Digital Security
Research Group

Stupid mistakes. Architecture and business logic vulnerabilities.

Alexandr Polyakov

Alexey Sintsov

ConFidEncE 2010

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

Who are this guys?

Alexandr Polyakov

- 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

Alexey Sintsov

- Security Researcher/Exploit developer
- Auditer/Pen-tester(http://dsecrg.com)

- Article writer for magazine (http://xakep.ru)
- Speaker at CONFIdence, HITB, PCIDSSRUSSIA2010, Ruscrypto, Chaos Construction

OWASP

PCI DSS.RU
by Digital Security

Digital Security ДМК

Безопасность Oracle глазами аудитора: нападение и защита

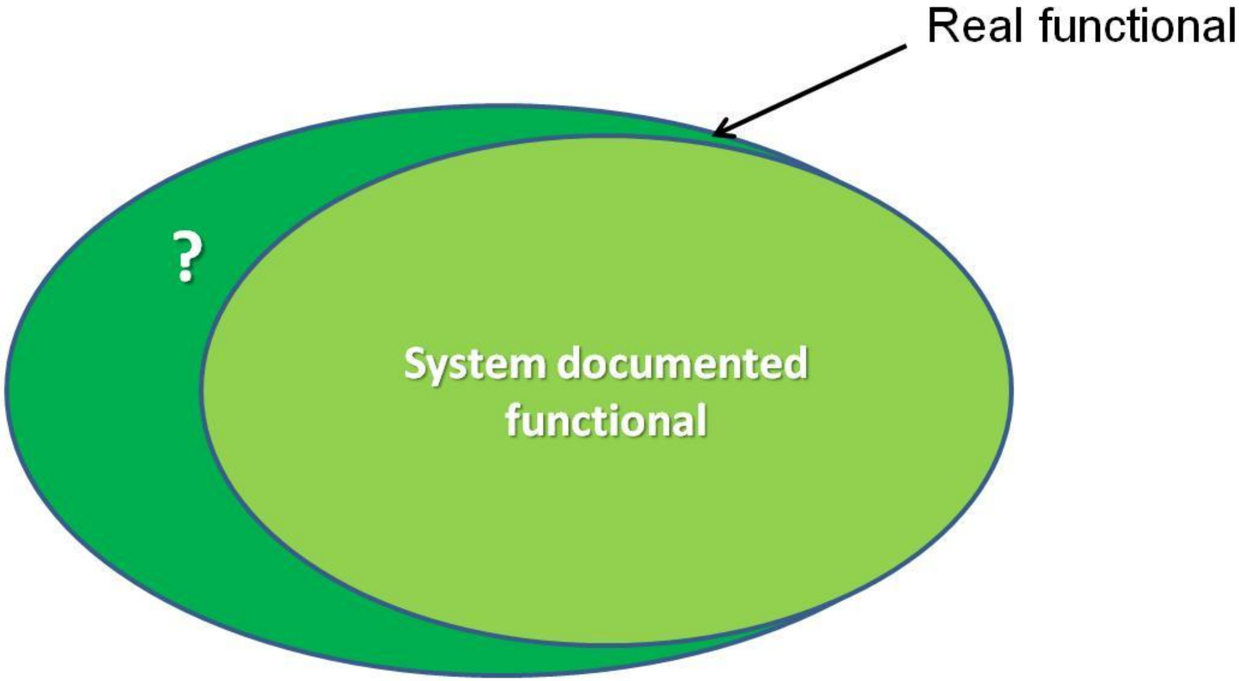
Александр Поляков

ERPScan
Security Scanner for SAP NetWeaver

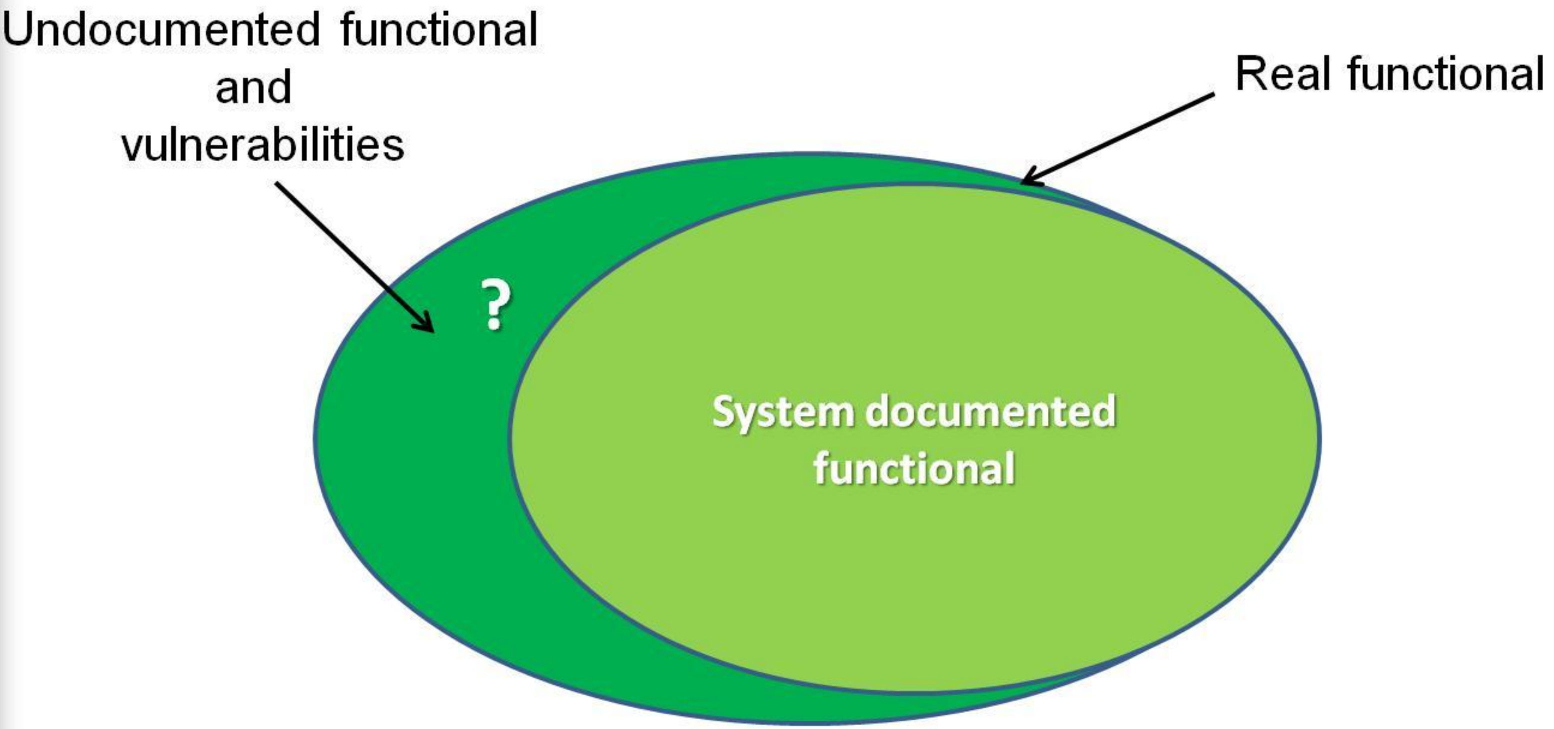
Digital Security
Research Group

And we do business application security analyze…

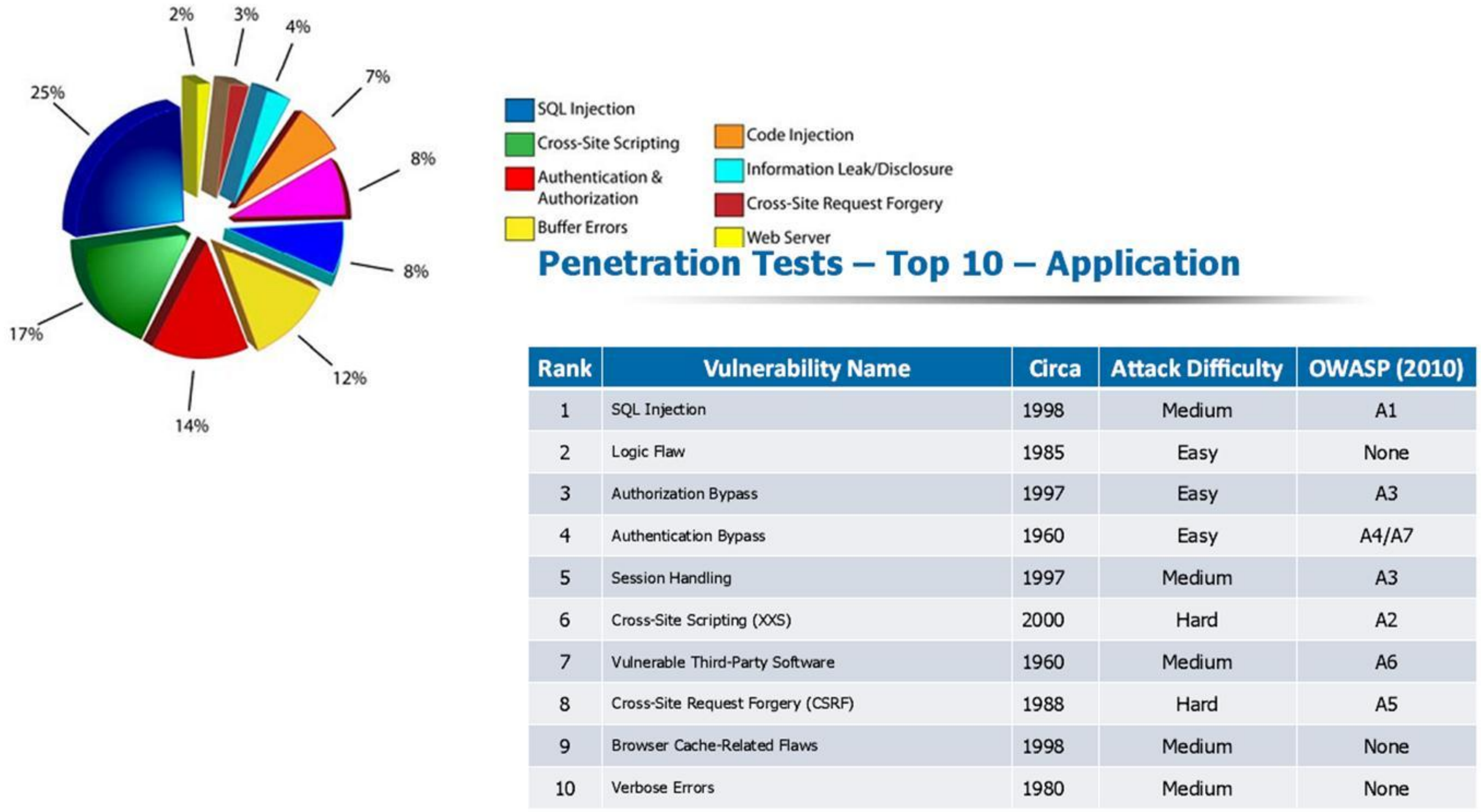
They do what?



