République Tunisienne
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique et de la Technologie
Centre de Calcul El-Khawarizmi

Charte d'hébergement des sites web universitaires "Réseau National Universitaire (RNU)"

Sommaire

PARTIE 1 : Généralités

Le Centre de Calcul El Khawarizmi (CCK) en tant que fournisseur de services Internet pour les établissements sous la tutelle du Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie, assure 24h/24 et 7jours/7 le bon fonctionnement des services du réseau national universitaire (RNU).

1. Critères d'hébergement

Les critères d'accueil sur le réseau national universitaire (RNU) sont fondés sur la compatibilité des sites avec les missions de la recherche et de l'enseignement conformément aux recommandations mentionnées dans le guide de la conception et la mise en œuvre des sites web universitaires universitaires (www.universites.tn/projetsiteweb).

2. Autorisation

L'autorisation d'hébergement sur le réseau national universitaire (RNU) sera prononcées après accord du:

- Bureau de l'appui à la production numérique au Cabinet de M. le Ministre de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie
- Centre de Calcul El-khawarizmi

3. Responsabilité

- La responsabilité des données mises en ligne relève légalement du premier responsable de l'établissement.
- Les demandes d'hébergement des sites doivent spécifier le nom de l'administrateur du site et, le cas échéant, du webmaster. **En cas de changement de l'administrateur, une notification par écrit doit être adressée au CCK**.
- Il est à noter que les mises à jour de données relatives aux sites web universitaires ou bases de données ou autres doivent être autorisées à partir d'une adresse IP source connue.
- L'établissement, doit informer le CCK avant et après la mise à jour, dans le cas contraire, le CCK n'est pas responsable de la perte de la dernière version valide.
- L'adresse e-mail reclamation@cck.rnu.tn est mise à disposition de l'établissement pour toute question, information ou réclamation d'un problème concernant l'hébergement de son site web.

4. Impératifs de qualité

Les administrateurs des sites s'engagent à assurer la mise à jour régulière et la meilleure qualité de leurs ressources en ligne.

5. Sécurité

Les sites hébergés doivent appliquer la charte d'un développement sécurisé des sites web universitaires **(PARTIE 2)**.

6. Développement des sites web universitaires

Les sites hébergés doivent respecter les recommandations techniques de développement des sites web universitaires **(PARTIE 3).**

7. Plates-formes d'hébergement

Les établissements doivent respecter les systèmes d'exploitation, les bases de données et les langages de développement disponibles au CCK conformément aux **plates-formes d'hébergement (PARTIE 4).**

8. Demande d'hébergement des sites web universitaires

Tout établissement ayant l'intention de demander un service d'hébergement ou d'accès spécifique doit formuler une demande figurant dans **la partie 5**.
Les demandes doivent parvenir au CCk via le Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie

9. Durée de l'hébergement d'un site web

La durée est fixée pour une année renouvelable. Le renouvellement est tributaire du respect de la circulaire du Monsieur le Ministre de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie, relative à la sécurisation des sites web universitaires.

10. Rappel des principales lois tunisiennes

Il est rappelé que toute personne sur le sol Tunisien doit respecter la législation Tunisienne, en particulier dans le domaine de la sécurité informatique :

- Loi n° 5 - 2004 du 3 février 2004, relative à la sécurité informatique,
- Loi organique n° 63 - 2004 du 27 juillet 2004, portant sur la protection des données à caractère personnel,
- Circulaire n° 19 - 2007, relative au renforcement des mesures de sécurité informatique dans les établissements publiques (Nomination d'un Responsable de Sécurité des Systèmes d'Information RSSI, Cellule Technique de Sécurité et un Comité de pilotage),
- Circulaire n° 22 - 2004, sur la sûreté des locaux appartenant aux ministères et aux entreprises publiques,
- Circulaire n° 19 - 2003, relative aux mesures de sécurité et de prévention des bâtiments des ministères et des collectivités locales et des entreprises publiques,
- Le décret n°97/501 du 14 Mars 1997 relatif à l'usage de l'Internet à des fins professionnelles.

