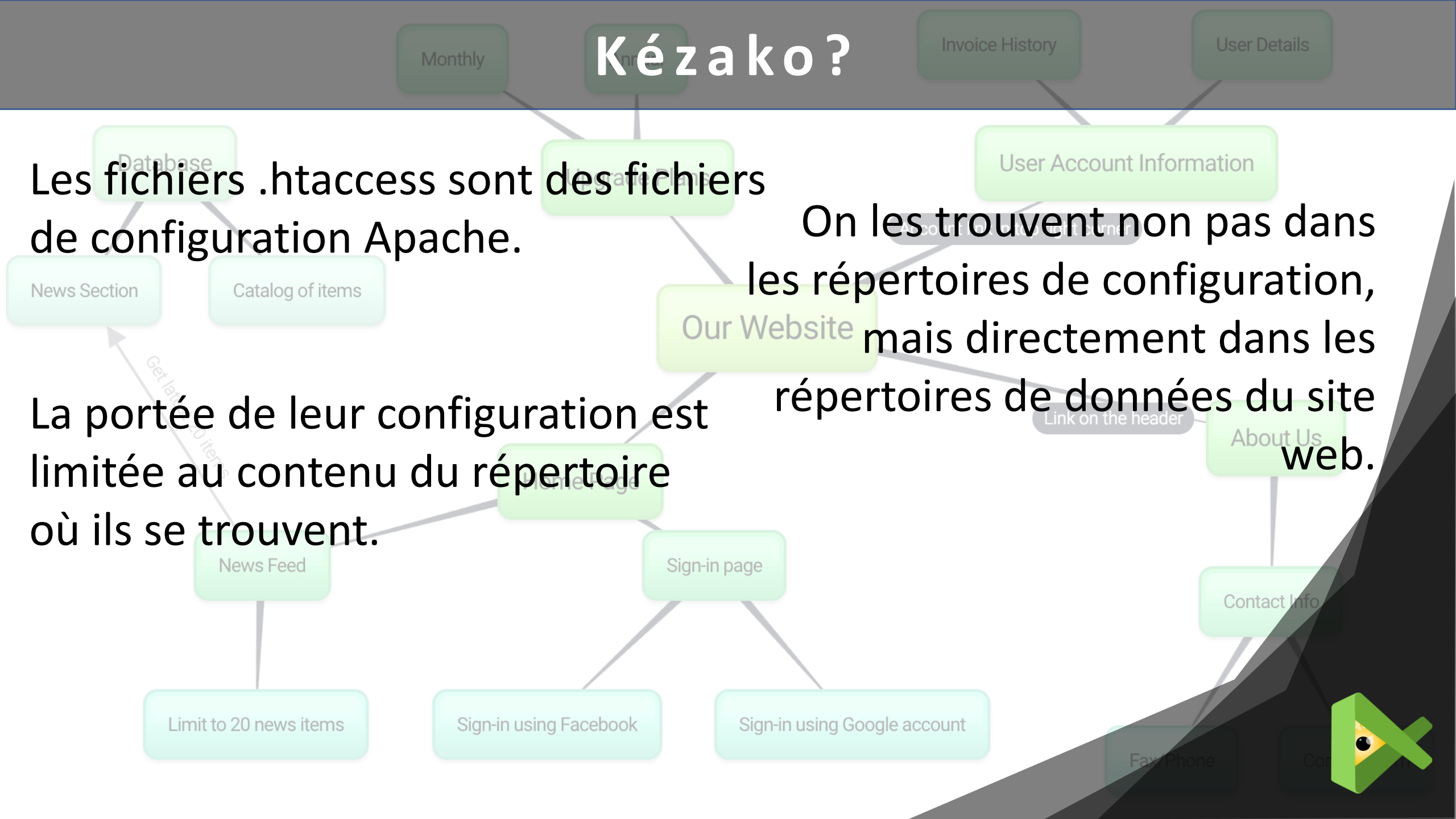
.htaccess

Kézako?

Les fichiers .htaccess sont des fichiers de configuration Apache.

La portée de leur configuration est limitée au contenu du répertoire où ils se trouvent.

On les trouvent non pas dans les répertoires de configuration, mais directement dans les répertoires de données du site web.

