NACHRICHTEN AG

18. Juni 2025

Cookies unter Kontrolle: So bleibt Ihre Online-Sitzung sicher!

Erfahren Sie am 18.06.2025 alles über Cookies und deren Sicherheit in webbasierten Anwendungen im Landkreis Cham.

Cham, Deutschland - Am 18. Juni 2025 hat das Landratsamt bekannt gegeben, dass die geschlossene Verwaltungsstelle vorübergehend geschlossen bleibt. Laut der Mitteilung sind insbesondere die notwendigen Cookies, die für den Betrieb der Webseite erforderlich sind, nicht deaktivierbar. Diese Cookies, wie z.B. das ASP.NET_SessionId, sorgen dafür, dass die Seite reibungslos funktioniert und sind an Benutzeraktionen gekoppelt, etwa beim Festlegen von Datenschutzeinstellungen oder beim Ausfüllen von Formularen. Benutzer haben jedoch die Möglichkeit, ihre Browsereinstellungen zu ändern, was allerdings die Funktionalität bestimmter Bereiche der Website beeinträchtigen kann.

Diese Cookies, die keine personenbezogenen Daten speichern, sind essenziell für den Betrieb der Webseite. So findet man beispielsweise im System das Cookie __RequestVerificationToken, das gesetzt wird, sobald ein Anmeldeformular aufgerufen wird. Es bleibt bis zum Ende der Browsersitzung aktiv und trägt zur Sicherstellung der Sicherheit beim Anmelden bei. Ein weiteres wichtiges Cookie ist das ld-cookieselection, das die Auswahl der Cookie-Einstellungen des Nutzers speichert.

Wichtige Informationen zu Sitzungs-Cookies

Gemäß den Best Practices, die in verschiedenen technischen Blogs diskutiert werden, sollte der Standardname der Sitzungs-ID in ASP.NET, hier ASP.NET_SessionId, möglichst geändert werden. Der Grund: Ein standardmäßiger Name lässt Rückschlüsse auf die verwendete Technologie zu ج ein gefundenes Fressen für potenzielle Angreifer. Die Länge der Sitzungs-ID empfiehlt sich dabei auf mindestens 128 Bit zu setzen, um Brute-Force-Angriffe abzuwehren. Außerdem sollte die ID vollständig zufällig generiert werden, um Vorhersagbarkeit zu vermeiden. Daten wie Passwörter sollten niemals in Cookies gespeichert werden, sondern lieber an gesicherten Orten auf dem Server verwahrt werden.

Ein weiteres wichtiges Thema ist die Nutzung von HTTPS für alle sitzungsbasierten Anwendungen, vor allem wenn sensible Daten verarbeitet werden. Sicherheitsaspekte stehen hier klar im Vordergrund, und dazu gehört auch, dass die Secure- und HttpOnly-Eigenschaften für Cookies aktiviert sind. Um gleichzeitige Sessions zu vermeiden, sollten nach einem Timeout, bei Abmeldung oder beim Schließen des Browsers die Sessions gelöscht werden. Außerdem wäre es ideal, Ablaufdaten für Cookies auf die kürzest mögliche Zeit zu setzen, um Sicherheitsrisiken zu minimieren.

Sichere Cookies in ASP.NET Core

Eine neue Regel in der Softwareentwicklung, die auch als CA5383 bekannt ist, betont die Notwendigkeit, sichere Cookies in ASP.NET Core zu nutzen. Diese Regel sorgt dafür, dass Cookies nur über die TLS-Verschlüsselung (HTTPS) übertragen werden, um sicherzustellen, dass sie nicht leicht abgehört werden können. Das bedeutet, dass alle Anwendungen, die mit sensiblen Daten arbeiten, von diesen Sicherheitsfeatures profitieren sollten.

Zusammenfassend lässt sich sagen, dass Sicherheit im Bereich der Cookies und Webanwendungen von höchster Wichtigkeit ist. Durch die richtige Handhabung und Indentifizierung dieser Cookies lassen sich viele Sicherheitsrisiken abwenden, und die Integrität der Benutzerdaten bleibt gewahrt. Wer also Online-Dienste nutzt, sollte sich der Bedeutung dieser technischen Details bewusst sein und stets auf sicheren Betrieb achten.

Für weitere Details zu den Cookies und deren Verwaltung, empfiehlt sich ein Blick auf die Informationen von Landkreis Cham, die dazu ausführlich berichtet. Auch die Best Practices auf Tech Community Microsoft und die allgemeinen Regelungen auf Microsoft Docs bieten wertvolle Informationen.

Details	
Ort	Cham, Deutschland
Quellen	• www.landkreis-cham.de • techcommunity.microsoft.com • learn.microsoft.com