

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

**MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY
UNIVERSITETINING JIZZAX FILIALI**



KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI
mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami
2026-yil 25-26-sentabr

(1-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to'plami – Jizzax: O'zMU Jizzax filiali, 2026-yil 25-26-sentabr. 507-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globalashuv sharoitida davlatimizni yanada barqaror va jadal sur'atlar bilan rivojlantirish bo'yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e'tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma'ruza tezislari to'plamida mamlakatimiz va xorijlik turli yo'nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o'qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas'ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay'ati a'zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., t.f.f.d.(PhD), dots. Abdumalikov A.A., p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O'ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo'rayev M.M.

Mazkur to'plamga kiritilgan ma'ruza tezislarining mazmuni, undagi statistik ma'lumotlar va me'yoriy hujjatlarning to'g'riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o'zlari mas'uldirlar.

4. Latkowski, T. & Osowski, S. Data mining for feature selection in gene expression autism data // Expert Systems with Applications 42, (2015). – pp. 864 – 872.
5. Li, J. & Liu, H. Challenges of Feature Selection for Big Data Analytics//IEEE Intelligent Systems 32, (2017). – pp. 9 – 15.
6. Liu, C., Wang, W., Zhao, Q., Shen, X. & Konan, M. A new feature selection method based on a validity index of feature кичм тўплам. Pattern Recognition Letters 92, (2017). – pp. 1 – 8.
7. Mokshin V. V., et al. “Parallel Genetic Algorithm of Feature Selection for Complex System Analysis”, Journal of Physics: Conf. Series 1096 (2018) 012089. – pp. 1 – 11.
8. Mirzaev N.M., Khaydarova M.Yu., Mirzaeva G.R., Ibragimova S.N. Models of recognition algorithms for objects described in the large dimensional feature space // Journal of Physics: Conf. Series–London, vol:1210, 2019. – pp.1 – 8.
9. Majdi Mafarja, Seyedali Mirjalili. Hybrid binary ant lion optimizer with rough set and approximate entropy reducts for feature selection // Soft Computing, vol: 23 (15), 2019. – pp. 4 – 20.
10. Nyararai Mlambo, Wilson K. Cheruiyot, Michael W. Kimwele. A Survey and Comparative Study of Filter and Wrapper Feature Selection Techniques// The International Journal Of Engineering And Science (IJES).Vol. 5, Issue 8. 2016. – pp. 57 – 67.

WEB-ILOVALARDA UCHRAYDIGAN XAVFLARNI (SQL INJECTION, XSS) ANIQLASH VA OLDINI OLISHNING AVTOMATLASHTIRILGAN USULLARI

Mamaraimov Abror Kamalidin o‘g‘li

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti Jizzax filiali

mamaraimovabror@gmail.com

Ziyotov Suhrobbek Ulug‘bek o‘g‘li

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti Jizzax filiali

Ziyatovsuhrob786@gmail.com

Jozilov Jobir Ochil o‘g‘li

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy Universiteti Jizzax filiali

jobborjozilov@gmail.com

Annotatsiya: Ushbu maqolada web-ilovalarda eng ko‘p uchraydigan ikki turdagi zaiflik — SQL Injection (SQL in’ektsiyasi) va Cross-Site Scripting (XSS) hujumlarining tabiati, ularni aniqlashning an’anaviy va zamonaviy avtomatlashtirilgan (jumladan, mashinali o‘rganish va chuqur o‘rganishga asoslangan) usullari, shuningdek amaliyotda qo‘llaniladigan oldini olish mexanizmlari tahlil qilingan. Maqolada statik va dinamik xavfsizlik testlash vositalari (SAST/DAST), signaturaga asoslangan va anomaliyaga asoslangan

tizimlar, neyron tarmoqlar (LSTM, CNN, BERT asosidagi modellar) yordamida aniqlash yondashuvlari qiyosiy tarzda ko‘rib chiqilgan.

Kalit so‘zlar: web-ilovalar xavfsizligi, SQL Injection, Cross-Site Scripting (XSS), mashinali o‘rganish, chuqur o‘rganish, Web Application Firewall (WAF), OWASP, statik va dinamik tahlil, kiberxavfsizlik.

