



ERPScan

Security Scanner for SAP

*Invest in security
to secure investments*

Practical pentesting of ERP's and business applications

Alexander Polyakov


CTO in ERPScan

Alexey Tyurin

Director of consulting department in ERPScan

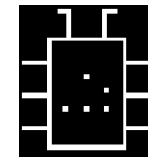


- CTO of ERPScan
- EBASS (OWASP-EAS) project leader
- Business application security expert
- R&D Professional of the year by Network Products Guide
- Organizer of ZeroNights conference

 @sh2kerr



- 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



 @antyyurin



- 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



- 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



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



- **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)

<http://erpscan.com/wp-content/uploads/pres/Forgotten%20World%20-%20Corporate%20Business%20Application%20Systems%20Whitepaper.pdf>



ERP Pentesting Approach



- 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://www.owasp.org/index.php/OWASP_Enterprise_Application_Security_Project
<http://eas-sec.org>



- Network Implementation issues (EASSEC-NI-9-2013)
- OS Implementation issues (EASSEC-OI-9-2013)
- Database Implementation issues (EASSEC-DI-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



- 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



- 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



Shell

Program vulnerabilities:		Architecture flaws:	
-	Can be patched quickly	+	Harder to patch and harder to re-design (old design - in production for 10 years)
-	Need to write & test numerous payloads	+	One vulnerability - one exploit
-	After gaining OS shell you still need to access data	+	Direct access to application and API (mostly)
+	Easier to find	-	Harder to find (deeper knowledge on the system required)



- 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”





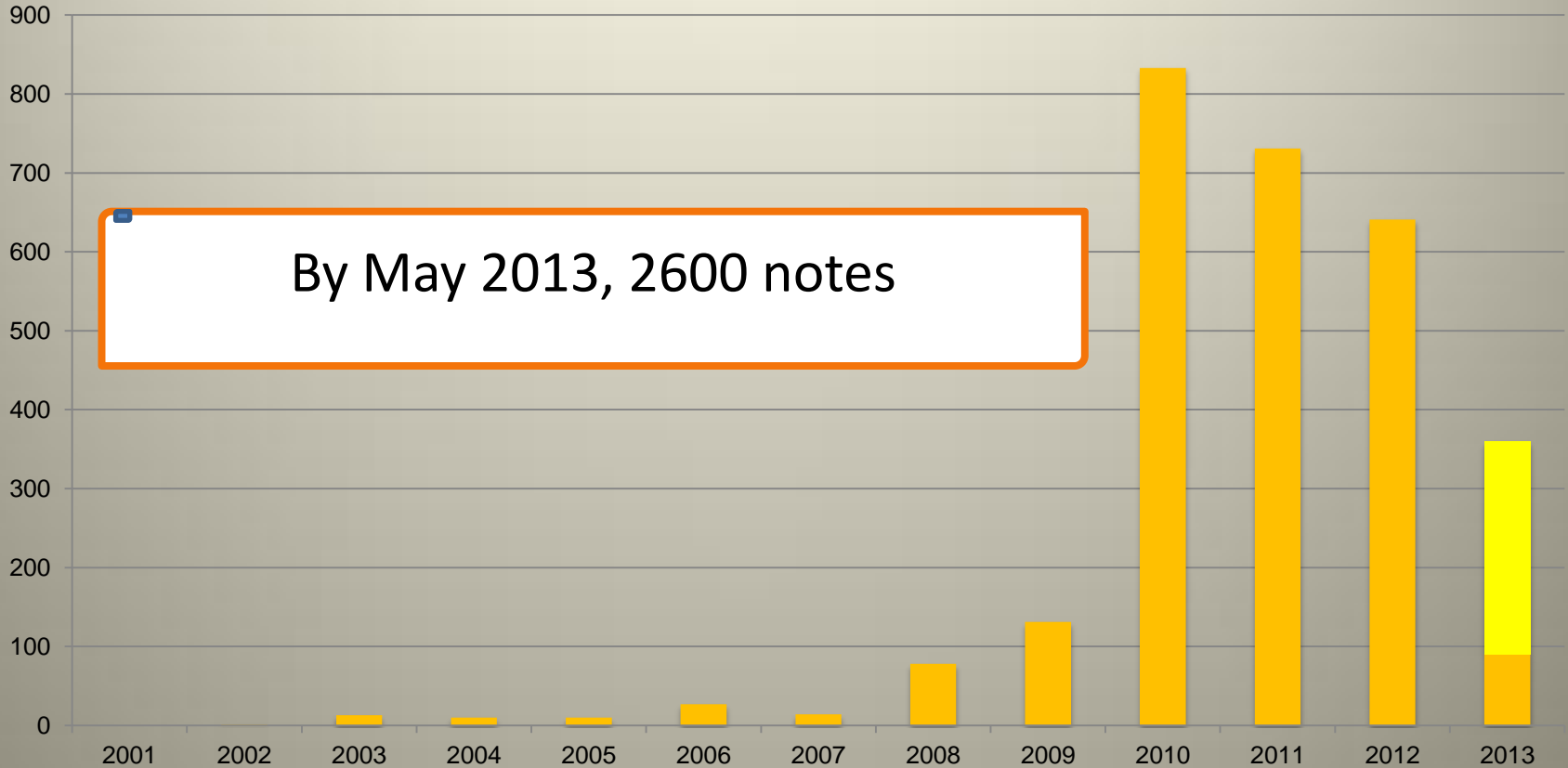
- Additional platform
- Base platform for IT stuff. Like:
 - SAP Portal , SAP XI, SAP Solution Manager, SAP Mobile, SAP xMII
- Purpose: Integration of different systems
- If compromised:
 - Stopping of all connected business processes
 - Fraud
 - Industrial espionage



