



# SAP ICC

## Security Code Scan Assessment

PUBLIC

# Security Code Scan Assessment Analysis & Importance

## Analysis:

- Security vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

80%

*applications written on  
Web contain at least one  
vulnerability on initial  
assessment*

33%

*Web and mobile  
applications account for  
data breaches*

25%

*annually attacks at the  
application layer are  
growing*

4/5

*apps written in web  
scripting languages fail  
the OWASP assessment*

## Importance:

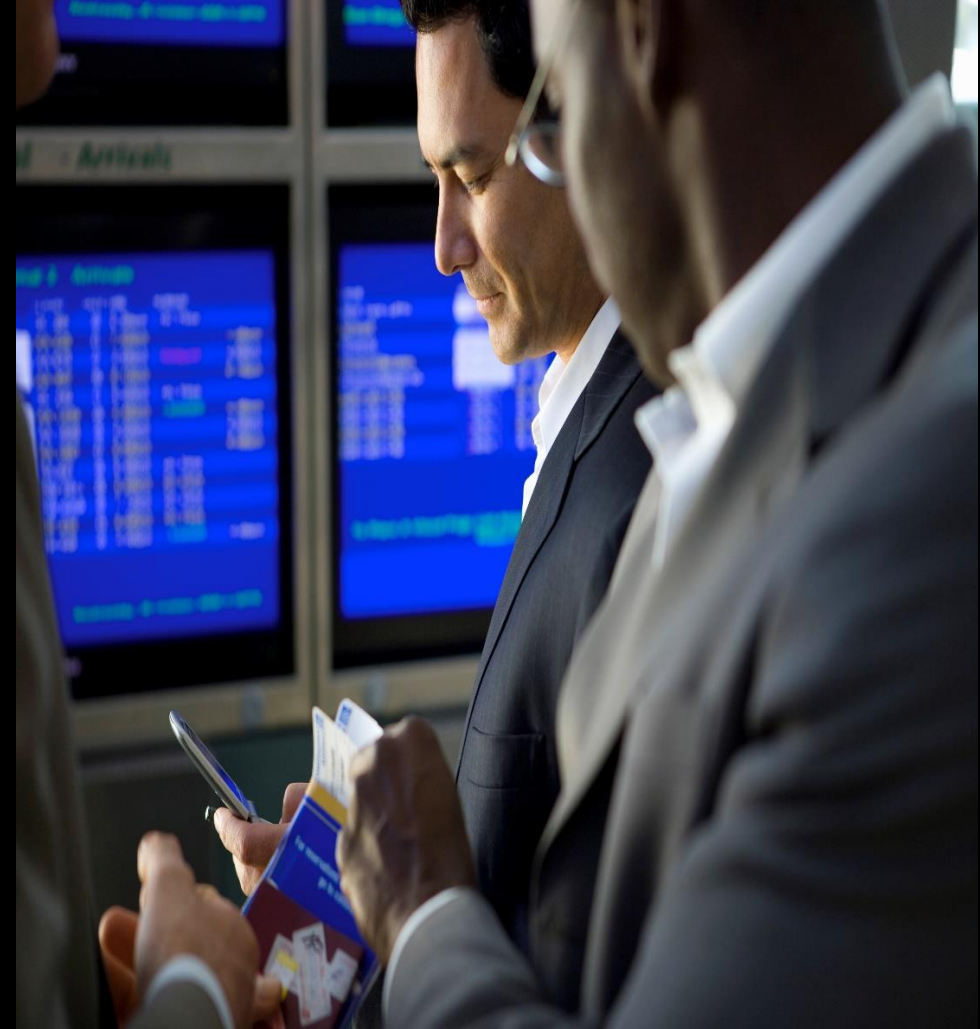
- Help to identify, understand and remediate **critical vulnerabilities**.
- Strong security ensures having **powerful technology**.
- Ensures that your applications are **managed securely**.
- No hardware, software or infrastructure required.

