

EUSKAL HERRIKO UNIBERTSITATEA

KUDEAKETAREN ETA INFORMAZIO SISTEMEN  
INFORMATIKAREN INGENIARITZAKO GRADUA

INFORMAZIO SISTEMEN SEGURTASUNA  
KUDEATZEKO SISTEMAK

---

STONKX

---

*Egileak:*

Aingeru RUIZ

Yeray LÓPEZ

Álvaro DONO

*Gainbegiraleak:*

Mikel EGAÑA

2023ko azaroaren 26a

eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea

## Gaien Aurkibidea

<b>1</b>	<b>Sarrera</b>	<b>1</b>
<b>2</b>	<b>Funtzionalitateak</b>	<b>1</b>
2.1	Web-orrialdean erregistratu . . . . .	1
2.2	Web-orrialdean saioa hasi . . . . .	2
2.3	Erabiltzaile-eremua . . . . .	2
2.4	Zapatilen zerrenda . . . . .	3
2.5	Zapatilak gehitu eta ezabatu . . . . .	3
2.6	Erabiltzaileen datuen aldaketa . . . . .	4
2.7	Zapatilen datuen aldaketa . . . . .	5
2.8	Berrien sekzioa . . . . .	6
<b>3</b>	<b>Auditoriak</b>	<b>6</b>
3.0.1	Application Error Disclosure ( <i>profile.php</i> ) . . . . .	7
3.0.2	<i>Anti-CSRF Token</i> falta ( <i>login.php</i> eta <i>signup.php</i> ) . . . .	7
3.0.3	<i>Content Security Policy</i> goiburua ( <i>CSP</i> ) ez konfiguratuta	8
3.0.4	<i>Anti-Clickjacking</i> goiburuaren falta . . . . .	8
3.0.5	Gelan ikusitako ahuleziak . . . . .	9
<b>4</b>	<b>Gure datu-basea</b>	<b>11</b>
4.1	Bibliografia . . . . .	11

## Irudien Zerrenda

### 1 Sarrera

*StonkX* izeneko zapata-denda ireki dugu. Zentzuzkoa denez, gure dendaren ospea bultzatzeko, web-orrialde bat sortu behar izan dugu. Hemen, edozeinek erregistratu zein saioa hasteko aukera izango du. Behin kontua sortuta, zapatilak ikusi, gehitu eta hauen datuak aldatu ahal izango da. Erabiltzaileak berak bere datuak editatzeko ahalmena izango du.

### 2 Funtzionalitateak

#### 2.1 Web-orrialdean erregistratu

Web-orrira sartu bezain laster *sign up* egiteko aukera emango zaigu orrialde nagusian. Hemen hutsune guztiak bete beharko ditugu gure datuekin eta erre-

gistratzeko botoiari ematean, gure datuak datu-basean gordeko dira eta gure datuekin erlazionatutako erabiltzaile eta pasahitza bana sortuko dira.

- [Hasiera](#)
- [Zapatilak](#)
- [Profile page](#)
- [Log out](#)

### Sign Up

Ezizena...	Pasahitza...	Izen Abizenak...	NANa...
Telefonia...	Emaila...	dd/mm/aaaa 	Sign Up

## 2.2 Web-orrialdean saioa hasi

Saioa hasteko aukera ere emango da aurretik aipatutako orrialde nagusian. *Saioa hasi* dioen botoia sakatuz gero, dagokion orrialdera eramango gaitu eta saioa hasi dezakegu kontua jadanik sortu baldin badugu eta datu zuzenak sartuz.