- 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

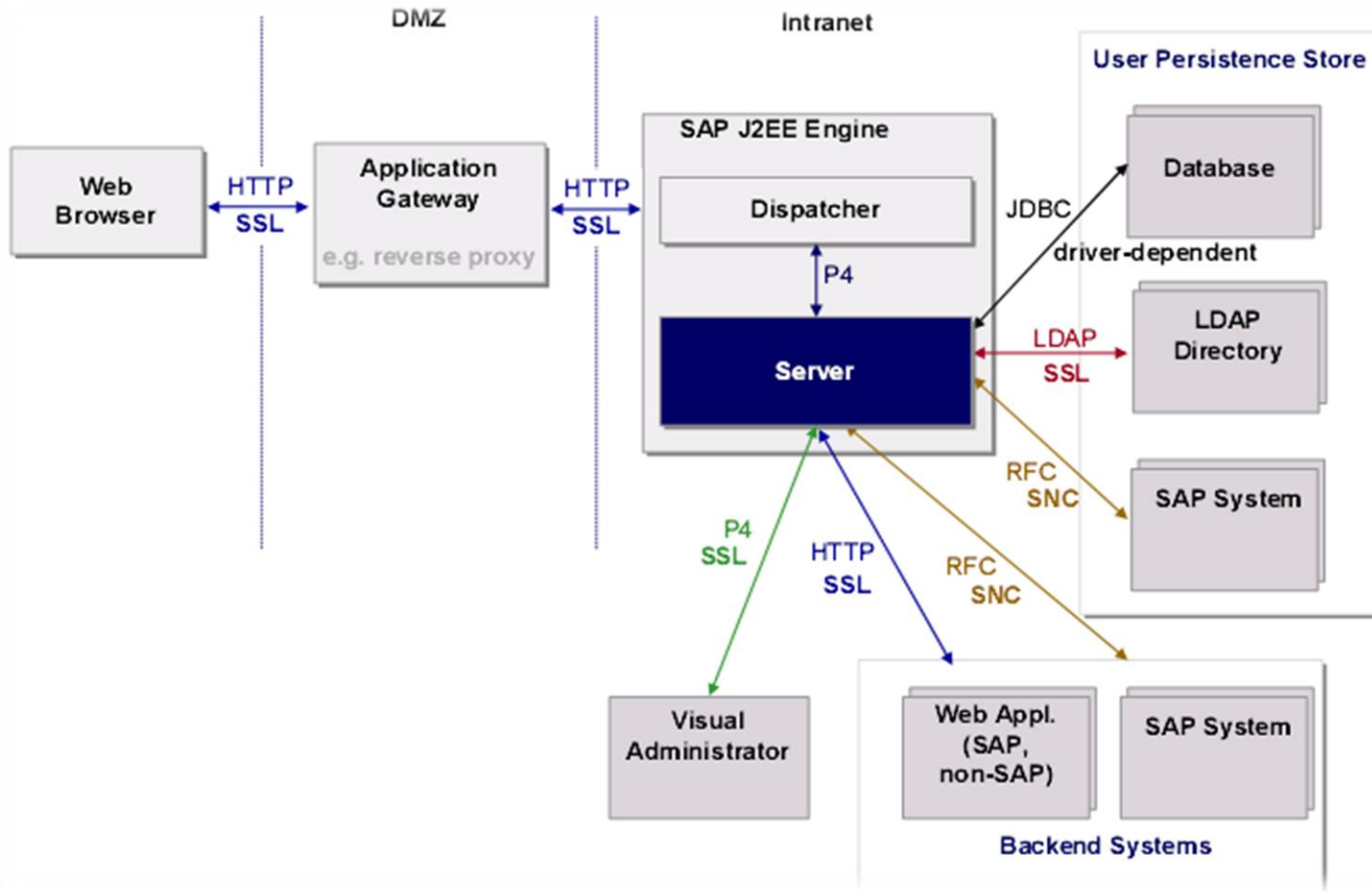


SAP security notes





J2EE platform architecture





J2EE platform services

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



Prevention:

- Deny access to open ports from users subnet (except 5NN00). Only administrators must have access.
- Disable unnecessary services



User management

- **UME: User management engine.** Using UME, you can manage all user data through web interface:
<http://server:port/useradmin>
- **SPML: Service Provisioning Markup Language (SPML).** A new unified interface for managing UME:
<http://server:port/spml/spmlservice>





- **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



- 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/jsps/test.jsp`
- `inurl:/irj/go/km/docs/`



A lot of results

The screenshot shows a Google search results page in Russian. The search query is 'inurl:/irj/portal'. The results are as follows:

- Portal Empresarial de Navantia**
www.navantia.es/irj/portal/anonymous?lang... - Перевести эту страницу [+7]
Navantia es la empresa española líder del sector de la construcción naval militar.
- Tata Motors SRM**
srm.tatamotors.com/irj/portal - Перевести эту страницу [+7]
Вы посещали эту страницу несколько раз (2). Дата последнего посещения: 07.02.11
- SAP Portal: howto avoid irj/portal path to access the portal | Whatsup**
www.martin-english.com/.../sap-portal-howt... - Перевести эту страницу [+7]
27 Nov 2007 – SAP Portal: howto avoid irj/portal path to access the portal.
- Portal FIRA**
www.fira.gob.mx/irj/portal/anonymous - Перевести эту страницу [+7]
No portal roles are assigned for this user.If this problem persists, contact your system administrator. Log Off.



1200 web applications



- 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



- 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



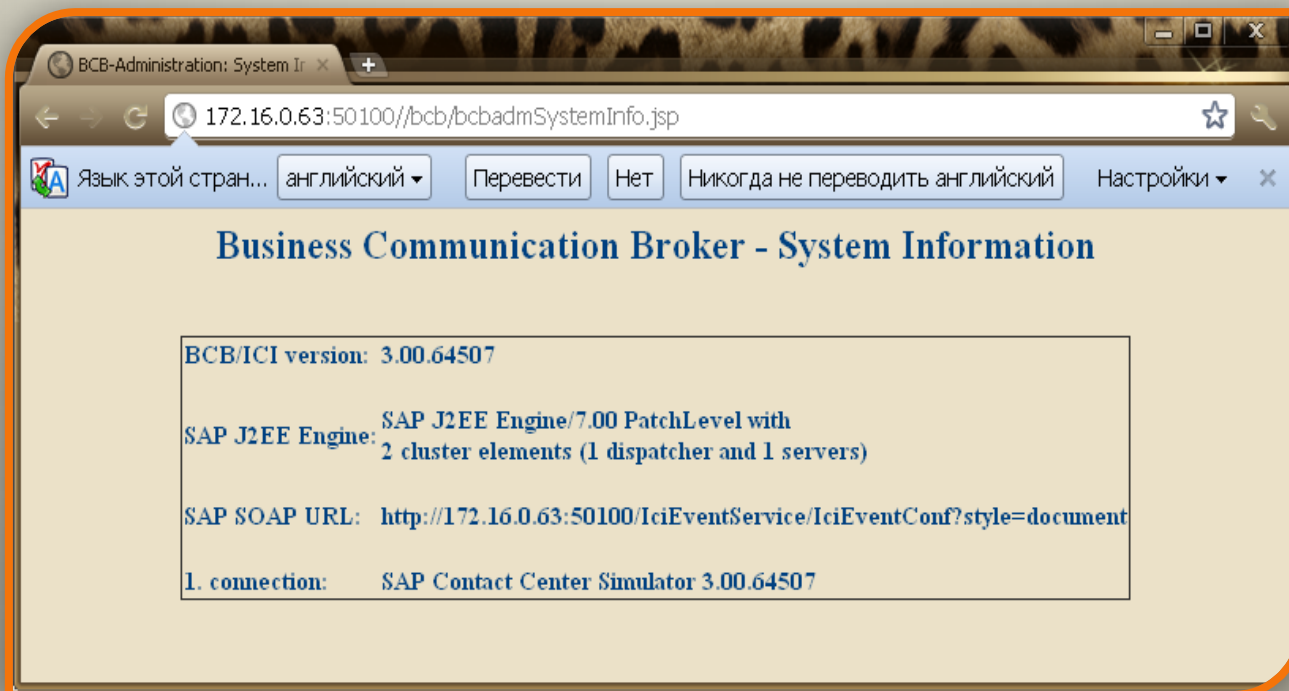
Inf. disclosure in REP (DSECRG-11-023)