Kirish

Zamonaviy raqamli iqtisodiyot va davlat xizmatlarining katta qismi web-ilovalar orqali amalga oshirilmoqda, bu esa ularning xavfsizligini kiberxavfsizlikning ustuvor yo‘nalishlaridan biriga aylantirmoqda. OWASP tashkilotining tahlillariga ko‘ra, in'ektsiya turidagi hujumlar (shu jumladan SQL Injection) va Cross-Site Scripting veb-ilovalarga qarshi eng keng tarqalgan va eng xavfli hujum turlari qatoriga kiradi [1]. Bu hujumlar orqali tajovuzkorlar ma'lumotlar bazasidagi maxfiy ma'lumotlarni o‘g‘irlashi, foydalanuvchi seansini o‘g‘irlashi yoki zararli skriptlarni boshqa foydalanuvchilar brauzerida bajarishi mumkin.

Web-dasturlashda uchraydigan xavfsizlik tahdidlari va ularga qarshi himoya usullari OWASP tamoyillari asosida tahlil qilingan ishlarda XSS, SQL Injection va CSRF kabi zaifliklar keng tarqalgan xatoliklar sifatida ko‘rsatilgan [2]. Shu bilan birga, milliy tadqiqotlarda web-ilovalar zaifliklarini aniqlashda Burp Suite, OWASP ZAP, Arachni, Wapiti kabi statik va dinamik skanerlardan foydalanish samaradorligi alohida tahlil qilingan [3].

Mazkur maqolaning maqsadi — SQL Injection va XSS hujumlarini aniqlash hamda oldini olishning zamonaviy avtomatlashtirilgan usullarini tizimli tahlil qilish va amaliy tavsiyalar shakllantirishdan iborat.

1. SQL Injection va XSS hujumlarining tabiati

SQL Injection — foydalanuvchi kiritgan ma'lumotlar to‘g‘ri filtrlanmasdan SQL so‘roviga qo‘shilishi natijasida yuzaga keladigan zaiflik bo‘lib, u orqali tajovuzkor ma'lumotlar bazasiga ruxsatsiz kirishi, ma'lumotlarni o‘zgartirishi yoki o‘g‘irlashi mumkin [4]. Cross-Site Scripting (XSS) esa veb-sahifaga zararli JavaScript kodini kiritish orqali boshqa foydalanuvchilar brauzerida ushbu kodni bajartirishga asoslangan hujum turidir; u odatda uchta turga bo‘linadi — saqlanuvchi (stored), aks etuvchi (reflected) va DOM asosidagi XSS [5].

Ikkala hujum turi ham asosan kiritma ma'lumotlarni yetarlicha tekshirmaslik (input validation yetishmovchiligi) natijasida yuzaga keladi, shuning uchun ularni aniqlash va oldini olish usullarida ko‘p jihatdan o‘xshash yondashuvlar qo‘llaniladi [6].

2. Aniqlashning an'anaviy usullari

An'anaviy usullar ikki asosiy guruhga bo‘linadi:

- **Statik xavfsizlik testi (SAST)** — dastur manba kodini bajarilishidan oldin tahlil qilib, zaif joylarni aniqlaydi;
- **Dinamik xavfsizlik testi (DAST)** — ishlab turgan ilovaga real so‘rovlar yuborish orqali zaifliklarni amalda aniqlaydi.

O‘zbekistonlik tadqiqotchilar tomonidan o‘tkazilgan tajribada Arachni va OWASP ZAP kabi ochiq kodli skanerlar solishtirilgan bo‘lib, ular hujum qiluvchi

va himoyalanuvchi (victim) tugunlar o'rtasidagi tarmoqda benchmarking asosida sinovdan o'tkazilgan [3]. Shuningdek, sanoatda keng qo'llaniladigan SQLMap vositasi SQL in'ektsiya zaifliklarini avtomatik aniqlash va ulardan foydalanish jarayonini avtomatlashtiruvchi ochiq manbali penetratsion test vositasi sifatida qayd etiladi [7]. Bunday signaturaga asoslangan yondashuvlarning asosiy kamchiligi — ular oldindan ma'lum bo'lgan hujum naqshlariga (pattern) tayanishi, natijada yangi yoki o'zgartirilgan (obfuscated) hujum turlarini aniqlashda samaradorligi pasayishidir [8].

3. Mashinali va chuqur o'rganishga asoslangan avtomatlashtirilgan usullar

So'nggi yillarda SQL Injection va XSS'ni aniqlashda mashinali o'rganish (ML) va chuqur o'rganish (DL) usullari faol qo'llanilmoqda, chunki ular hujum naqshlarini oldindan bilmasdan ham anomaliyalarni statistik xususiyatlar asosida aniqlay oladi.

