

GENERATIV SUN'IY INTELLEKT SHAROITIDA WEB-SESSIYA TOKENLARI XAVFSIZLIGINI TA'MINLASH, TAHDIDLAR VA HIMOYA MEXANIZMLARI

Umarov Shuxratjon Azizjonovich

FDTU dotsenti, fizika-matematika fanlari bo'yicha falsafa doktori (PHD)

Ahmadjonov Ahlidin Bahriddin o'g'li,

FDTU 1-bosqich magistranti

e-mail: ahmadjonov117@gmail.com

Anotatsiya. Ushbu maqolada generativ sun'iy intellekt rivojlanayotgan sharoitda web-sessiya tokenlari xavfsizligini ta'minlash masalalari tahlil qilinadi. Tadqiqot davomida session hijacking, XSS va CSRF kabi asosiy tahdidlar ko'rib chiqilib, ularning sun'iy intellekt vositalari yordamida yanada murakkablashib borayotgani asoslab beriladi. Shuningdek, tokenlarni himoyalashning zamonaviy usullari, jumladan, HTTPS protokoli, cookie parametrlarini sozlash, token rotatsiyasi va qo'shimcha autentifikatsiya mexanizmlari samaradorligi yoritiladi.

Kalit so'zlar: web-xavfsizlik, sessiya tokenlari, generativ sun'iy intellekt, XSS, CSRF, session hijacking, autentifikatsiya

KIRISH

Zamonaviy raqamli muhitda web-ilovalar kundalik hayotning ajralmas qismiga aylangan. Ushbu ilovalarda foydalanuvchilarni identifikatsiya qilish va ularning sessiyalarini boshqarish uchun sessiya tokenlaridan keng foydalaniladi. Biroq, axborot texnologiyalarining rivojlanishi, ayniqsa generativ sun'iy intellekt texnologiyalarining keng joriy etilishi kiberxavfsizlikka yangi tahdidlarni yuzaga keltirmoqda.

Generativ sun'iy intellekt tizimlari avtomatlashtirilgan hujumlarni amalga oshirish, zaifliklarni tez aniqlash va zararli kodlarni generatsiya qilish imkonini berib, an'anaviy xavfsizlik mexanizmlarini chetlab o'tishga xizmat qilmoqda. Shu sababli web-sessiya tokenlarini himoyalash masalasi yanada dolzarb ahamiyat kasb etmoqda.

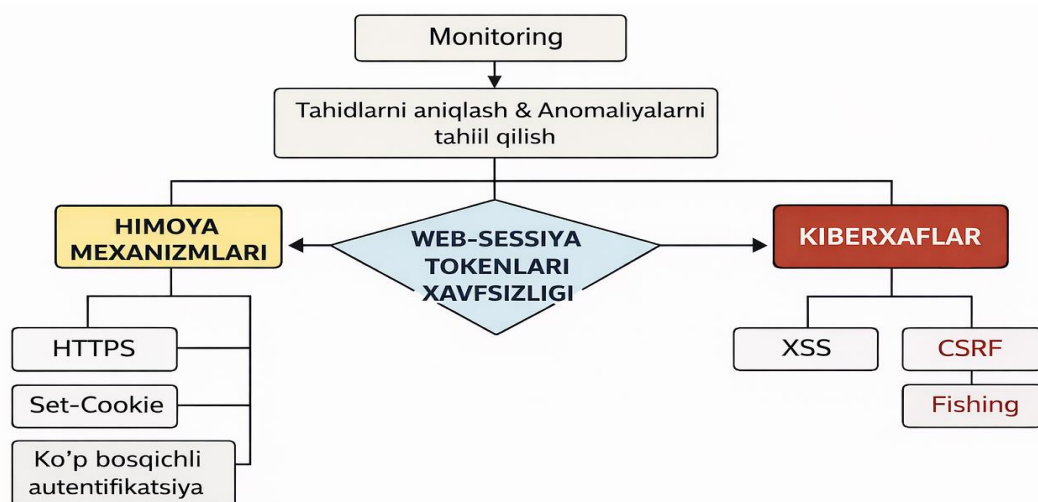
METODOLOGIYA

Mazkur tadqiqotda web-sessiya tokenlari xavfsizligini tahlil qilish uchun kompleks yondashuv qo'llanildi. Tadqiqot metodologiyasi nazariy tahlil, taqqoslash usuli va amaliy kuzatuv elementlarini o'z ichiga oladi.

