

Invest in security to secure investments



**Oracle PeopleSoft applications  
are under attacks!**



Alexey Tyurin

- The only 360-degree SAP Security solution - ERPScan Security Monitoring Suite for SAP
- **Leader** by the number of **acknowledgements from SAP** ( 150+ )
- **60+ presentations key security conferences** worldwide
- **25 Awards and nominations**
- Research team - **20 experts with experience in different areas of security**
- Headquartered in Palo Alto (US) and Amsterdam (EU)



- Working together since 2007

“We would like to thank the world-class security experts of ERPScan for the highly qualified job performed to help us assess the security of our pre-release products”.

Senior Director, Head of Global Security Alliance Management  
Product Security, Technology and Innovation Platform  
SAP Labs, Palo Alto, USA



**SAP**® Certified  
Integration with SAP Applications

- ERPScan researchers were acknowledged 15 times during quarterly Oracle patch updates since 2008
- Totally 40+ Vulnerabilities closed in Oracle Applications
  - Oracle Database
  - Oracle Peoplesoft
  - Oracle Weblogic
  - Oracle JDE
  - Oracle BI

Oracle provides recognition to people that have contributed to our Security-In-Depth program. Oracle recognizes Alexander Polyakov from ERPScan for contributions to Oracle's Security-In-Depth program.

- Director of Oracle Security department of the ERPScan company
- WEB/EBA/Network security fun
- Hacked many online banking systems
- Hacked many enterprise applications



Tweeter: @antyurin

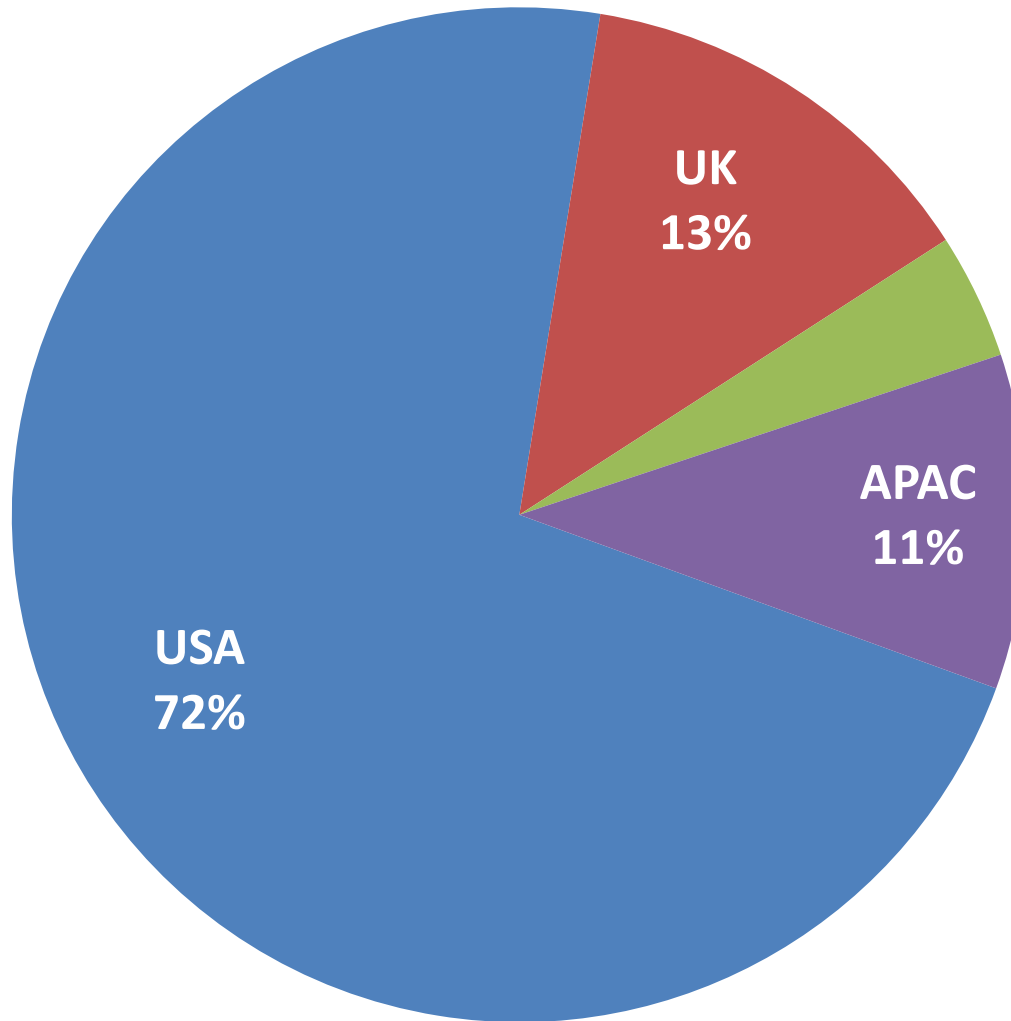
- Introduction to Oracle PeopleSoft
- PeopleSoft Architecture
- Attacks on back-end systems
- External attacks on PeopleSoft

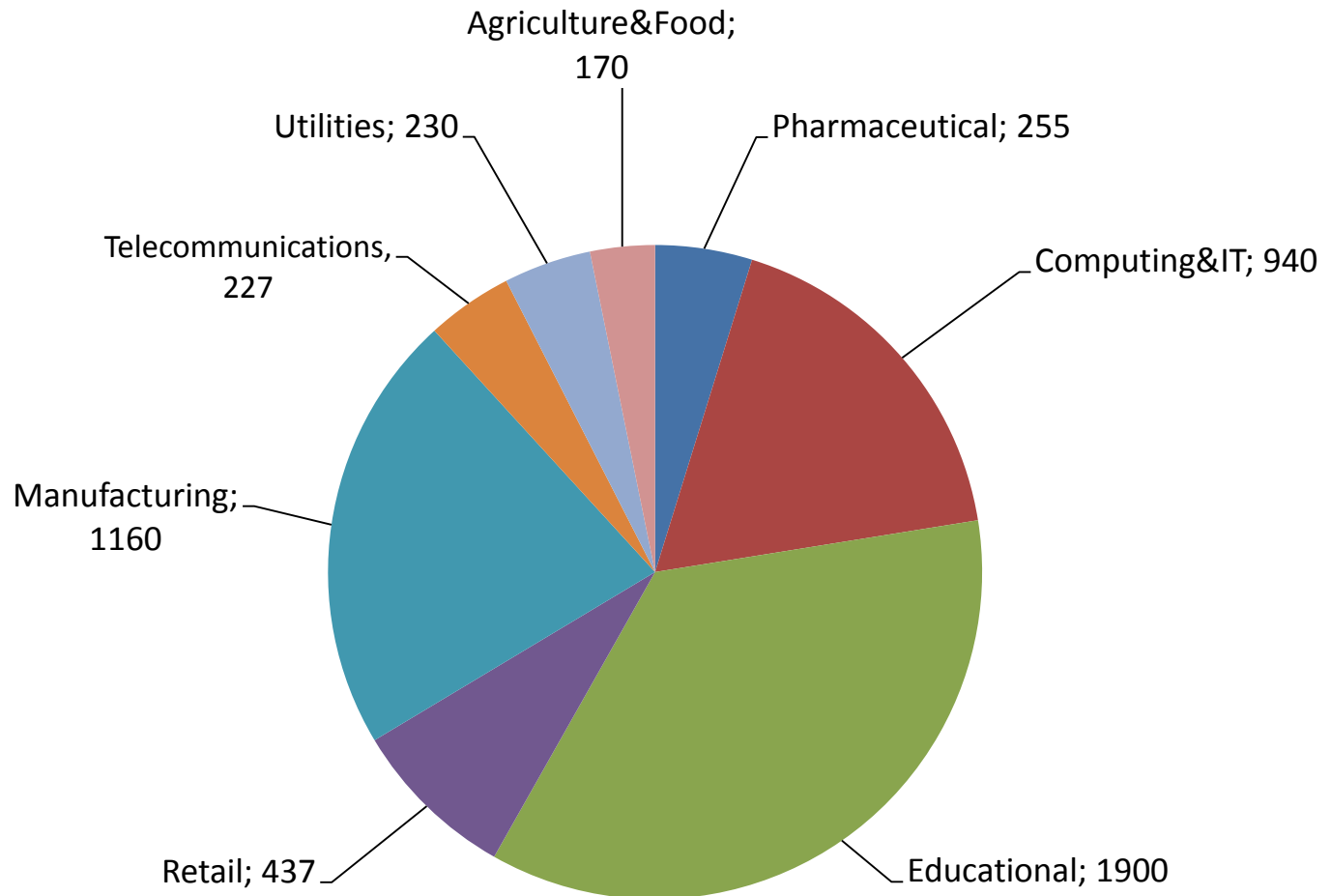
# Introduction to Oracle PeopleSoft

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



- Large companies. HRMS/ FMS
- Government. HRMS
- Universities. Student Administration system





