UAlg DEEI
UNIVERSIDADE DO ALGARVE
FACULDADE DE CIÊNCIAS E TECNOLOGIA

DAW – Exame Ép. Recurso

09.01.2016 16:30 – 18:30
CP 0.22 CP 0.23

LER O ENUNCIADO ATÉ AO FIM ANTES DE COMEÇAR!

O objectivo do exame é adicionar uma nova funcionalidade ao site web "microposts" que foi construído ao longo dos laboratórios da disciplina.

É dado acesso a uma implementação do site web com as funcionalidades correspondentes ao LAB6. A base de dados já se encontra implementada (informação sobre a base de dados encontra-se em ANEXO).

Apenas se solicita ao aluno a criação do código controlador PHP necessário para implementar a nova funcionalidade.

O site actualizado deve ficar obrigatoriamente alojado numa pasta com o nome "`recurso`" em

```
http://all.deei.fct.ualg.pt/~a12345/recurso
```

(onde 12345 é o seu número de aluno).

PRELIMINARES

- Se preferir trabalhar inicialmente no seu portátil pode fazer o download do código numa pasta "zip" do URL

```
https://github.com/jmatbastos/recurso/archive/master.zip
```

- Faça login por ssh (com o PuTTY por exemplo) no servidor com o IP 10.10.23.183 e crie a pasta "`recurso`" com as permissões correctas

```
a12345@daw:~$ mkdir ~/public_html/recurso
a12345@daw:~$ chmod a+rx ~/public_html/recurso
```

- Caso queira trabalhar directamente com o código no servidor web, faça download do código do site web para a pasta "recurso" que acabou de criar, com o comando "git", e ponha as permissões correctas

```
a12345@daw:~ $ git clone
https://github.com/jmatbastos/recurso.git ~/public_html/recurso
a12345@daw:~$ chmod a+r ~/public_html/recurso/*
```

FUNCIONALIDADE “PASSWORD ENCRIPTADA COM SEMENTE”

Pretende-se melhorar a funcionalidade de encriptar a password que é guardada na base de dados

O método actual de criação da password encriptada

```
$passe = substr(md5($_POST['pass1_utilizador']),0,32);
```

não é seguro porque, se dois ou mais utilizadores por coincidência utilizarem a mesma password, exactamente o mesmo token/hash é guardado na base de dados. Se houver acesso à base de dados, isto é uma falha de segurança grave.

Pretende-se agora utilizar uma “semente/salt” diferente sempre que se encripta a password.

O método é o seguinte:

To Store a Password

1. Generate the random salt.
2. Prepend the salt to the password and hash it with a **standard** password hashing function like md5.
3. Save both the salt and the hash in the user's database record.

To Validate a Password

1. Retrieve the user's salt and hash from the database.
2. Prepend the salt to the given password and hash it using the same hash function.

Compare the hash of the given password with the hash from the database. If they match, the password is correct. Otherwise, the password is incorrect.

1. [4 valores] Uma forma muito simples de encriptar a password com semente é a seguinte

```
$seed=substr(time(),-4);
$passe=substr($seed.md5($seed.$_POST['pass1_utilizador']),0,32);
```

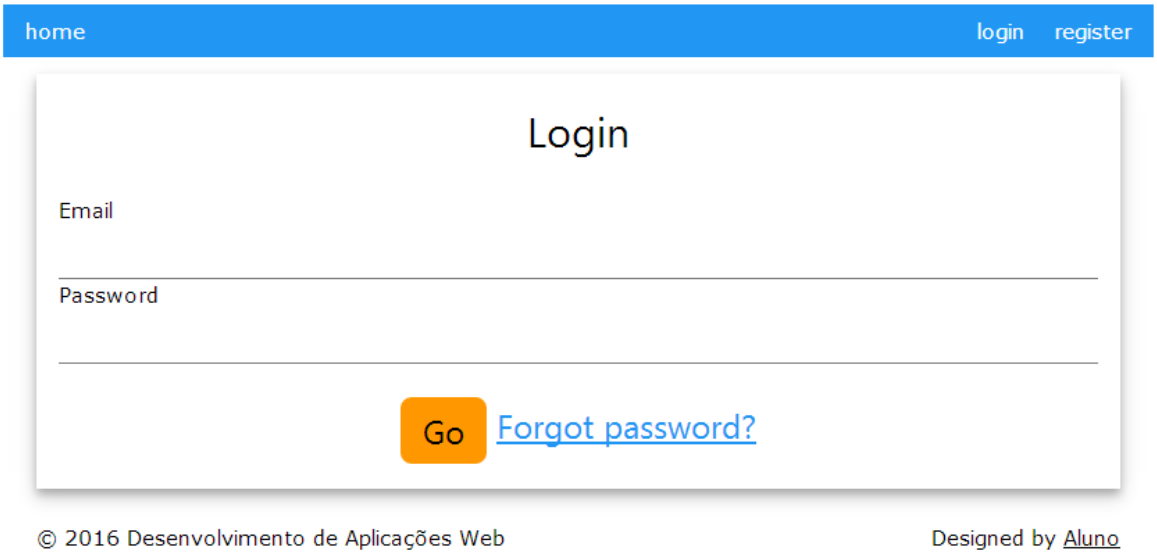
Actualize os programas **`register_action.php`** e **`login_action.php`** para passarem a utilizar o método de encriptar a password acima descrito

