



Assurance des véhicules des employés de l'agence HsH de VICHY



Présentation de l'entreprise HsH (« Home sweet Home »)

HsH : Chiffres et Services

HsH est l'un des premiers réseaux immobilier français.

- Créée en 1984, HsH est aujourd'hui le troisième réseau d'agences immobilières en France.
- Plus de 1 000 points de ventes répartis sur tout le territoire, une implantation et des moyens qui favorisent les transactions grâce à nos 5 500 collaborateurs.
- Le réseau HsH bénéficie d'un atout unique dans le secteur de l'immobilier : son fichier commun de plus de 100 000 biens.
- 5 500 collaborateurs.
- Plus de 50 000 transactions par an.
- Plus de 100 000 annonces sur www.HsH-immo.com
- Un site central et des sites locaux.
- Plus de 35 ans de succès.

Une gamme de services complète pour répondre à l'ensemble des besoins de ses clients :

- Achat et vente
- Gestion locative
- Gestion de syndic de copropriété
- Immobilier d'entreprise et fonds de commerce
- Aide au financement

L'agence de Vichy



M. JAVERZAC gère l'agence HsH de Vichy qui emploie une équipe de 9 commerciaux qui jouent le rôle d'intermédiaires entre vendeur et acheteur, propriétaire et locataire.

Avant d'afficher un bien en vitrine, ils le visitent, l'évaluent et négocient les conditions de vente ou de location.

Actuellement, l'agence ne possède aucune voiture de société : les employés utilisent leur véhicule personnel lors de leurs déplacements professionnels.

M. JAVERZAC a négocié auprès de son assureur, Séraphin LAMPION, Directeur des Assurances MONDASS, un contrat permettant de couvrir l'ensemble des voitures de ses salariés, lors des déplacements professionnels.

Il souhaite donc pouvoir centraliser l'ensemble des données (marque, modèle, immatriculation, carte grise, etc.) qu'il transmettra à son assureur.

Le prestataire informatique

Créée en 1997, SIVY (« Société d'informatique de Vichy ») est une entreprise de services du numérique (ESN) spécialisée dans le conseil en systèmes et logiciels informatiques (administration systèmes et réseaux, logiciels de gestion, développement web, etc...).

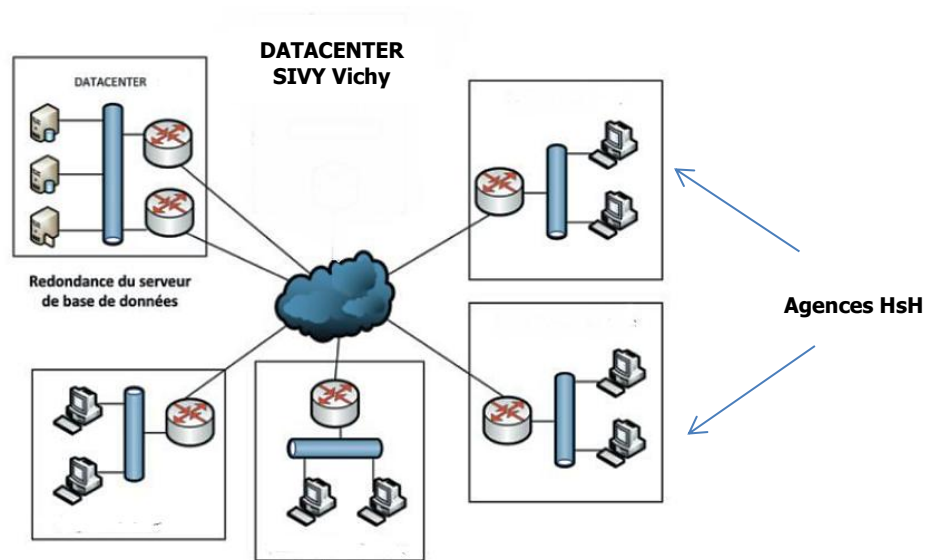
Depuis 2019, SIVY en pleine croissance en particulier dans le bassin Vichyssois, a procédé à une fusion par apport de titres avec HsH. De ce fait, SIVY est devenu une filiale de HsH. L'ESN SIVY est organisée en trois pôles de compétences :

