Indizea

[**Django 2**](#_pwhbewz0me8l)

[**Android 3**](#_6fq23gt55vz)

# 

# Django

1. Requirements.txt fitxategia aldatzea

Requirements.txt artxiboa aldatu egin da liburu-denden arteko gatazkak saihesteko eta proiektuaren mendekotasunen arteko bateragarritasuna bermatzeko. Liburu-denden bertsioak eguneratuta edukitzean eta haien arteko edozein gatazka potentzial konpontzean, murriztu egiten da liburutegi zaharkitu edo inkonpatibleengatik segurtasun-urrakortasunak izateko arriskua. Liburutegi iportatzaileenak asgiref eta pillow izango lirateke.

2. Baimena Google bidez inplementatzea django-allauth erabiliz

Autentifikazio- eta baimen-funtzionaltasuna gehitu du, django-allauth liburutegiaren bidez Google erabiliz. Liburutegi honek erabiltzaileen autentifikazioa Google bezalako kanpo-hornitzaileen bidez erabiltzeko modu segurua eskaintzen du, eta horrek aplikazioan erabiltzaileen saio-hasierako kredentzialak zuzenean biltegiratzeko eta kudeatzeko beharra ezabatzen du.

Gainera, account-etik nireaccount-era autentifikatzeko aplikazioaren izen lehenetsia aldatu da, antzeko izena izan lezaketen beste aplikazio batzuekiko gatazkak saihesteko. Horrek laguntzen du izenen espazio argia izaten, eta saihestu egiten du aplikazio-izenen talkak, segurtasun-akatsak edo -arazoak eragin ditzaketenak.

3. Django eta ORM inprimakiak erabiltzea SQL injekzioak saihesteko

Djangoren Django eta ORM inprimakien erabilera inplementatu du datu-basearekiko elkarreraginak maneiatzeko. Horrek ziurtatzen du SQL kontsultak modu seguruan sortzen direla eta SQL injekzioak saihesten direla.

SQL kontsultak zuzenean idatzi beharrean, erabiltzailearen datuak Django inprimakien bidez erabiltzen dira, datuen osotasuna bermatzeko balidazio-mekanismo txertatuak eskaintzen dituztenak. Gainera, Djangoren ORMa erabiltzean, datu-baseko eragiketa guztiak Djangok emandako metodo seguruak erabiliz egiten dira, eta horrek automatikoki saihesten ditu SQL injekzioak, eta kontsultak modu seguru eta sendoan sortzea bermatzen du.

Aldaketa horiek egitean, nabarmen hobetzen da proiektuaren segurtasuna, eraso-bektore potentzialak murrizten direlako eta garapen segururako gomendatutako praktikak erabiltzen direlako.

Gomendioak:

Mendekotasunen mantentze erregularra: Requirements.txt fitxategia aldian-aldian eguneratuta edukitzea gomendatzen da, gela guztiak eguneratuta daudela eta erabilitako liburutegietan ezagutzen diren urrakortasunik ez dagoela ziurtatzeko. Horrek segurtasun-arriskuak arintzen lagun dezake.

Segurtasun-eguneratzeen jarraipena: Garrantzitsua da proiektuan erabilitako liburutegien segurtasun-eguneratzeen berri izatea. Segurtasun-jakinarazpenetara harpidetzea edo iturri fidagarrien bidez informatuta egotea gomendatzen da, beharrezkoak diren partxeak edo eguneratzeak eskuragarri egon bezain laster aplikatzeko.

Kodearen auditoria: Kode-auditoria erregularrak egiteak lagundu dezake balizko segurtasun-urrakortasunak identifikatzen, hala nola datu sentikorren erabilera desegokia edo sarrera-balidaziorik eza. Kodeak aldizka berrikustea gomendatzen da, eta analisi estatikorako tresnak erabiltzea, segurtasun-arazoak detektatzeko.

Django-allauth konfigurazio segurua: Kanpoko hornitzaileen bidez autentifikatzeko django-allauth erabiltzen denean, garrantzitsua da segurtasun-aukerak behar bezala konfiguratzea, hala nola sartzeko tokens kudeaketa eta OAuth baimenen konfigurazioa, autentifikazioaren osotasuna eta segurtasuna bermatzeko.

