O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
Dj.Sultanov
“ ” 2023-yil

Ro‘yxatga olindi: №
2023-yil “ ”

DASTURIY VOSITALAR XAVFSIZLIGI

O‘QUV DASTURI

Bilim sohasi: 600 000 - Axborot-kommunikatsiya texnologiyalari

Ta’lim sohasi: 610 000 - Axborot-kommunikatsiya texnologiyalari

Ta’lim yo‘nalishi: 60612100 - Kiberxavfsizlik injiniringi

Toshkent – 2023

Fan/modul kodi	O‘quv yili 2023-2024	Semestr 5	ECTS - kreditlar 6
Fan/modul turi Majburiy	Ta’lim tili O‘zbek/rus		Xaftadagi dars soatlari 5

	Fanning nomi	Auditoriya mashg’ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
1.	**Dasturiy vositalar xavfsizligi**	**74**	**106**	**180**

2. I. Fanning mazmuni

Fanni o‘qitishdan maqsad – Fanni o‘qitishdan maqsad – talabalarda dasturiy ta’minotni xavfsizlik nuqtai-nazaridan kelib chiqqan holda yozish ko‘nikmalarini hosil qilishdan iborat.

Fanning vazifalari - dasturiy ta’minotni yaratishning hayotiy sikli, dastur kodini xavfsiz yozish, dasturlarda kriptografik himoya usullaridan foydalanish, dastur kodini xavfsizlik xususiyati bo‘yicha testlash, axborot xavfsizligining dasturiy vositalarini yaratish va ularni tahlil qilish masalalarini muvaffaqiyatli hal etishga tayyorlashdan iborat.

“Dasturiy vositalar xavfsizligi” o‘quv fanini o‘zlashtirish jarayonida amalga oshiriladigan masalalar doirasida talaba:

– dasturiy vositalarni yaratishda xavfsizlik talablariga e’tibor berish va xavfsiz dasturiy vositalarni hozirgi zamondagi o‘rni muhimligi haqida haqida tasavvurga ega bo‘lishi;
– dasturiy vositani ishlab chiqishning hayotiy siklini;
– dasturiy vositalarni yaratishdagi mavjud xavfsizlik muammolarini;
– dasturiy vositalarni ularni hayotiy siklining turli bosqichlarida tekshirishni;
– dasturiy vositalar kodini statik testlashni;
– dasturiy vositalarni xavfsizlik nuqtai nazaridan testlashni;
– dasturiy vositalarni foydalanishga tayyorlashni va ularga xizmat ko‘rsatishni bilishi va ulardan foydalana olishi;
– dasturiy vositalarni xavfsizlik nuqtai nazaridan amalga oshirish, ularni statik va xavfsizlik testlari yordamida baholash hamda dasturiy vositalarni foydalanishga tayyorlash va ularga xizmat ko‘rsatish ko‘nikmalariga ega bo‘lishi kerak.

II. Asosiy nazariy qism (ma’ruza mashg‘ulotlari)

II.I. Fan tarkibiga quyidagi mavzular kiradi:

1-mavzu. Dasturiy vositalar xavfsizligi faniga kirish.

Fanning maqsadi va vazifasi. Axborot xavfsizligining asosiy tushunchalari. Xavfsiz dasturiy vositalarni yaratish zaruriyati. Dasturiy vositalarda xavfsizlik muammolari. Dasturiy vositani ishlab chiqarishning hayotiy sikli va uning modellari.

2-mavzu. Dasturiy vositani ishlab chiqarishning hayotiy sikli.

Dasturiy vositaning hayotiy sikli tushunchasi, modellari. Sharshara modeli. Iterativ model. V modeli.

3-mavzu. Dasturiy vositalarga qo‘yilgan xavfsizlik talablari.

Dasturiy vositalarga qo‘yiladigan vazifaviy va novazifaviy talablar. Xavfsizlik talablari. SQUARE (Security Quality Requirements Engineering) metodologiyasi.

4-mavzu. Dasturiy vositalar arxitekturasi va loyihalash.

Dasturiy vositalarni loyihalash. Ma’lumot oqimi diagrammalari va darajalari. Dasturiy vosita arxitekturasi. Dasturiy vosita arxitektura stillari. Truba va filter arxitekturasi (pipe and filter). Obyektga yo‘naltirilgan arxitektura. Mijoz – server arxitekturasi. Obyekt broker arxitekturasi. Hodisaga asoslangan arxitektura (oshkor bo‘lmagan chaqiruv). Qatlamli arxitektura. Saqlagich arxitekturasi. Jarayonlarni nazoratlash arxitekturasi.

5-mavzu. Dasturiy vositalarda mavjud xavfsizlik muammolari.

Dasturiy vositalar zaifligi va uning sabablari. Keng tarqalgan dasturiy vosita zaifliklari: buferning to‘lib toshishi, osma (Dandling) ko‘rsatkich, kod ineksiyasi, veb ilovalardagi XSS (Cross-site scripting), SQL ineksiya, nazoratlanmagan formatdagi qatorlar (Uncontrolled Format String), OT buyruqlari ineksiyasi (OS Command Injection), Time-of-check-to-time-of-use (TOCTOU).