Birinchi bosqichda web-ilovalarda sessiya tokenlaridan foydalanish mexanizmlari o'rganilib, ularning ishlash tamoyillari va zaifliklari tahlil qilindi. Shu bilan birga, session hijacking, XSS va CSRF kabi asosiy hujum turlari ilmiy manbalar asosida tahlil etildi.

Ikkinchi bosqichda generativ sun'iy intellekt texnologiyalarining kiberxavfsizlikka ta'siri o'rganildi. Xususan, AI yordamida hujumlarni avtomatlashtirish, zaifliklarni aniqlash va zararli skriptlar yaratish imkoniyatlari baholandi.

Uchinchi bosqichda mavjud himoya mexanizmlari HTTPS protokoli, cookie parametrlarini sozlash, token rotatsiyasi va ko'p bosqichli autentifikatsiya usullari tahlil qilinib, ularning samaradorligi solishtirildi. Tadqiqot davomida ochiq manbali ilmiy adabiyotlar, xalqaro standartlar (OWASP tavsiyalari) hamda zamonaviy kiberxavfsizlik hisobotlari asosiy manba sifatida foydalanildi.



1-rasm. Generativ AI sharoitida sessiya xavfsizligini boshqarish modeli

Mazkur model metodologik jihatdan web-xavfsizlikni o'rganishda tizimli yondashuvni aks ettiradi. Unda tahdidlar va himoya mexanizmlari o'zaro qarama-qarshi kuch sifatida tasvirlanib, generativ sun'iy intellektning ikki tomonlama ham himoya, ham xavf manbai sifatidagi roli ochib berilgan.

NATIJALAR

Tadqiqot natijalari shuni ko'rsatdiki, web-sessiya tokenlari xavfsizligi generativ sun'iy intellekt sharoitida sezilarli darajada yangi tahdidlarga duch kelmoqda. O'rganilgan ma'lumotlar asosida an'anaviy hujum turlari, jumladan session hijacking, XSS va CSRF, sun'iy intellekt vositalari yordamida yanada tezkor va samarali amalga oshirilishi mumkinligi aniqlandi.

Tahlillar natijasida aniqlanishicha, generativ AI tizimlari orqali avtomatlashtirilgan hujum skriptlarini yaratish imkoniyati mavjud bo'lib, bu esa web-ilovalardagi zaifliklarni qisqa vaqt ichida aniqlash va ekspluatatsiya qilishga olib keladi. Shu bilan birga, phishing hujumlarining aniqlik darajasi oshib, foydalanuvchilarni aldash ehtimoli sezilarli darajada yuqori ekanligi kuzatildi.

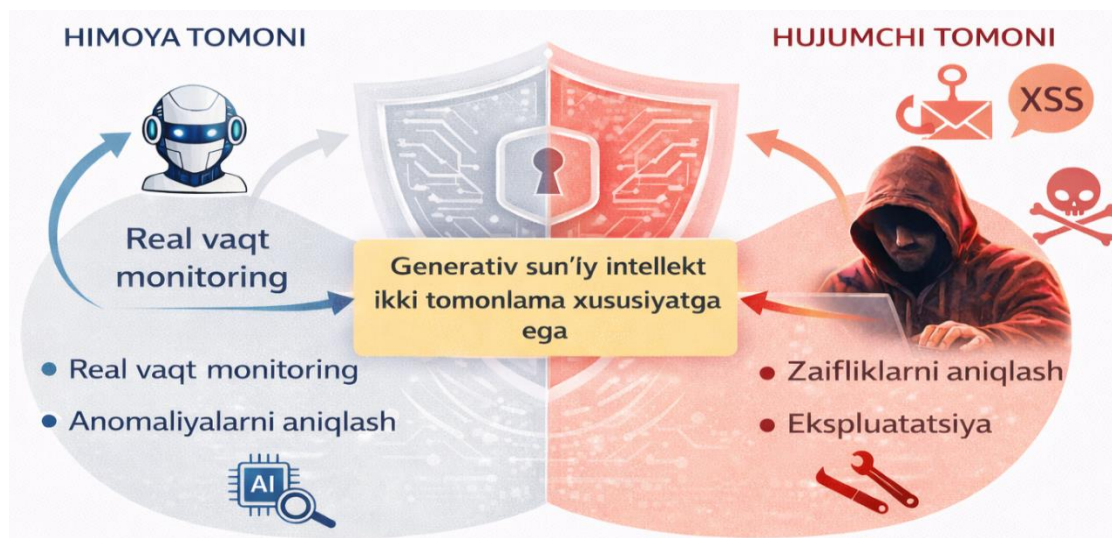
1-jadval. Web-sessiya tokenlari xavfsizligini ta'minlash usullari va ularning samaradorligi

