

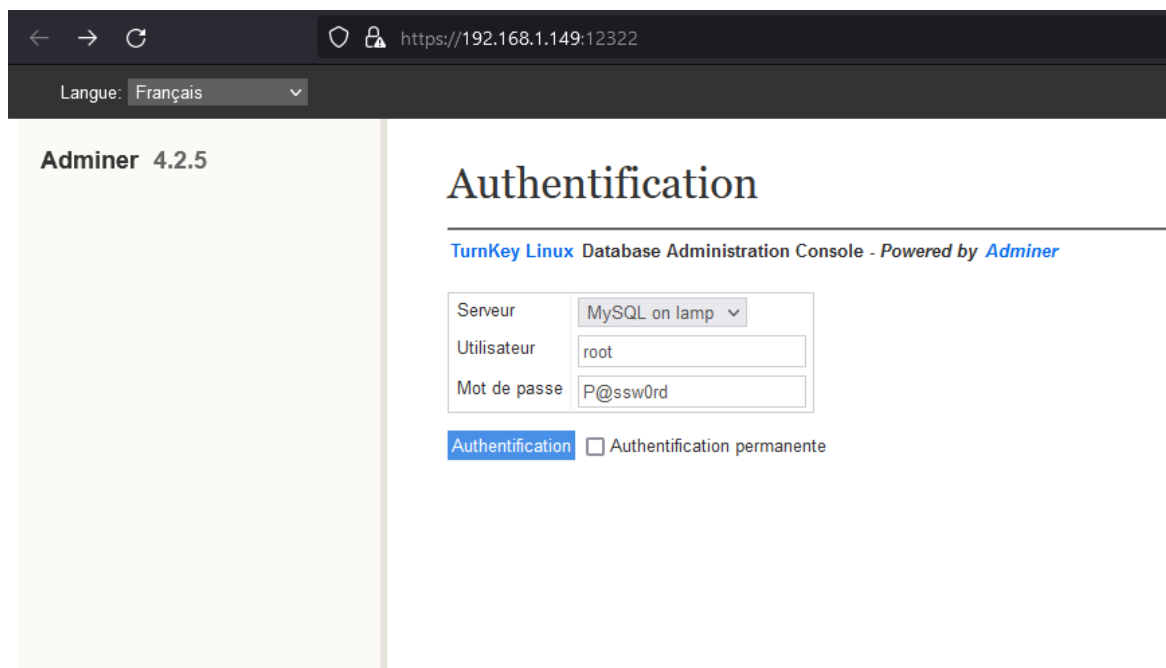
Compte-rendu – Remontée de bugs des applicatifs V2

I) – Authentification impossible sur *applifrais*

Premièrement, nous allons vérifier au niveau de la *console administrateur de la base donnée*, si l'utilisateur *gsbuser* existe ainsi que son mot de passe *gsbsecret*.

Pour cela, nous entrons donc dans le champ Utilisateur : *root* ;

Ainsi que son mot de passe : *P@ssw0rd*



Nous cliquons ensuite sur le terme *Privilèges*, qui comme son nom l'indique, va nous lister l'ensemble des comptes existants ainsi que les privilèges qu'ils possèdent.



Base de données - Rafraîchir	Interclassement	Tables	Taille - Calcul
<input type="checkbox"/> information_schema	utf8_general_ci	?	?
<input type="checkbox"/> festival	utf8_general_ci	?	?
<input type="checkbox"/> gsb_frais	utf8_general_ci	?	?
<input type="checkbox"/> mysql	utf8_general_ci	?	?
<input type="checkbox"/> performance_schema	utf8_general_ci	?	?

Nous remarquons qu'il existe bel et bien l'utilisateur *Martin*, nous cliquons alors sur *Modifier* pour vérifier ses privilèges.

Langue: Français
MySQL » localhost » Privilèges

Adminer 4.2.5
DB:
Requête SQL Importer Exporter

Privilèges

Utilisateur	Serveur	
root	127.0.0.1	Modifier
root	:::1	Modifier
debian-sys-maint	localhost	Modifier
festival	localhost	Modifier
martin	localhost	Modifier
root	localhost	Modifier

Créer un utilisateur

Nous remarquons également que ce dernier a eu l'entièreté des privilèges qui lui ont été accordés, donc nous allons pouvoir nous connecter à la *base de donnée du serveur de production*.