# Security Code Scan Assessment

## Introduction

### What are we doing?

- Help partners/ISV's to identify security threats, vulnerabilities in their products.
- Depending the underlying technology, partner can have either
  - One Year Subscription access to the online Security Code Scan tool for non ABAP or
  - One Year Subscription license of SAP Code Vulnerability Analyzer (CVA) license for ABAP
- Static Code Scan of partners application for unlimited number of times in an year.
- **Why are we doing?** Based on a survey, 250+ out of almost 400 existing SAP partners do not perform Security Code Scan assessment on their own.
- Almost 100 partners have ABAP add-ons while others are on other platforms.
- To ensure that partners products are secure



# Security Code Scan Assessment

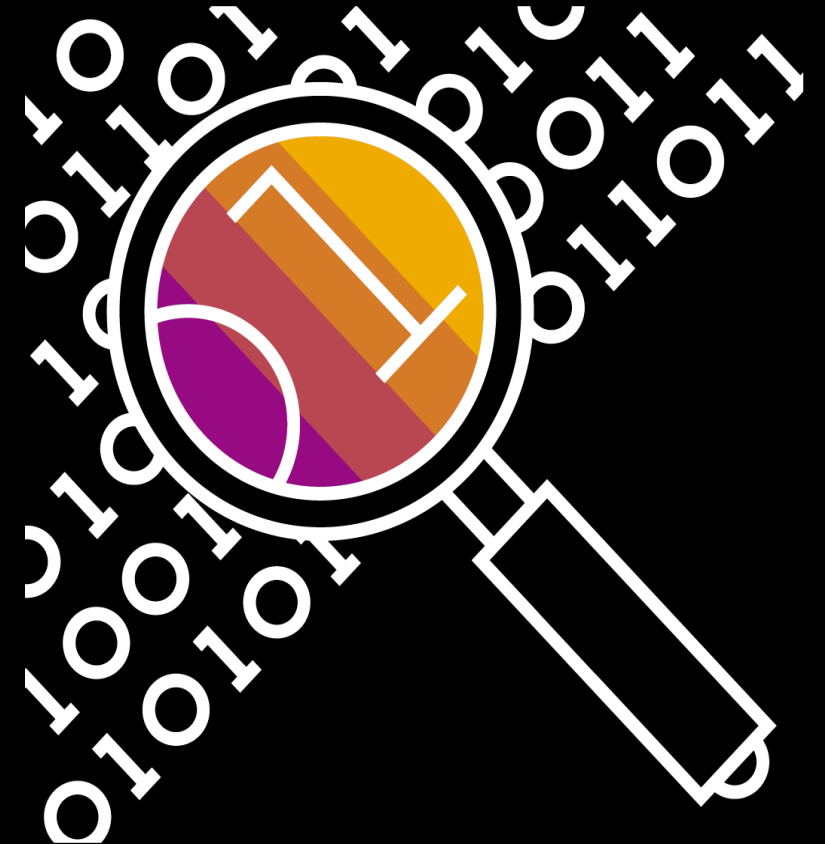
## Static Security Code scan – non ABAP

### What is Static Security Code scan?

- Performed without actually executing the programs.
- Technique used to scrutinize all code paths and data flows.
- They push the testing as early into the process as possible and as close to the component being built as possible.
- Can assess the security of microservices, web, mobile and desktop applications.

### Why Static Security Code scan?

- It identifies detects in the program at early stages and decrease in cost to fix.
- It can detect flaws in the program's inputs and outputs that cannot be seen through dynamic testing.
- It automatically scans uncompiled codes and identifies vulnerabilities.



# Security Code Scan Assessment

## SAP ABAP Security Code Scan

### What is SAP ABAP Security Code Scan

- SAP ABAP Security Code Scan is a service which use SAP CVA carries out a static analysis of ABAP source code and reports possible security risks.
- SAP CVA is a product in its own right and is subject to separate remuneration

### Why use SAP CVA in ABAP Security Code Scan

#### Scan efficiently

- Reduced false-positive rate by dataflow analysis
- Scanning directly from within the ABAP development environment with broad range of predefined checks

#### Developer guidance

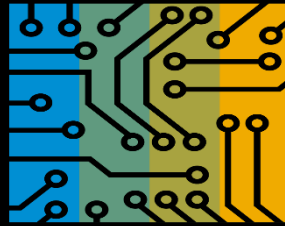
- Detailed help and explanations to all errors and assistance to find the right location for the fix
- Prioritization of checks

Integrated into standard ABAP check frameworks, SAP transport system and ABAP Test Cockpit (ATC)

# Security Code Scan Assessment Benefits



Unlimited High-quality  
scanning results for the apps



Comply with SAP  
Corporate Security guidelines



Reduces application code  
vulnerabilities early in the  
lifecycle



Gain Insight into the  
Security of your Software.