Il est rappelé que constituent des infractions les informations ou messages à caractère injurieux, diffamatoire, d'incitation au racisme, révisionniste, etc...

11. Suspensions

En cas de non respect des législations en vigueur ou des présentes conditions d'hébergement, le CCK se réserve le droit, selon son appréciation de la situation, de suspendre l'accès à certaines pages ou données, voire, en cas de manquement grave, de recourir à la suspension de l'hébergement.

Le signataire de la charte est informé et accepte que le CCK:

- Procède à des contrôles permanents du bon déroulement de l'hébergement de l'entité à héberger et qu'en cas de manquement de l'utilisateur à ses obligations et ses responsabilités telles qu'énoncées ci-dessus ou, le cas échéant, à la demande des autorités, le CCK peut suspendre l'accès aux sites web universitaires.
- Prenne des mesures d'urgence, y inclus la décision de limiter ou d'interrompre temporairement l'hébergement de le/les entités à héberger pour préserver la sécurité en cas d'incident dont le CCK aurait connaissance.
- Puisse à tout moment modifier la présente charte notamment pour tenir compte des évolutions législatives.

Le signataire de la présente charte, représentant de l'établissement
Coordonnées complètes de l'établissement:
Adresse :……
…….
Téléphone: …… Fax : ……
Code postal : ……

Reconnaît avoir pris connaissance de la présente charte d'hébergement des sites web universitaires et s'engage à la **respecter sans restriction et à la faire respecter** et **désigne comme responsable technique du site web universitaire**:

Nom,Prénom:……
Fonction ou discipline : ……
En tant que webmaster du site web.
Adresse Electronique : …….
Téléphone fixe:……*Portable:*……...

Le Signataire :
Nom, Prénom: ……..
Fonction : ……
Adresse Electronique : ……
Téléphone :……

Lu et approuvé

Le Centre de Calcul El Khawarizmi
Fait à …… le, ……..

PARTIE 2 : Charte de sécurité des sites web universitaires

1. Procédure de sécurisation des sites web universitaires

Les rubriques de sécurité à respecter par un développeur sont:

Sécurisation des interactions entre les bases de données et les sites web universitaires:

- Déceler et empêcher les injections SQL
- Protection des références d'objets directs
- Limites du chiffrement du contenu de bases de données

Gestion de l'authentification de sessions:

- Protection contre le détournement de sessions
- Mise en place du contrôle d'accès aux URL
- Blocage de la falsification de requêtes inter-sites

Contrôle des fuites d'informations:

- Messages d'erreurs édulcorés sur l'écran de l'utilisateur
- Gestion des erreurs de requêtes et sur les pages

Validation des saisies:

- Etablissement de limites de confiance
- Déceler et supprimer les menaces de XSS (cross-site scripting)
- Exposer les dangers de la validation côté client
- Prévention contre le vol électronique

2. Recommandations techniques

Pour la gestion des sessions:

- Stocker les mots de passe et les profils dans le serveur et ne jamais transiter par le navigateur client.
- Faire transiter les paramètres de navigation via l'url si ceux ci sont correctement validés et contrôlés par le serveur.
- Stocker les paramètres de présentation (comme le thème ou la langue) dans un cookie.
- Faire résider du coté serveur et ne jamais transiter dans les formulaires les données secrètes. Les données des formulaires ne doivent pas contenir d'informations secrètes et cachées. Les champs cachés doivent être utilisés pour conserver des numéros de séquence et pour prévenir des attaques par brute-force (champs conservant le nombre d'essai).

Dans le cas des formulaires à plusieurs pages, les données peuvent transiter par le côté client dans les cas suivants:

- Lorsqu'un contrôle d'intégrité est strictement effectué.
- Lorsque les données sont contrôlées et validées après chaque page ou bien lors de la dernière soumission.
- Les données secrètes (comme les mots de passe ou les droits de l'utilisateur) ne doivent jamais être modifiables par le client (aussi bien en mode GET qu'en mode POST). Ces données doivent être conservées via un numéro de session.

Contrer les attaques de type XSS: Les entrées utilisateurs doivent être soigneusement contrôlées et validées avant exécution (type, longueur, neutralisation des caractères spéciaux).

