République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique.

Option : Génie Logiciel (G.L)

Thème

Elaboration d'un système de double authentification sur Raspberry.

Réalisé par :

- **ABI AYAD Chakib.**

Présenté le 10 octobre 2019 devant le jury composé de MM :

- *Mohammed TADLAOUI* *(Président)*
- *Asma AMRAOUI* *(Examinatrice)*
- *Yassamine SELADJI* *(Encadrante)*
- *Karim BOUABDALLAH* *(Co-Encadrant)*

Année universitaire : 2018-2019

Dédicaces

Je dédie ce travail spécialement au Dr. Mokhtar TERKI HASSAINE, un homme bon qui n'a jamais cessé de m'encourager et de me pousser vers le haut, paix à son âme…

A ma famille, à mes amis, et à toute personne ayant contribué de près ou de loin à la réussite de ce projet.

Remerciements

Je tiens à exprimer toute ma reconnaissance à Madame Y. SELADJI et Monsieur K. BOUABDALLAH, qui n'ont cessé de m'encourager durant ce travail. Ils m'ont orienté, conseillé et corrigé avec compétence et efficacité. Qu'ils en soient vivement remerciés.

Je remercie vivement Monsieur M. TADLAOUI, de m'avoir fait l'honneur de présider mon jury.

J'adresse tous mes remerciements à Madame A. AMRAOUI, de l'honneur qu'elle m'a fait en acceptant d'être examinatrice de ce projet.

Monsieur K. MEDJAHDI, qui m'a été d'une grande assistance, il a su me guider dans la bonne direction, et m'a aussi donné de précieux conseils tout au long de mon cursus et de ce mémoire. Pour tout cela, je le remercie.

Je tiens aussi à exprimer toute ma gratitude à tous les enseignants du tronc commun, spécialement à Mme Tebbal, Mr Labbas, Mme Hassaine et aussi Mr Benmammar durant mon master. Ils m'ont appris ce que rigueur et précision voulaient dire.

Je voudrais aussi remercier mes parents qui m'ont initié à la réflexion logique depuis ma plus tendre enfance. Qu'ils soient remerciés pour leur disponibilité permanente et pour les nombreux encouragements qu'ils m'ont prodigués. Enfin je remercie chaque personne qui de près ou de loin, m'a fourni une aide informatique ou autre.

Table des matières

Table des figures

Introduction générale

L'utilisation de plus en plus croissante d'Internet a sans doute augmenté l'usage de services basés sur ce dernier, du e-commerce, de moyens de communications moins drastiques, ainsi que du partage d'informations en général. Cette augmentation fragilise les systèmes de cyber sécurité qui se font de plus en plus vieux et obsolètes face aux nouvelles et diverses méthodes et technologies utilisés par les pirates informatiques, et face à ces cas de figures, on a besoin de nos jours, de moyens de communications plus sûrs, car l'intégrité, la confidentialité et les la disponibilité des systèmes sont d'une importance capitale. Ces questions sont traitées quotidiennement à travers le monde entier.

L'authentification des utilisateurs et la manière dont elle est effectuée est l'un des principaux domaines d'amélioration de la sécurité informatique ces dernières années. Bien que plusieurs entreprises et compagnies utilisent toujours l'authentification via un ID statique et un simple mot de passe, cette méthode se fait de plus en plus vieillissante et une méthode d'authentification plus optimale est nécessaire. L'une des solutions à ce problème est l'authentification à double facteur, fondamentale à la sécurité de tout système informatisé. Ce mémoire explore la technique de la double authentification ainsi que sa mise en œuvre.

La méthode d'authentification à deux facteurs se caractérise de deux phases. Lors de la première phase, l'authentificateur reçoit une demande générée par l'application, d'authentifier un utilisateur spécifié. Lorsque la demande est reçue, l'application délivre un code à usage unique à l'utilisateur. Au cours de la deuxième phase, l'utilisateur ayant obtenu le code, il doit l'envoyer par SMS au numéro communiqué par l'application, le système procède ensuite à la vérification de la parité du code généré avec le code reçu par l'utilisateur, pour ainsi valider l'inscription de ce dernier. Tout ceci dans un délai de temps fixé au préalable.

