Blekinge Tekniska Högskola
Institutionen för datavetenskap

Revision: 1
Dnr: BTH-4.1.14-0312-2022

KURSPLAN

Säkerhet i webbsystem

Web System Security

7,5 högskolepoäng (7.5 credits)

Kurskod: DV2621
Huvudområde: Datavetenskap, Programvaruteknik
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska
Gäller från: 2022-08-29
Fastställd: 2022-03-01

1. Beslut

Denna kurs är inrättad av dekan 2021-12-03. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2022-03-01 och gäller från 2022-08-29.

2. Förkunskapskrav

För tillträde till kursen krävs 90 hp varav 40 hp inom det tekniska området varav en avklarad kurs på minst 6 hp ska vara inom programmering i C, C++, PHP eller Python samt en avklarad kurs på minst 4 hp inom nätverkssäkerhet, datakommunikation, nätverksteknologier och en avklarad kurs på minst 4 hp inom webbteknologier eller databaser eller minst 120 hp varav minst 90 hp inom det tekniska området samt minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare).

3. Syfte och innehåll

3.1 Syfte

Säkerhet i webbapplikationer omfattar hantering av svagheter och sårbarheter både på serversidan och på klientsidan. Kursens syfte är att studenterna skall lära sig hur svagheter och sårbarheter kan utnyttjas, hur de kan upptäckas, samt vilka lösningar kan användas för att skydda webbapplikationer och minimera risken att sådana attacker lyckas.

3.2 Innehåll

- Webbsystemarkitekturer och teknologier
- Spaningsattacker mot webbapplikationer
- Webbserversårbarheter
- Injektionsattacker och motmedel
- Allmän säkerhet för webbsessioner
- Vanliga autentiseringssårbarheter
- Vanliga auktoriserings- och åtkomstkontrollsfel
- Förfalskning av serverbegäran
- Sårbarheter i affärslogistiken
- OWASP-projekt (Open Web Application Security Project)
- Säkerhetsstandarder och ramverk för webbapplikationer: ISO 27000-serien, PCI-DSS, HIPPA, SOC2, SOX, NIST
- Testprocesser för säkerhet av webbplatser

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:

- redogöra för kända sårbarheter och svagheter webbprotokoll och applikationer
- redogöra för säkerhetsaspekter tillhörande olika teknologier, ramverk och plattformar
- redogöra för autentiseringsmekanismer och motmedel
- redogöra för webbapplikationer, sessionshantering och tillhörande svagheter

• förstå Cross-site scripting- (XSS) och Cross-site request forgery (CSRF)-attacker
• förstå Server-side Request Forgery (SSRF)-attacker
• förstå anledningar för och konsekvenser av olika injektionssårbarheter

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:
• tillämpa bästa praxis för säkra webbapplikationer
• utföra interna och externa säkerhetstester för webbapplikationer och relaterad infrastruktur
• utnyttja material från OWASP i tillämpliga delar

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:
• analysera och utvärdera säkerheten i ett webb-klient/server-system
• identifiera sårbarheter och svagheter samt genomföra lämpliga förbättringsåtgärder

5. Läraktiviteter

Undervisningen sker i form av föreläsningar, inspelat videomaterial, samt presentationer och grundläggande litteratur och annat skrivet material. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare ske via e-post, kursens lärarplattform och via fysiska eller online-möten.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2210	Laboration	4,5 hp	GU
2220	Praktiskt moment	1,5 hp	GU
2230	Salstentamen	1,5 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

• The Web Application Hacker's Handbook. Second Edition. Finding and Exploiting Security Flaws. Dafydd Stuttard, Marcus Pinto, ISBN: 978-1-118-02647-2.
• Web Penetration Testing with Kali Linux. Joseph Muniz. Aamir Lakhani, ISBN: 978-1782163169.
• Mastering Modern Web Penetration Testing. Prakhar Prasad, ISBN: 978-1785284588.
Material såsom forskningsartiklar och annat kursmaterial tillhandahålls på kursens lärplattform och via BTHs biblioteksresurser, samt rekommendationer för vidare läsning.

10. Övrigt

Denna kurs ersätter kursen DV2577