

### Konventionelle Scanner erzeugen zu viele Falsch Positive

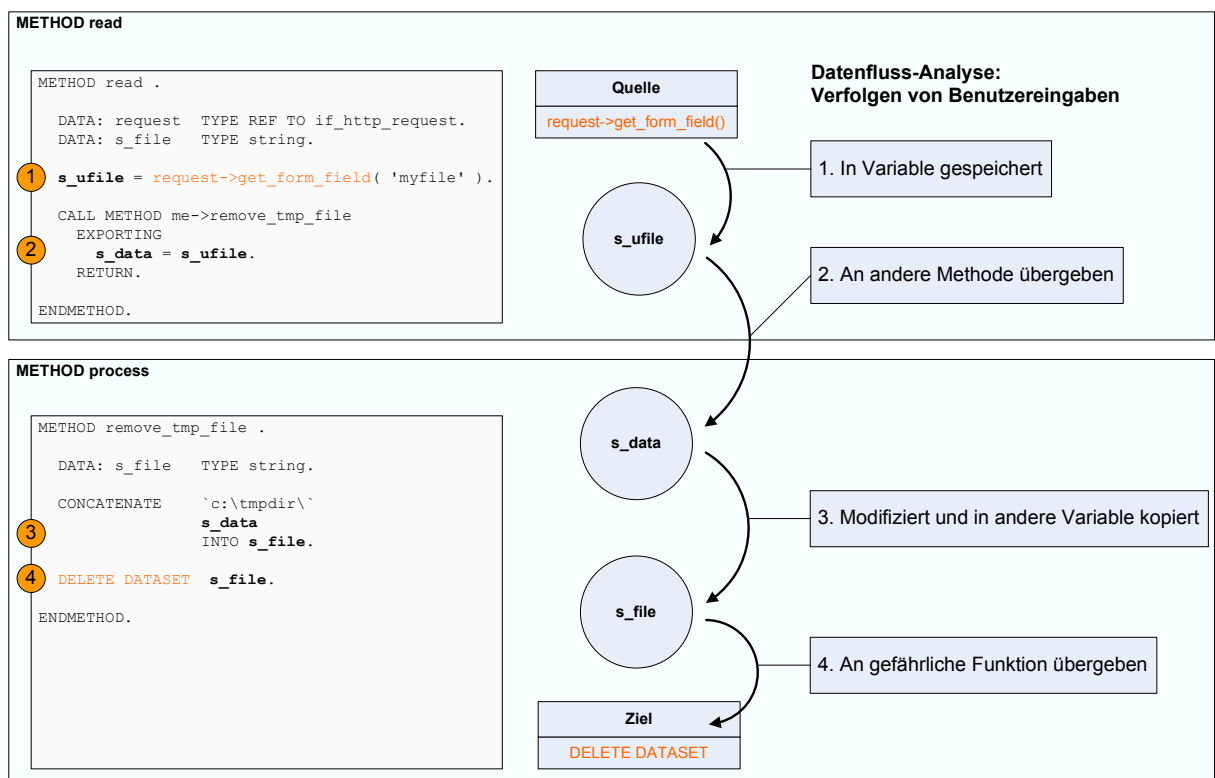
Konventionelle Codescanner identifizieren verdächtigen Code durch „Pattern Matching“. So können sie jedes Vorkommen einer vorgegebenen ABAP Anweisung finden, wie z.B. DELETE DATASET.

Sicherheitsrelevant ist aber, ob eine potentiell gefährliche Anweisung auch ausnutzbar ist: Können Angreifer eine gefährliche Anweisung tatsächlich erreichen und für ihre Zwecke missbrauchen?

Um bei dem Beispiel zu bleiben: Das Löschen einer Datei auf dem Server ist an sich nicht gefährlich. Es wird jedoch gefährlich, wenn ein unberechtigter Benutzer bestimmt, welche Datei gelöscht wird. Es ist aber sehr aufwendig durch „Pattern Matching“ alle Stellen zu finden, wo Benutzereingaben eine DELETE DATASET Anweisung erreichen. Denn dazu muss man manuell den gesamten zugehörigen ABAP Code analysieren. Dieser Ansatz ist weit entfernt von statischer Codeanalyse.

### Die Lösung heißt Datenfluss-Analyse

Datenfluss-Analyse ist eine Technik, die Quellen und potentiellen Ziele von Eingaben findet. Dann wird geprüft, ob es Verbindungen zwischen diesen Quellen und Zielen gibt. Jede identifizierte Verbindung zeigt einen Datenfluss und damit einen mit hoher Wahrscheinlichkeit ausnutzbaren Angriffspunkt an.



**CODEPROFILER** setzt die Datenfluss-Analyse in Verbindung mit einem umfangreichen Regelwerk ein, das dutzende von Datenquellen und gefährlichen Datenzielen beinhaltet.

### Fazit

- Nur Datenfluss-Analyse liefert aussagekräftige, verlässliche Testergebnisse im Bereich Sicherheit.
- Ohne Datenfluss-Analyse ist erheblicher manueller Aufwand nötig, um Testergebnisse zu validieren.