- Infrastructures et serveurs qui ont pour activité le paramétrage et la sécurisation des éléments d'interconnexion et des serveurs ;
- Gestion des applications qui est dédié au développement d'applications spécifiques pour les besoins de ses clients ;
- Données à caractère personnel et données sensibles qui a pour mission de veiller à l'identification des risques et au respect de la législation sur les données à caractère personnel.

C'est tout naturellement que HsH a confié à SIVY la gestion de l'ensemble de son informatique.

L'infrastructure informatique de HsH s'organise de la manière suivante :

- chaque agence est interconnectée par une liaison VPN (« Virtual Private Network ») ;
- SIVY assure une continuité des accès à ses serveurs via une redondance de ses éléments d'interconnexion ;
- La redondance des serveurs de bases de données assure la continuité des accès aux données stockées, notamment aux données à caractère personnel.



Les logiciels de gestion de l'agence (catalogue, clients, devis, facturation...) ont été développés par le Département « Gestion des applications » de HsH, autour d'une plateforme Intranet, donc en utilisant les technologies du web :

- HTML et feuilles de style CSS.
- JavaScript / PHP.
- Système de Gestion de Bases de données MySQL.
- Etc...

PREMIERE PARTIE – Conception et développement de l'application web / bases de données



Il s'agit de développer une fonctionnalité supplémentaire : une interface de GESTION DES DONNEES RELATIVES AUX VOITURES que les commerciaux utilisent lors de leurs déplacements.

Les tâches qui vous sont confiées sont les suivantes :

- Concevoir et mettre en œuvre la BD à partir du recueil des données, effectué par le chef de projet (cf. paragraphe suivant).
- Modifier un script PHP (fourni) permettant d'afficher le contenu des MODELES de voitures (une table « MODELE » a été créée pour tester le script) dans un tableau HTML en utilisant une feuille de style CSS.
- Ecrire des scripts permettant :
 - L'ajout de nouvelles données dans la table « MODELE » ;
 - L'ajout simultané des données d'une VOITURE et de sa CARTE GRISE ;
 - De retrouver tous les PROPRIETAIRES d'un MODELE donné.
- Elaborer un JEU DE TEST (=données insérées dans la BD) permettant de valider les scripts précédents.

On vous fournit le DOSSIER D'ANALYSE suivant, contenant le recueil des données à implémenter dans la future BD, des exemples de données, des maquettes d'écran avec leurs fonctionnalités, et des renseignements techniques :

Recueil des données

Données	Commentaires
Nom du propriétaire	
Prénom du propriétaire	
Adresse du propriétaire	
Ville du propriétaire	
Code Postal du propriétaire	
Libellé du modèle de voiture	
Carburant du modèle de voiture	Valeurs possibles : ESSENCE, DIESEL, GPL, ELECTRIQUE
Numéro d'immatriculation de la voiture	Format : AA-999-AA
Couleur de la voiture	Valeurs possibles : claire, moyenne, foncée
Date de la carte grise	

Exemple de contenu de la table MODELE (table créée pour tester le script PHP fourni)

Volkswagen	essence
Renault	essence
Volkswagen	diesel
Renault	diesel
Peugeot	diesel
Peugeot	gpl
Ligier	electriq
Mercedes	essence
Range Rover	essence

Extrait de la liste des employés (gérée actuellement sous EXCEL)

