



LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Avancerad webbsäkerhet Advanced Web Security

EITN41, 7,5 högskolepoäng, A (Avancerad nivå)

Gäller för: Läsåret 2023/24

Fakultet: Lunds tekniska högskola

Beslutad av: Programledning C/D

Beslutsdatum: 2023-04-18

Allmänna uppgifter

Undervisningsspråk: Kursen ges på engelska

Syfte

Kursen ska ge studenten fördjupad kunskap om de säkerhetsproblem som relaterar till webbt teknologi. En del områden som kräver kryptografiska primitiver kommer behandlas i detalj och en förståelse för dessa ska ge studenten verktyg att applicera sin kunskap på andra säkerhetstekniker.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- Beskriva vissa avancerade säkerhetsproblem som uppstår vid användning av webbaserade säkerhetstjänster.
- Beskriva hur kryptografisk data kan representeras på webben.
- Beskriva möjligheter och problem relaterade till e-handel och elektroniska betalningar.

Färdighet och förmåga

För godkänd kurs skall studenten

- Kunna analysera säkerhetsprotokoll, identifiera svagheter och problem, och föreslå lösningar.
- Visa förståelse för de tekniska lösningarna som finns för att undvika säkerhetsproblem.
- Visa förståelse för säkerhetsbegränsningarna i de berörda protokollen.
- Applicera designval i de berörda protokollen på andra protokoll.
- Kunna implementera givna säkerhetsprotokoll

Värderingsförmåga och förhållningssätt

För godkänd kurs skall studenten

- Kunna diskutera och presentera lösningarna till hemuppgifter.
- Kunna diskutera designbeslut i de säkerhetsprotokoll som berörs i kursen.

Kursinnehåll

Datarepresentation: CMS, ASN.1, BER, CER och DER-kodning

PKI & Säkerhet i webbtjänster: PKCS#12, CRL, OCSP, signeringsprocedurer

Anonymitet: Anonymitetslösningar, Chaum-mixar, Tor, attacker

Elektroniska val: protokoll för elektroniska val, homomorfisk kryptering, ZK-proofs, threshold decryption

Elektroniska meddelanden: OTR, Signal

e-handel: Elektroniska betalningar, SET, 3D Secure, Bitcoin, microbetalningar, untraceable E-cash

Allt kursmaterial och undervisningsmoment kommer att vara på engelska.

Kursens examination

Betygsskala: TH - (U,3,4,5) - (Underkänd, Tre, Fyra, Fem)

Prestationsbedömning: Betygsatta hemuppgifter ger betyg 3 eller 4. Om betyg 4 uppnås på hemuppgifter kan betyg 5 erhållas genom muntlig tentamen.

Om så krävs för att en student med varaktig funktionsnedsättning ska ges ett likvärdigt examinationsalternativ jämfört med en student utan funktionsnedsättning, så kan examinator efter samråd med universitetets avdelning för pedagogiskt stöd fatta beslut om alternativ examinationsform för berörd student.

Antagningsuppgifter

Förutsatta förkunskaper: EIT060/EITA25 Datasäkerhet, EITF05 Webbsäkerhet

Begränsat antal platser: Nej

Kursen överlappar följande kurser: EITN40

Kurslitteratur

- Föreläsninganteckningar.
- Akademiska artiklar.

Kontaktinfo och övrigt

Kursansvarig: Paul Stankovski Wagner, paul.stankovski_wagner@eit.lth.se

Hemsida: <http://www.eit.lth.se/kurs/EITN41>

Övrig information: Kursmaterialet kommer att vara på engelska.