ERASOA BESTE WEB BATI

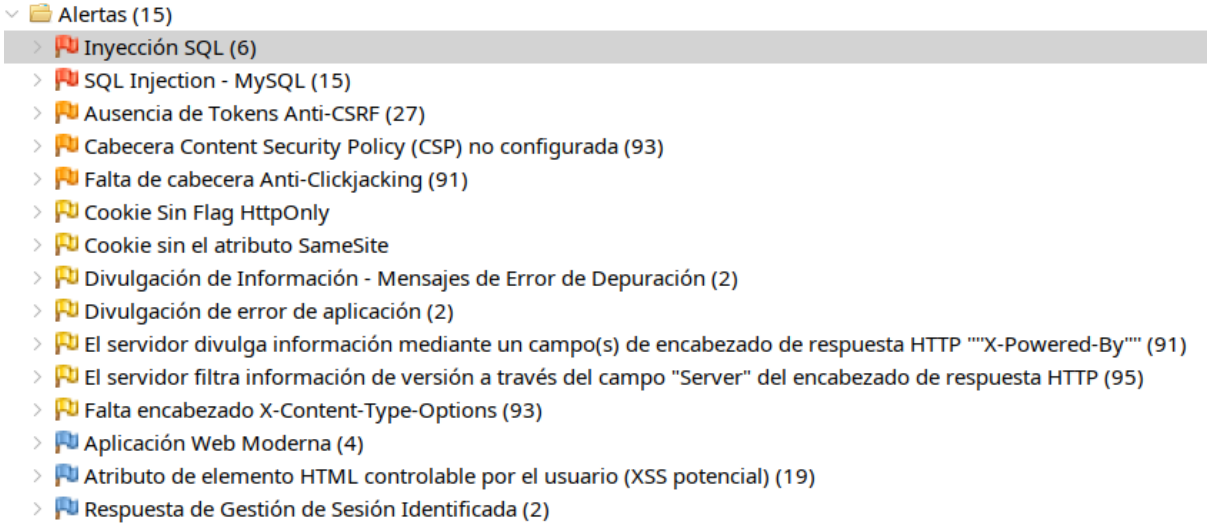
Egileak: Lier Laiseka, Asier Fernández, Hodei Castro eta Andoni Ortiz de Zarate.

Aurkibidea

Aukeratutako WEB orria

- Beste taldearen izena: Alubias comunistas

Detektatuako ahuleziak



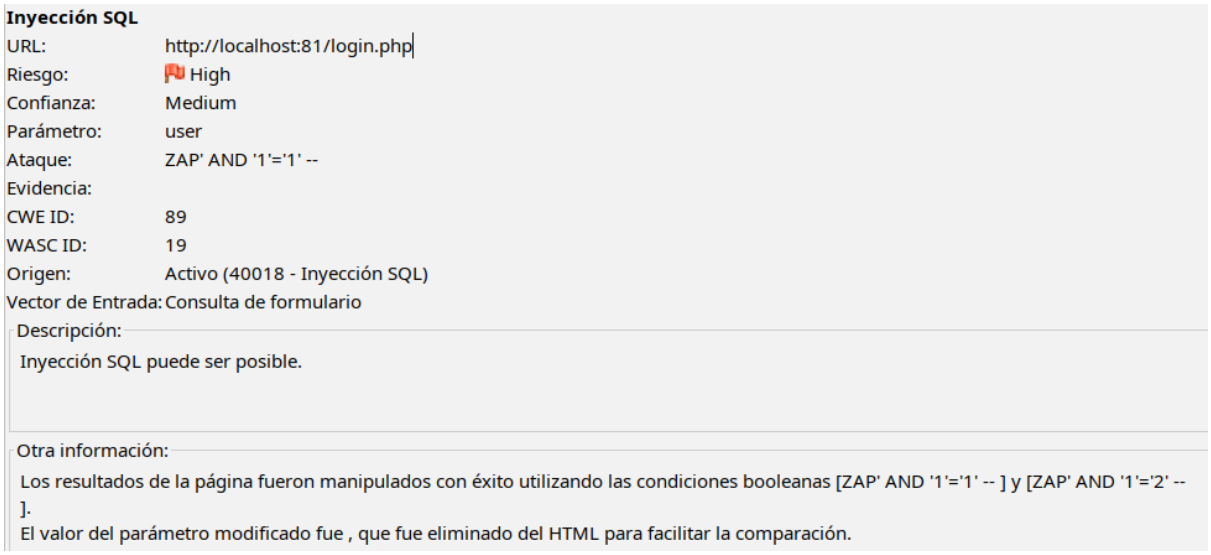
Azalpena:

- **Inyección SQL (SQL Injekzioa):** Erasotzaileak kode maliziosoa sar dezake datu-basean baimenik gabe sartzeko, datuak aldatzeko edo ezabatzeko. Ahultasun larriena da.
- **Ausencia de Tokens Anti-CSRF (CSRF Token falta):** Eskaerak balioztatzeko kode bakarra falta da; horrek erasotzaileari aukera ematen dio erabiltzailearen izenean baimenik gabeko ekintzak burutzeko.
- **Cabecera Content Security Policy (CSP) no configurada:** Ez da definitu zein iturritako edukia (script-ak, irudiak) karga dezakeen nabigatzaileak, eta horrek XSS erasoak jasateko arriskua handitzen du.
- **Falta de cabecera Anti-Clickjacking (X-Frame-Options):** Webgunea beste gune bateko "iframe" baten barruan kargatzea ahalbidetzen du, erabiltzaileak engainuzko klikak egitea erraztuz.
- **Cookie Sin Flag HttpOnly:** Cookie-ak JavaScript bidez atzitu daitezke; erasotzaile batek XSS bidez saio-identifikatzaileak lapurtu ditzake errazago.
- **Cookie sin el atributo SameSite:** Ez da zehaztu cookie-ak nola bidali behar diren beste guneetatik datozen eskaeretan, CSRF erasoen aurkako babesa ahulduz.
- **Divulgación de Información (Mensajes de Error / Depuración):** Aplikazioak errore-mezuetan informazio tekniko gehiegi erakusten du (adibidez, fitxategien bideak edo bertsioak), erasotzaileari pistak emanez.
- **Server / X-Powered-By goiburuak:** Zerbitzariak erabiltzen duen teknologia eta bertsioa (adib. PHP 7.2) publikoki erakusten ditu, ahultasun espezifikoak bilatzea erraztuz.

- **Falta encabezado X-Content-Type-Options:** Nabigatzaileak fitxategi baten formatua "asmatzea" (MIME sniffing) ahalbidetzen du, eta horrek script maliziosoak exekutatzeko arriskua sortzen du.
- **Atributo de elemento HTML controlable (XSS Potencial):** Erabiltzaileak sartutako datuak ez dira behar bezala garbitzen HTMLan txertatu aurretik, JavaScript kode maliziosoa exekutatzeko aukera emanez.

Aukeratutako ahulezia

Ahulezi altua bakarra “Inyeccion SQL” denez, hori erabiliz erasoa egingo dugu.



Zer da SQL injekzioa? SQL Injekzioa web-segurtasuneko ahultasun kritiko bat da. Erasotzaileari aukera ematen dio aplikazioak datu-basearekin egiten dituen kontsultetan (queries) interferitzeko. Funtsean, erasotzaileak SQL kode maliziosoa "txertatzen" du sarrera-eremuetan (input), datu-baseak kode hori agindu legitimo gisa exekutatu dezan.

Zergatik gertatzen da? Arazoa sortzen da aplikazioak **ez duelako bereizten** erabiltzaileak sartutako datuen eta SQL komandoen artean.

Programatzaileak erabiltzailearen sarrera (adibidez, erabiltzaile-izena) zuzenean itsasten badu SQL kontsulta baten barruan, inolako garbiketa edo balioztapenik gabe, datu-baseak dena interpretatzen du kode bezala.

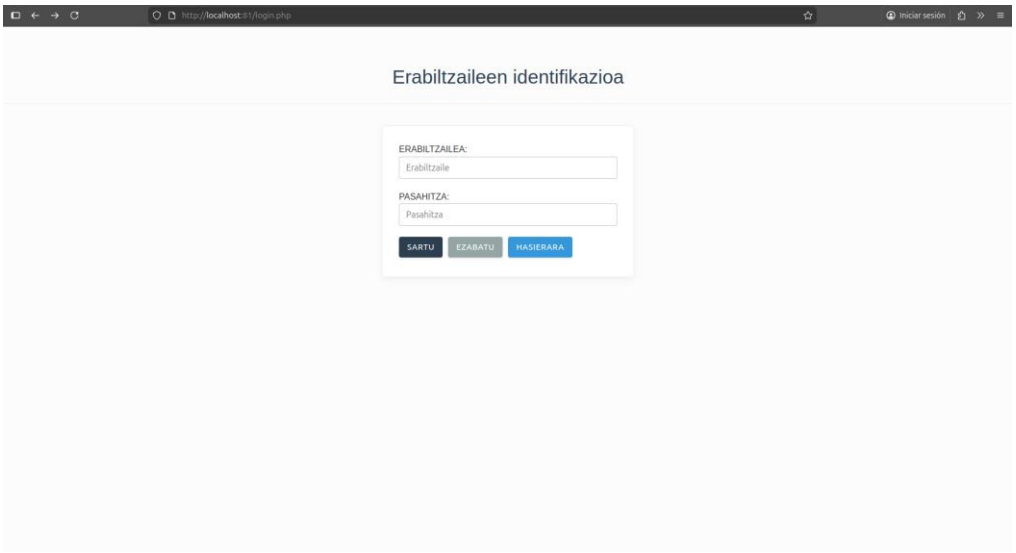
Nola saihestu? Segurtasun neurririk eraginkorrena "Prepared Statements" erabiltzea da.