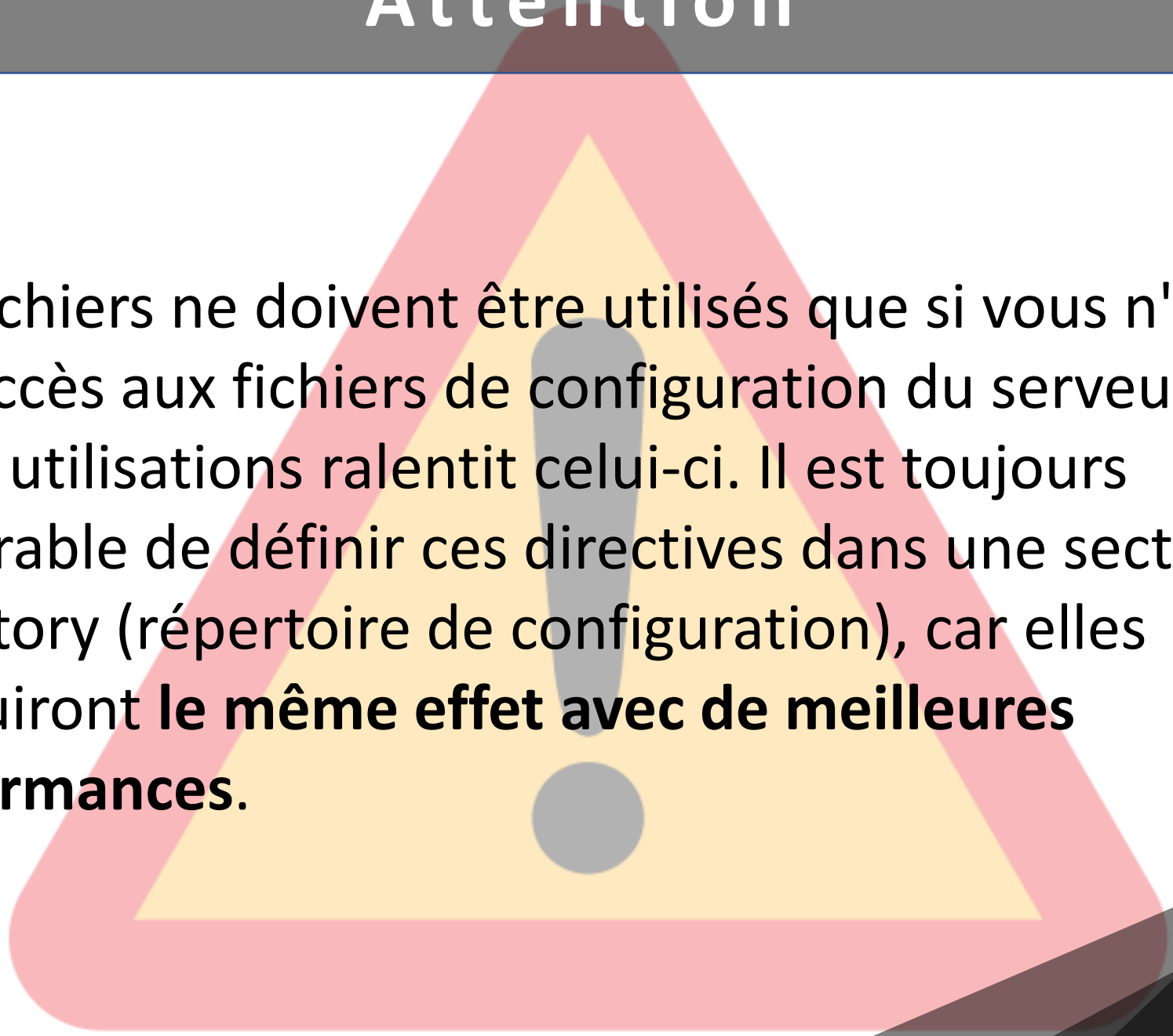


Titre page

Ces fichiers permettent à des utilisateurs n'ayant que des droits d'écriture dans les répertoires de données du site web de gérer les points suivants:

- Amélioration de la sécurité
- Redirections
- Erreurs (404, …)
- Et bien d'autres choses…

Attention



Ces fichiers ne doivent être utilisés que si vous n'avez pas accès aux fichiers de configuration du serveur. Leurs utilisations ralentit celui-ci. Il est toujours préférable de définir ces directives dans une section Directory (répertoire de configuration), car elles produiront **le même effet avec de meilleures performances**.

pratique du .htaccess
Verrouillage des répertoires

Par défaut, si vous essayez d'accéder aux répertoires d'un site, le serveur les affichera.

