Provkonstruktion

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

Syfte

Syftet med provet är att utvärdera elevernas förståelse av säkerhet och skydd mot attacker inom webbserverprogrammering samt deras förmåga att tillämpa säkerhetsåtgärder i praktiken.

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.

Prov

Faktafrågor

1. Vad är en SQL-injektion?
A) En typ av databas
B) En typ av attack där en hacker försöker manipulera en databasfråga
C) En säkerhetsåtgärd
D) En typ av fel i programmering

2. Vilken av följande är en konsekvens av Cross-Site Scripting (XSS)?
A) Förbättrad webbserverprestanda
B) Stöld av sessioncookies
C) Färre inloggningsproblem
D) Ökad databas säkerhet

3. Vilket av följande skyddar dataöverföringar mellan webbläsare och server?
A) HTTPS
B) HTTP
C) FTP
D) SMTP

4. Vilken metod kan användas för att skydda användardata?
A) Att dela lösenord
B) Att inte validera inmatning
C) Kryptering
D) Att använda osäkra autentiseringar

5. Vad står CSRF för?
A) Centralized Security Risk Factor
B) Cross-Site Request Function
C) Common Security Resource Framework
D) Cross-Site Request Forgery

6. Vilken säkerhetsåtgärd hjälper till att skydda mot automatiserade attacker?
A) Open Source Software
B) CAPTCHA
C) HTML5
D) CSS

7. Vad är en DDoS-attack?
A) En attack som skyddar webbplatser
B) En attack som överbelastar en tjänst med trafik
C) En typ av datalagring
D) En säkerhetsåtgärd

8. Vad är inmatningsvalidering?
A) Att kontrollera om en webbsida är säker
B) Att verifiera användardata innan det behandlas
C) En metod för webbutveckling
D) En typ av attack

9. Vilka av följande är vanliga angrepp mot webbapplikationer?
A) Fysisk skada
B) Virus
C) SQL-injektion och XSS
D) Hårdvarufel

10. Vad innebär säkerhetstester?
A) Att skanna efter virus

B) Att förbättra visuell design
C) Att identifiera säkerhetsluckor i applikationer
D) Att utföra användartester

11. Vad är syftet med HTTPS?
A) Att skydda data under överföring
B) Att öka hastigheten på en webbplats
C) Att göra webbplatser mer attraktiva
D) Att förbättra serverns kapacitet

12. Vilken konsekvens kan en hackerattack leda till?
A) Inga problem
B) Förlust av användardata
C) Ökad prestanda
D) Säkrare betalningar

13. Vilken av följande metoder rekommenderas för säker autentisering?
A) Använda enklare lösenord
B) Tvåfaktorsautentisering
C) Delning av lösenord
D) Använda lika lösenord överallt

14. Varför är datakryptering viktigt?
A) Gör data mindre tillgänglig
B) Förbättrar hastigheten
C) Skyddar känslig information
D) Minskar lagringsutrymmesbehovet

15. Vilken typ av säkerhetsåtgärd rekommenderas för kodning?
A) Att lämna koden öppen
B) Att följa kodningsstandarder och bästa metoder
C) Att debuggersignaler lämnas för utvecklare
D) Att programmera utan granskning

Resonerande frågor

1. Diskutera varför säkerhet är en viktig aspekt av webbserverprogrammering.
Syftet med denna fråga är att ge eleverna möjlighet att visa på djup förståelse av ämnet.

2. Förklara hur en SQL-injektion fungerar och vilka konsekvenser den kan få för en webbapplikation.
Eleven ges möjlighet att bevisa sin förmåga att analysera specifika säkerhetshot.

3. Reflektera över hur en säkerhetsåtgärd du lärt dig kan tillämpas i ett verkligt projekt.
Denna fråga ger utrymme för tillämpning av teoretiska kunskaper i praktiken.

4. Diskutera vikten av inmatningsvalidering och hur den kan förhindra attacker.
Eleven får möjlighet att visa på sin förmåga att tänka kritiskt kring säkerhetsmetoder.

5. Resonera kring skillnaderna mellan olika typer av attacker, som XSS och CSRF.
Denna fråga låter eleverna visa djup förståelse och skillnad i attacker.

6. Hur skulle du gå tillväga för att genomföra ett säkerhetstest av en webbapplikation?
Syftet är att bedöma elevens praktiska tillämpning av säkerhetstester.

7. Resonera om hur medvetenhet kring säkerhetshandbok påverkar utvecklare.
Frågan ger möjlighet att koppla teoretiska aspekter med praktiskt tillämpande.

8. Vilka etiska överväganden bör beaktas vid utveckling av webbapplikationer?
Denna fråga syftar till att få eleven att reflektera över etik och ansvar i webbprogrammering.

Bedömning

Provets faktafrågor ger totalt 15 poäng, där varje korrekt svar ger 1 poäng. De resonerande frågorna ger totalt 8 poäng, där varje tillfredsställande svar ger 1 poäng.

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

Tags: Prov