SQL INJECTION (TUZILGAN SO‘ROVLAR TILI)

A.B.Xurramov
M.J.Safarova
Toshkent amaliy fanlar universiteti o‘qituvchisi, Toshkent, O‘zbekiston.
Z.A.Inomova
Toshkent amaliy fanlar universiteti talabasi, Toshkent, O‘zbekiston.

Annotatsiya: *Ushbu maqolada ma’lumotlar ba’zasi bilan ishlashda SQL Injection vazifasi va ishlashi haqida bilib olish mumkin.*

Kalit so‘zlar: *SQL, SQL Injection, Proofpoint, Injection xatoliklarni aniqlash.*

SQL Injection qanday ishlaydi

SQL Injection ilovaning SQL ma'lumotlar bazasi bilan o‘zaro ta'siridan foydalanadi. Bu erda SQL Injection qanday ishlashi haqida qisqacha ma'lumot:

- So‘rovlar qurilishi: Ilovalar odatda ma'lumotlar bazalari bilan o‘zaro ishlash, odatda ma'lumotlarni olish yoki saqlash uchun SQL so‘rovlaridan foydalanadi. Ushbu so‘rovlar ba'zan foydalanuvchi kiritishidan keladigan satr qismlari bilan qatorlarni birlashtirish yoki ulash orqali tuzilishi mumkin.
- Zararli kiritish: Agar ilova foydalanuvchi kiritishini to‘g‘ri bajarmasa, tajovuzkor SQL kodi bilan kiritishni ta’minlashi mumkin. Ilova ushbu kirishni oddiy ma'lumot sifatida tan olish o‘rniga, ma'lumotlar bazasi uni SQL so‘rovining bir qismi sifatida bajaradi.
- Manipulyatsiya qilingan so‘rovlar: Zararli kiritish SQL so‘roviga birlashtirilganda, so‘rovning tuzilishi yoki maqsadini o‘zgartiradi. Bu tajovuzkorga ruxsatsiz ma'lumotlarni olish, autentifikatsiyani chetlab o‘tish yoki hatto ma'lumotlar bazasida ma'muriy operatsiyalarni bajarishga imkon beradi.

SQL in'ektsion hujumining muvaffaqiyati ko‘p jihatdan dastur o‘zining SQL so‘rovlarini qanday qurishiga va foydalanuvchi kiritishini qanday boshqarishiga bog‘liq. Kirishni tozalash va tasdiqlash bo‘yicha tegishli choralar ushbu zaifliklarning oldini olishga yordam beradi.

SQL so‘rovlari nima?

SQL relyatsion ma'lumotlar bazasini boshqarish tizimida (RDBMS) saqlanadigan ma'lumotlarni boshqarish yoki relyatsion ma'lumotlar oqimini boshqarish tizimida (RDSMS) oqimlarni qayta ishlash uchun standart dasturlash tilidir. Oddiy qilib aytganda, bu ma'lumotlar bazasidan ma'lumotlarni saqlash, yangilash, o‘chirish, qidirish va olish uchun ishlatiladigan deklarativ dasturlash tili.

SQL so‘rovlari - bu relyatsion ma'lumotlar bazalari bilan o‘zaro ishlash uchun Strukturalangan so‘rovlar tilida yozilgan tuzilgan buyruqlar yoki ko‘rsatmalar. Ushbu so‘rovlar foydalanuvchilarga ma'lumotlar bazasida saqlangan ma'lumotlar ustida turli xil operatsiyalarni bajarishga imkon beradi, masalan, ma'lumotlarni olish, kiritish, yangilash va o‘chirish.

SQL so‘rovlari ma'lumotlar bazasida keng ko‘lamli maxsus funktsiyalarni bajarishi mumkin, jumladan:

- Ma'lumotlar bazasidan ma'lumotlarni olish
- Ma'lumotlar bazasiga yozuvlarni qo‘shish, yangilash yoki o‘chirish
- Butunlay yangi ma'lumotlar bazalarini yarating
- Ma'lumotlar bazasida yangi jadvallar yarating
- Ma'lumotlar bazasida saqlangan protseduralarni o‘rnatish
- Ma'lumotlar bazasida ko‘rinishlarni yaratish
- Jadvallar, protseduralar va ko‘rinishlarga ruxsatlarni o‘rnating

SQL so‘rovlari bayonotlar sifatida tuzilgan maxsus buyruqlardir. Ular foydalanuvchilarga ma'lumotlar bazalaridan ma'lumotlarni qo‘shish, o‘zgartirish yoki olish imkonini beruvchi dasturlarga birlashtirilgan.