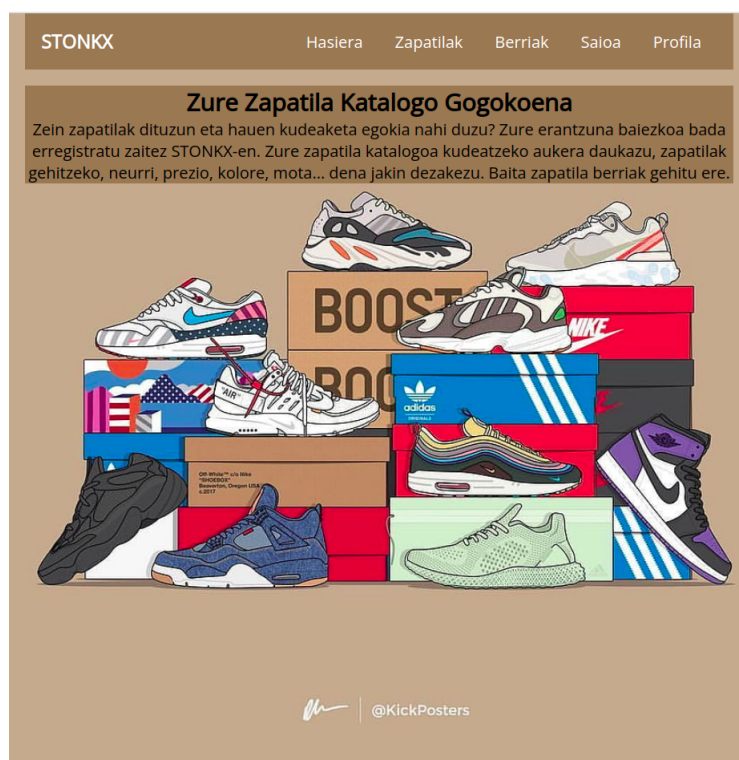
- [Hasiera](#)
- [Zapatilak](#)
- [Profile page](#)
- [Log out](#)

### Log In

Ezizena...	Pasahitza...	Log In
------------	--------------	--------

## 2.3 Erabiltzaile-eremua

Leiho honetan erabiltzaileak hainbat aukera izango ditu eskuragarri. Edozein botoia sakatuz eta funtzionalitate jakin hori dagokion leihoa irekiko da.



## 2.4 Zapatilen zerrenda

Zapatilen zerrenda ikusi ahal izateko, saioa hasi beharko dugu web-orrian. Hemen formularioa bete eta datu-baseko zapatilen zerrenda osoa ikusteko gai izango gara.

- [Hasiera](#)
- [Zapatilak](#)
- [Profile page](#)
- [Log out](#)

## Nire Zapatila Kolekzioa

- Izena Marka Mota
- [Mercurial](#) - Nike - kirola

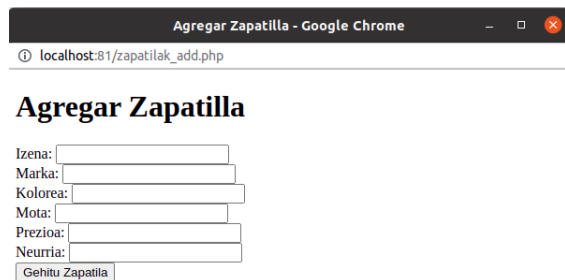
Gehitu Zapatila Berria

## 2.5 Zapatilak gehitu eta ezabatu

Hasteko eta lehen esan dugun moduan, zapatilak gehitzeko saioa jada hasita izan behar dugu gure erabiltzaile eta pasahitzarekin, eta leiho berean *Zapatila gehitu* botoia sakatuko dugu. Zapatilak gehitzeko orrira joango gara eta han za-

patila berri baten datuak sartuko ditugu. Sistemak berak datu-basean gordeko du (beti ere zapatila berri horren ID-a beste zapatilen desberdina baldin bada).

Orain, zapatila bat ezabatzeko baita saio bat hasieratuta beharko dugu eta lehen geunden orrialdetik *Zapatila ezabatu* sakatu. Behin zapatilak ezabatze-ko orrian gaudela, ezabatu nahi duguna ID-aren bidez bilatu egingo dugu eta existitzen bada datu-basetik ezabatu egingo da.



