O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Dasturiy vositalar xavfsizligi

Mavzu: SQL ineksiya tahdidi va undan himoyalanish usullari.

MUSTAQIL ISH

Bajardi: Abdullayev R.

Tekshirdi: Olimov I.

Toshkent-2024

Mundarija

Kirish

Veb-ilovalar kundalik hayotimizning ajralmas qismiga aylandi. Veb-ilovalar bugungi kunda keng tarqalgan, chunki ular kundalik hayotning zaruriyatiga aylangan. Har kuni sodir bo'ladigan minglab xavfsizlik buzilishlari mavjud. Bagchi ma'lumotlariga ko'ra, firma veb- saytlari va veb-ilovalarining 75% Internet xavfsizligi buzilishiga qarshi himoyasiz edi. U Gompertz modeli orqali Internet xavfsizligi buzilishining o'sishini va hujumga duchor bo'lishini tahlil qildi. Internetdagi eng keng tarqalgan hujum SQL Injection orqali amalga oshiriladi. Klassik SQL in'ektsiyalarining oldini olish va aniqlash oson edi, shuningdek, SQL in'ektsiyalarini engish uchun ko'plab protseduralar, metodologiyalar muhokama qilindi.

Ushbu ilovalarning ko’pchiligida ularning faoliyatiga jiddiy zarar yetkaziadigan veb zaifliklarga ega bo’lishi mumkin. Ushbu holatlar yuzasidan kelib chiqib butun jaxon axborot xafsizligi soha vakillari veb ilovalar xafsizlik chora tadbirlarini ko’rishga turli qarorlar va farmoishlar qo’llashgan. Jumladan, O’zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi PF 60-sonli farmoni bilan tasdiqlangan ―2022–2026-yillarga mo’ljallangan Yangi O’zbekistonning taraqqiyot strategiyasi to’g’risida‖gi 89-maqsad: Fuqarolarning axborot olish va tarqatish erkinligi borasidagi huquqlarini yanada mustahkamlash.

Kiberjinoyatchilikning oldini olish tizimini yaratish bo’yicha ustuvor vazifalarni bajarish belgilangan. Veb ilova zaifliklarni aniqlashga umumiy yondashuvlar Veb ilovalarini aniqlovchi skanerlarning samaradorligini baholashdan avval veb ilovalar zaifliklari haqida asosiy tushunchaga ega bo’lish juda muhimdir. Ushbu tadqiqot ishida veb-ilovalar zaifligining eng muhim sinov holatlarini amalga oshiradigan OWASP benchmark 2021 versiyasidan foydalanilgan. Har xil turdagi ineksiyalar, sessiyalarni boshqarish va autentifikatsiya buzilishi, saytlararo skriptlash, kirishlarni boshqarishning yetishmovchiligi, saytlararo so‘rovlarni

soxtalashtirish, xavfsizlikni noto‘g‘ri sozlash, himoyalanmagan API’lar, hujumdan himoyalanishning yetarli emasligi va ma’lum zaifliklarga ega komponentlardan foydalanishlar va bunga misollar. Biz quyida ba’zi muhim zaifliklarni keltirib o’tamiz: Cross-site Scripting (XSS) - bu zararli skriptni ilovaga kiritishni o’z ichiga olgan ineksiya hujumi. Ushbu turdagi hujum g’arazgo’y shaxs zararli skriptni brauzer Agar hujum muvaffaqiyatli bo’lsa, g’arazgo’y shaxs jabrlanuvchining kirish huquqlariga ega bo’ladi. Natijada, agar jabrlanuvchi dastur ichidagi kritik ma’lumotlarga kirish imkoniga ega bo’lsa, bu jiddiy zaiflikdir. Afsuski, bunday hujumlarning muvaffaqiyatli bo’lishiga imkon beruvchi zaifliklar hamma joyda mavjud ekanligi ta’kidlangan. Zaiflik skanerlari saytlararo skriptlarning ba’zi zaifliklarini avtomatik ravishda aniqlashi mumkin bo’lsa-da, turli veb-dasturlar Flash, JavaScript, Silverlight va ActiveX kabi turli interpreterlardan foydalanadi, bu esa avtomatik aniqlashni qiyinlashtiradi. Mirrored or Non-Persistent XSS, ekspluatatsiya veb-ilovaga yuborilganda va keyin uni bajarish uchun maqsadli brauzerda aks ettirilganda sodir bo’ladi. Ushbu hujumni amalga oshirishning eng odatiy usullaridan biri zararli kontentni URL manzilida parametr sifatida taqdim etishdir. Veb zaifliklarni zaiflik skanerlari yordamida aniqlash Veb-ilovalarda zaifliklar aksariyat holatlarda uchrab turadi. Shu sababli, zaiflik skanerlari ilovalardagi uchrab turuvchi zaifliklarni aniqlash uchun ishlatiladi, shunda ularni minimallashtirish yoki yo’q qilish imkoniyati mavjud bo’ladi. Skanerning aniqligi va samaradorligi har doim ham benuqson emas va hamma skanerlar ham foydalanuvchi uchun qulay bo’lavermaydi .