Les caractères suivants doivent être bannis (de même que pour leurs versions encodées) :

! @ $ % ^ & * ( ) - _ + ` ~ \ | [ ] { } ; : ' " ? / , . > <

Ceci évitera l'exécution de code Javascript ainsi que d'autres attaques dont l'injection SQL.

Contrer les attaques SQL injection: Ne jamais faire confiance à l'utilisateur. Ne jamais le sous-estimer et penser qu'il n'est pas informé. Il faut alors filtrer tout ce que peut rentrer l'utilisateur avant de faire quoi que ce soit.

Désinfectez les entrées : Cette solution a d'intérêt spécialement pour les champs en entrée de type date, email et entier. Mais, Il est toujours utile de désinfecter les données entrées par l'utilisateur pour s'assurer qu'elles ne contiennent pas de codes dangereux, que ce soit pour le serveur SQL ou en HTML elle-même.

Exemple: une adresse E-mail ne peut contenir que les caractères suivants :

- abcdefghijklmnopqrstuvwxyz
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 0123456789
- @.-_+

Quotesafing les entrées : Les guillemets « ' » sont à proscrire, ce sont une des causes des failles d'injection. Une solution utile est de coder un script qui enlève tous les guillemets ou qui les échappe en rajoutant un antislash devant.

Exemple en php: On peut utiliser la fonction addslashes() ou bien utiliser les options magic_quotes_gpc et magic_quotes_runtime.

```
function secure($texte)
{
return mysql_real_escape_string($texte);
```

```
}
$sql = "SELECT id_article, titre, contenu FROM articles WHERE titre LIKE
    '%".secure($_POST["valeur"])."%' OR contenu LIKE
    '%".secure($_POST["valeur"])."%'";
```

La fonction secure(), ajoutera des antislashs si nécessaire devant tous les guillemets ('), ce qui les rendra interprétés par mysql non en tant que fin de chaîne mais comme des simples caractères.
Elle utilise la fonction mysql_real_escape_string(), conçue spécialement pour éviter ce type de failles.

Utiliser les paramètres rebond « The prepare statement » : Bien que quotesafing est un bon mécanisme, et considérant que l'entrée de l'utilisateur est du type SQL", une meilleure approche existe: **The prepare statement**. Cette solution est soutenue par la quasi-totalité des interfaces de programmation de base de données.

Dans cette technique, une chaîne de requête SQL est créée avec des paramètres fictifs - un point d'interrogation pour chaque paramètre - et il est compilé dans un formulaire interne. Plus tard, cette requête compilée est "exécutée" avec une liste de paramètres.

Exemple en Perl :
Version non sécurisée

```
Statement s = connection.createStatement();
ResultSet rs = s.executeQuery("SELECT email FROM member WHERE name = "
                    + formField); // *boom*
```

Version sécurisée

```
PreparedStatement ps = connection.prepareStatement(
   "SELECT email FROM member WHERE name = ?");
ps.setString(1, formField);
ResultSet rs = ps.executeQuery();
```

L'utilisation des procédures stockées pour l'accès aux bases de données: L'utilisation des procédures stockées peut éliminer entièrement la requête SQL comme suit:

- En encapsulant les règles pour une action - requête, la mise à jour, supprimer, etc - en une procédure unique, elle peut être testée et documentée sur une base autonome et des règles appliquées.
- Lorsque les opérations (ensemble de requêtes) deviennent plus complexes (ou sont utilisées plusieurs fois), il faut voir une seule définition de l'opération, car il est plus robuste et plus facile à entretenir.

Note: il est toujours possible d'écrire une procédure stockée qui elle-même construit une requête dynamiquement.

Ne jamais laisser paraître les erreurs SQL sur votre site : Un utilisateur malveillant peut planter le script volontairement afin de recueillir des informations sur

le nom des champs et des tables du serveur. D'où il faut retourner un code d'erreur si une fonction échoue, plutôt que d'afficher la requête. D'ailleurs, cet affichage provoque une vulnérabilité de **type XSS**, car l'utilisateur malin qui injectera du JavaScript dans le champ fera d'une part échouer l'interaction avec la base, et d'autre part afficher son code.

