TURAN SECURITY

OWASP TOP O'NTA ZAIFLIKLARI

ODDIY TILDA

01 BROKEN ACCESS CONTROL

Foydalanuvchi o'ziga berilgan huquqdan tashqarida harakat qilishga imkon beruvchi va saytga kirish nazoratini amalga oshirishdagi zaiflik tufayli broken access control yuzaga keladi.

Komil

Oddiy Foydanaluvchi

User ID : 456

abc.uz

User ID : 123 so'rovini ushlab, uni 456ga o'zgartiring

AZIZ

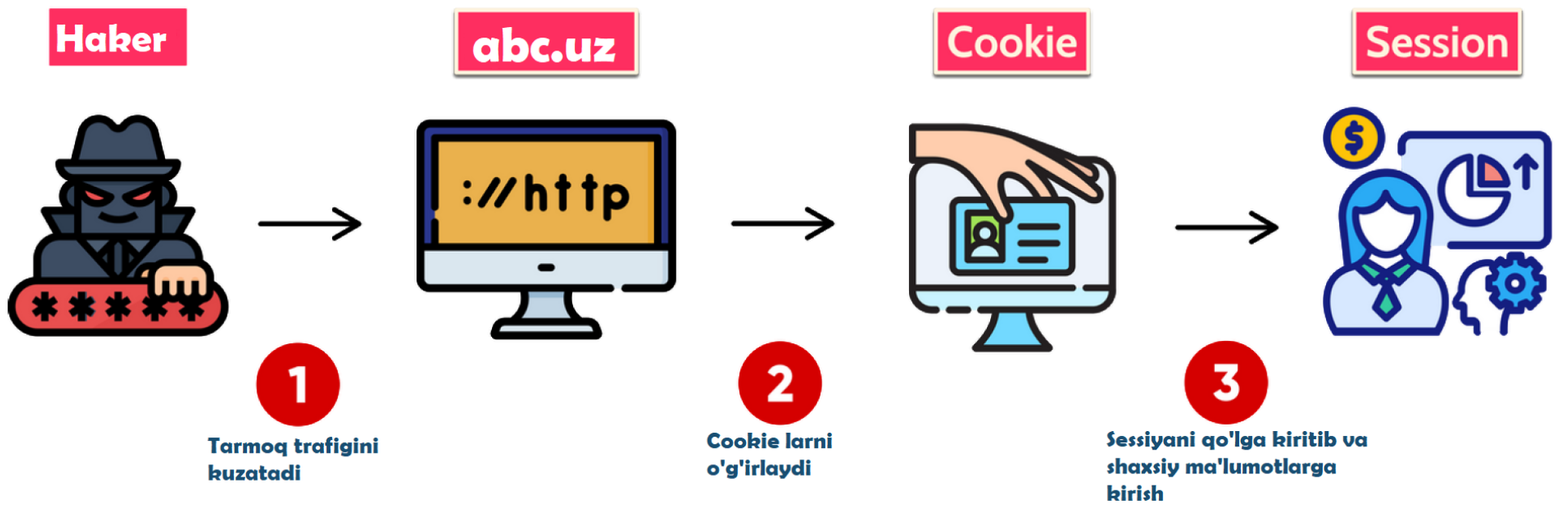
Admin Huquqli Foydalanuvchi

User ID : 123

Misol uchun, hujumchi ilovadagi zaiflikdan foydalanib, o'ziga tegishli bo'lmagan ma'lumotlarga yuqoriroq huquq bilan tizimga kirishi va ruxsat etilmagan harakatlarni bajarishi mumkin.

02 CRYPTOGRAPHIC FAILURE

Kriptografik xatolik zaifligi ma'lumotlarni ochiq matn tarzda saqlash yoki uzatishda, yoki ma'lumotlarni eski yoki kuchsiz shifrlash bilan himoya qilishga urinishda yuzaga kelishi mumkin.