C'est du pain bénit pour d'éventuels attaquants.

Insérez le code suivant dans votre fichier .htaccess si vous souhaitez empêcher le listing des fichiers d'un répertoire :

```
Options All -Indexes
```

Empêcher le listing des répertoire :

```
IndexIgnore *
```

pratique du .htaccess
Cacher la signature du serveur

Certains serveurs donne des informations sur leurs systèmes (comme on en voit dans php.ini).

C’est également du pain bénit pour des attaquants.

Insérez le code suivant dans votre fichier .htaccess si vous souhaitez empêcher la transmission de ces informations:

```
ServerSignature Off
```

pratique du .htaccess
Protéger le fichier .htaccess lui-même

Les fichiers .htaccess permette de gérer une partie de la sécurité... A votre avis, quels fichiers sont ciblés en priorités par un attaquant?

Pour protéger vos fichiers .htaccess et .htpasswds, insérez ceci dans votre fichier .htaccess:

```
<Files ~ "^.*\.([Hh][Tt][AaPp])">
order allow,deny
deny from all
satisfy all
</Files>
```

pratique du .htaccess
Redirections

Pour rediriger une URL A vers une URL B, procédez comme suit :

```
Redirect 301 /anciennepage/ http://www.monsite.com/nouvellepage
```

Pour rediriger vers le protocole https (indispensable dès lors que votre site fait transiter des informations qui ne sont pas publique):

```
RewriteCond    %{SERVER_PORT} ^80$
RewriteRule    ^(.*)$ https://%{SERVER_NAME}%{REQUEST_URI} [L,R]
```

Pratique du .htaccess
Forcer le téléchargement par extention

Vous souhaitez que tout les fichier .doc, .docx et .xls soit automatiquement téléchargé lorsque l'on pointe vers eux?

Utilisez le code suivant:

```
AddType application/octet-stream .doc .docx .xls
```

pratique du .htaccess
Empêcher les injections de fichiers

Il est possible d'envoyer des fichiers sur un serveur afin d'en prendre le contrôle. Pour limiter cette possibilité, vous pouvez inclure le code suivant dans votre fichier .htaccess :

```
RewriteCond %{REQUEST_METHOD} GET
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\.\.//?)+ [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_.]//?)+ [NC]
RewriteRule .* - [F]
```

pratique du .htaccess
Protection par mot de passe

Vous souhaitez protéger les pages contenues dans un répertoire par mot de passe ? Voici le code à mettre dans le fichier .htaccess placé à la racine du dossier cible:

```
AuthName "message a afficher"
AuthType Basic
AuthUserFile "/cheminVersFichierPassword/.htpasswd"
Require valid-user
```

pratique du .htaccess
Protection par mot de passe (2)

Vos mots de passes et les noms d'utilisateurs correspondant sont stockés dans un fichier .htpasswd . Vous pouvez y mettre autant de noms et de mots de passes que souhaitez, sous le format suivant:

```
login:mot_de_passe_crypté
login:mot_de_passe_crypté
login:mot_de_passe_crypté
```