SQL so‘rovlarining bir nechta asosiy misollari quyidagilarni o‘z ichiga oladi:

❖ SELECT: Jadvallardan ma'lumotlarni olish uchun mo‘ljallangan. 1-ustun, 2-ustunni TANLASH jadval nomidan WHERE sharti;

❖ INSERT INTO: Jadvalga yangi ma'lumotlarni kiritish uchun mo‘ljallangan. INSERT INTO jadval nomi (ustun1, ustun 2) VALUES (qiymat1, qiymat2);

❖ YANGILASH: Jadvaldagi mavjud ma'lumotlarni o‘zgartirish uchun mo‘ljallangan.

YANGILANISh jadval nomi SET ustuni1=qiymat1 WHERE sharti;

Bular SQL so‘rovlarining asosiy misollari. Oddiy ma'lumotlarni qidirishdan tortib murakkab ma'lumotlarni o‘zgartirish va tahlil qilishgacha bo‘lgan imkoniyatlarga ega, SQL kuchli va ko‘p qirrali til bo‘lib, murakkab operatsiyalar va relyatsion ma'lumotlarni manipulyatsiya qilish imkonini beradi.

SQL Injection turlari

SQL in'ektsiya zaifliklari keyingi SQL operatsiyalariga ta'sir qiluvchi zararli SQL kodlari kiritish maydonlariga kiritilganda paydo bo‘ladi. Ushbu tahdidlarni uchta toifaga bo‘lish mumkin: In-band SQLi, Inferential SQLi va Out-of-band SQLi.

1. In-band SQLi

Bu SQL Injectionning eng keng tarqalgan va sodda shakli. In-band SQLi jinoyatchiga zararli kodni kiritish va xuddi shu vosita orqali fikr-mulohaza olish imkonini beradi. Tarmoqli SQL Injectionning eng keng tarqalgan ikkita turi - bu xatoga asoslangan SQLi va ittifoqqa asoslangan SQLi.

Xatoga asoslangan SQLi

So‘rovlarni manipulyatsiya qilish orqali tajovuzkorlar serverning xato xabarlaridan qimmatli ma'lumotlar bazasi ma'lumotlarini ajratib olishadi. Ba'zan, bu usul hatto to‘liq ma'lumotlar bazasini xaritalashi mumkin.

Ittifoqqa asoslangan SQLi

Ushbu texnika UNION SQL operatoriga bog‘liq. Buzg‘unchilar bir nechta SELECT operatsiyalari natijalarini birlashtiradi va birlashtirilgan ma'lumotlar ilovaning javobida aks etadi.

2. Inferensial SQLi

Inferential SQL Injection, tarmoq ichidagi SQL Injectiondan farqli o‘laroq, tajovuzkorning ekspluatatsiyasi uchun ko‘proq vaqt talab qilishi mumkin, ammo u hali ham juda samarali bo‘lishi mumkin. Ushbu turdagi hujumda veb-ilova orqali hech qanday ma'lumot o‘tkazilmaydi va tajovuzkor tarmoq ichidagi hujum natijasini ko‘ra olmaydi (ya'ni, ilova javobining HTML-da). Shu bilan bir qatorda, tahdid ishtirokchilari foydali yuklarni yuborish va veb-ilovaning javobini va ma'lumotlar bazasi serverining xatti-harakatlarini kuzatish orqali ma'lumotlar bazasi strukturasini qayta qurishlari mumkin. Inferentsial SQLi ning ikkita asosiy shakli bu ko‘r-boolean-asoslangan SQLi va ko‘r-vaqtga asoslangan SQLi.

