User authentication in TransbaseCD RDBMS

Research Seminar in Cryptography

September 7, 2016
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.


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

TransbaseCD 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.


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

“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.”


Used by Daimler AG to distribute Service Manuals and Electronic Parts Catalogs to workshops and dealers.
Mercedes-Benz EPC
Connecting using JDBC driver
Connecting using JDBC driver
Connecting using JDBC driver
Connecting using JDBC driver

password('C2mpTbicc')
Connecting using JDBC driver

password(?)

password(‘C2mpTbicc’)
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
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
Research questions

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