3. Rappel sur les attaques les plus courantes:

Ci dessous une description des attaques les plus courantes:

Entrée de paramètres invalides : L'internaute modifie les paramètres utilisées dans les URL, les entêtes HTTP, les formulaires ou les paramètres cachés et fournit des valeurs non attendues par le site web…

L'absence de filtre au niveau du site web peut conduire à des comportements imprévisibles allant du crash par buffer overflow à l'accès à des données confidentielles ou au système d'exploitation.

Injection de commandes: A l'aide de méta codes, éventuellement encodés en hexadécimal, unicode ou UTF, l'internaute insère dans les requêtes des commandes qui, en l'absence de filtres seront passées au site web. Ces commandes peuvent contenir, par exemple des appels au système d'exploitation, l'utilisation de programmes externes via des commandes shell ou des appels vers les bases de données.
Injection SQL: Utilisant le principe des injections de commandes, les injections SQL permettent d'exécuter des commandes directement sur les bases de donnée, afin d'avoir accès à des données confidentielles.

Cross Site Scripting: Cette technique consiste à contaminer un site Web avec un code malicieux qui sera récupéré par les utilisateurs visitant ce site. Le script malicieux s'exécute sur le navigateur des utilisateurs et permet au hacker de récupérer leurs droits d'accès (cookie, sessions utilisateurs) ou leurs mots de passe et autres informations confidentielles.

Violations de cookie et de session: La plupart des mécanismes de maintien de session sont trop rudimentaires, basés sur des jetons de sessions et parfois même sur des seuls cookies sans vérification de leur intégrité côté serveur. En procédant à des « reverse engineering » des cookies et/ou en récupérant des jetons de session active, un hacker peut les modifier afin d'acquérir l'identité et les droits d'accès d'un autre utilisateur.

Violation de contrôle d'accès: Découvrir des vulnérabilités au niveau des mécanismes de contrôle d'accès se limite souvent à envoyer une requête vers des ressources ou du contenu à accès réservé ! Les hackers réussissant à exploiter ces vulnérabilités peuvent utiliser d'autres comptes clients et tous les droits qui vont avec.

Buffer Overflow: Certains composants logiciels d'applications Web, typiquement CGI, librairies, drivers et composants serveurs du marché, ne vérifient pas

suffisamment que les données entrées tiennent dans les limites des mémoires tampons. Les hackers peuvent lancer des attaques sur les sites web universitaires présentant ces vulnérabilités afin de les crasher et parfois en prendre le contrôle.

Traitement inapproprié des erreurs: Les messages d'erreurs renvoyés par les sites web universitaires en cas de dysfonctionnements peuvent contenir des informations purement internes. Un utilisateur malveillant sollicite ces dysfonctionnements applicatifs afin de recueillir des informations sur la structure interne du site web et ses vulnérabilités.

Directory Traversal/ Forceful Browsing: Un utilisateur malveillant peut modifier ses requêtes afin qu'elles ne demandent pas au site web de lui retourner un fichier mais la branche toute entière. Si le site web ne possède pas une page par défaut au niveau de chaque branche et si le serveur web est mal configuré, le hacker peut obtenir l'accès à des informations non prévues voire à tout le contenu de la branche.

Denis de service applicatifs: Les attaques par DoS sont le plus souvent associées aux attaques au niveau réseau par SYN flood émanant d'une ou plusieurs sources (on parle dans ce cas d'attaques distribuées DDoS). Les attaques par DoS au niveau applicatif existent aussi…Un seul hacker peut générer suffisamment de trafic pour saturer les ressources d'un serveur Web sur certaines URL particulières, rendant le système indisponible pour les autres utilisateurs.

Les attaques dites « inconnues » : Les attaques exploitant des techniques et des vulnérabilités inconnues sont particulièrement dangereuses car les mesures préventives n'ont pas pu être prises. Le nombre de ces « zero day exploits » est en forte croissance pour les raisons suivantes :

- De nouvelles vulnérabilités sont régulièrement découvertes dans les composants logiciels tiers ou spécifiques utilisés par les sites web universitaires,
- Les possibilités de manipulation des requêtes sont virtuellement illimitées ce qui rend les combinaisons d'attaques et les vulnérabilités potentielles impossibles à répertorier, les hackers cherchent constamment à innover afin de mieux contourner les filtres de sécurité en place. Ils combinent ainsi différentes techniques d'attaques ainsi que les vers, virus et trojans pour en concevoir de nouvelles.