	A	B	C	D	E
1	Davolio	Rose	5, rue de la Poste	03200	VICHY
2	Fuller	Andrew	Place de la Gare	03200	VICHY
3	Daverling	Janet	1, Boulevard d'Italie	03200	VICHY
4	Peacock	Margaret	23, Impasse des Fleurs	03000	MOULINS
5	Buchanan	Steven	15, Place de l'Hôtel de Ville	03000	MOULINS
6	Bucyama	Michael	15, Rue des Pinsons	03000	MOULINS
7	King	Andrew	57, Boulevard de la Gare	03000	MOULINS
8	Callahan	Laura	23, Boulevard Central	03100	MOUNTLUCON
9	Bucsworth	Annette	7, rue de la Paix	03100	MONTLUCON

DOCUMENTS : liste de voitures et carte grise

	Stock de Voitures	Date Mise en Circulation
BR-363-SJ	Volkswagen claire Essence	21/02/2011
SR-163-RJ	Volkswagen Moyenne Essence	21/02/2011
AZ-147-QA	Renault foncée Essence	22/02/2011
RT-578-00	Volkswagen claire Diesel	22/02/2011
TT-123-AM	Peugeot foncée GPL	23/02/2011

Carte Grise

Propriétaire : Rose DAVOLIO Date : 21/02/2011
 5, Rue de la Poste
 03200 Vichy

Véhicule : BR-363-SJ Volkswagen
 Couleur : Claire
 Carburant : Essence

REGLES de GESTION

- A chaque VOITURE on associe un MODELE et une COULEUR (prises dans l'ensemble des valeurs autorisées).
- Une CARTE GRISE concerne un seul PROPRIETAIRE et une VOITURE.
- Pour un PROPRIETAIRE, on peut établir plusieurs CARTES GRISES.

L'INTERFACE WEB – pages à développer

Les scripts PHP à développer doivent utiliser des feuilles de style CSS. Un premier script, avec sa feuille de style CSS, permet d'afficher la table MODELE (script MySQL fourni) a déjà été écrit et vous est également fourni.

Tous les 7 modèles de voitures

Id du modele	Libellé	Carburant
7	Ligier	electrique
5	Peugeot	diesel
6	Peugeot	gpl
2	Renault	essence
4	Renault	diesel
1	Volkswagen	essence
3	Volkswagen	diesel

Les NOUVELLES FONCTIONNALITES attendues sont les suivantes :

1) AFFICHAGE (en plus des MODELES) :

- Liste des VEHICULES
- Liste des PROPRIETAIRES

Ex :

Nombre de véhicules : 2

Immat	Date de circulation	Date de CarteGrise	Couleur	modele	Proprietaire
EF-2571-Z	2019-07-31	2019-07-31	claire	Volkswagen	Davolio
EG-0047-A	2019-09-01	2019-09-01	foncee	Volkswagen	Fuller

[Retour Menu](#)

2) AJOUT

- MODELE
- VEHICULE
- PROPRIETAIRE

EX :

Ajout d'un Modele

Caractéristiques

Id du Modele :

Libellé :

Carburant :

[Retour Menu](#)

Libellé :

127.0.0.1:8080

Le modele est enregistré

[Retour Menu](#)

Ajout d'un Proprietaire

Ajout de proprietaire

Nom : **Prenom :**

Adresse : **Ville :**

Code Postal :

[Retour Menu](#)

Adresse : **Ville :**

127.0.0.1:8888

Le propriétaire est enregistré.

[Retour Menu](#)

Ajout d'un vehicule

Proprietaire

Saisir un nom (ou une partie):

Voiture

Numéro d'immatriculation :

Couleur :

Date 1ere immatriculation (AAAA-MM-JJ) : **Date carte grise (AAAA-MM-JJ) :**

Saisir un nom (ou une partie):

Résultat :

Voiture

Numéro d'immatriculation :

Couleur :

Date 1ere immatriculation (AAAA-MM-JJ) : **Date carte grise (AAAA-MM-JJ) :**

Ajout d'un vehicule

Proprietaire

Saisir un nom (ou une partie):

Proprietaire

Saisir un nom (ou une partie):

Résultat :