- Personal information
  - SSN
  - Salary data
- Payment information
  - Credit card data
  - Bank account data
- Bidding information
  - RFP
  - Prices

- Espionage
  - Theft of financial information
  - Corporate trade secret theft
  - Theft of supplier and customer lists
  - Stealing HR data Employee Data Theft
- Sabotage
  - Denial of service
  - Tampering with financial reports
- Fraud
  - False transactions
  - Modification of master data

- Two Charged with Hacking PeopleSoft to Fix Grades (California state university) - 2007
  - <http://www.pcworld.com/article/139233/article.html>
- Student sentenced to jail for hacking university grades (Florida A & M University) - 2009
  - <http://www.geek.com/news/student-sentenced-to-jail-for-hacking-university-grades-742411/>
- Undergrad suspected in massive breach (University of Nebraska) - 2012
  - <http://www.computerworld.com/article/2503861/cybercrime-hacking/undergrad-suspected-in-massive-univ--of-nebraska-breach.html>
- Hacking Higher Education - last years
  - <http://www.darkreading.com/security/hacking-higher-education/d/d-id/1109684>



**A** DATA CENTRE SOFTWARE NETWORKS **SECURITY** BUSINESS HARDWARE SCIENCE BOOTNOTES

## Student sentenced for F-ucked up grade hack

Act of God clods

14 Apr 2009 at 23:52, [Dan Goodin](#)



0



## Two Charged with Hacking PeopleSoft to Fix Grades

A university student in Florida on Tuesday was sentenced to 22 months in prison for his part in the plot, which used keyloggers to access protected computer systems and make hundreds of unauthorized changes to grades. [By Robert McMillan](#), IDG News Service

Nov 4, 2007 7:00 AM



Christopher Jacquette, 29, of Tallahassee was also ordered to serve three years in prison for his part in the plot, which used keyloggers to access protected computer systems and make hundreds of unauthorized changes to grades. According to federal prosecutors. Along with cohorts Lawrence Secrese and Christopher Jacquette, the caper reads like a modern-day episode of *The Three Stooges*.

The tale begins in August 2007, when Jacquette installed keyloggers on the computers after sneaking into a locked ballroom where student registration took place. In order, the trio had access to the school's PeopleSoft accounts. They pruned the database of grades belonging to them and their friends, in many cases from Fs to As.

Two California men are facing 20 years in prison on charges they hacked into a California state university's PeopleSoft system to change their grades.

In an October 25 grand jury indictment, [John Escalera](#), 29, and [Gustavo Razo](#), 28, were charged with using Escalera's position within [California State University, Fresno's](#) IT help desk center to gain access to the university's grades database.

The men could face 20 years in prison and US\$250,000 in fines if convicted of the eleven counts on the [indictment](#), which includes charges of unauthorized computer access, identity theft, conspiracy and wire fraud.

Though they are charged with identity theft, a university spokeswoman could not immediately say whether or not sensitive information such as social security numbers had been compromised during the crime.

## 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 : **143** Page : [1](#) (This Page) [2](#) [3](#)

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

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2015-0497</a>				2015-04-16	2015-04-17	4.3	None	Remote	Medium	Not required	None	Partial	None
Unspecified vulnerability in the PeopleSoft Enterprise Portal Interaction Hub component in Oracle PeopleSoft Products 9.1.00 allows remote attackers to affect integrity via unknown vectors related to Enterprise Portal.														
2	<a href="#">CVE-2015-0496</a>				2015-04-16	2015-04-17	4.0	None	Remote	Low	Single system	Partial	None	None
Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53 and 8.54 allows remote authenticated users to affect confidentiality via vectors related to PIA Search Functionality.														
3	<a href="#">CVE-2015-0487</a>				2015-04-16	2015-04-17	4.0	None	Remote	Low	Single system	None	Partial	None
Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53 and 8.54 allows remote authenticated users to affect integrity via vectors related to PIA Core Technology, a different vulnerability than CVE-2015-0472.														
4	<a href="#">CVE-2015-0485</a>				2015-04-16	2015-04-17	3.5	None	Remote	Medium	Single system	Partial	None	None
Unspecified vulnerability in the PeopleSoft Enterprise SCM Strategic Sourcing component in Oracle PeopleSoft Products 9.1 and 9.2 allows remote authenticated users to affect confidentiality via unknown vectors related to Security.														
5	<a href="#">CVE-2015-0472</a>				2015-04-16	2015-04-17	3.5	None	Remote	Medium	Single system	None	Partial	None
Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53 and 8.54 allows remote authenticated users to affect integrity via vectors related to PIA Core Technology, a different vulnerability than CVE-2015-0487.														
6	<a href="#">CVE-2015-0453</a>				2015-04-16	2015-04-17	3.3	None	Local Network	Low	Not required	Partial	None	None
Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.53 and 8.54 allows remote attackers to affect confidentiality via vectors related to PORTAL.														
7	<a href="#">CVE-2015-0394</a>				2015-01-21	2015-04-14	4.0	None	Remote	Low	Single system	Partial	None	None
Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.52 and 8.53 allows remote authenticated users to affect confidentiality via unknown vectors related to Report Distribution.														