Chapitre 1 : Introduction et problématique

1.1 Introduction

La technologie appelée « Mot de passe à usage unique » permet de s'authentifier comme le dit son nom, avec un mot de passe à usage unique (aussi appelé mot de passe dynamique), cette méthode reste théoriquement le meilleur système de mot de passe de nos jours.

L'idée est d'ajouter un facteur incertain à l'authentification, les utilisateurs devront donc donner différents messages pour l'authentification à chaque fois. En utilisant cette méthode, les applications elles-mêmes peuvent obtenir une garantie de sécurité plus élevé que celles qui utilisent une authentification à mot de passe statique. Les méthodes d'implémentations du mot de passe à usage unique incluent le facteur de synchronisation entre l'utilisateur et l'application, qui est d'une importance capitale. Quelles que soient les méthodes utilisées pour mettre au point les propriétés dynamiques du mot de passe à chaque authentification, le but est de s'assurer que ce dernier est bien aléatoire.

Utiliser des mots de passes statiques pour l'authentification, comme communément fait, a quelques inconvénients : ils peuvent être devinés, oubliés, volés ou bien écris quelque part, perdus, ou bien délibérément communiqués à d'autres personnes, ce qui constitue bien sûr un risque alarmant pour notre sécurité. Un meilleur moyen et nettement plus sécurisé de s'authentifier, est appelé « authentification à deux facteurs », « double authentification » ou bien « authentification forte », basé sur les mots de passes à usage unique, au lieu de s'authentifier avec un simple mot de passe. L'authentification forte utilisant deux facteurs d'identification requiert souvent un périphérique supplémentaire, ce qui peut être vu comme un inconvénient à l'utilisateur et couteux pour les entreprises et les compagnies ayant ce système. Pour éviter l'usage de périphérique ou matériel supplémentaire, le téléphone est utilisé pour envoyer le mot de passe à usage unique.

Le projet décrit comment effectivement comment mettre en place l'authentification forte utilisant un téléphone portable sans avoir à dépenser pour un matériel supplémentaire pour effectuer cette dernière.

1.2 Contexte

Par définition, l'authentification signifie utiliser un ou plusieurs mécanismes pour prouver que la personne est ce qu'elle prétend être. Une fois que l'identité de l'homme ou de la machine est validée, l'accès peut être accordé. Il existe trois facteurs universellement reconnus pour l'authentification existant aujourd'hui : ce que vous savez (par exemple, les mots de passe, les NIP), ce que vous avez (par exemple, les cartes à puce ou les jetons) et ce que vous êtes (par exemple, les empreintes digitales, la reconnaissance faciale, la biométrie, etc.). -Les authentifications à deux facteurs sont un mécanisme qui met en œuvre deux des facteurs mentionnés ci-dessus et est donc considéré comme plus fort et plus sûr que le système d'authentification d'un facteur implanté traditionnellement ». L'un des exemples d'authentification à deux facteurs comprend le retrait de l'argent d'un guichet automatique. Quand quelqu'un veut retirer de l'argent du guichet automatique, d'abord, il doit entrer sa carte ATM, c'est-à-dire ce que vous avez et, à nouveau, il doit entrer le numéro de broche, c'est-à-dire ce que vous savez pour accéder à son compte.

1.3 Motivation

Il y a quelques années de cela, des clients de l'une des plus grandes banques ont été victime de l'attaque « Man In The Middle », un vol d'identité qui a beaucoup diminué le niveau de confiance entre la banque et ses clients, la réputation du système de la banque en ligne, ainsi que de la banque elle-même. Comme son nom l'indique, les pirates se sont mis au milieu entre les clients et la banque, et ont écouté toutes les communications entre eux, dans le but de voler leurs informations personnelles et leurs comptes. Ils ont ensuite envoyé des e-mails qui semblaient légitimes aux clients leur demandant de vérifier leurs comptes via un faux site mis en place par les pirates, ceux qui leur a permis de prendre les mots de passes des comptes des clients affiliés à cette banque. Après ça, les clients ne se sentent plus en sécurité, et le nombre d'arnaques pour voler les mots de passes ne cessent d'augmenter année après année, ce qui motive toute la communauté professionnelle à se perfectionner pour éviter ces cybers attaques sophistiquées.