Voiture

3) RECHERCHE

- MODELE

EX :

Choisir le modèle

Libellé (ou une partie):

[Retour Menu](#)

Choisir le modèle

Libellé (ou une partie):

Résultat :

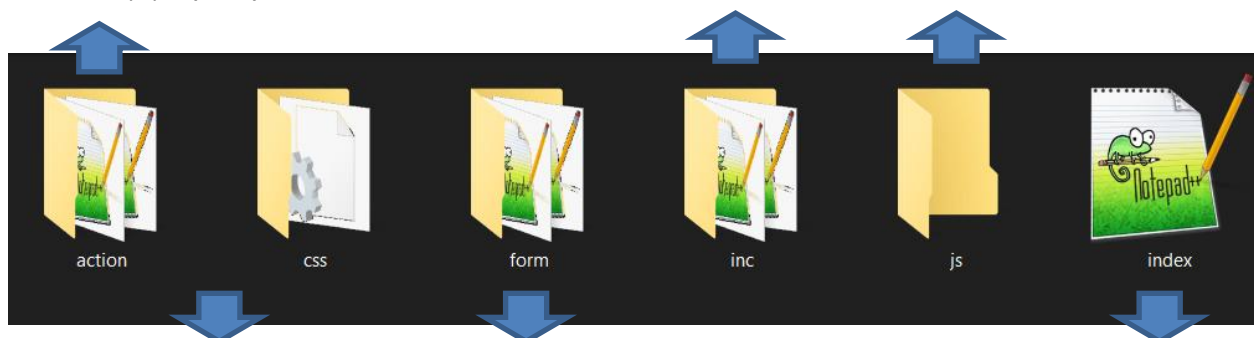
Architecture de l'application web

L'ensemble des ressources (scripts PHP, fichier(s) CSS, scripts JavaScript etc...) devront être organisés de la manière suivante au sein du serveur web :

Scripts PHP inclus par les formulaires.
Permettent d'effectuer des « actions ».
Cf. « Liste_modeles.php » (fourni)

Scripts PHP à inclure (EX : `include('inc/db.php')`
dans « index.php »). Fournis

Scripts JavaScript (si nécessaires)



Feuille(s) de style CSS
Fournie.

Scripts PHP dont le rôle est d'afficher un formulaire,
puis d'inclure :

- `db.php`
- `function.php`

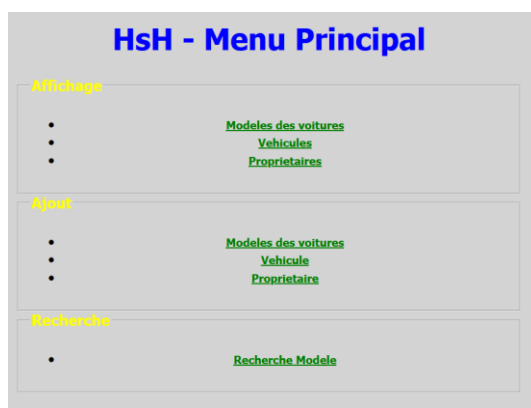
Et surtout :

- un script PHP effectuant des « actions »,
par exemple un accès à la BD. Scripts
placées dans le dossier « action ».

EX : « Formulaires_Liste_Modeles.php » (fourni)

```
<?php
include('../inc/db.php');
include('../inc/function.php');
echo headerForm();
include('../action/Liste_modeles.php');
echo footer();
?>
```

« index.php » désigne la page d'accueil du site. Ce script
(fourni) a pour rôle d'afficher le menu principal :



DEUXIEME PARTIE – Sécurisation de l'application Web

Depuis l'introduction des pages web « dynamiques » à travers des technologies telles PHP exploitant des bases de données, les risques sont réels de voir son site « abusé » et « détourné » de son utilisation initiale.

