Zertifikat

Die

plan42 GmbH

bestätigt hiermit, dass die

Deutscher Landwirtschaftsverlag Gmbh

über ein sicheres Web-Portal für die Seite www.landlive.de verfügt.

Ein externer Penetrationstest wurde durchgeführt, dessen Ergebnisse im Bericht „Sicherheitsuntersuchung der Web-Anwendungen Landlive & Technikbörse", Version 1.4, dokumentiert sind.

Die wichtigsten Empfehlungen der

OWASP Top 10 2013

sind nachweislich erfüllt.

München, den 04.07.2014

M. Heinzmann

Marc Heinzmann (Auditor)

+49 89 307657-16 info@plan42.com www.plan42.com

Untersuchungsgegenstand

Untersuchungsgegenstand war die aus dem Internet erreichbare technische IT-Infrastruktur zur Unterstützung des Fundraising-Prozesses bestehend aus dem Spendenserver, dem Monitoring-Server und dem VEWA-Server. Die Penetrationstester erhielten Kennungen für die zu testende Anwendung.

Prüfung nach OWASP Top 10

Der Untersuchungsgegenstand wurde auf alle Schwachstellen geprüft, die das Open Web Application Security Project (OWASP) in seine „OWASP Top 10“ aufgenommen hat. Hierbei handelt es sich um die 10 kritischsten Bedrohungen, denen Webanwendungen ausgesetzt sind. Zur Feststellung auf vorhandene Schwachstellen wurden die Prüfungen gemäß Application Security Verification Standard 2013 (ASVS) durchgeführt.

A1 – Injection (manipulierte Anfragen)

Diese Schwachstelle tritt auf, wenn Anwendungen manipulierte Anfragen verarbeiten und so schädliche Befehle ausführen oder unautorisierten Zugriff gewähren.

Durchgeführte Prüfungen: ASVS V4

A2 – Fehler in Authentifizierung und Session Management

Diese Schwachstelle tritt auf, wenn Funktionen für Authentifizierung und Session Management nicht korrekt implementiert sind. Angreifer können dann z. B. Passwörter ausspähen oder auf andere Weise die Identität anderer Benutzer anzunehmen.

Durchgeführte Prüfungen: ASVS V1 & V2

A3 – Cross-Site Scripting (XSS)

Diese Schwachstelle tritt auf, wenn die Anwendung nicht vertrauenswürdige Daten ungeprüft bzw. unmaskiert im Browser ausgibt und so die Ausführung von Schadcode oder die Weiterleitung auf manipulierte Websites ermöglicht.

Durchgeführte Prüfungen: ASVS V4

A4 – Unsichere direkte Objektreferenzen

Diese Schwachstelle tritt auf, wenn Referenzen zu sensiblen, anwendungsinternen Objekten, wie z. B. Dateien oder Datenbankschlüssel, von außen zugänglich sind. Angreifer können dann unautorisierten Zugriff auf die Daten erlangen.

Durchgeführte Prüfungen: ASVS V3

A5 – Sicherheitsrelevante Fehlkonfiguration

Diese Schwachstelle tritt auf, wenn die einzelnen Ebenen der Anwendung (Betriebssystem, Webserver, Anwendungsserver, Datenbank, etc.) nicht sicher konfiguriert sind.

Durchgeführte Prüfungen: ASVS V3, V6, V7, V9

A6 – Kryptografisch unsichere Speicherung

Diese Schwachstelle tritt auf, wenn sensible Daten mangels ausreichender Verschlüsselung bei der Speicherung, Übertragung oder Ausgabe im Browser von Angreifern ausgelesen oder manipuliert werden können.

Durchgeführte Prüfungen: ASVS V8

A7 – Unzureichender URL-Zugriffsschutz

Diese Schwachstelle tritt auf, wenn der direkte Zugriff auf geschützte URLs möglich ist. Durch gezielte URL-Manipulierung lassen sich dann Zugriffsbeschränkungen umgehen.

Durchgeführte Prüfungen: ASVS V3

A8 – Cross-Site Request Forgery (CSRF)

Diese Schwachstelle tritt auf, wenn Angreifer mithilfe manipulierter HTTP-Anfragen Aktionen im Namen und Kontext eines Benutzers durchführen können.

Durchgeführte Prüfungen: ASVS V2

A9 – Komponenten mit bekannten Schwachstellen

Diese Schwachstelle tritt auf, wenn fertige Komponenten wie z. B. Libraries, Frameworks und andere Softwaremodule mit bekannten Schwachstellen eingesetzt werden. Dies beeinträchtigt die Sicherheit der gesamten Anwendung.

Durchgeführte Prüfungen: Schwachstellen-Scan

A10 – Ungeprüfte Weiterleitungen

Diese Schwachstelle tritt auf, wenn die Anwendung das Ziel einer Weiterleitung nicht ausreichend prüft. Angreifer können dann Weiterleitungen manipulieren und ihre Opfer dadurch auf Schadcode- oder Phishing-Seiten umleiten.

Durchgeführte Prüfungen: ASVS V4

Fazit

Im Web-Portal www.landlive.com wurden die wichtigsten Empfehlungen der OWASP Top 10 umgesetzt. Einige geringe Restrisiken wurden vom Deutschen Landwirtschaftsverlag akzeptiert.

+49 89 307657-16 info@plan42.com www.plan42.com