

Prov: Autentisering och säkerhet i webbtjänster

Prov: Autentisering och säkerhet i webbtjänster

Årskurs: Gymnasiet

Ämne: Webbtjänster

Tema: Autentisering och säkerhet i webbtjänster

Koppling till styrdokument

Centralt innehåll

Undervisningen ska belysa vikten av autentisering och säkerhet inom webbtjänster, inklusive olika metoder för att skydda användardata. Centrala aspekter inkluderar hur man implementerar säkra autentiseringstekniker samt hur man hanterar säkerhetsrisker kopplade till webbtjänster.

Kunskapskrav

Eleven redogör för olika metoder för autentisering och säkerhet i webbtjänster. Eleven kan ge exempel på säkerhetsprotokoll och beskriva hur dessa kan implementeras samt identifiera potentiella säkerhetsrisker.

Prov

Faktafrågor

1. Vilken av följande metoder är en typ av autentisering?

- A) Datakryptering
- B) ****Användarnamn/lösenord****
- C) Brandväggar
- D) Antivirusprogram

2. Vad står förkortningen JWT för?

- A) Java Web Token
- B) ****JSON Web Token****
- C) JavaScript Web Token

D) Java Web Tool

3. Vilken teknik används för att verifiera en användares identitet via en tillfällig kod skickad till en mobiltelefon?

- A) Lösenordsskydd
- B) ****Tvåfaktorsautentisering****
- C) Biometrisk autentisering
- D) OAuth

4. Vilket av följande är en vanlig säkerhetsrisk kopplad till webbtjänster?

- A) ****Dataintrång****
- B) Regelbundna uppdateringar
- C) Användardatabas
- D) Kodsäkerhet

5. Vad är syftet med autentisering?

- A) Att registrera användare
- B) ****Att bekräfta en användares identitet****
- C) Att lagra användardata
- D) Att analysera trafik

6. Vilken typ av autentisering använder användarnamn och lösenord?

- A) ****Basautentisering****
- B) Token-baserad autentisering
- C) Biometrisk autentisering
- D) OAuth

7. Vad är en säkerhetsprotokoll?

- A) En säkerhetsmetod som skyddar användardata
- B) ****Ett regelverk för hur data ska överföras säkert****
- C) En typ av databas
- D) En användarprofil

8. Vad innebär auktorisering?

- A) Att bekräfta identiteten hos en användare
- B) ****Att ge en användare åtkomst till resurser****
- C) Att spara användardata
- D) Att skapa konton

9. Vilket av följande beskriver enkelt hemlig nyckelbaserad autentisering?

- A) ****En förutbestämd nyckel används för att autentisera****
- B) Biometrisk identifiering
- C) Öppen nyckelinfrastruktur
- D) Användarnamn och lösenord

10. Vilken metod kan förbättra säkerheten när man loggar in på en

webbtjänst?

- A) ****Använda starka lösenord****
- B) Dela lösenord med andra
- C) Använda samma lösenord för flera tjänster
- D) Stänga av tvåfaktorsautentisering

11. Vad står förkortningen OAuth för?

- A) Open Authorization
- B) ****Open Authorization Framework****
- C) Open Access Framework
- D) Object Authorization

12. Vad är det primära målet med datakryptering?

- A) Att autentisera användaridentiteter
- B) ****Att skydda data under överföring****
- C) Att lagra backupkopior
- D) Att analysera datatrafik

13. Vilken typ av data kan riskeras vid en dataintrång?

- A) Endast offentliga data
- B) ****Personlig och känslig information****
- C) Systemdata
- D) Inga data riskeras

14. Vad kännetecknar en säkerhetsstandard?

- A) En rekommendation för webbutveckling
- B) ****En uppsättning krav för att skydda information****
- C) En enkel kodlösning
- D) En användartjänst

15. Vilken av följande tekniker används för att skydda webbanslutningar?

- A) HTML5
- B) ****SSL/TLS****
- C) FTP
- D) HTTP

Resonerande frågor

1. Vilka autentiseringstekniker anser ni är mest effektiva för att skydda webbtjänster? Varför?

(Syfte: Att ge eleverna möjlighet att diskutera och resonera kring effektiviteten av olika autentiseringstekniker.)

2. Hur kan användare skydda sig själva mot identitetsstöld och dataintrång?
(Syfte: Att låta eleverna reflektera över och ge praktiska exempel på

självförsvar.)

3. Vad är de största utmaningarna för utvecklare när det gäller att säkerställa säkerheten för webbtjänster?

(Syfte: Att hjälpa eleverna att identifiera och diskutera utvecklarens perspektiv på säkerhet.)

4. Hur kan organisationer säkerställa att deras autentiseringstekniker är up-to-date?

(Syfte: Att driva diskussion om vikten av kontinuerlig uppdatering av säkerhetstekniker.)

5. Vilka framtida trender tror ni kommer att påverka säkerhetstekniker inom webbtjänster?

(Syfte: Att ge eleverna möjlighet att tänka framåt och diskutera potentiella utvecklingar inom området.)

6. Hur bör webbtjänster hantera användardata för att minimera säkerhetsrisker?

(Syfte: Att uppmuntra eleverna att diskutera datahanteringsstrategier.)

7. Vilka konsekvenser kan en dataintrång ha för en webbplats?

(Syfte: Att diskutera realtidsimplikationer och risker kopplade till säkerhetsincidenter.)

8. Hur kan användarkunskap om säkerhet påverka deras beteende online?

(Syfte: Att reflektera över hur utbildning i säkerhet kan förändra användarbeteende.)

Bedömning

Faktafrågor: Varje rätt svar ger 1 poäng. Totalt 15 poäng tillgängliga.

Resonerande frågor: Varje fråga bedöms med upp till 3 poäng baserat på djup och relevans av svaret. Totalt 24 poäng tillgängliga.

För betyg E krävs minst 8 poäng, för betyg C krävs minst 12 poäng (minst 3 poäng från resonerande frågor) och för betyg A krävs minst 18 poäng (minst 5 poäng från resonerande frågor).