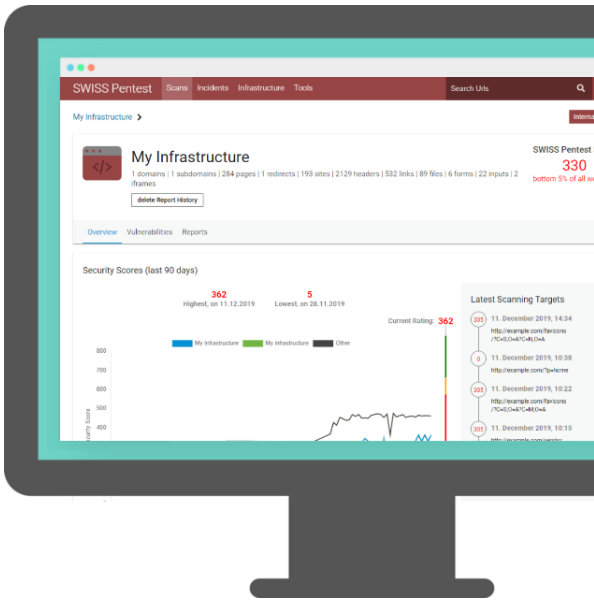
KASTGROUP

swisspentest

Umfassende Websecurity durch künstliche Intelligenz – Finanzdienstleister Standard

Die swisspentest Plattform bietet mit mehreren hundert vollautomatisierten Sicherheitstests eine umfassende Schwachstellenerkennung für Web Applikationen. Durch das kontinuierliche Simulieren von Angriffen auf ein Ziel können Fehlkonfigurationen, verwundbare Bibliotheken und inkorrekte Infrastrukturhärtungsprotokolle schnell und unkompliziert gefunden werden.

Die Plattform ist als isolierter Container (SaaS) oder in der lokalen Virtuellen Maschine (On-Premis) verfügbar. Diese erreicht durch das effiziente Klonen eines Ziels und durch ein Deep Learning Modul zur Verminderung von false-positives die bestmögliche Präzision.



Key Features

Internationale Standards

Um eine genaue Schwachstellenanalyse bieten zu können, wurden die Sicherheitsscans compliant mit dem OWASP Testing Guide entwickelt und die Reports nach den Mitre A&ttack, CWE und CVSS Standards generiert.

Abwehr

Der swisspentest kann Angriffe auf die Benutzer Ihrer Webseite automatisch detektieren und umgehend Abwehrprozesse zum Schutz deren Accounts einleiten.

Portal

Über das zentrale User Interface der swisspentest Plattform können Angriffsziele, Scanning-Optionen oder Abwehrprozesse administriert werden. Zusätzlich werden alle gefundenen Sicherheitslücken mit ausführlichen Beschreibungen und präzisen technischen Details angezeigt.

Die umfangreiche Toolbox des Portals erweitert dessen Funktionen auf die Gebiete der Web-Usability und bietet weitere nützliche Web-Insights.

Use Cases

Aktuelles Sicherheitslevel auf einen Blick

Die übersichtliche Präsentation der Testergebnisse in Diagrammen und Statistiken ermöglicht eine optimale Einschätzung des aktuellen Sicherheitslevels einer Infrastruktur.

Alle nicht intrusiven Sicherheitsscans werden an einem Klon ausgeführt, welcher regelmässig durch das effiziente Crawlen des Ziels neu generiert wird. Dies reduziert die Anzahl von HTTP-Anfragen, welche an ein Ziel gesendet werden und verhindert somit eine Überlastung der Ziel-Webseite.

Webseitenentwicklung

- ✓ **Entwicklungsphase**
  Mithilfe der generierten Patch Codes, können Sicherheitslücken schnell geschlossen werden.
- ✓ **Testphase**
  Während des Testings können intrusive Scans aktiviert werden, welche auf das aggressive Eindringen trainiert wurden.
- ✓ **Produktive Phase**
  Um eine gute Usability zu sichern, können während der Produktionsphase die Pentests auch ohne Intrusive Scans ausgeführt werden.

Security Platform: Internal Structure

Deep Learning Modul

Um false-positives zu vermeiden, wird ein Deep Learning Modul mittels TensorFlow eingesetzt. Dieses besteht aus einem modifizierten LSTM Netzwerk, welches mithilfe von ausgewerteten Quellcodes der Alexa Top 1000 und einer eigens entwickelten “Loss Function” trainiert wurde. Die Genauigkeit wird durch die Verwendung des t-SNE Algorithmus für die Feature-Selection weiter gesteigert.

TensorFlow

Abwehrprozesse

Durch die Integration von Reporting-HTTP Headers in eine Webseite werden Berichte von Browser-detektierten Angriffen der Webseitenbenutzer an den swisspentest gesendet.
Diese werden automatisch analysiert und triggern gegebenenfalls vordefinierte API Calls, welche die Sitzung des betroffenen Benutzers beenden und sperren können.

Threat Intelligence

Die Threat Intelligence Engine überprüft das Deep Web nach Risiken wie Phishing Angriffe, welche für die eigene Organisation gefährlich sind.
Wird eine Bedrohung gefunden, erfolgt eine Alarm Meldung, welche manuell analysiert und anschliessend eskaliert oder geschlossen werden kann.