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

Lektionsplanering

Årskurs: Gymnasiet

Ämne: Webbutveckling 2

Tema: Säkerhet och skydd mot attacker

Koppling till styrdokument

Centralt innehåll

Denna lektion syftar till att ge en förståelse för säkerhetsaspekter inom webbserverprogrammering och hur man skyddar sina webbapplikationer från olika typer av attacker. Eleverna ska lära sig om vanliga säkerhetshot och hur man tillämpar säkerhetsåtgärder i sina projekt.

Kunskapskrav

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

Lärarledda instruktioner

Introduktion till webbapplikationssäkerhet (10 min)

- Förklara varför säkerhet är viktigt inom webbutveckling och webbserverprogrammering.
- Diskutera olika typer av hot, inklusive hackerattacker, dataintrång, DDoS-attacker och informationsläckor.

Vanliga säkerhetshot (15 min)

- Gå igenom detaljerade exempel på vanliga attacker, såsom SQL-injektion, Cross-Site Scripting (XSS), och session hijacking.
- Diskutera konsekvenserna av dessa attacker och hur de kan påverka både användare och webbplatsägare.

Säkerhetsåtgärder och bästa metoder (15 min)

- Presentera säkerhetsåtgärder som kan implementeras, inklusive inskränkningar av inmatningar, användning av HTTPS, och korrekt hantering av användardata.
- Gå igenom vikten av stark autentisering och hur man implementerar metoder för att förhindra angrepp.
- Diskutera hur man genomför säkerhetstester och hållbara kodningsmetoder.

Reflektion och diskussion (10 min)

- Sammanfatta viktiga punkter om säkerhetshot och skyddsåtgärder.
- Diskutera hur eleverna kan tillämpa denna kunskap i sina egna webbapplikationer.
- Svara på eventuella frågor från eleverna.

Aktivitet

Eleverna delas in i grupper och får i uppgift att identifiera och presentera säkerhetsrisker i en fiktiv webbapplikation. De ska beskriva hur dessa risker kan åtgärdas med specifika säkerhetsåtgärder. Varje grupp presenterar sina fynd och förslag för klassen.

Exit-ticket

- Vad är en SQL-injektion? (En attack där en hacker försöker manipulera en databasfråga genom att infoga skadlig kod.)
- Nämn en typ av attack och dess potenta konsekvenser. (XSS; kan leda till stöld av sessioncookies eller användardata.)
- Hur skyddar HTTPS webbplatsinformation? (Genom att kryptera dataöverföringar mellan webbläsaren och servern.)
- Vilka metoder kan du använda för att säkerställa användardata? (Kryptering, inskränkningar av inmatningar.)
- Ge ett exempel på hur man kan förhindra CSRF-attacker. (Genom att använda tokens för att verifiera användarinteraktioner.)

Hemuppgift

Som hemuppgift ska eleverna skriva en reflekterad text om en säkerhetsåtgärd de anser vara viktig inom webbserverprogrammering. De ska diskutera varför åtgärden är viktig och hur den kan tillämpas praktiskt i ett projekt. Skriv “Hemuppgift” så tar jag fram en hemuppgift åt dig.

Citat

”Säkerhet är inte något du kan köpa; det är något du bygger.” – Okänd

Citatet betonar vikten av kontinuerlig uppmärksamhet och arbete för att skapa säkerhet i webbapplikationer.

Tags: Lektion