The screenshot shows a web browser window with the address bar containing '172.16.0.63:50100/rep/build_info.jsp'. The page title is 'Build information'. The main content is a table titled 'Software Build information of DM0 - REPOSITORY'.

Name of property	Value of property
make.rel	NW04S_06_REL
SP-Number	06
jdk.version	1.3
latest.change	10491
sync.time	2006-03-04 20:19
build.date	2006-03-04 20:19



Inf. disclosure in BCB (DSECRG-11-027)





- 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

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



VisualAdmin protocol

Follow TCP Stream

Stream Content

```

00000674 00 00 00 01 00 00 10 38 c5 00 11 11 11 11 07 00 .....8 .....
00000684 00 00 00 00 00 00 01 2a 00 00 00 01 00 08 00 73 .....* .....S
00000694 65 63 75 72 69 74 79 1c 00 1c 00 00 00 00 00 00 ecurity. ....
000006A4 00 00 4a 00 32 00 45 00 45 00 5f 00 47 00 55 00 ..J.2.E. E_.G.U.
000006B4 45 00 53 00 54 ac ed 00 05 73 72 00 4a 63 6f 6d E.S.T... .sr.Jcom
000006C4 2e 73 61 70 2e 65 6e 67 69 6e 65 2e 73 65 72 76 .sap.eng ine.serv
000006D4 69 63 65 73 2e 73 65 63 75 72 69 74 79 2e 72 65 ices.sec urity.re
000006E4 6d 6f 74 65 2e 6c 6f 67 69 6e 2e 53 65 72 69 61 mote.log in.Seria
000006F4 6c 69 7a 61 62 6c 65 50 61 73 73 77 6f 72 64 43 lizableP asswordc
00000704 61 6c 6c 62 61 63 6b 84 c8 13 98 e5 15 c3 9f 02 allback. ....
00000714 00 03 5a 00 08 69 73 45 63 68 6f 4f 6e 5b 00 08 ..Z..ise choon[..
00000724 70 61 73 73 77 6f 72 64 74 00 02 5b 43 4c 00 06 password t..[CL.
00000734 70 72 6f 6d 70 74 74 00 12 4c 6a 61 76 61 2f 6c promptt. .Ljava/]
00000744 61 6e 67 2f 53 74 72 69 6e 67 3b 78 70 01 75 72 ang/Stri ng;xp.ur
00000754 00 02 5b 43 b0 26 66 b0 e2 5d 84 ac 02 00 00 78 ..[c.&f. .].....x
00000764 70 00 00 00 09 aa c8 aa a4 aa c5 aa a6 aa cd aa p.....
00000774 a5 aa c4 aa b0 ff e5 74 00 0a 50 61 73 73 77 6f .....t ..Passwo
00000784 72 64 3a 20 rd:
  
```

Entire conversation (15696 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close



