Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədris məsələləri üzrə prorektor v.i.e:
dos. Zaur Məmmədov
"07" Yanvar 2026-cı il

FƏNN SİLLABUSU
(işçi tədris proqramı)

İxtisasın şifri və adı: 6006017 – İnformasiya təhlükəsizliyi
Fakültə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər

I.Fənn haqqında məlumat:
Fənnin adı: Veb təhlükəsizlik
Kodu: İPF-B10
Tədris ili: 2025/2026
Semestr: II (Yaz)
Tədris yükü: 45 (30 saat mühazirə, 15 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 5 kredit

II. Müəllim haqqında məlumat:
Soyadı, adı, ata adı, elmi dərəcəsi və elmi adı:
Qədirov Nicat İdris oğlu, baş müəllim,
Salmanlı Salman Əliqulu oğlu, müəllim
Kafedranın ünvanı: Lənkəran şəhəri, Fizuli küçəsi, 170a, LDU-nun 1 saylı tədris binası
Məsləhət günləri və saatı: IV gün, saat:11^{00}-13^{00}
E-mail ünvanı:
Nicat Qədirov <nqadirov74@mail.ru>, <nqadirov74@gmail.com>
Salman Salmanli <salmansalmanli654@gmail.com>

III. Tövsiyə olunan dərslik, dərs vəsaiti və metodik vəsaitlər:
1. Hoffman, Andrew. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. N.p., O'Reilly Media, 2020.
2. Tomas Kormen. Alqoritmlərin Sirri (Azərbaycan). Altun Kitab, 2022.
3. Elie Saad, Rick Mitchell. OWASP Web Security Testing Guide, version 4.2.2020
4. OWASP Top Ten (https://owasp.org/ww-project-top-ten/)
5. Pinto, Marcus, and Stuttard, Dafydd. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. United Kingdom, Wiley, 2011.
6. İnternet.

XIII. Fənn üzrə təlim nəticələri:

Veb Təhlükəsizliyi kursunun təlim nəticələri nəzəri biliklərə və praktik bacarıqlara bölünür. Kursu bitirdikdən sonra tələbələr aşağıdakı bilik və bacarıqlara yiyələnməlidirlər.

1. Nəzəri biliklər:

– Əsas təhlükəsizlik prinsipləri: Klassik CIA triadasını (Confidentiality, Integrity, and Availability - məxfilik, bütövlük, əlçatanlılıq) bilmək;

– Təhlükələrin təsnifatı: SQL inyeksiyası, XSS və CSRF kimi tipik zəifliklər (məsələn, OWASP Top 10 siyahısından) anlamaq;

– Arxitektura və protokollar: HTTP/HTTPS, brauzer təhlükəsizlik siyasətlərini və identifikasiya mexanizmlərini anlamaq.

2. Praktik bacarıqlar:

– Zəifliklərin təhlili: Vep proqramlarda təhlükəsizlik təhlili aparmaq, zəif cəhətləri müəyyən etmək və təhlükələri modelləşdirmək bacarığı;

– Təhlükəsiz proqramlaşdırma: Kodlaşdırma və sistem layihələndirilməsi zamanı risklərin azaldılması metodlarını tətbiq etmək;

– Proqram vasitələrindən istifadə: Təhlükəsizlik auditi və hücumların monitorinqi üçün ixtisaslaşmış proqram təminatından istifadəni bacarmaq;

– Təhlükələrə cavab: Təhdidləri lokallaşdırmaq və haker hücumlarının və ya məlumat sızmalarının nəticələrini azaltmaq bacarığı.

3. Kompitensiya:

– Veb resurslar üçün hərtərəfli informasiya təhlükəsizliyini təmin etmək bacarığı;

– Riskləri tənqidi qiymətləndirmək və resurs məhdudiyyətləri daxilində adekvat təhlükəsizlik tədbirləri seçmək bacarığı;

– Texniki riskləri müştərilərə və ya rəhbərliyə izah etmək üçün peşəkar ünsiyyət bacarıqları.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

_____

_____

_____

XV. Kollokvium sualları:

I kollokvium sualları (___ . ___ . 2026-cı il tarixlərində keçiriləcək):

1. Proqram təminatının qorunması tarixi – Eniqma
2. Proqram təminatının qorunması tarixi – Frikinq
3. Proqram təminatının qorunması tarixi - Kompüter sındırılmasının başlanğıcı
4. Müasir veb-proqramların strukturu – REST API
5. Müasir veb-proqramların strukturu – JSON formatı. JavaScript
6. Müasir veb-proqramların strukturu – Autentifikasiya və avtorizasiya
7. Müasir veb-proqramların strukturu – Veb Serverlər
8. Müasir veb-proqramların strukturu – Verilənlər bazası və kliyent tərəfdə verilənlərin saxlanılması
9. Proqramların arxitekturasında zəif yerlərin müəyyən edilməsi – Təhlükəli və təhlükəsiz arxitekturanın əlamətləri
10. Proqramların arxitekturasında zəif yerlərin müəyyən edilməsi – Təhlükəsizlik səviyyələri.