Blind SQL Injection: Les Blind SQL Injections, ou "injections SQL à l'aveuglette" font partie des techniques avancées d'injections SQL. On les utilise dans le cas de scripts à réponse binaire, c'est à dire qui retournent une réponse du type soit vrai, soit faux. C'est le cas par exemple des formulaires d'authentification. Ce type de script n'affiche pas le résultat d'une injection mais indique simplement s'il y a erreur ou succès, d'où la difficulté apparente d'exploitation.
A partir d'une simple faille d'injections SQL, il est possible de récupérer des informations très importantes pour un attaquant potentiel, tels que le nombre de champs d'une table, leur type, leur nom, le nom des tables, la version du serveur etc.

Dans le cas des injections SQL dites "blind", ou "à l'aveuglette", il y'a exploitation à fond du langage SQL afin de faire révéler aux scripts vulnérables des informations cruciales.

PARTIE 3: Guide de développement des sites web universitaires

1. Recommandations liées à la portabilité:

Indépendance de la plate-forme de développement : Le site web doit être indépendant de toute plate-forme de développement surtout au niveau des liens (vérifier les liens pour éviter les liens relatifs).
Compatibilité avec les navigateurs : Le site web doit être compatible avec la majorité des navigateurs du web (i.e. Internet explorer, FireFox, …)
Résolution : Insertion des paramètres d'optimisation : indiquer la résolution qui permet une exploitation optimale du site web (exemple : résolution 1024/768 la plus standard)

2. Recommandations liées à l'ergonomie :

Temps d'ouverture : il doit être optimisé.
Emplacement et visibilité des liens : tous les liens du site web doivent être lisible.
Langues d'édition : le site web doit être complet pour chaque langue d'édition.
Structure visuelle : le site web doit être homogène pour garder l'identité graphique du site.
Navigation : La signalisation doit être lisible et facilement repérable afin de faciliter la navigation des internautes dans le site web.
Accessibilité : le site web doit être conforme aux recommandations W3C de l'accessibilité des personnes à besoin spécifique, en particulier les recommandations WCAG (www.w3.org/TR/WCAG20).

3. Recommandations liées au graphisme :

Harmonie des couleurs : Essayer de dégager une identité graphique pour le site en respectant la charte graphique préalablement définie. Vous pouvez vous permettre d'utiliser des dérivées de couleurs.

Esthétique de l'interface : Soignez bien l'interface graphique afin de dégager un visuel reflétant l'image de marque de l'établissement.

Originalité de l'interface : Éviter de reprendre des templates existantes sur le web afin de garantir l'originalité du site web.

Emplacement des éléments : L'interface du site web doit offrir un degré important de lisibilité avec une bonne disposition des éléments (textes, images, animations flash…).

Utilisation des CSS : La mise en page du site web doit passer obligatoirement par le contrôle des feuilles de style (CSS)

Insertion du copyright : pour mentionner la propriété intellectuelle.
Essayer d'avoir une bonne signalisation : pour faciliter l'accès aux différents éléments du site.

4. Recommandations liées au code source :

Conformité de la syntaxe : Essayer de standardiser la syntaxe par rapport au langage de développement ainsi qu'à la version en question.

Erreur de code : Vérifier le code en utilisant des outils de formatage ou de vérification de code pour éviter les erreurs.

Qualité des scripts : Eviter l'utilisation des scripts obtenus à partir de l'internet et qui peuvent causer des défaillances techniques au niveau du site web. (Ces scripts peuvent faire des redirections vers des sites malveillants).

Anomalies des actions dans les formulaires : Veuillez vérifier les actions de formulaires avant d'envoyer le site web pour hébergement (vérifier la validité des actions).
Optimisation des requêtes : il faut optimiser les requêtes pour optimiser le temps de réponse.