Langue: Français
MySQL » localhost » Privilèges » Utilisateur: martin@localhost

Adminer 4.2.5
DB:
Requête SQL Importer Exporter

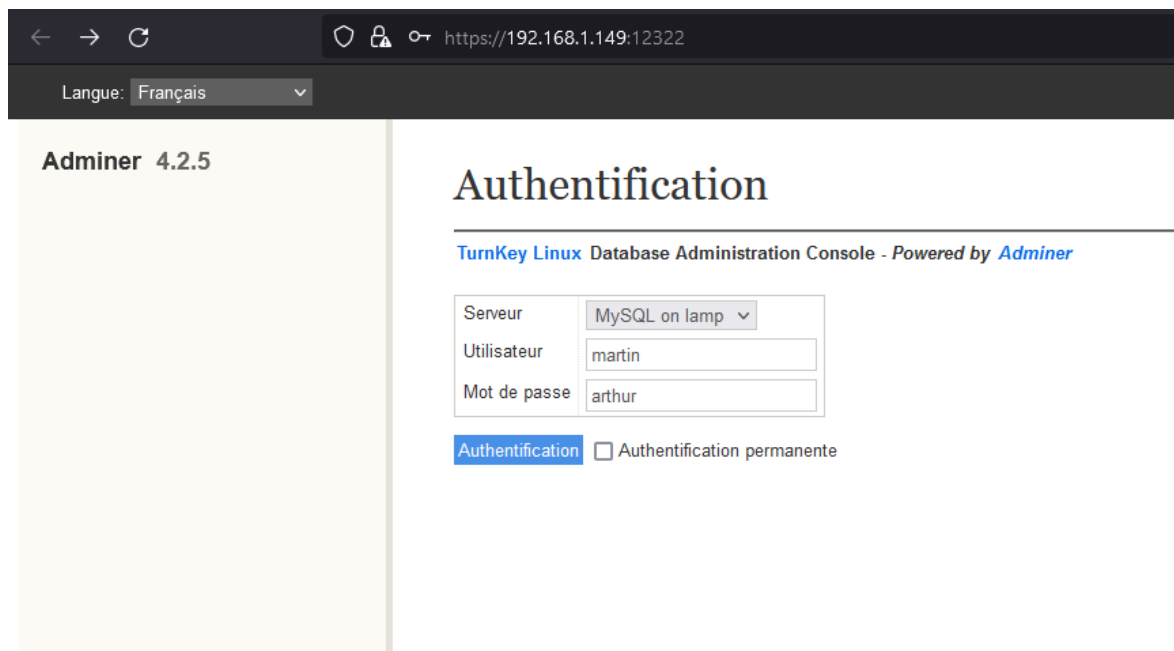
Utilisateur: martin@localhost

Serveur: localhost
Utilisateur: martin
Mot de passe: ☒ *234FAA6BBCDA359B6D2E Haché

