WEB ILOVALARGA BO'LADIGAN ASOSIY HUJUMLAR

Qurbonmurodov Diyorbek Ulug'bek o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabasi

Annotatsiya: *Ushbu maqolada veb ilovalarga bo'ladigan hujumlar va bu hujumlardan ko'zlanadigan maqsadlar, amalga oshiriladigan hujum turlari va ular haqida qisqacha nazariy ma'lumot berib o'tildi. Bu hujumlarning oldini olishning birlamchi choralari keltirildi.*

Kalit so'zlar: *veb ilovalar, XSS, DDOS, XXE, CSRF , SQL injection.*

Hozirgi kunda veb ilovalarga hujum uyushtirish holatlari ko'payib bormoqda. Chunki veb ilovalar kundan kunga hayotimizdan keng o'rin olib bormoqda va asosiy jarayonlarda ishtirok etmoqda. Shu sababli ham buzg'unchilar veb ilovalarni tez-tez nishonga olishmoqda. Bu hujumlarning asosiy maqsadi albatta bu moliyaviy tomonlama foyda ko'rishdir. Ba'zi hujumchilar veb ilovalardagi foydalanuvchilarning shaxsiy ma'lumotlarini sotish orqali pul ishlashsa, yana boshqa birlari aynan shu veb ilovalarni faoliyatini izdan chiqarish tahdidi orqali shu ilova egalaridan pul undirmoqchi bo'lishi mumkin. Bundan tashqari hujumlar shaxsiy ziddiyatlar ortidan kelib chiqishi ham mumkin. Umuman olganda veb ilovalarga bo'ladigan hujumlar veb ilova hamda uning egalarining obro'sizlanishiga, moliyaviy va ma'naviy zararlarga olib kelishi mumkin. Keling bugungi kundagi web ilovalarga bo'ladigan asosiy hujumlarga qisqacha to'xtalamiz. Bu hujumlar quyidagilar:

Saytlararo skriptlash (XSS): Bu tajovuzkorning veb-saytingizga zararli skript kodini yuklashini o'z ichiga oladi, undan keyin ma'lumotlarni o'g'irlash yoki boshqa turdagi buzg'unchiliklarni amalga oshirish uchun foydalanish mumkin. Garchi bu strategiya nisbatan murakkab bo'lmasa-da, u juda keng tarqalgan bo'lib qolmoqda va katta zarar etkazishi mumkin. Birgina 2022 yilgi sinovlarda topilgan yuqori xavfli zaifliklarning 19 foizi saytlararo skript hujumlari bilan bog'liq ekanligi bu kabi hujumning qanchalik ommalashganligiga bir isbot bo'ladi.

SQL Injection (SQLI): Bu xaker buzg'unchi kodni kiritish shakliga yuborganda sodir bo'ladi. Agar sizning tizimlaringiz ushbu ma'lumotni tozalay olmasa, ular ma'lumotlar bazasiga yuborilishi, ma'lumotlarni o'zgartirishi, o'chirishi yoki tajovuzkorga oshkor etilishi mumkin.

Saytlararo so'rovlarni qalbakilashtirish (CSRF): CSRFlar tajovuzkor oxirgi foydalanuvchini autentifikatsiya qilingan ilovada istalmagan harakatlarni bajarishga majburlaganda yoki aldaganda paydo bo'ladi. Bu elektron pochta yoki chat orqali havola orqali amalga oshirilishi mumkin va agar muvaffaqiyatli bo'lsa, masalan, pul o'tkazilishi yoki elektron pochta manzilining o'zgarishiga olib kelishi mumkin.

XML tashqi ob'ekti (XXE): Bu hujum dastur kodidagi noto'g'ri sozlangan XML tahlilchisiga tayanadi. Ushbu hujum parollar, xizmat ko'rsatishni rad etish, server tomonidan so'rovlarni soxtalashtirish va boshqa tizim ta'siri kabi maxfiy ma'lumotlarning oshkor etilishiga olib kelishi mumkin.

DDoS hujumlari: Bu hujumlar tajovuzkor serverni veb-so'rovlar bilan bombardimon qilganda sodir bo'ladi. Hujumchilar ushbu hujumni o'rnatish uchun buzilgan kompyuterlar yoki botlar tarmog'idan foydalanishi mumkin, bu esa serverni falaj qilishi va qonuniy tashrif buyuruvchilarning sizning xizmatlaringizga kirishiga to'sqinlik qilishi mumkin.

Bu hujumlarning natijasi anchagina jiddiy bo’lishi mumkin. Shu sababli ham veb ilova ma’murlari bunga juda ehtiyot bo’lishlari va oldini olish choralarini ko’rishi kerak. Biz ham ba’zi birlmachi choralarni keltirib o’tdik. Bu chora-tadbirlar biroz bo’lsada veb ilovalarga bo’ladigan hujumlarni oldini olishga yordam berishi mumkin:

Avtomatlashtirilgan zaifliklarni skanerlash va xavfsizlik testi: Kiber hodisa bilan yakunlanishi mumkin bo'lgan zaifliklarni aniqlash, tekshirish va hal qilishda yordam beradigan ushbu echimlarni ko'rib chiqing.

Veb-ilovalar xavfsizlik devorlari (WAFs): Ular dastur qatlamida ishlaydi va ilovalarga kirishni cheklash uchun ma'lum bo'lgan buzilish taktikalari haqida qoidalar va ma'lumotlardan foydalanadi. Ular barcha qatlamlar va protokollarga kirishlari mumkinligi sababli, WAFlar resurslarni hujumdan himoya qilishda juda samarali darvozabon bo'lishi mumkin.

Xavfsiz ishlab chiqish testi (SDT): Bu sinovchilar, ishlab chiquvchilar, arxitektorlar va menejerlarni o'z ichiga olgan barcha xavfsizlik guruhi a'zolari uchun mo'ljallangan. Buzg'unchilar foydalanadigan yangi usullar batafsil tavsiflangan va bu ishchi guruhga veb-sayt hujumlarining oldini olish va buzilishlarni katta ta'sir ko'rsatishni cheklash uchun mumkin bo'lgan yondashuvni topishga yordam beradi.

Xulosa.

Shunday qilib hozirgi kunda hayotimizda veb ilovalarning ahamiyati beqiyos. Bizdagi xizmat ko’rsatish jarayonlari deyarli to’liq elektron ko’rinishga o’tib bo’ldi va veb ilovalar orqali amalga oshirilyapti. Shu sababli ham biz muhim shaxsiy ma’lumotlarimizni bu ilovalar bilan bo’lishishga majbur bo’lamiz. Shu sababli ham

veb ilovalarning hujumlarga bardoshliligi biz uchun juda muhimdir. Yuqoridagi hujum turlari va ularni oldini olishning birlamchi choralaridan xabardor bo'lish biz duch kelishimiz mumkin bo'lgan holatlarda bizga yordam berishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. https://trustnetinc.com/web-application-attacks/
2. https://www.synopsys.com/blogs/software-security/why-cross-site-scripting-still-matters.html
3. https://www.mimecast.com/blog/web-application-attacks/