Web servise larda uchraydigan zaifliklar turlari

1.1.Web sahifalarda bo`lishi mumkin bo‘lgan zaiflik

Veb saytlar xavfsizligini ta'minlashda Open Web Application Security Project(OWASP) tavsiyalariga amal qilish zarurati yuqori bo'lganidan ushbu tavsiyalar ma'lum manoda standartga aylanib ulgirdi. Ushbu maqolamizda tashkilot hozirda veb saytlardagi qaysi 10 ta zaiflikni eng xavfli deb bilishini ko'rib chiqaylik.

Open Web Application Security Project® (**OWASP**) - bu veb saytlar xavfsizligi buyicha turli mualliflik maqolalari, video darsliklar yaratadigan, shuningdek forumlar konferensiyalar o'tkazadagigan onlayn hamjamiyat.

OWASP hamjamiyati dunyo miqyosidagi onlayn hamjamiyat bo'lib korporatsiyalar, ta'lim tashkilotlar va xavfsizlik sohasida faoliyat yuritadigan shaxslardan tashkil topgan.

Hamjamiyatning eng ko'zga ko'ringan loyihalari sifatida OWASP TOP 10 hisoboti, OWASP CLASP va OWASP ZAP veb prototokllari shuningdek veb sahifalarni tekshiruvdan o'tkazish uchun yaratilgan ochiq kodli skanerlarini keltirish mumkin.

OWASP Top 10 — bu hozirda eng keng tarqalgan o'nta veb saytlar zaifliklari ro'yxati. Ushbu ro'yxat tufayli dasturchilar, pentesterlar, xavfsizlik buyicha mas'ul xodimlar eng muhim xavf va tahdidlar, ularning oqibatlari va ularga qarshi choralar haqida o'z vaqtida xabardor bo'lishlari mumkin.

OWASP ro'yxati har uch-to'rt yilda bir marta yangilanadi (u oxirgi marta 2021 yilda yangilangan). OWASP TOP 10 hisoboti butun dunyo bo'ylab xavfsizlik bo'yicha ekspertlarning fikr-mulohazalariga asoslanadi.

OWASPning so‘nggi hisobotida eng xavfli va keng tarqalgan 10 ta zaifliklar ro‘yxati keltirilgan:

1. **Broken Access Control -** Kirish nazorati buzilishi
2. **Cryptographic Failures -** Kriptografik xatolar

3. **Injection -** Inyeksiya hujumlari

4.**Insecure Design -** Ishonchsiz dizayn

5.**Security Misconfiguration -** Notug'ri xavfsizlikkonfiguratsiyasi

6.**Vulnerable and Outdated Components -** Zaif va eskirgan komponentlar

7.**Identification and Authentication Failures -** Identifikatsiya va autentifikatsiyadagi xatolar

8.**Software and Data Integrity Failures -** Dasturiy ta'minot va ma'lumotlar yaxlitligidagi xatolar

9.**Security Logging and Monitoring Failures -** Xavfsizlik jurnali va monitoringdagi nosozliklar

10.**Server-Side Request Forgery -** Server tomoni so'rovini qalbakilashtirish yoki

SSRF (Server-Side Request Forgery)

Broken Access Control -Kirish nazorati buzilishi

Sayt xavfsizligi sohasida kirish nazoratini boshqarish - bu foydalanuvchilarga alohida bo'limlar yoki sahifalarga kirishini cheklash. Misol keltiramiz, deylik sizda internet magazin bor. Saytga yangi mahsulotlarni qo'shish yoki chegirmalarni o'rnatish uchun siz saytning administrator paneliga kirishingiz kerak bo'ladi.

Kirish nazorati bilan bog'liq muammolar xakerga cheklovlarni chetlab o'tib, tizimlar va maxfiy ma'lumotlarga ruxsatsiz kirishga, shuningdek, administrator va imtiyozli foydalanuvchi login parollarini qo'lga kiritish potensil xavfini yuzaga keltiradi.

Buzilgan kirish boshqaruviga misollar:

Xosting boshqaruv paneliga/Admin panelga kirish.

FTP/SFTP/SSH orqali serverga kirish.

Sayt boshqaruv paneliga kirish

Ma'lumotlar bazasiga kirish

2. Cryptographic Failures- Kriptografik xatolar

Kriptografik xatolar-Bu nisbatan yangicha nomlanish bulib oldinki TOP 10 hisobotlarda maxfiy ma'lumotlarni oshkor qilish(Sensitive Data Exposure) nomi bilan atalgan.

Asosiy e'tibor kriptografiya bilan bog'liq nosozliklarga (yoki uning mavjud emasligiga) qaratilgan. Bu ko'pincha maxfiy ma'lumotlarning tarqalib ketishiga ketishiga olib keladi.

Muhim ma'lumotlarning oshkor bo'lish xavfining asosiy sababi shifrlashning yo'qligi yoki kalitlarni yaratish va boshqarishning ishonchsiz usullaridan foydalanish, zaif shifrlash algoritmlari, xavfsiz parollarni saqlash usullari va boshqalar bilan bog'liq. Yana bir sabablaridan biri shundaki bazida dasturchilar zarurat bo'lmaganda ham muhim ma'lumotlarni saqlab boradilar.

