ISSN 2181-3187

VEB DASTURCHILAR UCHUN XAVFSIZLIKNI TA'MINLASHGA OID ASOSIY TUSHUNCHALAR VA ULARGA QARSHI KURASHISH USULLARI

Bahramov Muhammadali Eraliyevich
University of Management and Future Technologies
bahromov1997.04.09@gmail.com

Annotatsiya

Maqolada veb dasturchilar uchun muhim bo‘lgan 7 ta xavfsizlik tushunchasi muhokama qilinadi. Bular orasida, tizimning zaif tomonlarini exploatatsiya qilish (zero-day), XSS va SQL inyektsiyalari kabi hujumlar, foydalanuvchi ma'lumotlarini himoya qilish, minimallik printsipi va DDoS hujumlariga qarshi kurashish kabi asosiy xavf-xatarlar mavjud. Har bir kontseptsiyaning tavsifi va ularni kamaytirish usullari keltirilgan. Veb dasturchilar xavfsizlikni doimiy ravishda yaxshilab borishlari kerak.

Kalit so’zlar: xavfsizlik, veb dasturchilar, zero-day, XSS, SQL inyektsiyasi, foydalanuvchi ma'lumotlari, minimal huquqlar, DDoS hujumlari, xavf-xatarlarni kamaytirish, himoya qilish.

Cloud provayderlari va veb-ilovalar frameworklari sizni xavfsiz kod yozishdan himoya qilish uchun katta ishlar qilmoqda. Cloud xavfsiz standartlar va monitoringni taqdim etadi, Angular va React esa zararli JavaScriptni kiritishni oldini olish uchun HTMLni avtomatik ravishda sanitizatsiya qiladi. Biroq, hech qanday ilova 100% xavfsiz emas va yangi ekspluatatsiyalar kashf etilishi mumkin. Quyidagi darsda eng keng tarqalgan xakerlik usullari va ilovangizni ulardan qanday himoya qilish kerakligi tushuntiriladi.

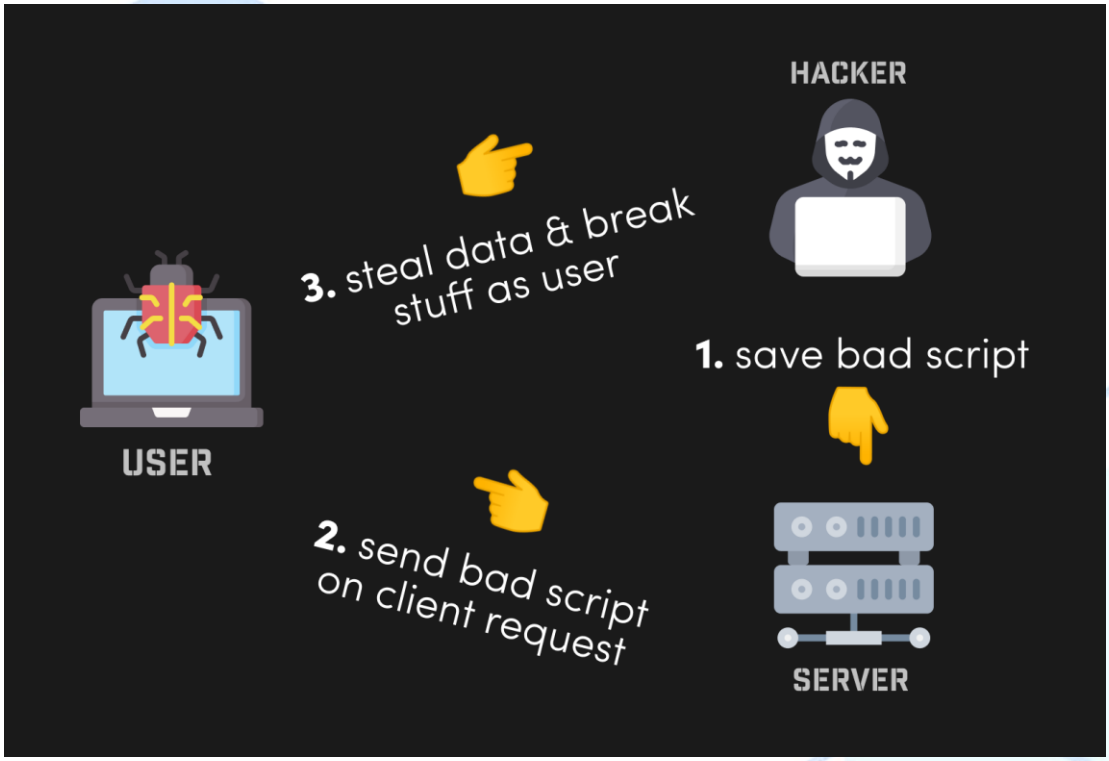
1. Zero-day zaifligi - bu hozirgi kunda noma'lum yoki tuzatilmagan xavfsizlik nuqsoni. Agar xaker bu zaiflikni ekspluatatsiya qilsa, unga zero-day ekspluatatsiyasi deyiladi. Zaiflik aniqlangandan so‘ng, uning ochilishi vaqtiga qarab, buni bir kunlik yoki 20 kunlik ekspluatatsiya deb atash mumkin.

