Blekinge Tekniska Högskola
Institutionen för datavetenskap

Revision: 4
Dnr: BTH-4.1.1–0263-2018

KURSPLAN

Webbsäkerhet

Web Security

7,5 högskolepoäng (7.5 credits)

Kurskod: DV2577
Huvudområde: Datavetenskap
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Ämnesgrupp: Datateknik
Undervisningsspråk: Svenska men undervisning på engelska kan förekomma.
Gäller från: 2018-03-01
Fastställd: 2018-03-01

1. Beslut

Denna kurs är inrättad av dekan 2017-12-20. Kursplanen är fastställd av prefekten vid institutionen för datalogi och datorsystemteknik 2018-03-01 och gäller från 2018-03-01.

2. Förkunskapskrav

För tillträde till kursen krävs avklarade kurser i Programmering 12 hp, Realtid- och operativsystem 6 hp, Datakommunikation 6 hp samt Databasteknik 6 hp. Genomgången kurs i Nätverkssäkerhet 4 hp eller Datorsystemsäkerhet 7,5 hp.

3. Syfte och innehåll

3.1 Syfte

Syftet med kursen är att studenten skall lära sig att förstå och upptäcka svagheter och sårbarheter i webbapplikationer samt att kunna utveckla lösningar för skydd och genomföra tester.

3.2 Innehåll

- Grunder och skyddsmetoder i protokoll för web, kryptering och epost.
- Webattacker och sårbarheter
- Websystemarkitekturer
- Autentisering / Auktorisering
- Klientattacker
- Kommando-exekvering
- Avslöjande och läckage av information
- Logiska attacker
- Utveckling av skyddade webplatser
- Metodiker
- Open Web Application Security Project(OWASP) implementering/testning
- Säkerhetsgranskning

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten:

- kunna redogöra för arkitekturer baserade på webb-protokoll utifrån gemensamma sårbarheter och svagheter samt känna till öppna sårbarhetsdatabaser
- kunna redogöra för säkerhetsaspekter vid användning av språk t.ex. PHP, JavaScript och SQL
- kunna förklara autentiseringsmekanismer och tekniker för att kringgå autentisering (bypass)
- kunna redogöra för programkodningsfel
- kunna förklara sårbarheter hos befintliga webbresurser och hur man handskas med dem vid design och under drift
- förstå designmönster för säkra webbapplikationer
- förstå Cross-site scripting (XSS) attacker och SQL-injektioner
- kunna beskriva och genomföra interna och externa penetrationstester
- Kunna förstå och förklara OWASP

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten:

- kunna skydda webbtjänster mot cyberattacker
- kunna tillämpa OWASP
- kunna skydda klient och server på webb-plattformar

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten:

- inhämta, utforska och värdera säkerhetsinformation för klient-server-system
- kunna identifiera och verkställa lämpliga motmedel

5. Läraktiviteter

Kursen innehåller föreläsningar och laborationer/projekt. Under föreläsningar presenteras de teoretiska aspekterna i kursen. Studenterna tillämpar innehållet från föreläsningarna i laborationerna och i projekt.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
1810	Laboration	4,5 hp	GU
1820	Salstentamen	3 hp	AF

Kursen bedöms med betygen A Utmärkt, B Mycket bra, C Bra, D Tillfredsställande, E Tillräckligt, FX Underkänd, något mer arbete krävs, F Underkänd.

I kurstillfällets kurs-PM framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

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

Material från institutionen.

10. Övrigt

Denna kurs ersätter kursen DV2571