Privilèges ?		*gsbl_frais*.*	.*
All privileges		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Grant option		<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Create user	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Event	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Process	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Proxy	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Reload	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Replication client	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Replication slave	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Show databases	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Shutdown	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Super	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	Create tablespace	<input type="checkbox"/>	<input type="checkbox"/>
Serveur	File	<input type="checkbox"/>	<input type="checkbox"/>
Base de données	Create routine	<input type="checkbox"/>	<input type="checkbox"/>
Base de données	Create temporary tables	<input type="checkbox"/>	<input type="checkbox"/>
Base de données	Lock tables	<input type="checkbox"/>	<input type="checkbox"/>
Table	Alter	<input type="checkbox"/>	<input type="checkbox"/>
Table	Create	<input type="checkbox"/>	<input type="checkbox"/>
Table	Create view	<input type="checkbox"/>	<input type="checkbox"/>
Table	Delete	<input type="checkbox"/>	<input type="checkbox"/>
Table	Drop	<input type="checkbox"/>	<input type="checkbox"/>
Table	Index	<input type="checkbox"/>	<input type="checkbox"/>
Table	Insert	<input type="checkbox"/>	<input type="checkbox"/>
Table	References	<input type="checkbox"/>	<input type="checkbox"/>
Table	Select	<input type="checkbox"/>	<input type="checkbox"/>
Table	Show view	<input type="checkbox"/>	<input type="checkbox"/>
Table	Trigger	<input type="checkbox"/>	<input type="checkbox"/>
Table	Update	<input type="checkbox"/>	<input type="checkbox"/>
Colonne	Select	<input type="checkbox"/>	<input type="checkbox"/>
Colonne	Insert	<input type="checkbox"/>	<input type="checkbox"/>
Colonne	Update	<input type="checkbox"/>	<input type="checkbox"/>
Colonne	References	<input type="checkbox"/>	<input type="checkbox"/>
Routine	Alter routine	<input type="checkbox"/>	<input type="checkbox"/>
Routine	Execute	<input type="checkbox"/>	<input type="checkbox"/>

Enregistrer
Supprimer

Nous revenons donc en arrière et nous entrons donc dans le champ Utilisateur : *martin* ; Ainsi que son mot de passe (qui nous a été miraculeusement fournis) : *arthur*



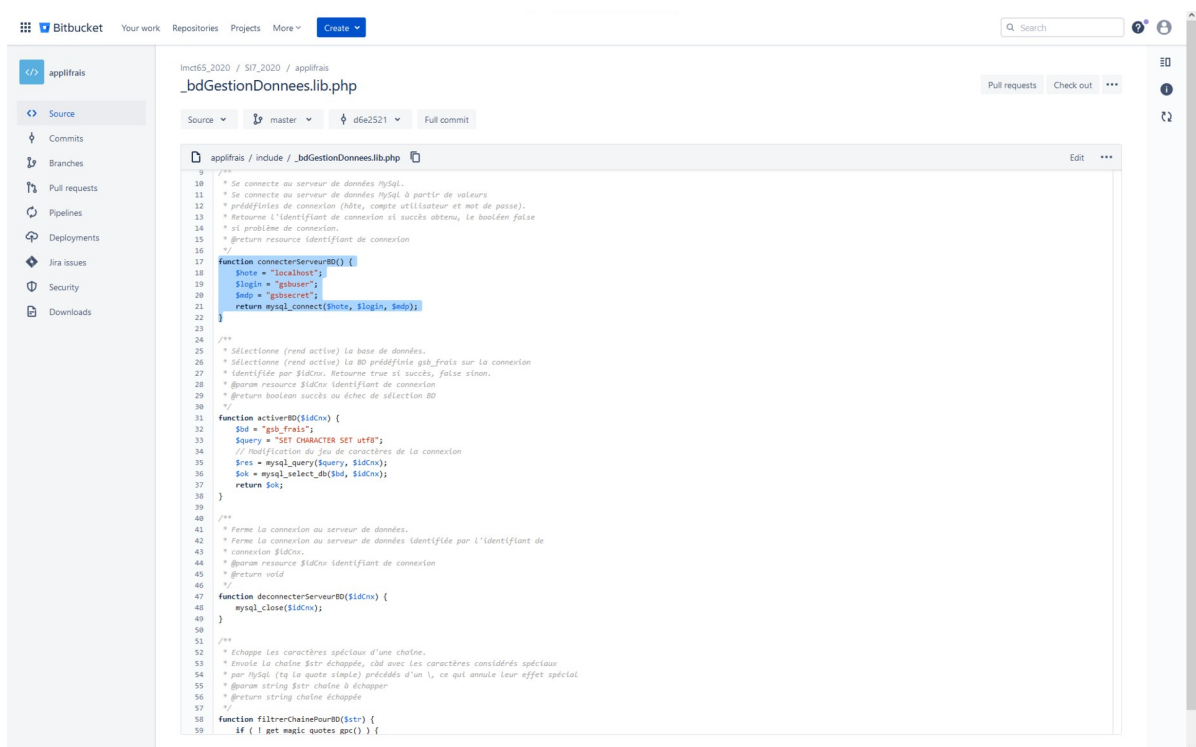
Nous accédons donc a une base de données totalement différente avec cet identifiant et ce mot de passe. Nous en déduisons qu'il y a un *environnement de travail pour le serveur de production*, ainsi qu'un *environnement de travail pour le développeur*.