Segurtasun-probak: Aldizkako segurtasun-probak egitea, hala nola sartze-probak eta kalteberatasunen ebaluazioak, lagungarria izan daiteke sisteman egon daitezkeen ahulguneak identifikatzeko eta zuzentzeko, erasotzaile posibleek ustiatu baino lehen.

Ondorioak:

Ondorioz, proiektuan egindako aldaketek nabarmen hobetu dute aplikazioaren segurtasuna eta sendotasuna. Dependentziak eguneratuta edukitzean, Google bidezko autentifikazio segurua django-allauth erabiliz inplementatzean eta SQL injekzioak saihesteko Django eta Django ORM formularioak erabiltzean, segurtasun-arriskuak murriztu dira eta balizko zaurgarritasunen aurkako babesa indartu da.

Funtsezkoa da garapen seguruko jardunbideei jarraitzea, segurtasun-jardunbide egokienekin egunean egotea eta auditoria erregularrak egitea aplikazioa balizko mehatxuen aurka babestuta egongo dela bermatzeko. Segurtasunaren ikuspegi proaktiboarekin, erabiltzaileen konfiantza mantendu dezakegu eta datuen osotasuna une oro babestu.

# Android

EncryptDecrypt klasea:

EncryptDecrypt klasea aldatu zen RSA enkriptazioa erabiltzeko Base64 erabili beharrean. Horrek segurtasun-geruza gehigarri bat ematen du informazio sentikorra gordetzean, hala nola JWT eta APIren URLa, SharedPreferences-en.

RSA gakoak sortzeko, zifratzeko eta deszifratzeko metodoak inplementatu ziren, Androiden gako seguruen azpiegitura erabiliz (Android Keystore).

Eskatutako baimenak:

INTERNET eta USE\_BIOMETRIC baimenak gehitu ziren AndroidManifest.xml fitxategian, aplikazioa Internetera sar dadin eta funtzio biometrikoak erabil ditzan, hurrenez hurren.

Erabiltzaileari baimen horiek exekuzio-denboran eskatzeko beharrezko kodea ezarri zen, Androiden segurtasun-politikak betez.

Baimenen erabilera:

Erabiltzaileari behar dituen baimenak eskatzen zaizkio (INTERNET eta USE\_BIOMETRIC) une egokian, Androiden segurtasun-jardunbide onenei jarraituz.

Baimen-eskaera gauzatze-denboran egiten da, aplikazioak eskatutako funtzioetarako sarbidea duela bermatzeko, gailuaren segurtasuna edo erabiltzailearen pribatutasuna arriskuan jarri gabe.

Espero diren emaitzak:

Banku-aplikazioaren segurtasuna hobetzea, enkriptazio-teknika sendoagoak erabiliz (RSA, Base64 erabili beharrean), SharedPreferencesen biltegiratutako informazio sentikorra babesteko.

Androiden baimen-politikak betetzea erabiltzaileari exekuzio-denboran beharrezko baimenak eskatzean, datuen erabilera segurua eta erabiltzaile-esperientzia gardena bermatzen duena.

Gomendioak:

Enkriptatzeko eta desenkriptatzeko tekniken inplementazioa berrikustea eta baliozkotzea gomendatzen da, horien eraginkortasuna eta segurtasuna bermatzeko.

Baimen-eskaeraren proba zehatzak egitea iradokitzen da, behar bezala egiten dela eta aplikazioak hainbat gailu eta erabilera-agertokitan behar bezala funtzionatzen duela ziurtatzeko.

Ondorioak:

Segurtasun-teknika hobetuak ezartzeak, hala nola RSA enkriptatzea eta baimenak egoki eskatzea, banku-aplikazio baten segurtasuna indartzen eta erabiltzaileen informazio sentikorra babesten laguntzen du. Funtsezkoa da segurtasun-jardunbide onenak jarraitzea eta Androiden baimen-politikak betetzea, erabiltzaileentzat esperientzia segurua eta fidagarria bermatzeko.