Maxfiy ma'lumotlarga misollar

Himoya qilinishi kerak bo'lgan ba'zi maxfiy ma'lumotlar:

- kredit karta raqamlari
- tibbiy ma'lumotlar
- Shaxsiy identifikatsiya qilinadigan ma'lumotlar (PII)

Boshqa shaxsiy ma'lumotlar.

3. Injection- Inyeksiya hujumlari

Inyeksion hujumlar ma'lumotlar kod interpretatoriga saytdagi forma yoki ma'lumotni veb-ilovaga yuborishning boshqa usuli orqali uzatilganda sodir bo'ladi. Masalan, xaker ruyxatdan o'tish formasidagi foydalanuvchidan ism kiritishi suraladigan maydonga SQL kodini kiritishi mumkin.

Agar formadagi kiruvchi ma'lumotlar dasturchi tomonidan to'g'ri tekshirilmasa himoyalanmagan bo'lsa, bu xaker tomonidan yuborilgan SQL kodning

bajarilishiga olib keladi — bunday hujumlar SQL inyektsiya nomi bilan ancha tanilgan.

Inyeksion hujumlarni foydalanuvchi tomonidan taqdim etilgan ma'lumotlarni tekshirish va/yoki tozalash orqali oldini olish mumkin.Birinchi navbatda foydalanuvchi tomonidan junatilayotgan xar bir maydondagi ma'lumotlarni qanday ma'lumot ekanligini tekshirish tug'ridan tug'ri ma'lumotlar bazasiga saqlamaslik kerak.

Inyeksion hujumlar sayt egalari uchun jiddiy xavf tug'diradi.Bu turdagi hujumlarga saytni tekshirish oldini olish buyicha keyingi darslarimizda batafsil gaplashamiz.

4. Insecure Design — Ishonchsiz dizayn

Dizayn kamchiliklari bilan bog'liq xavflarga e'tibor qaratiladigan 2021 yil uchun yangi yunalish.Ishonchsiz dizayn — bu «yo'qolgan yoki samarasiz boshqaruv dizayni» sifatida ifodalangan turli kamchiliklarni ifodalovchi keng kategoriya.

Ishonchsiz dizayn bu dastur ishlashidagi mantiqiy xatoliklar bilan bog'liq xatoliklarni o'z ichiga oladi.

Parollarni ochiq mantda(textda) saqlash.

Xatolik haqidagi xabarlarda muhim ma'lumotlarni ko'rsatib yuborish.

Ma'lumotlar kiritish formasida spam yoki xar xil botlardan himoya interfeysining mavjud emasligi.

5. Security Misconfiguration — Notug'ri xavfsizlik konfiguratsiyasi

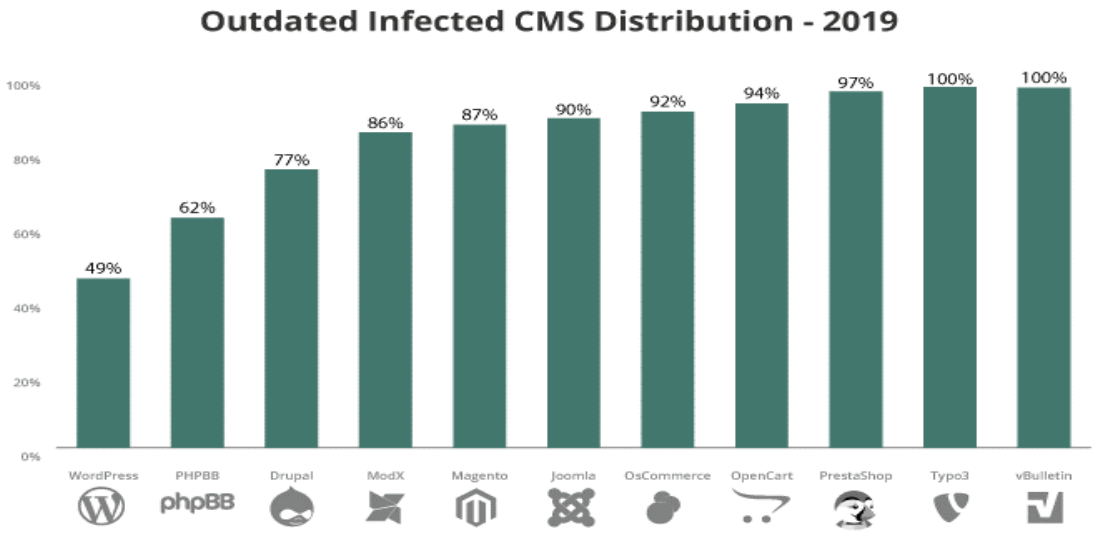
Xavfsizlik konfiguratsiyalarini noto'g'ri sozlash OWASP Top 10 da eng keng tarqalgan zaiflik hisoblanadi.Bu turdagi zaifliklar asosan dasturchilarning sayt xavfsizligiga e'tiborsizligidan kelib chiqadi. Dasturchilar qiladigan eng keng tarqalgan xatolardan biri bu standart CMS sozlamalarini o'zgartirmaslik ya'ni uz holatida saqlash.Veb saytga hujum qilish imkonini beradigan eng keng tarqalgan xatolarni keltirib o'tamiz:

- Tuzatilmagan kamchiliklar;
- Standart konfiguratsiyalar(default);
- Foydalanilmayotgan sahifalar mavjudligi;
- Himoyalanmagan fayllar va kataloglar;
- Zaif xeshlangan yoki shifrlanmagan parollar

Zamonaviy CMS(WordPress,Joomla va boshqalar)lar ishni oson qilishi vaqtni tejashi mumkin,lekin ularning xavfsizlik sozlamalarini o'z holatida qoldirilsa bu oqibati yomon holatlarga olib kelishi mumkin. Hozirgi kunda juda ko'p xakerlik hujumlari avtomatlashtirilgan instrumentlar(tools)lar yordamida amalga oshiriladi.

6. Vulnerable and Outdated Components — Zaif va eskirgan komponentlar

Saytning server va mijoz(client) qismidagi har bir dasturiy ta'minotni yangilamaslik ertami-kechmi jiddiy xavfsizlik xatarlarini keltirib chiqarishini hammamiz tushunamiz. Masalan, 2019 yilda barcha CMS da qilingan saytlarning kiber hujumga uchragan. CMS tizimlaridagi uchragan zaifliklar.



1.1-rasm CMS tizimlaridagi uchragan zaifliklar.

Ya'ni dasturchilar o'z vaqtida pluginlar, modullar yoki frameworklarni yangilanish chiqqan vaqtida yangilashmagan.

Nega biz dasturiy ta'minotni o'z vaqtida yangilamaymiz? Nima uchun bugungi kunda bu juda katta muammo?

Bu savolga bir nechta javoblar keltirish mumkin masalan:

- Dasturchilar yangilanish(updates) chiqqanidan o'z vaqtida xabardor bo'lmaydi yoki yangilashga ulgurmaydi (to'g'ri yangilash vaqt talab etadi).
- Eski kod bog'liqliklar(dependencies)ning yangi versiyalari bilan mos kelmaydi, ishlamaydi.
- Dasturchi yangilanishlarni qilgandan keyin sayt funksionali o'zgarib qolishidan yoki ishlamay qolishidan xavfsiraydi.
- Dasturchilar yangilanishni to'g'ri o'rnatish tajribasiga ega bo'lmasliklari mumkin.

Bu haddan tashqari oddiy tuyulishi mumkin, lekin har safar yangilanish ogohlantirishiga e'tibor bermasangiz, saytingizda yoki serveringizda ma'lum bo'lgan zaiflik saqlanib qolishiga ruxsat berasiz. Menga ishoning, xakerlar serveragi dasturiy ta'minot yoki saytlardagi modullar versiyalarini zaifliklarga albatta tekshirishadi. Muvaffaqiyatli xakerlik hujumlarini aniqlash har doim ham oson emas. Ko'pincha

1.2-rasm Xavfsizlik jurnali va monitoringdagi nosozliklar

Xakerlar nafaqat axborot tizimlariga ruxsatsiz kirishadi, balki xech qanday iz qoldirmagan sezdirmagan holda bir necha oy yoki yillar davomida tizimga ruxsatga ega bo'lib yurishadi.Bazida veb sayt egasi saytining xakerlar tomonidan buzib kirilganini xatto oylab bilmasligi mumkin. Buning oldini olish uchun saytda, serverda yoki tizimda bo'layotgan xar bir xarakatni monitoring,analiz qilib borish xavfsizlik jurnalalrini yuritib kuzatib borish kerak.

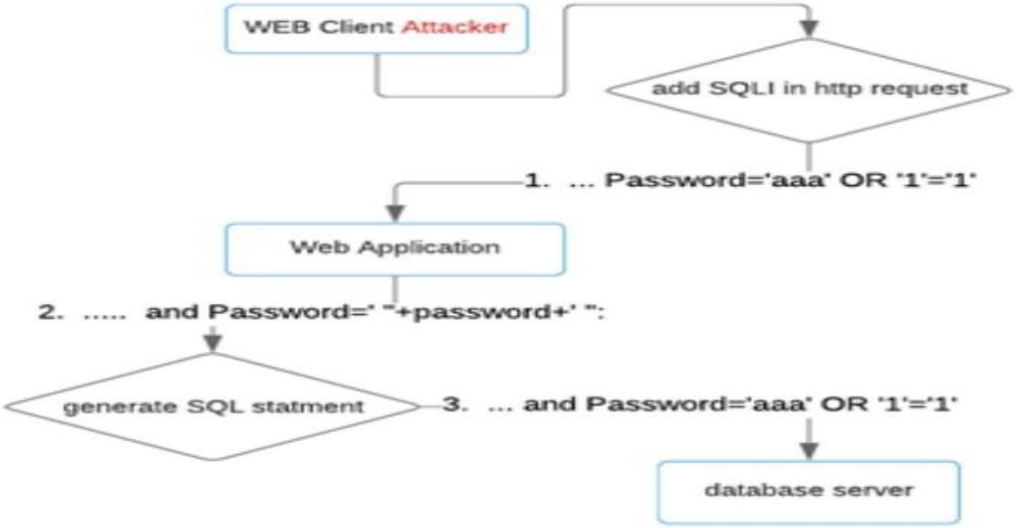
Sayt faoliyatini audit,monitoring qilish,loglar bilan tug'ri ishlash saytingizdagi har qanday shubhali o'zgarishlardan xabardor bo'lish imkonini beradi.Loglar saytdagi barcha hodisalarni qayd etadigan hujjatdir. Bu sizga potensial hujumlarningning oldini olish yoki hujum sodir bo'lganda zudlik aniqlash uning oqibatlarini kamaytirishga yordam beradi.