They do what?


Undocumented functional
and
vulnerabilities
Real functional
?
System documented
functional

Is it really popular?



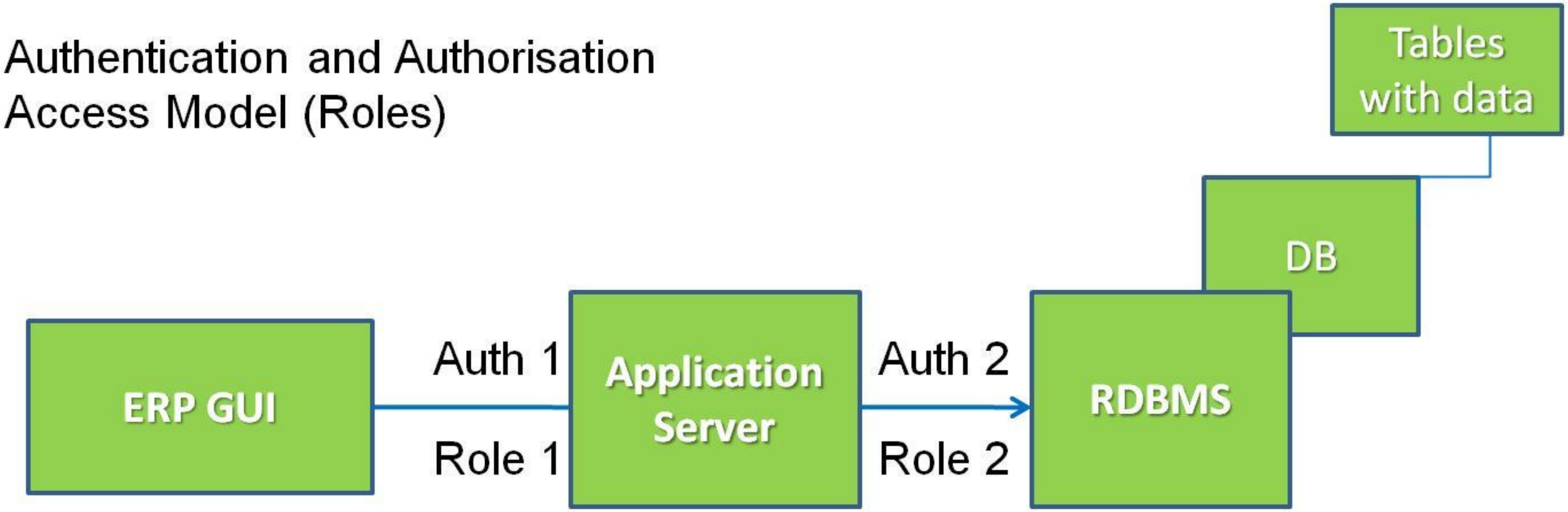
Penetration Tests – Top 10 – Application

Rank	Vulnerability Name	Circa	Attack Difficulty	OWASP (2010)
1	SQL Injection	1998	Medium	A1
2	Logic Flaw	1985	Easy	None
3	Authorization Bypass	1997	Easy	A3
4	Authentication Bypass	1960	Easy	A4/A7
5	Session Handling	1997	Medium	A3
6	Cross-Site Scripting (XXS)	2000	Hard	A2
7	Vulnerable Third-Party Software	1960	Medium	A6
8	Cross-Site Request Forgery (CSRF)	1988	Hard	A5
9	Browser Cache-Related Flaws	1998	Medium	None
10	Verbose Errors	1980	Medium	None

http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q1-Q2-2009.pdf
http://www.blackhat.com/presentations/bh-dc-10/Percoco_Nicholas/BlackHat-DC-2010-Percoco-Global-Security-Report-2010-slides.pdf

First line of defence

- Authentication and Authorisation
- Access Model (Roles)



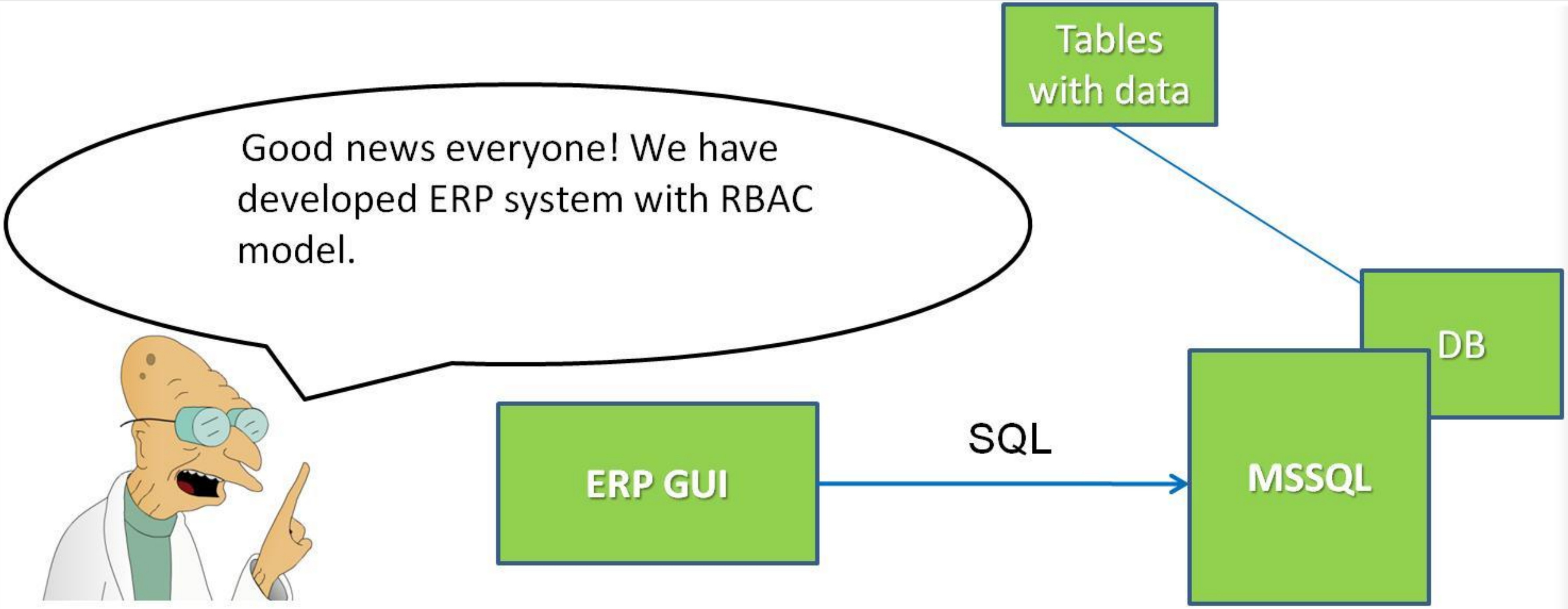
Agenda

Real stories from security assessment projects:

- Story about bad RBAC
- Story about bad auth model (0day will be presented)
- Sad story about big FAIL…

History 1. Beer

Real story…



Good news everyone! We have developed ERP system with RBAC model.

Tables with data

DB

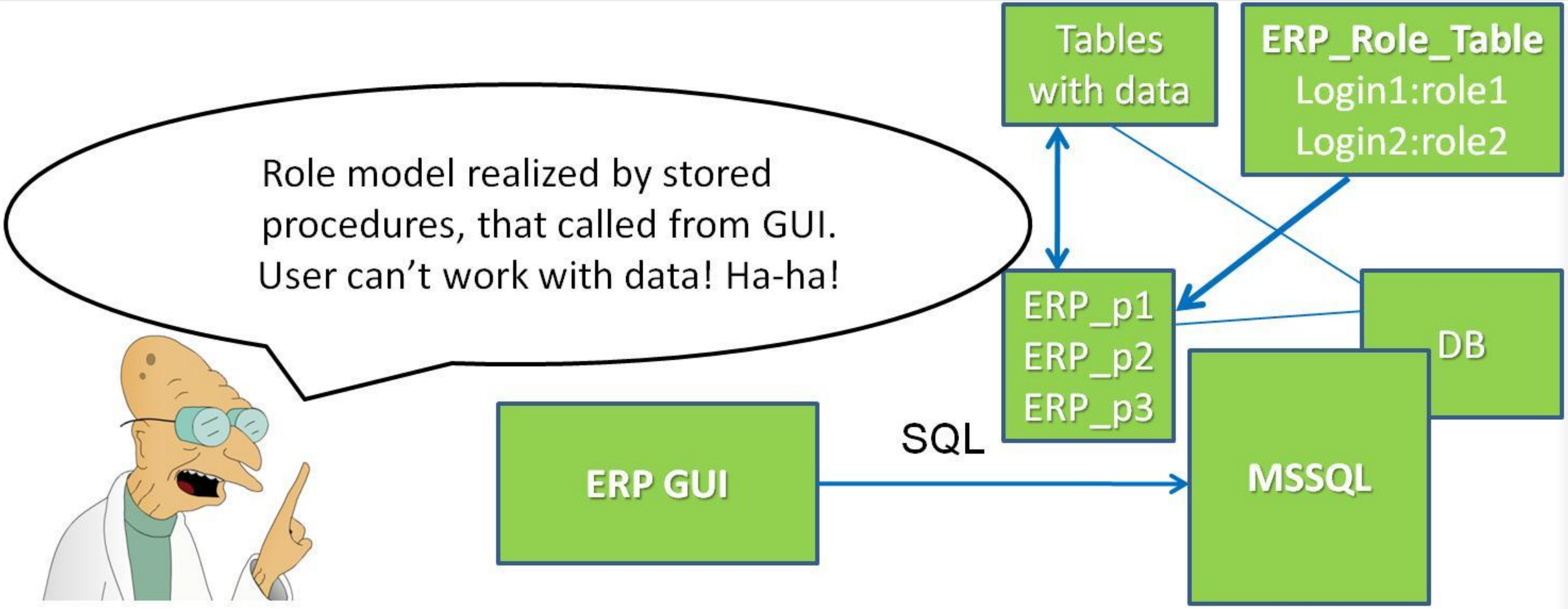
SQL

ERP GUI

MSSQL

- Role Based Access Control
- Auth via NTLM
- User account have not any rights on DB

Real story…


Role model realized by stored procedures, that called from GUI. User can’t work with data! Ha-ha!