- **Neyron tarmoqlarga asoslangan modellar.** SIDNet nomli yondashuv SQL Injection hujumlarini aniqlash uchun maxsus ishlab chiqilgan neyron tarmoq arxitekturasiga bo'lib, kiberxavfsizlikni kuchaytirish maqsadida taklif etilgan [9]. Probabilistik neyron tarmoqlarga asoslangan boshqa tadqiqotda SQL Injection hujumlarini aniqlash samaradorligini oshirish ko'rsatilgan [10].

- **Kontekstli til modellari (BERT va boshqalar).** Kontekstlashtirilgan so'z joylashtirish (contextualized word embedding) texnologiyasidan foydalanib, SQL so'rovlarining semantik tuzilishini chuqurroq tahlil qilish orqali aniqlash aniqligini oshirish mumkinligi ko'rsatilgan [11].

- **E'tibor mexanizmlari (Attention).** Yengil vaznli ko'p boshli o'z-o'ziga e'tibor (multi-head self-attention) mexanizmiga asoslangan model SQL Injectionni real vaqt rejimida, kam hisoblash resursi bilan aniqlashga qaratilgan [12].

- **Birlashtirilgan (fusion) yondashuvlar.** UniEmbed nomli model bir vaqtning o'zida XSS va SQL Injection hujumlarini bir nechta xususiyatlarni birlashtirish (multiple feature fusion) orqali aniqlaydi, bunda ko'p qatlamli perseptron (MLP) klassifikatori eng yuqori natijani ko'rsatgan [13].

- **XSS uchun maxsus yondashuvlar.** Generativ sun'iy intellekt yordamida yaratilgan GenXSS nomli tizim WAF ichida XSS hujumlarini avtomatik aniqlash uchun mo'ljallangan bo'lib, generativ modellar yordamida yangi hujum variantlarini ham modellashtira oladi [14]. Shuningdek, XSS va SQLga qarshi chuqur o'rganishga asoslangan yaxlit himoya yondashuvi taklif qilingan tadqiqotlar ham mavjud [15].

- **Umumiy sharh.** Sun'iy intellekt imkoniyatlaridan foydalangan holda SQL in'ektsiyalari, XSS va CSRF hujumlarini aniqlash, oldini olish va ularga javob berish masalalari bo'yicha umumlantirilgan tahlil ham nashr etilgan [16], unda signaturaga asoslangan va ML-asosidagi WAF'larning qisqacha qiyosiy tahlili keltirilgan [17].

Ushbu usullarning umumiy afzalligi — ular noma'lum (zero-day) hujum variantlarini ham nisbatan yuqori aniqlik bilan aniqlay olishi, kamchiligi esa katta

hajmdagi sifatli o'qitish (training) ma'lumotlariga muhtojligi va soxta ijobiy (false positive) natijalar ehtimolidir [18].

4. Oldini olishning amaliy usullari

Aniqlash usullari bilan bir qatorda, zaifliklarning oldini olishning arxitektura darajasidagi choralari muhim ahamiyatga ega:

1. **Parametrlashtirilgan so'rovlar (prepared statements) va ORM** — foydalanuvchi kiritmasi SQL kodidan alohida uzatilishi orqali in'ektsiyaning oldi olinadi [4].

2. **Kiritma ma'lumotlarni tekshirish va tozalash (input validation/sanitization)** — oq ro'yxat (whitelist) asosida ruxsat etilgan belgilar va formatlarni belgilash.

3. **Chiqish ma'lumotlarini kodlash (output encoding)** — HTML, JavaScript va URL kontekstlarida chiqariladigan ma'lumotlarni to'g'ri kodlash orqali XSSning oldi olinadi [5].

4. **Kontent xavfsizligi siyosati (Content Security Policy, CSP)** — brauzerga faqat ishonchli manbalardan skript yuklashga ruxsat berish orqali XSS ta'sirini cheklash.

5. **Web-ilova xavfsizlik devori (WAF)** — signaturaga asoslangan yoki ML-asosidagi WAF'lar real vaqt rejimida shubhali so'rovlarni bloklaydi [17].

6. **Kam imtiyoz tamoyili (principle of least privilege)** — ma'lumotlar bazasi hisob yozuvlariga faqat zarur bo'lgan minimal huquqlarni berish.

7. **Muntazam avtomatlashtirilgan tekshiruv** — CI/CD jarayoniga SAST/DAST vositalarini integratsiya qilish orqali zaifliklarni ishlab chiqish bosqichidayoq aniqlash [3].