# Oracle PeopleSoft Architecture

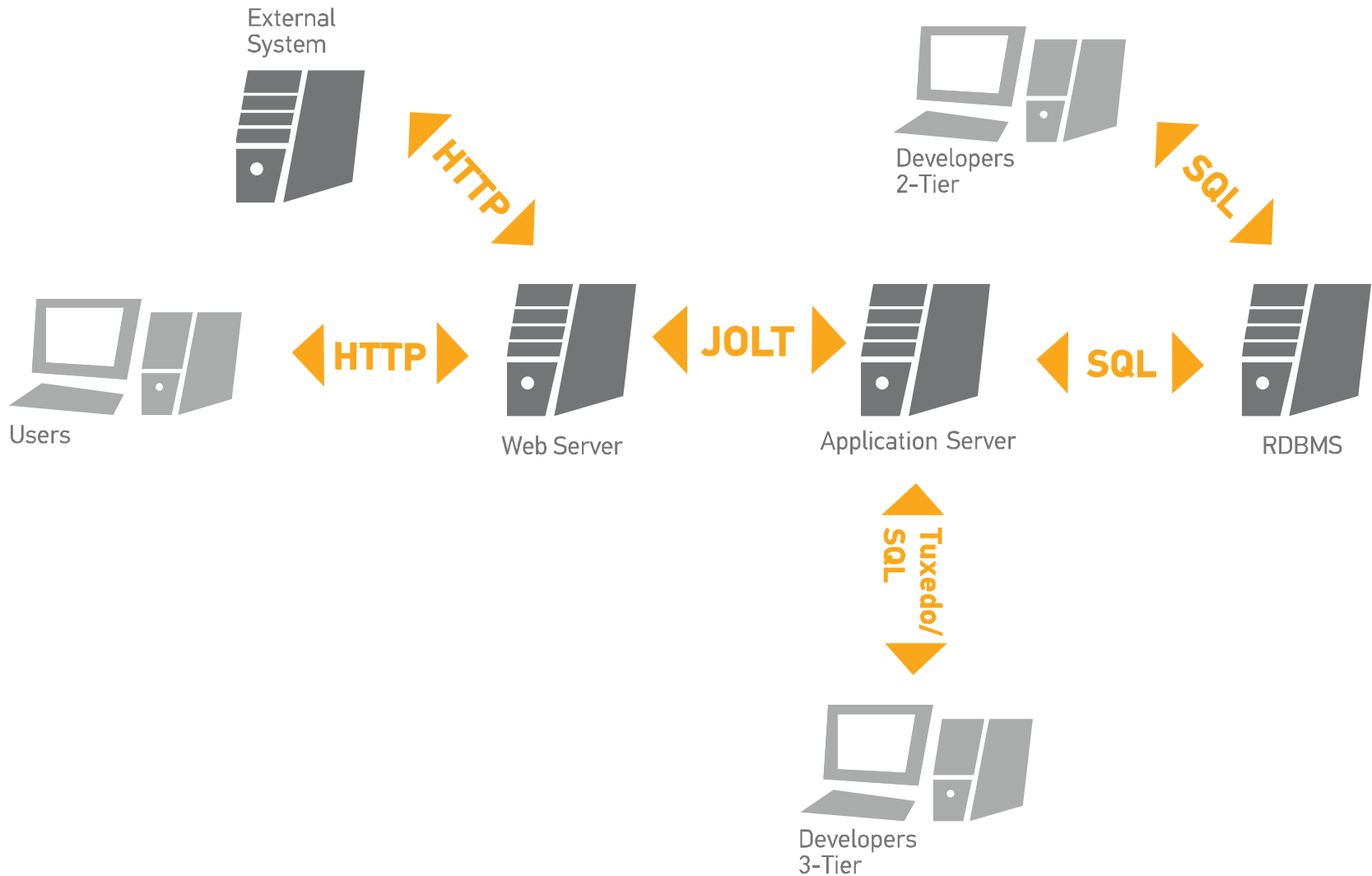
- Many applications, but they have one architecture
- PeopleSoft Internet Architecture
  - Internet oriented since version 8
- Based on several special core technologies

## PeopleTools:

- Technology
- Developer tools
- Framework
- PeopleCode

All of the applications are created using PeopleTools.

# 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

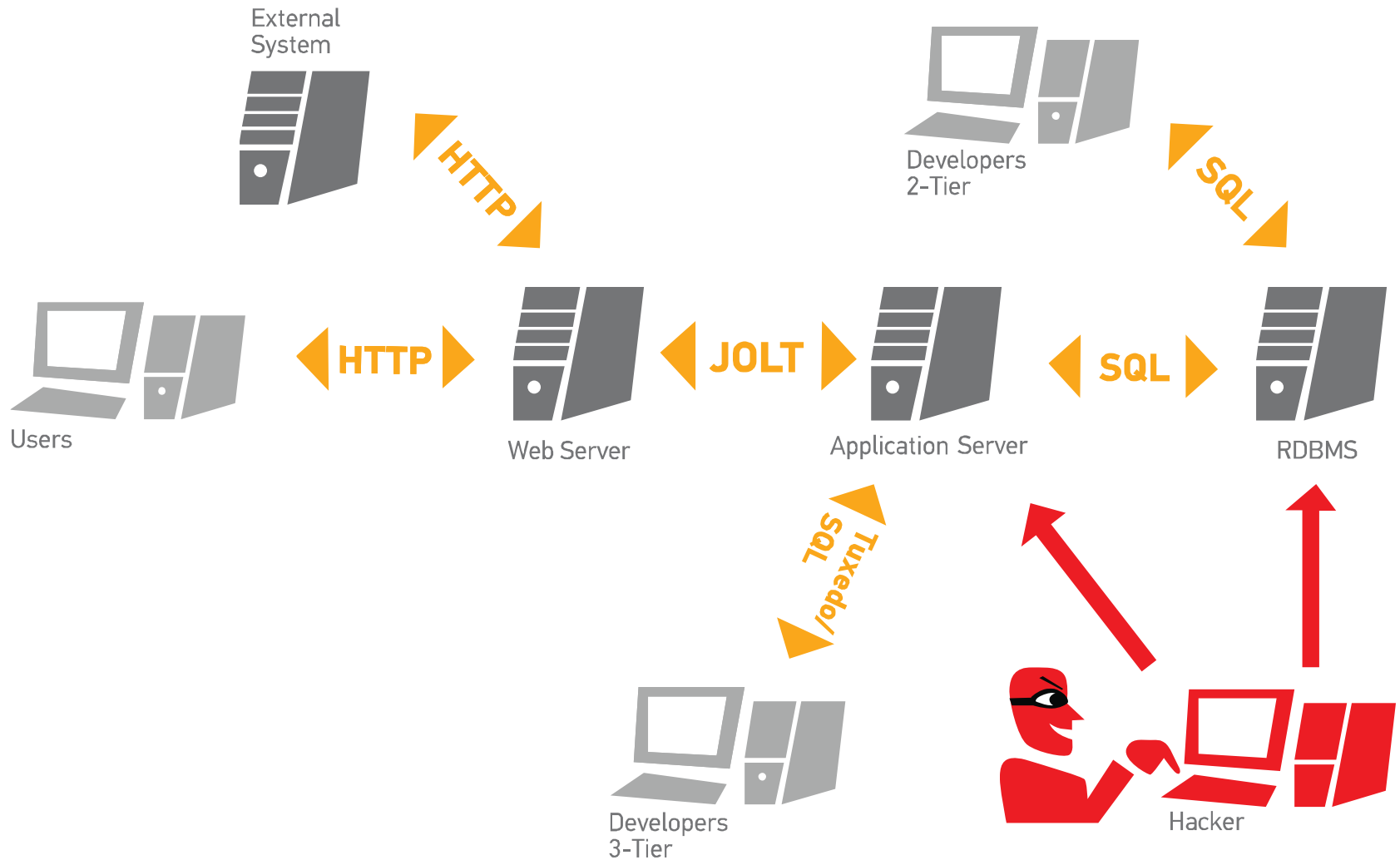
## Database server

- System Tables, PeopleTools metadata , PeopleSoft application data

- High privileged access in PeopleSoft (“PS” – super admin account)
  - *Attacks on business logic*
  - *Critical information in PeopleSoft*
- Remote Command Execution in OS
  - *Access to a company's internal network*
  - *Critical information in PeopleSoft*

*We can get RCE in OS if we have high priv. access. Conversely situation is true too*

# Attacks on back-end systems





- User ID – an account in PeopleSoft Application.
- Connect ID – a low privileged account in the RDBMS
- Access ID – a high privileged account in the RDBMS

## User authentication process:

- User logs in with his User ID and password to the Application Server.
- Application Server, in turn, connects to DBMS using Connect ID. User ID and passwords for it stored in DBMS tables are compared to the ones that were entered by the user.
  - Connect ID has limited rights, only to retrieve User ID and encrypted password from DBMS tables.
- If the comparison went successful, Application Server retrieves the necessary Access ID with the encrypted password.
  - Access ID with the password are stored in PSACCESSPRFL table.
  - Access ID account has high privileges.
- Finally, the system reconnects to DBMS using Access ID with full access.