Insecure password encryption in P4

```
/* 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/ef2940cbf2195de10000000a1550b0/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



Breaking connected ABAP 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



ERPScan
Security Scanner for SAP

Pentesting Oracle Peoplesoft

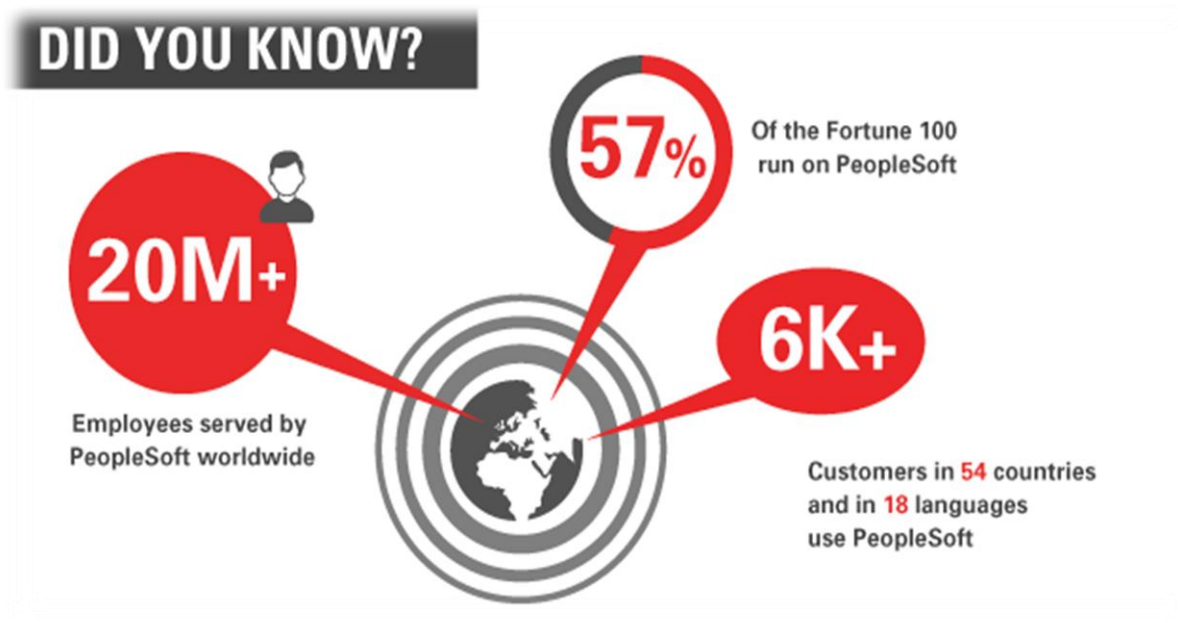


- Introduction to Oracle PeopleSoft
- PeopleSoft Internet Architecture
- Introduction to PeopleSoft Security
- Assessing PeopleSoft using EBASS (OWASP-EAS)
- A lot of DEMOs...



What is it?

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





PeopleSoft Internet Architecture

- 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.

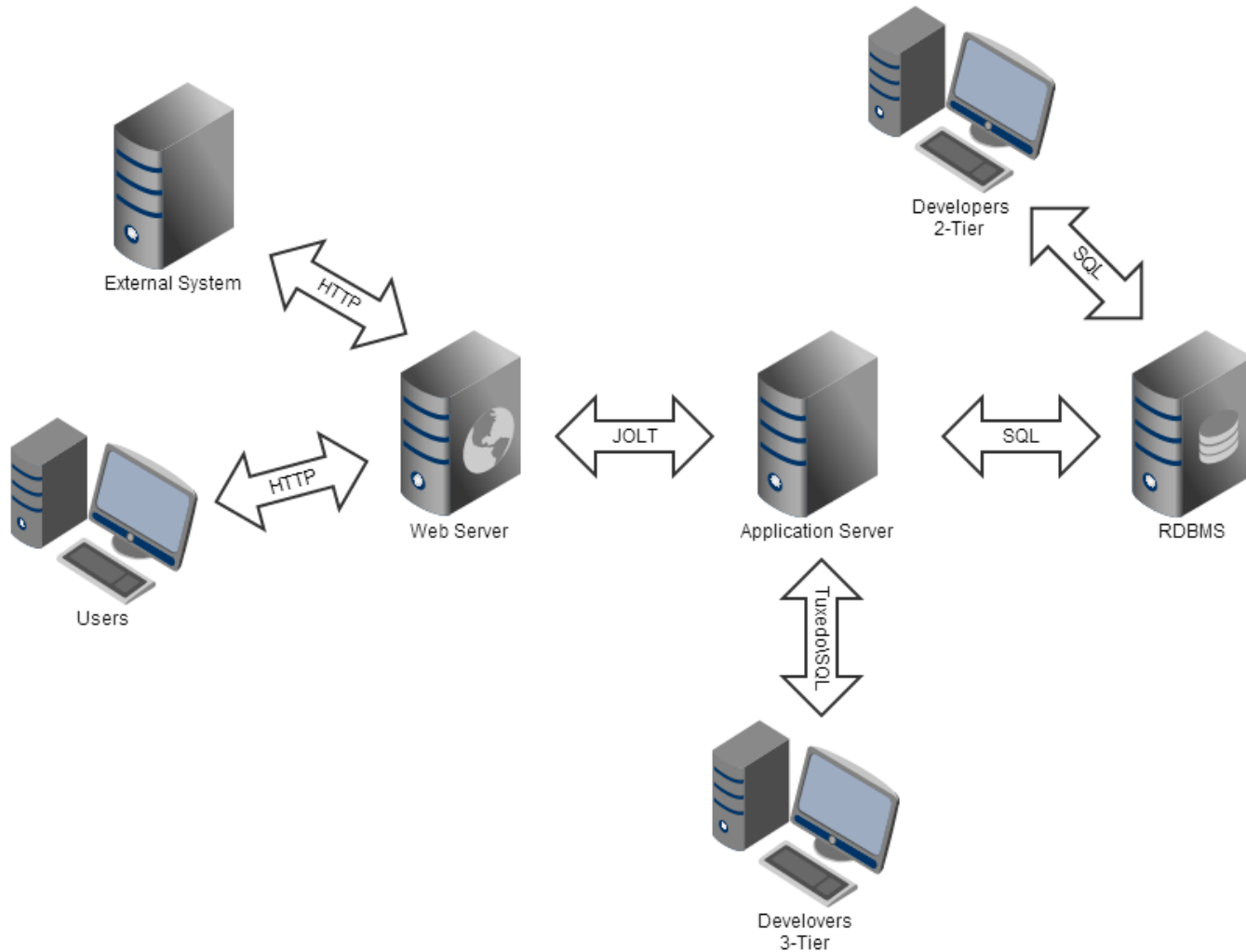


PeopleCode:

- 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



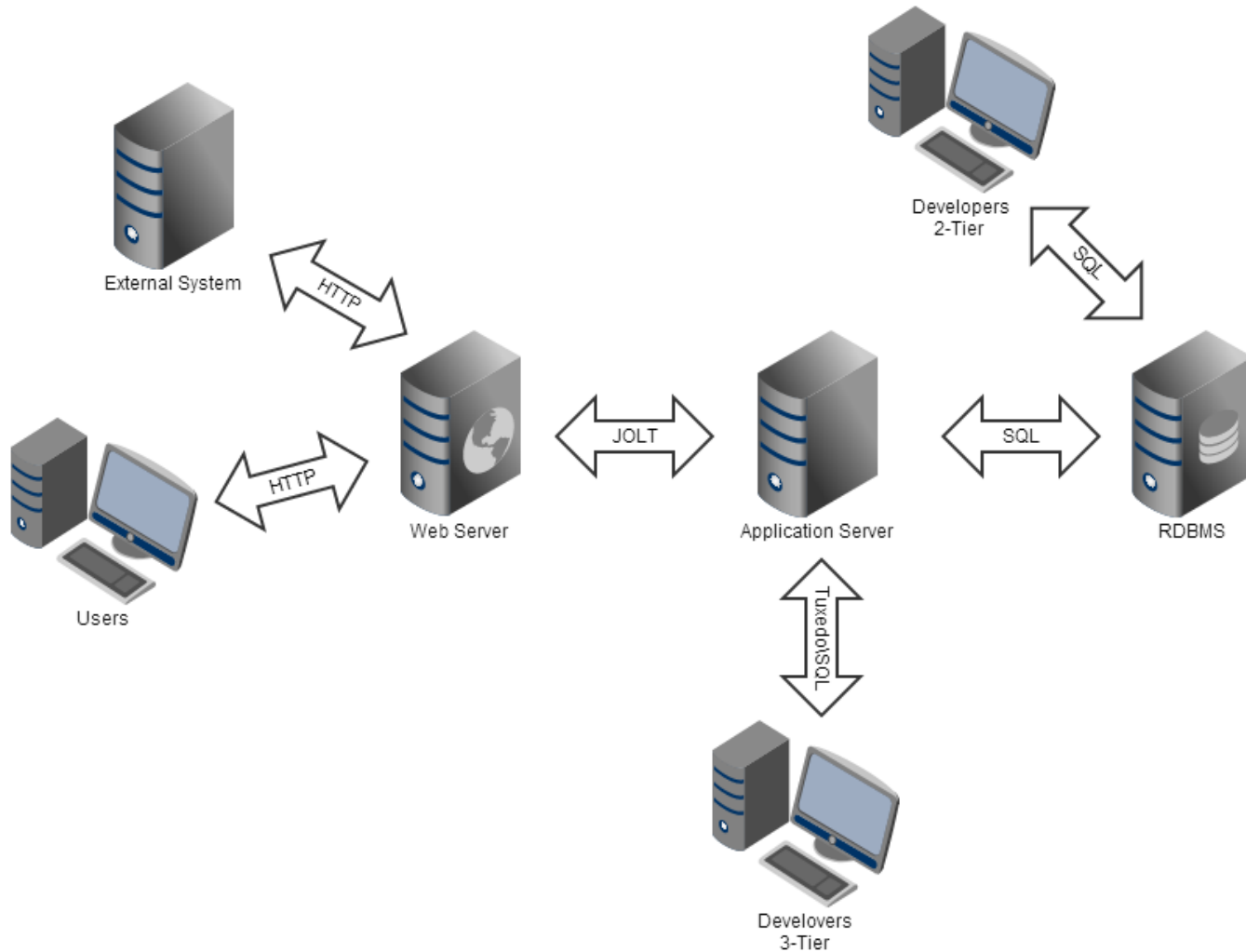


Components:

- Web browser
- Web server
- Application server
- Batch server
- Database server



PeopleSoft Internet Architecture





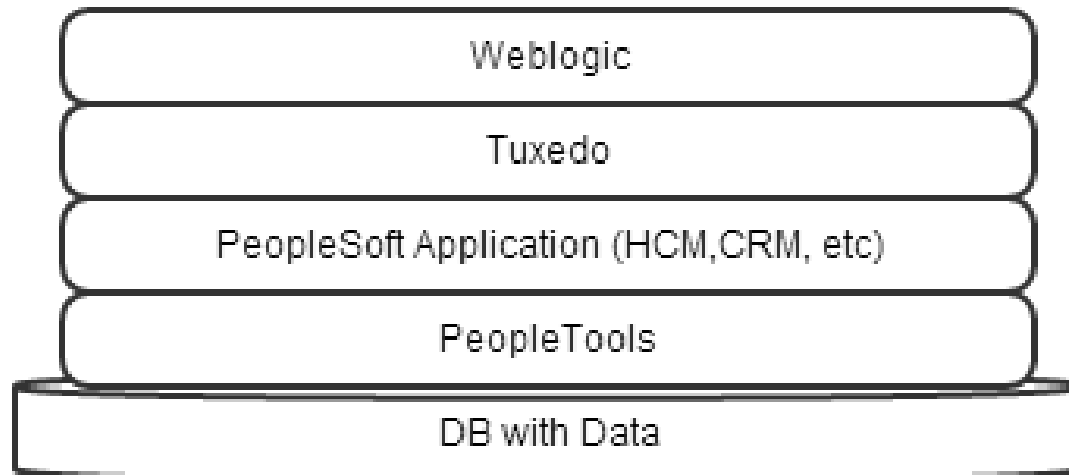
PeopleSoft Internet Architecture

- **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



PeopleSoft Internet Architecture

Another view:

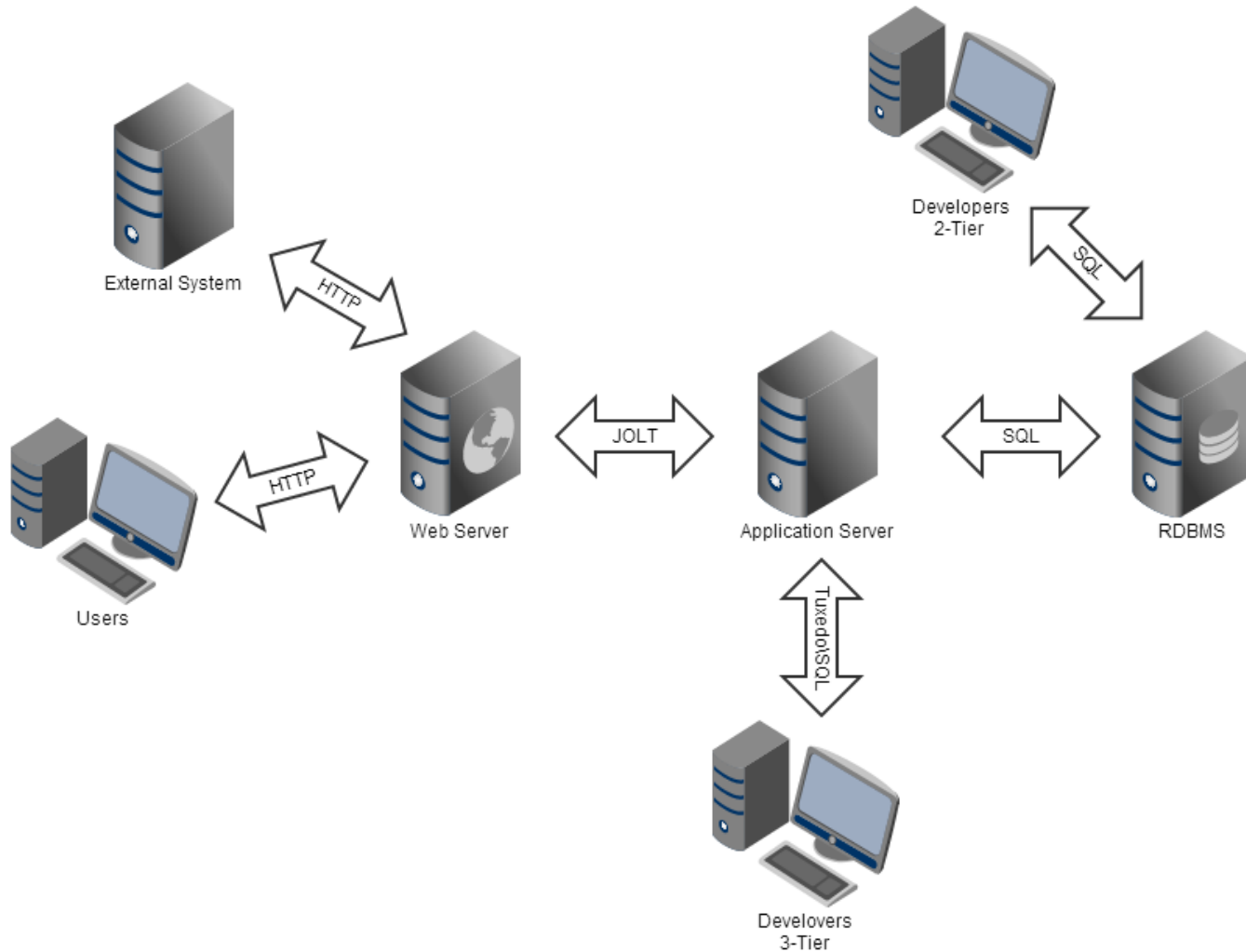




- Users (web browser)
 - All common web technologies
 - A single escalation point for common and administrative goals
- Developers (PeopleTools)
 - 2-Tier – direct connection to DBMS
 - 3-Tier – connection through Application Server. Special ports WSH, WSL. Essentially, basic SQL requests which are forwarded 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



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

[Oracle](#) » [Peoplesoft Products](#) : Security Vulnerabilities

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [Cve Number Descending](#) [Cve Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

Total number of vulnerabilities : **78** Page : [1](#) (This Page) [2](#)

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access
1	CVE-2013-2410				2013-04-17	2013-04-18	4.0	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise HRMS component in Oracle PeopleSoft Products 9.1.0 allows remote authentication related to Absence Management.								
2	CVE-2013-2408				2013-04-17	2013-04-18	4.3	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all related to PIA Core Technology and use of Internet Explorer 6.								
3	CVE-2013-2404				2013-04-17	2013-04-18	4.3	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all related to unknown vectors related to Portal.								
4	CVE-2013-2402				2013-04-17	2013-04-18	4.3	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all related to unknown vectors related to WorkCenter.								
5	CVE-2013-2401				2013-04-17	2013-04-18	3.5	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all related to unknown vectors related to Portal.								
6	CVE-2013-2374				2013-04-17	2013-04-18	4.0	None	Remote
	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.51, 8.52, and 8.53 all related to unknown vectors related to Rich Text Editor.								



- Old research
- buffer overflow in login process!!!
- we can control the return address
- but stack cookie... so only DoS

