WORUM ES GEHT

SESSIONS FÜR DIE AUTHENTIFIZIERUNG NUTZEN

Bei der Nutzung von Sessions für die Authentifizierung wird die aktive Anmeldung eines Benutzers in Form von Session-Cookies gespeichert, sodass der Benutzer sich nicht bei jedem Website-Aufruf (bei jedem Klick oder jeder Anfrage an den Server) erneut anmelden muss. Dies ermöglicht eine nahtlose Benutzererfahrung. Da zwischen dem an der Authentifizierung beteiligten Server und Browser jedoch kein Austausch über diese stattfindet, ist diese Methode nicht 100% sicher und es wird gerne versucht, diese Schwachstelle auszunutzen. Das folgende Beispiel zeigt das Problem.

SESSION HIJACKING – DIE TCP METAPHER

Quelle: https://lippke.li/session-hijacking

Tatort: Umkleideraum eines Schwimmbads

Heute ist das große Wasserball-Match Mannheim gegen Frankfurt.

Der Frankfurter Torwart Hans und sein Kapitän Peter ziehen Sich in der Umkleide um. Die Kabinen sind voneinander getrennt und Sie können sich nicht sehen. Sie können nur über Zurufen miteinander reden. Als coolen Gag (und für die Sicherheit) nutzen Sie den Code „Ente 42“, um sich gegenseitig zu bestätigen.

Hans: „Ente 42 – Bleibst Du beim Match mehr auf der rechten Seite heute?“

Peter: „Ja, aber nur in der 1. Hälfte – dann möchte ich meine Strategie ändern.“

Hans ist schnell umgezogen – Peter braucht etwas länger, weil er seine Badekappe sucht. Hans verlässt den Umkleideraum und der Mannheimer Phil kommt herein. Er hatte von der Tür aus mitgehört, worüber die beiden Frankfurter geredet haben.

Peter kämpft mit seiner Badekappe, als er eine Stimme hört.

(Phil): „Ente 42 – Wie sieht noch mal heute unsere Strategie aus? Ich hab’s wieder vergessen.“

Peter: (…antwortet sehr ausführlich…)

Das Geheimnis ist raus. Die Mannheimer besiegen die ahnungslosen Frankfurter mit 6:1.

AUFGABE

1. Lese die Metapher auf Seite 1.

2. Versuche zu beschreiben: **was geschieht hier genau? Was ist das Problem?**

3. Überlege dir, was das **Codewort «Ente 42»** in Bezug auf den Server-Client Kreislauf ist

4. Wenn Hans und Peter nun Server und Client wären, was ratest du ihnen für das nächste Mal?

5. **Zurück zu Sessions**: welche Massnahme hast du selbst schon erlebt im Zusammenhang mit dem Wort «Session», von der du vermutest, dass sie aus Sicherheitsgründen eingebaut wurde? Überlege dir, wie dies die Sicherheit von Sessions verbessert