A screenshot of a web browser window titled "Agregar Zapatilla - Google Chrome". The address bar shows "localhost:81/zapatilak\_add.php". The page content includes the heading "Agregar Zapatilla" followed by a form with the following fields: "Izena:", "Marka:", "Kolorea:", "Mota:", "Prezioa:", and "Neurria:". Each field has a corresponding text input box. Below these fields is a button labeled "Gehitu Zapatila".

## 2.6 Erabiltzaileen datuen aldaketa

Erabiltzaile-eremutik erabiltzaile baten datuak aldatzeko aukera izango dugu. Botoia sakatuz gero, datuak editatzeko dagokion orrialdera eramango gaitu. Hemen gure erabiltzailearen identifikadorea eta pasahitza sartuko dugu gu gara-rela egiaztatzeko eta datu berriak sartuko ditugu ere.



The screenshot shows a web browser window titled "Editar Perfil - Google Chrome". The address bar displays "localhost:81/edit.php". The page content includes the heading "Editar Perfil" followed by a form with the following fields and values:

- Nuevo Nombre: Yeray Lopez
- Nuevo DNI: 79130072K
- Nuevo Teléfono: 688888888
- Nueva Fecha de Nacimiento: 2002-01-28
- Nuevo Correo Electrónico: yeraylopez11@gmail.com

At the bottom of the form is a button labeled "Guardar Cambios".

## 2.7 Zapatilen datuen aldaketa

Saioa hasi ostean, erabiltzaile-eremuan *Zapatilen datuak aldatu* botoia sakatuko dugu. Horrela gure produktuen datuak aldatzen utziko digun leihora igaroko gara eta han zapatila bat identifikadoreaz bilatu ostean, honen datuak aldatzeko hutsuneak bete ahal izango ditugu.



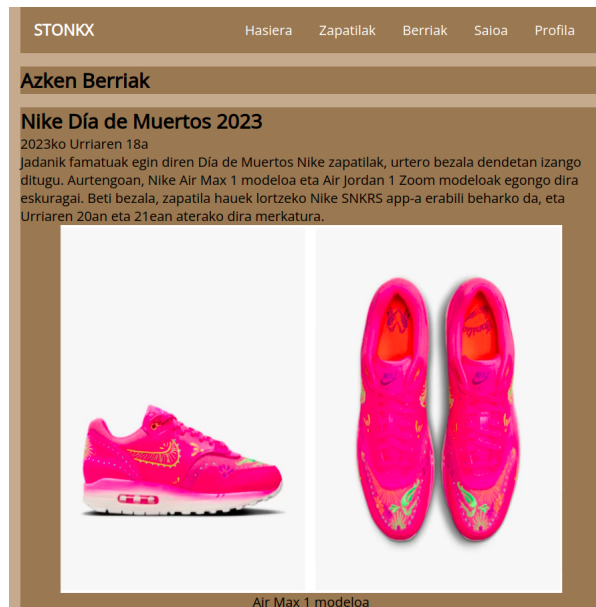
The screenshot shows a web browser window titled "Editar Zapatila - Google Chrome". The address bar displays "localhost:81/edit\_zapatila.php?zapatilaid=18". The page content includes the heading "Editatu Zapatila" followed by a form with the following fields and values:

- Izena: Mercurial
- Marka: Nike
- Kolorea: bb
- Mota: kirola
- Prezioa: bb
- Neurria: bb

At the bottom of the form are two buttons: "Gorde Aldaketak" and "Zapatila Ezabatu".

## 2.8 Berrien sekzioa

Webguneak zapatilen munduan gehiago barneratzeko, azken orduko berriak gehituz joango da, erabiltzaileek berrien berri izan dezaten.



