Top 5 Schwachstellen (Sortiert nach Kritikalität und Score)

Score	Typ	ID	Beschreibung	Betroffene Systeme
-3.21	DSGVO	DSGVO-Warnung	Cookies vor Zustimmung gesetzt	9

Problembeschreibung

Die Datenschutzgrundverordnung (DSGVO) stellt personenbezogene Daten unter besonderen Schutz. Insbesondere im Internet fallen personenbezogene Daten bei nahezu jedem Vorgang an. Der Grund: Beim Aufruf einer Webseite wird immer die IP-Adresse (Netzwerkadresse) des Nutzers übertragen. Der Europäische Gerichtshof und auch der Bundesgerichtshof haben IP-Adressen als personenbezogene Daten klassifiziert. Weitere Beispiele für personenbezogene Daten sind der Name, aber auch Adressdaten, Standortdaten (Handy), Nummernschilder, Bankverbindungen, Gesundheitsdaten, Personaldaten oder die Gehaltsabrechnung. Auf einer Webseite sind zahlreiche Aspekte DSGVO-relevant.

Gefahren

Für Betreiber der betroffenen Webseiten besteht die Gefahr einer Abmahnung durch einen Besucher.

Abhilfe

Die Betreiber der Webseite sollten Cookies und Skripte, welche Werbe- und Trackingzwecken dienen, nur nach ausdrücklicher Einwilligung des Nutzers einbinden und aktivieren. Für diese Zwecke existieren Cookie Consent Tools.

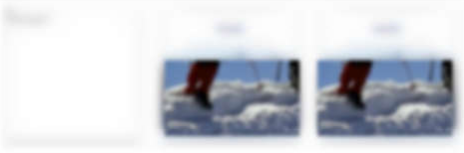
Schwachstellenliste

-2.44	DSGVO	Google Analytics	Cookie _gid von Google Analytics ohne Zustimmung gesetzt	16
-0.76	DSGVO	Google	Cookie NID von Google ohne Zustimmung gesetzt	5
--	DSGVO False Positive?	.AspNetCore.Antiforgery.w5W7x28NAIs	Cookie .AspNetCore.Antiforgery.w5W7x28NAIs ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	_ga_FJWTSSLTLW	Cookie _ga_FJWTSSLTLW ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	robee_ppid	Cookie robee_ppid ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	robee_vst_d	Cookie robee_vst_d ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	oPcYiN5v0t	Cookie oPcYiN5v0t ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	robee_sid	Cookie robee_sid ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	robee_uid	Cookie robee_uid ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	_ga_ZGDYCKEMVH	Cookie _ga_ZGDYCKEMVH ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	_zendesk_session	Cookie _zendesk_session ohne Zustimmung gesetzt	3
--	DSGVO False Positive?	_zendesk_shared_session	Cookie _zendesk_shared_session ohne Zustimmung gesetzt	3
--	DSGVO False Positive?	DSSignInURL	Cookie DSSignInURL ohne Zustimmung gesetzt	2
--	DSGVO False Positive?	DSSIGNIN	Cookie DSSIGNIN ohne Zustimmung gesetzt	2
--	DSGVO False Positive?	ClientId	Cookie ClientId ohne Zustimmung gesetzt	1
--	DSGVO False Positive?	cookieTest	Cookie cookieTest ohne Zustimmung gesetzt	1
--	DSGVO False Positive?	PHP.net	Cookie PHPSESSID von PHP.net ohne Zustimmung gesetzt	8
--	DSGVO False Positive?	Microsoft Azure App Insights	Cookie ai_session von Microsoft Azure App Insights ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	Azure / Microsoft	Cookie ARRAffinitySameSite von Azure / Microsoft ohne Zustimmung gesetzt	4
--	DSGVO False Positive?	Cloudflare	Cookie __cfruid von Cloudflare ohne Zustimmung gesetzt	3

Score	Typ	ID	Beschreibung	Betroffene Systeme
-2.16	App	PHP 5.5.27	1 System mit Sicherheitslücken gefunden	1

Betroffene Systeme

IPs	Direkt betroffene URLs	Serverbezogene Domains
150.		.com om



Zeilen pro Seite: 25 1-1 von 1

Problembeschreibung

Anwendungssicherheit ist einer der komplexesten und umfangreichsten Punkte im Bereich IT-Sicherheit. Webanwendungen gehören heutzutage zum alltäglichen Leben dazu und werden in vielen Bereichen eingesetzt. Wird eine Sicherheitslücke einer verwendeten Webanwendung ausgenutzt, ist dies für den Betroffenen oftmals nicht direkt erkennbar. Selbst bei ausgereifter Software können Sicherheitslücken immer wieder auftreten. Deshalb ist es wichtig, die Anwendungssicherheit regelmäßig zu überprüfen. Einige Sicherheitslücken in Anwendungen sind beispielsweise SQL-Injections, Cross-Site-Scripting, Remote-Code-Executions und Buffer Overflows. Manchmal können auch mehrere Schwachstellen gleichzeitig in einer Software vorkommen und ausgenutzt werden. Der CVSS Score ist ein Standard in der IT-Sicherheitsbranche und gibt Auskunft über die Kritikalität der Sicherheitslücke, er bewegt sich zwischen 0 und 10, wobei 10 extrem kritisch ist. Mit Hilfe dessen können die gefährlichsten Schwachstellen als erstes geschlossen werden. Generell sind die Sicherheitslücken als kritisch einzustufen falls ein öffentlicher Exploit verfügbar ist.

Gefahren

Die Gefahren solcher Schwachstellen sind vielfältig. SQL-Injections betreffen beispielsweise Datenbanken. So können Unbefugte Datensätze in der Datenbank löschen, manipulieren oder sensible Daten aus der Datenbank auslesen. Dadurch können wichtige Daten gelöscht oder Kundendaten an Unbefugte gelangen. Angriffe durch Cross-Site-Scripting betten gefährliche Programmcodes in eine eigentlich sichere Umgebung ein. Es wird häufig für Phishing-Angriffe verwendet. Durch Phishing geraten Nutzerdaten und Kennwort für die betreffende Anwendung an Unbefugte. Unbefugte können sich dann Zugriff zur betroffenen Anwendung verschaffen und sich als die Person ausgeben, dessen Daten gestohlen wurden. Zuletzt erlauben Remote-Code-Executions das Ausführen von Schadcode auf den Unternehmensservern. Hierdurch ist es möglich Anwendungen zu manipulieren, und tiefer in das Netzwerk vorzudringen. Der Schaden für das betroffene Unternehmen kann damit sehr groß sein. Es können nicht nur Daten verloren