Les risques à prévenir dans une application web sont principalement les suivants :

L'abus de ressources

Cette attaque consiste à accaparer tout ou partie des ressources d'un site web pour en bloquer le fonctionnement. Cela conduit au « DENI DE SERVICE » : les ressources sont devenues tellement rares que le serveur ne peut plus assurer sa fonction habituelle.

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos>

La destruction de données

Il s'agit de S'ATTAQUER AUX DONNEES, en utilisant une faille de l'application web. Par exemple, à l'aide d'une injection SQL, il est possible d'effacer le contenu d'une table et de rendre l'ensemble du site web inutilisable (remplacer tous les mots de passe de la table des utilisateurs par le même mot, etc...).

<https://www.cnil.fr/fr/securite-encadrer-la-maintenance-et-la-destruction-des-donnees>

La publication de données confidentielles

Il s'agit d'un accès non autorisé à des données : par exemple, lire le profil d'un utilisateur, le dossier médical d'un patient ou encore le fichier fiscal d'une entreprise. La publication de données ne perturbe pas l'utilisation d'un site, et toute la difficulté de ce type de risque est de savoir IDENTIFIER LE VOL.

<https://www.cnil.fr/fr/violation-de-donnees-le-cepd-publie-des-lignes-directrices-partir-de-cas-pratiques>

Le détournement du site

Détourner un site revient à s'en servir dans un BUT DIFFERENT de son objet initial. Par exemple, des serveurs Web peuvent également se faire détourner. Dans ce cas, un simple site web peut se transformer en un site FTP pirate ou bien un « zombie » utilisé dans un déni de service distribué.

<https://www.techniques-ingénieur.fr/actualite/articles/comment-identifier-les-pirates-informatiques-qui-detournent-des-sites-web-71953/>

La défiguration du site

La défiguration de site web est l'altération par un pirate de l'apparence d'un site Internet. La défiguration est le signe visible qu'un site internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu.

- Durant l'attaque, le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité.
- Par ailleurs, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales...) : ce qui porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires...

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/defiguration-de-site-internet>

L'usurpation d'identité

L'usurpation d'identité consiste à utiliser, sans votre accord, des informations permettant de vous identifier. Il peut s'agir, par exemple, de vos nom et prénom, de votre adresse électronique, ou encore de photographies....

Ces informations peuvent ensuite être utilisées à votre insu, notamment pour souscrire sous votre identité un crédit, un abonnement, pour commettre des actes répréhensibles ou nuire à votre réputation.

<https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite>



La sécurité d'une application se pratique à tous les stades de sa vie : elle commence au moment de la conception, elle est constante durant le développement ; et enfin, elle se concrétise par la surveillance des opérations journalières lorsque l'application est mise en production.

Le concept d'injection

Est-ce que les données qui sont reçues doivent avoir un format particulier pour que le code soit autorisé à les manipuler ? Par exemple, les critères à appliquer à un nom : peut-on accepter un nom d'un seul caractère, ou de 100 caractères ou encore un nom avec des chiffres, des accolades, des guillemets doubles, des espaces ?

- Il est nécessaire de savoir en tout point de l'application si les données reçues et manipulées sont « saines » ou non. Il est important de savoir à tout moment si l'on est en train d'utiliser des valeurs brutes ou validées. La stratégie la plus courante est d'imposer un SYSTEME DE FILTRAGE.
- L'injection de code est l'un des types d'attaques les plus courants. Si les attaquants connaissent le langage de programmation, la base de données ou le système d'exploitation utilisé par une application Web, ils peuvent « injecter du code » via des champs de saisie de texte, par exemple pour forcer le serveur Web à faire ce qu'ils souhaitent.

Ces types d'attaques par injection sont possibles sur les applications qui manquent de VALIDATION DES DONNEES. Par exemple, si un champ de saisie de texte permet aux utilisateurs de saisir ce qu'ils veulent, alors l'application est potentiellement exploitable.

Pour éviter ces attaques, l'application doit FILTRER autant que possible les données saisies et envoyées au serveur afin d'être exploitées.

