CSRF (CROSS-SITE REQUEST FORGERY) HUJUMLARI: MEXANIZMLARI, XAVFLARI VA KOMPLEKS HIMOYA STRATEGIYALARI

Behzod Sobirjonov Qahramonivich
FarDu Axborot texnologiyalari
kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Mahammadaliyeva Marhabo Kamoliddin qizi
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
marhaboxon29@gmail.com
Telefon raqam:91 396 19 03
https://doi.org/10.5281/zenodo.20080240

Annotatsiya

Ushbu ilmiy maqola veb-xavfsizlikning fundamental muammolaridan biri bo‘lgan CSRF (Cross-Site Request Forgery) hujumlarini nazariy va amaliy jihatdan tadqiq etadi. Maqolada HTTP protokolining ishlash prinsiplari, sessiyalarni boshqarishdagi kamchiliklar va zamonaviy brauzerlarning kuki-fayllarga bo‘lgan munosabati tahlil qilinadi. Tadqiqot davomida hujumning turli ssenariylari yoritilgan bo‘lib, Anti-CSRF tokenlari va SameSite atributlari kabi himoya mexanizmlarining samaradorligi tahlil qilingan.

Kalit so‘zlar: kiberxavfsizlik, CSRF, veb-ilova, HTTP protokoli, kuki-fayllar, sessiya boshqaruvi, Anti-CSRF token, SameSite, autentifikatsiya.

Annotation

This scientific paper provides a theoretical and practical investigation into CSRF (Cross-Site Request Forgery) attacks. The article analyzes the operating principles of the HTTP protocol, flaws in session management, and the behavior of modern browsers toward cookie files. The research highlights various attack scenarios and analyzes the effectiveness of defense mechanisms such as Anti-CSRF tokens and SameSite attributes.

Keywords: cybersecurity, CSRF, web application, HTTP protocol, cookies, session management, Anti-CSRF token, SameSite, authentication.

Аннотация

Данная научная статья исследует атаки CSRF (межсайтовая подделка запроса) как одну из фундаментальных проблем веб-безопасности. В статье анализируются принципы работы протокола HTTP, недостатки управления сессиями и поведение современных браузеров в отношении файлов cookie. В ходе исследования освещаются различные сценарии атак и анализируется эффективность механизмов защиты, таких как Anti-CSRF токены и атрибуты SameSite.

Ключевые слова: кибербезопасность, CSRF, веб-приложение, протокол HTTP, куки-файлы, управление сессией, Anti-CSRF токен, аутентификация.

KIRISH.

Raqamli texnologiyalar asrida veb-ilovalarning xavfsizligini ta'minlash global darajadagi strategik vazifaga aylandi. Ayniqsa, bank-moliya tizimlari, davlat xizmatlari va ijtimoiy tarmoqlar foydalanuvchilarning konfidentsial ma’lumotlari bilan ishlashi sababli kiberhujumchilarning asosiy nishoni bo‘lib qolmoqda. Cross-Site Request Forgery (CSRF) — bu "mijoz tomoni" (client-side) hujumi bo‘lib, u foydalanuvchi va server o‘rtasidagi ishonchli

munosabatni suiiste’mol qilishga asoslangan. CSRF hujumi ko‘pincha "XSS" (Cross-Site Scripting) bilan adashtiriladi, biroq ularning mexanizmi tubdan farq qiladi. Agar XSS foydalanuvchi ma'lumotlarini (masalan, kuki-fayllarni) o‘g‘irlashga qaratilgan bo‘lsa, CSRF foydalanuvchi nomidan ruxsatsiz harakatlarni amalga oshirishga (pul o‘tkazish, parolni o‘zgartirish, tizim sozlamalarini tahrirlash) yo‘naltirilgan. Ushbu maqola CSRF hujumining paydo bo‘lish shartlari va unga qarshi ko‘p bosqichli himoya tizimlarini yaratish masalalarini o‘rganadi.

