

Web Application Scanning (WAS)



Cyber Security
Services

Web Application Scanning (WAS) ist auch als die Suche nach Schwachstellen in Webanwendungen bekannt und ist ein automatisches Suchprogramm, das nach Schwachstellen in Webanwendungen sucht. Die Software analysiert und entwickelt zunächst ein Software-Konstrukt der gesamten Website. Hierdurch gewinnt der Scanner einen Einblick in die Anwendung und sucht anschließend automatisch nach allgemeinen Sicherheitsschwachstellen, indem er eine Reihe von Webangriffen startet. Die Berater können diese Sicherheitsschwachstellen anschließend manuell überprüfen.

Die Ziele des Web Application Scanning (WAS) Services sind:

- **Identifizieren** von Sicherheitsschwachstellen und -problemen auf der Website des Kunden mithilfe eines Schwachstellen-Scanners.
- Von dem Schwachstellen-Scanner identifizierte Probleme werden **manuell untersucht und gemeldet**.

Diese Art der Analyse umfasst die folgenden Schritte:

- **Scannen und Crawling:** Sammeln von Informationen über die laufende Webanwendung auch über Netzwerkschnittstellen, Webserver-Version, installierte Module, Versionsnummern sowie Durchblättern aller Ordner und Dateien der Website.
- **Schwachstellen identifizieren:** Aufbauend auf den Informationen der vorangehenden Phase überprüft der Berater bestehende Web-Schwachstellen oder Fehlkonfigurationen der Sicherheit manuell, indem speziell entwickelte Anfragen an die Webanwendung geschickt werden, um Schwachstellen und Sicherheitslücken zu erkennen.
- **Ergebnisanalyse:** Prüfen der Antworten der Anwendung auf die Web-Anfragen der vorangehenden Phase und manuelle Überprüfung der erkannten Web-Schwachstellen und Eliminieren der Fehlalarme.
- **Bericht:** Melden der erkannten Web-Schwachstellen einschließlich der Wirkungsbewertung und vorgeschlagener Abhilfemaßnahmen. Ingram Micro nutzt von der Industrie empfohlene Schwachstellenbewertungstools, um Schwachstellen in Webanwendungen zu identifizieren. Der Berater würde anschließend die Ergebnisse manuell überprüfen und einen Bericht mit den relevanten Erkenntnissen erstellen.

Nach Abschluss der Bewertung erhält der Kunde einen ausführlichen Bericht, der Folgendes enthält:

- **Zusammenfassung:** Eine Zusammenfassung des Zwecks dieser Analyse sowie eine kurze Erläuterung der geschäftlichen Bedrohungen, denen das Unternehmen ausgesetzt ist.
- **Erkenntnisse:** Eine ausführliche technische Erläuterung der Erkenntnisse der Analyse zusammen mit Schritten und Nachweisen der Erkenntnisse.
- **Schlussfolgerung und Empfehlungen:** Dieser Abschnitt enthält abschließende Empfehlungen und eine Zusammenfassung der während der Sicherheitsbewertung festgestellten Probleme.

Web Application Scanning (WAS)



Cyber Security
Services

Möchten Sie mehr über unsere Cyber Security Assessment Services erfahren?

Dann wenden Sie sich bitte an:

Michael Schumak
Technical Sales Consultant
michael.schumak@ingrammicro.com

Markus Sawinski
Sales Consultant
markus.sawinski@ingrammicro.com

Steffen Voigt
Business Development Manager
steffen.voigt@ingrammicro.com

Christian Voss-Freund
Presales Engineer
christian.voss-freund@ingrammicro.com
Tel: +49.89.4208.2760

| Artikelnummer | Beschreibung | Preis |
|---------------|--|-------------|
| 4V60022 | Web Application Scanning 1 -10Assets / IP Adresses | auf Anfrage |
| 4V60023 | Web Application Scanning 11-30Assets / IP Adresses | auf Anfrage |
| 4V60024 | Web Application Scanning 31-100Assets / IP Adresses | auf Anfrage |
| 4V60025 | Web Application Scanning 100-300Assets / IP Adresses | auf Anfrage |
| 4V60026 | Web Application Scanning 300 +Assets / IP Adresses | auf Anfrage |