

XignSys GmbH

Whitebox Penetrationstests eines Authentifizierungsdienstes als Mobile- und Web-Awendung

Die Xignsys GmbH hat ihr passwortloses SingleSignOn (SSO) Authentifizierungsverfahren für Mobile- und Webanwendungen auf Schwachstellen untersuchen lassen.

Das Ziel der Xignsys GmbH ist es, die digitale Souveränität von Endverbraucher zu erhöhen. Als Lösung dafür wurde ein passwortloses SSO Loginverfahren entwickelt, welches das Smartphone zum Anmelden bei Diensten und Webseiten verwendet. Dieses Verfahren kommt bei zahlreichen Digitalisierungsprojekten in ganz Deutschland erfolgreich zum Einsatz. Gerade bei einem so weit verbreiteten Authentifizierungssystem steht die Sicherheit an erster Stelle. Aus diesem Grund wurde ein umfangreicher Penetrationstest durchgeführt.

ZIELE

Das Ziel des Penetrationstests war es sicherzustellen, dass keine Sicherheitslücken oder Schwachstellen in dem Xign.me Authentifizierungsverfahren es einem Angreifer ermöglichen, andere Benutzer zu impersonieren oder auf andere Daten zuzugreifen.

HERAUSFORDERUNGEN

Bei der Durchführung so umfangreicher Whitebox Penetrationstests muss sichergestellt sein, dass die Entwickler:innen und die Tester:innen Hand in Hand arbeiten, um diese großen Mengen an Programmcode effektiv und ausführlich zu analysieren. Das Pentestteam der AWARE7 GmbH musste während der Untersuchung auf Schwachstellen die unterschiedlichsten Frontend-, Backend-Techniken sowie Programmiersprachen analysieren.

UMSETZUNG

Der Penetrationstests beginnt mit der Gewinnung von Informationen. Der Aufwand ist aufgrund der

Menge der genutzten Technologien und Zeilen Programmcode erhöht. Daher wurde gerade auf die Sammlung von Informationen und Identifikation von vulnerablen Funktionen und Programmcode-Zeilen der Großteil des verfügbaren Projektbudgets investiert. Die Ausnutzung der im vorherigen Schritt identifizierten Schwachstellen erfolgte durch den bereitgestellten Programmcode und die Beispielanwendung im Medizin-Bereich. So war es einfach möglich den Einfluss einer Schwachstelle auf die Informationssicherheit der Daten zu evaluieren. Da es sich bei der getesteten Anwendung um eine Test-Anwendung handelte, welche nicht im produktiven Betrieb genutzt wurde, war eine ausführliche Post-Exploitation Phase, bei der die reibungslose Funktion des Systems sichergestellt wird, nicht notwendig.

ERGEBNIS & ERFOLG

Im Projektzeitraum konnten einige vulnerable Funktionen und Programmzeilen identifiziert und innerhalb von kürzester Zeit behoben werden. Durch die enge Zusammenarbeit konnte das Sicherheitsniveau der entwickelten Software deutlich erhöht werden.

ÜBER DIE AWARE7 GMBH

Die AWARE7 GmbH ist ein ISO 27001 zertifiziertes Cyber Security Unternehmen aus Gelsenkirchen, das Technologien und Produkte entwickelt. Zudem werden Dienstleistungen zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels angeboten.

Die praktische Arbeit und die regelmäßige Veröffentlichung wissenschaftlicher Artikel macht es dem Unternehmen möglich, über

komplexe Betrugs- und Angriffsmethoden aufzuklären. So können Unternehmen, Behörden und Personen geschützt werden.

Die Durchführung umfangreicher Cyber Security Awareness Kampagnen, Penetrationstests und die Unterstützung beim Aufbau von Informationssicherheitsmanagementsystemen werden von dem auf IT-Sicherheit spezialisierten Unternehmen angeboten.



Ihr Ansprechpartner



Chris Wojtechowski
Geschäftsführender Gesellschafter

Cyber Security Awareness,
Live Hacking Shows &
Awareness Events

chris@aware7.de
Mobil: 0170 411 3255

AWARE7 GmbH
Munscheidstr. 14
45886 Gelsenkirchen

info@aware7.de
<https://aware7.de>