Tables with data

ERP_Role_Table
Login1:role1
Login2:role2

ERP_p1
ERP_p2
ERP_p3

DB

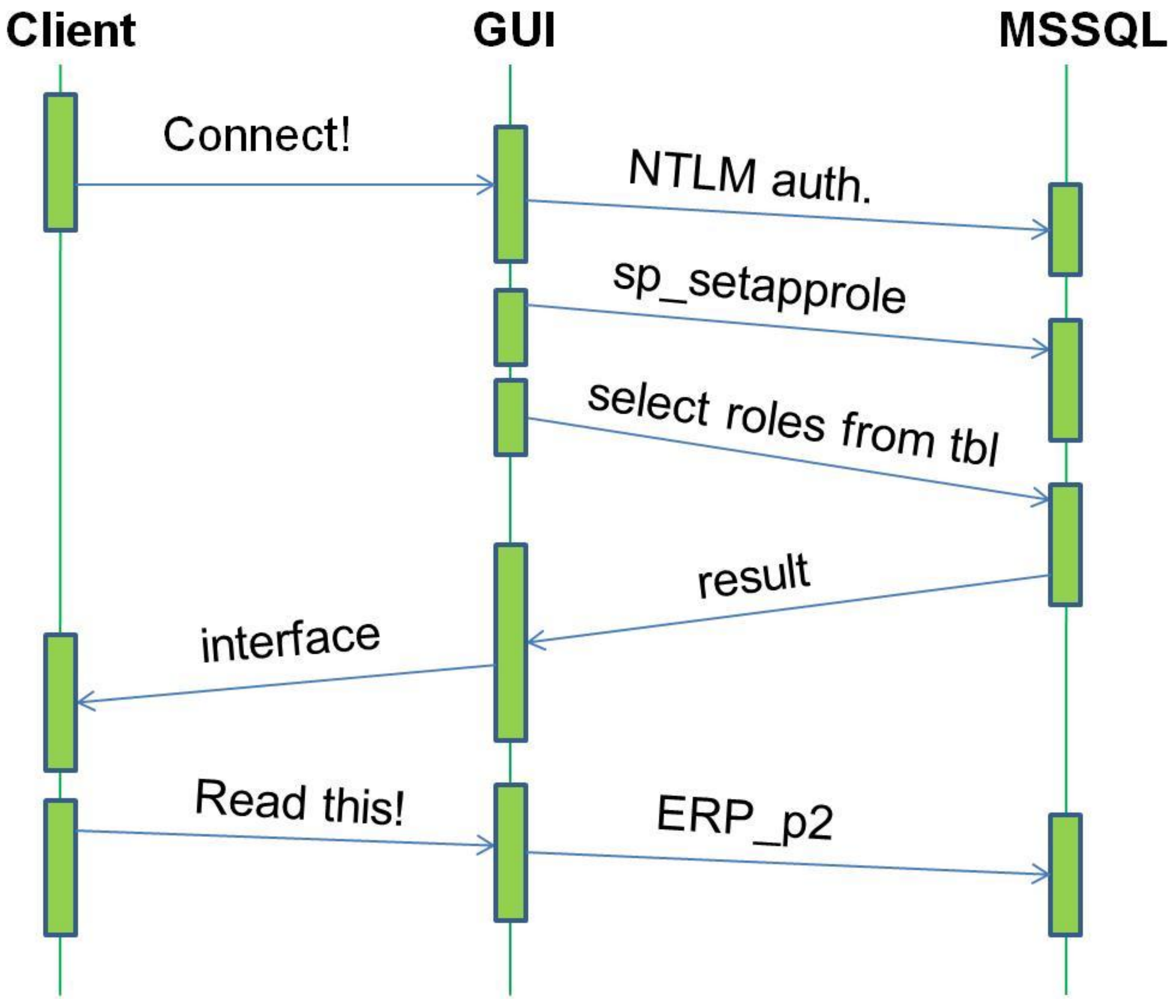
ERP GUI

SQL

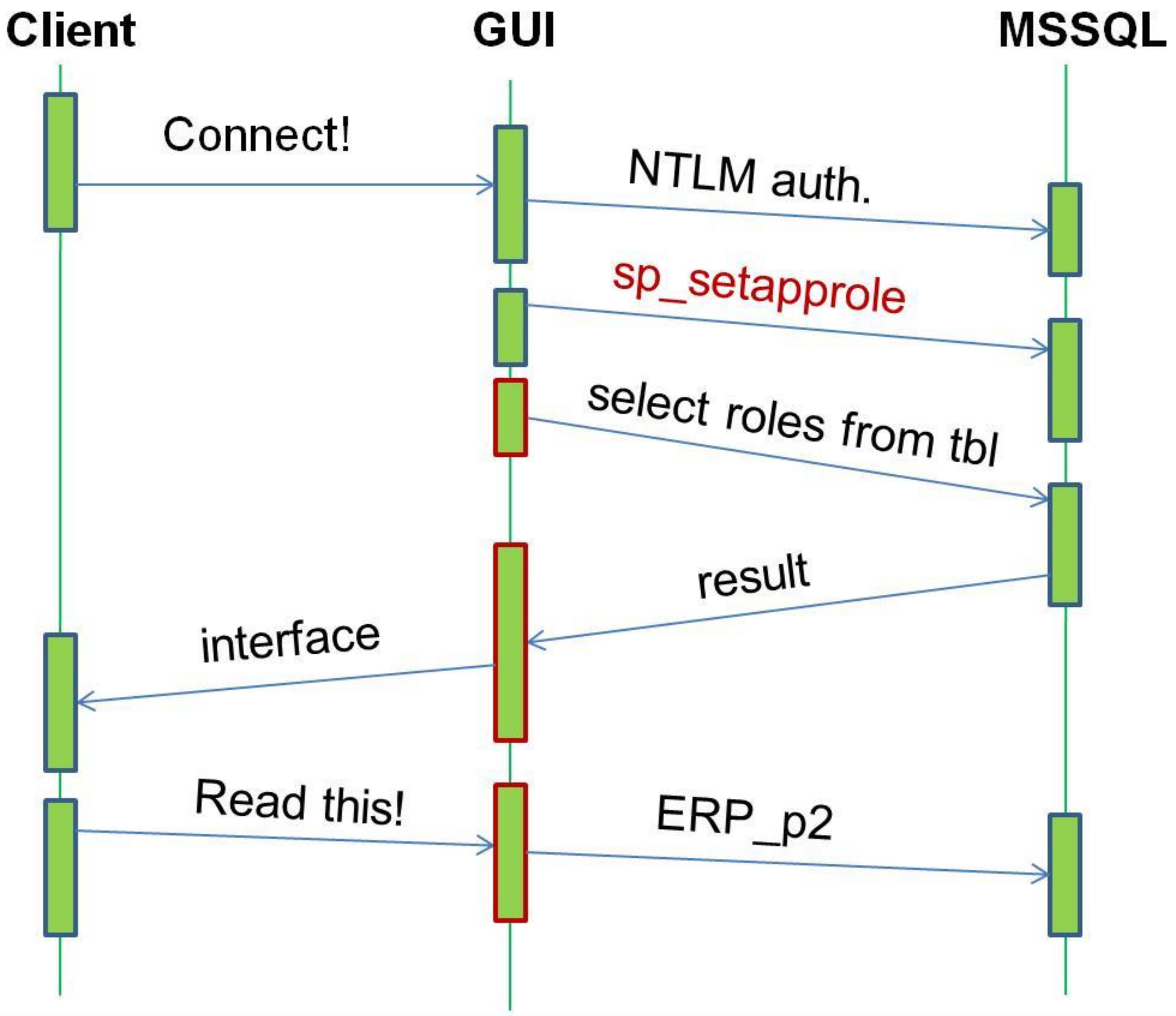
MSSQL

- Every account has special “role”
- Users can work with DB by stored procedures
- Every stored procedure can executed by user with special “role”

But(t)...


Client
GUI
MSSQL
Connect!
NTLM auth.
sp_setapprole
select roles from tbl
result
interface
Read this!
ERP_p2

But(t)...


Client
GUI
MSSQL
Connect!
NTLM auth.
sp_setapprole
select roles from tbl
result
interface
Read this!
ERP_p2

Conclusion

What we have?

- User can’t work with DB… (cool)
- But in fact: application role work with DB, not User account
- Users “role” checked by client software (GUI interface)
- Application use sp_setapprole impersonation mechanism (password is hardcoded) for extended rights

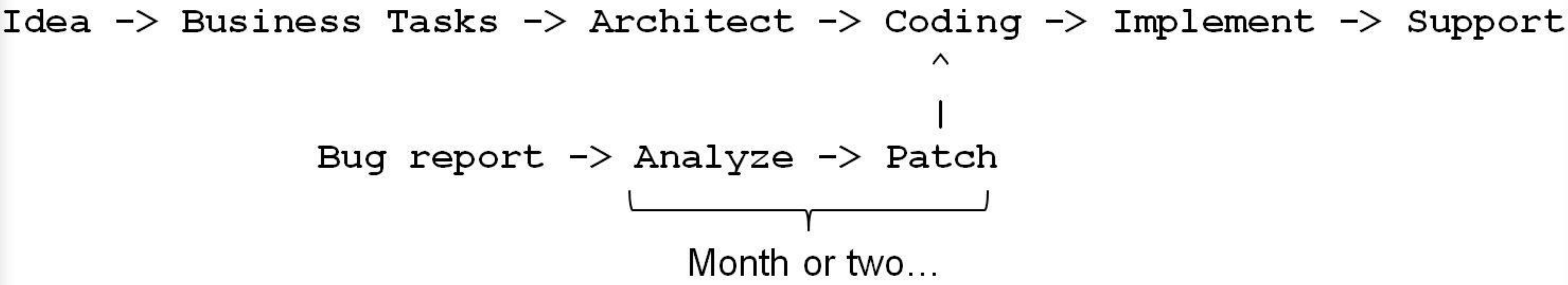
What about logging?