№	Himoya mexanizmi	Tavsifi	Xavfsizlikka ta'siri
1	HTTPS protokoli	Ma'lumotlarni shifrlash orqali tarmoq orqali uzatishni himoyalaydi	Token o'g'irlanish xavfini sezilarli darajada kamaytiradi
2	Cookie parametrlarini sozlash	HttpOnly, Secure va SameSite atributlarini qo'llash	XSS va CSRF hujumlariga qarshi himoyani kuchaytiradi
3	Token rotatsiyasi	Sessiya tokenlarini muntazam yangilab borish	Token amal qilish muddatini qisqartirib xavfsizlikni oshiradi
4	Ko'p bosqichli autentifikatsiya (MFA)	Foydalanuvchini bir nechta bosqich orqali tekshirish	Qo'shimcha xavfsizlik qatlamini yaratadi
5	AI asosidagi monitoring tizimlari	Sun'iy intellekt yordamida anomaliyalarni aniqlash	Tahdidlarni erta aniqlash va tezkor javob berishni ta'minlaydi

Shuningdek, tadqiqot natijalari shuni ko'rsatdiki, alohida-alohida qo'llanilgan himoya mexanizmlari yetarli darajada samarali bo'lmasligi mumkin. Eng yuqori xavfsizlik darajasiga erishish uchun ularni kompleks holda qo'llash zarur.

Umuman olganda, olingan natijalar generativ sun'iy intellekt sharoitida web-sessiya tokenlarini himoyalash uchun an'anaviy yondashuvlarni takomillashtirish va yangi, AI asosidagi xavfsizlik mexanizmlarini joriy etish zarurligini tasdiqlaydi.

MUHOKAMA



2-rasm. Generativ sun'iy intellektning kiberxavfsizlikdagi ikki tomonlama xususiyati

Mazkur tadqiqot natijalari generativ sun'iy intellekt texnologiyalarining rivojlanishi web-sessiya tokenlari xavfsizligiga sezilarli ta'sir ko'rsatayotganini tasdiqlaydi. An'anaviy kiberxavfsizlik tahdidlari, jumladan session hijacking, XSS va CSRF hujumlari, AI vositalari yordamida yanada avtomatlashtirilgan va murakkab shaklga ega bo'lmoqda. Bu esa mavjud himoya mexanizmlarining samaradorligini qayta ko'rib chiqishni talab etadi. Tahlillar shuni ko'rsatadiki, generativ AI nafaqat hujumchilar uchun, balki himoya tizimlari uchun ham kuchli vosita hisoblanadi. Bir tomondan, AI yordamida zaifliklarni aniqlash va ekspluatatsiya qilish tezlashmoqda, boshqa tomondan esa, ayni texnologiyalar orqali real vaqt monitoring, anomaliyalarni aniqlash va xavfsizlikni kuchaytirish imkoniyati mavjud. Bu holat sun'iy intellektning "ikki tomonlama" xususiyatga ega ekanligini ko'rsatadi. Shuningdek, tadqiqot davomida aniqlanishicha, alohida qo'llanilgan himoya mexanizmlari yetarli darajada samarali emas. Masalan, faqat HTTPS protokolidan foydalanish yoki faqat cookie parametrlarini sozlash orqali barcha tahdidlarga qarshi to'liq himoyani ta'minlab bo'lmaydi. Shu sababli, kompleks yondashuv ya'ni bir nechta himoya usullarini birgalikda qo'llash eng maqbul yechim sifatida namoyon bo'ladi.