Base de données - Rafraichir	Interclassement	Tables	Taille	Calcul
<input type="checkbox"/> information_schema		?		?
<input type="checkbox"/> gsb_frais	utf8_general_ci	?		?

Cela signifie donc, qu'il nous faut nous rendre dans le fichier *_bdGestionDonnees.lib.php*, aux lignes 17-22 où sont inscrits l'utilisateur et le mot de passe se connectant à la base de donnée locale du développeur.

Nous y retrouvons donc bien le *gsbuser* ainsi que son mot de passe *gsbsecret* qu'ils n'existent que sur la base de données locale du développeur. Nous les modifions donc par *martin* et son mot de passe *arthur* afin que Monsieur Arthur Martin puisse enfin se connecter par la suite.



Une fois ici, nous retournons sur la **console de la base de donnée du serveur de production**, ou nous cliquons sur **gsb_frais** ; puis **visiteur** ; puis **afficher les données**.
A partir d'ici, nous prenons n'importe quel **utilisateur** ainsi que son **mot de passe** pour se connecter à la nouvelle version de **applifrais**.

Adminer 4.2.5

Sélectionner la base de données

DB: gsb_frais

Requête SQL Importer Exporter

Authentifié en tant que: root@localhost

Base de données	Table	Interschema	Table	Catégorie
gsb_frais	visiteur	visiteur	visiteur	visiteur

Sélectionner la table: gsb_frais.visiteur

Table: Visiteur

Colonne	Type	Commentaire
id	CHAR(3)	
nom	CHAR(3)	
prénom	CHAR(3)	
login	CHAR(3)	
mdp	CHAR(3)	
adresse	CHAR(3)	
cp	CHAR(3)	
ville	CHAR(3)	
dateEnbauche	DATE	

Index

PRIMARY id

Modifier les index

Clics étranges

Diélecteurs

Ajoutez vos diélecteurs

Adminer 4.2.5

Base de données: gsb_frais

DB: gsb_frais

Requête SQL Importer Exporter

Authentifié en tant que: root@localhost

Tables et vues

Table	Interschema	Longueur des données	Longueur de l'index	Espace indexé	Incarnation automatique	Logins	Commentaires
visiteur	visiteur	16,384	0	1,338,000	-4		

Routines

Evénements

Sélectionner: Visiteur


Afficher les données Afficher la structure Modifier la table Nouvel élément

Sélection: 1-100

SELECT * FROM gsb_frais.visiteur LIMIT 10 (0.000 s)

id	nom	prénom	login	mdp	adresse	cp	ville	dateEnbauche
1	visiteur	visiteur	visiteur	visiteur	visiteur	visiteur	visiteur	visiteur

Nous essayons donc de nous connecter avec un *Utilisateur* ainsi que son *mot de passe* (tout deux choisis au hasard), et nous pouvons donc nous connecter.





Suivi du remboursement des frais

Villechalane Louis
Visiteur médical
Accueil
Se déconnecter
Saisie fiche de frais
Mes fiches de frais

Identification utilisateur

* Login :

* Mot de passe :

Cette page est conforme aux standards du Web



Suivi du remboursement des frais

Villechalane Louis
Visiteur médical
Accueil
Se déconnecter
Saisie fiche de frais
Mes fiches de frais

