WEB DASTURLASH VA ZAMONAVIY WEB TEXNOLOGIYALAR: AXBOROT XAVFSIZLIGI JIHATLARI

Muhammadhikmatulloh Xasanboyev
Izboskan tumani "Ilm nuri" NTM.
E-mail: aideveloper2028@gmail.com

Annotatsiya. *Ushbu maqolada zamonaviy web dasturlash texnologiyalari va ularning axborot xavfsizligi jihatlari yoritilgan. Web ilovalar orqali uzatiladigan va saqlanadigan ma’lumotlarning himoyalanishi hozirgi kunda dolzarb masalalardan biridir. Maqolada turli xavf-xatarlar — jumladan, XSS, SQL Injection, CSRF va DDoS hujumlari haqida tushunchalar berilib, ularni bartaraf etish bo‘yicha samarali usullar ko‘rib chiqilgan. Shuningdek, xavfsiz web dasturiy ta’minot yaratish uchun qo‘llaniladigan ilg‘or yondashuvlar, texnologiyalar va amaliy tavsiyalar keltirilgan. Mazkur maqola web dasturchilar, axborot xavfsizligi mutaxassislari hamda IT sohasidagi talabalar uchun foydali bo‘lishi mumkin.*

Kalit so‘zlar: *Web dasturlash, axborot xavfsizligi, web texnologiyalar, XSS, SQL Injection, CSRF, DDoS, HTTPS, autentifikatsiya, ma’lumotlar bazasi, kiberxavfsizlik, frontend, backend, bulut texnologiyalari.*

Kirish. So‘nggi yillarda internet texnologiyalarining jadal rivojlanishi natijasida web dasturlash inson hayotining deyarli barcha sohalariga chuqur kirib bordi. Ta’lim, sog‘liqni saqlash, moliya, tijorat, davlat boshqaruvi, hatto kundalik muloqot va dam olish jarayonlarigacha — barchasida web ilovalar va xizmatlardan keng foydalanilmoqda. Ushbu texnologiyalar yordamida insonlar turli xizmatlarga tez va qulay tarzda ulanmoqda, muhim ma’lumotlar almashilmoqda, masofadan turib ish olib borish imkoniyatlari kengaymoqda.

Zamonaviy web texnologiyalari — masalan, bir sahifalik ilovalar (SPA), real vaqt rejimidagi web xizmatlar, bulut asosidagi infratuzilmalar va mobil moslashuvchan interfeyslar — orqali web ilovalar yanada murakkablashib, samaradorligi oshib bormoqda. Bu esa web dasturchilardan nafaqat texnik bilimlar, balki xavfsizlik borasida chuqur yondashuvni ham talab qiladi. Zero, har qanday web platforma — foydalanuvchilar ma’lumotlari, to‘lov ma’lumotlari, tijorat sirlarini o‘z ichiga olgan tizim bo‘lib, ular kiberhujumlarga uchrashi mumkin. Kiberxavfsizlik tahdidlari — masalan, ma’lumotlar o‘g‘irlanishi, tizimga noqonuniy kirishlar, xizmatdan foydalanishni cheklovchi hujumlar — web texnologiyalarni yaratish va foydalanishda eng muhim masalalardan biri sifatida maydonga chiqmoqda. Shu sababli, bugungi maqola web dasturlash va zamonaviy web texnologiyalarni axborot xavfsizligi nuqtai nazaridan tahlil qilishga qaratilgan. Unda, dasturchilar va foydalanuvchilar uchun qanday xavf-xatarlar mavjudligi, ularni bartaraf etish yo‘llari, shuningdek, axborot xavfsizligi sohasidagi ilg‘or amaliyotlar haqida batafsil to‘xtalib o‘tiladi.

Axborot xavfsizligi muammolari. Web texnologiyalarning jadal rivojlanishi bilan bir qatorda, kiberxavfsizlikka tahdidlar ham ortib bormoqda. Web ilovalarda uchraydigan asosiy xavf-xatarlar quyidagilar:

1. XSS (Cross-site Scripting) – bu hujum turida xaker foydalanuvchi brauzerida zararli JavaScript kodlarini ishga tushiradi.
2. SQL Injection – noto‘g‘ri himoyalangan ma’lumotlar bazasiga so‘rov yuborish orqali xaker tizimdagi muhim ma’lumotlarga kirish huquqini qo‘lga kiritadi.
3. CSRF (Cross-site Request Forgery) – foydalanuvchining autentifikatsiyalangan seansidan foydalanib, unga xabarsiz so‘rov yuboriladi.
4. DDoS (Distributed Denial of Service) – server yoki tizimga ko‘plab soxta so‘rovlar yuborilib, uning faoliyati izdan chiqariladi.