Bundan tashqari, generativ sun'iy intellekt asosida amalga oshiriladigan hujumlarning tezkorligi va moslashuvchanligi an'anaviy xavfsizlik tizimlari uchun yangi muammolarni yuzaga keltirmoqda. Xususan, statik himoya mexanizmlari dinamik va o'zgaruvchan tahdidlarga qarshi yetarli darajada samarali bo'lmisligi mumkin. Shu bois, kelajakda adaptiv va o'z-o'zini o'rganadigan xavfsizlik tizimlarini ishlab chiqish dolzarb masala hisoblanadi.

Umuman olganda, muhokama natijalari web-sessiya tokenlari xavfsizligini ta'minlashda innovatsion yondashuvlarni joriy etish zarurligini ko'rsatadi. Xususan, generativ sun'iy intellektidan nafaqat tahdid manbai sifatida, balki samarali himoya vositasi sifatida foydalanish istiqbollari yuqori baholanadi.

XULOSA

Mazkur tadqiqot natijalari generativ sun'iy intellekt texnologiyalarining rivojlanishi web-sessiya tokenlari xavfsizligiga sezilarli ta'sir ko'rsatayotganini ko'rsatdi. An'anaviy tahdidlar, jumladan session hijacking, XSS va CSRF hujumlari sun'iy intellekt vositalari yordamida yanada avtomatlashtirilgan va murakkablashgan shaklga ega bo'lmoqda. Bu esa web-ilovalar xavfsizligini ta'minlashda yangi yondashuvlarni talab qiladi.

Tadqiqot davomida aniqlanishicha, sessiya tokenlarini himoyalashda alohida mexanizmlardan foydalanish yetarli emas. Eng samarali natijaga erishish uchun HTTPS protokoli, cookie parametrlarini to'g'ri sozlash, token rotatsiyasi va ko'p bosqichli autentifikatsiya kabi usullarni kompleks holda qo'llash zarur.

Shuningdek, generativ sun'iy intellekt nafaqat tahdid manbai, balki samarali himoya vositasi sifatida ham namoyon bo'lishi mumkin. Xususan, AI asosidagi monitoring tizimlari orqali anomaliyalarni aniqlash va tahdidlarga tezkor javob berish imkoniyati mavjud.

Kelgusida web-sessiya tokenlari xavfsizligini ta'minlashda adaptiv, o'z-o'zini o'rganuvchi va sun'iy intellektga asoslangan xavfsizlik tizimlarini ishlab chiqish muhim ahamiyat kasb etadi. Shu bilan birga, ushbu yo'nalishda olib boriladigan ilmiy tadqiqotlar kiberxavfsizlikni yanada mustahkamlashga xizmat qiladi.

ADABIYOTLAR

1. Abdullaev, A. (2020). Axborot xavfsizligi asoslari. Toshkent: Fan.
2. Ismoilov, Sh. (2019). Veb-texnologiyalar va axborot xavfsizligi. Toshkent: Iqtisodiyot.
3. Kaspersky. (2022). Cybersecurity threat landscape report.
4. Microsoft. (2023). Security best practices for web applications.
5. National Institute of Standards and Technology (NIST). (2021). Guidelines on security and privacy in public cloud computing.
6. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2022). Kiberxavfsizlik bo'yicha milliy strategiya. Toshkent.
7. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
8. Rakhmonov, D. (2021). Kiberxavfsizlik va uning zamonaviy tahdidlari. Toshkent: Universitet.
9. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.
10. Yusupov, B. (2023). Zamonaviy axborot tizimlarida xavfsizlik muammolari. Toshkent.
11. OWASP Foundation. (2021). OWASP top 10: The ten most critical web application security risks.
12. ISO/IEC. (2022). ISO/IEC 27001 information security management systems.