Server-Side Request Forgery — Server tomonidagi so'rovlarni qalbakilashtirish yoki Server tomonidagi so'rovlarni qalbakilashtirish qisqacha SSRF OWASP TOP 10 ning yangilangan 2021 yidlagi ruyxatiga hamjamiyat so‘rovidan keyin qushildi. Bu turdagi hujum so'ngi yillarda nisbatan ko'p uchramoqda buni quyidagi statistikadan ham ko'rish mumkin.

SQL Injection Attack, tajovuzkor ma'lumotlarni olish yoki buzish uchun mo'ljallangan Web Application ma'lumotlar bazasiga zararli kodni kiritishga harakat qilganda sodir bo'ladi. Bundan tashqari, ushbu hujumlar E-tijorat veb-saytlarida kredit karta raqamlarini olish uchun ishlatiladi yoki autentifikatsiyani chetlab o'tish uchun keng qo'llaniladi. Su va Wassermann SQL Injection-ni batafsil va rasmiy ravishda kod kiritish bo'yicha tushuntirishlar bilan bir qatorda SQL Check yordamida tekshirishni tasvirlab beradi.

SQL Injection hujumidan dastlabki himoya kirishni tekshirish edi, bunda foydalanuvchiga maxsus belgilarni kiritishga ruxsat berilmagan. Bir necha yillar davomida texnologiya rivojlangan va hujumchilar inyeksiya hujumlarini

qo'zg'atish uchun yanada murakkab va murakkab usullardan foydalanishga o'tishgan. Mualliflari SQL Injection hujumlarining fon tarixini tushuntiradi.



1.3-rasm. SQL injection hujumi amalga oshirish jarayoni.

Uilyam va boshqalar tomonidan belgilangan ro'yxat cheklangan, ammo SQL Injection hujumi qayerdan va qanday sodir bo'lishi haqida aniq fikr beradi va turli tadqiqotchilar uni himoya qilish uchun turli usullarni taqdim etgan. Biz g'oyani kengaytiramiz va hujumlarning yangi turlarini va hozirgi usullardan foydalangan holda ularni qanday himoya qilish mumkinligini aniqlaymiz.

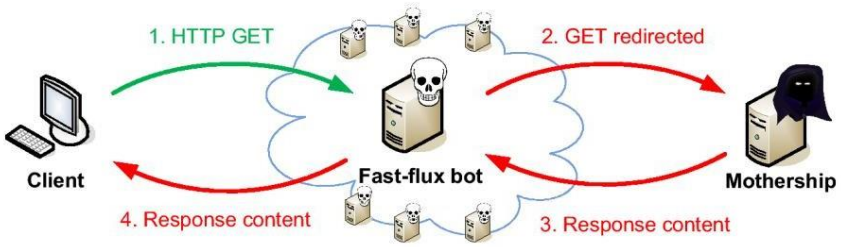
SQL - standartlashtirilgan dasturlash tili bo'lib, u relyatsion ma'lumotlar bazalari bilan o'zaro ishlash va ma'lumotlar bazasida saqlanadigan ma'lumotlarni manipulyatsiya qilish uchun ishlatiladi.

Tadqiqotlar shuni ko'rsatadiki, veb-ilovalarning aksariyati xavfsizlik nuqtai nazaridan zaifdir, shuningdek, Internetning o'sishi va ulardan foydalanish qulayligi tufayli veb-ilovalardan foydalanish tezlashdi

SQL injection hujumlari veb-ilovalar uchun eng xavfli tahdidlardan biridir. SQLi - bu tajovuzkorlar uchun ruxsatsiz kirish orqali ma'lumotlar bazalarida saqlangan cheklangan ma'lumotlarni olish maqsadida serverda zararli SQL so'rovlarini bajarish uchun protsedura. Ushbu hujumlar foydalanuvchi kiritishi

yordamida veb-ilovalar orqali amalga oshirilishi mumkin.

Ko'pgina tadqiqotchilar dasturchilarga SQLi muammosini bartaraf etish uchun manba kodlari uchun xavfsiz kodlashni amalga oshirish orqali o'z so'rovlarini himoya qilishga yordam beradigan turli usullarni ko'rib chiqdilar. Ko'pgina tadqiqotchilar SQLi ni yo'q qilish uchun qilingan bo'lsa-da, bu muammoni butunlay yo'q qilish uchun hali ham to'g'ri echim yo'q. SQLi ning oqibatlari turli xil halokatli usullarda ishlatilishi mumkin bo'lgan ma'lumotlar bazasiga ruxsatsiz kirish huquqiga ega bo'lgan tajovuzkorlardir.



