L'éditeur logiciel ***Medinfo*** spécialisé dans les solutions dédiées au milieu médical propose des solutions logicielles en abonnement SAAS. Dans ce cadre, ils hébergent eux-mêmes les applications métiers auxquelles ont accès les clients grâce à des formules d'abonnements.

Un pack de solutions est vendu aux cabinets vétérinaires pour la gestion des clients, la gestion des interventions, la gestion des consultations, la prise de rendez-vous et les visites chez les clients/patients.

Ce pack est un ensemble de solutions logicielles interconnectées qui ont été développées et améliorées depuis leur conception initiale.

Dans cet ensemble de logiciels, l'application **VetoPlan** qui permet de gérer les rendez-vous dans un navigateur sur PC ou sur téléphone mobile n'a pas été mis à jour depuis de nombreuses années car la sécurisation d'autres applications était prioritaires.

Pour autant l'application VetoPlan fait l'objet de nombreux actes malveillants : Les données de la base sont souvent corrompues; certains vétérinaires accèdent à des rendez-vous qu'ils n'ont pas créé. Ils soupçonnent aussi que leur base client a pu être dérobée.

Actuellement une équipe complète est dédiée à la correction des valeurs directement dans la base de données pour pallier au plus vite aux actes malveillants mais le cœur du problème n'est pas réglé.

Suite à un incident où un hacker a réussi à modifier le mot de passe d'un utilisateur en lui envoyant un lien sur son mail professionnel, l'entreprise Medinfo a fait appel à une société experte en sécurité pour auditer l'application VetoPlan.

Cet audit de sécurité a mis en évidence des défauts de conception et d'implémentation.

Vous intégrez l'équipe qui a pour rôle de corriger les problèmes de sécurité dans l'application VetoPlan.

L'organisation ne souhaite pas changer d'architecture applicative pour le moment. De nouvelles technologies sont à l'étude mais ne seront utilisées que pour la prochaine version majeure.

Vous devez donc corriger les problèmes identifiés directement dans l'application existante même si les technologies employées ne sont plus d'actualité.

Le Product Owner a défini avec le client et la société d'audit les axes de sécurisation prioritaires à mettre en œuvre.

Le premier sprint concerne la correction d'une faille de sécurité présente dans plusieurs fonctionnalités de l'application et illustrée par le scénario de risque 6.

Script SQL de la base de données

```
-- phpMyAdmin SQL Dump
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";
-- Base de données :  `vetoplan`
– —---------------------------------------
-- Structure de la table `client`
– —---------------------------------------
CREATE TABLE `client` (
  `idC` int(11) NOT NULL,
  `nomC` varchar(255) DEFAULT NULL,
  `prenomC` varchar(255) DEFAULT NULL,
  `rueC` varchar(255) DEFAULT NULL,
  `cpC` char(5) DEFAULT NULL,
  `villeC` varchar(255) DEFAULT NULL,
  `notes` text,
  `idU` int(11) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
– —---------------------------------------
-- Contenu de la table `client`
– —---------------------------------------
INSERT INTO `client` (`idC`, `nomC`, `prenomC`, `rueC`, `cpC`, `villeC`, `notes`, `idU`) VALUES
(1, 'Yann', 'Barrot', 'Le chambon', '24390', 'Tourtoirac', NULL, 1),
(2, 'Harispe', 'Michel', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, 2),
(3, 'Garay', 'Nicolas', '123 allee des Genêts', '40440', 'Ondres', NULL, 3),
(4, 'Fontaine', 'Christophe', '24 rue du chemin de fer', '94110', 'Arcueil', NULL, 4),
(5, 'Da Ros', 'Joel', 'chemin forestier', '94400', 'Alfortville', NULL, 4);
– —---------------------------------------
-- Structure de la table `rdv`
– —---------------------------------------
CREATE TABLE `rdv` (
  `idR` int(11) NOT NULL,
  `idU` int(11) DEFAULT NULL,
  `idC` int(11) DEFAULT NULL,
  `dateR` datetime DEFAULT NULL,
  `rueR` varchar(255) DEFAULT NULL,
  `cpR` char(5) DEFAULT NULL,
  `villeR` varchar(255) DEFAULT NULL,
  `animalR` text,
  `notes` text
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