Bienvenue sur l'intranet GSB

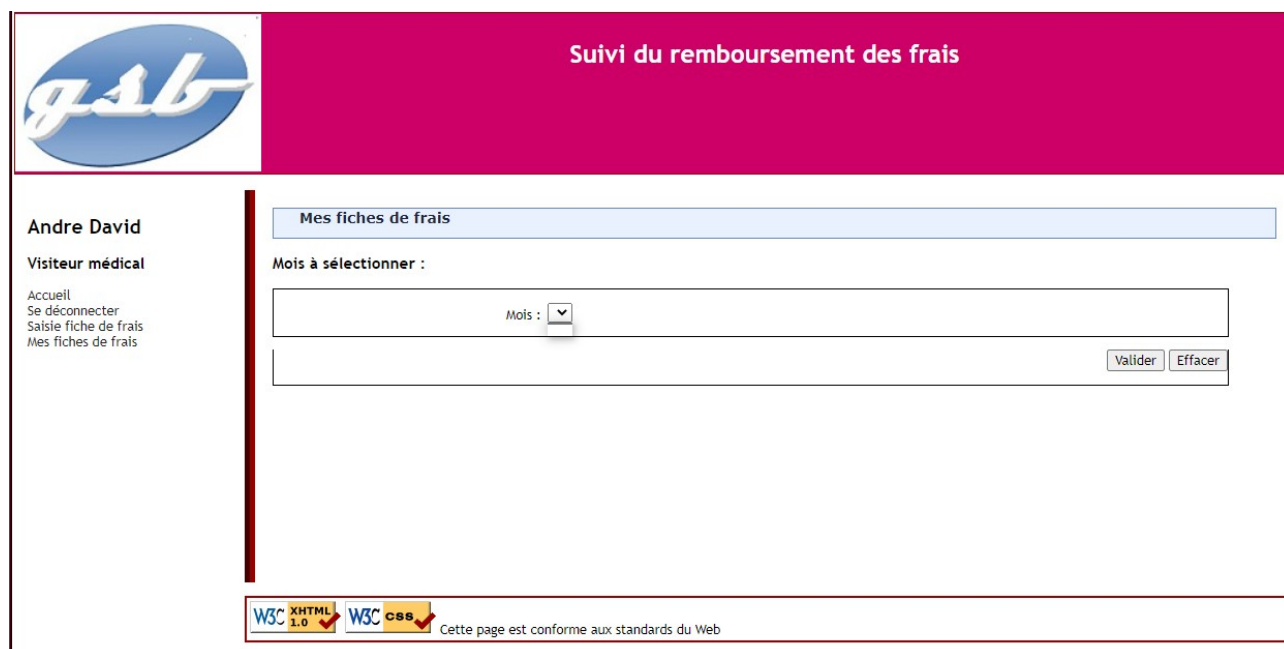
 

Cette page est conforme aux standards du Web

II) – Bugs

Bugs 0000001

Le client se retrouve face à une liste déroulante vide supposée afficher ses fiches de frais.



Pour connaître la source de ce bug, nous décidons de regarder dans les logs d'erreurs accessibles sur le serveur.

```
PHP 1. (main)() /var/www/applifrais/cConsultFichesFrais.php:0, referer: http://192.168.1.126:8080/cConsultFichesFrais.php
PHP 2. mysql_fetch_assoc() /var/www/applifrais/cConsultFichesFrais.php:54, referer: http://192.168.1.126:8080/cConsultFichesFrais.php
PHP Warning: mysql_free_result() expects parameter 1 to be resource, boolean given in /var/www/applifrais/cConsultFichesFrais.php on line 64, referer: http://192.168.1.126:8080/cConsultFichesFrais.php
PHP Stack trace: referer: http://192.168.1.126:8080/cConsultFichesFrais.php
```