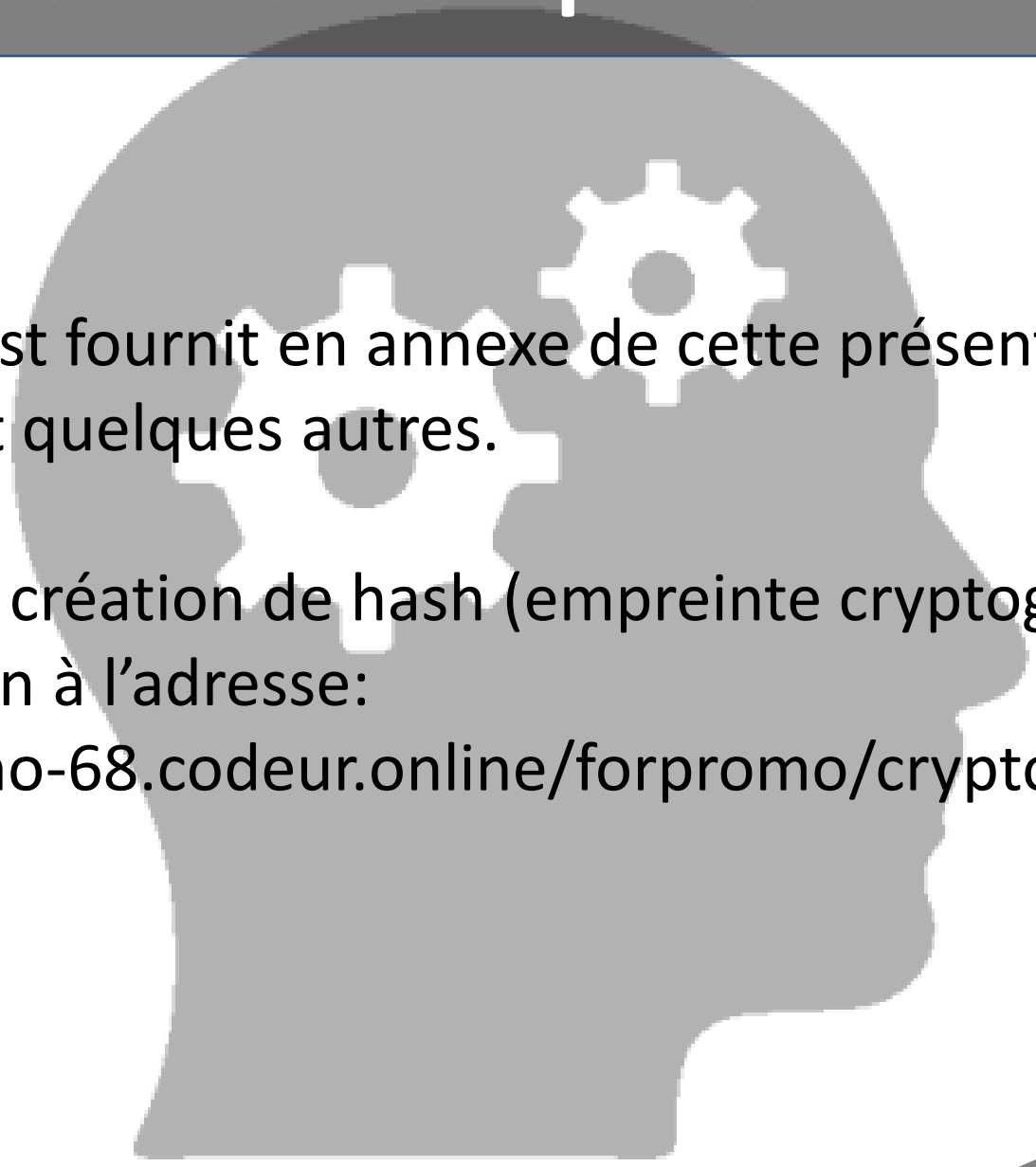
Comme indiqué, le mot de passe doit être stocké sous forme cryptée. Voyons comment procéder dans la slide suivante …

pratique du .htaccess
Protection par mot de passe (3)

Obtenir le Hash de votre mot de passe : vous pouvez utiliser une fonction php, en écrivant ceci sur une page .php :

```php
<?php
$pass_hache = password_hash($_POST['base_a_hasher'], PASSWORD_DEFAULT);
echo $pass_hache;
?>
```

Pour aller plus loin…



- Un fichier texte est fournit en annexe de cette présentation. Il reprend les codes vu ici et quelques autres.

- Un formulaire de création de hash (empreinte cryptographique) est mis à votre disposition à l'adresse:

https://adrienr.promo-68.codeur.online/forpromo/cryptokey-hash/

Sources

- https://fr.wikipedia.org/wiki/.htaccess
- https://httpd.apache.org/docs/current/fr/howto/htaccess.html