Sessiyalarni boshqarish va Kuki-fayllar

Veb-serverlar har bir foydalanuvchini tanib olish uchun sessiya mexanizmidan foydalanadi. Foydalanuvchi tizimga kirganida server unga "Session ID" taqdim etadi. Ushbu ID foydalanuvchi brauzerida kuki-fayl sifatida saqlanadi. HTTP protokoli "stateless" (holatni saqlamaydigan) bo‘lgani uchun, brauzer keyingi har bir so‘rovda ushbu kuki-fayllarni avtomatik ravishda serverga yuboradi.

Same-Origin Policy (SOP) va uning cheklovlari

Same-Origin Policy — bu brauzer xavfsizligining asosiy tamoyili bo‘lib, u bir manbadan (domain) kelgan skriptlarning boshqa manba ma'lumotlariga kirishini cheklaydi. Biroq, SOP brauzerning boshqa domenga so‘rov (request) yuborishini taqiqlamaydi. Masalan, hacker.com saytida turgan rasm tegi bank.uz saytiga so‘rov yubora oladi. Aynan mana shu mantiqiy bo‘shliq CSRF hujumi uchun zamin yaratadi. Hujumchi CSRFni amalga oshirish uchun foydalanuvchini o‘zining nazoratidagi zararli sahifaga yo‘naltirishi kerak. Bu jarayon quyidagi ssenariylar orqali kechadi:

Eng sodda va xavfli usul. Agar veb-ilova muhim operatsiyalarni GET so‘rovlari orqali amalga oshirsa, hujumchi quyidagi ko‘rinishdagi koddan foydalanishi mumkin:

<img src="https://bank.uz/api/transfer?amount=5000&to=hackerID" style="display:none;">

Foydalanuvchi sahifaga kirishi bilan brauzer rasmni yuklashga urinadi va natijada bank serveriga pul o‘tkazish so‘rovi ketadi.

Sinxronlashtirilgan Anti-CSRF Tokenlar

Bu metodda server har bir sessiya uchun unikal va taxmin qilib bo‘lmaydigan tasodifiy satr (token) yaratadi. Ushbu token har bir HTML formaga yashirin maydon sifatida qo‘shiladi. Server so‘rovni qabul qilganda, kelgan tokenni sessiyadagi token bilan solishtiradi. Hujumchi boshqa domenda bo‘lgani uchun ushbu tokenni o‘qiy olmaydi va uning soxta so‘rovi rad etiladi.

XULOSA

CSRF hujumi veb-texnologiyalarning mantiqiy arxitekturasidagi bo‘shliqlardan foydalanadi. Ushbu maqolada ko‘rib chiqilganidek, faqatgina bitta himoya usuli bilan cheklanish yetarli emas. Zamonaviy kiberxavfsizlik "Depth-in-Defense" (Chuqurlashtirilgan himoya) tamoyilini talab qiladi. Dasturchilar va xavfsizlik muhandislari brauzerlarning yangi imkoniyatlaridan foydalangan holda, ko‘p qatlamli himoya tizimlarini loyihalashlari zarur.

Adabiyotlar, References, Литературы:

1. O‘zbekiston Respublikasining Qonuni. "Kiberxavfsizlik to‘g‘risida" O‘RQ-764-son. 2022-yil 15-aprel. (Mahalliy huquqiy asos uchun).
2. G‘aniyev S. K., Karimov M. M., Tashev K. A. *Axborot xavfsizligi*. Darslik. — Toshkent: "Aloqachi", 2016. — 420 b. (O‘zbekistondagi axborot xavfsizligi bo‘yicha fundamental darslik).

3. Gulyamov S. S. *Kiberjinoyatchilik va kiberxavfsizlik*. O‘quv qo‘llanma. — Toshkent: TDYU, 2020.
4. OWASP Foundation. "Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet". OWASP Series, 2023. [Elektron manba]: https://cheatsheetseries.owasp.org/