- Every table has triggers, that logging request to “special “ table
- But “special” table in the same DB with the same rights and don’t have any triggers…

Attack

1. Sniff the encrypted password for sp_setapprole
2. Connect via RDBMS client
3. Use encrypted application password (sp_setapprole)
4. Update ERP_ROLE_TABLE
5. Profit – new GUI functions are available.

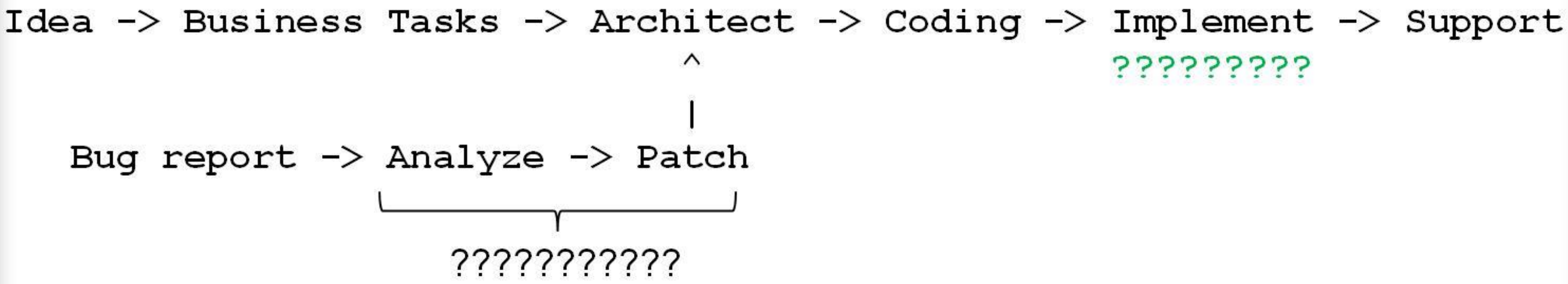
Simple bug in ‘coding’ stage



```
Idea -> Business Tasks -> Architect -> Coding -> Implement -> Support
                                          ^
                                          |
             Bug report -> Analyze -> Patch
```

Month or two…

Bug in ‘Architect’ stage



```
Idea -> Business Tasks -> Architect -> Coding -> Implement -> Support
                                ^                     ?????????
                                |
   Bug report -> Analyze -> Patch
                 ????????????
```

Digital Security
Research Group

History 2. Retail

Let us introduce

Progress® OpenEdge® is the leading SaaS platform for simplifying and streamlining the development, integration, and management of business applications for deployment ‘in the cloud’. With OpenEdge, Independent Software Vendors and Business Service Providers can enjoy flexible deployment to a variety of public and private cloud providers. Join the growing community of SaaS providers that rely on OpenEdge to help make smarter and faster decisions, resulting in greater operational responsiveness.

© progress.com

Popular software

This **RDBMS** used by Fortune 100:

- PepsiCo
- Mars (Master Foods)
- Daewoo
- Coca-Cola
- Mariott (hotels)
- Gillette
- Johnson & Johnson
- Black & Decker
- Lucent Technologies
- Lockheed Martin
- Colgate-Palmolive
- Heineken
- Mercedes-Benz
- Ford Motor
- Company
- British Petroleum
- AT&T
- Rockwell
- Mazda Motor Corporation
- Danon
- United Technologies
- McDonnell-Douglas
- Sony

and more, more, more…

Known vulnerabilities

CVE-2007-2417

Heap-based buffer overflow in _mprosrv.exe in
Progress Software Progress 9.1E and OpenEdge 10.1x

CVE-2007-3491

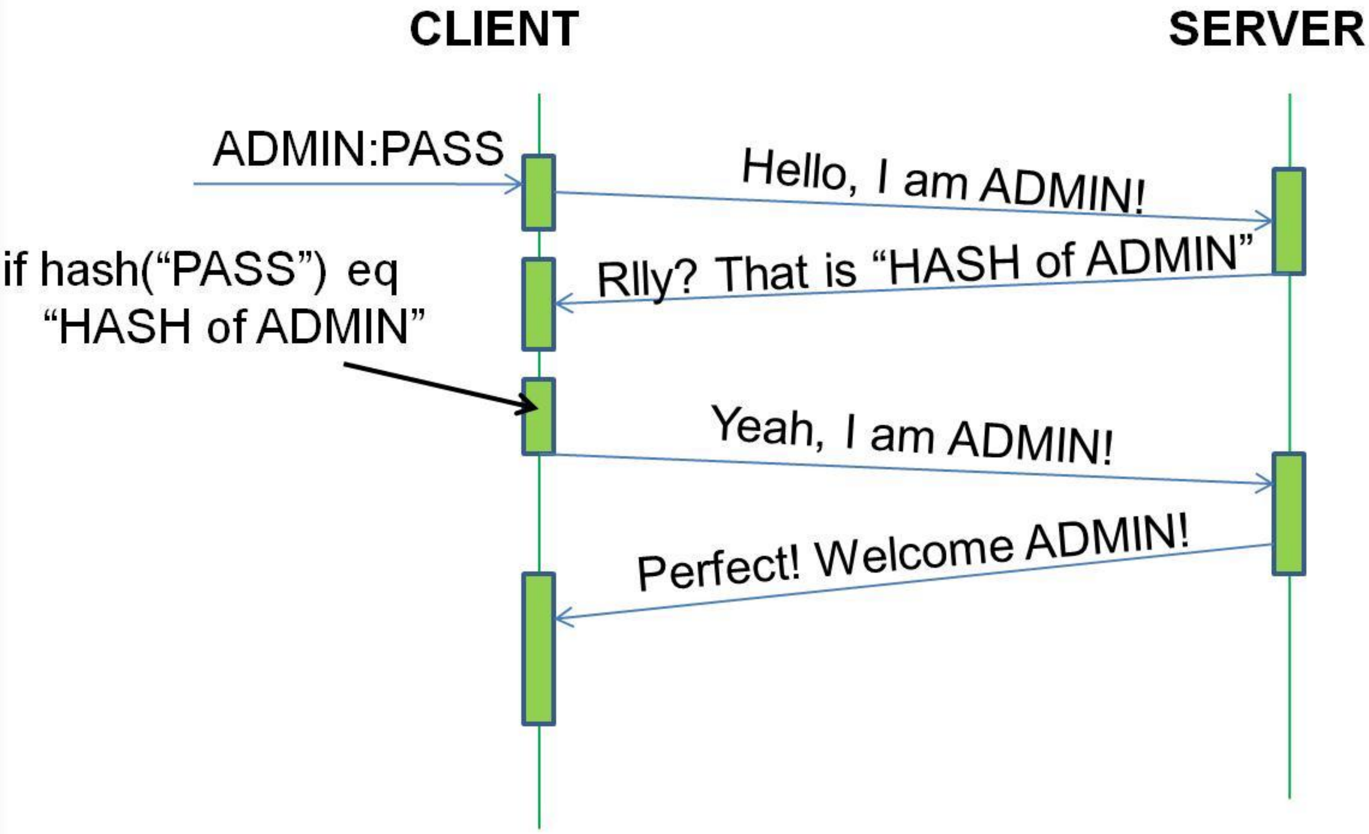
Buffer overflow in _mprosrv in Progress Software OpenEdge before 9.1E0422,
and 10.x before 10.1B01

CVE-2007-2506

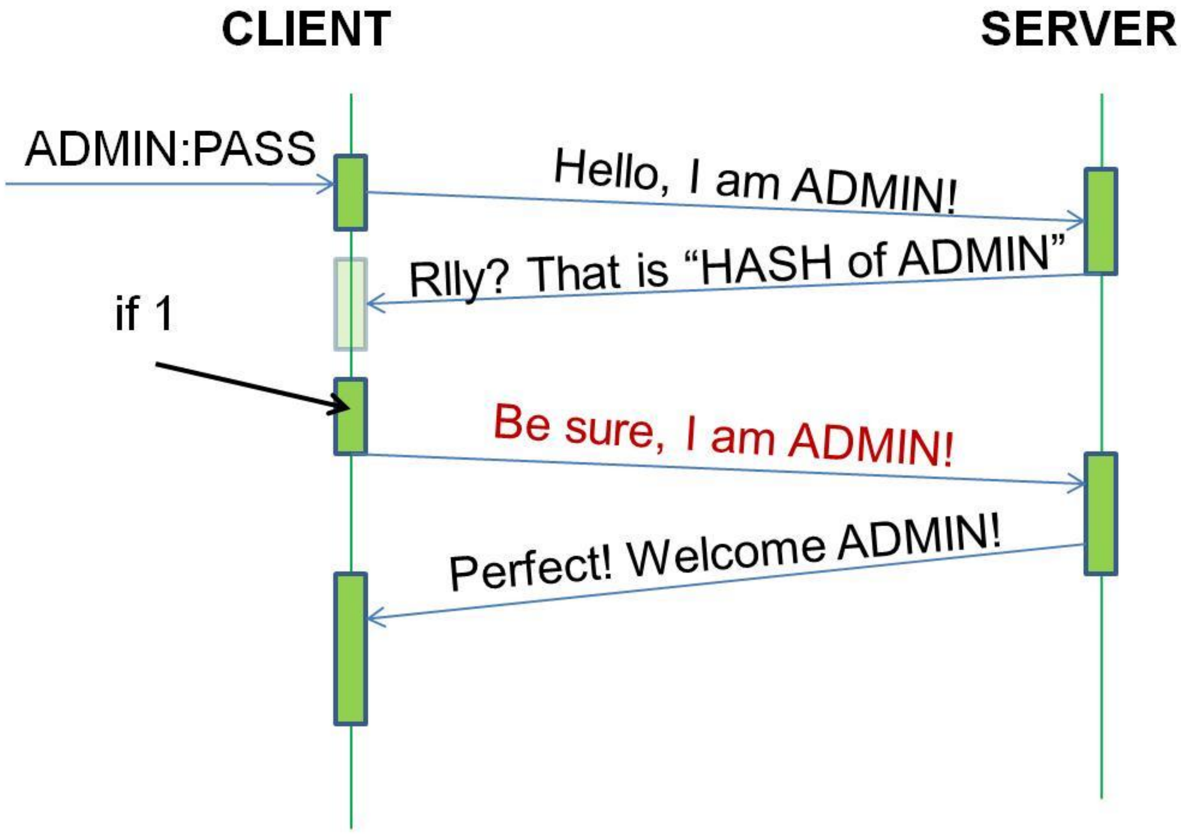
WebSpeed 3.x in OpenEdge 10.x in Progress Software Progress 9.1e,
and certain other 9.x versions, allows remote attackers to cause a
denial of service (infinite loop and daemon hang)