II kollokvium sualları (___ . ___ . 2026-cı il tarixlərində keçiriləcək):

1. Saytlar arası scriptinq (XSS - Cross-Site Scripting): Yadda Saxlanan XSS hücumları (Stored XSS)
2. Saytlar arası scriptinq (XSS - Cross-Site Scripting): Əks olunan XSS hücumları (Reflected XSS)
3. Saytlar arası scriptinq (XSS - Cross-Site Scripting): DOM əsasında XSS hücum (DOM-based XSS)
4. Saytlar arası sorğuların saxtalaşdirilması (CSRF - Cross-Site Request Forgery): Sorğu parametrlərinin saxtalaşdırılması
5. Saytlar arası sorğuların saxtalaşdirilması (CSRF - Cross-Site Request Forgery): GET sorğusunun məzmununun dəyişdirilməsi
6. XXE hücum (XML xarici qurumlarına (obyektlərə) hücum (XXE - XML External Entity)).
7. İnyeksiya (kodun yeridilməsi): SQL inyeksiyası
8. İnyeksiya (kodun yeridilməsi): kod inyeksiyası
9. Xidmətdən imtina (DoS – denial of service): ReDoS hücum (regular-expression-based DoS)
10. Xidmətdən imtina (DoS – denial of service): Paylanmış DoS hücumu (distributed denial of service, DDoS)

XVI. İmtahan sualları:

1. Proqram təminatının qorunması tarixi – Eniqma
2. Proqram təminatının qorunması tarixi – Frikinq
3. Proqram təminatının qorunması tarixi - Kompüter sındırılmasının başlanğıcı
4. Müasir veb-proqramların strukturu – REST API
5. Müasir veb-proqramların strukturu – JSON formatı. JavaScript
6. Müasir veb-proqramların strukturu – Autentifikasiya və avtorizasiya
7. Müasir veb-proqramların strukturu – Veb Serverlər
8. Müasir veb-proqramların strukturu – Verilənlər bazası və kliyent tərəfdə verilənlərin saxlanılması
9. Proqramların arxitekturasında zəif yerlərin müəyyən edilməsi – Təhlükəli və təhlükəsiz arxitekturanın əlamətləri
10. Proqramların arxitekturasında zəif yerlərin müəyyən edilməsi – Təhlükəsizlik səviyyələri.
11. Saytlar arası scriptinq (XSS - Cross-Site Scripting): XSS zəifliyinin aşkarlanması.
12. Saytlar arası scriptinq (XSS - Cross-Site Scripting): Yadda Saxlanan XSS hücumları (Stored XSS)
13. Saytlar arası scriptinq (XSS - Cross-Site Scripting): Əks olunan XSS hücumları (Reflected XSS)
14. Saytlar arası scriptinq (XSS - Cross-Site Scripting): DOM əsasında XSS hücum (DOM-based XSS)
15. Saytlar arası sorğuların saxtalaşdirilması (CSRF - Cross-Site Request Forgery): Sorğu parametrlərinin saxtalaşdırılması
16. Saytlar arası sorğuların saxtalaşdirilması (CSRF - Cross-Site Request Forgery): GET sorğusunun məzmununun dəyişdirilməsi

17. XXE hücum (XML xarici qurumlarına (obyektlərə)) hücum (XXE - XML External Entity)).
18. XXE hücum: Birbaşa hücum.
19. XXE hücum: Dolayı hücum.
20. İnyeksiya (kodun yeridilməsi).
21. İnyeksiya (kodun yeridilməsi): SQL inyeksiyası
22. İnyeksiya (kodun yeridilməsi): SQL inyeksiyası
23. İnyeksiya (kodun yeridilməsi): kod inyeksiyası
24. İnyeksiya (kodun yeridilməsi): əmr inyeksiyası
25. Xidmətdən imtina (DoS – denial of service)
26. Xidmətdən imtina (DoS – denial of service): ReDoS hücum (regular-expression-based DoS)
27. Xidmətdən imtina (DoS – denial of service): Məntiqi DoS zəifliklər
28. Xidmətdən imtina (DoS – denial of service): Paylanmış DoS hücumu (distributed denial of service, DDoS)
29. Müasir veb-proqramların müdafiəsinin təmin edilməsi
30. Müasir veb-proqramların müdafiəsinin təmin edilməsi.
31. Proqramların təhlükəsiz arxitekturası: Audentifikasiya və Avtorizasiya. SSL və TLS protokolları.
32. Proqramların təhlükəsiz arxitekturası: Hesabların qorunması. Hesabların xeşləşdirilməsi. İki faktorlu audentifikasiya.
33. XSS hücumlarına qarşı mübarizə: İstifadəçi daxiletməsinin təmizlənməsi, DOMParser, SVG, BLOB qəbulediciləri
34. XSS hücumlarına qarşı mübarizə: Hiperlink ssenarisi, HTML-də simvol obyektləri, CSS, Məzmun Təhlükəsizlik Siyasəti (Content Security Policy, CSP)
35. CSRF hücumlarına qarşı mübarizə: Başlıqların yoxlanılması.
36. CSRF hücumlarına qarşı mübarizə: Token.
37. XXE hücumlardan müdafiə.
38. SQL inyeksiyalarla mübarizə.
39. DoS hücumlara müqavimət (mübarizə): ReDos və məntiqi Dos hücumlarla mübarizə
40. DoS hücumlara müqavimət (mübarizə): DDos hücumlarla mübarizə.

"Veb təhlükəsizlik" fənninin sillabusu **6006017 - "İnformasiya təhlükəsizliyi"** ixtisasının təhsil proqramı, tədris planı əsasında tərtib edilmişdir.

Sillabus **"Texnologiya və texniki fənlər"** kafedrasında müzakirə edilərək təsdiq edilmişdir (07.01.2026-cı il, protokol № 1).

Fənn müəllimi: **b.m. N.İ. Qədirov**
m. S.Ə. Salmanlı

Kafedra müdiri: **dos. R.F. Əliyev**