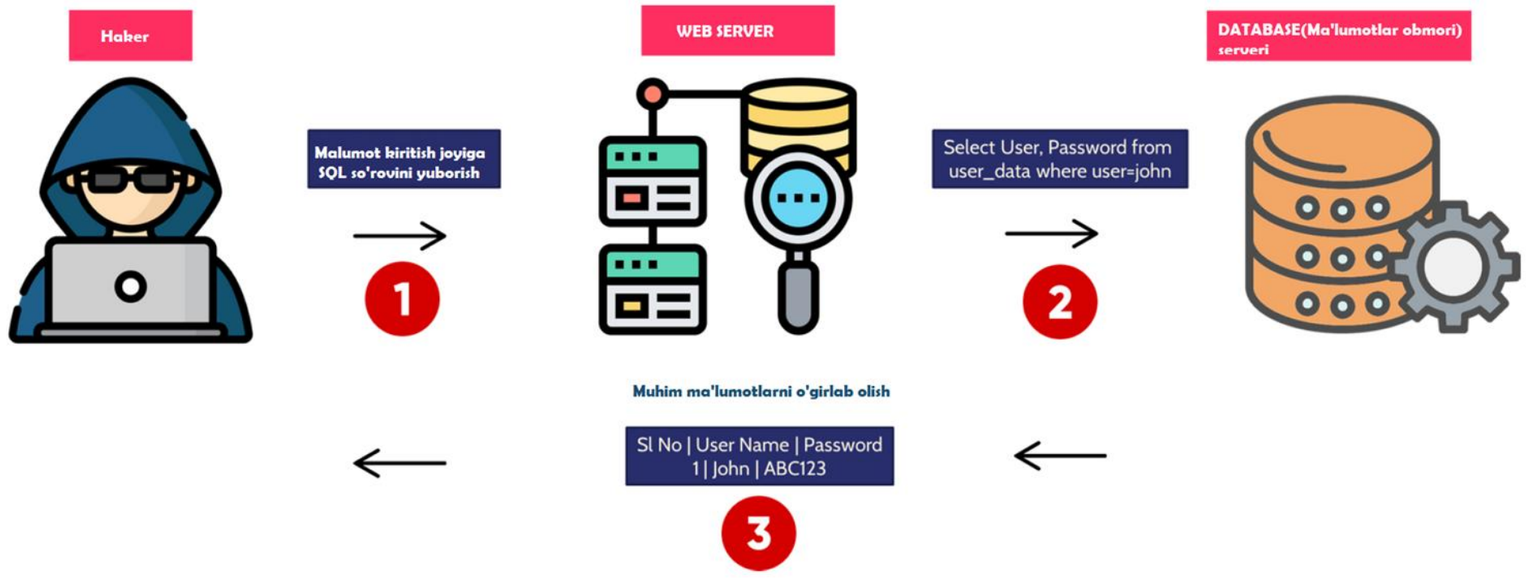


Misol uchun, barcha sahifalar uchun TLS (Transport Layer Security)ni majburiy bo'lmagan saytni ko'rib chiqaylik. Hujumchi foydalanuvchining sessiya cookielarini o'g'irlaydi va keyin bu cookieni o'zining browseriga qo'yib, foydalanuvchining (autentifikatsiya qilingan) sessiyasini o'g'irlaydi, foydalanuvchining shaxsiy ma'lumotlariga ega bo'ladi.

03

INJECTION

Injection hujumlari xavfsizlikka tahdid soluvchi zaifliklarning bir turi bo‘lib, ular ilova foydalanuvchisi kiritgan ma’lumotlarni olib, xavfsiz bo‘lmagan tarzda ishlatganda yuzaga keladi.



Injection hujumlari eng xavfli hujumlardan biridir. Bu hujumlarda shunchaki zararli ma’lumotlarni yuborib, ilovani u bajarishi kerak bo‘lmagan ishlarni bajarishga majbur qiladi.

