WSA Webservice Securtiy Analyzer

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Gerhard Hassenstein
Experte: Dr. Igor Metz (Glue Software Engineering AG)

«WSA – Webservice Security Analyzer» ist eine API zur Prüfung von SOAP Nachrichten. Sie ermöglicht es, dem Übermittler einer Nachricht detaillierte Informationen über alle sicherheitsrelevanten Anforderungen zurückzugeben. Dies beinhaltet unter anderem, ob die Signatur oder die Verschlüsselung mit aktuellen und gültigen Algorithmen durchgeführt wurde.
Da es sich bei diesem Projekt um eine API handelt wird der Payload nicht gespeichert.

Ausgangslage

Die itServe AG hat sich auf das Übermitteln von Swissdec Lohnmeldungen (www.swissdec.ch) spezialisiert. Da für ihre Kunden die Übermittlung im Bereich SOAP Security oft eine grosse Herausforderung ist und bisher keine Tools zur Unterstützung auf dem Markt erhältlich sind, soll dieses Projekt zu einer Verbesserung der Situation für den Kunden führen. Zusätzlich erhofft sich die Firma, dieses Projekt auch für interne Testzwecke und weitere Projekte verwenden zu können.

Ziel

Das Ziel dieses Projektes ist es, den Kunden zu unterstützen, indem bei SOAP Nachrichten, welche Fehler aufweisen, detaillierte Informationen auszugeben. Damit soll die Fehlerkorrektur vereinfacht werden. Das Ganze soll durch «WSA – Webservice Security Analyzer» funktionieren. Es soll die Möglichkeit bestehen, diese API in die Testsysteme der itServe AG zu integrieren.

Umsetzung

In einer ersten Phase wurde der gesamte OASIS Standard für die Security ausgearbeitet. Anschliessend wurde entschieden, welche Testfälle für die itServe AG relevant sind.
In einem weiteren Schritt wurde der Ablauf der Checks ausgearbeitet. Dies ist notwendig, da es Abhängigkeiten bei den Checks, in unserem Fall Interceptoren, gibt.
Als Beispiel kann man dies anhand einer Prüfung der Signatur zeigen. Bevor der Payload berechnet werden kann, müssen vorgängig die ID Referenzen geprüft werden. Anschliessend ging es an die Implementation eines Prototyps, welcher genau diese Testfälle abarbeiten kann.
Zu diesem Zweck wurde definiert, welches die beste Architektur für dieses System ist. Nach der Analyse diverser Möglichkeiten, wurde die Observer Pattern Architektur gewählt. Dies zum einen, weil die API einfach erweitert werden und für weitere itServe Projekte wiederverwendet werden kann. Zum anderen, damit möglichst bald mit dem Prototyp angefangen werden konnte. Mithilfe dieser Architektur können Interceptoren in einer bestimmten Reihenfolge hinzugefügt und entfernt werden.
Jeder der Checks ist ein Interceptor, welcher in einer bestimmten Reihenfolge abgearbeitet werden muss. Zu jedem Interceptor wurden Testfälle erarbeitet.
Zum Schluss folgte die Umsetzung des Prototyps. Diese war zeitaufwändiger als erwartet.

Zukunft

Die itServe AG ist an einer Weiterführung des Projektes interessiert. In einem produktiven Test sollen erste Erfahrungen gesammelt werden, um die Anwendung auszubauen und weiterzuentwickeln.

Urs Michael Küttel