Ko‘r-mantiqiy asoslangan SQLi

Mantiqiy asosga asoslangan SQL Injection ma'lumotlar bazasiga SQL so‘rovini yuborish va so‘rovning TRUE yoki FALSE qaytishiga qarab dasturni boshqa javob berishga majburlash orqali ishlaydi.

Ko‘r vaqtga asoslangan SQLi

Vaqtga asoslangan SQL Injection - bu ma'lumotlar bazasiga SQL so‘rovini yuboradigan, javob berishdan oldin dasturni ma'lum vaqtni (soniyalarda) kutishga majbur qiladigan SQL Injection usuli.

3. Tarmoqdan tashqari SQLi

Tarmoqdan tashqari SQL injection juda keng tarqalgan emas, chunki u maqsadli ma'lumotlar bazasi tajovuzkorning mashinasiga qayta ulanishini talab qiladi. Ushbu turdagi SQL Injection tajovuzkor hujumni boshlash va natijalarni yig‘ish uchun bir xil kanaldan foydalana olmaganida yuzaga keladi. Buning o‘rniga, tajovuzkor hujumni boshlash uchun elektron pochta kabi boshqa kanaldan foydalanadi.

Xulosa qilib aytadigan bo‘lsak, tarmoq ichidagi SQLi eng keng tarqalgan va ulardan foydalanish oson, Inferential SQLi esa tajovuzkordan foydalanish uchun ko‘proq vaqt talab qilishi mumkin, ammo baribir juda samarali bo‘lishi mumkin. Tarmoqdan tashqari SQLi juda keng tarqalgan emas, chunki u maqsadli ma'lumotlar bazasi tajovuzkorning mashinasiga qayta ulanishini talab qiladi.

SQL injection misoli

SQL in'ektsiyalari murakkab hujumlar bo‘lishi mumkin bo‘lsa-da, bu soddalashtirilgan misol ularning qanday ishlashini ko‘rsatadi.

Faraz qilaylik, ikkita ma'lumotlar bazasi jadvali mavjud: Foydalanuvchilar loginlari va Mijoz ma'lumotlari. Foydalanuvchi loginlari jadvalida foydalanuvchi nomi va parol uchun ikkita maydon mavjud. Mijoz ma'lumotlari jadvalida ism, familiya, manzil, elektron pochta, telefon raqami va kredit karta raqami kabi qo‘shimcha ma'lumotlar mavjud.

Buzg‘unchi foydalanuvchi loginlari jadvalidan foydalanuvchining foydalanuvchi nomi va parolini olish uchun login formasiga zararli kodni kiritishi mumkin. Agar tajovuzkor foydalanuvchi nomi maydoniga quyidagi kodni kiritsa,

' YOKI 1=1 --

Keyin bajarilgan SQL bayonoti quyidagicha ko‘rinadi:

Foydalanuvchi nomi = '' YOKI 1=1 --' VA parol = '' QAYERDAGI foydalanuvchilar orasidan * TANLANING

Bayonot oxiridagi qo‘sh chiziqcha asl SQL bayonotining qolgan qismini sharhlash uchun ishlatiladi, bu esa parolni ham tekshiradi.

Yuqoridagi gap har doim to‘g‘ri bo‘ladi, chunki 1=1 har doim to‘g‘ri bo‘ladi va qo‘sh chiziqcha gapning qolgan qismini izohlaydi. Natijada, parolni tekshirish e'tiborga olinmaydi va tajovuzkor haqiqiy parolsiz tizimga kirishi mumkin.

SQL injection hujumining ta'siri.

SQL inyeksion hujumlari tajovuzkorning malakasi, niyati va tizim zaifligiga qarab turli oqibatlarga olib kelishi mumkin. Ruxsatsiz kirishga erishilganda, SQLi hujumlarining mumkin bo‘lgan ta'siri quyidagilarni o‘z ichiga oladi:

• Ma'lumotlarning buzilishi : SQLi ning eng tezkor va zararli ta'siridan biri bu ma'lumotlar bazasi yozuvlariga ruxsatsiz kirishdir. Buzg‘unchilar foydalanuvchi hisob ma'lumotlari, shaxsiy ma'lumotlar, moliyaviy ma'lumotlar va boshqalar kabi nozik ma'lumotlarni ko‘rishlari mumkin.

