LU04.A04 - (A1) Brocken Authentication

Internal reference: exer/04-4.md Um Session-Hijacking zu verhindern, sollten Entwickler starke Sicherheitsmaßnahmen implementieren, um Session-Token vor Diebstahl oder Vorhersage zu schützen. Nachfolgend eine Auswahl an Sicherheitsmaßnahmen:

Sichere und zufällige Session-Token verwenden

Generieren Sie kryptografisch sichere Token mithilfe starker Randomisierung (z. B. UUIDs, HMAC oder SHA-256). Vermeiden Sie vorhersehbare Muster (z. B. fortlaufende IDs oder Zeitstempel). Erhöhen Sie die Token-Länge, um Brute-Force-Angriffe zu erschweren.

Sichere Cookies implementieren

Verwenden Sie das **Secure-Flag**, um sicherzustellen, dass Cookies nur über HTTPS gesendet werden. Setzen Sie das **HttpOnly-Flag**, um zu verhindern, dass JavaScript auf Session-Cookies zugreift. Aktivieren Sie **SameSite-Attribute**, um den seitenübergreifenden Zugriff einzuschränken.

Kurze Session-Lebensdauer und -Generierung verwenden

Implementieren Sie kurze **Session-Ablaufzeiten**, um das Angriffsfenster zu begrenzen. Generieren Sie **Session-Token** nach dem Login und der Rechteausweitung neu.

Session-Binding implementieren

Sitzungstoken (Session-Token) an **IP-Adressen** oder **User-Agents binden**, um Wiederverwendung zu verhindern. Auf plötzliche Änderungen der **Sitzungsattribute** achten und Sitzungen bei Erkennung ungültig machen.

Verdächtige Aktivitäten überwachen und erkennen

Rate limiting implementieren, um Brute-Force-Angriffe zu erkennen. **Sitzungsaktivitäten protokollieren** (Monitoring) und auf Anomalien analysieren (z. B. mehrfache Anmeldungen von

verschiedenen Standorten).

Multi-Faktor-Authentifizierung (MFA) verwenden

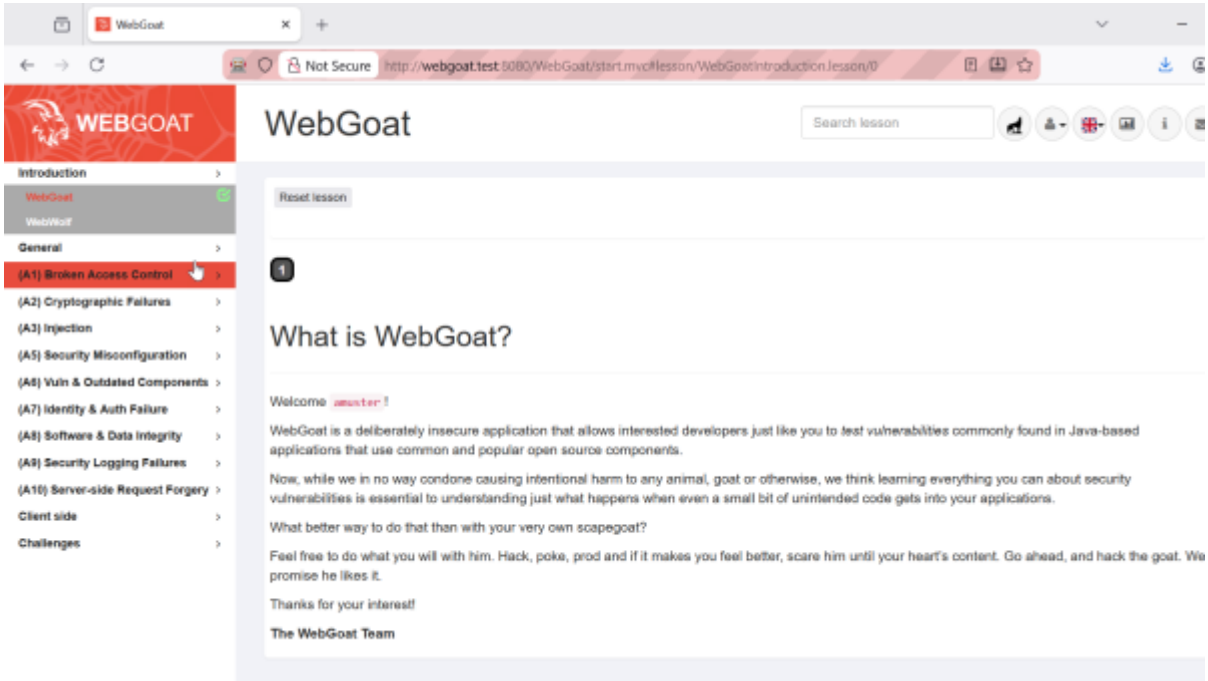
Selbst wenn ein Angreifer eine Sitzung stiehlt, bietet MFA eine zusätzliche Sicherheitsebene. Für sensible Aktionen (z. B. Änderung von Kontoeinstellungen) eine erneute Authentifizierung erzwingen.

Sitzungen beim Abmelden ungültig setzen

Serverseitige Sitzungslöschung beim Abmelden sicherstellen, um Wiederverwendung zu verhindern. Eine Abmeldefunktion (Log out) implementieren, die Sitzungsdaten ordnungsgemäß löscht.

Übungen

Bearbeiten Sie mit WebGoat die Übung in Kurs-Repository 02/02_Exercises/01-05



WARNUNG

Dieses Programm dient ausschließlich Bildungszwecken. Wenn Sie diese Techniken ohne Genehmigung anwenden, werden Sie mit hoher Wahrscheinlichkeit erwischt. Bei unautorisierten Hacking-Aktivitäten werden Sie von den meisten Unternehmen entlassen oder von den öffentlichen Behörden juristisch verfolgt respektive belangt. Die Behauptung, Sie hätten Sicherheitsforschung betrieben, ist nicht haltbar, da dies die erste Ausrede aller Hacker ist.
