

Über **CODEPROFILER**

CodeProfiler ist das weltweit erste Produkt, das automatisierte Tests für ABAP und BSP Anwendungen durchführt. Seine Datenbank enthält Muster von vielen bekannten unsicheren Programmierpraktiken im Zusammenhang mit ABAP Entwicklungen.









Anwendungsfälle

CodeProfiler ist die beste Wahl um ein Mindestlevel an Sicherheit für alle ABAP basierten Geschäftsanwendungen zu erreichen. Typische Anwendungsfälle sind:

- Ihre Firma möchte prüfen ob immer Berechtigungsprüfungen stattfinden, wenn kritische Geschäftstransaktionen ausgeführt werden.
- Sie möchten sicherstellen, dass Ihr Softwarelieferant keine Hintertüren im Code eingebaut hat.
- Ihre Firma möchte testen ob es Sicherheitsschwächen im eigenen ABAP Code gibt, welche Business Assets gefährden oder Compliance Anforderungen verletzen.

Testgruppen (Auszug)

Die Testgruppen enthalten verschiedene Testmuster für typische Sicherheitslücken im ABAP Code.

- **Fehlende Berechtigungsprüfungen** 
ABAP Code kann jede Geschäftstransaktion ohne Privilegien ausführen. Daher muss immer eine *programmatische* Berechtigungsprüfung erfolgen, bevor ABAP Code wichtige Prozesse ausführt. Anderenfalls könnten Benutzer Zugriff auf kritische Prozesse erhalten.
- **Gefährliche ABAP Befehle**
Diese Muster prüfen, ob ABAP Befehle verwendet werden, die ein Sicherheitsrisiko darstellen. Beispiele sind der Zugriffe auf Server-Dateien und systemnahe Befehle.
- **Hintertüren** 
Es gibt verschiedene Möglichkeiten Hintertüren im ABAP Code einzubauen. Sie gewähren böswilligen Entwicklern verdeckten Zugang zu Sonderfunktionen durch geheime Aktionen.
- **Hartcodierte Benutzer-Legitimationen** 
Diese Testmuster prüfen ob hartcodierte Benutzer-Legitimationen im Code vorhanden sind.
- **Generischer Code** 
Entwickler schreiben manchmal Code, der für eine Vielzahl von Anwendungsfällen benutzt werden kann. Diese Flexibilität kann zu Schwachstellen führen. Böswillige Benutzer könnten unerwartete Anwendungsmöglichkeiten entdecken, die niemand beabsichtigt hatte.
- **Ausführung von Befehlen** 
In manchen Fällen kann ABAP Code zur Laufzeit generiert und ausgeführt werden. Wir prüfen, ob solche gefährlichen Praktiken verwendet werden und ob sie angreifbar sind.
- **SQL Injection** 
Diese Schwachstelle erlaubt böswilligen Benutzern OSQL Befehle zu manipulieren. Dies ermöglicht unberechtigten Lese/Schreib-Zugriff auf Informationen in der SAP Datenbank.
- **Cross Site Scripting (XSS)** 
XSS ist ein Hauptrisiko in jeder Webapplikation und kann u. a. zu Identitätsdiebstahl führen. Die Testmuster prüfen ob BSP Applikationen durch XSS angreifbar sind.
- **Forceful Browsing** 
Böswillige Benutzer können bei Webanwendungen UI-Beschränkungen, wie z. B. deaktivierte Buttons, durch Forceful Browsing umgehen. Die Testmuster prüfen ob solche Angriffe in BSP Anwendungen möglich sind.



Dieses Symbol zeigt Schwachstellen an, die in manchen Fällen gegen Compliance verstoßen.