

Autenticação

- Muitas aplicações web necessitam de autenticar os utilizadores
 - On-line banking
 - Comercio electrónico
 - Sites com acesso restrito
- A autenticação é feita tipicamente através do nome e password

Métodos de autenticação

- Autenticação baseada no protocolo HTTP
 - Fácil de usar
 - Não necessita guardar o estado
 - Muito utilizada para limitar o acesso a directórios
- Autenticação baseada numa form e numa sessão
 - Utilização genérica
 - Mais utilizada

Autenticação HTTP - como funciona?

- Todos os diretórios no servidor web podem ser protegidos se tiverem estes 2 ficheiros:
- .htaccess

```
AuthName "acesso restrito"
```

```
AuthType Basic
```

```
AuthUserFile /users/leyn/public_html/.htpasswd  
require user leyn
```

- .htpasswd

```
leyn:79WeSn3vYGsKQ
```

- A password encontra-se codificada (não encriptada!) em Base-64 utilizando o utilitário

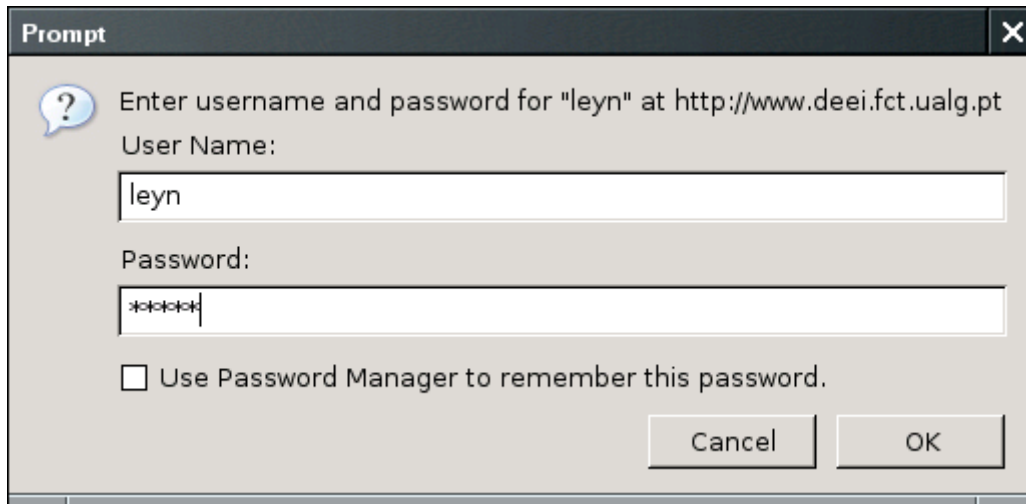
```
$htpasswd -c .htpasswd leyn
```

Resposta HTTP do servidor quando se pede a uma página com acesso restrito

```
HTTP/1.1 401 Authorization Required
Date: Thu, 08 Feb 2007 19:10:48 GMT
Server: Apache/1.3.33 (Debian GNU/Linux)
WWW-Authenticate: Basic realm="leyn"
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
2.0//EN">
<HTML><HEAD>
<TITLE>401 Authorization Required</TITLE>
</HEAD><BODY>
<H1>Authorization Required</H1>
This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.<P>
<HR>
<ADDRESS>Apache/1.3.33 Server at
www.deei.fct.ualg.pt Port 80</ADDRESS>
</BODY></HTML>
```

Resposta HTTP do cliente depois de introduzidas as credenciais



The image shows a 'Prompt' dialog box with a question mark icon. The text inside reads: 'Enter username and password for "leyn" at http://www.deei.fct.ualg.pt'. Below this, there are two input fields: 'User Name:' containing 'leyn' and 'Password:' containing '*****'. At the bottom, there is a checkbox labeled 'Use Password Manager to remember this password.' which is unchecked. There are 'Cancel' and 'OK' buttons at the bottom right.

```
GET /~leyn/ HTTP/1.1
```

```
Host: www.deei.fct.ualg.pt
```

```
User-Agent: Mozilla/5.0
```

```
Accept: text/html
```

```
Accept-Language: en-us
```

```
Accept-Encoding: gzip, deflate
```

```
Accept-Charset: ISO-8859-1
```

```
Authorization: Basic bGV5bjpvYmlkdQ==
```