Donc en regardant la ligne correspondante à notre erreur, on peut voir une erreur à la ligne 64 du fichier *cConsultFicheFrais.php*. On se rend donc à la ligne 64 dans le fichier *cConsultFicheFrais.php*

```
<?php
<label for="lstMois">Mois : </label>
<select id="lstMois" name="lstMois" title="Sélectionner le mois souhaité pour la fiche de frais">
<?php
// on propose tous les mois pour lesquels le visiteur a une fiche de frais
$req = obtenirRegMoisFicheFrais(obtenirIdUserConnecte());
$idJeuMois = mysql_query($req, $idConnexion);
while ( $idJeuMois ) {
    $mois = $idJeuMois["mois"];
    $noMois = intval(substr($mois, 4, 2));
    $annee = intval(substr($mois, 0, 4));
}
<option value=""><?php echo $mois; ?><?php if ($moisSaisi == $mois) { ?> selected="selected"<?php ?>
<?php
    $idMois = mysql_fetch_assoc($idJeuMois);
    mysql_free_result($idJeuMois);
}
</select>
```

```
46 46 <?php
47 47 <label for="lstMois">Mois : </label>
48 48 <select id="lstMois" name="lstMois" title="Sélectionner le mois souhaité pour la fiche de frais">
49 49 <?php
50 50 // on propose tous les mois pour lesquels le visiteur a une fiche de frais
51 51 // Utilisation de la nouvelle fonction optimisee
52 52 $req = obtenirRegMoisFicheFrais2(obtenirIdUserConnecte());
53 53 $idJeuMois = mysql_query($req, $idConnexion);
54 54 $idMois = mysql_fetch_assoc($idJeuMois);
55 55 while ( $idJeuMois ) {
56 56     $mois = $idJeuMois["mois"];
57 57     $noMois = intval(substr($mois, 4, 2));
58 58     $annee = intval(substr($mois, 0, 4));
59 59 }
60 60 <option value=""><?php echo $mois; ?><?php if ($moisSaisi == $mois) { ?> selected="selected"<?php ?>
61 61 <?php
62 62     $idMois = mysql_fetch_assoc($idJeuMois);
63 63     mysql_free_result($idJeuMois);
64 64
65 65
```

En comparant avec la v1, on ne constate aucune différence. Le problème vient donc de la fonction `obtenirReqMoisFicheFrais()`.

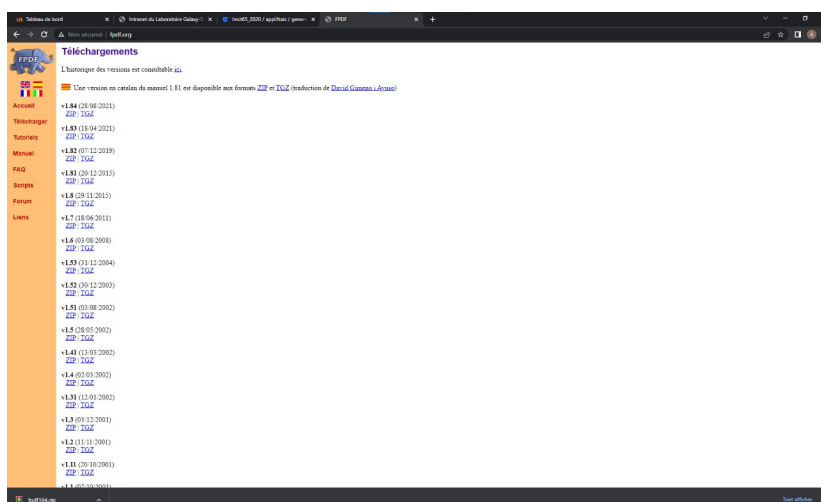
```
function obtenirReqMoisFicheFrais2($unIdVisiteur) {  
    $req = "select mois from fichefrais where idvisiteur ='"  
        . $unIdVisiteur . "' order by 1 desc ";  
    return $req ;  
}
```

En regardant dans la requête, on s'aperçoit que le nom de la table est correctement orthographié, cependant le serveur de production fonctionnant avec linux, et le serveur de développement avec Windows. Les deux systèmes ont une tolérance différente face à la casse. Le serveur Linux est plus sensible et exige que les nom de table soit orthographiés de la même façon (même casse) dans le requête que dans la table, ce qui n'est pas le cas avec Windows qui lui vérifie seulement que le nom correspond bien, qu'importe la casse des caractères.

Cependant la résolution ne s'arrête pas ici. En tentant de généré le pdf, on obtient une page d'erreur. Le problème vient de la librairie FPDF. En effet, dans le fichier `générerPDF.php`, le programme requiert l'utilisation de cette librairie pour générer un pdf.

```
require('fpdf/fpdf.php');
```

La solution consiste à télécharger ladite librairie depuis le site de son éditeur.



Et mettre le dossier dans le serveur à l'intérieur du répertoire de l'application applifrais.