ALTERE o código original e coloque o seu código entre as linhas “PRINCIPIO DO SEU CODIGO” e “FIM DO SEU CODIGO” (o seu codigo pode ter qualquer numero de linhas; adicione as linhas que precisar)

FUNCIONALIDADE “RECOVER PASSWORD”

Pretende-se implementar a funcionalidade “recover password” através do envio de um email contendo um URL (“link”) apontando para uma página web onde se pode escolher uma nova password.

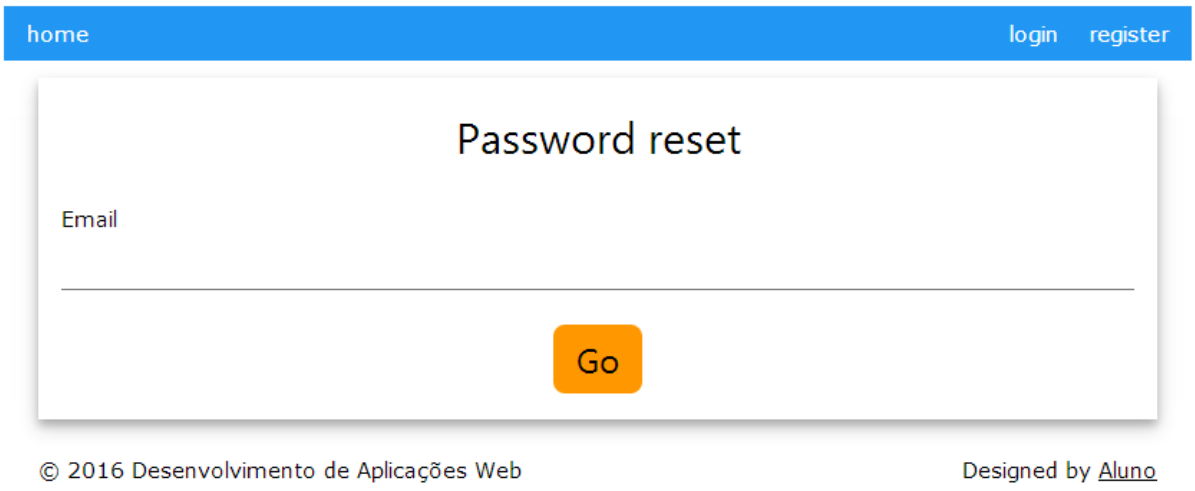
A página de “login.php”



contem agora um link,

```
<a href="password_reset.php" class="w3-text-blue" >Forgot password?</a>
```

para a página “password_reset.php”,



que contem um formulário onde o utilizador vai colocar o email com que se registou no site.

O formulario utiliza o método “POST” para enviar dados ao servidor:

```
<form method="post" action="password_reset_action.php">
```

2. [8 valores] Construa o programa **`password_reset_action.php`** que:

- verifica se o email introduzido consta da base de dados
- em caso de sucesso
  - Cria um token “md5” do tempo actual
    ```
    $reset_digest = substr(md5(time()),0,32);
    ```
  - guarda este valor na base de dados (tabela users, coluna reset_digest), bem como tempo actual (tabela users, coluna reset_digest, coluna reset_sent_at)
  - envia ao utilizador registado um email personalizado com o assunto “Password reset” e com o texto

```
Olá Sr.(a) José Silva

Para obter uma nova password clique no link

http://all.deei.fct.ualg.pt/~a12345/recurso/new_password.php?token=fad9bc3391f298e6186f8a

Se NÃO pediu uma nova password IGNORE este email.


Cumprimentos,

webmaster!
Página Web:        http://intranet.deei.fct.ualg.pt/DAW/
E-mail:               webmaster@deei.fct.ualg.pt

NOTA: Não responda a este email, não vai obter resposta!
```