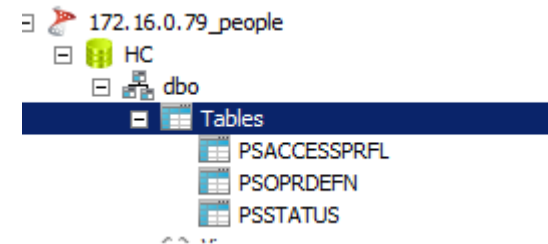
Some facts :

- Common Connect ID – “people” with password  
“people”/”peop1e”
- Default Access ID:  
“SYSADM” for Oracle  
“sa” for MSSQL
- Connect ID password is often the same as Access ID password

*Let's try to perform dictionary attack on RDBMS*

## Connect ID has:

- Access to 3 tables
- Users' passwords hashed with salt



OPRID	VERSION	OPRDEFNDESC
PS	1	[PS] Peoplesoft Superuser

OPERPSWD	OPERPSWDSALT	ENCRYPTED	SYMBOLICID
{1}SOxL1Xp6dGJoQxwmmGnaf3vJLAM=	JKqRwrfTqCQiQ2PeMf3TCQ==	1	sa

- AccessID and its password is encrypted

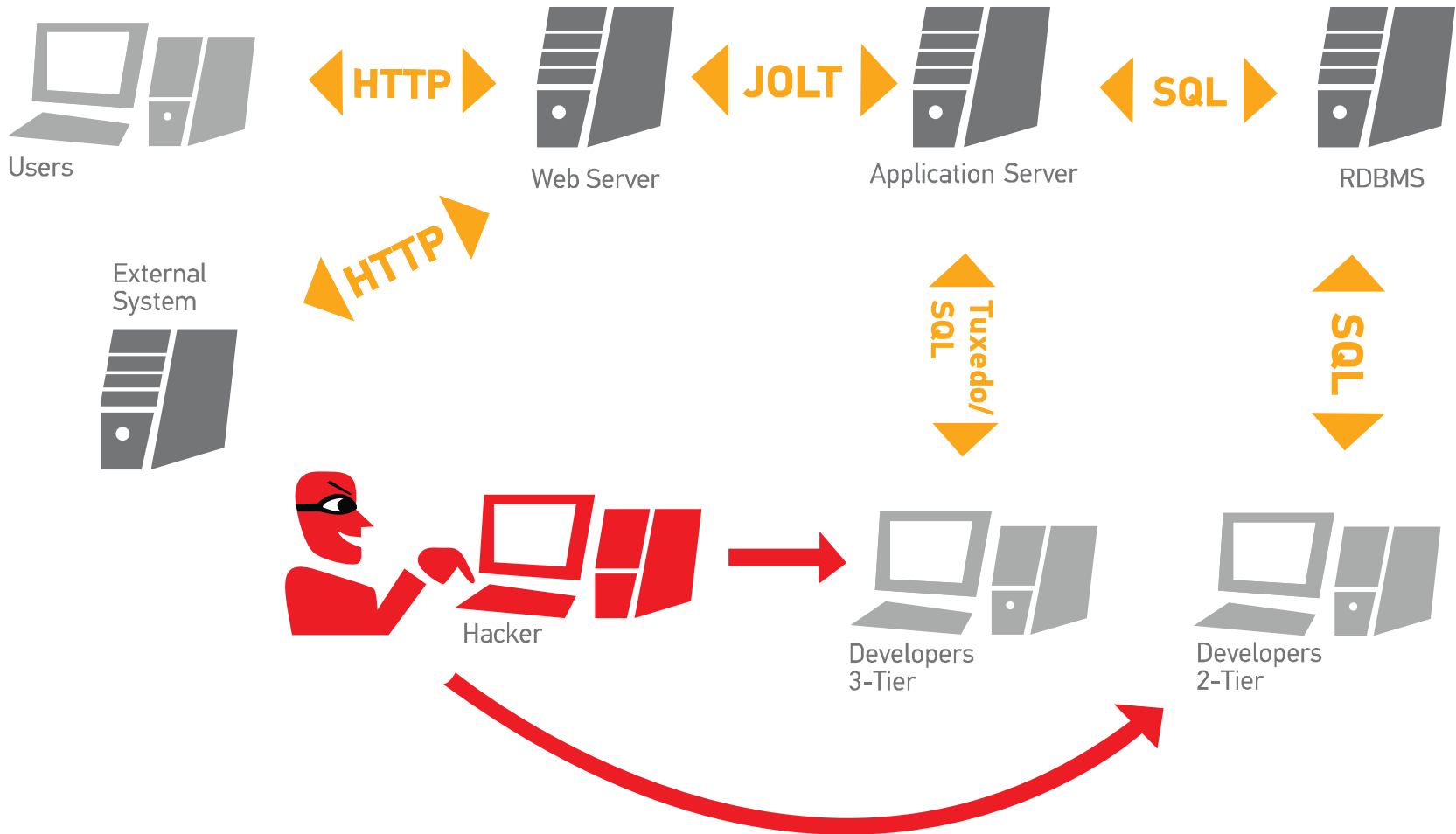
SYMBOLICID	VERSION	ACCESSID	ACCESSPSWD	ENCRYPTED
sa	28	kCSYMM0Crag=	gjb8YZpHnJo=	1

- “The ACCESSID and ACCESSID password are stored and encrypted in the PeopleSoft security table PSACCESSPRFL.”  
[http://docs.oracle.com/cd/E18083\\_01/pt851pbr0/eng/psbooks/tadm/chapter.htm?File=tadm/htm/tadm13.htm](http://docs.oracle.com/cd/E18083_01/pt851pbr0/eng/psbooks/tadm/chapter.htm?File=tadm/htm/tadm13.htm)
- “The Symbolic ID is used as the key to retrieve the encrypted ACCESSID and ACCESSPSWD from PSACCESSPRFL”  
[http://docs.oracle.com/cd/E26239\\_01/pt851h3/eng/psbooks/tsec/chapter.htm?File=tsec/htm/tsec06.htm](http://docs.oracle.com/cd/E26239_01/pt851h3/eng/psbooks/tsec/chapter.htm?File=tsec/htm/tsec06.htm)

Is Access ID really encrypted?

- Is Access ID really encrypted?
  - No.
- It's just XOR with a hardcoded key
  - sBzLcYlPrag= -> SYSADM
  - kCSYMM0Crag= -> sa
  - gjb8YZpHnJo= -> asdQWE12
- Some facts for a brute force attack:
  - Access ID max length – 8 symbols
  - Access ID's max password length – 10 symbols
- *If we have Connect ID and network access to RDMBS, we can get Access ID.*







SYMBOLICID	VERSION	ACCESSID	ACCESSPSWD	ENCRYPTED
sa	28	kCSYMM0Crag=	gjb8YZpHnJo=	1



- 2-Tier – direct connection to DBMS.

- Trusted developers (?)