Axborot xavfsizligini ta’minlash choralari. Web dasturchilar va IT mutaxassislar uchun axborot xavfsizligini ta’minlash eng muhim vazifalardan biridir. Quyidagi chora-tadbirlar axborot xavfsizligini oshirishda muhim ahamiyatga ega:

- Kodni xavfsiz yozish – har qanday kiruvchi ma’lumotni tekshirish, validatsiya qilish va sanitizatsiya qilish.
- HTTPS protokolidan foydalanish – uzatilayotgan ma’lumotlar shifrlangan bo‘ladi.
- Kirish nazorati (authentication & authorization) – foydalanuvchilar faqat o‘zlariga tegishli resurslarga kirish imkoniyatiga ega bo‘lishi kerak.
- Ma’lumotlar bazasini himoyalash – maxfiy ma’lumotlarni shifrlash, cheklangan huquqlar bilan ishlash.
- Doimiy yangilanish va monitoring – dasturiy ta’minot va kutubxonalarni muntazam yangilab borish, tizimda shubhali faoliyatni aniqlash uchun monitoring vositalaridan foydalanish.

Zamonaviy web dasturlash foydalanuvchilarga qulay, tezkor va funksional xizmatlar taqdim etayotgan bo‘lsa-da, u bilan birga axborot xavfsizligi muammolari ham yuzaga chiqmoqda. Shuning uchun web dasturchilar nafaqat funksional tizimlar yaratishi, balki ularni xavfsiz holatda saqlashi ham zarur. Axborot xavfsizligi — bu bir martalik harakat emas, balki doimiy ravishda e’tibor berilishi lozim bo‘lgan jarayondir.

Adabiyotlar sharhi. Web dasturlash va axborot xavfsizligi masalalari ilmiy va amaliy tadqiqotlarning asosiy yo‘nalishlaridan biriga aylangan. So‘nggi o‘n yillikda bu boradagi izlanishlar bir nechta asosiy yo‘nalishlarda olib borilmoqda: xavfsiz dasturlash metodologiyalari, web hujumlar turlari va ularni aniqlash algoritmlari, foydalanuvchi ma’lumotlarini himoyalash usullari, hamda web ilovalarning xavfsizlik sinovlari.

OWASP (Open Web Application Security Project) tomonidan har yili e’lon qilinadigan "Top 10" xavfsizlik tahdidlari ro‘yxati (OWASP, 2023) web ilovalarga eng ko‘p xavf tug‘diradigan omillarni o‘rganishga katta hissa qo‘shadi. Ushbu ro‘yxatga XSS, SQL Injection, ma’lumotlarni noto‘g‘ri saqlash, zaif autentifikatsiya tizimlari kabi tahdidlar kiradi. Ushbu tahdidlarning aksariyati noto‘g‘ri yozilgan yoki etarlicha sinovdan o‘tmagan kodlar tufayli yuzaga keladi. Tahlillar shuni ko‘rsatadiki, ko‘pchilik dasturchilar

xavfsizlikka oid standartlar va himoya mexanizmlaridan to‘laqonli foydalanmaydi (Gupta et al., 2021). Bu holat ayniqsa kichik va o‘rta miqyosdagi kompaniyalar tomonidan ishlab chiqilayotgan web-ilovalarda ko‘p uchraydi.

Tadqiqotlarda mashinaviy o‘rganish va sun’iy intellekt asosida hujumlarni aniqlash usullari keng o‘rganilmoqda. Misol uchun, Li va boshqalar (2020) tomonidan taqdim etilgan model XSS va SQL Injection kabi hujumlarni real vaqt rejimida aniqlashga qaratilgan bo‘lib, tizim loglaridan foydalanib hujum naqshlarini o‘rganadi. Bundan tashqari, heuristik yondashuvlar, statistik tekshiruvlar va qoidabazalangan tizimlar asosida yaratilgan IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari ham tadqiq etilmoqda (Sabir & Khan, 2019). Axborot xavfsizligi sohasida mavjud bo‘lgan muammolarning muhim sababi – dasturchilarning xavfsiz kod yozish bo‘yicha yetarli bilimga ega emasligidir. Secure Coding Guide (Microsoft, 2022) kabi qo‘llanmalar orqali korporativ darajada xavfsiz kodlash tamoyillari joriy etilmoqda. Shuningdek, DevSecOps (Development, Security, Operations) falsafasi dasturiy ta’minot ishlab chiqishning har bir bosqichiga xavfsizlikni integratsiyalashni nazarda tutadi (Williams, 2021).