• Ma'lumotlarning yo‘qolishi yoki buzilishi : Zararli shaxslar yozuvlarni o‘zgartirishi, kiritishi va o‘chirishi mumkin, bu esa ma'lumotlar yaxlitligini yo‘qotishi, ma'lumotlarni foydasiz qilishi yoki noto‘g‘ri ma'lumotlarni kiritishi mumkin.

• Xizmatni rad etish : Yozuvlarni bloklash, jadvallarni o‘chirish yoki ma’lumotlar bazasini boshqa yo‘l bilan buzish orqali tajovuzkorlar ilovani qonuniy foydalanuvchilar uchun mavjud bo‘lmasligi mumkin.

• Ma'lumotlar bazasi serverini egallab olish : Kengaytirilgan SQLi hujumlari tajovuzkorlarning ma'lumotlar bazasi serveri ustidan nazoratni qo‘lga kiritishiga olib kelishi mumkin. Ma'lumotlar bazasi serveri tarmoqning qolgan qismidan to‘g‘ri ajratilmagan hollarda, bu keyingi murosaga erishish uchun qadam bo‘lishi mumkin.

• Masofaviy kodni bajarish : Ba'zi ma'lumotlar bazasi tizimlari SQL orqali tizim darajasidagi buyruqlarni bajarishga imkon beradi. Agar tajovuzkor bunday tizimlarda SQLi zaifligini aniqlasa va undan foydalansa, ular serverda o‘zboshimchalik bilan buyruqlarni bajarishi mumkin, bu esa tizimning to‘liq buzilishiga olib keladi.

• Ma'lumotlarga ta'sir qilish : Buzg‘unchilar SQLi-dan ilovaning xatti-harakatlarini o‘zgartirish uchun foydalanishi mumkin, bu esa odatda foydalanuvchilar uchun ochiq bo‘lmagan maxfiy ma'lumotlarni oshkor qilishi mumkin.

• Shaxsni o‘g‘irlash va firibgarlik : Shaxsiy va moliyaviy ma'lumotlarga kirish orqali tajovuzkorlar shaxsni o‘g‘irlash , ruxsatsiz tranzaktsiyalar va boshqa firibgarlik faoliyatini amalga oshirishi mumkin.

• Obro‘ga putur etkazish : To‘g‘ridan-to‘g‘ri texnik ta'sirlardan tashqari, SQLi hujumlari qurboni bo‘lgan kompaniyalar jiddiy obro‘ga putur etkazadi. Mijozlar va hamkorlar kompaniyaning o‘z ma'lumotlarini himoya qilish qobiliyatiga ishonchini yo‘qotishi mumkin.

• Moliyaviy oqibatlar : SQLi hujumidan keyin tozalash qimmatga tushishi mumkin. Texnik tuzatish, huquqiy maslahatlar, jamoatchilik bilan aloqalar bo‘yicha harakatlar, zarar ko‘rgan foydalanuvchilarga kompensatsiya to‘lash va ma'lumotlarni himoya qilish qoidalarini buzganlik uchun jarimalar bilan bog‘liq xarajatlar bo‘lishi mumkin.

• Intellektual mulkni oshkor qilish : Korxonalar xususiy algoritmlarni, biznes rejalarni va boshqa intellektual mulkni o‘z ma'lumotlar bazalarida saqlashi mumkin. SQLi hujumi ushbu qimmatli ma'lumotlarning o‘g‘irlanishiga olib kelishi mumkin.

SQLi ning potentsial ta'sirini tushunish xavfsiz kodlash amaliyotlarini qo'llash, zaiflikni muntazam ravishda baholash va ma'lumotlar bazalari va ilovalarni bunday tahdidlardan himoya qilish uchun kirish testlarini o'tkazish muhimligini ta'kidlaydi.

SQL qarshi hujumlarining oldini olish va aniqlash.