Some tools (like DataMover)

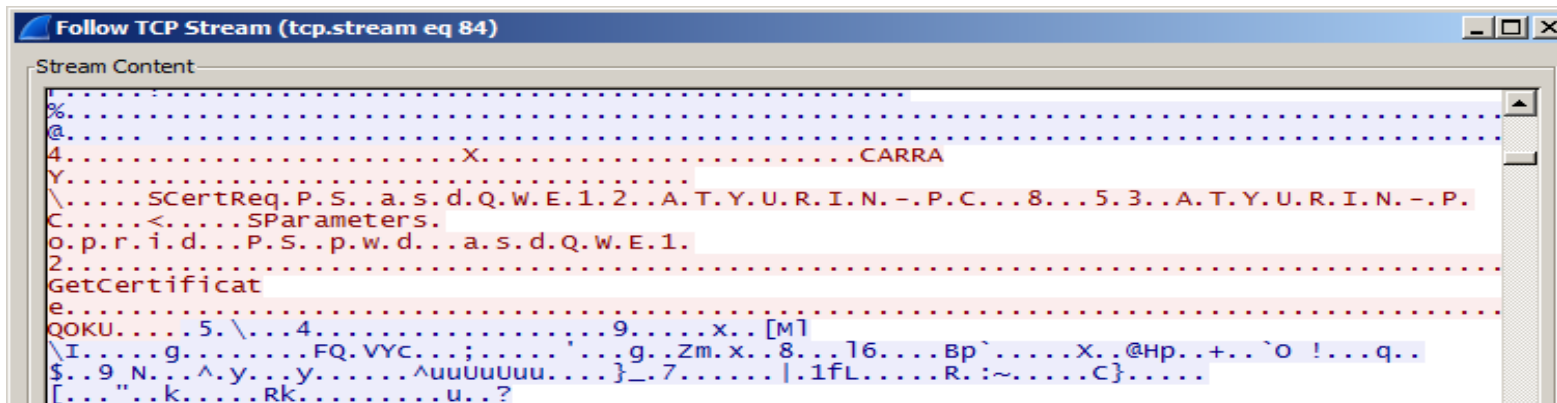
	ConnectId	REG_SZ	people
	ConnectPswd	REG_SZ	kyD3QPxnrag=
	DBChange	REG_SZ	YES
	DBName	REG_SZ	HC
	DBType	REG_SZ	MICROSFT
	EnableAuthSrv	REG_SZ	NO

- A config is stored in the Windows registry
- “Encryption” is the same

- *If we steal a config, we can have full access in RDBMS.*



- 3-Tier – connection through Application Server.
  - A developer uses only his own PS User ID and password
  - It's possible to restrict access for a developer (read-only privs)
  - Application Server connects to a RDBMS with Access ID account.
  - Special “protocol” - WSH, WSL (Tuxedo).
  - It's a plain-text protocol. A user's password in each packet.
- *Man in the middle attack will be useful*



- 3-Tier – connection through Application Server.
- Data inside packets look like plain SQL queries.

```
{.|.}~.....SSamReq.....tS.E.L.E.C.T. 'V.E.R.S.I.O.N. .F.R.O.M. .P.S.V.E.  
R.S.I.O.N. .W.H.E.R.E. .O.B.J.E.C.T.T.Y.P.E.N.A.M.E. .=. .'.S.Y.S.  
.....
```

```
{.|.}~.....SSamReq.....S.E.L.E.C.T. 'D.I.S.T.I.N.C.T. 'L.A.N.G.U.A.G.E.  
.C.D. .F.R.O.M. .P.S.L.A.N.G.U.A.G.E.S. .W.H.E.R.E. .I.N.S.T.A.L.L.E.D. .=. .
```

```
{.|.}~.....SSamReq.....S.E.L.E.C.T. 'C.O.U.N.T.  
(.*). .F.R.O.M. .P.S.T.I.M.E.Z.O.N.E.D.F.N.L.G. .W.H.E.R.E. .T.I.M.E.Z.O.N.E.=.:1. .  
a.n.d. .P.T.E.F.F.D.T.T.M.=.:2.....C.S.T.....42.0.0.7.-.0.1.-.0.1.-.0.0...0.  
0...0.0...0.0.0.0.0.0.....
```

*Can a 3-tier developer send any SQL command to a RDBMS with Access ID?*

*It should be so!*

# Developers

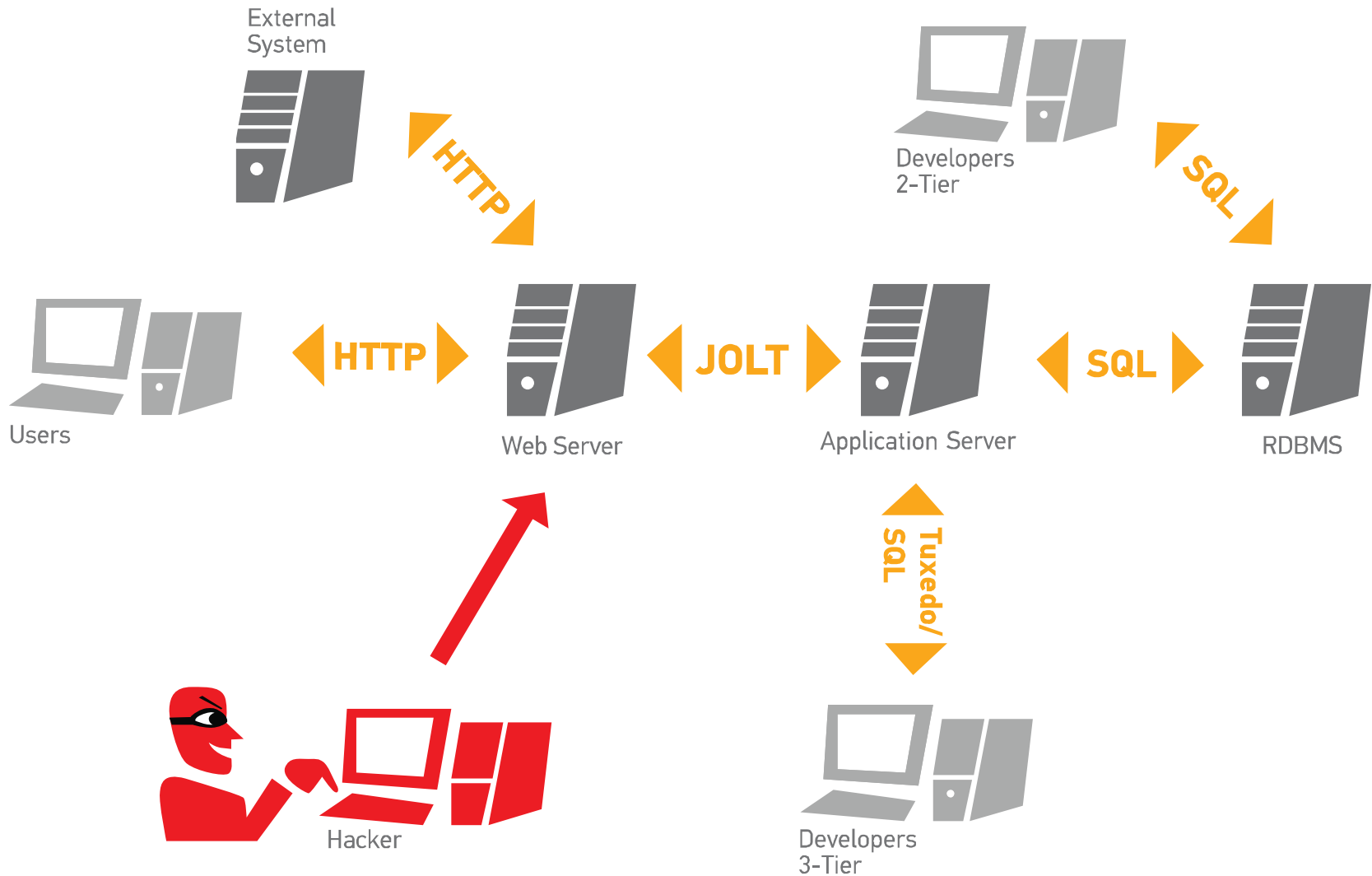
### 3-Tier – connection through Application Server.