Turan Security

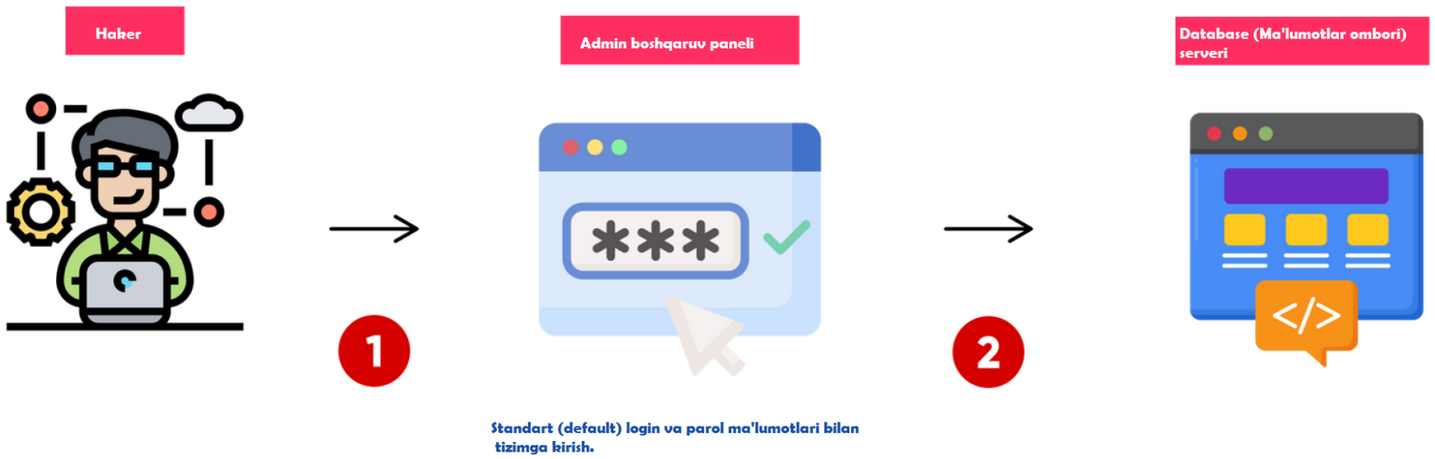
04 INSECURE DESIGN

Xavfsiz bo‘lmagan dizayn "yetarli yoki samarali bo‘lmagan boshqaruv dizayni" sifatida ifodalanadi.

Masalan, zararli niyatli shaxs -10 ta chipta buyurtma qilishi mumkin, chunki ilova mantiqida foydalanuvchi chiptalar soniga manfiy qiymat kiritishi mumkinligi hisobga olinmagan. Tizim avtomatik tarzda foydalanuvchi chiptani bekor qilgani uchun pul qaytarishi kerak deb javob beradi. Natijada, zararli foydalanuvchi chipta bron qilish va pul ishlash imkoniyatiga ega bo‘ladi.

05 SECURITY MISCONFIGURATION

Noto‘g‘ri sozlamalar bilan bog‘liq zaifliklar – bu dasturiy ta'minot komponentlari konfigidagi(sozlamasidagi) kamchiliklar bo‘lib, masalan masofadan boshqarish funksiyalari kabi keraksiz xizmatlar yoqilgan bo‘lishi mumkin.



Standart (default) login va parol ma'lumotlari bilan tizimga kirish.

Masalan, veb-server dasturida standart foydalanuvchi login va parollari qoldirilgan mumkin, bu esa zararli foydalanuvchi tizimga kirish imkonini beradi. Yoki dastur tarkibida konfiguratsiya fayllari va skriptlar kabi namunaviy fayllar bo‘lishi mumkin, ular haker tomonidan ekspluatatsiya qilinishi ehtimoli bor.

Turan Security

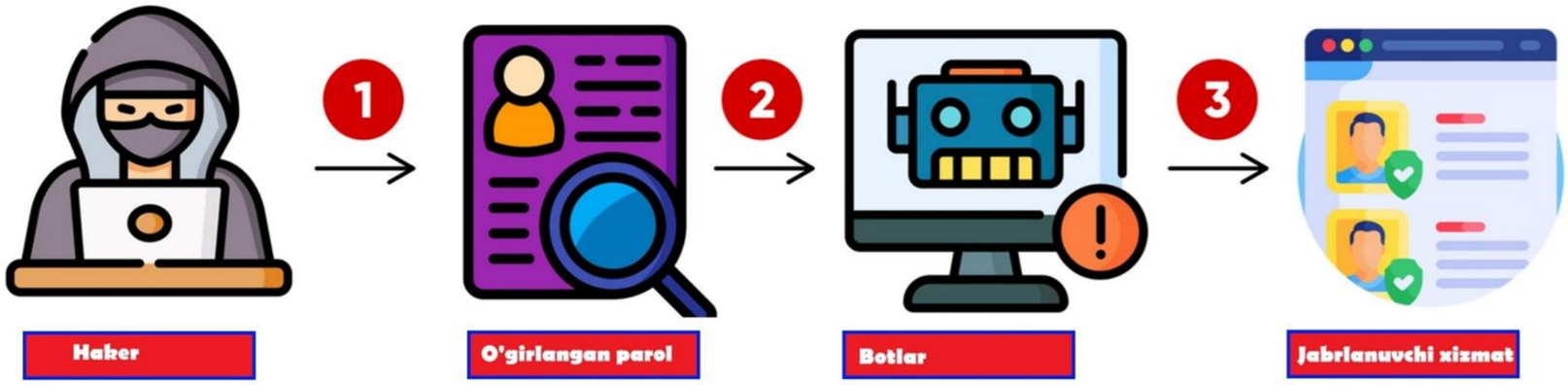
06 VULNERABLE COMPONENTS

"Zaif" yoki "eski" komponentlar atamasi. Ilova yoki dasturdagi eski kodlar xakerlik yoki boshqa yo‘llar bilan xavfsizlikka putur yetkazilishi mumkin bo‘lgan dasturiy ta'minotdagi kamchiliklar uchun ishlatiladi.