## 3 Auditoriak



### Alertas (12)

- > Application Error Disclosure
  - > Ausencia de fichas (tokens) Anti-CSRF (2)
  - > Cabecera Content Security Policy (CSP) no configurada (8)
  - > Falta de cabecera Anti-Clickjacking (6)
  - > Cookie No HttpOnly Flag (2)
  - > Cookie sin el atributo SameSite (2)
  - > El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP
  - > Server Leaks Version Information via "Server" HTTP Response Header Field (15)
  - > X-Content-Type-Options Header Missing (9)
  - > Amplia gama de Cookies (2)
  - > Modern Web Application (3)
  - > Session Management Response Identified (3)

### 3.0.1 Application Error Disclosure (*profile.php*)

*Application Error Disclosure* alertak dio web-orrialdeak informazio garrantzitsua errebelatzen egon ahal dela salbuespen edo errore baten ondorioz. Hau konpontzeko, bide honetatik igaro gara:

- **Salbuespen eta errorearen kudeaketa**

Errore zein salbuespen informazio zehatzagoa ikusteko kudeaketa berezi bat inplementatu dugu.

```
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);

ini_set('display_errors', 0);
ini_set('display_startup_errors', 0);
error_reporting(0);
```

### 3.0.2 Anti-CSRF Token falta (*login.php* eta *signup.php*)

Errore hau gure web-orrialdeak *Cross-Site Request Forgery* erasoetara ahula dela esan nahi du. *Token* hauek eraso hauei aurka egiteko balio dute (defentsa moduan). Hau konpontzeko *login.php* artxiboan hurrengoa egin dugu:

```
$SESSION['csrf_token'] = bin2hex(random_bytes(32));
$csrf_token = $SESSION['csrf_token'];

<div class="login-form-form">
  <form action="includes/login.inc.php" method="post">
    <input type="text" name="erabiltzaile" placeholder="Ezizena...">
    <input type="password" name="pasahitza" placeholder="Pasahitza...">
    <button type="submit" name="submit">Log In</button>
  </form>
</div>

<div class="login-form-form">
  <form action="includes/login.inc.php" method="post">
    <input type="hidden" name="csrf_token" value="<?php echo $csrf_token; ?>">
    <input type="text" name="erabiltzaile" placeholder="Ezizena...">
    <input type="password" name="pasahitza" placeholder="Pasahitza...">
    <button type="submit" name="submit">Log In</button>
  </form>
</div>
```



Eta *signup.php* artxiboan:

```

$ _SESSION['csrf_token'] = bin2hex(random_bytes(32));
$csrf_token = $_SESSION['csrf_token'];
?>
<div class="signup-form-form">
  <form action="includes/signup.inc.php" method="post">
    <input type="text" name="erabiltzaile" placeholder="Ezizena...">
    <input type="password" name="pasahitza" placeholder="Pasahitza...">
    <input type="text" name="izenAbizena" placeholder="Izen Abizenak...">
    <input type="text" name="nan" placeholder="NANa...">
    <input type="text" name="telefonoa" placeholder="Telefonoa...">
    <input type="text" name="email" placeholder="Emaila...">
    <input type="date" name="data" placeholder="Jaiotze Data...">
    <button type="submit" name="submit">Sign Up</button>
  </form>
</div>

<div class="signup-form-form">
  <form action="includes/signup.inc.php" method="post">
    <input type="hidden" name="csrf_token" value="<?php echo $csrf_token; ?>">
    <input type="text" name="erabiltzaile" placeholder="Ezizena...">
    <input type="password" name="pasahitza" placeholder="Pasahitza...">
    <input type="text" name="izenAbizena" placeholder="Izen Abizenak...">
    <input type="text" name="nan" placeholder="NANa...">
    <input type="text" name="telefonoa" placeholder="Telefonoa...">
    <input type="text" name="email" placeholder="Emaila...">
    <input type="date" name="data" placeholder="Jaiotze Data...">
    <button type="submit" name="submit">Sign Up</button>
  </form>
</div>