Connexion à la base de données : Pour les sites web universitaires dynamiques essayer de na pas utiliser un chemin direct pour la base de données, travailler toujours avec l'ODBC. Pour d'autres technologies il est fortement conseillé d'utiliser un seul fichier de connexion dans lequel on insère tous les paramètres d'accès à la base de données.

Version du langage de développement : Il est fortement conseillé d'utiliser les dernières versions du langage de développement (version stable) afin de profiter des améliorations apportées au niveau des fonctionnalités et de la sécurité. Notez bien que dans certains cas, il faut informer le Centre de Calcul El-Khawarizmi lors du changement de versions pour des raisons de compatibilité avec la plateforme d'hébergement. Le Centre de Calcul El-Khawarizmi n'est pas responsable des problèmes de dysfonctionnement liés à ce changement.

5. Recommandations liées au contrôle qualité :

Le code source du site web doit faire preuve au niveau des tests qualités, de sa conformité pour les versions utilisées (en fonction du langage de développement utilisé).Des tests de performance du code doivent être réalisés.

6. Recommandations liées au référencement :

Les erreurs éventuelles de code source (Norme W3C) : les outils de recherche pénalisent tous les sites web universitaires qui ne respectent pas les normes d'édition recommandées par le W3C**.**

Taille des images :

Essayer de travailler toujours en mode optimisé afin d'éviter des images lourdes (ne pas dépasser 30 Ko au max) et des pages longues (ne dépasser pas deux pages d'écran)

Test des liens : il faut vérifier tous les liens du site web afin d'éviter les liens cassés.

Analyse des balises Alt pour remplacer le contenu de l'image en cas d'un problème d'affichage par les navigateurs.

7. Recommandations liées à la maintenance :

Interface d'administration : Le site web doit avoir une interface d'administration permettant la gestion de la base de données avec un niveau optimum de gestion de la sécurité lors de l'exécution d'une action. Il est obligatoire de développer une seule base de données.

Script de backup intégré au BackOffice : De préférence, l'interface d'administration doit permettre l'exécution d'un script de sauvegarde de la base de données afin d'éviter la perte de l'information.

Gestion des versions du site : Le webmaster doit gérer l'historique des versions du site ce qui permettra d'avoir une bonne politique d'archivage des versions.

Essayer toujours d'insérer la dernière date de mise à jour : c'est très important comme information pour vos utilisateurs.

8. Recommandations liées à l'arborescence du site:

Convention de nommage : il faut essayer de donner des noms significatifs pour les fichiers (sans accent ni majuscule), exemple : la page présentation = presentation.html, .asp, .php…

Arborescence physique du site : Nous insistons sur l'organisation du site web, ce qui facilite les mises à jour et les sauvegardes. Développer avec une architecture claire, par **exemple** : si le site web est trilingue, voici l'architecture recommandée sur la racine du site web:

- Un fichier lisez moi (.txt) dans lequel vous mentionnez tous les détails techniques pour le bon fonctionnement du site web.
- Un fichier index (.html/ .php/ .asp/ .jsp) qui présente la page de démarrage du site web.
- Les dossiers relatifs aux langues du site web, chacun de ces dossiers contient l'ensemble des fichiers et dossiers relatifs à chaque langue.

Le site web doit être conçu d'une manière modulaire ce qui permettra d'avoir un niveau de facilité dans sa gestion (ajout / suppression d'un module).

9. Recommandations liées aux types d'éditeurs utilisés :

Types d'éditeurs utilisés : ne pas utiliser des éditeurs qui génèrent des codes spécifiques.

Mise à jour périodique en cas d'utilisation d'un CMS : il faut veiller à la mise à jour et à l'application des correctifs nécessaires de la version utilisée.

