

Tarefa 4.7. Aplicacións web. Autenticación. Sesións. Cookies

Faremos unha aplicación web para uso online na que se xestione o arrendamento de algún tipo de produto. Empregaremos **mysql**, **PDO**, **sesións** e **autenticación** de usuarios.

Faremos unha aplicación online: engadiremos usuarios, sesións e cookies e algo de seguridade.

OLLO: Os scripts PHP conectaranse a un servidor MYSQL chamado “*db-pdo*”, con usuario “*tarefa*”, contrasinal “*Tarefa4.7*”, e base de datos “*tarefa*”.

BBDD

1. Teremos unha táboa **usuarios**, na que gardaremos o **nome** de usuario, un **contrasinal** hasheado, **nomeCompleto**, **email**, a última **data** de conexión, e o seu **rol**: usuario ou administrador. Haberá un usuario **admin**, con contrasinal “abc123.”, que NON se poderá borrar da táboa, con rol de administrador.
2. Crea unha táboa **produto**. Cada produto debe ter:
 - 3 campos distintos ou máis se o precisa(exemplo: **idProducto**, nome, descrición,...)
 - Un campo **imaxe** (gardamos a ruta do ficheiro onde está a imaxe, como na folia 3.8)
 - Un **prezo** por día
 - Terás que ter entre 10 e 20 produtos.
3. Crea unha táboa **aluga**, que garde **idProducto**, **CodCliente**, **dataInicio**, **dataFin**, **prezoTotal**, **devolto** (si/non).
4. Crea unha táboa **comentarios**, con campos **usuario**, **Comentario**, **data**, no que gardes comentarios dos usuarios.
5. Crea na carpeta onde están os ficheiros .php unha carpeta **imaxes** na que gardes as imaxes

Páxinas web

Todas as páxinas php (agás rexistro.php) deberán ter un enlace “Pegar Sesión”.

Teremos as seguintes páxinas como mínimo:

rexistro.html: Un formulario para rexistrar usuarios: nome, contrasinal, email. Os usuarios rexistraranse con rol de usuario, un administrador poderá despois cambiarlle o rol a administrador.

login.php: Terá un formulario de entrada, ademais de un enlace a rexistro.html, e outro a pechar sesión.

pechaSesion.php: Unha páxina que borre e peche sesión e redirixa a login.php

mostra.php: terá un comportamento diferentes para os usuarios e para os administradores:

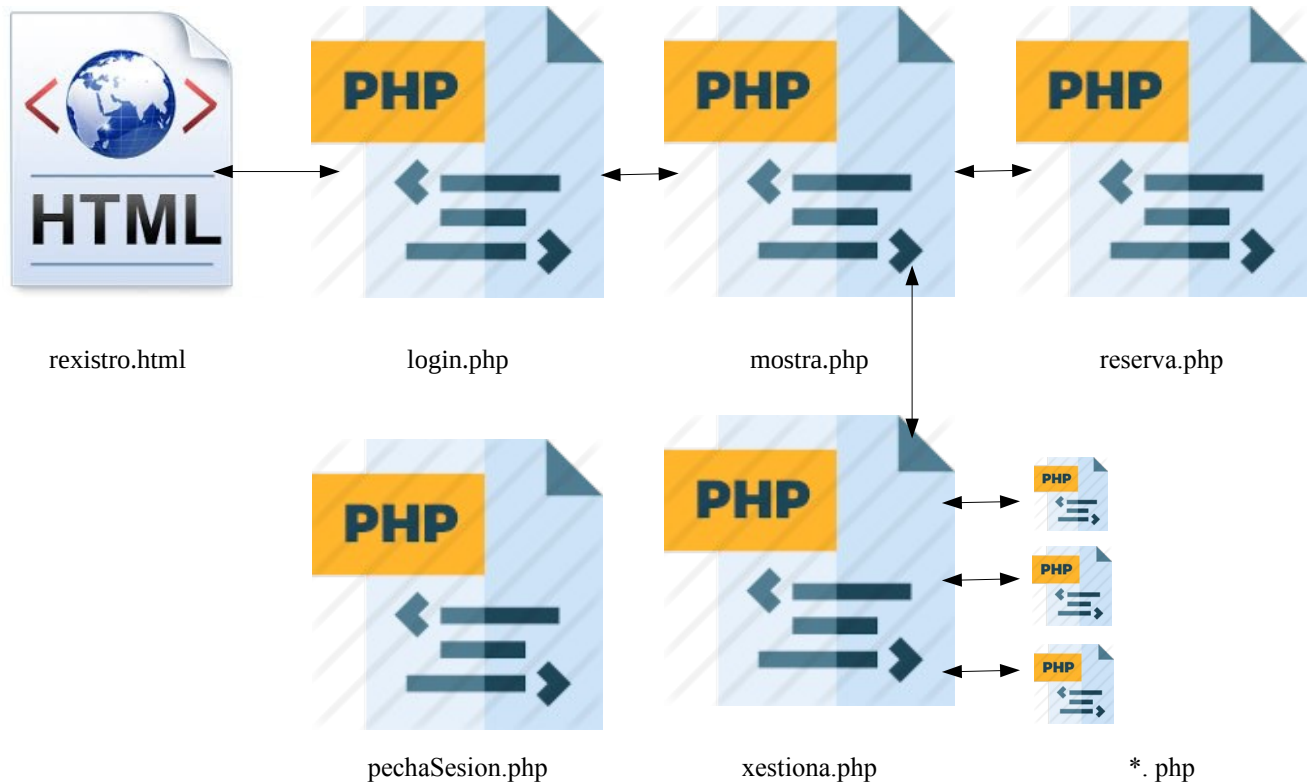
- a) usuario: Se o rol é usuario os usuarios poden ver os produtos. Poderán ver os produtos, e seleccionar un produto para alugar, chamando a **reserva.php**. Un usuario poderá cancelar unha reserva feita por el. Tamén poderá dar de alta algún comentario (ollo co XSS), e ver os últimos 3 comentarios gardados (ao final dos produtos)
- b) administrador: redirixirá a **xestionar.php**

xestionar.php: permitirá xestionar os *productos* (alta, baixa e modificación). Poderá ver tamén todos os usuarios. Ademais,

poderemos ver os produtos sen reservar e os produtos reservados.

reserva.php: páxina na que se indican **dataInicio**, **dataFin** para o produto seleccionado en **mostra.php**

Podes empregar algunha páxina máis se así o precisas para mostrar/xestionar produtos e usuarios



COOKIES

Gardaremos unha cookie indicando a lingua do usuario (cun select nun formulario *formcookies* no **login.php**: cando se envíe ese formulario recargaremos login.php), e saudarémolo nesa lingua na páxina de **mostra.php**. Esta cookie debería poder durar unha semana, para a tarefa caducará aos 5 minutos de iniciar sesión.

Seguridade

A túa aplicación non debe permitir ataques **XSS** nin de **Fixación de Sesións**.

Entrega

Finalmente, cando todo funcione, exporta a base de datos nun ficheiro **oTeuNome.sql**, e comprime este ficheiro cos demais ficheiros .php e .html e a carpeta **imaxes**, nun ficheiro **tarefa4.7OTeuNome.zip** ou **tarefa4.7OTeuNome.7z** e súbeo á Aula Virtual