<https://www.pierre-giraud.com/php-mysql-apprendre-coder-cours/utilisation-filtre/>

<https://inforisque.fr/fiches-pratiques/securite-validation-PHP.php>

<http://www.oujood.com/php/filtre-de-php.php>

<https://geekflare.com/fr/web-application-injection-attacks/>

<https://openclassrooms.com/fr/courses/6179306-securisez-vos-applications-web-avec-lowasp/6520701-protégez-votre-code-contre-l-injection>

Votre Mission :

Vous êtes chargé de compléter le code de l'application web précédemment développée avec toute mesure de sécurité qui vous semblerait utile et nécessaire afin de se prémunir contre les principales failles de sécurité.

REMARQUE : l'attaque par « force brute » sera traitée dans une prochaine version de l'application.

Une fois ce travail effectué, vous devez rédiger une documentation qui présentera de manière synthétique pour chaque faille traitée :

- Une description de la faille (nom, description) ;
- Les mesures mises en œuvre (principe, extrait de code, page(s) web où ces mesures ont été appliquées).

TROISIEME PARTIE – LE REQUETEUR SQL

L'interface à développer est un « REQUETEUR » permettant de CONSTRUIRE des requêtes SQL en fonction des choix effectués par l'utilisateur. Une fois la requête construite, le résultat correspondant sera affiché dans une page web. La maquette et le principe de fonctionnement est le suivant :

Requêteur

Formulez votre requête :

Tables:

carteprise

condition ? :

☒ oui ☐ non

REMARQUE : la liste des tables disponibles doit être chargée automatiquement à partir de la BD (cf. bases et tables système MySQL). Une requête doit donc permettre d'interroger la base MySQL afin de récupérer la liste des tables créées, ce qui servira à charger la zone de liste déroulante.

Formulez votre requête :

Tables:

carteprise

carteprise
concessionnaires
modele
proprietaire
voiture

Pas de condition : liste de TOUS les propriétaires

Formulez votre requête :

Tables:

proprietaire

condition ? :

☒ oui ☐ non

Valider

Resultat de la requête

id_pers	nom	prenom	adresse	ville	codepostal
1	Davolio	Rose	5, rue de la Poste	VICHY	03200
2	Fuller	Andrew	Place de la Gare	VICHY	03200
3	Daverling	Janet	1, Boulevard d'Italie	VICHY	03200
4	Peacock	Margaret	23, Impasse des Fleurs	MOULINS	03000
5	Buchanan	Steven	15, Place de l'Hotel de Ville	MOULINS	03000
6	Bucyama	Michael	15, Rue des Pinsons	MOULINS	03000
7	King	Andrew	57, Boulevard de la Gare	MOULINS	03000
8	Callahan	Laura	23, Boulevard Central	MOUNTLUCON	03100
9	Bucsworth	Annette	7, rue de la Paix	MONTLUCON	03100

[Lancer une nouvelle requete](#)

Condition : liste de CERTAINS propriétaires

Formulez votre requête :

Tables:

proprietaire

condition ? :

☒ oui ☐ non

Choisir les critères :

Colonnes:

id pers

Opérateur de comparaison :

>

Valeur :

Valider

En cochant sur OUI, on affiche la zone de saisie de la condition.

Colonnes:

id pers

id_pers
nom
prenom
adresse
ville
codepostal

Liste des colonnes pour la table sélectionnée (le résultat doit être issu d'une interrogation de la base)

Choisir les critères :

Colonnes:

ville

Opérateur de comparaison :

=

Valeur :

VICHY

Valider

Resultat de la requête

id_pers	nom	prenom	adresse	ville	codepostal
1	Davolio	Rose	5, rue de la Poste	VICHY	03200
2	Fuller	Andrew	Place de la Gare	VICHY	03200
3	Daverling	Janet	1, Boulevard d'Italie	VICHY	03200

[Lancer une nouvelle requete](#)