0DAY EXPLOIT DEMO

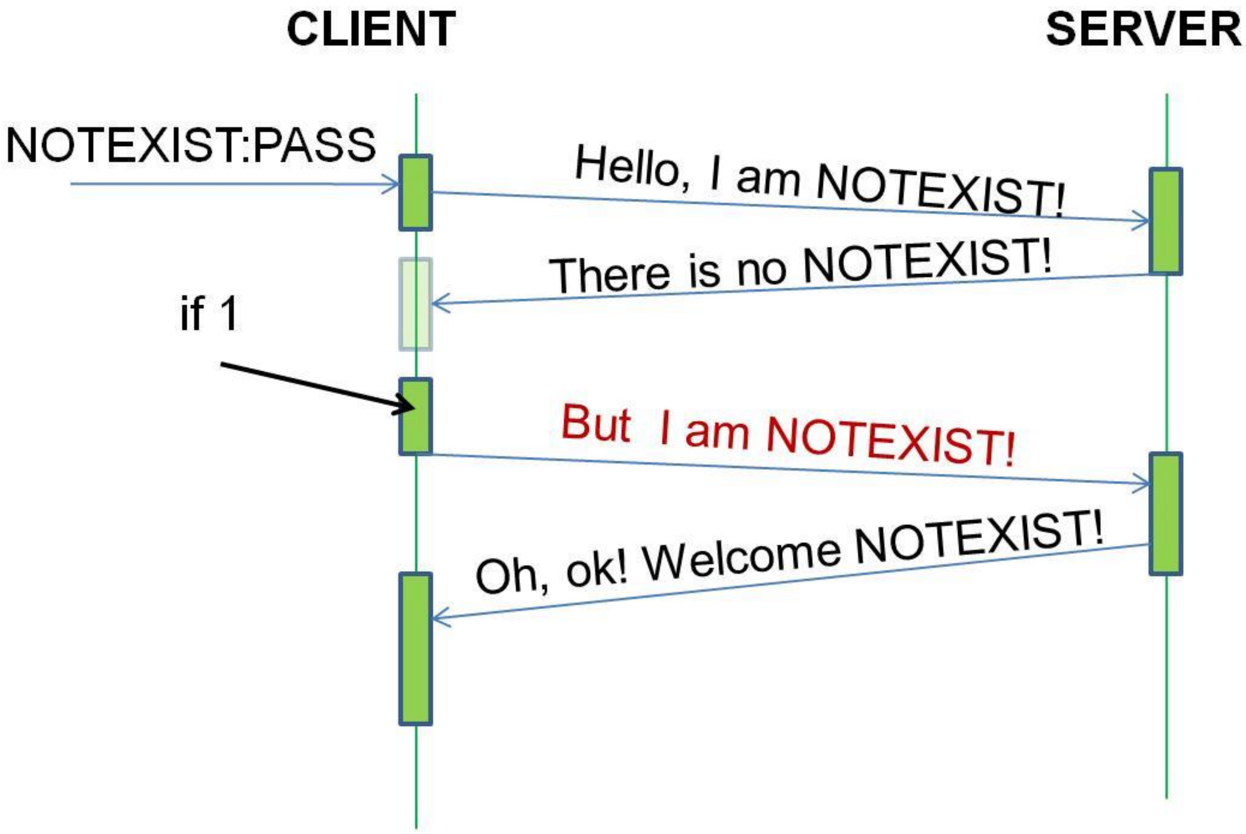
Bug


CLIENT
SERVER
ADMIN:PASS
Hello, I am ADMIN!
Rlly? That is “HASH of ADMIN”
if hash(“PASS”) eq
“HASH of ADMIN”
Yeah, I am ADMIN!
Perfect! Welcome ADMIN!

Bug


CLIENT
SERVER
ADMIN:PASS
Hello, I am ADMIN!
Rlly? That is “HASH of ADMIN”
if 1
Be sure, I am ADMIN!
Perfect! Welcome ADMIN!

Bug


CLIENT
SERVER
NOTEXIST:PASS
Hello, I am NOTEXIST!
There is no NOTEXIST!
if 1
But I am NOTEXIST!
Oh, ok! Welcome NOTEXIST!

What did you seen?

- Hypnotoad
- Real story
- Auth bypass 0day [DSECRG-09-063]
  http://dsecrg.com/pages/vul/show.php?id=163

Responsible disclosure

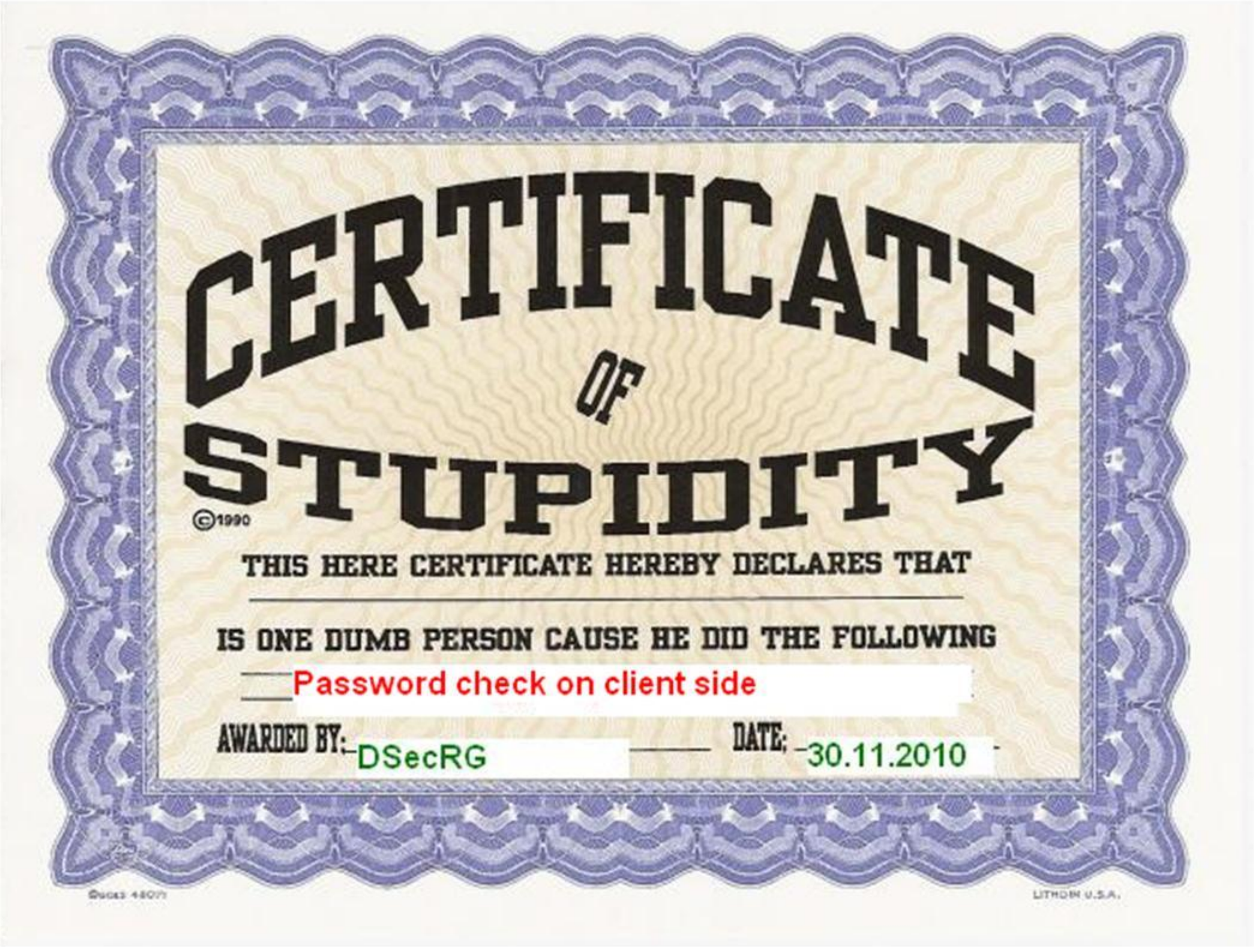
Official answer:

"The Progress Software OpenEdge RDBMS database security flaws that you have notified us about do exist in a network client-server model that uses the built-in user accounts. However, this configuration does not represent the current state of deployed OpenEdge applications. While some old/legacy applications may continue to use this architecture, the numbers continue to decline. **We find this configuration used mostly at companies where the data's value does not warrant moving to a more secure application architecture**." © *Progress*

Can not be patched – backward compatibility conflict, but we can defend system

- Use n-tier model
- **Do not use build-in user accounts (empty _user table)**

Congratilations!