Dans certains cas, le pirate met en place un piège et attend la victime. La victime non prévenue croit qu'elle fait son travail tout à fait normalement sans savoir que ses

données sont en train d'être piratées. Le pirate est capable ensuite d'intercepter le nom d'utilisateur et le mot de passe qu'il peut ainsi utiliser à des fins criminelles et non légales.

Ces attaques ont rapidement encouragé l'arrivé de la double authentification, une mesure de sécurité que plusieurs institutions financières ont adoptée. De nos jours, il y a un besoin urgent d'être sûr que seulement les personnes autorisées peuvent accéder aux données sensibles et sécurisées. Avec tous les outils présents sur Internet, il y a une forte possibilité de pirater un système entier ou bien de voler des identifiants pour accéder aux données diverses. On conclut donc que l'authentification à un seul facteur seulement n'est pas adéquate en termes de sécurité avec les risques élevés que courent les sociétés.

Pour palier toutes ses attaques on a besoin d'un système qui résout tous les problèmes mentionnés. La solution pour cela est « L'authentification à deux facteurs ».

L'authentification forte prévient les entreprises et leurs clients de différentes attaques liées à l'accès illicite et au vol de données. Ce modèle utilise une authentification avec un nom d'utilisateur et un mot de passe (qui peut être statique ou bien dynamique), cette approche authentifie les utilisateurs mais ne donne pas la certitude sur son identité, il faut donc ajouter un système qui génère un mot de passe à usage unique que les utilisateurs utiliseront tel un deuxième facteur d'authentification, le client sera donc fortement identifié et il sera aussi libéré de toutes les attaques citées précédemment.

1.4 Objectif

Un des déficits principaux des systèmes d'authentification via un seul facteur est la facilité avec laquelle ils peuvent être piratés. Cette menace a augmenté au fil du temps pendant que de nouvelles méthodes bien plus modernes peuvent être employées pour deviner et cracker des systèmes d'authentification. Le besoin de meilleurs et plus sûrs systèmes a fait place du concept du système d'authentification à deux facteurs. Dans ce nouveau système, le premier facteur est juste le mot de

passe habituel que chacun crée tout en enregistrant ou créant un compte. Le deuxième facteur est le mot de passe à usage unique, ce dernier qu'on génère au niveau de l'application pour l'afficher à l'utilisateur pour qu'il puisse l'envoyer par SMS au numéro également affiché sur la plateforme.

La mise en place et l'utilisation d'un système d'authentification à deux facteurs est plus complexe et difficile à casser par un pirate. Dans le cadre de mémoire, on va concevoir une simple application qui aura pour but de présenter une plateforme d'inscription pour un utilisateur. L'authentification d'un utilisateur se passe en deux étapes, lors de la première l'utilisateur doit remplir un formulaire contenant toutes les informations nécessaires pour s'inscrire accompagnées d'un mot de passe simple.

Une fois la première étape finie, l'utilisateur se voit affiché un numéro de téléphone et un code généré par l'application, qu'il devra envoyer au numéro, le code s'expirera après un délai imparti, pour générer ce code, on a mis un place une fonction PHP qui permet de générer un code aléatoire à chaque utilisation.

La phase de l'implémentation du mémoire inclut la mise en place d'un site web en utilisant HTML, PHP, CSS et JavaScript.

Enfin, on va concevoir une application simulant une inscription en ligne, qui va authentifier un utilisateur avec deux différents mots de passes, le premier est choisi par l'utilisateur lui-même, le second par contre, est généré grâce à l'application, ce système à double authentification avec un mot de passe à usage unique surtout tente de réduire le problème des mots de passes sniffés, car après une seule utilisation du mot de passe à usage unique, ce dernier se périme comme son nom l'indique.