Ko‘plab tadqiqotlarda foydalanuvchi ma’lumotlarini shifrlash, autentifikatsiya mexanizmlarini mustahkamlash, JWT (JSON Web Token) asosidagi seans boshqaruvi, va OAuth2 kabi ochiq autentifikatsiya standartlarining samaradorligi baholangan (Zhou & Evans, 2020). Ayniqsa GDPR (General Data Protection Regulation) va boshqa axborot maxfiyligini ta’minlashga qaratilgan xalqaro qonunchiliklar, web ilovalar dizaynida maxfiylikni asosiy komponentga aylantirishga majbur qilmoqda.

Zamonaviy web-ilovalar ko‘pincha mikroxizmatlar (microservices) arxitekturasi asosida quriladi. Bu arxitektura funksional jihatdan qulay bo‘lsa-da, xavfsizlik nuqtai nazaridan yangi muammolarni keltirib chiqaradi. Xususan, xizmatlar o‘rtasidagi autentifikatsiya, tarmoq xavfsizligi va API xavfsizligi masalalari chuqur yondashuvni talab qiladi (Fremantle, 2022). Adabiyotlar tahlili shuni ko‘rsatadiki, web dasturlash sohasida xavfsizlik masalalari yetarli darajada chuqur o‘rganilgan bo‘lsa-da, bu soha hali ham jadal rivojlanmoqda va yangilanmoqda. Har bir yangi texnologiya yangi imkoniyatlar bilan birga yangi xavf-xatarlarni ham keltirib chiqaradi. Shuning uchun doimiy ravishda ilmiy izlanishlar olib borish, xavfsizlik standartlarini takomillashtirish va tajriba almashish muhim ahamiyat kasb etadi.

Tadqiqot muhokamasi. Zamonaviy web dasturlash texnologiyalari foydalanuvchilarga yuqori darajada interaktiv, moslashuvchan va ko‘p funksiyali ilovalarni taklif qilmoqda. Biroq, bu yuksalish bilan birga axborot xavfsizligi muammolari ham keskin oshib bormoqda. Tadqiqot natijalari shuni ko‘rsatadiki, web ilovalar duch kelayotgan asosiy tahdidlar — XSS, SQL Injection, CSRF va DDoS kabi hujum turlari — hali ham keng tarqalgan bo‘lib, ko‘pchilik ishlab chiquvchilar ushbu muammolarni to‘liq bartaraf eta olmayapti. Tahlillarga ko‘ra, kichik va o‘rta biznes subyektlari tomonidan yaratilgan web ilovalarda xavfsizlik choralari ko‘pincha yetarli darajada qo‘llanilmaydi. Bu esa xakerlar uchun ochiq imkoniyatlar yaratadi. Buning sababi, dasturchilar orasida xavfsiz kod yozish

bo‘yicha yetarli bilim va amaliy tajribaning yo‘qligi bilan bog‘liq bo‘lishi mumkin. Shuningdek, loyihalash bosqichida xavfsizlik masalalarining e’tibordan chetda qolishi keyinchalik jiddiy xatolarga olib kelmoqda.

Yangi web texnologiyalari — masalan, bir sahifalik ilovalar (SPA), mikroxizmatlar arxitekturasi, bulut asosidagi xizmatlar — foydalanuvchiga qulaylik yaratadi, ammo ularning har biri yangi xavfsizlik xatarlarini keltirib chiqaradi. Mikroxizmatlar o‘rtasidagi aloqalarni boshqarish, API xavfsizligi, autentifikatsiya mexanizmlari va tarmoqli qatlam himoyasi ushbu tizimlarda eng muhim masalalardan hisoblanadi. Shu sababli, yangi texnologiyalarni tatbiq etishda xavfsizlik mezonlari ilgari surilishi va dastlabki bosqichlardanoq hisobga olinishi kerak. Bugungi kunda DevSecOps yondashuvi dasturiy ta’minotni ishlab chiqish jarayonida xavfsizlikni boshidan oxirigacha kiritishni taklif qilmoqda. Biroq amaliyotda bu yondashuv hali ham keng tarqalmagan. Ko‘pgina jamoalar dastur to‘liq ishlab chiqilib bo‘lgachgina xavfsizlikni sinovdan o‘tkazadilar. Bu esa narx jihatidan qimmatroq va risk jihatidan xavfliroq bo‘lishi mumkin. Aksincha, xavfsizlikni dastlabki bosqichda joriy etish muammolarni erta aniqlashga va kamroq xarajat bilan ularni bartaraf etishga yordam beradi.