5. Kompleks yondashuv taklifi

Yuqoridagi tahlil shuni ko'rsatadiki, yagona usul (faqat WAF yoki faqat kod darajasidagi himoya) to'liq xavfsizlikni ta'minlay olmaydi. Shu sababli quyidagi ko'p qatlamli (defense-in-depth) arxitektura tavsiya etiladi:

- **1-qatlam:** xavfsiz dasturlash amaliyoti (parametrlashtirilgan so'rovlar, kodlash) — ishlab chiqish bosqichida;
- **2-qatlam:** CI/CD jarayonida avtomatlashtirilgan SAST/DAST skanerlash [3];
- **3-qatlam:** ishlab chiqarish muhitida ML-asosidagi WAF orqali real vaqtli monitoring va anomaliyalarni aniqlash [16];
- **4-qatlam:** log-fayllarni tahlil qilish va insidentlarga javob berish tizimi (SIEM bilan integratsiya).

Xulosa

SQL Injection va XSS hujumlari hozirgi kunda ham web-ilovalar xavfsizligiga eng katta tahdid solayotgan zaiflik turlaridan biri bo'lib qolmoqda. An'anaviy signaturaga asoslangan usullar tezkor va tushunarli bo'lsa-da, yangi va murakkablashtirilgan hujum turlarini aniqlashda yetarli emas. Mashinali va chuqur o'rganishga asoslangan zamonaviy usullar — xususan, kontekstli til modellari, e'tibor mexanizmlari va generativ yondashuvlar — aniqlash aniqligini sezilarli darajada oshirmoqda. Biroq eng samarali natijaga faqat aniqlash usullarini xavfsiz

dasturlash amaliyoti, arxitektura darajasidagi himoya choralari (WAF, CSP, parametrlashtirilgan so'rovlar) bilan uyg'unlashtirilgan ko'p qatlamli tizim orqaligina erishish mumkin. O'zbekistonda olib borilayotgan tadqiqotlar ham ushbu yo'nalishning milliy axborot xavfsizligi strategiyasi doirasida dolzarbligini tasdiqlaydi [2, 3].

Foydalanilgan adabiyotlar

1. OWASP Foundation. OWASP Top 10 – 2021: The Ten Most Critical Web Application Security Risks. — <https://owasp.org/Top10/>
2. Veb dasturlashda xavfsizlik masalalari va himoyalash usullari // Zenodo, 2025. DOI: 10.5281/zenodo.15623537
3. Web ilova zaifliklarini aniqlash // "Pedagog" respublika ilmiy jurnali, 6-tom, 2-son, 2023-yil, 15-fevral. <https://bestpublication.org/index.php/pedg/article/view/3786>
4. Paul A., Sharma V., Olukoya O. SQL injection attack: Detection, prioritization & prevention // Journal of Information Security and Applications, 85 (2024), 103871.
5. Odeh A., Taleb A.A. XSSer: hybrid deep learning for enhanced cross-site scripting detection // Bulletin of Electrical Engineering and Informatics, 13(5), 2024, 3317–3325.
6. Nair S.S. Securing against advanced cyber threats: a comprehensive guide to phishing, XSS, and SQL injection defense // Journal of Computer Science and Technology Studies, 6(1), 2024, 76–93.
7. DarkMap: SQL in'ektsiya kamchiliklarini aniqlash va ulardan foydalanishni avtomatlashtiruvchi ochiq manbali vosita (sqlmap tavsifi). — <https://github.com/Darkfile-beka/DarkMap>

KO'P DARAJALI TA'LIM BOSHQARUV TIZIMLARIDA SUN'IY INTELLEKT IMKONIYATLARI VA XAVFSIZLIK

Axmedov Juraboy Raxmonberdiyevich

O'zbekiston Milliy universitetining Jizzax filiali Axborot tizimlari va texnologiyalari kafedrası professori v.b, pedagogika fanlari doktori (DSc)

Nurmamatov Mirzabek O'roqboy o'g'li

Email:taa@jbnuu.uz

Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti Jizzax filiali magistranti

Annotatsiya: Mazkur maqolada maktab kutubxonalarini raqamlashtirish jarayonida sun'iy intellekt va axborot xavfsizligi masalalarining o'zaro bog'liqligi tahlil qilinadi. Tadqiqotda Lib-Edu.uz platformasi misolida ko'p darajali boshqaruv tizimlarida sun'iy intellekt elementlarini qo'llash istiqbollari va shu bilan birga yuzaga keladigan axborot xavfsizligi xatarlari ko'rib chiqiladi. Maqolada ta'lim muassasalari uchun mo'ljallangan veb-platformalarda ma'lumotlar maxfiyligi, autentifikatsiya, avtorizatsiya va kriptografik himoya usullarining ahamiyati