SQL in'ektsion hujumlarining oldini olish va aniqlash xavfsiz kodlash, infratuzilmani mustahkamlash, monitoring va ta'limning kombinatsiyasini talab qiladi. Bu erda SQL qarshi hujumlarining oldini olish va aniqlash bo'yicha eng yaxshi amaliyotlar:

Oldini olish

• Parametrlangan so'rovlardan foydalaning (tayyorlangan bayonotlar) : SQL bilan har doim parametrlangan so'rovlar yoki tayyorlangan bayonotlardan foydalaning. Bu foydalanuvchi kiritgan ma'lumotlar har doim ma'lumot sifatida va hech qachon bajariladigan kod sifatida ko'rilmasligini ta'minlaydi.

• Saqlangan protseduralardan foydalaning : Saqlangan protseduralardan foydalanib, siz SQL-ning xom buyruqlariga ta'sir qilishni cheklab, ma'lumotlarga kirishni mavhumlashtirishingiz va markazlashtirishingiz mumkin.

• ORM (Ob'ekt bilan bog'liq xaritalash) : ORM lardan foydalaning, chunki ular ko'pincha parametrlangan so'rovlarga asoslanadi va xom SQL bilan to'g'ridan-to'g'ri ishlov berishni kamaytiradi, lekin tanlangan ORM ning SQLi ga qarshi xavfsizligini ta'minlang.

• Barcha foydalanuvchi kiritishidan qochish : Agar siz to'g'ridan-to'g'ri SQL so'rovlariga ma'lumotlarni kiritishingiz kerak bo'lsa, barcha foydalanuvchi kiritgan ma'lumotlar to'g'ri chiqib ketganligiga ishonch hosil qiling. Bu zaxira chorasi bo'lishi mumkin, lekin bu asosiy himoya bo'lmasligi kerak.

• Eng kam imtiyoz printsipi : Veb-ilovalar tomonidan ishlatiladigan SQL ma'lumotlar bazasi hisoblari minimal zarur imtiyozlarga ega ekanligiga ishonch hosil qiling. Misol uchun, ma'lumotlarni oladigan foydalanuvchi hisobi kiritish yoki o'chirish ruxsatiga ega bo'lmasligi kerak.

• Veb-ilovalar xavfsizlik devorlari (WAFs) : Veb-ilova va Internet o'rtasidagi HTTP trafigini filtrlash va kuzatish uchun WAF-ni o'rnating. WAF ko'plab in'ektsiya hujumlarini bloklashi mumkin.

• Batafsil xato xabarlarini o'chirib qo'ying : Ma'lumotlar bazasi xato xabarlari umumiy ekanligiga ishonch hosil qiling va ma'lumotlar bazasi tuzilmasi haqida ma'lumotlar sizib chiqmasligiga ishonch hosil qiling.

• Kirishni tekshirish : Kirishni tekshirish uchun oq ro'yxat yondashuvidan foydalaning. Barcha foydalanuvchi ma'lumotlarini qat'iy qoidalar to'plamiga (masalan, tur, uzunlik, format va diapazon) muvofiq tasdiqlang.

• Muntazam ravishda yangilash va tuzatish : ma'lum zaifliklardan himoya qilish uchun ma'lumotlar bazasi dasturlarini, veb-ilovalar ramkalarini va kutubxonalarni muntazam yangilab turing.

Aniqlash

➢ Muntazam xavfsizlik tekshiruvlari va kirish testlari : Vaqti-vaqti bilan potentsial zaifliklarni aniqlash va tuzatish uchun xavfsizlik auditlari va kirish testlarini o'tkazing.

