES}” string in the beginning of an encrypted password.
7. Unencrypted communications
General problem with communications:

- **User or Remote system to Web Server:**
  HTTP and HTTPS are both used by default in PeopleSoft apps. HTTP has no encryption.

- **Application server to RDBMS and Developer to RDBMS (2-tier):**
  By default, there is no encryption. In some RDBMS (like MS SQL) we can grab credentials very easily.
JOLT (between Application server and RDBMS):
By default, there is no encryption.
Default ports: TCP/9001-9005.
It looks like HTTP traffic, but it’s a little bit weird.
• Developer through Application Server to RDBMS (3-tier)
  By default, there is no encryption.
  Default ports: TCP/7001-7005.
  It looks like plaintext SQL queries.
WSL Request

ERPScan
Security Scanner for SAP

ERPScan — invest in security to secure investments
Conclusion

It is possible to be protected from almost all those kinds of issues and we are working hard to make it secure

Guides

Regular security assessments

Monitoring technical security

Code review

Segregation of Duties

EAS-SEC project
I'd like to thank SAP's Product Security Response Team for the great cooperation to make SAP systems more secure. Research is always ongoing, and we can't share all of it today. If you want to be the first to see new attacks and demos, follow us at @erpscan and attend future presentations:

- September 12-13 SEC-T Conference (Stockholm, Sweden)
- September 21 HackerHalted Conference (Atlanta, USA)
- October 7-8 HackerHalted Conference (Reykjavik, Iceland)
- October 30-31 RSA Europe (Amsterdam, Netherlands)
- November 7-8 ZeroNights (Moscow, Russia)
Greetz to our crew who helped