1.4-rasm.Tez oqim hujumi

Hujum maqsadi: aniqlashdan qochish. Ushbu turdagi tajovuzkor SQL Injection naqshini o'zgartiradi, shunda u umumiy aniqlash va oldini olish usullaridan aniqlanmaydi. Ushbu usulda tajovuzkor SQL bayonotida o'n oltilik, Unicode, sakkizlik va ASCII kodlarini ko'rsatishdan foydalanadi. Bu umumiy aniqlash va oldini olish bilan aniqlanmaydi. Chunki ular kodlangan satrlarni aniqlay olmadi va shuning uchun bu hujumlarni aniqlanmaslik imkonini beradi.

Blind SQL Injection Attack

Hujum maqsadi: Ma'lumot olish Ko'pgina veb-ilovalar SQL xato xabarlarini ko'rsatishni o'chiradi. Ushbu hujumda ma'lumot to'g'ri/noto'g'ri savollarni berish orqali chiqariladi. Agar inyektsiya nuqtasi butunlay ko'r bo'lsa, hujum qilishning yagona yo'li WAIT FOR DELAY yoki BENCH-

MARK buyrug'idan foydalanishdir. Ushbu turdagi inyektsiya Deep Blind SQL Injection Attack deb nomlanadi.

Fast Flux SQL Injection Attack

Hujum maqsadi: ma'lumotlarni olish, fishing. Fishing Internet foydalanuvchilari uchun muhim xavfsizlik tahdididir. Fishing bu ijtimoiy muhandislik hujumi boÿlib, unda tajovuzkor yuzini uchinchi shaxs sifatida koÿrsatish orqali foydalanuvchidan maxfiy ma’lumotlarni qo’lga kiritadi. An'anaviy fishing xostini faqat umumiy domen nomi serverini yoki IP manzilini kuzatish orqali osongina aniqlash mumkin. Ushbu orqaga qaytish texnikasi hosting veb-saytlarining yopilishiga olib kelishi mumkin.

Hujumchilar yuklangan hujumni amalga oshirish serverning yuk muvozanatiga sezilarli ta'sir ko'rsatishi mumkinligini tushunishdi. Jinoiy aktivlarini himoya qilish uchun ushbu harakatga qarshi turish uchun fishing veb-saytlari operatori Fast Flux texnikasidan foydalanishni boshladi. Fast Flux - bu doimiy ravishda o'zgarib turadigan server tarmog'i orqasida fishing va zararli dasturlarni tarqatish saytlarini yashirish uchun domen nomlari serveri texnikasi. Tez oqimga hujum qilish texnikasini diagramma orqali tushunish mumkin.

Big SQL Injection, ya'ni tez oqim yordamida bir vaqtning o'zida hujum uchun ko'plab so'rovlar ishlatiladi. Bu Asprox botnet yordamida amalga oshirilishi mumkin. Fast Flux rejimida DNS (domen nomi serveri) bir vaqtning o'zida turli xil zararli dasturlarni yuqtirgan IP-larni va doimiy ravishda o'zgarib turadigan IP-larni joylashtiradi. Birinchi tezkor oqim SQL In'ektsiya banner82.com saytida aniqlangan, u hozir yopilgan, ammo tadqiqotchilar tomonidan chuqur o'rganilgan.

Murakkab SQL qarshi hujumi

Murakkab SQL Injection Attack - bu veb-saytga hujum qiladigan va ilgari

muhokama qilingan SQL in'ektsiyalariga qaraganda jiddiyroq ta'sirga olib keladigan ikki yoki undan ortiq hujumlarning aralashmasi. Murakkab SQL in'ektsiyasi turli xil SQL in'ektsiyalariga qarshi profilaktika va aniqlash usullarining jadal rivojlanishi tufayli paydo bo'ldi. Buni yengish uchun zararli tajovuzkorlar murakkab SQL Injection deb nomlangan texnikani ishlab chiqdilar. Murakkab SQL Injection SQL Injection va boshqa veb-ilova hujumlari aralashmasidan olingan bo'lib, ularni quyida tavsiflash mumkin.

SQL Injection + DDoS Attacks DDoS (Distributed Denial Of Service) serverni osib qo'yish, foydalanuvchi unga kira olmasligi uchun resurslarni sarflash uchun ishlatiladigan hujum sifatida ta'riflanadi. Uni veb-ilova DDoS deb tasniflash mumkin. SQLda biz kerakli natijani olish uchun juda murakkab so'rovlarni yaratishimiz mumkin. Kodlash, siqish, qo'shilish kabi ilg'or SQL buyruqlari yordamida DDoS hujumini amalga oshirish uchun SQL Injectionda turli xil buyruqlar mavjud. Oldini olish uchun ushbu mavzu bo'yicha juda kam tadqiqot olib borildi, chunki bu juda murakkab hujumdir. xavfsizlik nuqtai nazaridan tushunish uchun. Ushbu turdagi hujumni davom ettirish uchun zaiflikni topish, zaiflikka tayyorgarlik ko'rish va nihoyat, murakkab koddan hujum uchun foydalanilishi mumkin bo'lgan asosiy qadamlar mavjud.