```

OS Name: Windows
OS Version: 2003 Enterprise Edition (Kernel 5.2, Build 3790, Service Pack 1)
OS Parameters: %SystemRoot%\system32\csrss.exe ObjectDirectory=\windows
SharedSection=1024,3072,512 windows=On SubSystemType=windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=off MaxRequestThreads=16
Physical memory: 4095MB total, 3101MB available
Paging space: 5971MB total, 4543MB available

=====
Process diagnostics - Start
=====

Stack Trace
=====
stack trace for process ID: 2076
Thread 2796 (Exception thread):
Address Frame Function Arguments Module!Symbol Name
0x2df3bafc 0x0012db94 0x00410041 0x03340000 0x2e01b450 0x238c2f1f EXP pssys!UpmGet+0x6c
0x00410041 0x00410041 0x8d8d5048 0xffffffff68 0x06fc45c6 0xf09015ff *** PSAPPSRV!<symbol>
0xc483d7ff 0x00410045 0xffffffff68 0x06fc45c6 0xf09015ff 0x8d8d0041 *** <module>!<symbol>
0x8d8d5048 0x00410049 0x06fc45c6 0xf09015ff 0x8d8d0041 0xffffffff38 *** <module>!<symbol>
0xffffffff68 0x0041004d 0xf09015ff 0x8d8d0041 0xffffffff38 0x05fc45c6 *** <module>!<symbol>
0x06fc45c6 0x00410051 0x8d8d0041 0xffffffff38 0x05fc45c6 0xf08c15ff *** <module>!<symbol>
0xf09015ff 0x00410055 0xffffffff38 0x05fc45c6 0xf08c15ff 0x8d8d0041 *** <module>!<symbol>
0x8d8d0041 0x00410059 0x05fc45c6 0xf08c15ff 0x8d8d0041 0xfffffeac *** <module>!<symbol>
0xffffffff38 0x0041005d 0xf08c15ff 0x8d8d0041 0xfffffeac 0x04fc45c6 *** <module>!<symbol>
0x05fc45c6 0x00410061 0x8d8d0041 0xfffffeac 0x04fc45c6 0xf08c15ff *** <module>!<symbol>

```

* 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):

PSIGW/PeopleSoftListeningConnector/	sawbridge
PSIGW/PeopleSoftServiceListeningConnector/	IMServlet/
PSIGW/HttpListeningConnector/	psc/
PSIGW/AS2ListeningConnector/	psp/
PSIGW/AS2ResponseConnector/	cs/
PSIGW/ExampleServletListeningConnector/	xmllink/
PSIGW/PS81ListeningConnector/	PSAttachServlet/
PSIGW/QueryListeningConnector/	psreports/
PSIGW/QASRepositoryWriter/	SchedulerTransfer/
PSIGW/JMSListeningConnectorAdministrator/	SyncServer/
PSINTERLINKS/BusInterlinkServLet	monitor/
pspc/upload/	ppmi/
pspc/csproxy/	PP/
pspc/providers/	RP/
pspc/PSPortletShowServlet	wsrptest/WSRPTTestPortlet/
pspc/test/	wsrptest/jsp/wsrptest2.jsp
pspc/PIAPortlet/	PSEMHUB/hub



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 admin “/console”
- on the same port with PeopleSoft application by default.
- Anyone can try to access the inside with default accounts

The screenshot shows a light blue textured login window titled "Welcome". Below the title is the instruction "Log in to work with the WebLogic Server domain". There are two input fields: "Username:" and "Password:". A "Login" button is located at the bottom right of the form.