```

### 3.0.3 Content Security Policy goiburua (CSP) ez konfiguratuta

Alerta hau dio gure web-orrialdeak *CSP* goiburua faltan duela. Azken hau segurtasun-mekanismo bat da injekzio-eraso edo *script* maltzurretatik babesten gaituena. Goiburu hau konfiguratzeko:

```

<head>
  <meta charset="utf-8">
  <title>PHP Project 01</title>
</head>
<head>
  <meta charset="utf-8">
  <meta http-equiv="Content-Security-Policy" content="default-src 'self'; script-src 'self'">
  <title>PHP Project 01</title>
</head>

```

Alerta hau konpontzeko, *PHP* artxibo guztietako metadatuaren goiburuan hurrengoa jarriko dugu: **<meta http-equiv="Content-Security-Policy">**. Alerta batzuk geratzen dira oraindik, *sitemap.xml* eta *robots.txt* artxiboak falta direla esaten, baina hauek gaur egun ez dira hainbat erabiltzen eta ez dira derrigorrez inplementatu behar, orduan ez ditugu sortuko.

### 3.0.4 Anti-Clickjacking goiburuaren falta

Alerta honetako 13 alerta daude, zeintzuk guztiak *PHP* guztietan agertzen dira, *clickjackinga* beste web sistemetatik irudi opakuetatik gure web sistemara *script* edo komando bat bidali ahal dio, eraso bat egiten. Honen soluzioa, oso

sinplea da, *PHP* goiburuan soilik etiketa hau jarri behar da eta orduan, *X-Frameak* ahalbidetuko ditugu baina soilik gure web sistematik:

```
header('X-Frame-Options: SAMEORIGIN');
```

### 3.0.5 Gelan ikusitako ahuleziak

#### 1. Sarbide-kontrola haustea

Gure web sisteman ez dago sarbide-kontrolaren hausterik, ez dagoelako *admin* pribilegiarik erabiltzaileetan.

#### 2. Akats kriptografikoak

Gure lanean datu basearen erabiltzaileen datuei loturiko akats kriptografikoak ekiditeko, saioa hasten duen erabiltzailearen datuak aldagai batean gorde behar dira, gero beste *PHP* fitxategietan erabiltzeko. Horretarako:

```
$_SESSION['erabiltzaile'] = $erabiltzailea;
$_SESSION['pasahitza'] = $pasahitza;
```

Hau da, *\$\_SESSION* aldagian gordeko dira saioa hasi duen erabiltzailea eta bere pasahitza. Aldagai hori beste fitxategietan erabiltzea posible izango da, beti ere erabiliko dugun *PHP* fitxategian *session\_start()*; lerroa gehituz.

#### 3. Injekzioa

Gure proiektuan ZAP analisiak ez ditu SQL injekziorik detektatu.

#### 4. Diseinu ez-segurua

Diseinuaren antolaketa web sistema egin baino lehen egin genuen, eta aldaketak izatekotan lehen entregan egin genituen, baina entrega honetarako ez ditugu aurkitu diseinuan segurtasun akatsak.

#### 5. Segurtasun-konfigurazioa ez da nahikoa

ZAP analisisian goiburu konfigurazioan segurtasun-konfigurazio optimo bat lortu dugu web sistemarako.

#### 6. Osagai kalteberak eta zaharkituak

Atal honetan ez daude arazorik, lehen entregan problema hau jada zuzenduta zegoen, ekipo guztietan erabili ahal zela ziurtatuta dagoelako.

#### 7. Identifikazio- eta autentifikazio-akatsak

Identifikazioaren aldetik, ikusi dugu pasahitzak datu basean gordetzen zirela, baina segurtasun aldetik, pasahitza gorde beharrean, hauen *hashak* gordetzea seguruagoa da. Lehen, erregistroan erabiltzaile batek formularioa betetzen eta bidaltzen zuenean, pasahitza eremuan jartzen zuena *\$pasahitza* aldagaian gorde eta datu basean gordetzen genuen jarraian.

