Presentation i Google Slides
Dokument i Google Docs
Hemläxa kopplad till lektionen
Prov kopplad till lektionen

Lektionsplanering: Säkerhet och skydd mot attacker

Årskurs: Gymnasiet
Ämne: Webbserverprogrammering 1
Tema: Säkerhet och skydd mot attacker

Koppling till styrdokument

Centralt innehåll

Denna lektion syftar till att ge en förståelse för säkerhetsaspekter vid webbserverprogrammering samt att diskutera vanliga attacker mot webbapplikationer och hur man kan skydda sig mot dem. Eleverna lär sig om säkerhetspraxis och hur man implementerar de bästa metoderna för att skydda sina webbprojekt.

Kunskapskrav

Eleven ska kunna beskriva vanliga säkerhetshot inom webbserverprogrammering och tillämpa säkerhetsåtgärder i sina egna webbapplikationer.

Lärarledda instruktioner

Introduktion till säkerhet inom webbprogrammering (10 min)

- Förklara vikten av säkerhet i webbapplikationer och dess påverkan på användare och företag.
- Diskutera olika typer av säkerhetshot som består av webbapplikationer, såsom hackerattacker, dataintrång och DDoS-attacker.

Vanliga attacker och deras konsekvenser (15 min)

- Gå igenom vanliga typer av attacker, inklusive SQL-injektion, Cross-Site Scripting (XSS), och CSRF (Cross-Site Request Forgery).

- Diskutera konsekvenserna av dessa attacker och hur de kan undvikas.
- Ge exempel på dokumenterade fall där säkerhetsbrister lett till allvarliga konsekvenser.

Säkerhetsåtgärder och bästa metoder (15 min)

- Presentera säkerhetsåtgärder som kan implementeras i webbapplikationer, inklusive användning av HTTPS, inmatningsvalidering, och kryptering av känslig information.
- Diskutera vikten av säkra autentiseringsmetoder och hur man skyddar användardata.
- Gå igenom hur man genomför säkerhetstester av sina applikationer.

Reflektion och diskussion (10 min)

- Sammanfatta viktiga punkter om att skydda webbapplikationer och de olika säkerhetshot som finns.
- Diskutera hur nödvändigt det är att tänka på säkerhet under hela webbprojektets livscykel.
- Svara på eventuella frågor från eleverna.

Aktivitet

Eleverna delas in i grupper och får i uppdrag att identifiera säkerhetsrisker i en hypotetisk webbapplikation. De ska presentera sina fynd och föreslå säkerhetsåtgärder som kan vidtas för att åtgärda problemen. Denna aktivitet syftar till att utveckla deras förmåga att tänka kritiskt kring säkerhet.

Exit-ticket

- Vad är en SQL-injektion? (En typ av attack där en hacker försöker manipulera en databasfråga genom att infoga skadlig kod)
- Nämn en typ av attack och dess konsekvenser. (XSS; kan leda till stöld av sessioncookies.)
- Varför är HTTPS viktigt? (Det skyddar dataöverföringar mellan webbläsare och server genom kryptering.)
- Vilka metoder kan du använda för att skydda användardata? (Kryptering, säker autentisering, korrekt inmatningsvalidering.)
- Ge ett exempel på en säkerhetsåtgärd för webbsidor. (Användning av CAPTCHA för att skydda mot automatiserade attacker.)

Hemuppgift

Som hemuppgift ska eleverna skriva en reflektion över en säkerhetsåtgärd de anser vara viktig inom webbserverprogrammering. De ska diskutera

varför den är viktig och hur den kan tillämpas praktiskt i ett projekt.

Citat

”Säkerhet börjar med att tänka som en hacker.” – Okänd

Citatet betonar vikten av att förstå säkerhetshot för att effektivt kunna skydda sina applikationer.

Tags: Lektion