```
– —----------------------------------------
-- Contenu de la table `rdv`
– —----------------------------------------
INSERT INTO `rdv` (`idR`, `idU`, `idC`, `dateR`, `rueR`, `cpR`, `villeR`, `animalR`, `notes`) VALUES
(1, 1, 1, '2023-03-11 14:20:00', '20 chemin de la mothe', '24390', 'Hautefort', NULL, NULL),
(2, 1, 1, '2023-01-15 14:00:00', '20 chemin de la mothe', '24390', 'Hautefort', NULL, NULL),
(3, 2, 2, '2023-02-20 10:45:00', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, NULL),
(4, 2, 2, '2023-02-07 11:30:00', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, NULL),
(5, 2, 2, '2023-01-10 15:00:00', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, NULL),
(6, 2, 2, '2023-01-01 16:30:00', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, NULL),
(7, 2, 2, '2023-01-01 16:30:00', 'Gaineko Etxea', '64220', 'Saint Jean Pied de port', NULL, NULL),
(8, 3, 3, '2023-01-01 16:30:00', '123 allee des Genêts', '40440', 'Ondres', NULL, NULL),
(9, 3, 3, '2023-02-23 16:30:00', '123 allee des Genêts', '40440', 'Ondres', NULL, NULL),
(10, 4, 4, '2023-01-09 16:30:00', '24 rue du chemin de fer', '94110', 'Arcueil', 'Chien', 'Opération oreille droite'),
(11, 4, 4, '2023-02-15 16:30:00', '24 rue du chemin de fer', '94110', 'Arcueil', 'Chien', 'Visite de contrôle de l\'opération sur l\'oreille droite : RAS'),
(12, 4, 4, '2023-03-30 16:30:00', '24 rue du chemin de fer', '94110', 'Arcueil', 'Chien', 'Suite opération oreille droite, retrait des points de suture.'),
(13, 4, 4, '2023-06-29 17:00:00', '24 rue du chemin de fer', '94110', 'Arcueil', 'Chien', 'vaccination CHLRP, vérifier la cicatrisation post-op');
– —----------------------------------------
-- Structure de la table `utilisateur`
– —----------------------------------------
CREATE TABLE `utilisateur` (
  `idU` int(11) NOT NULL,
  `mailU` varchar(150) NOT NULL,
  `mdpU` varchar(50) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
– —----------------------------------------
-- Contenu de la table `utilisateur`
– —----------------------------------------
INSERT INTO `utilisateur` (`idU`, `mailU`, `mdpU`) VALUES
(1, 'alex.garat@vetoplan.fr', 'seSzpoUAQgII.'),
(2, 'jj.soueix@vetoplan.fr', 'seSzpoUAQgII.'),
(3, 'lionel.romain@vetoplan.fr', 'seSzpoUAQgII.'),
(4, 'amal.hecker@vetoplan.fr', 'seSzpoUAQgII.');