SQL Injection + XSS. IBM Dewey menejeri SQL Injection + XSS hujumi haqida shunday deydi: “Agar siz uning murvatini tushunsangiz, bu saytlararo skript hujumidir. SQL in'ektsiyasi u erga borish uchun shunchaki vosita edi. O'z bayonotida u SQL Injection - bu hujumni o'rnatish usuli ekanligini, qolgan ishni XSS (Cross Site Scripting) bajaradi. Ushbu hujumlar uchinchi to'lqin hujumlari sifatida tanilgan, chunki ular odatda hujumning eski usuli emas, lekin ular Tarmoq monitoringi qurilmalaridan yashirish uchun buyruqlardir.

XSS (Cross Site Scripting) mijoz tomonidan kodni kiritish hujumi sifatida

aniqlanishi mumkin, bunda tajovuzkor qonuniy veb-sayt yoki dasturga zararli kodni kiritishi mumkin. Skript odatda veb-saytning kiritish maydonlariga kiritiladi. Qo'ygandan so'ng, skriptlar avvalgidek bajariladi va tajovuzkorning rolini bajariladi.

WebGoat serverini ishga tushirish uchun:

```
java -jar webgoat-server-8.0.0.M23.jar
```

Dastur ishga tushgach quyidagi code larni ko’rish mumkin.

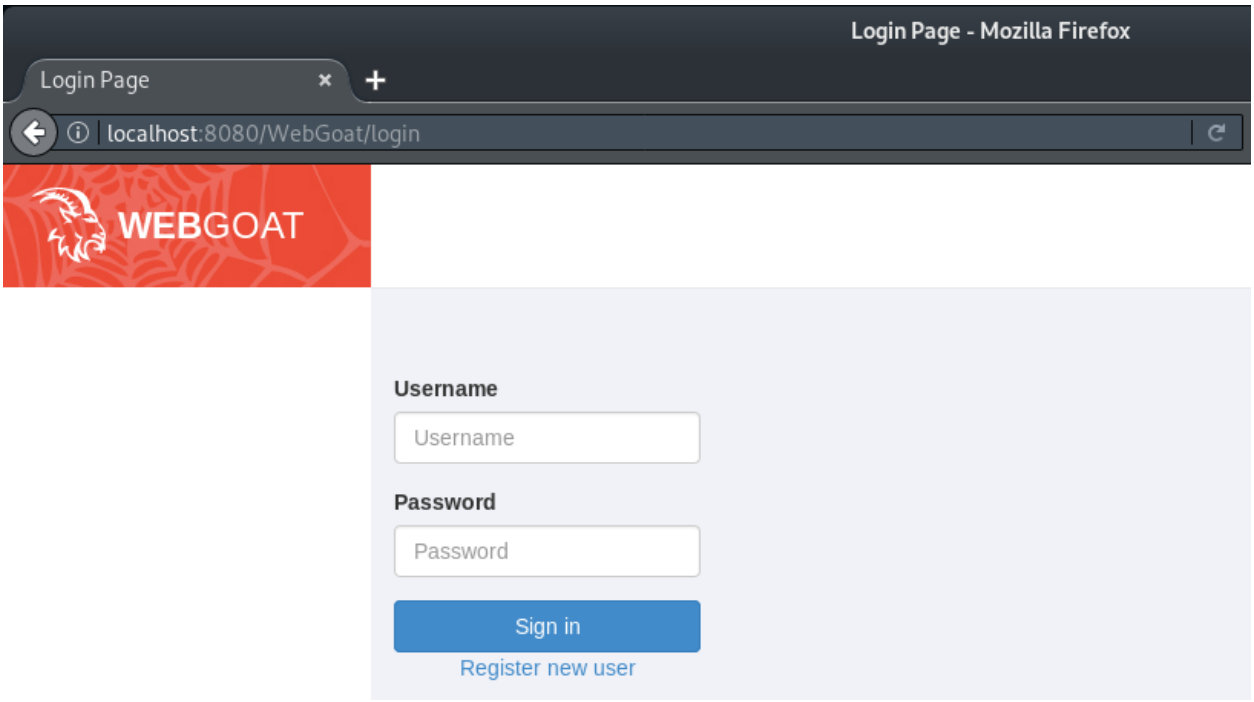
```
: Looking for @ControllerAdvice: org.springframework.boot.context.embedded.AnnotationConfigEmbedde
dWebApplicationContext@4abdb505: startup date [Fri Jan 25 18:55:20 GMT 2019]; root of context hier
archy
2019-01-25 18:55:50.556  INFO 2088 --- [           main] o.s.j.e.a.AnnotationMBeanExporter
: Registering beans for JMX exposure on startup
2019-01-25 18:55:50.621  INFO 2088 --- [           main] o.s.c.support.DefaultLifecycleProcessor
: Starting beans in phase 0
2019-01-25 18:55:51.089  INFO 2088 --- [           main] s.b.c.e.t.TomcatEmbeddedServletContainer
: Tomcat started on port(s): 8080 (http)
2019-01-25 18:55:51.101  INFO 2088 --- [           main] org.owasp.webgoat.StartWebGoat
: Started StartWebGoat in 33.293 seconds (JVM running for 34.964)
```

