ZAMONAVIY VEB-ILOVALARDA COOKIE VA SESSIYALARNI BOSHQARISH MEXANIZMLARINING XAVFSIZLIK TAHLILI VA KIBER-HUJUMLARDAN HIMOYA QILISH USULLARI

Xo‘jaqulova Diyora
Toshkent Davlat Iqtisodiyot Universiteti
Raqamli Iqtisodiyot Va Axborot Texnologiyalari Fakulteti Talabasi
xojaqulovadiyora7@gmail.com
Ilmiy rahbar: Amonov Alisher
https://doi.org/10.5281/zenodo.20552726

Annotatsiya. Ushbu tezisda zamonaviy veb-ilovalarda cookie va sessiyalarni boshqarish mexanizmlarining xavfsizlik tahlili hamda ularni kiber-hujumlardan himoya qilish masalalari tadqiq etilgan. HTTP protokolining "stateless" (holatsiz) tabiati sababli yuzaga keladigan xavfsizlik bo‘shliqlari, xususan, seanslarni o‘g‘irlash (Session Hijacking) va cookie-fayllarni soxtalashtirish (Cookie Poisoning) kiber-tahdidlari tahlil qilingan. Tadqiqot doirasida, Single Sign-On (SSO) muhitida va Teskari Proksi (Reverse Proxy) platformalariga asoslangan tarmoq arxitekturasida "end-to-end" xavfsiz ulanishni ta’minlovchi yangi "session-av" konsepti taklif etilgan. Sarlavhaga kiritilgan sessionID, sessionDuration, scomment va ICD (Integrity Cookie Digit) atributlari yordamida seanslar yaxlitligini dastur darajasida (application-level) majburiy nazorat qilish algoritmi ishlab chiqilgan. Taklif etilayotgan model milliy axborot tizimlari va bank-moliya platformalarining kiber-barqarorligini oshirishda amaliy ahamiyatga ega.

Kalit so‘zlar: Kiberxavfsizlik, HTTP protokoli, Cookie boshqaruvi, Sessiyani o‘g‘irlash (Session Hijacking), Cookie Poisoning, Teskari Proksi (Reverse Proxy), Single Sign-On (SSO), ICD (Integrity Cookie Digit).

KIRISH

Bugungi kunda mamlakatimizda raqamli iqtisodiyotni rivojlantirish, davlat va bank xizmatlarini to‘liq elektron shaklga o‘tkazish hamda axborot xavfsizligini ta’minlash davlat siyosatining eng muhim ustuvor yo‘nalishlaridan biri hisoblanadi. O‘zbekiston Respublikasi Prezidentining "Raqamli O‘zbekiston — 2030" strategiyasini tasdiqlash to‘g‘risida"gi Farmoni[1] hamda O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni[2] doirasida milliy axborot tizimlari va veb-resurslarining daxlsizligini ta’minlash, kiber-tahdidlarga qarshi barqaror infratuzilmani yaratish vazifalari belgilangan. Veb-ilovalarning xavfsizligi bevosita foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlarini himoya qilish bilan uzviy bog‘liqdir. Hozirgi vaqtda global internet trafigining asosiy qismini HTTP (Hypertext Transfer Protocol) protokoli tashkil etadi va uning o‘sish sur’ati P2P (Peer-to-Peer) trafigidan sezilarli darajada o‘zib ketdi[3]. HTTP protokoli mijoz va server o‘rtasidagi so‘rov/javob (request/response) tranzaksiya modeliga asoslangan bo‘lib, uning keng ommalashganiga sabab — arxitekturasining soddaligi va yuqori samaradorligidir [3]. Biroq, HTTP protokoli tabiati guruhiga ko‘ra "stateless" (holatsiz) hisoblanadi, ya’ni u har bir so‘rovni mustaqil deb ko‘radi va oldingi seanslar xotirasini saqlamaydi.

ASOSIY QISM

Ushbu muammoni hal qilish va tranzaksiyalar holatini kuzatib borish (state maintenance) uchun cookie mexanizmlaridan keng foydalaniladi. Cookie-fayllar foydalanuvchilarni

[1] O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi "Raqamli O‘zbekiston — 2030" strategiyasini tasdiqlash va uni muvaffaqiyatli amalga oshirish chora-tadbirlari to‘g‘risida"gi PF-6079-son Farmoni. – Toshkent, 2020.
[2] O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni. – Toshkent, 2022.
[3] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. Hypertext Transfer Protocol -- HTTP/1.1. RFC 2616. – pp. 15-28.

autentifikatsiya qilish, sessiyalarni boshqarish hamda veb-saytdagi shaxsiy sozlamalarni (masalan, elektron savat tarkibini) eslab qolish vazifasini bajaradi [3]. Biroq, HTTP protokolining soddaligi va cookie mexanizmlarining standart realizatsiyasi ularni kiber-hujumchilar uchun oson nishonga aylantirmoqda. Cookie-fayllar axborot maxfiyligiga jiddiy tahdid solishi mumkin. Ular sessiyalarni o‘g‘irlash (session hijacking), cookie-fayllarni soxtalashtirish va qayta ishlatish kabi jiddiy kiber-hujumlar ob’yektiga aylanmoqda[4]. Ilgari ushbu xavflarni kamaytirish bo‘yicha bir qancha ilmiy tadqiqotlar olib borilgan bo‘lsa-da, ularning aksariyati dasturiy ilova darajasida majburiy xavfsizlik arxitekturasini to‘liq ta’minlay olmagan.