Nom de fichier	Taille de fi...	Type de fic...	Dernière modif...	Droits d'ac...	Propriétaire...
fpdf		Dossier de ...			
images		Dossier de ...	15/09/2022 10:...	drwxr-xr-x	root root
include		Dossier de ...	29/09/2022 12:...	drwxr-xr-x	root root
scripts		Dossier de ...	15/09/2022 10:...	drwxr-xr-x	root root
styles		Dossier de ...	15/09/2022 10:...	drwxr-xr-x	root root
cAccueil.php	611	Fichier sou...	15/09/2022 10:...	-rw-r--r--	root root
cConsultFichesFrais.p...	7 627	Fichier sou...	15/09/2022 10:...	-rw-r--r--	root root
cSaisieFicheFrais.php	8 361	Fichier sou...	15/09/2022 10:...	-rw-r--r--	root root
cSeConnecter.php	2 377	Fichier sou...	15/09/2022 10:...	-rw-r--r--	root root
cSeDeconnecter.php	273	Fichier sou...	15/09/2022 10:...	-rw-r--r--	root root
genererPDF.php	4 562	Fichier sou...	29/09/2022 12:...	-rw-r--r--	root root

Sélection de 1 fichier. Taille totale : 4 562 octets

Bugs 0000003

Pour ce bug, nous remarquons très vite qu'il provient du service web Festival. En effet, ce dernier possède un bug quant-à la création de nouveaux établissement. Ces derniers ne prennent pas en compte l'image qui leur ait associé, et donc ne l'affichent pas.

Pour cela, nous commençons par aller sur la console web du service Festival et nous regardons le contenu du dossier *images* ; pour cela nous entrons la commande suivante :
ls /var/www/festival/images

Nous remarquons qu'aucune des deux images ajoutées aux deux établissements que nous avons créés, n'est présente.

Etablissements			
Collège Ste Jeanne d'Arc-Choisy	Voir détail	Modifier	
Collège de Moka	Voir détail	Modifier	
Institution Saint-Malo Providence	Voir détail	Modifier	
Établibug	Voir détail	Modifier	Supprimer
Essaie	Voir détail	Modifier	Supprimer
Centre de rencontres internationales	Voir détail	Modifier	Supprimer

[Création d'un établissement](#)

Essaie	
Id:	055665
Adresse:	1 Test rue des Essaies
Code postal:	64500
Ville:	EssaieVille
Téléphone:	0123654987
E-mail:	
Type:	Autre établissement
Responsable:	Madame dzzdzd rgrgrgrrr

[Retour](#)

Établibug	
Id:	04185125
Adresse:	2 Bug rue du Test
Code postal:	65500
Ville:	Bugville
Téléphone:	0123456789
E-mail:	bug@unbuged.com
Type:	Etablissement scolaire
Responsable:	Monsieur bug? bug!

[Retour](#)

C'est alors que nous continuons nos recherches en allant inspecter les logs du serveur web, au sein du fichier *error.log* se trouvant dans l'arborescence suivante : */var/log/apache2*

Le bug lié à cette prise en compte des images ou non, devrait alors être inscrit dans les logs, et ceux dans les dernières lignes qui sont les plus récentes.

Après un peu de recherches, nous trouvons enfin les lignes d'erreurs.

```
[Thu Sep 29 07:59:41.966314 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP Warning:
move_uploaded_file(images/image2.png): failed to open stream: Permission denied in
/var/www/festival/cGestionEtablissements.php on line 41, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966362 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP Stack trace:, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966382 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 1. {main}()
/var/www/festival/cGestionEtablissements.php:0, referer: http://192.168.1.126:8888/cGestionEtablissements.php?
action=demanderCreerEtab
[Thu Sep 29 07:59:41.966398 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 2.
chargementFichier() /var/www/festival/cGestionEtablissements.php:113, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966411 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 3. move_uploaded_file()
/var/www/festival/cGestionEtablissements.php:41, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab

[Thu Sep 29 07:59:41.966443 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP Warning:
move_uploaded_file(): Unable to move '/tmp/php92c9sj' to 'images/image2.png' in
/var/www/festival/cGestionEtablissements.php on line 41, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966452 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP Stack trace:, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966464 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 1. {main}()
/var/www/festival/cGestionEtablissements.php:0, referer: http://192.168.1.126:8888/cGestionEtablissements.php?
action=demanderCreerEtab
[Thu Sep 29 07:59:41.966475 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 2.
chargementFichier() /var/www/festival/cGestionEtablissements.php:113, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
[Thu Sep 29 07:59:41.966487 2022] [:error] [pid 1262] [client 192.168.1.109:55390] PHP 3.
move_uploaded_file() /var/www/festival/cGestionEtablissements.php:41, referer:
http://192.168.1.126:8888/cGestionEtablissements.php?action=demanderCreerEtab
```