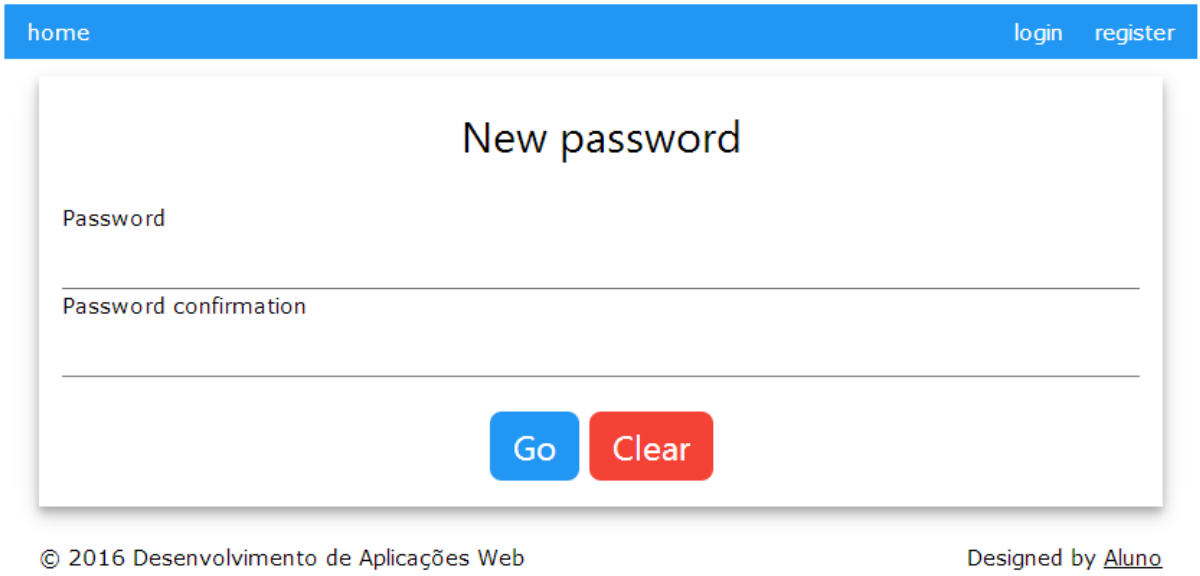
Note que o texto do email contem um link para a página “`new_password.php`” (substituir 12345 pelo seu numero de aluno) com o valor do token embutido

  - envia para o browser a mensagem

```
Password reset activated! </br> Email sent to you :-)
```

Nota: tem que utilizar um email válido a que tenha acesso, para comprovar o correcto funcionamento do programa!

O formulario `new_password.php`



utiliza o método “POST” para enviar a nova password ao servidor, bem como o token recebido (como um input do tipo “hidden”)

```
<form method="post" action="new_password__action.php">
      <input type=hidden name="token" value="{TOKEN}">
```

3. [8 valores] Crie o programa **`new_password_action.php`** que vai actualizar a base de dados com a nova password do utilizador.

- verifica se o token recebido existe na base de dados
- em caso de sucesso e se não passou mais de uma hora entre a hora actual e a hora de envio do email
  - encripta e actualiza a password na base de dados
  - envia para o browser uma mensagem

```
Password reset successfully!
```

- em caso de insucesso envia para o browser a mensagem

```
ERROR: WRONG TOKEN OR TOKEN EXPIRED, PASSWORD RESET FAILED!
```

NOTAS:

- Ponha o seu código entre as linhas “PRINCIPIO DO SEU CODIGO” e “FIM DO SEU CODIGO” (o seu codigo pode ter qualquer numero de linhas; adicione as linhas que precisar)

- Caso considere necessário escrever código noutro local, comente o seu código e justifique num ficheiro “README.TXT”. Pode utilizar esse ficheiro também para outra qualquer informação que julgue pertinente.

- Caso tenha trabalhado no seu portatil, **é obrigatório fazer o upload de todos os ficheiros** para a pasta “recurso” no seu site web pessoal

```
http://all.deei.fct.ualg.pt/~a12345/recurso
```

(onde 12345 é o seu número de aluno). Utilize scp (Linux) ou WinSCP (Windows) para fazer a cópia. **Verifique que o site fica operacional**.

ANEXO 1 Acesso à base de dados MySQL

- O acesso à base de dados MySQL pode ser feita utilizando um cliente gráfico à sua escolha (por exemplo http://www.heidisql.com/),

ou em linha de comando

```
a12345@daw:~$mysql -u a12345 -p -h 10.10.23.183 db_a12345
```

ou ainda utilizando o software **phpMyAdmin** disponível no URL

http://all.deei.fct.ualg.pt/phpMyAdmin

ANEXO 2 : estrutura da base de dados

```
CREATE TABLE `microposts` (
  `id` int(11) NOT NULL auto_increment,
  `content` text,
  `user_id` int(11) default NULL,
  `created_at` datetime NOT NULL,
  `updated_at` datetime NOT NULL,
  `likes` int(11) NOT NULL DEFAULT '0',
  PRIMARY KEY  (`id`),
  KEY `fk_user_id` (`user_id`),
  CONSTRAINT `fk_user_id` FOREIGN KEY (`user_id`) REFERENCES
`users` (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


CREATE TABLE `users` (
  `id` int(11) NOT NULL auto_increment,
  `name` varchar(255) default NULL,
  `email` varchar(255) default NULL,
  `created_at` datetime NOT NULL,
  `updated_at` datetime NOT NULL,
  `password_digest` varchar(255) default NULL,
  `remember_digest` varchar(255) default NULL,
  `admin` tinyint(1) default NULL,
  `activation_digest` varchar(255) default NULL,
  `activated` tinyint(1) default NULL,
  `activated_at` datetime default NULL,
  `reset_digest` varchar(255) default NULL,
  `reset_sent_at` datetime default NULL,
  PRIMARY KEY  (`id`),
  UNIQUE KEY `index_users_on_email` (`email`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```