Shundan kelib chiqqan holda, ushbu ilmiy ishda foydalanuvchi va veb-server o‘rtasida "end-to-end" (oxirigacha) xavfsiz ulanishni ta’minlovchi, Teskari Proksi arxitekturasiga asoslangan xavfsiz cookie boshqaruvi mexanizmi taklif etiladi.

Tarmoq arxitekturasi va Reverse Proxy komponentining o‘rni

Zamonaviy korporativ tarmoqlarda xavfsizlikni yuqori darajada ta’minlash uchun tashqi va ichki tarmoqlar o‘rtasida himoya to‘siqlari (Firewalls) hamda Demilitarizatsiyalashgan zona (DMZ) tashkil etiladi. Taklif etilayotgan modelda foydalanuvchilar (Users) va korporativ tarmoq (Enterprise Network) ichidagi veb-ilova serverlari (Web Application Servers) o‘rtasida bevosita bog‘lanish cheklanadi. Ushbu arxitekturaning markaziy bo‘g‘ini sifatida HTTP Reverse Proxy (Teskari Proksi) elementi DMZ zonasida joylashtiriladi[5]. Tashqi xavfsizlik devori (Outer Firewall) orqali kelayotgan barcha HTTP so‘rovlar dastlab Reverse Proxy tomonidan qabul qilinadi va tahlildan o‘tkazilgandan so‘ng, ichki xavfsizlik devori (Inner Firewall) orqali tegishli veb-serverga yo‘naltiriladi. Ushbu yondashuv SSO (Single Sign-On) muhitida foydalanuvchi seanslarini yagona nuqtada xavfsiz boshqarish va dastur darajasidagi (application-level) majburiy xavfsizlik siyosatini joriy etish imkonini beradi [1].

EBNF grammatikasi va "Session-AV" konseptining kiritilishi

Standart cookie mexanizmlaridagi zaifliklarni bartaraf etish maqsadida, HTTP sarlavhasidagi an’anaviy cookie deklaratsiyasining EBNF (Extended Backus-Naur Form) grammatik ta’rifiga o‘zgartirish kiritildi [5]. Model doirasida foydalanuvchi va veb-server o‘rtasidagi "end-to-end" (oxirigacha) seanslarni to‘liq nazorat qilish uchun yangi "session-av" (session attribute-value) konsepti hamda RP-Set-Cookie sarlavhasi taklif etiladi.

Ushbu sarlavha tarkibiga sessiya xavfsizligi va yaxlitligini ta’minlovchi quyidagi to‘rtta yangi atribut kiritilgan:

- sessionID: Muayyan foydalanuvchi uchun unikal sessiyani aniqlovchi maydon. Amaliyotda bir vaqtning o‘zida bitta foydalanuvchi bir nechta faol HTTP seanslariga ega bo‘lishi mumkin. Ushbu atribut yordamida barcha valid seanslar yagona tizimga bog‘lanadi. Bunga userID parametri yoki tarmoq parametrlari (masalan, IP-manzil) kombinatsiyasi orqali erishiladi [5].
- sessionDuration: Sessiyaning amal qilish muddatini (vaqt oralig‘ini) qat’iy belgilovchi atribut. Bu vaqt tugagach, seans avtomatik ravishda haqiqiy emas deb topiladi va qayta autentifikatsiya talab etiladi.
- scomment: Joriy sessiyaga tegishli xizmat ko‘rsatuvchi sharhlar yoki maxsus teglarni qo‘shish uchun xizmat qiladi. Taklif etilayotgan arxitekturada ushbu maydon majburiy (mandatory) hisoblanadi va proksi darajasida qaror qabul qilishni optimallashtiradi [5].

[4] Kristol, D., & Montulli, L. HTTP State Management Mechanism. RFC 2965. – pp. 4-12.
[5] Security Management in SSO Architecture based on Reverse Proxy Platforms. // IEEE Xplore Digital Library. — 2026. — pp. 1-6.

- ICD (Integrity Cookie Digit): Cookie-fayllarning xavfsizligini, ularning yo‘lda o‘zgartirilmaganligini (yaxlitligini) ta’minlovchi maxsus raqamli atribut (kriptografik nazorat yig‘indisi). Ushbu maydon kiber-hujumchilar tomonidan cookielarni soxtalashtirish (cookie poisoning) xavfini to‘liq bartaraf etadi [5].