- **Weird Design.** We see all queries of the default authentication process between Application Server and RDMBS

```
v.w.x.y.z.[.\].^._`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..V.E.R.S.I.O.N.,,.O.P.E.R.P.S.W.
D...O.P.E.R.P.S.W.D.S.A.L.T.,,.E.N.C.R.Y.P.T.E.D.,,.S.Y.M.B.O.L.I.C.I.D.,,.A.C.C.
T.L.O.C.K..F.R.O.M..P.S.O.P.R.D.E.F.N..W.H.E.R.E..O.P.R.I.D..=..:1.....P.
S.....
@.....
4.....SqlReques.....
t.....
S....Q...4.....D.....X.....P...CARRA
Y.....SSamReply.....SSamExecRows.....
@...>
{.1}.S.O.x.L.1.X.p.6.d.G.J.o.Q.x.w.m.m.G.n.a.f.3.v.J.L.A.M.=.....0J.K.q.R.w.r.f.T.
q.C.Q.i.Q.2.P.e.m.f.3.T.C.Q.=.....S.a.....2.....4.....
SSamFetchTran.....
@.....|.....
4.....X.....CARRA
Y.....SCTX
e.n.-.u.s.A.T.Y.U.R.I.N.-.P.C..P.S..a.s.d.Q.w.E.1.2...@.z.r.....qy8....e4^8..w
Y.<.X..'WO.5.....B.....@.....d.d..M.M..y.y.
Y.....
+,...-/0.1.2.3.4.5.6.7.8.9.:;<.=.>?.@.A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.
v.w.x.y.z.[.\].^._`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..A.C.C.E.S.S.I.D.,,.A.C.C.E.S.S.P.
S.W.D.,,.E.N.C.R.Y.P.T.E.D..F.R.O.M..P.S.A.C.C.E.S.S.P.R.F.L..W.H.E.R.E..S.Y.M.B.
O.L.I.C.I.D..=..:1.....S.a....."
".....
4.....
t.....SqlReques.....
S8....R...4.....X.....P...CARRA
Y.....SSamReply.....
[.....SSamExecRows.....".....k.C.S.Y.M.M.O.C.r.a.g.=.....".....g.j.b.8.Y.Z.p.H.n.J.o.
```

- A 3-Tier developer knows an Access ID and its password

# Attacks on front-end systems





peoplesoft inurl:cmd=login



**Поиск**

Новости

Видео

Картинки

Ещё ▾

Инструменты поиска

Результатов: примерно 7 120 (0,42 сек.)

## PeopleSoft - Emerson Process Management

<https://home.emersonprocess.com/.../home/?cmd=login...> ▾ Перевести эту страницу

You must have cookies enabled in order to sign in to your PeopleSoft application.

Return to Sign In with cookies enabled. If your attempt fails, please contact ...

## PeopleSoft Enterprise Sign-in - University of Missouri System

<https://myhr.umsystem.edu/.../h/?...cmd=login...> ▾ Перевести эту страницу

... with this application. For help in using PeopleSoft myHR, including training

resources, contact PeopleSoft HR Support at PSHRSUPPORT@umsystem.edu.

## My UH - University of Houston System

<https://my.uh.edu/psp/paprd/?cmd=login> ▾ Перевести эту страницу

You must have cookies enabled in order to sign in to your PeopleSoft application.

Return to Sign In with cookies enabled. If your attempt fails, please contact ...

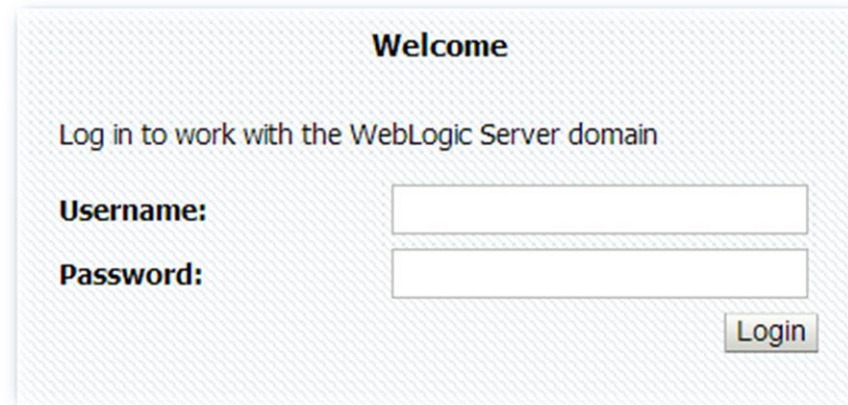
## Oracle | PeopleSoft Enterprise Sign-in - ESS - NYC.gov

<https://a127-ess.nyc.gov/.../prdess/?cmd=login...> ▾ Перевести эту страницу

Oracle PeopleSoft logo. Error. Your User ID and/or Password are invalid. User ID:

Password: Forgot your password? NYCAPS News.

- WebLogic management “/console”
- On the same port with PeopleSoft application by default
- Anyone can try to access the inside with default accounts



**Welcome**

Log in to work with the WebLogic Server domain

**Username:**

**Password:**

- A default Weblogic has no additional accounts, except “system” with a custom password
    - Weblogic with PS has 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”
  - WebLogic account bruteforcing is blocked by default
- If we get access to a Weblogic server with system account, we will get our goal – RCE*



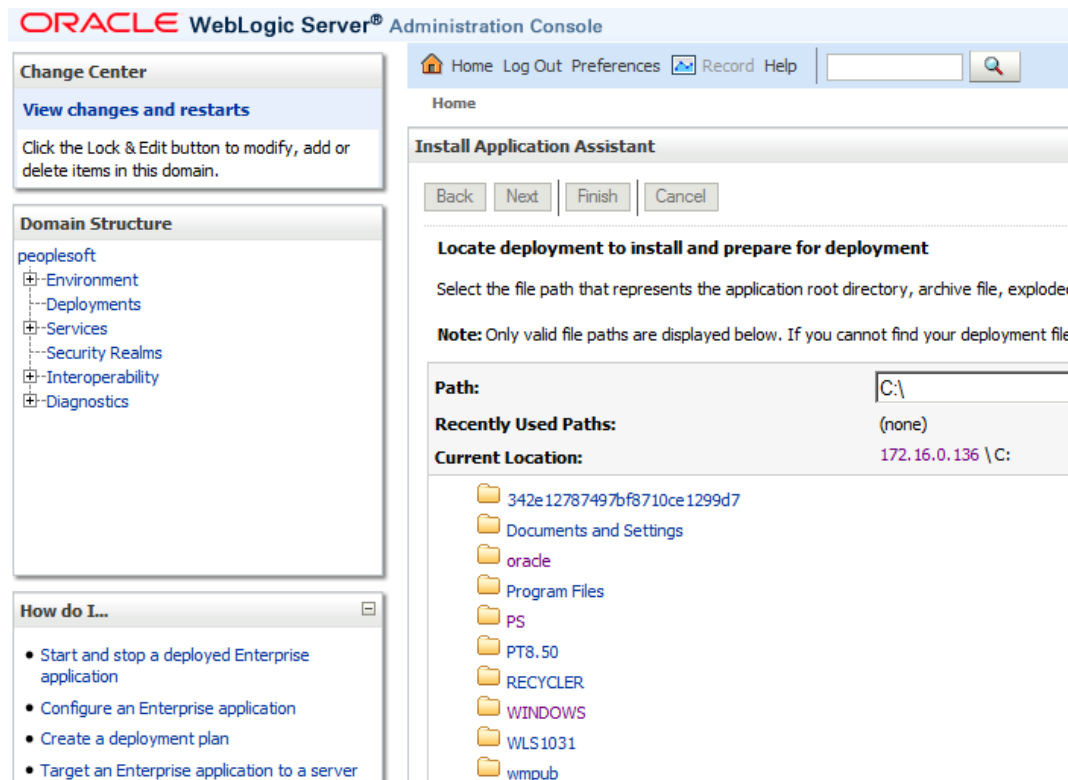
What about operator and monitor users?

Almost nothing

Force browsing will help us. There are no sufficient authorization checks.

Examples:

## 1) Browse a server's file system



2) How about installing a new application (RCE)?

Yes, we can do it!

Some restrictions:

- Only with .war/.jar extension
- Only “local” files

How can we upload the file?

