

# User authentication in TransbaseCD RDBMS

Research Seminar in Cryptography

September 7, 2016

# TransbaseCD RDBMS

# TransbaseCD RDBMS

**transbase**®  
the SQL engine

# TransbaseCD RDBMS



“Transbase CD is a variant of the SQL database system that stores the database contents in ROM files. These are typically distributed on media like DVDs in large quantities. Transbase CD supports mechanisms for online distribution of partial updates.”

<https://www.transaction.de/en/products/technologies/transbase-cd.html>

# TransbaseCD RDBMS



“Transbase CD is a variant of the SQL database system that stores the database contents in ROM files. These are typically distributed on media like DVDs in large quantities. Transbase CD supports mechanisms for online distribution of partial updates.”

<https://www.transaction.de/en/products/technologies/transbase-cd.html>

Used by Daimler AG to distribute Service Manuals and Electronic Parts Catalogs to workshops and dealers.

# Mercedes-Benz EPC

# Mercedes-Benz EPC

EPC net - EPC02087

File Options Functions Search Help

Identification number WDB 2030921F863754 WDBP92H97F863754

MD mode 1. Car 203092 C 280 4-MATIC 203.092 42 BRAKES 030 FRONT WHEEL BRAKE

Item...	Part number	Designation/description	Quantity
<input type="checkbox"/> 10	A 003 420 25 83	CALIPER LEFT, WITHOUT LINING	001
<input type="checkbox"/> 10	A 003 420 26 83	CALIPER RIGHT, LESS LINING	001
<input type="checkbox"/> 15	A 000 420 92 55	BLEEDER VALVE LEFT AND RIGHT	002
<input type="checkbox"/> 20	A 000 421 10 48	PROTECTIVE CAP BLEEDER VALVE	002
<input type="checkbox"/> 35	A 000 420 67 15	BRAKE ANCHOR CALIPER	002
<input type="checkbox"/> 40	A 124 421 05 71	SCREW CALIPER TO STEERING KNUCKLE M12X1.5X35 [408] ONLY REPLACEABLE BY PAIRS	004
<input type="checkbox"/> 45	A 000 421 98 86	RS COLLAR BRAKE CYLINDER	002
<input type="checkbox"/> 50	A 001 421 04 86	BOOT BELLOWS	002
<input type="checkbox"/> 60	A 003 420 60 20	BRAKE PAD PARTS KIT [431] WHEN SELLING BRAKE LININGS T	001
<input type="checkbox"/> 80	A 211 540 17 17	SENSOR BRAKE LINING WEAR INDICATOR	001

Shopping list transfer file

Write protection	Shopping list	Date/Time	Dam...	Item no.	Part number	ES1	ES2	Designation/description	Quantity	Qty o...	Price
<input type="checkbox"/>	-- Temporary shopping list --										

Market: North America - Catalog: 69N -

# Connecting using JDBC driver



# Connecting using JDBC driver

The screenshot displays the DbVisualizer Free 9.5 - EPC interface. The main window is titled "Database Connection: EPC" and shows the connection details for a Transbase database. The connection string is `jdbc:transbase://localhost:2034/ALLTEXT`. The driver is identified as `transbase`. The database user is `tbuser`. The interface includes a menu bar (File, Edit, View, Database, SQL Commander, Tools, Window, Help), a toolbar, and a sidebar with "Connections" and "Favorites" sections. The "Connections" section shows a tree view of the database structure, including folders for "Folder", "EPC", "TBADMIN", "SYSTEM TABLE", "SYSTEM VIEW", "TABLE", and "VIEW". The "Database" section shows the connection settings, including the database type, driver, and authentication details. The "Authentication" section shows the database user and password. The "Connection Message" section displays the following information:

```
@(#) Transbase Database System Version: V6.6.2.15 (Build 428) 2007/11/27 (Release) License:
EF4159A0-51DFCC67-CA6355A6-0721CE9C U.S.-Patent Nr. 6,381,596 and 6,510,335 Copyright (c) 1987 -
2005 by Transaction Software, D 81829 Munich
V6.6.2.15
Transbase JDBC driver
Release Version 3.0 Build 20101213(419)
```

At the bottom of the window, there is a status bar indicating "Evaluation period has ended" and a system tray showing "73M of 341M".

