Provkonstruktion

Årskurs: Gymnasiet

Ämne: Webbutveckling 2

Tema: Säkerhet och skydd mot attacker

Syfte

Syftet med provet är att bedöma elevernas förståelse för säkerhetsaspekter inom webbserverprogrammering samt deras förmåga att identifiera säkerhetshot och tillämpa lämpliga säkerhetsåtgärder i webbapplikationer.

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.

Prov

Faktafrågor

1. Vad är en SQL-injektion?

- A) En metod för att optimera databaser
- B) Ett sätt att kryptera användardata
- C) En attack där en hacker försöker manipulera en databasfråga genom att infoga skadlig kod
- **D) En typ av webbläsartillägg**

2. Vilken typ av attack kan leda till stöld av sessioncookies?

- A) CSRF
- **B) XSS**

- C) Brute force
- D) DoS

3. Vad gör HTTPS för att skydda webbplatsinformation?

- A) Använder starka lösenord
- **B) Krypterar dataöverföringar mellan webbläsaren och servern**
- C) Blockerar annonser
- D) Förbättrar laddningstiden

4. Hur kan man förhindra CSRF-attacker?

- **A) Genom att använda tokens för att verifiera användarinteraktioner**
- B) Genom att alltid använda HTTPS
- C) Genom att optimera databasen
- D) Genom att uppdatera programvaran regelbundet

5. Vilket av följande är ett exempel på en DDoS-attack?

- A) En attack som stjäl kreditkortsnummer
- **B) En attack som syftar till att överbelasta en server med trafik**
- C) En attack som manipulerar användardata
- D) En attack som skapar falska användarkonton

6. Vad är syftet med att använda stark autentisering?

- A) Att förbättra användarupplevelsen
- **B) Att förhindra obehörig åtkomst till användarkonton**
- C) Att öka webbplatsens hastighet
- D) Att analysera webbplatsens trafik

7. Vilken säkerhetsåtgärd kan implementeras för att förhindra SQL-injektion?

- **A) Använda inskränkningar av inmatningar**
- B) Läsa användardata i klartext
- C) Installera antispam-program
- D) Använda gamla databaser

8. Vilket av följande är en konsekvens av en dataintrång?

- **A) Förlust av användardata**
- B) Ökad webbplatstrafik
- C) Förbättrad sökmotoroptimering
- D) Mer användarattribut

9. Vad innebär “session hijacking”?

- A) Att skapa en ny användarsession
- **B) Att stjäla en aktiv session och agera som användaren**
- C) Att stänga ned alla sessioner
- D) Att förlänga sessionens varaktighet

10. Vilken metod används för att skydda insamlad användardata?

- A) Kryptering
- **B) Oskyddad lagring**
- C) Kodbokföring
- D) Offentlig åtkomst

11. Vad är Cross-Site Scripting (XSS)?

- **A) En attack som injicerar skadlig kod i en webbplats**
- B) En metod för att säkerhetskopiera data
- C) En typ av databashandling
- D) Ett sätt att öka webbplatsens hastighet

12. Vilken typ av test bör göras regelbundet för att säkerställa säkerheten i webbapplikationer?

- **A) Säkerhetstester**
- B) Prestandatester
- C) Användartester
- D) Grafiska tester

13. Vad innebär “phishing”?

- A) Att optimera en databas
- **B) Att lura användare att ge ut känslig information**
- C) Att blockera en webbplats
- D) Att uppdatera mjukvara

14. Vad bör göras vid upptäckta säkerhetsbrister?

- A) Ignorera dem
- **B) Åtgärda dem omedelbart**
- C) Rapportera dem till användarna
- D) Fördröja åtgärden

15. Vilken inverkan kan en DDoS-attack ha på en webbplats?

- **A) Gör webbplatsen otillgänglig för användare**
- B) Förbättrar webbplatsens rankning

- C) Ökar serverns lagringsutrymme
- D) Minskar säkerhetsriskerna

Resonerande frågor

1. Beskriv hur en XSS-attack fungerar och föreslå tre åtgärder för att förhindra den. Syftet är att ge eleverna möjlighet att visa djupare kunskap om attackens mekanik och åtgärder.

2. Diskutera betydelsen av programmeringsmetoder i säkerhetsarbetet och ge exempel på bästa praxis. Syftet är att utforska hur kodningsmetoder påverkar säkerheten i webbapplikationer.

3. Analysera konsekvenserna av ett dataintrång för både användare och företag. Syftet är att få eleverna att reflektera över de breda effekterna av säkerhetsbrister.

4. Jämför och kontrastera skillnaderna mellan HTTP och HTTPS ur ett säkerhetsperspektiv. Syftet är att låta eleverna visa förståelse för olika protokoll och deras inverkan på säkerheten.

5. Reflektera över hur användarutbildning kan bidra till att säkerställa webbapplikationers säkerhet. Syftet är att få eleverna att tänka på det mänskliga elementet i säkerhet.

6. Ge exempel på hur vanliga bibliotek och ramverk kan påverka säkerheten i applikationer. Syftet är att analysera källan till potentiella hot genom externa resurser.

7. Diskutera skillnaderna mellan aktiva och passiva säkerhetsåtgärder och ge exempel på båda. Syftet är att undersöka olika kategorier av säkerhetsåtgärder.

8. Redogör för hur man kan implementera säkerhetsåtgärder i en agila utvecklingsmetod. Syftet är att visa hur säkerhet kan integreras i hela utvecklingsprocessen.

Bedömning

Provets faktafrågor ger totalt 30 poäng, där varje fråga är värd 2 poäng.

För resonerande frågor finns totalt 20 poäng, där varje fråga är värd 5 poäng.

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

Tags: Gymnasiet, Webbutveckling, Webbutveckling 2