Some attempts:

**1. SSRF + “jar” trick**

- No success. The file has a wrong extension

**2. Via PS servlet**

- No success. The file has a wrong extension

**3. A classic “UNC” trick for bypassing only “local” files restriction.**

We should use [\\any\\_server\evil.jar](#)

+ Success! But only for Windows OS

DEMO

# PeopleSoft Portal

- “PS” – super administrator
- There are many default users.
- Before PeopleTools 8.51: password = login  
Like, PS:PS, VP1:VP1, PTDMO:PTDMO
- After PeopleTools 8.51: password = PS’s password  
PS:Password, VP1:Password, PTDMO:Password
- PS account bruteforcing is not blocked by default

*This is a pretty good situation for brute force attacks*

- Information disclosure:



The screenshot shows a web browser with the address bar at 172.16.0.79/PSIGW/PeopleSoftListeningConnector. The page title is "PeopleSoft Integration Gateway". The content displays "PeopleSoft Listening Connector", "Tools Version : 8.53", and "Status:ACTIVE".

Below this, there is a "PeopleSoft." logo and a section titled "Registered Hosts Summary - 8.50." which contains a table with the following headers:

Hostname	OS Type	OS Version	IP Address	State	Peer ID	Peer Type	Peer Version
----------	---------	------------	------------	-------	---------	-----------	--------------

The browser then shows an error message: "Error: The return content is not xlink data, please check log file". The log file path is provided as "C:\APPS\HRM\websrv\HC\applications\peoplesoft\PORTAL.war\WEB-INF\psftdocs\HRDEMO\xmlinkservlet.log".



- Some of input points: PSIGW/\*, Business Interlink, SyncServ
- !!!No authentication !!!

- Common XXE injection impact:
  - We can read plain text files (not all)
  - SSRF
  - SSRF+gopher (if JDK  $\leq$  1.6)
  - SSRF+grab NTLM hashes/SMBRelay (if JDK  $\leq$  1.6 and OS = Windows)
  - Classic entities DoS?
  - SSRF+jar trick for file uploading

+ we can list directories and read XML files! (no binary)

CVE-2013-3800, CVE-2013-3819, CVE-2013-3821

Patched in CPU on the 16<sup>th</sup> July 2013 (cpujul2013)

## Encryption of password in config files:

- Some passwords of PeopleSoft are stored in plaintext
- Some – DES
- Some – 3DES
- Some – AES (Weblogic)

## DES

- The key for DES is hardcoded
- Was used for encryption in the older systems
- Has no ID at the beginning (such as “{V1.1}”)

## 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.

1. *If we have network access to the RDBMS, we can read Connect ID, get Access ID and pwn PS DB.*
1. *From the multitude of configuration files, we can retrieve various accounts (in the case of v. 1.1 or an old PT version with DES). If an administrator re-use a password, we can try to login with the PS account in Portal.*

- PS IGW supports remote configuration. There are opportunities to read and write a IGW configuration file via special XML requests. Auth is required.
- Old PT versions use “password” as a default password for different services. New PT versions use PS’s password as a default password for different services
- No defense against brute force attack
- The PS IGW password is stored in a config file. PS IGW’s password is DES/3DES encrypted. The file is readable via XXE.

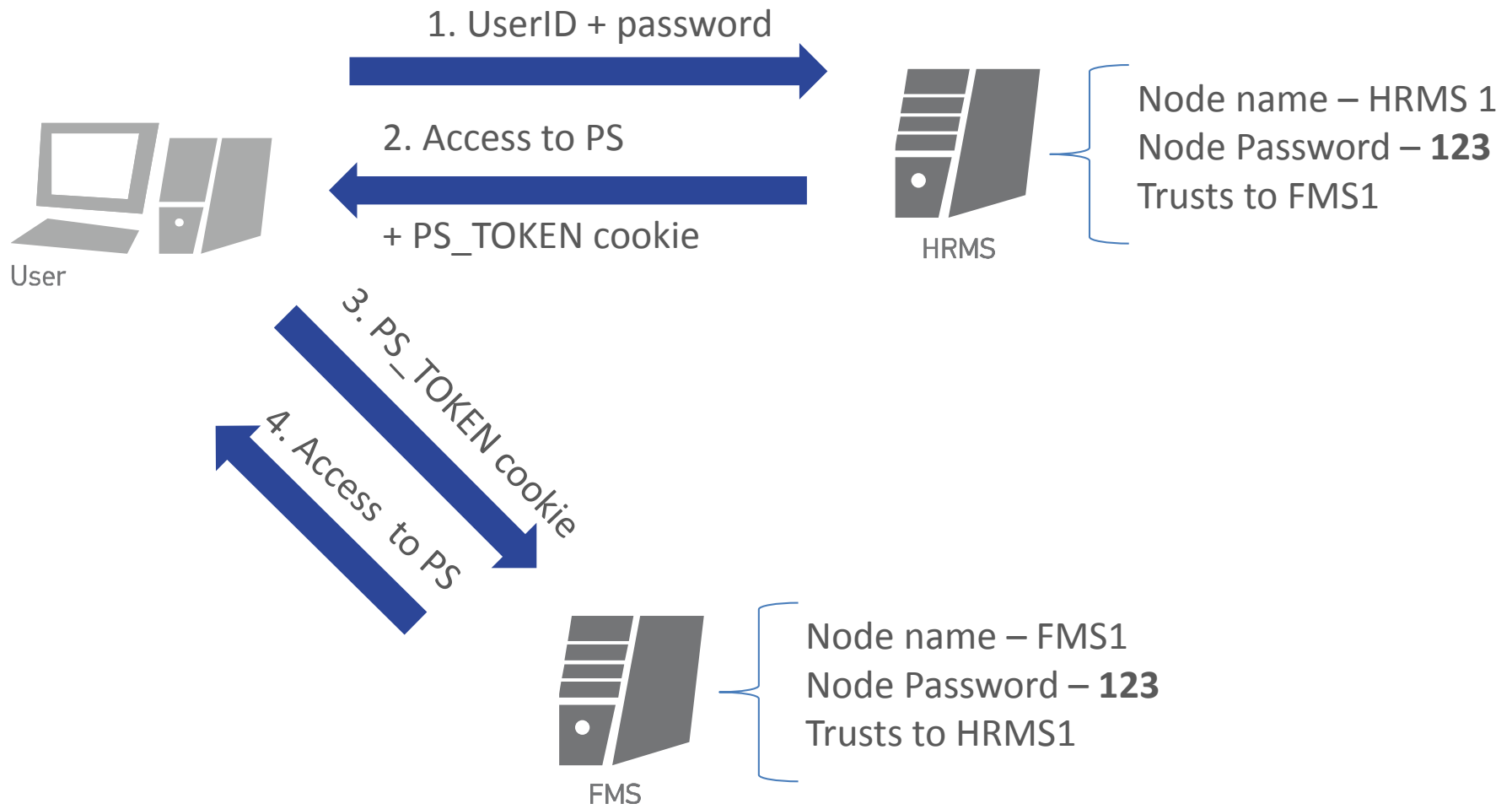
- *Turn on a XXE feature for a IGW's XML parser*
- *Read a lot of different passwords*
- *Change a path of Java classes location and get RCE \**
- *Set a XSL transformation and get RCE \**

\* Haven't been fully tested yet

# PeopleSoft SSO



- A PeopleSoft application supports his own Single Sign On technology
- A PS application sets a special “PS\_TOKEN” cookie for a user after successful login. Another PS application checks the cookie and authenticates the user
- How does it work? Pre-Shared Key.
- The same password should be set on each node  
“Nodes represent any organization, application or system that will play a part in integrations.”
- A node has a name. It is necessary to set nodes trusted by the system
- A user name should be in both applications



## PS\_TOKEN:

[http://docs.oracle.com/cd/E15645\\_01/pt850pbr0/eng/psbooks/tsec/chapter.htm?File=tsec/htm/tsec10.htm](http://docs.oracle.com/cd/E15645_01/pt850pbr0/eng/psbooks/tsec/chapter.htm?File=tsec/htm/tsec10.htm)

- UserID
- Language Code
- Date and Time Issued
- Issuing System – Node name
- Signature = SHA1\_Hash ( UserID + Lang + Date Time issued + Issuing System + Node Password )

Node Password is a “pre-shared key”. This is only one unknown value

What can we do in theory?