Integrate application  
security into your SDLC



Deep and Lasting  
Relationships with Customers

# Security Code Scan Assessment

## Platforms Covered & Flaw Checks

### SAP Cloud Platform



(Excludes HANA XS engine)

### On-Premise Applications



**C/C++, Legacy Business Application** (COBOL, Visual Basics), **Java**(Java SE, Java EE, JSP), **.Net** (C#, ASP.NET, VB.NET)

### Web Platforms



**JavaScript** (including AngularJS, Node.js, and jQuery), **Typescript**, **Python**, **Perl**, **PHP**, **Ruby on Rails**, **ColdFusion**, and **Classic ASP**.

### Mobile Platform



**iOS** (Objective-C and Swift), **Android** (Java), **Phone Gap**, **Cordova**, **Titanium**, **Xamarin**.

### SAP NetWeaver Platform



SAP ERP 6.0

### SAP S/4 HANA Platform



SAP S/4HANA 1809 or above

### Top Security Flaw checks:

Cross-site scripting(XSS) attack check, buffer overflow check, SQL injection attack check, Directory traversal attack check, Confidentiality, Integrity

### Other critical checks like:

Application business criticality check, CRLF Injection, Credential management, Information leakage, Code quality, error handling. Availability Impact Check and Understand Severity, Exploitability and Remediation effort.

### ABAP related checks:

Security Analyses in Extended Program Check ( SLIN), Dynamic and Client-Specific Accesses in SELECT, Invalid access to CDS Views etc.

# Security Code Scan Assessment

## Technical support for the static scan – ABAP & non ABAP

Language and Platform	Versions
Java (Java SE, Java EE)	JDK 1.4, 1.5, 1.6, 1.7, 1.8
C# (Windows/.NET 1.1, 2.0, 3.0, 3.5, 4.0, 4.5, 4.6, 4.7/ Core 1.0, 1.1, 2.0)	Visual Studio .NET 2003, 2005, 2008, 2010, 2012, 2013, 2015, 2017/ Mono 4.x
ASP.NET with C# or VB.NET (Windows/.NET 1.x, 2.0, 3.x, 4.x / Core 1.1, 2.0 for C# only)	Visual Studio .NET 2003, 2005, 2008, 2010, 2012, 2013, 2015, 2017
VB.NET (Windows/.NET 1.1, 2.0, 3.0, 3.5, 4.0, 4.5, 4.6, 4.7)	Visual Studio .NET 2003, 2005, 2008, 2010, 2012, 2013, 2015, 2017
C/C++ (Windows/.NET 2.0, 3.0, 3.5, 4.0, 4.5, 4.6)	Visual Studio .NET 2005, 2008, 2010, 2012, 2013, 2015/ Mono 4.x
JavaScript and TypeScript	
PHP	5.2-7
Scala	2.13 and earlier
Ruby on Rails	Ruby 1.9.3, 2.0.x, 2.1.x, 2.3 / Rails 3.x, 4.x
Classic ASP	Classic ASP 1.x, 2.x, 3.0
ColdFusion (compiled as Java)	ColdFusion 7, 8, 9, 10, 11
Perl	5.x (CGI Applications)
Python	2.x, 3.x
Android	Android SDK
iOS	Xcode 4.x-9.x (LLVM)
Xamarin	Visual Studio 2012 and later/ Xamarin Studio/ Mono 4.x
PhoneGap/Cordova	PhoneGap or Cordova
Titanium	Titanium SDK
C/C++ (Solaris 8, 9, 10 on SPARC)	gcc 3.3, 3.4, 4.0, 4.1
C/C++ (Red Hat Enterprise Linux 3, 4, 5, 6, CentOS 3, 4, 5, 6, Fedora Core 6, OpenSUSE Linux 10, 11)	3.2-3.4, 4.0-4.9
C/C++ (Windows)	Visual Studio .NET 2002-2015 (Visual C++ 7.0-14.0)
COBOL	Enterprise COBOL for z/OS, MicroFocus, ILE COBOL, and COBOL-85
RPG	RPG III, RPG IV, RPGLE
Visual Basic 6	Visual Basic 6
ABAP Language SAP NetWeaver Platform	SAP S/4HANA 1809, SAP ERP 6.0 EHP7 and more



# Security Code Scan Assessment

## Priorities categorized after the scan - non ABAP

<b>Very High</b>	The offending line or lines of code is a very serious weakness and is an easy target for an attacker. The code should be modified immediately to avoid potential attacks.
<b>High</b>	The offending line or lines of code have significant weakness, and the code should be modified immediately to avoid potential attacks
<b>Medium</b>	A weakness of average severity. These should be fixed in high assurance software. A fix for this weakness should be considered after fixing the very high and high for medium assurance software
<b>Low</b>	This is a low priority weakness that will have a small impact on the security of the software. Fixing should be consideration for high assurance software. Medium and low assurance software can ignore these flaws.
<b>Very Low</b>	Minor problems that some high assurance software may want to be aware of. These flaws can be safely ignored in medium and low assurance software.
<b>Informational</b>	Issues that have no impact on the security quality of the application but which may be of interest to the reviewer.