# Connecting using JDBC driver

The screenshot shows the DbVisualizer Free 9.5 interface. The title bar reads "DbVisualizer Free 9.5 - EPC/TBADADMIN/SYSTEM VIEW/SYSUSER". The menu bar includes File, Edit, View, Database, SQL Commander, Tools, Window, and Help. The left sidebar shows a tree view of databases under "EPC", with "TBADMIN" expanded to show "SYSTEM VIEW" and "SYSUSER" selected. The main window displays the "Table: SYSUSER" with columns USERNAME, USERCLASS, PASSWD, and USERID. The table contains three rows of data.

	USERNAME	USERCLASS	PASSWD	USERID
1	PUBLIC	no access		0
2	TBADADMIN	dba	C54o2XQ1VNMdmqpjQNXxoA.e/K1REI6	1
3	TBUSER	access	RgHM.Pm/TIAzuTBnb0TfPc.e/K1REI6	2

At the bottom of the window, there is a status bar with "Max Rows: 1000", "Max Chars: -1", "0.000/0.000 sec", "3/4", "1-3", and "74M of 341M". A red warning icon in the bottom left corner indicates "Evaluation period has ended".

# Connecting using JDBC driver

DbVisualizer Free 9.5 - EPC/TBADMIN/SYSTEM VIEW/SYSUSER

File Edit View Database SQL Commander Tools Window Help

Databases

Connections

- Folder
- EPC
  - TBADMIN
    - SYSTEM TABLE
    - SYSTEM VIEW
      - LOADINFO
      - SYBLOB
      - SYSCOLUMN
      - SYSCOLUMNPRIV
      - SYSCONSTRAINT
      - SYSDOMAIN
      - SYSEXTERNAL
      - SYSEXTERNALMET
      - SYSEXTERNALPRI
      - SYSINDEX
      - SYSREFCONSTR
      - SYSURROGATE
      - SYSTABLE
      - SYSTABLEPRIV
      - SYSTRIGGER
      - SYSUSER**
      - SYSVIEW
      - SYSCUSER

Table: SYSUSER  
EPC/TBADMIN/SYSTEM VIEW/SYSUSER

Info Columns Data Row Count Primary Key Indexes Grants

	USERNAME	USERCLASS	PASSWD	USERID
1	PUBLIC	no access		0
2	TBADMIN	dba	C54o2XQ1VNMdmqjQNx:xA.e/K1REI6	1
3	TBUSER	access	RgHM.Pm/TIAzuTBnb0TfPc.e/K1REI6	2

password('C2mpTbicc')

Max Rows: 1000 Max Chars: -1 0.000/0.000 sec 3/4 1-3 74M of 341M

Evaluation period has ended

# Connecting using JDBC driver

The screenshot shows the DbVisualizer interface with the following components:

- Connections:** A tree view on the left showing the database hierarchy: EPC > TBADMIN > SYSUSER.
- Table: SYSUSER:** The main window displays the table structure and data. The columns are USERNAME, USERCLASS, PASSWD, and USERID.
- Data Table:**

*	USERNAME	USERCLASS	PASSWD	USERID
1	PUBLIC	no access		0
2	TBADMIN	dba	C54o2XQ1VNMdmqpjQNx:xaA.e/K1REI6	1
3	TBUSER	access	RgHM.Pm/TIAzuTBnb0TfPc.e/K1REI6	2
- Annotations:** Red arrows point to the PASSWD cells. The first arrow points to the empty cell for PUBLIC with the text "password(?)". The second arrow points to the password for TBADMIN with the text "password('C2mpTbicc')".
- Status Bar:** Shows "Max Rows: 1000", "Max Chars: -1", "0.000/0.000 sec", "3/4", "1-3", and "74M of 341M".
- Footer:** A red warning icon and text "Evaluation period has ended".

# Research questions

## Research questions

- How to reset “tadmin” password having read-write access to database?

## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented

## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure



## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tadmin” wider access to data in the db?

## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?

## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (tjdbc.jar)

## Research questions

- How to reset “tadmin” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tadmin” wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (tjdbc.jar)
  - Document authentication protocol

## Research questions

- How to reset “tbadmIn” password having read-write access to database?
  - Such feature officially not documented
  - Requires reverse-engineering password data structure
  - Has “tbadmIn” wider access to data in the db?
- Is it possible to sniff password from db connection?
  - Reverse-engineer JDBC driver (tbjdbc.jar)
  - Document authentication protocol

Available:

- VirtualBox VM image with Windows XP and TransbaseCD (MB EPC) installed