Xaker eski komponentlarning zaifliklaridan foydalanishi mumkin va ruxsatsiz ma'lumotlarga kirish, ma'lumotlarni o'zgartirish, yoki xizmat ko'rsatishni rad etishga (DoS) sabab bo'ladi. Komponentlar OS, ma'lumotlar bazasi, API, server va boshqalarni o'z ichiga olishi m-n.

07 IDENTIFICATION & AUTHENTICATION FAILURES

Foydalanuvchining shaxsini aniqlash, autentifikatsiya yoki sessiya boshqaruvi bilan bog'liq funktsiyalar to'g'ri amalga oshirilmagan taqdirda, identifikatsiya va autentifikatsiya xatoliklari yuzaga kelishi mumkin.

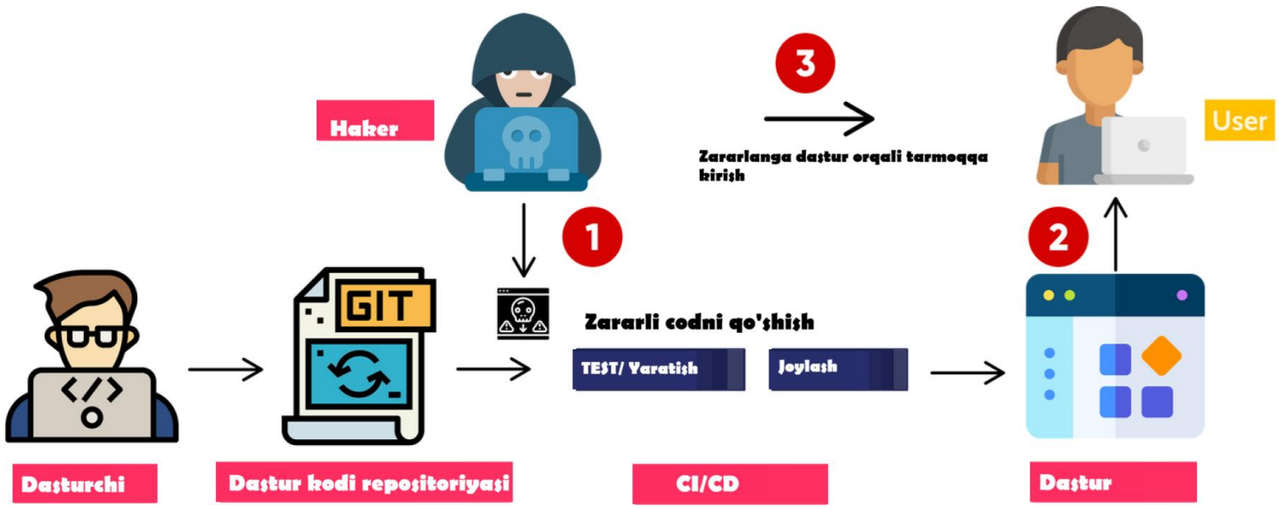


Hujumchilar identifikatsiya va autentifikatsiya xatoliklaridan foydalanib, parollar, kalitlar, sessiya tokenlari yoki boshqa amalga oshirishdagi kamchiliklarni ekspluatatsiya qilish orqali boshqa foydalanuvchilarning shaxsini o'zlashtirishlari mumkin.

Turan Security

08 SOFTWARE AND DATA INTEGRITY FAILURES

Dastur va ma'lumotlar yaxlitligi xatoliklari, yaxlitlik buzilishlariga qarshi himoya qilinmagan yoki ishonchsiz manbalardan dastur ishlatadigan kod va infratuzilma bilan bog'liq.