"Session-AV" atributlarining kiber-tahdidlarga qarshi samaradorligi va himoya mexanizmi

Teskari Proksi (Reverse Proxy) darajasida joriy etilgan yangi sarlavha atributlari an’anaviy HTTP cookie-fayllariga xos bo‘lgan jiddiy xavfsizlik bo‘shliqlarini bartaraf etishga xizmat qiladi. Quyida ushbu atributlarning asosiy kiber-hujumlarga qarshi ishlash algoritmi keltirilgan:

- Sessiyalarni o‘g‘irlash (Session Hijacking) va qayta ishlatish (Cookie Replay) hujumlariga qarshi: Hujumchi foydalanuvchining cookie-faylini o‘g‘irlagan taqdirda ham, sessionID tarkibidagi foydalanuvchi identifikatori (userID) va tarmoq parametrlari (masalan, IP-manzil yoki qurilma barmog‘i/fingerprint) kombinatsiyasi tekshiriladi. Agar so‘rov kelayotgan yangi IP-manzil proksi xotirasidagi dastlabki seans parametrlari bilan mos kelmasa, Reverse Proxy tizimi sessiyani avtomatik ravishda bloklaydi. Bundan tashqari, sessionDuration atributi seansning faol bo‘lish vaqtini qat’iy cheklashi sababli, eskirgan cookie-fayllarni qayta ishlatish imkoniyati nolga tenglashtiriladi.
- Cookie-fayllarni soxtalashtirishga (Cookie Poisoning) qarshi: Ushbu hujum turida kiber-jinoyatchilar brauzer xotirasidagi cookie qiymatlarini (masalan, foydalanuvchi huquqlarini belgilovchi teglarni) o‘zgartirishga urinadilar. Taklif etilayotgan arxitekturadagi ICD (Integrity Cookie Digit) atributi cookie ma’lumotlarining yaxlitligini kriptografik nazorat yig‘indisi (hash) orqali tekshiradi. Agar foydalanuvchi yoki hujumchi tomonidan cookie qiymatlariga biror-bir o‘zgartirish kiritilsa, ICD qiymati buziladi va Reverse Proxy ushbu so‘rovni "soxtalashtirilgan" deb hisoblab, korporativ tarmoq ichidagi veb-serverlarga o‘tkazmaydi.

An'anaviy va yangi xavfsiz cookie boshqaruvi modellarining qiyosiy tahlili

Olib borilgan tadqiqotlar va arxitekturaviy tahlillar shuni ko‘rsatadiki, amaldagi standart cookie boshqaruv tizimlaridan farqli o‘laroq, Reverse Proxy bazasidagi model dastur darajasida (application-level) majburiy xavfsizlikni ta’minlaydi. An’anaviy tizimlarda har bir ichki veb-server o‘z sessiya xavfsizligini mustaqil boshqarishi kerak edi, bu esa umumiy tizimda zaif nuqtalarning ko‘payishiga olib kelardi. Yangi modelda esa barcha xavfsizlik siyosatlari markazlashtirilgan holda, Demilitarizatsiyalashgan zonadagi (DMZ) proksi serverda bajariladi. Bu ichki veb-serverlarning yuklamasini kamaytiradi va umumiy infratuzilmaning kiber-barqarorligini oshiradi.

XULOSA

Kuzatilayotgan global va milliy raqamlashtirish jarayonlarida veb-ilovalarning xavfsizligini ta’minlash eng dolzarb vazifalardan biridir. Ushbu tezis doirasida olib borilgan tadqiqot natijasida quyidagi xulosalarga erishildi. HTTP protokolining "stateless" tabiati va standart cookie-fayllarning zaifligi tizim xavfsizligiga jiddiy tahdid solishi asoslab berildi. Reverse Proxy va SSO platformalariga asoslangan, "session-av" konseptini o‘z ichiga oluvchi kengaytirilgan seans boshqaruvi modeli ishlab chiqildi. Kiritilgan sessionID, sessionDuration, scomment va ICD atributlari orqali Session Hijacking va Cookie Poisoning kabi xavfli kiber-hujumlarni dastur darajasiga yetib bormasidanoq to‘xtatish imkoniyati isbotlandi. Tadqiqot natijalari kelgusida bank-moliya tizimlari va davlat elektron xizmat ko‘rsatish platformalarining xavfsizligini modernizatsiya qilishda amaliy qo‘llanma bo‘lib xizmat qilishi mumkin.

Adabiyotlar, References, Литературы:

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi "Raqamli O‘zbekiston —

2030" strategiyasini tasdiqlash va uni muvaffaqiyatli amalga oshirish chora-tadbirlari to‘g‘risida"gi PF-6079-son Farmoni. – Toshkent, 2020.
2. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni. – Toshkent, 2022.
3. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. Hypertext Transfer Protocol -- HTTP/1.1. RFC 2616. – pp. 15-28.
4. Kristol, D., & Montulli, L. HTTP State Management Mechanism. RFC 2965. – pp. 4-12.
5. Security Management in SSO Architecture based on Reverse Proxy Platforms. // IEEE Xplore Digital Library. — 2026. — pp. 1-6.