6-mavzu. Dasturiy vositalarda zaifliklar turlari va tasnifi.

OWASP tashkiloti e’lon qilgan zaifliklar tasnifi va ularga qarshi himoya choralari.

7-mavzu. Tahdidlarni tasniflash.

Tahdidlarni tasniflash. STRIDE metodologiyasi. Tahdidlarni modellashtirish. Threat Modelling Tool vositasi.

8-mavzu. Xavfsiz dasturlash tillari.

Dasturlash tillariga asoslangan xavfsizlik, xavfsiz va xavfsiz bo‘lmagan dasturlash tillari, dasturlash tillarining xavfsizlikni ta’minlashdagi imkoniyatlari, xotira xavfsizligi, tiplar xavfsizligi, foydalanishlarni nazoratlash, o‘zgaruvchilarni o‘zgarmastlik imkoniyatlari.

9-mavzu. Quyi (C++) dasturlash tilining xavfsizlik imkoniyatlari.

Xavfsiz va xavfsiz bo‘lmagan funksiyalar. C++ tilida xavfsiz kod yozish uslublari.

10-mavzu. Yuqori (C#) dasturlash tilining xavfsizlik imkoniyatlari.

Imtiyoz tushunchasi va turlari. Autentifikatsiya, ma’lumot va kodlarni boshqarishdagi xavfsizlik. S# tilida xavfsiz kod yozish uslublari.

11-mavzu. Sandboxing (qumli quti).

Ajratish (izolyatsiyalash, qumli quti). Klassik operatsion tizimlarda foydalanishlarni nazoratlash. Dasturlash tillariga asoslangan foydalanishlarni nazoratlash. Dasturlash tillarida mavjud xavfsizlik siyosati va imtiyozlar.

12-mavzu. Axborotni sirqib chiqishi.

Axborotni sirqib chiqishi, konfidensiallik & yaxlitlik. Axborotni tasniflash usullari (NATO va Beniluks davlatlari tasnifi). Yashirish va aniq axborotni sirqib chiqishi. Dasturiy vositalarda axborotni sirqib chiqishini oldini olish usullari.

13-mavzu. Dasturiy vosita kodini yozish.

Dasturlash tillari. Mos dasturlash tilini tanlash. Dasturiy kodlarni shakllantirish bo‘yicha standartlar. Kodlashda beriladigan tavsiyalar: nomlash shartlari, formatlash talablari, kod strukturasi, kommentariya qo‘yish tartibi, xatoliklarni tutish va ularga javob berish.

14-mavzu. Dasturiy vositalarning statik tahlili.

Dasturiy vositani statik tahlillash, uning maqsadi va vazifasi. MISRA standarti. ISO 26262: ASIL standarti. Statik tahlillashning afzalliklari.

15-mavzu. Dasturiy vositalarning statik tahlillash vositalari.

Statik tahlillash vositalari: Helix QAC, Klocwork. Statik tahlillashni amalga oshirish tartibi.

16-mavzu. Dasturiy vositalarni xavfsizlikka testlash.

Dasturiy vositalarning xavfsizligini testlash, testlashdan maqsad, testlash prinsiplari, testlash usullari: zaiflikni aniqlash, suqilib kirish testlari, xavfsizlikni skanerlash, xavfsizlik auditi, risklarni baholash. Dasturiy vositalar vazifasini bajarishini testlash usullari: oq, kulrang va qora quti.

17-mavzu. Dasturiy vositalarni foydalanishga tayyorlash.

Dasturiy vositani foydalanishga tayyorlash, uning asosiy bosqichlari (versiya, o‘rnatish, aktivlashtirish, o‘chirib tashlash, yangilash, versiyani kuzatib borish), dasturiy vositani foydlanishga tayyorlash vositalari. Dasturiy vositani chiqarish jarayoni. Dasturiy vositalarni foydalanishga tayyorlashning asosiy bosqichlari.

III. Amaliy mashg‘ulotlar bo‘yicha ko‘rsatma va tavsiyalar

Amaliy mashg’ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Dasturiy vositalarni ishlab chiqarishning hayotiy siklini amaliy tadbiqi.
2. Dasturiy vositalar uchun talablarni shakllantirish va loyihalashni amalga oshirish.
3. OWASP WebGoat simulyatorida SQL inektsiya tahdidini amalga oshirish.

