Vulnerability: A debugger's readability to CPU registers through Debug Access Port (DAP) during normal operation.

- **Description:** Debug unit can read and modify register values of processors and peripherals. Usually, debugging involves halting the execution once a failure has been observed and collects state information retrospectively to investigate the problem. HALT operation can be initiated by a host who can be an off-chip debugger connected to an on-chip Debug Access Port (DAP) via a JTAG interface or an on-chip processor [1]. During HALT operation, a processor stops executing according to the instruction indicated by the program counter's (PC) value, and a debugger can examine and modify the processor state via DAP. In HALT mode, the program counter's value is readable from the DAP. However, if someone can bypass the privilege access to read the PC value during normal execution through DAP, she can learn the execution flow of a program, resulting in an integrity violation.

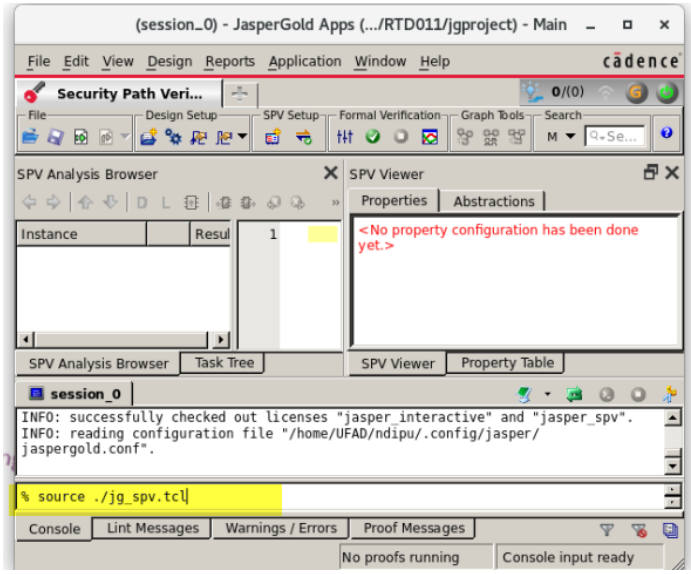
Related Security Property: Program Counter's value should not be readable through Debug Access Port (DAP) when a processor is not in HALT mode debugging.

- It should be checked in design time, whether program counter's value is readable from debug access port or not during normal mode of operation.

Design:
MSP430 microcontroller with debug infrastructure has been used to check this property. RTL codes for MSP430 micro-controller are included in ./src folder.

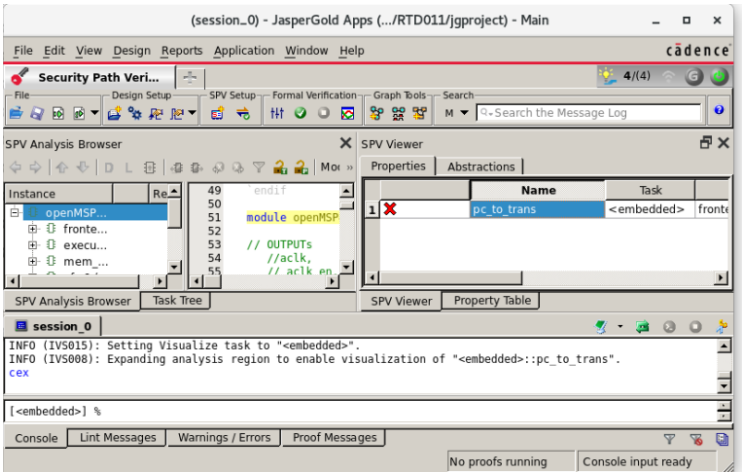
Converted Assertion:
```
check_spv -create -from {frontend_0.pc} -from_precond {dbg_0.dbg_en_s==1'b0} -to {dbg_uart_txd} -name "pc_to_trans"
```

Which tool to use: Cadence JasperGold Security Path Verification (SPV).
How to use: Use "jg -spv" command to invoke JaspaerGold SPV. Utilize "jg_spv.tcl" file to check the assertion.
[N.B: Utilize "jg_spv_21.tcl" file to check the assertion if you are using JasperGold 2021.06 FCS release.]



Result:

For the current design of the MSP430 micro-controller, the property violates, indicating that the program counter's value is readable from debug access port during normal operation.



Counterexample: The counterexample provided by JasperGold SPV tool-

Reference:

1. Farzana, Nusrat, et al. "SoC Security Verification using Property Checking." *2019 IEEE International Test Conference (ITC)*. IEEE, 2019.