Metodo honekin, SQL kodea eta datuak bereizita bidaltzen dira. Datu-baseak badaki zein zati den komandoa eta zein zati den datua, eta, beraz, nahiz eta erasotzaileak ' OR 1=1 idatzi, datu-baseak hori testu soil gisa tratatuko du, ez kode exekutagarri gisa.

Erasoa aurrera eraman

Erasoa egiteko hurrengo pausuak jarraitu behar ditugu.

1) ZAP-ek esaten digu non dagoen ahulezia. URL: http://localhost:81/login.php



2) Behin “Login” zatian egonda, hurrengoa lortu behar dugu.
   - ❖ Datu-basea behartzea "BAI" (TRUE) erantzutera: Baldintza beti egia izatea lortzen dugu, erabiltzailea nor den edo pasahitza zein den axola gabe.
   - ❖ Pasahitzaren beharra ezabatzea: Datu-basea engainatzen dugu pasahitzaren egiaztapena guztiz ignora dezan, atea "giltza unibertsal" batekin irekiko bagenu bezala.

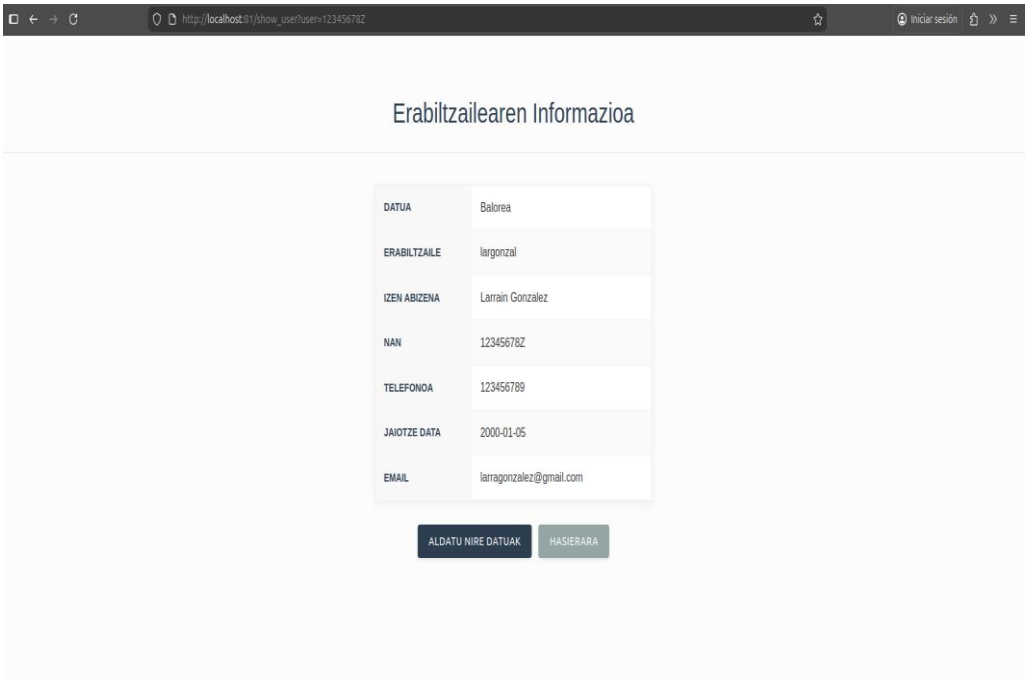
     Laburbilduz: Helburua da sistemari sinestaraztea baldintzak bete direla, baimenik gabe administratzaile gisa sartu ahal izateko.

Guzti hori saihesteko eta guk erabili dugun komandoa ADMINISTRATZAILE bezala sartzeko webhorrira, hurrengo izan da.

ERABILTZAILEA: admin' OR 1=1 -- -

PASAHITZA: edozein

3) Emaitza:


http://localhost:81/show_user?user=12345678Z
Iniciar sesión
Erabiltzailearen Informazioa
DATUA
Balorea
ERABILTZAILE
largonzal
IZEN ABIZENA
Larrain Gonzalez
NAN
12345678Z
TELEFONOA
123456789
JAIOTZE DATA
2000-01-05
EMAIL
larragonzalez@gmail.com
ALDATU NIRE DATUAK
HASIERARA