Après inspection, nous remarquons que les erreurs proviennent des lignes 41 et 113 du fichier *cGestionEtablissements.php* ; et en les observants sur le BitBucket de *festival*, nous voyons qu'à la ligne 41 il s'agit de la condition :

```
if (! move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
```

Ainsi qu'à la ligne 113, il s'agit de la fonction :

```
chargementFichier()
```

Après quelques recherches sur internet, nous apprenons que le bug pourrait potentiellement venir du fichier de configuration du serveur nommé *php.ini*. Ce dernier se trouvant alors à l'adresse suivante, que nous entrons dans FileZilla après s'être connecté au serveur SFTP de notre service web : */etc/php5/apache2*

Il faut donc nous rendre aux lignes 820 et 660 du fichier *php.ini* et modifier la taille maximum des variable *upload_max_filesize* et *post_max_size* à 8M.

```
817
818 ; Maximum allowed size for uploaded file
819 ; http://php.net/upload-max-filesize
820 upload_max_filesize = 8M
821
```

```

656 ; Maximum size of POST data that PHP will accept.
657 ; Its value may be 0 to disable the limit. It is ignored if POST data reading
658 ; is disabled through enable_post_data_reading.
659 ; http://php.net/post-max-size
660 post_max_size = 8M

```

Une fois cela modifié et envoyé sur le serveur SFTP, nous essayons d'ajouter nos fichiers images aux établissements du service web. Nous inspectons ensuite le dossier images à l'adresse suivante sur FileZilla : `/var/www/images`

Et nous remarquons effectivement que les deux images ont bien été ajoutées au dossier en question, ce qui confirme bien que le bug a été résolu.

Hôte : `ftp://192.168.1.126` Nom d'utilisateur : `root` Mot de passe : `*****` Port : Connexion rapide

Statut : Démarrage de l'envoi de `C:\Users\PUJOL\Desktop\Projet de gestion des configurations\NantesLaColiniere.jpg`
Statut : Transfert de fichier réussi, 647 830 octets transférés en 1 seconde
Statut : Transfert de fichier réussi, 1 665 874 octets transférés en 1 seconde
Statut : Récupération du contenu du dossier « `/var/www/images` »...
Statut : Listing directory `/var/www/images`
Statut : Contenu du dossier « `/var/www/images` » affiché avec succès

Site local : `C:\Users\PUJOL\` Site distant : `/var/www/images`

Nom de fichier Taille de fi... Type de fic... Dernière modification Droits d'ac... Propriétai

Nom de fichier	Taille de fi...	Type de fic...	Dernière modification	Droits d'ac...	Propriétai
adminer.png	7 505	Fichier PNG	19/04/2017 08:13:08	-rw-r--r--	root root
DijonLeCastel.jpg	1 665 874	Fichier JPG	29/09/2022 12:55:53	-rw-r--r--	root root
NantesLaColiniere.jpg	647 830	Fichier JPG	29/09/2022 12:55:53	-rw-r--r--	root root
shell.png	7 104	Fichier PNG	19/04/2017 08:13:08	-rw-r--r--	root root
tab.png	734	Fichier PNG	19/04/2017 08:13:08	-rw-r--r--	root root
webmin.png	9 970	Fichier PNG	19/04/2017 08:13:08	-rw-r--r--	root root

13 fichiers et 32 dossiers. Taille totale : 7 687 993 octets

6 fichiers. Taille totale : 2 339 017 octets

Serveur / Fichier local Direction Fichier distant Taille Priorité Statut