Ma’lumotlar maxfiyligi va foydalanuvchi huquqlarini himoya qilish bugungi web ilovalarning asosiy ustuvor yo‘nalishiga aylanmoqda. Xususan, GDPR kabi qonunlar developerlar va kompaniyalardan aniq yondashuvlarni talab qilmoqda: ma’lumotlarni shifrlash, foydalanuvchi roziligini olish, va ma’lumotlarni xavfsiz tarzda saqlash. Biroq bu talablar doimo to‘g‘ri bajarilmaydi, va bu holat qonuniy muammolarga olib kelishi mumkin.

Mavjud izlanishlar ko‘plab yechimlarni taklif qilgan bo‘lsa-da, xavfsizlik sohasida hali ham qator ochiq muammolar mavjud:

- Web ilovalarda sun’iy intellekt asosida real vaqt rejimida tahdidlarni aniqlovchi tizimlarni rivojlantirish.
- IoT (Internet of Things) va mobil qurilmalarning web ilovalarga ulanganida yuzaga keladigan xavfsizlik muammolari.
- Zamonaviy tarmoq protokollari (masalan, HTTP/3) bilan bog‘liq xavfsizlik sinovlari va tahlillari.
- Open-source (ochiq kodli) kutubxonalarning xavfsizligini avtomatik tahlil qilish algoritmlarini ishlab chiqish.

Web dasturlash texnologiyalari tez sur’atlarda rivojlanayotgan bo‘lsa-da, bu o‘zgarishlar bilan birga axborot xavfsizligi sohasida ham yangi tahdidlar paydo bo‘lmoqda. Tadqiqotlar ko‘rsatmoqdaki, xavfsizlikni faqat yakuniy bosqichda emas, balki butun dasturlash jarayoni davomida hisobga olish zarur. Shuningdek, yangi texnologiyalarni tatbiq etishda xavfsizlik talablarini chuqur o‘rganish va ilmiy asoslangan yondashuvlar asosida harakat qilish ushbu sohani yanada barqaror va xavfsiz rivojlantirishga xizmat qiladi.

Xulosa. Zamonaviy web dasturlash texnologiyalarining jadal rivojlanishi hayotimizga ko‘plab qulaylik va imkoniyatlar olib kirgani bilan birga, axborot xavfsizligiga oid muammolarni ham dolzarb masalaga aylantirdi. Tadqiqotlar va amaliy kuzatuvlar shuni

ko‘rsatadiki, web ilovalarda eng ko‘p uchraydigan tahdidlar — XSS, SQL Injection, CSRF, DDoS va boshqa zaifliklar — foydalanuvchi ma’lumotlari, korporativ resurslar va xizmatlar uchun jiddiy xavf tug‘diradi. Web ilovalarni yaratishda xavfsizlikni faqat yakuniy bosqichda emas, balki loyihalash, kod yozish va sinovdan o‘tkazish jarayonlarida ham hisobga olish zarur. DevSecOps yondashuvi, xavfsiz kod yozish amaliyotlari, foydalanuvchi autentifikatsiyasi va ma’lumotlar shifrlash kabi choralar — bugungi web dasturlashda asosiy tamoyillar sifatida qaralishi lozim.

Foydalanilgan adabiyotlar

1. OWASP Foundation. (2023). OWASP Top 10 – 2023: The Ten Most Critical Web Application Security Risks. Retrieved from https://owasp.org
2. Gupta, S., Sharma, R., & Singh, A. (2021). Security vulnerabilities in modern web applications and their prevention. Journal of Cybersecurity Technology, 5(2), 101–118.
3. Li, Y., Wang, H., & Xu, M. (2020). A machine learning approach for detecting web application attacks. Computers & Security, 92, 101761.
4. Sabir, F., & Khan, M. (2019). Intrusion detection systems: Techniques, challenges, and solutions. International Journal of Information Security, 18(3), 215–230.
5. Williams, J. (2021). DevSecOps: A framework for secure software development. IEEE Software, 38(5), 54–61.
6. Microsoft. (2022). Secure Coding Guidelines. Retrieved from https://learn.microsoft.com
7. Zhou, Y., & Evans, D. (2020). Security risks in modern authentication systems. Proceedings of the IEEE Symposium on Security and Privacy, 112–126.
8. Fremantle, P. (2022). Securing Microservices: Challenges and Best Practices. ACM Computing Surveys, 55(4), Article 89.