PARTIE 4: Plates-formes d'hébergement des sites web universitaires

1. Plates-formes d'hébergement des sites web universitaires

Le Centre de Calcul el-Khawarizmi dispose les environnements d'hébergement suivants:

- ***Systèmes d'exploitation*** **:** Windows 2000 Server, Windows 2003 Server et Linux **.**
- ***Langages de développement web***: ASP et ASP.NET, PHP4 et PHP5, JSP
- ***Bases de données*** : MYSQL 5 et MS-SQL 2000
- ***Serveurs Web*** : Apache 2, IIS 6, Tomcat 5

2. Recommandations pour les sites web universitaires dynamiques

- Un site web dynamique hébergé au CCK ne doit pas utiliser des langages de développement hybrides (par exemple PHP et ASP).
- Un site web doit utiliser une seule base de données.
- Chaque site web dynamique doit avoir un seul fichier de connexion à sa base de données qu'il suffit d'inclure dans d'autres pages nécessitant une connexion à la base.
- Dans toute page web dynamique, il est obligatoire de fermer la connexion à la base de données après s'en être servi.

3. Demandes spécifiques

Tout établissement ayant l'intention de demander un service d'hébergement ou d'accès spécifique doit informer le CCK dans les délais nécessaires et en prendre l'accord.
Une demande spécifique doit être justifiée et peut être par exemple:

- L'hébergement d'un site web utilisant un environnement autre que ceux disponibles au CCK,
- L'installation d'un kit marchant sur un site web pour mettre en oeuvre un système de paiement sécurisé,
- La demande d'installation d'un certificat SSL sur le nom de domaine d'un site web permettant ainsi d'y accéder en https,
- La demande d'accès HTTP authentifié sur quelques URLs du site,
- La demande de restreindre l'accès à quelques URLs du site (par exemple les URLs d'administration) pour certaines adresses IP,
- La demande justifiée d'un accès SSH au serveur web, etc…

PARTIE 5 : FORMULAIRE D'HEBERGEMENT D'UN SITE WEB UNIVERSITAIRES

*Ce document est à adresser **signés cachetés** sous format papier au Centre de Calcul El-Khawarizmi, cf. adresse ci-dessous.*

Nom de l'Établissement	
Adresse *(tél, fax, E-mail)*	
Nom et fonction du responsable de l'établissement	
Coordonnées personnelles *(tél, E-mail)*	
Nom du responsable du contenu du site *(site collectif ou individuel)*	
Coordonnées du responsable du contenu *(tél, fax, GSM(obligatoire), E-mail)*	
Nom du responsable technique du site (*webmaster)* *(site collectif ou individuel)*	
Coordonnées du responsable technique du site *(adresse, tél, fax, GSM(obligatoire), émail)*	

Description des objectifs du site :

……
……
……
……
……

Description de l'infrastructure matérielle nécessaire (remplir soigneusement le formulaire de détails techniques du site web) :

……
……
……
……
……
……
……

Nom du site (URL):

……

Remarques : préciser le(s) délai(s) approximatif(s) de la première mise en service du site :

……
……
……

Signature du demandeur (*)

(*)Si la demande concerne la création d'un site d'une structure d'enseignement et de recherche

Signature du responsable de l'établissement de tutelle

Accord du Directeur Général Centre de calcul el-Khawarizmi

Date : ……..

DETAIL TECHNIQUE D'UN SITE WEB

Identification

Établissement……..……
Adresse :…….……
Responsable…….……
Fonction…….……
Tél:.…… Fax:……Gsm:...… …….E-mail:…… ……..…
Structure d'appartenance (MESRST, UNIVERSITE, OOU,…)……..
URL site :…….
Responsable du contenu du site:……..……..…….....
Fonction:…… ……Tél:…..……GSM:…….....
E-mail……
Responsable(s) technique(s) du site..……
Fonction(s)…..…….....Tél(s): .....GSM:……...
E-mail(s)……..……..……

Description du site

- **Type du site web (cochez le ou les cases convenables)** :

  □ **Contenu Statique** (version actuelle finale):
  - Nombre de dossiers :……..
  - Nombre de pages (statique, dynamique):……
  - Nombre d'images :……
  - **Espace de stockage demandé (en Mo)**: ……..……
  Justifier votre choix…….……

  □ **Contenu Dynamique** (version actuelle finale):
  - Fichiers de connexion et de configuration……..……
  - Méthodes de connexion à la base (ou aux bases) :……
  - Nom de(s) base(s) :…… ……..……
  - **Espace de stockage demandé (en Mo)**: ……
  Justifier votre choix…….……..…….