CERTIFICATE OF STUPIDITY

©1990

THIS HERE CERTIFICATE HEREBY DECLARES THAT

IS ONE DUMB PERSON CAUSE HE DID THE FOLLOWING

Password check on client side

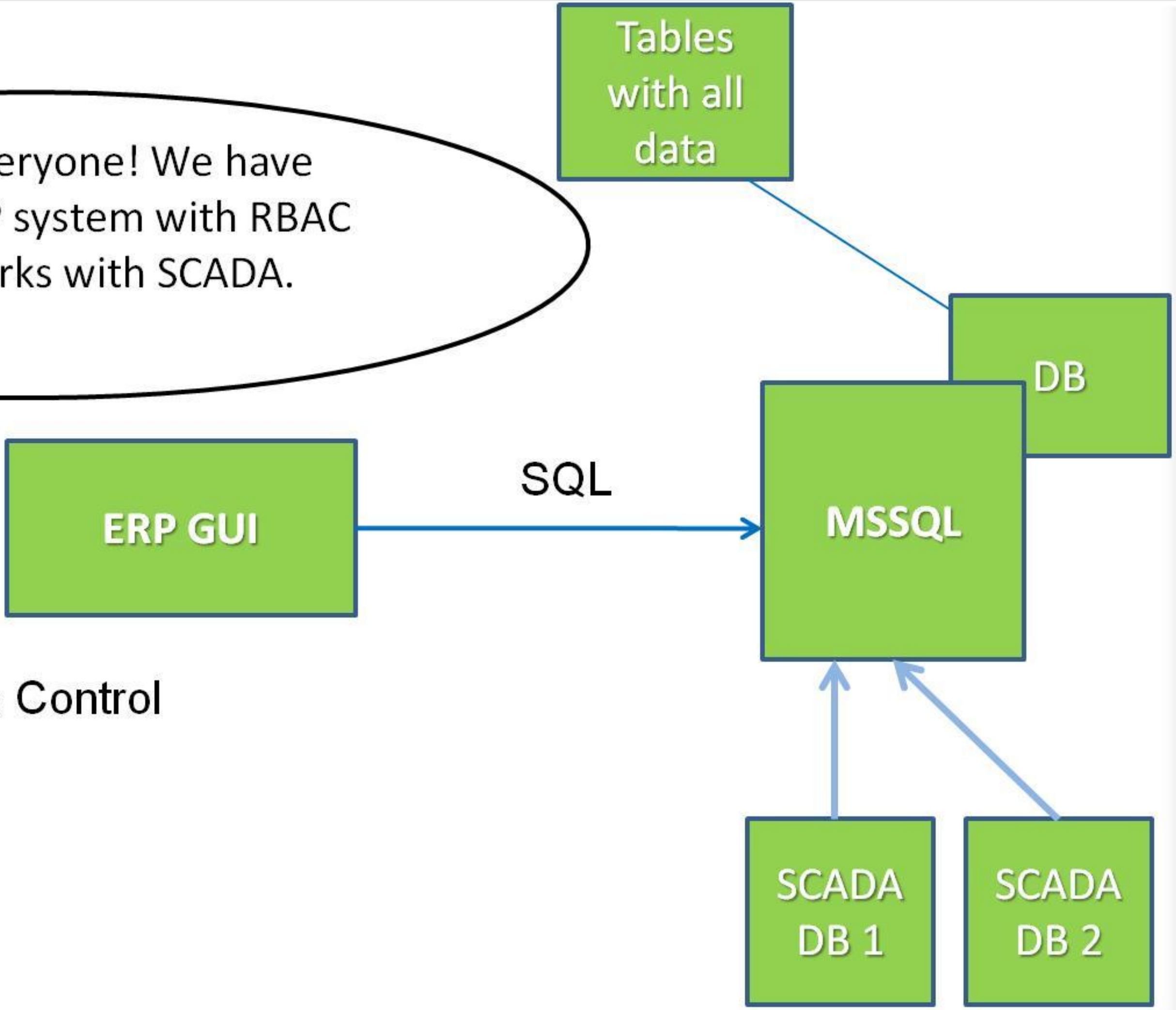
AWARDED BY: DSecRG DATE: 30.11.2010

©GOES 48071 LITHO IN U.S.A.

History 3: Who want to steal some gasoline?

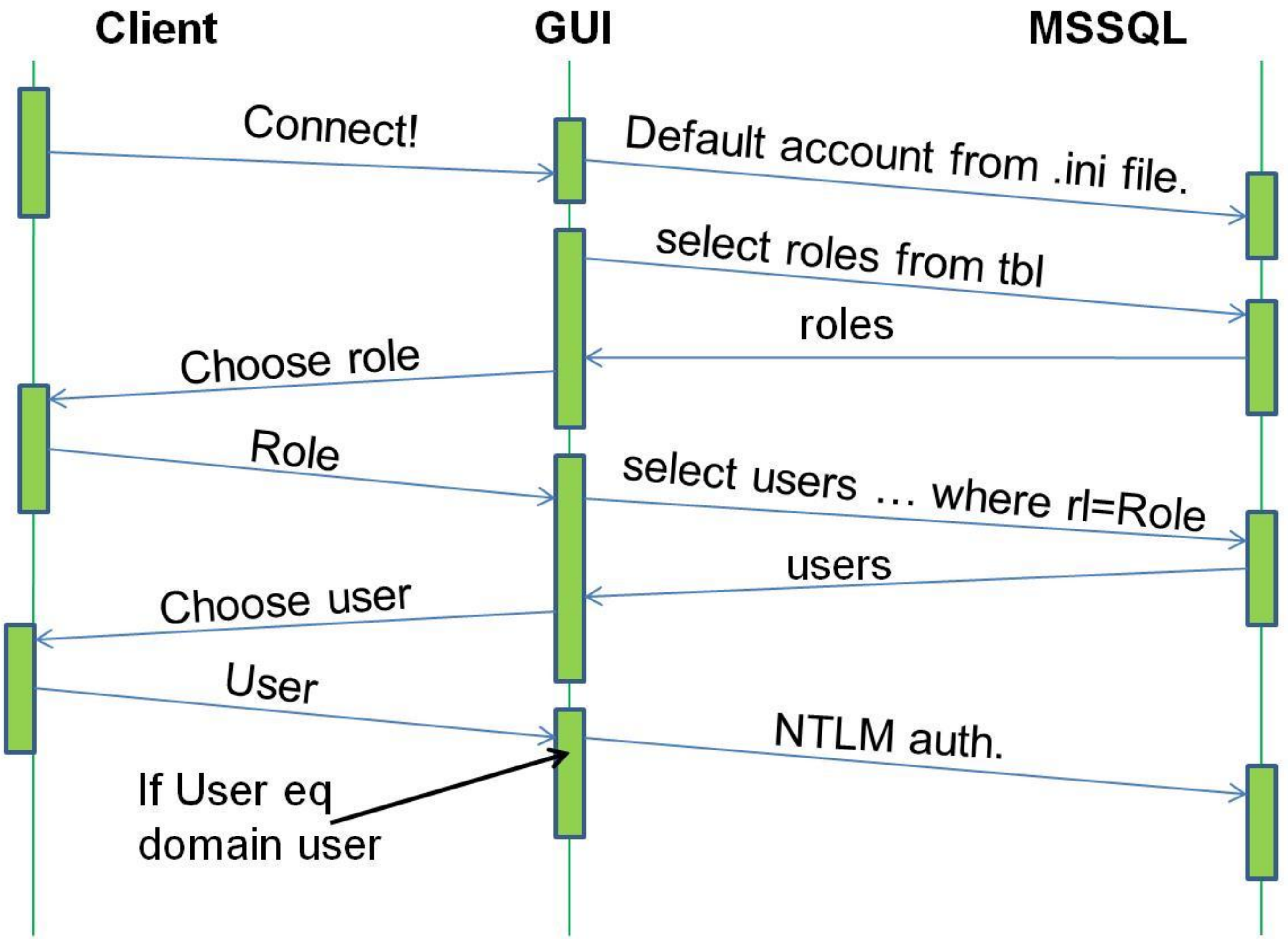
OIL sector – another story

Good news everyone! We have developed ERP system with RBAC model that works with SCADA.