*To successfully complete the assessment all the Very high and high priority issues have to be resolved/mitigated by partners comments.*

# Security Code Scan Assessment

## CVA for SAP NetWeaver & SAP S/4 HANA on Premise - ABAP

### SAP NetWeaver releases 7.50 SP3

Security Analyses in Extended Program Check (SLIN)  
Critical Statements  
Find Specific Critical Statements  
Dynamic and Client-Specific Accesses in SELECT  
Dynamic and Client-Specific Assesses with INSERT, UPDATE, MODIFY, DELET  
Use of ADBC Interface  
Client-Specific Shared Objects methods

### SAP S/4HANA on Premise 1809 or above

DDIC: DB Tables( Logging Check)  
Security Checks for ABAP (CVA)  
Security Checks for BSP (CVA)  
Critical Statements  
Find Specific Critical Statements  
Dynamic and Client-Specific Accesses in SELECT  
Dynamic and Client-Specific Assesses with INSERT, UPDATE, MODIFY, DELET  
Use of ADBC Interface  
Client-Specific Shared Objects methods  
Invalid access to CDS Views

*For detailed security check scope, please contact SAP ICC consultant*

# Security Code Scan Assessment

## CVA priorities categorized after the scan - ABAP

Priority 1	The offending line or lines of code is a very serious weakness and is an easy target for an attacker. The code should be modified immediately to avoid potential attacks.
Priority 2	The offending line or lines of code have significant weakness, and the code should be modified immediately to avoid potential attacks
Priority 3	This is a low priority weakness that will have a small impact on the security of the software. Fixing should be consideration for high assurance software. Medium and low assurance software can ignore these flaws.

*To successfully complete the assessment all the Priority 1 and Priority 2 issues have to be resolved/mitigated by partners comments.*

# Security Code Scan Assessment

## ICC Marketing Benefits

### **SAP Security Code Scan Assessment Overview**

A letter provided from SAP Integration and Certification Center (SAP ICC) after successfully completing the assessment. Partners can only share the SAP Security Code Scan Assessment overview on their websites.

---

### **SAP Security Code Scan Assessment Report**

The information regarding the 3rd party review results and SAP Security Code Scan Assessment report should remain confidential.

---

### **Promoting the Assessment**

Our solution XYZ version # has been successfully\* completed the Security Code Scan Assessment by SAP on DATE.". Here successfully means all the very high and high priority issues are resolved or mitigated by partners comments.

---

### **Listing in SAP Certified Solutions Directory (CSD)**

The [certification listing](#) is enhanced with additional details regarding successful security code scan assessment. Once the certification expires the listing will be removed regardless of the security code scan assessment.

---

# Security Code Scan Assessment: Pricing

Applications on Any Platform	Amount in Euros	Benefits
	Standalone	Partners can avail unlimited scans for a particular product/solution within one year
	5,000 Euros per year subscription	

# Security Code Scan Assessment

## Related Links

### SAP ICC Application Form

Please fill in [SAP ICC online application form](#) with information about your company and about the software application that you want to integrate in order to apply for an integration certification.

### Know More About Certification & Security Code Scan Assessment – non ABAP

- To learn more about certification please visit [Software Certification](#) page.
- <https://blogs.sap.com/2017/11/02/security-code-scan-assessment-for-non-abap-software/>
- [https://en.wikipedia.org/wiki/Static\\_program\\_analysis](https://en.wikipedia.org/wiki/Static_program_analysis)
- [https://en.wikipedia.org/wiki/List\\_of\\_tools\\_for\\_static\\_code\\_analysis](https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis)

### Know More About Certification & Security Code Scan Assessment – ABAP

- <https://blogs.sap.com/2017/01/19/code-vulnerability-analyzer-checks/>
- <https://www.sap.com/documents/2018/11/ec5d12c6-287d-0010-87a3-c30de2ffd8ff.html>
- <https://wiki.scn.sap.com/wiki/display/ABAP/SAP+NetWeaver+Application+Server,+add-on+for+code+vulnerability+analysis>

To know more about Security Code Scan Assessment please contact [icc@sap.com](mailto:icc@sap.com)

# Thank you.

Follow us



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/copyright](http://www.sap.com/copyright) for additional trademark information and notices.