- SQL so‘rovlarini monitoring qilish : SQLi urinishlarini ko‘rsatishi mumkin bo‘lgan noodatiy yoki kutilmagan so‘rovlarni aniqlash uchun ma'lumotlar bazasiga nisbatan bajarilgan SQL so‘rovlarini kuzatib boring.
- Xato monitoringi : Hujum urinishlarini ko‘rsatishi mumkin bo‘lgan noodatiy tizim yoki dastur xato xabarlarini kuzatib boring.
- Intrusion Detection Systems (IDS): IDS yechimlarini zararli harakatlarni kuzatish va ogohlantirish uchun joylashtiring.
- Jurnal monitoringi va tahlili : Jurnallarni muntazam ravishda ko‘rib chiqing va hujumlar belgilarini aniqlash uchun avtomatik jurnal tahlilidan foydalaning.
- Ma'lumotlar bazasi yaxlitligini tekshirish : Ruxsatsiz o‘zgartirishlarni aniqlash uchun joriy ma'lumotlar bazasi tuzilmalari va tarkibini ma'lum yaxshi zaxira nusxasi yoki asosiy chiziq bilan muntazam ravishda solishtiring.
- Dasturchilar va IT xodimlarini o‘rgating : Barcha jamoa a'zolari SQLi xavflari va oldini olish usullarini bilishlariga ishonch hosil qiling.
- Honeypots : yangi SQLi usullarini aniqlashga yordam beradigan tajovuzkorlarni yo‘naltirish va o‘rganish uchun ma'lumotlar bazasi honeypotlarini o‘rnating.

Oldini olish va aniqlash mexanizmlarini o‘z ichiga olish va proaktiv xavfsizlik holatini saqlab qolish SQL Injection va boshqa tahdidlardan samarali himoyalanish uchun juda muhimdir.

Proofpoint qanday yordam berishi mumkin

Proofpoint SQL inyeksion hujumlariga qarshi kurashishda yordam beradigan sanoatning yetakchi kiberxavfsizlik yechimlarini taqdim etadi. Kompaniyaning ushbu sohadagi ba'zi echimlari quyidagilarni o‘z ichiga oladi:

• Insider Threat Management (ITM) : Proofpoint’ning keng qamrovli ITM yechimlari tashkilotlarga maxfiy ma’lumotlarni ichki tahdidlar va ma’lumotlar yo‘qolishidan himoya qilishga yordam beradi. U foydalanuvchi faoliyatining chuqur ko‘rinishini ta'minlaydi, foydalanuvchi xavfini aniqlaydi, ichki ma'lumotlarning buzilishini aniqlaydi va xavfsizlik hodisalariga javob berishni tezlashtiradi.

• Kengaytirilgan tahdidlardan himoyalanish (ATP) : Proofpoint-ning takomillashtirilgan ATP xizmati nol kunlik qarshi hujumlarini to‘xtatish uchun ichki imkoniyatlarni o‘z ichiga oladi.

• Rivojlanayotgan tahdidlar razvedkasi : Proofpoint-ning paydo bo‘layotgan tahdid razvedkasi yechimlari tahdid ishtirokchilari tomonidan o‘tkaziladigan eng so‘nggi taktikalar, texnikalar va tartiblarni ko‘rish imkonini beradi.

Xulosa. SQL Injection (ko‘pincha SQLi deb qisqartiriladi) - bu SQL (Structured Query Language) ma'lumotlar bazalaridan foydalanadigan ilovalarga qaratilgan kiber tahdid. Buzg‘unchilar so‘rovlarga zararli SQL kodini kiritish orqali ilova kodidagi zaifliklardan foydalanadi, bu ularga potentsial qimmatli ma'lumotlarni o‘z ichiga olishi mumkin bo‘lgan shaxsiy ma'lumotlar bazasiga ruxsatsiz kirish imkonini beradi.

SQL in'ektsiya hujumi turli xil salbiy oqibatlarga olib kelishi mumkin, jumladan ma'lumotlarning buzilishi , ma'lumotlarning buzilishi va tizim boshqaruvining yo‘qolishi. Ushbu kiber-hujumlar SQL ma'lumotlar bazasidan foydalanadigan har qanday

dasturni nishonga oladi, veb-saytlar eng zaif va tez-tez ekspluatatsiya qilinadigan maqsadlardir.

FOYDALANILGAN ADABIYOTLAR:

1.https://www.proofpoint.com/us/threat-reference/sql-injection
2. https://www.proofpoint.com/us/products/advanced-threat-protection/et-intelligence
3. https://portswigger.net/web-security/sql-injection
4. Z.M.Adizova, A.A.Avezov, F.F.Norova “Ma’lumotlar bazasi” Buxoro 2022.
5. J.T.Usmonov, “Ma’lumotlar boshqarish tizimi”. Toshkent 2016.