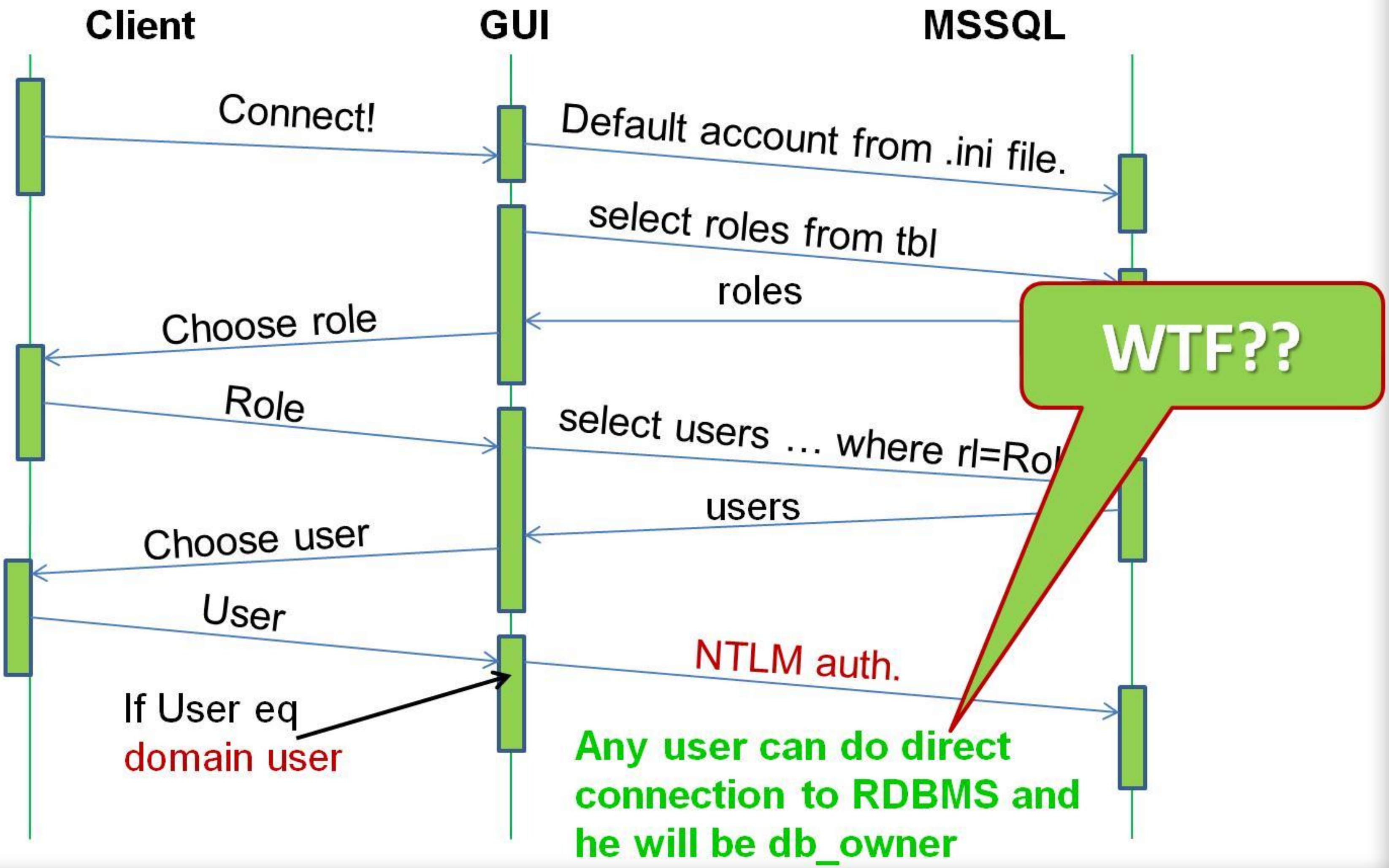


- Role Based Access Control
- Auth via NTLM

Problems

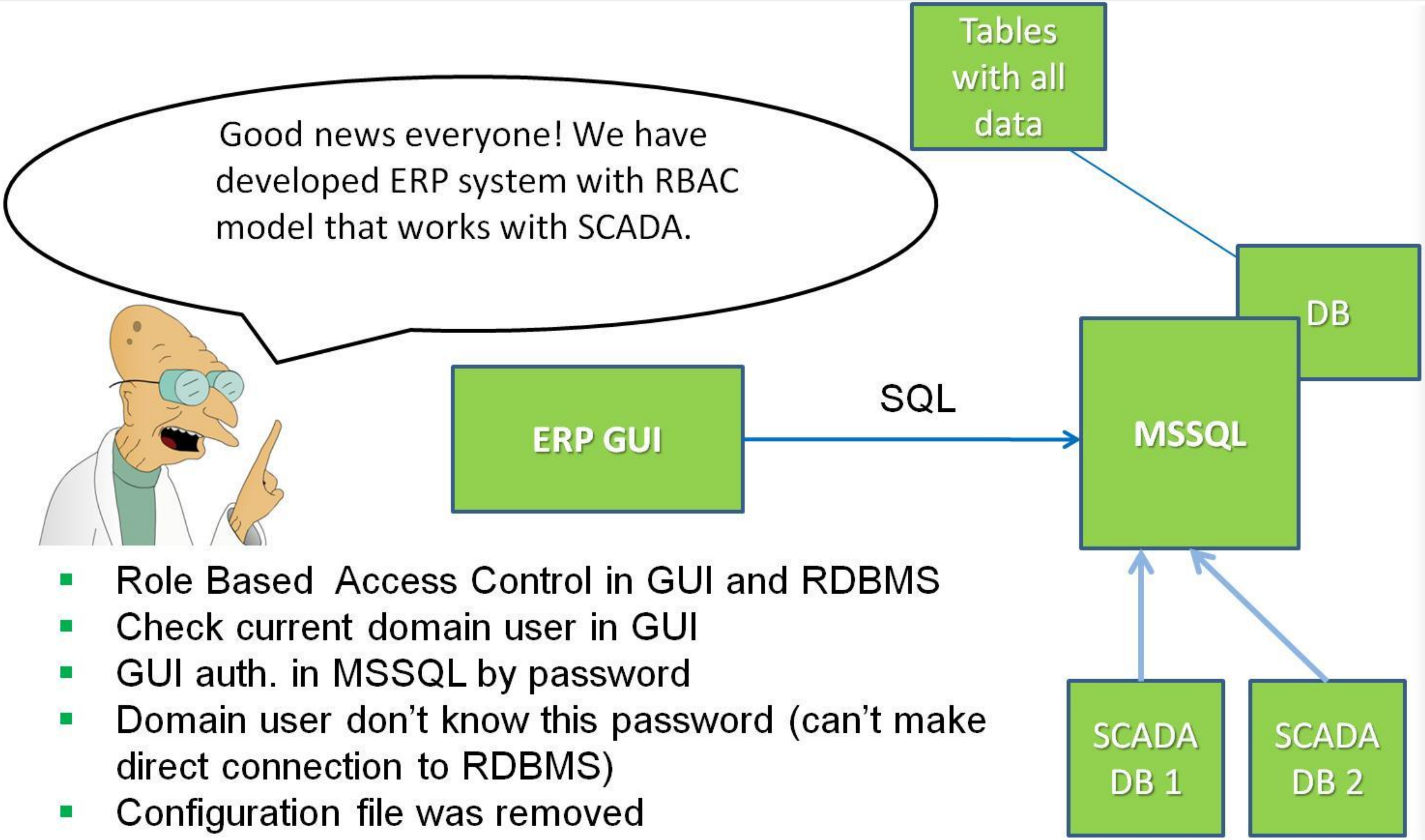

Client
GUI
MSSQL
Connect!
Default account from .ini file.
select roles from tbl
roles
Choose role
Role
select users … where rl=Role
users
Choose user
User
NTLM auth.
If User eq
domain user

Problems



Any user can do direct connection to RDBMS and he will be db_owner

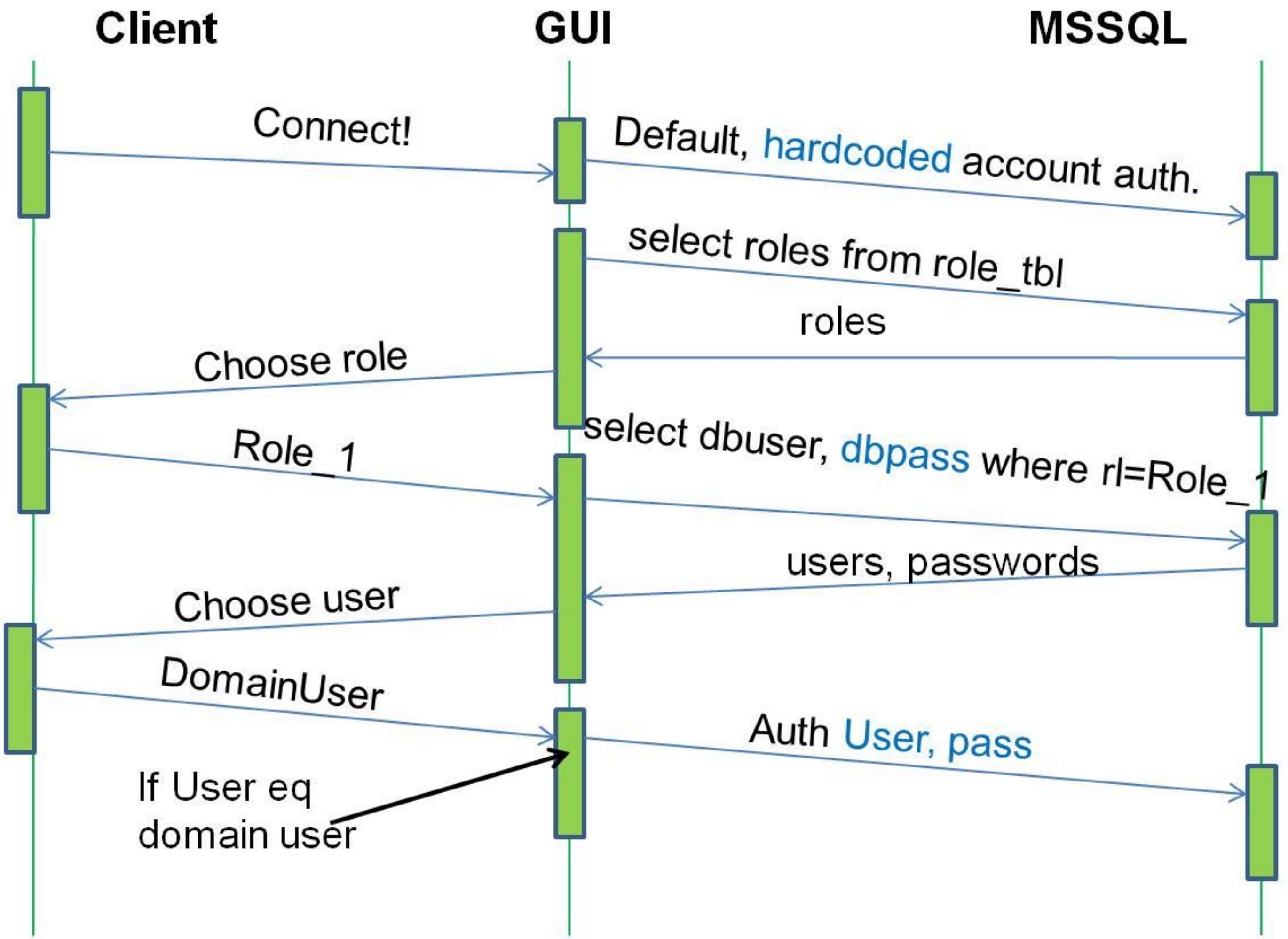
OIL sector – another story


Good news everyone! We have developed ERP system with RBAC model that works with SCADA.
Tables with all data
DB
ERP GUI
SQL
MSSQL
SCADA DB 1
SCADA DB 2

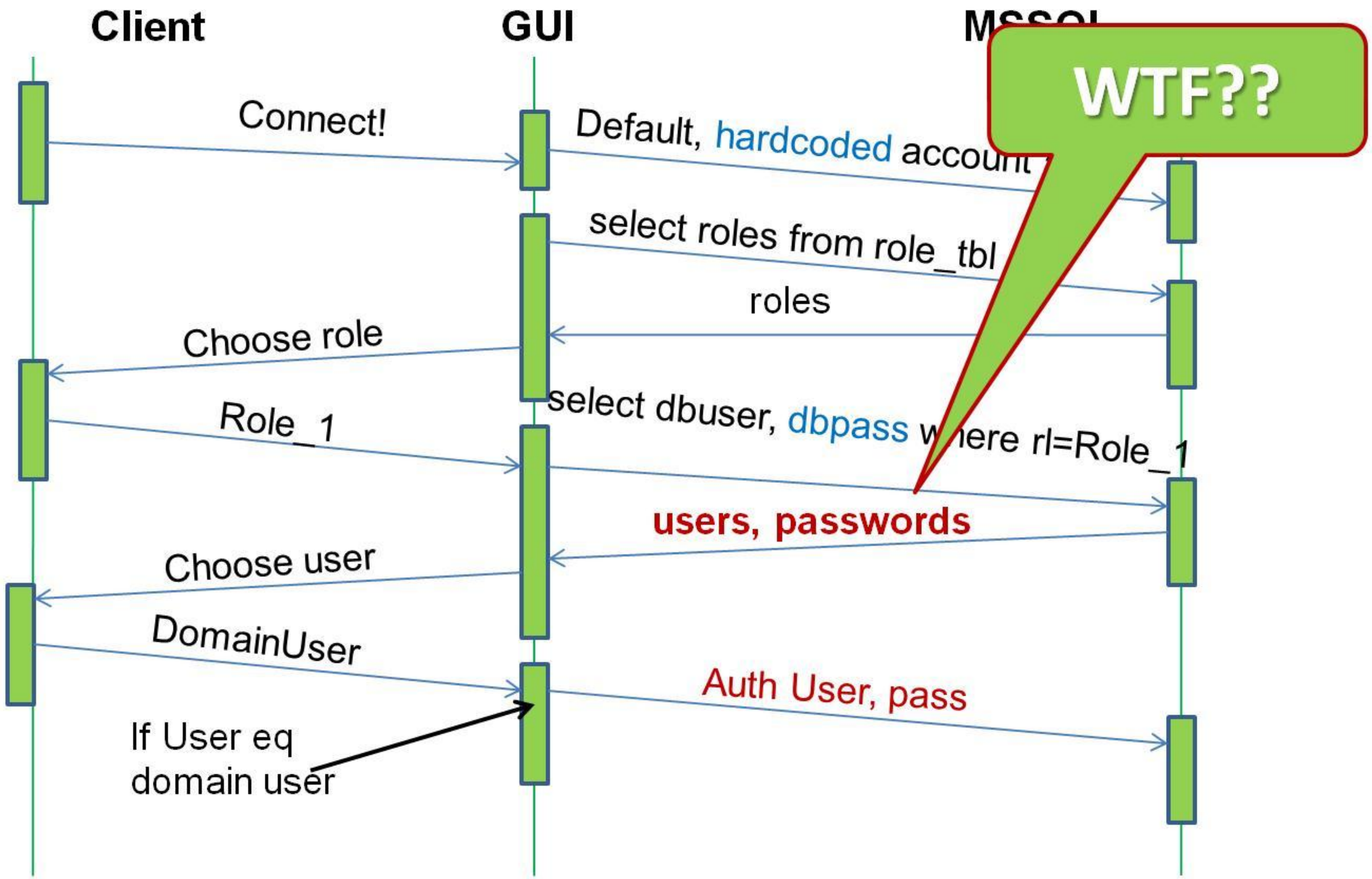
- Role Based Access Control in GUI and RDBMS
- Check current domain user in GUI
- GUI auth. in MSSQL by password
- Domain user don’t know this password (can’t make direct connection to RDBMS)
- Configuration file was removed