```
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands

wls:/offline> connect('weblogic','123', '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 AdminServer .>
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”

Name/OID	URL
ServletRuntimeURL.16.90.11...	HTTP:///HelloWorld*.jspx
ServletRuntimeURL.16.81.10...	HTTP:///IMServlet/*
ServletRuntimeURL.16.206.1...	HTTP:///PP/*
ServletRuntimeURL.16.187.1...	HTTP:///PSAttachServlet/*
ServletRuntimeURL.16.155.1...	HTTP:///PSEMHub*.jspx
ServletRuntimeURL.16.161.5...	HTTP:///PSEMHub/hub/*
ServletRuntimeURL.16.78.24...	HTTP:///PSIGW*.jspx
ServletRuntimeURL.16.197.8...	HTTP:///PSIGW/AS2ListeningConnector/*
ServletRuntimeURL.16.76.10...	HTTP:///PSIGW/AS2ResponseConnector/*
ServletRuntimeURL.16.188.1...	HTTP:///PSIGW/ExampleServletListeningConnector/*
ServletRuntimeURL.16.230.1...	HTTP:///PSIGW/HttpListeningConnector/*
ServletRuntimeURL.16.216.2...	HTTP:///PSIGW/JMSListeningConnectorAdministrator/*
ServletRuntimeURL.16.0.37...	HTTP:///PSIGW/PS81ListeningConnector/*
ServletRuntimeURL.16.204.1...	HTTP:///PSIGW/PeopleSoftListeningConnector/*
ServletRuntimeURL.16.58.17...	HTTP:///PSIGW/PeopleSoftServiceListeningConnector/*
ServletRuntimeURL.16.84.12...	HTTP:///PSIGW/QASRepositoryWriter/*
ServletRuntimeURL.16.244.4...	HTTP:///PSIGW/QueryListeningConnector/*
ServletRuntimeURL.16.113.2...	HTTP:///PSINTERLINKS*.jspx
ServletRuntimeURL.16.232.7...	HTTP:///PSINTERLINKS/BusInterlinkServlet/*
ServletRuntimeURL.16.55.15...	HTTP:///PSOL*.jspx
ServletRuntimeURL.16.118.6...	HTTP:///PSOL/servlet/FullTextSearch
ServletRuntimeURL.16.209.2...	HTTP:///PSOL/servlet/PSOLManager
ServletRuntimeURL.16.232.2...	HTTP:///RP/*
ServletRuntimeURL.16.69.10...	HTTP:///SchedulerTransfer/*
ServletRuntimeURL.16.200.1...	HTTP:///SyncServer/*
ServletRuntimeURL.16.106.2...	HTTP:///_async*.jspx
ServletRuntimeURL.16.241.1...	HTTP:///_async/AsyncResponseService
ServletRuntimeURL.16.240.1...	HTTP:///_async/AsyncResponseServiceHttps
ServletRuntimeURL.16.141.2...	HTTP:///_async/AsyncResponseServiceJms
ServletRuntimeURL.16.118.1...	HTTP:///_async/AsyncResponseServiceSoap12
ServletRuntimeURL.16.106.1...	HTTP:///_async/AsyncResponseServiceSoap12Https
ServletRuntimeURL.16.188.9...	HTTP:///_async/AsyncResponseServiceSoap12Jms
ServletRuntimeURL.16.141.2...	HTTP:///bea_wls_deployment_internal*.jspx
ServletRuntimeURL.16.103.1...	HTTP:///bea_wls_deployment_internal/DeploymentService
ServletRuntimeURL.16.50.19...	HTTP:///bea_wls_diagnostics*.jspx
ServletRuntimeURL.16.198.1...	HTTP:///bea_wls_diagnostics/accessor



5. Insecure options



- 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



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.



Jolt Request

```

.....A.....SPCnObjs.....SLangd.....JOLT.....
1.....
..
.....GetCertificate.....;..Sperfmon,
0.|.1.|.0.|.0.|.0.|.u.n.k.n.o.w.n_|.|...`..SCertReq..P.S..1.2.3..A
T.Y.U.R.I.N.-.P.C...8...5.3..1.7.2...1.6...0...7.9.....SParameters...u.s.e.r.i
d...P.S..l.a.n.g.u.a.g.e.C.d...E.N.G..t.i.m.e.z.o.n.e.O.f.f.s.e.t...-2.4.0..c.m.d
.l.o.g.i.n..p.w.d...1.2.3.....SHeaders...H.o.s.t..1.7.2...1.6...0...7
9..C.o.n.n.e.c.t.i.o.n.k.e.e.p.-.a.l.i.v.e..C.o.n.t.e.n.t.-.L.e.n.g.t.h..4.3..C.a.c
h.e.-.C.o.n.t.r.o.l..m.a.x.-.a.g.e.=.0..A.c.c.e.p.t~.t.e.x.t./h.t.m.l.,.a.p.p.l.i.c
a.t.i.o.n./x.h.t.m.l.
+.x.m.l.,.a.p.p.l.i.c.a.t.i.o.n./x.m.l.;.q.=.0...9.,.*./.*;.q.=.0...8..o.r.i.g.i.n
$.h.t.t.p.://./1.7.2...1.6...0...7.9..U.s.e.r.-.A.g.e.n.t..M.o.z.i.l.l.a./5...0.
(.w.i.n.d.o.w.s..N.T..6...1;..W.O.W.6.4.)..A.p.p.l.e.w.e.b.K.i.t./5.3.7...3.
6..
(.K.H.T.M.L.,.l.i.k.e..G.e.c.k.o.)..c.h.r.o.m.e./2.7...0...1.4.5.3...1.1.0..S.
a.f.a.r.i./5.3.7...3.6..C.o.n.t.e.n.t.-.T.y.p.eB.a.p.p.l.i.c.a.t.i.o.n./x.-.w.w.w
-.f.o.r.m.-.u.r.l.e.n.c.o.d.e.d..R.e.f.e.r.e.r.n.h.t.t.p.://./1.7.2...1.6...0...7
9./p.s.p./H.R.D.E.M.O./E.M.P.L.O.Y.E.E./H.R.M.S./?.c.m.d=.l.o.g.o.u.t..A.c.c.e
p.t.-.E.n.c.o.d.i.n.g".g.z.i.p.,.d.e.f.l.a.t.e.,.s.d.c.h..A.c.c.e.p.t.-.L.a.n.g.u.a
g.e.F.r.u.-.R.U.,.r.u.;.q.=.0...8.,.e.n.-.U.S.;.q.=.0...6.,.e.n.;.q.=.0...4..C.o.o.k
i.e.....H.P.T.a.b.N.a.m.e.=.D.E.F.A.U.L.T.;..H.P.T.a.b.N.a.m.e.R.e.m.o.t.e.=.;..h
t.t.p.%3.a.%2.f.%2.f.1.7.2...1.6...0...7.9.%2.f.p.s.p.%2.f.h.r.d.e.m.o.
.%2.f.e.m.p.l.o.y.e.e.%2.f.h.r.m.s.%2.f.r.e.f.r.e.s.h.=.l.i.s.t.:%2.0.
.%3.f.t.a.b.%3.d.h.c._u.x._m.a.n.a.g.e.r._d.a.s.h.b.o.a.r.d.%7.c.%3.f.r.p.
.%3.d.h.c._u.x._m.a.n.a.g.e.r._d.a.s.h.b.o.a.r.d.%7.c.%3.f.t.a.b.
.%3.d.h.c._t.a.l.e.n.t._s.u.m.m.a.r.y.%7.c.%3.f.r.p.
.%3.d.h.c._t.a.l.e.n.t._s.u.m.m.a.r.y.%7.c.%3.f.t.a.b.
.%3.d.r.e.m.o.t.e.u.n..f.i.e.d.d.a.s.h.b.o.a.r.d.%7.c.%3.f.r.p.
.%3.d.r.e.m.o.t.e.u.n..f.i.e.d.d.a.s.h.b.o.a.r.d.%7.c.|.%3.f.t.a.b.
.%3.d.d.e.f.a.u.l.t.|.3.f.r.p.
.%3.d.d.e.f.a.u.l.t.;.p.e.o.p.l.e.s.o.f.t.-.8.0.-.P.O.R.T.A.L.-.P.S.J.S.E.S.S.I.O.
N.I.D.=1.V.7.G.R.B.Z.F.1.v.y.4.T.b.Q.v.r.B.6.s.p.Q.v.0.x.9.1.x.1.h.S.Q!.2.2.1.0.0.
4.6.4.9;..S.i.g.n.O.n.D.e.f.a.u.l.t.=.P.S.;..P.S._L.O.G.I.N.L.I.S.T.=.-1;..E.
x.p.i.r.e.P.a.g.e.=.;..P.S._T.O.K.E.N.E.X.P.I.R.E.=.-1;..P.S._T.O.K.E.N.=.....
cookies=H.P.T.a.b.N.a.m.e=D.E.F.A.U.L.T.;H.P.T.a.b.N.a.m.e.R.e.m.o.t.e.=h.t.t.p