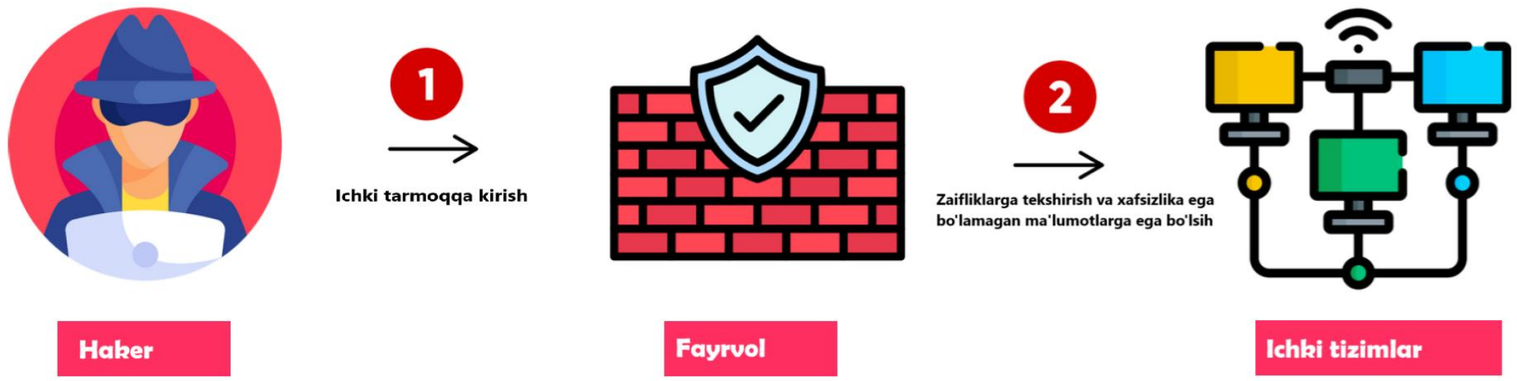


Xafsiz bo'lmagan CI/CD (Continuous Integration/Continuous Deployment) tizimi ruxsatsiz kirish, zararli kod yoki tizimning buzilishiga olib kelishi mumkin.

09

LOGGING AND MONITORING FAILURES

Xavfsizlik hodisalarini yetarlicha qayd etmaslik, kuzatmaslik yoki hisobot bermaslik shubhali xatti-harakatlarni aniqlashni qiyinlashtiradi va hujumchining sizning ilovangizdan muvaffaqiyatli foydalanish ehtimolini sezilarli darajada oshiradi.

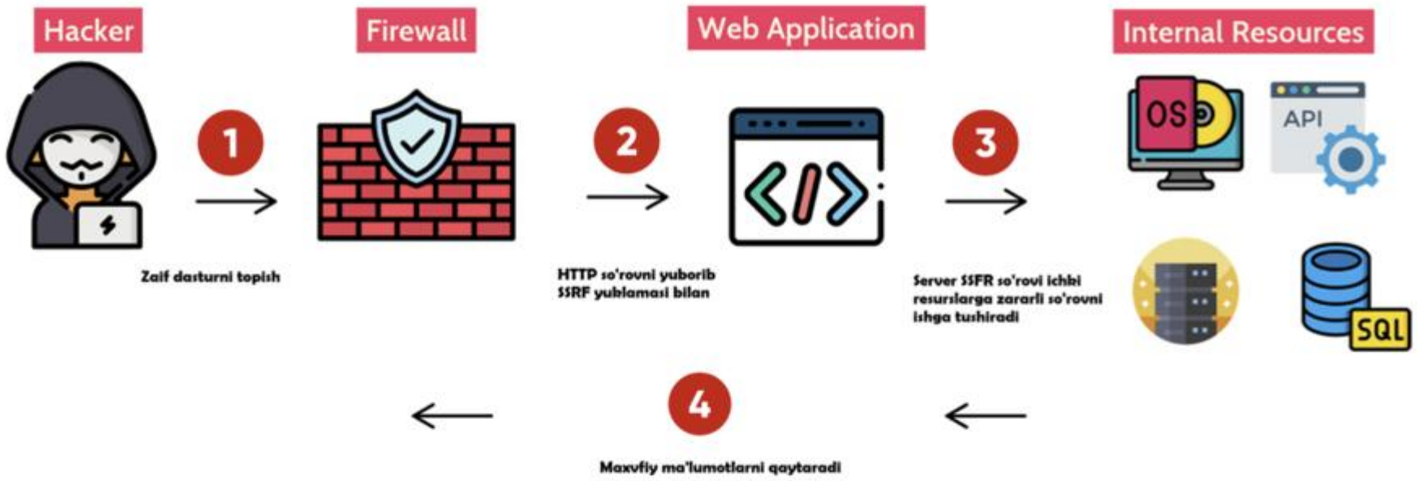


Bolalar maktablari veb-sayti operatori monitoring va loglashning yo'qligi sababli xujumni aniqlay olmaydi. Hujumchi minglab baholar, shaxsiy ma'lumotlar yozuvlariga kirib, ularni o'zgartirdi.

10

SERVER-SIDE REQUEST FORGERY

Server tomoni so'rovni aldash (SSRF) hujumlari, tashqi tarmoqdan kirib bo'lmaydigan va fayrvol ortida joylashgan ichki tizimlarni nishon olish uchun ishlatiladi.



Oddiy SSRF hujumi davomida hujumchi serverni ichki xizmatlarga ulanishga majbur qilishi mumkin

Turan Security

PLAYBOOK MADE WITH

Turan Security

Turan Security | Special thanks to Min of Defence