Autenticação HTTP com PHP

- O directório de acesso restrito *não* precisa de ter os ficheiros .htaccess e .htpasswd
- a página de entrada no directório é um script PHP que gera o cabeçalho

HTTP/1.1 401 Authorization Required

- o script PHP tem acesso às credenciais de autenticação através das variáveis
 - `$_SERVER["PHP_AUTH_USER"]`
 - `$_SERVER["PHP_AUTH_PW"]`

Autenticação HTTP com PHP – exemplo

```
<?php
if (!isset($_SERVER['PHP_AUTH_USER'])) {
    header('WWW-Authenticate: Basic realm="My Realm"');
    header('HTTP/1.0 401 Unauthorized');
    echo 'Text to send if user hits Cancel button';
    exit;
} else {
    echo "<p>Hello {$_SERVER['PHP_AUTH_USER']}.</p>";
    echo "<p>You entered {$_SERVER['PHP_AUTH_PW']} as your password.</p>";
}
?>
```

Autenticação com sessões em PHP

- utilizador valida-se (login, password) através de uma form/formulário
- Aplicação PHP no servidor cria um array `$_SESSION` e envia ao browser o cookie `PHPSESSID` correspondente
- Todos os pedidos seguintes do browser enviam no cabeçalho HTTP "**cookie**" o cookie `PHPSESSID`
- A sessão está válida enquanto
 1. o cookie não expirar
 2. o array `$_SESSION` não for destruído

Exemplo

<http://intranet.deei.fct.uaig.pt/DAW/auth-dbsessions/archive/files.html>

```
<html>
<head>
  <title> Please Log In for Access </title>
</head>
<body>
<h1> Login Required </h1>
<p>You must log in to access this area of
the site. If you are
  not a registered user, <a
href="signup.php">click here</a>
  to sign up for instant access!</p>
<p><form method="post"
action="protectedpage.php">
<table>
  <tr>
    <td>User ID:</td>
    <td><input type="text" name="uid"
size="8" /></td>
  </tr>
  <tr>
    <td>Password:</td>
    <td> <input type="password" name="pwd"
SIZE="8" /></td>
  </tr>
</table>
<input type="submit" value="Log in" />
</form>
</p>
</body>
</html>
```



protectedpage.php

```
<?php
include_once 'common.inc';
include_once 'db.inc';

session_start();

$uid = $_POST['uid'];
$pwd = $_POST['pwd'];

if(!isset($uid))
    header("Location: login.html");

$_SESSION['uid'] = $uid;

$db = dbconnect($connection_string);
$query = "SELECT * FROM users
        WHERE userid = '$uid'
        AND password = '$pwd'";
$result = mysql_query($query, $db);
if (!$result)
    error('A database error occurred while
checking your login details.');
```

```
if (mysql_num_rows($result) == 0) {
    unset($_SESSION['uid']);
}
```

```
echo <<<END
```

```
<html>
  <head>
    <title> Access Denied </title>
  </head>
  <body>
    <h1> Access Denied </h1>
    <p>Your user ID or password is incorrect,
or you are not a
      registered user on this site. To try
logging in again, click
      <a href="login.html">here</a>. To
register for instant
      access, click <a
href="signup.php">here</a>.</p>
  </body>
</html>
```

```
END;
```

```
}
```

```
else {
```

```
$tuple =
mysql_fetch_array($result,MYSQL_ASSOC);
$_SESSION['username'] = $tuple['fullname'];
```