```



```
+ .5.u.F.k.5.S.E.Z.L.p.K.O.R.e.Z.E.y.i.C.Y.H.E.q.N.o.6.o.P.W.f.K.b.G.4.A.M.G.G.g.o.5J0
LT.....
$......#......0.....#......#...
#..... V..SICPanelRep
.U.T.F.-.8..... 1<html dir="ltr" lang="en">
<head>
</head>
<body class="PSPAGE">
<script type="text/javascript">
var pthPrefresh = {cookie:"http%3a%2f%2f172.16.0.79%2fpsp%2fHRDEMO%2fEMPLOYEE%2fHRMS%
2frefresh",tabQS:"?tab=DEFAULT",domain:"null"};
refreshOnExpired(pthPrefresh.cookie,pthPrefresh.tabQS,pthPrefresh.domain);
setTimeout2();
ptEvent.add(window, 'scroll', positionWAIT_empty);
</script>
<table width="100%" border="0" cellspacing="0" cellpadding="0">
<tr>
<td>
<td>
<Pagelet Name="UniversalNavigation" Load="A">
<SOURCE Node="LOCAL_NODE" href="s/
WEBLIB_PORTAL.PORTAL_HOMEPAGE.FieldFormula.IScript_HPDefaultHdr" />
</Pagelet>
<pagelet name="TopNav" Load="A">
<source node="LOCAL_NODE" href="s/
WEBLIB_PT_NAV.ISCRIPT1.FieldFormula.IScript_PT_NAV_PAGELET?
navtype=dropdown&ptlayout=N" />
</pagelet>
</td>
</tr>
<tr>
<td>
<td>
<table id="ptpglts" width="100%" summary="">
..<tr>
..<td width="33%" valign="top">
...<ul id="ptcol1" class="ptpgltdroppable">
....<!-- Begin Pagelet=PT_MENU_NEW_FEATURES -->
<!-- PageletState=MAX -->
```



- **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

```

.....X.....CARRA
.....SCTX
R.I.N.-.P.C..P.S..[REDACTED]1.2..E.N.G..@.....e.....X.5...e.I.}..
..RP.e!
.....@.....:..d.d...M.M...y.y.y.y.,.....42.0.1.3.-.0.6.-.1.3.
.0.0.0.1.5.0.....
.....!. "#.$.%.&.'.(.*)*.
.5.6.7.8.9.:;<.=.>?.@.A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.
.`.a.b.c.d.e.f.g.h.i.j.k.l.m.n.o.p.q.r.s.t.u.v.w.x.y.z.
....SSamReq.....S.E.L.E.C.T. .T.I.M.E.Z.O.N.E.,. .P.T.E.F.F.
.Z.O.N.E.S.T.D.L.B.L.,. .T.I.M.E.Z.O.N.E.D.S.T.L.B.L.,. .O.B.S.E.R.
.O.F.F.S.E.T.,.D.S.T.O.F.F.S.E.T.,. .D.S.T.S.T.A.R.T.,. .D.S.T.E.N.
.,. .S.T.A.R.T.D.S.T..D.S.T.A.B.S.O.L.U.T.E.,. .S.T.A.R.T.D.S.T...
.S.T.A.R.T.D.S.T..D.S.T.D.A.Y.,. .S.T.A.R.T.D.S.T..D.S.T.D.A.Y.O.
.R.T.D.S.T..D.S.T.H.O.U.R.,. .S.T.A.R.T.D.S.T..D.S.T.M.I.N.U.T.
...D.S.T.A.B.S.O.L.U.T.E.,. .E.N.D.D.S.T..D.S.T.M.O.N.T.H.,. .E.N.
.Y.,. .E.N.D.D.S.T..D.S.T.D.A.Y.O.F.W.E.E.K.,. .E.N.D.D.S.T..D.S.
.D.S.T..D.S.T.M.I.N.U.T.E. .F.R.O.M. .P.S.T.I.M.E.Z.O.N.E.D.E.F.
.M.E. .S.T.A.R.T.D.S.T.,. .P.S.D.S.T.T.I.M.E. .E.N.D.D.S.T. .W.H.E.
.S.T..D.S.T.I.D. .=. .D.S.T.S.T.A.R.T. .A.N.D. .E.N.D.D.S.T..D.S.
.N.D. .A.N.D. .O.B.S.E.R.V.E.D.S.T. .=. .'.Y.'. .O.R.D.E.R. .B.Y. .
.P.T.E.F.F.D.T.T.M.....
.....
.....!...Sq]Reques

```



DEMO



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



Future work

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)**



ERPScan
Security Scanner for SAP



Greetz to our crew who helped