  □ **Contenu du site web** (dans sa version actuelle finale):
  - **Espace de stockage demandé (en MO)**:
  Justifier votre choix…….……

- **Services offerts par le site web** :

□	Administration en ligne du site web	□	Paiement électronique
□	Intranet aux étudiants et/ou enseignants	□	Gestion d'une conférence en ligne
□	Résultats en ligne	□	Gestion des sites d'événements scientifiques : séminaires, expositions,
□	Gestion des colloques : Dépôt de demandes/dossiers en ligne…	□	Programme de recherche, projet de recherche…
□	Autres à spécifier……		

Donner ***les périodes critiques*** d'exploitation de ces services et ***les seuils*** (en nombre d'accès simultanés) qui peuvent être atteints durant ces périodes :…….

Description Technique du site web

<table>
<tr><td rowspan="7">CARACTERISTIQUES GENERALES</td><td>Nom du site web :
……..……</td><td>Version actuelle:
…..……</td></tr>
<tr><td colspan="2">Fonction(s) :
……..……
……
……
……</td></tr>
<tr><td colspan="2">Etat du site web :
☐ En étude ☐ En exploitation ☐ En cours de tests ☐ En cours de développement ☐ En cours de MAJ (refonte ou migration)</td></tr>
<tr><td colspan="2">Mode de développement :
☐ Développement en interne ☐ Développement mixte
☐Acquisition de progiciel</td></tr>
<tr><td colspan="2">Date de mise en service demandée :
……..……..…..……</td></tr>
<tr><td colspan="2">Outils de développement coté serveur :
- Langage utilisé : …..……..……
- SGBD utilisé : ……..…….……..……
- Packages à installer : …..……..……..</td></tr>
<tr><td colspan="2">Langue supportée : ☐ Arabe ☐ Français ☐ Anglais</td></tr>
<tr><td colspan="2">Observations :
……..……..……
……..……..……</td></tr>
<tr><td rowspan="2">CARACTERISTIQUES TECHNIQUES</td><td colspan="2">Configuration Requise du serveur frontal :
Processeur (mono, bi, quadri,…nombre des coeurs)……..……..……
RAM(Go)……..……Configuration disque ……
Système d’exploitation requis : ……version ……
Nombre requis de serveur(s) frontaux :…….</td></tr>
<tr><td colspan="2">Configuration Requise du serveur base de données:
Processeur (mono, bi, quadri, nombre des coeurs…)……
RAM(Go)……..……Configuration disque …….
Système d’exploitation requis : …… version ……
Version SGBDD :……
Nombre requis de serveur(s) BDD :……..</td></tr>
</table>

	Architecture du site web : ☐ 2-tiers ☐ 3-tiers ☐ n-tiers
	Programmation modulaire : ☐ OUI ☐ NON
	Nature de la BDD :☐ BDD centralisée ☐ BDD distribuée ☐ BDD parallèle ☐ Autre, à spécifier……..
	Observations: …… ……
Connection (front office)	Nombre d'utilisateurs simultanés en front office: ……
Connection (Back office)	- Nombre prévu d'accès simultanés à la base de données moyennant le site web : …….. - Nombre prévu d'accès simultanés à la base de données moyennant le logiciel client du SGBD utilisé :……

Scénario d'utilisation du site web
A décrire et à commenter:

……
……
……
……
……
……
……
……
……
……

Schéma de l'architecture du site web (à décrire et à commenter):

……
……
……
……
……
……
……

Mise à jour du contenu du site

Responsable de la mise à jour du site web..……
Fonction: …..……...E-mail:……..……
Tél:……GSM:……...……
……..

Adresse IP autorisée pour la mise à jour:……

L'adresse IP appartient au plage d'adresse IP affectée à l'établissement. Elle est routable, de la forme 41.229..X.Y où X,Y sont des nombres compris entre 2 et 254.

Signature du demandeur

Si la demande concerne la création d'un site d'une structure d'enseignement et de recherche:

Accord du Directeur Général
Centre de calcul el-Khawarizmi

Signature et cachet du responsable de l'établissement de tutelle

Date : ……..