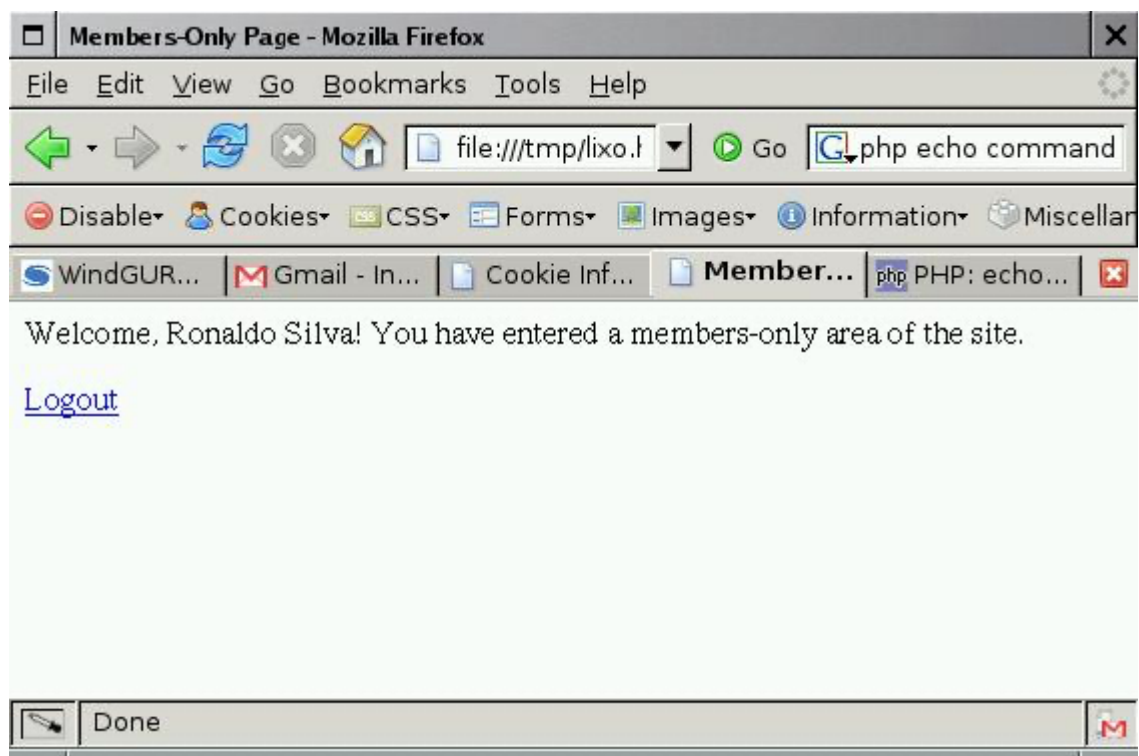
```
echo<<<END
```

```
<html>
<head>
  <title> Members-Only Page </title>
</head>
<body>
<p>Welcome, <?=$_SESSION['username']?>! You
have entered a members-only area
  of the site.</p>
<p><a href="logout.php">Logout</a></p>

</body>
</html>

END;

?>
```



Cookie Information - http://www.adeec.fct.ualg.pt/~figo/auth-db-sessions/protectedpage.php - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Go php echo command

Disable Cookies CSS Forms Images Information Miscellaneous

WindGURU: ... Gmail - Inbox... Cookie Inf... Aplicações D... PHP: echo - ...

Cookie Information -

http://www.adeec.fct.ualg.pt/~figo/auth-db-sessions/protectedpage.php

[Collapse All](#) [Expand All](#)

http://www.adeec.fct.ualg.pt/~figo/auth-db-sessions/protectedpage.php

1 cookie

NAME	PHPSESSID
VALUE	d53ffc5d358a2eb7581d97c4d2b58737
HOST	www.adeec.fct.ualg.pt
PATH	/
SECURE	No
EXPIRES	At End Of Session

[Edit Cookie](#)

[Delete Cookie](#)

Done