

# ERASOA BESTE WEB BATI

```
0100100100010011001100100110  
100100101100111101010101100111  
110101001100100100110010100101  
100100101100111101010101100111  
001110011000100110110001111111  
1100110 Hacker Attack! 0011001  
101010010001110011000100110110  
000111001100010011011000101001  
100111000101001001000111001100  
10010111001001011001111010101  
10010111001001011001111010101  
011011101101010011001001001100
```

# Aurkibidea

Aurkibidea .....	2
Aukeratutako WEB orria .....	3
Detektatuako ahuleziak .....	3
Aukeratutako ahulezia .....	4
Erasoa aurrera eraman .....	5

# Aukeratutako WEB orria

- Beste taldearen izena: [Alubias comunistas](#)

## Detektatuako ahuleziak

- Alertas (15)
  - Inyección SQL (6)
    - SQL Injection - MySQL (15)
    - Ausencia de Tokens Anti-CSRF (27)
    - Cabecera Content Security Policy (CSP) no configurada (93)
    - Falta de cabecera Anti-Clickjacking (91)
    - Cookie Sin Flag HttpOnly
    - Cookie sin el atributo SameSite
    - Divulgación de Información - Mensajes de Error de Depuración (2)
    - Divulgación de error de aplicación (2)
    - El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By"" (91)
    - El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP (95)
    - Falta encabezado X-Content-Type-Options (93)
    - Aplicación Web Moderna (4)
    - Atributo de elemento HTML controlable por el usuario (XSS potencial) (19)
    - Respuesta de Gestión de Sesión Identificada (2)

Azalpena:

- **Inyección SQL (SQL Injekzioa):** Erasotzaileak kode maliziosoan 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 erasoaren aurkako babesia 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 goiburua:** 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 maliziosa exekutatzeko aukera emanez.

## Aukeratutako ahulezia

Ahulezi altua bakarra "Inyección SQL" denez, hori erabiliz erasoa egingo dugu.

**Inyección SQL**

URL:	http://localhost:81/login.php
Riesgo:	High
Confianza:	Medium
Parámetro:	user
Ataque:	ZAP' AND '1'='1' --
Evidencia:	
CWE ID:	89
WASC ID:	19
Origen:	Activo (40018 - Inyección SQL)
Vector de Entrada:	Consulta de formulario
Descripción:	Inyección SQL puede ser posible.

Otra información:

Los resultados de la página fueron manipulados con éxito utilizando las condiciones booleanas [ZAP' AND '1'='1' -- ] y [ZAP' AND '1'='2' -- ].  
El valor del parámetro modificado fue , que fue eliminado del HTML para facilitar la comparación.

**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 maliziosa "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.

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

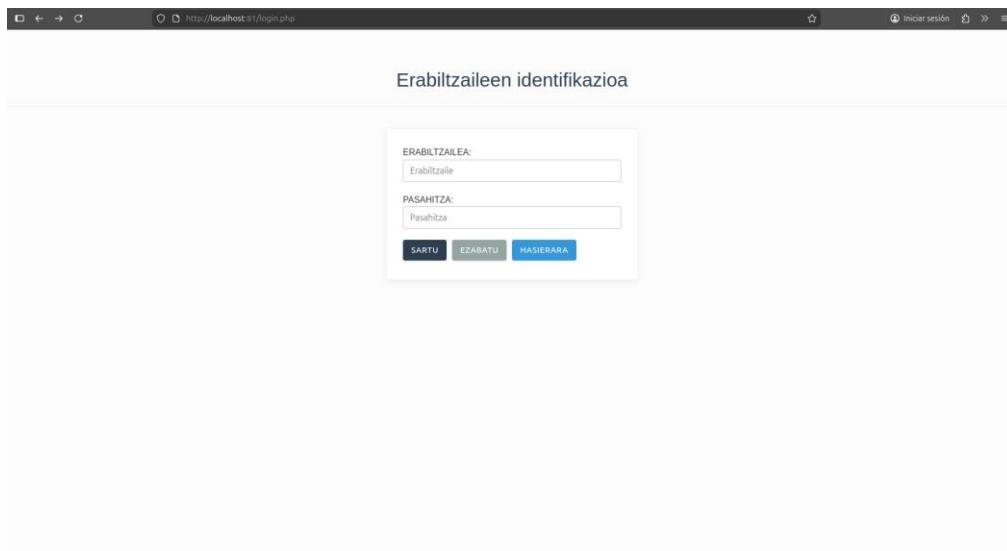
**Nola saihestu?** Segurtasun neurririk eraginkorrena "Prepared Statements" erabiltzea da.

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 engainatzentz dugu pasahitzaren egiaztapena guztiz ignora dezan, atea "giltza unibertsal" batekin irekiko bagenu bezala.  
Laburbilduz: Helburua da sistemari sinestaraztea baldintzak bete direla, baimenik gabe administratzale 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) Emaitzta:

The screenshot shows a web browser window with the URL [http://localhost:81/show\\_user?user=12345678Z](http://localhost:81/show_user?user=12345678Z). The page title is "Erabiltzailearen Informazioa". Below the title is a table displaying user data:

DATUA	Balorea
ERABILTZAILE	largonza1
IZEN ABIZENA	Larrain Gonzalez
NAN	12345678Z
TELEFONOA	123456789
JAIOTZE DATA	2000-01-05
EMAIL	larragonzalez@gmail.com

At the bottom of the page are two buttons: "ALDATU NIRE DATUAK" (Dark Blue) and "HASIERARA" (Grey).