- Get a PS\_TOKEN cookie
- Get all necessary values and a signature from the PS\_TOKEN. It's base64 encoded
- Make offline brute force attack on PS\_TOKEN. Just add passwords to the values and compare results of hash with a signature.
- SHA1 – we can do it really fast with GPU

*If we get a node password, we can create a new cookie with “PS” user name and get full access in PeopleSoft Application.*

- Reverse Engineering  
(Thx for <https://goo.gl/hRklU6> )

General view:

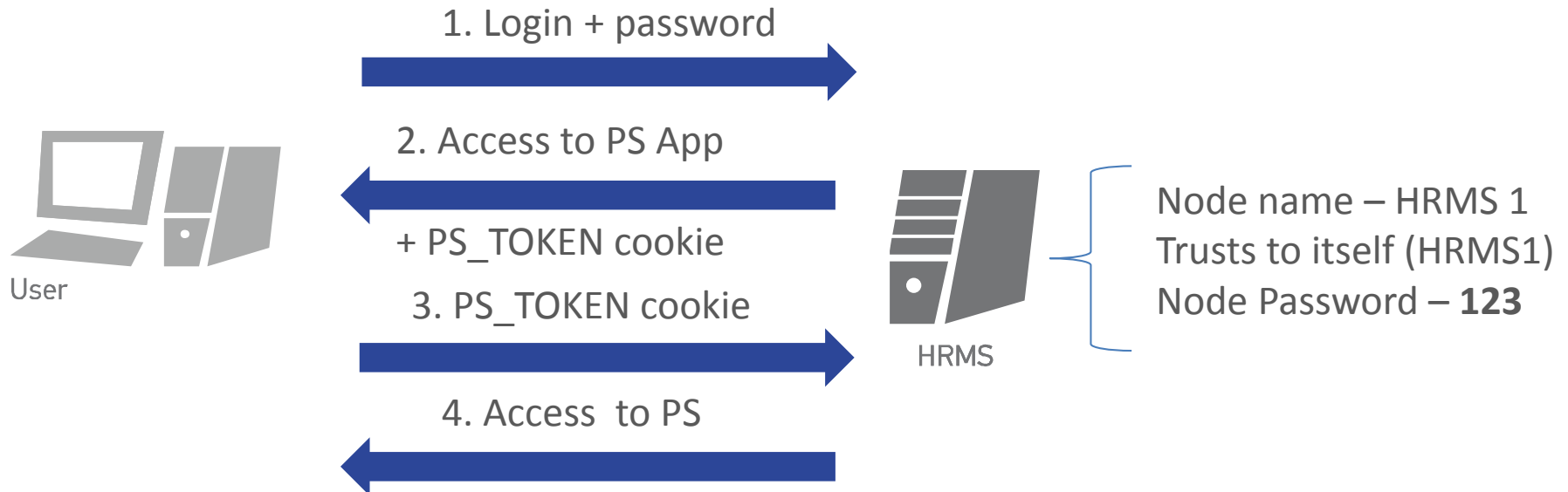
- Magic/Static numbers
- Lengths of parts
- SHA-1 hash
- Compressed data:
  - UserID
  - Lang
  - Node Name
  - Date And Time
- Don't trust Oracle's documentation =(
- Our new tool - "tokenchpoken" can parse, brute and re-create a PS\_TOKEN cookie

```
print "possible the header"
print full_str[0:4].encode('hex')+" - full length"
print hex(len(full_str))+" real length"
print full_str[4:8].encode('hex')+" - magic number"
print full_str[8:12].encode('hex')+" - static"
print full_str[12:16].encode('hex')+" - static"
print full_str[16:20].encode('hex')+" - static"

print
print "possible the hash"
print full_str[20:24].encode('hex')+" - full hash length"
print hex(len(full_str[20:64])) , " - real hash length"
print full_str[24:26].encode('hex')+" - str size"
print full_str[26].encode('hex')+" - S"
#print full_str[26] , " - full hash length?"
print full_str[27:30].encode('hex')+" - hdr"
print full_str[30:35].encode('hex')+" - unknown"
print full_str[35:43].encode('hex')+" " + full_str[35:44] , " - 8.10"
print full_str[43].encode('hex')+" - hash length"
print full_str[44:64].encode('hex')+" - SHA-1"
print
print "possible the body"
print full_str[64:68].encode('hex')+" - full body length"
print hex(len(full_str[64:]))+" real body length"
print len(full_str[64:])
print full_str[68:70].encode('hex')+" - str size"
print full_str[70].encode('hex')+" - S"
#print full_str[26] , " - full hash length?"
print full_str[71:75].encode('hex')+" - hdr"
print full_str[75].encode('hex')+" - full data length"
print hex(len(full_str[76:]))+" real body length"
print full_str[76:]+" - data"
```

- A PS application can consist of some nodes. But there must be one default local node. Of course, it trusts itself.
- There is a lot of situation when an administrator has to set a Node Password.

*So we can perform the attack on a standalone PS application.*



DEMO



## Restriction:

- As we want to get a PS\_TOKEN cookie, we need to have valid credentials on a PS server for the attack.

And how about an anonymous attack?

It looks like:

- It's impossible to have access to some resources (components) of a PS Portal without authentication.
- But sometimes it's necessary. Like, "Jobs forms" or "Forgot password?"
- You must set up a special auto-login UserID in a PS application with minimal privs
- And, of course, the PS application gives you a PS\_TOKEN cookie

*So, we can get PS\_TOKEN and perform an attack "without" valid credentials.*

- PS SSO can be used in other Oracle's application. Like, JD Edwards
- PS\_TOKEN can be used for authentication in PS IGW
- A PS\_TOKEN cookie is often set for a parent domain (.server.com)
- There is a (default) value for a node password – “password”

How can we defense a PS application?

- Use certificates instead of passwords
- Set a really strong password for nodes (max – 24 symbols)
- Set “No Authentication” for nodes

## Internal attack vectors:

- Get Connect ID -> Get Access ID - > Pwn PS
- If you are a developer, you are an admin

## External attack vectors:

- Weblogic default account -> Authoriz bypass -> RCE
- XXE -> Read configs -> Pwn PS
- Brute PS IGW account ->...-> RCE
- Get PS\_TOKEN -> Brute a Node Password -> Create a new PS\_TOKEN -> Pwn PS

## 60+ Innovative Presentations in security conferences in 25+ countries





## ERPScan Research – Leadership in ERP Security

- 300+ vulnerabilities in top vendors including SAP and Oracle
- 60+ Innovative Presentations in security conferences in 25+ countries
- Award-winning research papers “SAP Security in figures”
- Authors of the Book about Oracle Database security
- Experts in different areas from Mobile to Hardware

*The company expertise is based on research conducted by the ERPScan research center*

*Each ERP landscape is unique and we pay close attention to the requirements of our customers and prospects. ERPScan development team constantly addresses these specific needs and is actively involved in product advancement. If you wish to know whether our scanner addresses a particular aspect, or simply have a feature wish list, please e-mail us or give us a call. We will be glad to consider your suggestions for the next releases or monthly updates.*

**228 Hamilton Avenue, Fl. 3,  
Palo Alto, CA. 94301**

**USA HQ**

**Luna ArenA 238 Herikerbergweg,  
1101 CM Amsterdam**

**EU HQ**

[www.erpscan.com](http://www.erpscan.com)  
[info@erpscan.com](mailto:info@erpscan.com)