Digital Security
Research Group

Solution



Solution


Client
GUI
MSSQL
WTF??
Connect!
Default, hardcoded account
select roles from role_tbl
roles
Choose role
Role_1
select dbuser, dbpass where rl=Role_1
users, passwords
Choose user
DomainUser
Auth User, pass
If User eq
domain user

FAIL

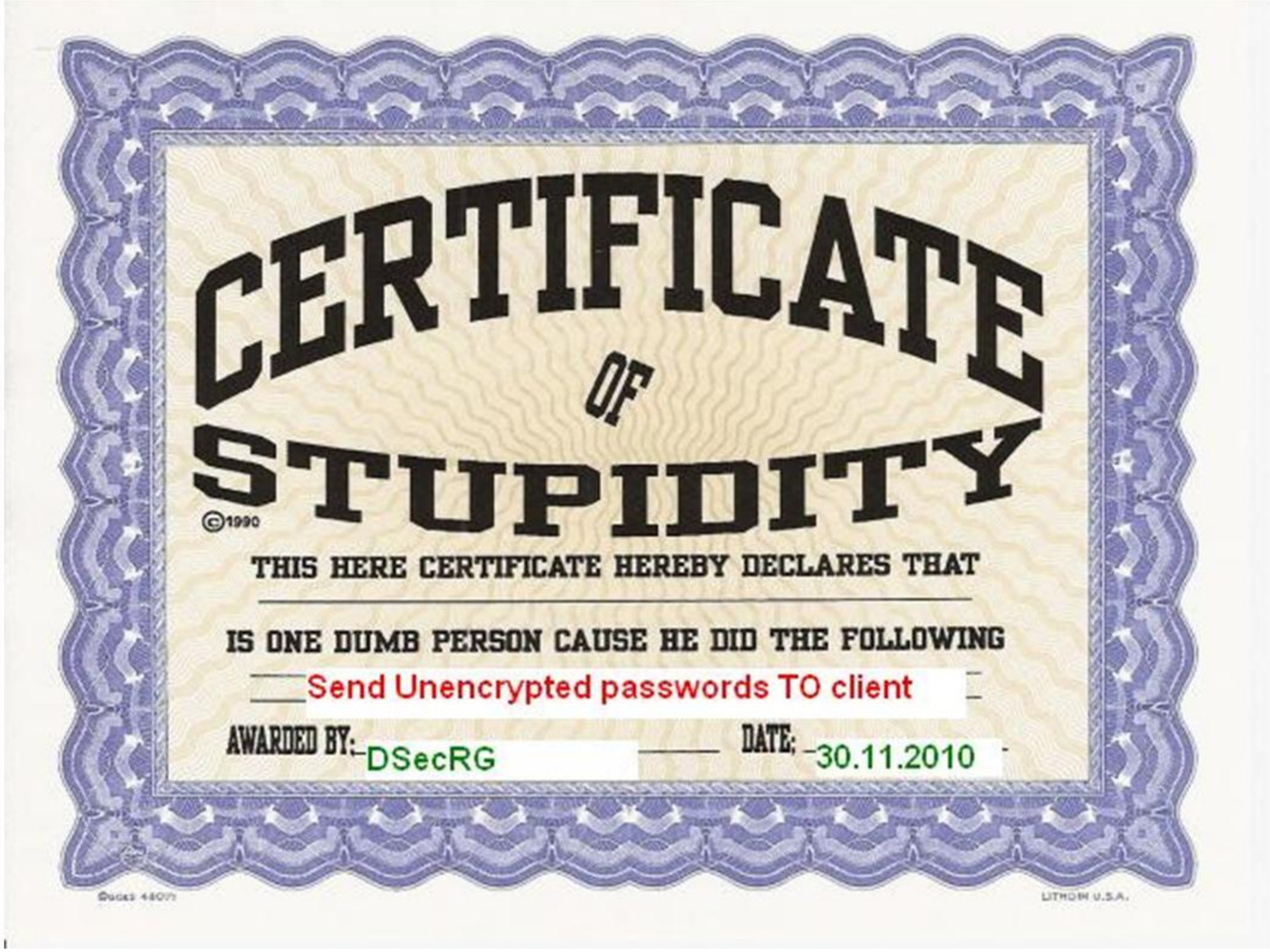
- Sniff the passwords
- Try direct connection to DB
- If u are not db_owner try another account

- BTW passwords in database are encrypted ….
- … with simple function pw_appencrypt and pw_appdecrypt used by GUI when doing ‘SELECT’

And more

- ERP RDBMS has Link to SCADA RDBMS with public link under sa account.

Congratilations!



CERTIFICATE OF STUPIDITY

©1990

THIS HERE CERTIFICATE HEREBY DECLARES THAT

IS ONE DUMB PERSON CAUSE HE DID THE FOLLOWING

Send Unencrypted passwords TO client

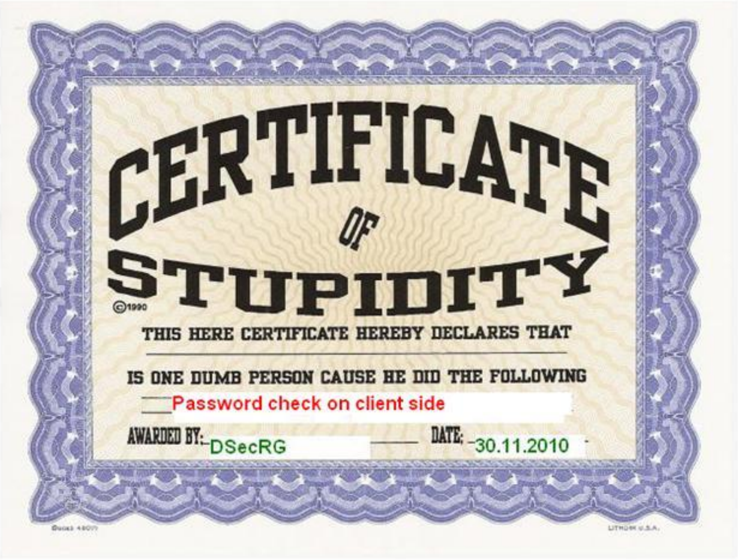
AWARDED BY: DSecRG

DATE: 30.11.2010

Goes 4807

LITHO IN U.S.A.

Vote for mini PWNIE



CERTIFICATE OF STUPIDITY

©1990

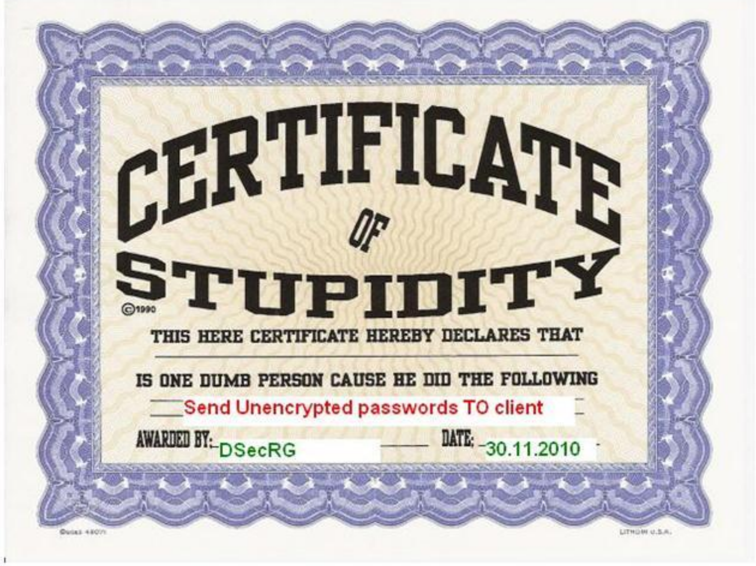
THIS HERE CERTIFICATE HEREBY DECLARES THAT

IS ONE DUMB PERSON CAUSE HE DID THE FOLLOWING

Password check on client side

AWARDED BY: DSecRG DATE: 30.11.2010

OR



CERTIFICATE OF STUPIDITY

©1990

THIS HERE CERTIFICATE HEREBY DECLARES THAT

IS ONE DUMB PERSON CAUSE HE DID THE FOLLOWING

Send Unencrypted passwords TO client

AWARDED BY: DSecRG DATE: 30.11.2010

What are this stories about?

- Think about security when doing architecture of your system
- Do not count on 3rd party applications
- Segmentation – important part of your security
- RBAC on RDBMS level
- n-tier architecture

- Not all problems in "stack overflow" or simple passwords
- Security analyze is not (only) fuzzing or scanning

Before hack/defend the System – understand this System.

Question?

www.twitter.com/sh2kerr
a.polyakov@dsec.ru

www.twitter.com/asintsov
a.sintsov@dsec.ru

ConfidEncE 2010