	4. Microsoft Threat Modeling Tools yordamida tahdidlarni modellashtirish. 5. C++ dasturlash tilida to‘g‘ri kod yozish va kirish qiymatini tekshirishni amalga oshirish. 6. Faylni qulflash va yangi yaratilgan faylga foydalanishni cheklashni amalga oshirish. 7. Helix QAC va SonarQube yordamida statik testlashni amalga oshirish. 8. OWASP ZAP dasturi yordamida tizimni xavfsizlikka testlash. 9. Inno Setup Compiler vositasi yordamida loyihalarni foydalanishga tayyorlash. **IV. Mustaqil ta’lim va mustaqil ishlar** *Mustaqil ta’lim uchun tavsiya etiladigan tapshiriqlar:* *Quyidagi mavzulardan ikkitasi bo‘yicha mustaqil ish tayyorlanadi va topshiriladi:* 1. C++ dasturlash tilida xotirani to‘lib toshish tahdidi va undan himoyalanish usullari. 2. SQL ineksiya tahdidi va undan himoyalanish usullari. 3. XSS tahdidi va undan himoyalanish usullari. 4. C/C++ dasturlash tilida ko‘rsatkichlar bilan bog‘liq muammolar. 5. Java dasturlash tilida kod yozish qoidalari. 6. FindBugs vositasi yordamida Java kodidan baglarni aniqlash. 7. Java dasturlash tilida mavjud imtiyoz turlari va ulardan foydalanish. 8. Xavfsiz dasturiy vositalarni yaratishning dolzarbiligi va undagi muammolar. 9. Dasturiy vositalarda xavfsizlikni ta’minlashda kriptografik himoya usullaridan foydalanish. 10. OWASP tashkilot va uning faoliyat turi. 11. Statik tahlillash vositalarining qiyosiy tahlili. 12. Dasturiy vositalar xavfsizligiga oid so‘ngi statistik ma’lumotlar tahlili. *Quyidagi mavzulardan biri bo‘yicha taqdimot materiali tayyorlanadi va topshiriladi:* 1. Mobil ilova uchun barmoq izi asosida foydalanishga ruxsat berishni amalga oshirish. 2. Mijoz-serser arxitekturasiga asoslangan messenjer yaratish. 3. Mobil qurilmalar uchun eslatmalarni qaydlash ilovasini yaratish. 4. Mobil qurilmalar uchun fayllarni shifrlagan holda saqlash ilovasini yaratish. 5. Mobil qurilmalar uchun tug‘ulgan kunlarni saqlovchi va eslatuvchi ilovani yaratish.
3.	**V. Fan o‘qitilishining natijalari (shakllanadigan kompetentsiyalar)** *Fanni o‘zlashtirish natijasida talaba:* • dasturiy vositalar xavfsizligini muhimligini va dasturiy vositalarni ishlab chiqarishning hayotiy siklini tushuntirib bera oladi; • dasturiy vositalarda mavjud xavfsizlik muammolarini aytib bera oladi; • dasturiy vositalarni yaratishda xavfsizlik talablariga e’tibor berish va xavfsiz dasturiy vositalarni hozirgi zamondagi o‘rni muhimligi haqida haqida tasavvurga ega bo‘lishi; • xavfsizlik talablariga mos holda dasturiy vositalarni yaratish ko‘nikmasiga ega bo‘ladi; • dasturiy vositalarni xavfsizlikka testlay oladi; • dasturiy vositalarni foydalanishga tayyorlay oladi.
4.	**VI. Ta’lim texnologiyalari va metodlari** • ma’ruzalar; • amaliy ishlarni bajarish va xulosalash; • interfaol keys-studylar; • blits-so‘rovi; • guruhlarda ishlash; • taqdimotlar tayyorlash; • jamoa bo‘lib ishlash va himoya qilish uchun loyihalar.
5.	**VII. Kreditlarni olish uchun talabalar:** Fanga oid nazariy va uslubiy tushunchalarni to‘la o‘zlashtirish, tahlil natijalarini to‘g‘ri aks ettira olish, o‘rganilayotgan jarayonlar haqida mustaqil mushohada yuritish va nazorat uchun berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo‘yicha yozma ishni yoki test topshirish.
6.	**Asosiy adabiyotlar** 1. S.K.Ganiyev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet. 2. S.K.Ganiyev, A. A.Ganiyev, Z.T.Xudoyqulov; Kiberxavsizlik asoslari: o'quv qo'llanma, -T.: “Nihol print” OK, 2021. – 224 b. 3. Q.S.Raxmanov, Sh.T.Kasimova; C++ tilida dasturlash: o'quv qo'llanma, - T.: Aloqachi, 2017. - 360 b. **Qo‘shimcha adabiyotlar** 1. Secure Programming in C. Lef Ioannidis. MIT EECS. January 5, 2014. 2. CERT C++ Secure Coding Standard. https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=637 3. M.Payer. Software Security: Principles, Policies, and Protection. HexHive Books, April, 2019, 0.35v., p.-130. 4. Secure Programming Cookbook for C and C++. Matt Messier, John Viega. O’Reilly publisher. July 2003. ISBN: 0-596-00394-3, pp. 784.
7.	Fan dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 2023-yil 30-avgustdagi 9(731)/1(732)-son bayonnomasi bilan tasdiqlangan.
8.	**Fan/modul uchun mas’ullar:** Z.T. Xudoykulov – Muhammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi mudiri I.S.Olimov – Muhammad al-Xorazmiy nomidagi TATU, “Kriptologiya” kafedrasi assistenti
9.	**Taqrizchilar:** O.A. Allanov – Muhammad al-Xorazmiy nomidagi TATU, “Kiberxavfsizlik va kriminalistika” kafedrasi mudiri, PhD N.B. Nasrullayev - Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali direktori, PhD, dotsent