Team 10 Rupp, Brandl

Kontrollfrage 7

Frage 7.1

> Nach welchem Mechanismus wählt der Server die Cipher Suite für eine Verbindung aus den vom Client angebotenen Cipher Suites aus?

Der Client schickt dem Server eine Liste der für ihn verfügbaren Cypher Suites.
Der Server wählt anhand der Verfügbaren TLS-Version die sicherste aus.

Frage 7.2

> Wie sieht die Kommunikation zwischen Client und Server aus, wenn der Client Port 80 anfragt und auf Port 443 umgeleitet wird?

Port 80 ist HTTP. Durch die Weiterleitung über Port 443 wird die Kommunikation durch HTTPS verschlüsselt.

Frage 7.3

> Was bewirken die Parameter maxage=31536000; includeSubDomains bei HSTS?

maxage definiert die Zeit in Sekunden in der der Browser sich die HSTS-Config merkt z.B. dass die Website nur über HTTPS erreichbar ist.
includeSubDomains sorgt dafür, dass die Regeln auch für die Subdomains angewandt werden

Frage 7.4

> Welche Vorteile hat es aus Sicht der Sicherheit, wenn Sie die Logs mehrerer Systeme zentral sammeln können?

Zentralisierte Logs lassen sich einfacher und zeitsparender überwachen. Security Breaches sind schneller und einfacher zu finden.
Die Überwachung zentralisierter Logs lässt sich leichter automatisieren.

Frage 7.5

> Sehen Sie Gefahren bei der Umsetzung eines Logservers, so wie er im Praktikum verwendet wurde?

Ja, durch die zentralisierte Verwaltung von Logsystemen kann Malware darüber verteilt werden.
Stichwort: Log4shell etc.