Pasahitza *hasheatua* gordetzeko, beste aldagai bat sortu dugu, *\$hashed-Pas*, eta honetan *password\_hash()* funtzioa erabiliz, \$pasahitza aldagaian dagoen pasahitzaren *hash* kodea gorde dugu. Horrela datu basean \$pasahitza aldagaian dagoena gorde beharrean, *\$hashedPas* aldagaian dagoen *hash* kodea gorde dugu.

```
$hashedPas = password_hash($pasahitza, PASSWORD_DEFAULT);
```

erabiltzaileEmail	erabiltzailePasahitza	erabiltzaile
alvarodono@gmail.com	\$2y\$10\$MsKsT9yzhKrR61Fq9VAQ6.H2uv2PALYQ07h14XNryP4...	alvarodg
dfdfgdfg@dfsfsksg.com	\$2y\$10\$zgP9nilyff/kfUgoolFktuN1LSHNIUaZ8BCwgTcn5Rb...	dgalvaro

### 8. Datuen eta softwarearen osotasunaren akatsak

Atal honetan ez dugu problemarik aurkitu, web sistema *Docker*rekin abiarazteak problema hau ekiditen du parte handi batean, aurretik behar den softwarea erabiltzen delako.

### 9. Akatsak segurtasunaren monitorizazioan

Kasu honetan monitorizazioan hobekuntza bat aplikatuko dugu, non log txar guztiak gordeko ditugun. Datu basean taula berria sortuko da log txarrak gordetzeko.

Log txarren taula beharko da erabiltzaile bakoitzeko log txar bat kontatzeko. Huts egindako log kopurua 5 izatekotan, mezu bat agertuko da kontu blokeo bat simulatz.

Saioa hasiera arrakastatsua bada, erabiltzaile horren log txarrak ezabatu-ko dira.

erabizena	pasahitza	dataOrdua	hutsSaioak	blokeatuta
alvarodg	froga	2023-11-24 00:00:00	1	0

Ikus dezakegunez hurrengo irudian, alerta garrantzitsuenak eta bestelako alerta batzuk zuzentzea lortu dugu:

- Alertas (10)
  - > Cabecera Content Security Policy (CSP) no configurada (2)
  - > Cookie No HttpOnly Flag
  - > Cookie sin el atributo SameSite
  - > El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By"" (11)
  - > Server Leaks Version Information via "Server" HTTP Response Header Field (16)
  - > X-Content-Type-Options Header Missing (10)
  - > Amplia gama de Cookies (2)
  - > Modern Web Application (4)
  - > Session Management Response Identified (3)
  - > User Agent Fuzzer (96)

## 4 Gure datu-basea

*database.sql* artxiboan beharrezkoak izan diren taulak eraiki ditugu. Hainbat erabiltzaile eta zapatilen adibideak sartu ditugu:

- GitHub errepositorioa: <https://github.com/AingeruRBlol/SegurLana>
- Web-orrialdearen diseinuari buruz ideia batzuk beste egile batengatik hartuta daude.

### 4.1 Bibliografia

Hona hemen erabilgarriak izan diren informazio-iturriak:

- Web-orrialdearen itxura aldatzeko: <https://github.com/codigowebmp/menu-desplegable>
- Anti CSRF Token:  
<https://www.youtube.com/watch?v=GWeLbi01uFE>
- Cross-Site Scripting (XSS):  
<https://www.youtube.com/watch?v=LGWQE4LTeuk>
- Pasahitz *hasheatuak*:  
<https://www.youtube.com/watch?v=UsfOT0esKBk&t=866s>  
<https://www.youtube.com/watch?v=XfOxyQcbawc&t=63s>
- Bestelako bideoak:  
<https://youtu.be/GWeLbi01uFE>  
<https://youtu.be/txHc4zk6w3s>  
[https://youtu.be/JrSFc\\_KeNzc](https://youtu.be/JrSFc_KeNzc)  
<https://content-security-policy.com>  
<https://developer.mozilla.org/es/docs/Web/HTTP/CSP>
- *StackOverflowen* ere aritu gara konponbide batzuk aurkitzeko: Pasahitza egiaztatu