ALTER TABLE `client`  ADD PRIMARY KEY (`idC`),   ADD KEY `idU` (`idU`);
ALTER TABLE `rdv`  ADD PRIMARY KEY (`idR`),  ADD KEY `idU` (`idU`), ADD KEY `idC` (`idC`);
ALTER TABLE `utilisateur` ADD PRIMARY KEY (`idU`), ADD UNIQUE KEY `mailU` (`mailU`);
ALTER TABLE `client`  MODIFY `idC` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=5;
ALTER TABLE `rdv`  MODIFY `idR` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=14;
ALTER TABLE `utilisateur`   MODIFY `idU` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=5;
ALTER TABLE `client`  ADD CONSTRAINT `client_ibfk_1` FOREIGN KEY (`idU`) REFERENCES `utilisateur` (`idU`);
ALTER TABLE `rdv` ADD CONSTRAINT `rdv_ibfk_1` FOREIGN KEY (`idU`) REFERENCES `utilisateur` (`idU`), ADD CONSTRAINT `rdv_ibfk_2` FOREIGN KEY (`idC`) REFERENCES `client` (`idC`);
```

ANNEXES

Annexe 1 : Besoins de sécurité pour les user stories de l'application VetoPlan

	Intitulé de la user story	Disponibilité	Intégrité	Confidentialité	Preuve
1	En tant que vétérinaire je peux consulter mes rendez-vous	**	**	**	-
2	En tant que vétérinaire je peux consulter les informations détaillées d'un de mes rendez-vous.	*	**	**	-
3	En tant que vétérinaire je peux rédiger une annotation et changer le type d'animal examiné d'un de mes rendez-vous.	*	**	*	*
4	En tant que vétérinaire je peux créer un nouveau rendez-vous.	*	**	*	-
5	En tant que vétérinaire je peux changer mon mot de passe.	*	**	**	*

- : pas de besoin * : besoin important **: besoin très important

Annexe 2 : Extrait du rapport d'audit de l'analyse des risques et menaces de l'environnement

Acteurs à l'origine de la malveillance

Acteurs malveillants	Modes opératoires	Probabilité
Attaquant externe (hacker)	L'attaquant externe modifie des données dans la base	**
	L'attaquant externe ajoute des données corrompues dans la base	**
	L'attaquant externe surcharge le système	***
Vétérinaire	L'utilisateur consulte des données qu'il ne détient pas	**
	L'utilisateur modifie des données qu'il ne détient pas	*
	L'acheteur surcharge le système	*
Utilisateur non connecté	L'utilisateur consulte des données qu'il ne détient pas	*
	L'utilisateur modifie des données qu'il ne détient pas	*
	Le visiteur surcharge le système	*

* : faible probabilité ** : forte *** : très forte probabilité

Impacts des évènements redoutés

Numéro de l'événement	Évènement	Impact pour l'entreprise Gravité	
1	Le système ne répond pas	Perte de clients	*
2	Un utilisateur non connecté parvient à consulter un rendez-vous	Problème de confiance	*
3	Un utilisateur non connecté parvient à modifier l'animal et les notes d'un rendez-vous	Perte de clients Problème de confiance	**
4	Un vétérinaire parvient à consulter un rendez-vous ne lui appartenant pas		
5	Un vétérinaire parvient à modifier l'animal et les notes d'un rendez-vous ne lui appartenant pas	Perte de clients Problème de confiance	**
6	Un attaquant externe parvient à faire créer un faux rendez-vous à un vétérinaire	Perte de clients Problème de confiance Désorganisation des rendez-vous	**
7	Un attaquant externe parvient à faire en sorte qu'un vétérinaire modifie son mot de passe sans qu'il ne le sache	Perte de clients Application inaccessible Problème de confiance	**
8	Un attaquant externe parvient à consulter un rendez-vous	Problème de confiance	*
9	Un attaquant externe parvient à faire modifier l'animal et les notes d'un rendez-vous par un vétérinaire		
10	Un attaquant externe parvient à modifier l'animal et les notes d'un rendez-vous	Perte de clients Problème de confiance	**

* : modéré ** : très élevé

Scénarios de risques et mesures à prévoir

Numéro de l'événement	Scénario de risque	Mesure à prévoir
4	En tant que vétérinaire malveillant, je souhaite pouvoir récupérer les informations des clients d'autres vétérinaires.	
5		
6	En tant qu'attaquant externe, je souhaite faire créer un faux rendez-vous par un vétérinaire.	6.1 Implémenter un système de protection contre les failles CSRF

Remarques :

Les numéros d'événements des tableaux "***Impacts des évènements redoutés***" et "***Scénarios de risques et mesures à prévoir***" sont liés.