WebGoat interfeysiga kirish

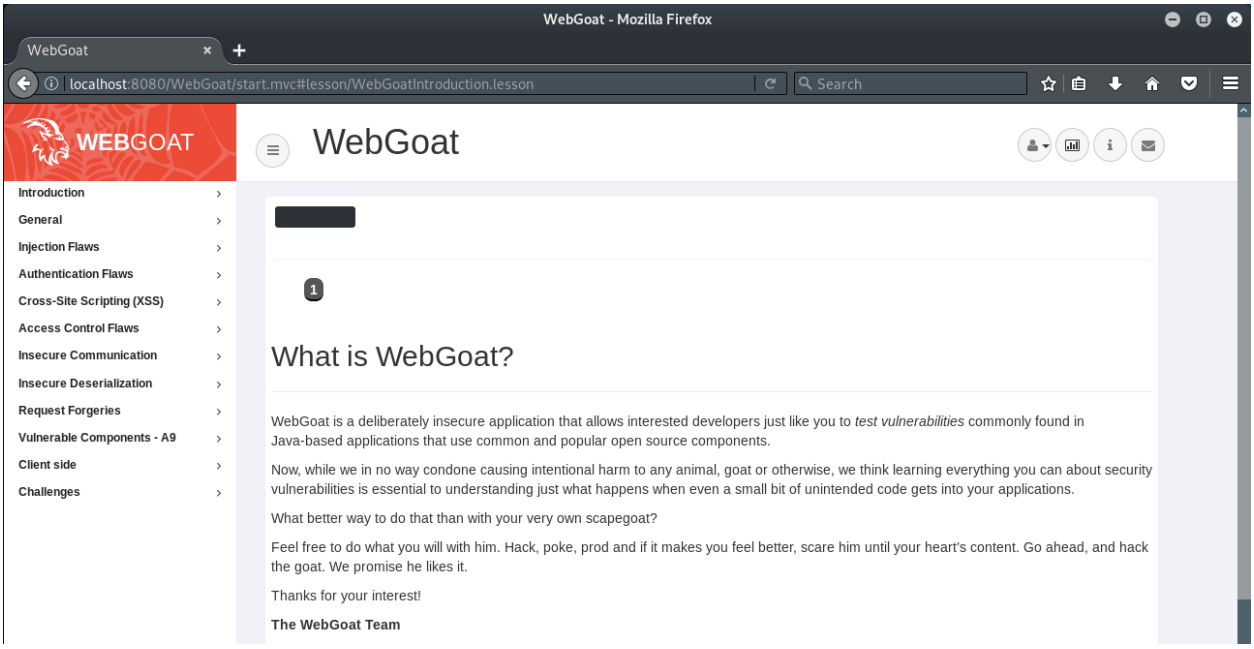
WebGoat interfeysiga kirish uchun brauzeringizni oching va quyidagi manzilga o'tiladi:

```
http://localhost:8000/WebGoat
```

Keyin sizga WebGoat kirish ekrani taqdim etiladi:



Darslar va topshiriqlarga kirish uchun siz " *Yangi foydalanuvchini ro'yxatdan o'tkazish* " ni tanlashingiz va login yaratishingiz kerak bo'ladi.



Quyigai topshiriqlar ro’yxatidan topshiriqlarni bajarish mumkin.

Xulosa:

SQL Injection hujumlari har jihatdan jiddiy masala sifatida qaralishi va veb-ilovalar va ma'lumotlar bazalarining xavfsizligi uchun zarur choralar ko'rilishi va hujumlardan himoyalanishi kerak.

Web-ilovalar kodini tahlil qiladi va tajovuzkorlarga veb-ilovada SQL Injection hujumlarini amalga oshirishga imkon beruvchi zaifliklarni aniqlash tavfsiya qilinadi. Shuningdek, mijozlarga veb-ilovalarini yangilab turishlarini, zamonaviy xavfsizlik dasturlari va yangilanishlarini o'rnatishlarini va kuchli parollardan foydalanishlarini tavsiya qilinadi.

FOYDALANILGAN ADABIYOTLAR:

1. O’zbekiston Respublikasi Prezidentining Farmoni, 2022 — 2026-yillarga mo’ljallangan yangi O’zbekistonning taraqqiyot strategiyasi to’g’risida. 2022-yil.
2. Core_Security. (2018). What is Penetration Testing Available: https://www.coresecurity.com/content/penetration-testing
3. T.Laskos. (2017). Arachni Apllication Security Scanner Framework.
4. INFOSEC_Institute. (2016). The History of Penetration Testing.
5. OWASP.(2016).Fuzzing.Available: https://www.owasp.org/index.php/Fuzzing
6. 6.OWASP. (2016). Cross Site Scripting. London
7. 7.PortSwigger_Ltd. (2018, 2018). SQL injection