The Practical Importance Of Ensuring The Security Of Web Applications

Ahmedov Ahadjon Murodjon o'g'li
Student of Kokand University
Scientific supervisor: Asqarov Elbek Erkinjon o'g'li
Teacher of the Department of Digital
Technologies and Mathematics, Kokand University,
elbek.asqarov10@gmail.com

Abstract
This article discusses the relevance of ensuring the security of web applications, modern threats, methods for eliminating them and their practical significance. Web applications are now of central importance not only for economic activity, but also for social relations, security and even expert-forensic systems. In particular, technologies such as facial recognition and biometric authentication are becoming an integral part of the security of today's web applications.
Keywords: web security, SQL injection, XSS, authentication, encryption, OWASP, biometric systems, user data
Annotatsiya
Ushbu maqolada web ilovalar xavfsizligini ta'minlashning dolzarbligi, zamonaviy tahdidlar, ularni bartaraf etish usullari va amaliy ahamiyati yoritilgan. Web ilovalar bugungi kunda nafaqat iqtisodiy faoliyat, balki ijtimoiy munosabatlar, xavfsizlik va hatto ekspert-криминалistik tizimlar uchun ham markaziy ahamiyat kasb etmoqda. Xususan, yuzni tanib olish, biometrik autentifikatsiya kabi texnologiyalar bugungi web ilovalar xavfsizligining ajralmas qismiga aylanmoqda.
Kalit so‘zlar: web xavfsizlik, SQL injection, XSS, autentifikatsiya, shifrlash, OWASP, biometrik tizimlar, foydalanuvchi ma'lumotlari

Kirish

Bugungi raqamli davrda web ilovalar hayotimizning ajralmas qismiga aylangan. Onlayn banking, ta'lim tizimlari, e-commerce platformalari, ijtimoiy tarmoqlar va hatto xavfsizlik tizimlari web asosda ishlamoqda. Ammo bu qulayliklar bilan bir qatorda, web ilovalarga qarshi tahdidlar va xakerlik hujumlari ham jadal rivojlanmoqda. Xavfsizlikning buzilishi nafaqat foydalanuvchi ma'lumotlarining o‘g‘irlanishiga, balki butun tizimlarning ishdan chiqishiga olib kelishi mumkin.
Web ilovalar xavfsizligining dolzarbligi. Ma’lumotlar hajmining oshishi, ulardan foydalanish tezligining ko‘payishi, turli platformalarning o‘zaro integratsiyalashuvi web xavfsizlik masalasini birinchi darajali muammoga aylantirdi. Foydalanuvchi ma'lumotlarining himoyasizligi xakerlar uchun katta imkoniyatlar yaratadi. Ayniqsa, moliyaviy va biometrik ma'lumotlar bugungi kunda eng qimmat aktiv hisoblanadi.
Web xavfsizlik tahdidlari va ularning turlari. Web ilovalarga nisbatan eng ko‘p uchraydigan tahdidlar:

- **SQL Injection** – serverga soxta SQL so‘rov yuborish orqali ma’lumotlar bazasiga noqonuniy kirish;
- **XSS (Cross-site Scripting)** – foydalanuvchi brauzerida zararli skriptlarni ishga tushirish;
- **CSRF (Cross-site Request Forgery)** – foydalanuvchini o‘z xabarisiz boshqa so‘rov yuborishga majbur qilish;
- **Brute Force** – login-parollarni taxmin qilish orqali tizimga kirish;
- **Session Hijacking** – sessiya identifikatorini o‘g‘irlab tizimga kirish.

Amaliy yechimlar va tavsiyalar

- **Autentifikatsiya va avtorizatsiya** – foydalanuvchini aniq aniqlash va unga ruxsat doirasida imkoniyat berish;
- **Ma’lumotlarni shifrlash** – ayniqsa HTTPS orqali xavfsiz uzatish;
- **Biometrik identifikatsiya** – foydalanuvchini yuz tasviri, barmoq izi yoki ko‘z qovog‘i orqali aniqlash. Bu ayniqsa onlayn banking va xavfsizlik tizimlarida keng qo‘llanmoqda;
- **WAF (Web Application Firewall)** – zararli trafikni filtrlaydi;
- **OWASP Top 10** – eng ko‘p uchraydigan 10 ta tahdidlar ro‘yxati va ularning oldini olish strategiyalari;
- **Xavfsizlik testlari** – doimiy tarzda penetratsiya testlari o‘tkazish.

4. Amaliy misollar va ilg‘or tajribalar

- **Facebook** – 2 bosqichli autentifikatsiya orqali xavfsizlikni oshirgan;
- **Google** – HTTPS’ni majburiy holga keltirgan;
- **PayPal** – tranzaksiyalar uchun biometrik autentifikatsiyani joriy etgan;
- **Ekspert tizimlarda yuzni tanib olish** – huquqni muhofaza qilish organlarida jinoyatchilarni aniqlashda foydalanilmoqda. Bu yerda yuz komponentalariga asoslangan tanish algoritmlari qo‘llaniladi, masalan, ko‘z, burun, og‘iz shakli, va ularning joylashuviga qarab aniqlash.

Biometrik tizimlar xavfsizligi bilan integratsiya. Biometrik identifikatsiya usullari, ayniqsa yuzni tanib olish texnologiyasi, web ilovalarda xavfsizlikni oshirishda muhim rol o‘ynaydi. Bu tizimlar foydalanuvchidan faqat parol emas, balki yuz tasvirini yoki barmoq izini so‘raydi. Yuzni komponentalar orqali tanish – ya’ni ko‘zlar, burun, og‘iz singari belgilarni alohida ajratish va analiz qilish orqali aniqlik darajasi oshadi. Ushbu tizimlar ko‘p bosqichli qaror qabul qilish modeliga asoslangan bo‘lib, lokal klassifikatorlardan olingan natijalarni integratsiyalash orqali umumiy qaror shakllanadi.

Xulosa. Web ilovalarning xavfsizligini ta'minlash – bu nafaqat dasturiy, balki tizimli va strategik yondashuvni talab qiluvchi jarayon. Har bir ishlab chiquvchi, tizim administrator va foydalanuvchi o‘zining rolini tushunib, xavfsizlik choralarini ko‘rishi kerak. Ayniqsa, biometrik autentifikatsiya va yuzni tanib olish texnologiyalarining web xavfsizlikka integratsiyasi bu sohadagi yutuqlarning amaliy isboti hisoblanadi.

References:

OWASP Foundation – www.owasp.org
Mozilla Developer Network – https://developer.mozilla.org
Vacca J.R. Biometric Technologies and Verification Systems. Elsevier, 2007
Кахаров Ш.С., Уринов Э.М. "Шахсни юз тасвири орқали идентификациялашда кўп поғонали биометрик тизим қуриш масаласи ва ечимлари". 2021
Кухарев Г.А. Биометрические системы. СПб: Политехника, 2001