2. Ma'lum zaifliklarga ega paketlar - bu xavfsizlik nuqsonlari aniqlangan va hujjatlashtirilgan dastur paketlari yoki kutubxonalaridir. Agar bu paketlar yangilanmasa yoki tuzatilmasa, xakerlar tomonidan ekspluatatsiya qilinishi mumkin. Dasturchilar bu paketlardan ehtiyotkorlik bilan foydalanishlari kerak, ularni yangilab borish yoki xavfsizroq alternativalar bilan almashtirish zarur.

3. Cross-site Scripting (XSS) - bu veb ilovalarda zararli JavaScript kodini qo‘shish hujumidir. Bu kod foydalanuvchi brauzerida ishga tushadi va xakerlarga foydalanuvchi ma'lumotlarini o‘g‘irlash yoki tizimga zarar etkazish imkonini beradi.

ISSN 2181-3187

XSS hujumlari odatda foydalanuvchi kiritgan ma'lumotlarni to‘g‘ri sanitizatsiya qilmaslik sababli yuzaga keladi.



1. Xaker ba'zi JavaScript kodlarini bazaga saqlaydi, masalan: <script>alert('you got got')</script>, veb-ilova orqali izoh yuborish orqali.

2. Jabrlangan foydalanuvchi izoh bilan veb-sahifani ochadi, lekin dasturchi xakerning izohini sanitizatsiya qilmagan, shuning uchun brauzer uni ishonchli skript/HTML deb o'ylaydi.

3.Shu paytda, xakerning JavaScript kodi foydalanuvchi sifatida ishlay boshlaydi.

4.SQL Injection

bu hujum usuli bo‘lib, u veb-ilovaga zararli SQL so‘rovlarini yuborish orqali ma'lumotlar bazasiga kirishga harakat qiladi. Xaker foydalanuvchi kiritgan ma'lumotlarni noto‘g‘ri tekshirish yoki sanitizatsiya qilish orqali tizimga kiradi va ma'lumotlarni o‘zgartirishi, o‘chirishi yoki o‘g‘irlashi mumkin. Bu xavf-xatarni oldini olish uchun parametrli so‘rovlar va ma'lumotlarni to‘g‘ri sanitizatsiya qilish kerak.

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = '';

5.Credential Leaks – bu foydalanuvchining login va parol ma'lumotlarining tasodifiy yoki xato tarzda oshkor bo‘lishidir. Bunday ma'lumotlar xavfsiz bo‘lmagan platformalar yoki xato konfiguratsiyalar orqali oshkor bo‘lishi mumkin. Xakerlar bu ma'lumotlarni o‘g‘irlab, tizimga kirish uchun ishlatishlari mumkin. Bunday xavflardan himoya qilish uchun parollarni shifrlash, ikki faktorli autentifikatsiya (2FA) va xavfsiz ma'lumot saqlash amaliyotlaridan foydalanish zarur.

ISSN 2181-3187

6."Principle of Least Privilege" (Minimal Huquqlar Printsipi) – bu tizimdagi foydalanuvchilarga va dasturlarga faqat kerakli darajadagi huquqlarni berish tamoyilidir. Bu printsip orqali foydalanuvchilar yoki dasturlar faqat o'z vazifalarini bajarish uchun zarur bo'lgan resurslarga kirish huquqiga ega bo'lishi kerak, bu esa tizimdagi xavf-xatarlarni kamaytiradi. Dastur yoki foydalanuvchi uchun ortiqcha huquqlarni berish xavf tug‘diradi.

7.DDoS (Distributed Denial of Service) hujumlari – bu tizimni yoki veb-saytni ishlamay qolishiga olib keladigan hujumlar bo‘lib, ular ko‘plab zararli so‘rovlar yuborish orqali tizimni to‘liq band qiladi. Bu, natijada, haqiqiy foydalanuvchilarga xizmat ko‘rsatishni to‘xtatadi. DDoS hujumlarini oldini olish uchun, xavfsizlikni mustahkamlash, trafigni kuzatish va ilg‘or himoya choralarini ko‘rish zarur.

Xulosa

Xavfsiz veb-ilovalarni yaratish dasturchilar uchun juda muhimdir. Zero-day ekspluatatsiyalari, SQL inyektsiyalari, XSS va DDoS hujumlari kabi keng tarqalgan zaifliklarni tushunish va ularga qarshi choralar ko‘rish tizimning himoyasini ta'minlashda yordam beradi. Xavfsizlikni oshirish uchun xavfsiz paketlar, foydalanuvchi kirishini sanitizatsiya qilish va minimal huquqlar printsipini qo‘llash zarur. Doimiy ravishda xavfsizlikni tekshirish va yangilab borish muhim.

Foydalanilgan adabiyotlar

1. Randell D. Wallace and Don F.Dagenais.The changing world of electronic signatures // https: www.library.lp.findlaw.com.
2. Craig Buckler Node.js: Novice to Ninja
3. Google.com
4. https://nodejs.org/en
5. https://itoolkit.co/blog/2023/08/what-are-hashing-salting-algorithms/#:~:text=In%20cryptography%2C%20salting%20refers%20to,number%20generator%20for%20creating%20salts