1.5 Portée du mémoire

Le système d'authentification à deux facteurs est une technologie innovante utilisée pour résoudre les problèmes existants de l'authentification d'un seul et unique facteur avec un simple nom d'utilisateur et un mot de passe. La double authentification résout

ce problème en utilisant la combinaison de "quelque chose que vous connaissez", quelque chose que vous avez » et quelque chose que vous êtes ». Comparé les trois méthodes individuellement, toutes les méthodes présentent des vulnérabilités. Quelque chose que vous connaissez peut-être partagée, quelque chose que vous avez peut-être volée et quelque chose que vous êtes est plus fort mais il est coûteux à utiliser dans tous les cas. Donc, la combinaison fournit une authentification plus forte.

Le projet vise à la réalisation d'une authentification forte à l'aide de deux facteurs qui est très facile à déployer en utilisant un téléphone mobile pour :

1. Fournir une authentification facile d'utilisation et rentable.
2. Éviter l'utilisation d'un nom d'utilisateur et d'un système de mot de passe simples qui ne sont plus assez sûrs.
3. L'utilisation du mobile comme votre moyen d'authentification.
4. Ne pas utiliser de matériel physique additionnel.

1.6 Pourquoi utiliser un téléphone mobile ?

Dans le quotidien, les téléphones mobiles sont devenus les moyens de communications les moins chers et les plus importants. Il existe de nombreuses applications utilisant cette technologie pour simplifier la vie humaine en termes de coût et de temps. La croissance des téléphones mobiles dans la génération actuelle est étonnante.

Le système qu'on a conçu génère un mot de passe à usage unique qui est utilisé pour l'authentification de l'utilisateur. Le mot de passe à usage unique généré peut être affiché à l'utilisateur sur la plateforme web, mais l'envoi du mot de passe à usage unique par l'utilisateur au serveur via SMS est le moyen le plus simple.

Donc le système d'authentification à double facteurs utilise les téléphones portables comme un périphérique d'authentification qui permet aux personnes d'éviter de porter un appareil mobile externe, cela donne aussi l'assurance que seulement le propriétaire du téléphone portable a été autorisé à accéder à son compte.

1.7 Avantages d’utilisation du système

Avec la double authentification, on peut identifier de manière positive les utilisateurs et leur fournir des services facilement et de manière sécurisée, sans avoir besoin d'un système sécurité supplémentaire.

Les utilisateurs peuvent avoir les avantages d'un processus très simple qui omet la nécessité de se souvenir de plusieurs mots de passe.

Un autre avantage à souligner, quand un pirate réussi à pirater d’une manière quelconque le mot de passe statique, grâce à l’authentification à deux facteurs, le pirate doit aussi craquer le mot de passe dynamique (à usage unique) pour pouvoir pénétrer le système, ce qui est assez difficile.

1.8 Limites de sécurité du système

L'authentification mobile à double facteurs ne peut pas résoudre le problème du phishing (le phishing est défini comme un processus de collecte de données personnelles, telles que les informations d'identification, les informations sur les cartes de crédit et d'autres données sensibles en se faisant passer comme une personne de confiance par une communication électronique).

Un utilisateur ne peut pas se connecter au système si les serveurs du fournisseur de services de passerelle GSM sont en panne où il ne peut pas recevoir le mot de passe à usage unique même s'il est un utilisateur authentique.

Ce système ne peut pas être utilisé lorsque le fournisseur de services de réseau mobile d'un utilisateur met fin à la connexion en raison du retard dans les paiements de facture et aussi du signal médiocre du réseau.

1.9 Systèmes existants

1.9.1 Types de systèmes existants

Il existe plusieurs systèmes pour traiter l'authentification mobile à deux facteurs. Ils peuvent différer dans la livraison du mot de passe à l'utilisateur autorisé ou à une entité différente en fonction des contraintes de sécurité. Certains d'entre eux sont les suivants :

Tokens(jetons)

Un jeton est un dispositif utilisé pour autoriser l'utilisateur à accéder aux différents services. Un jeton peut être un logiciel ou un matériel. Les jetons logiciels sont utilisés pour identifier la personne par voie électronique, c'est-à-dire qu'elle peut être utilisée comme mot de passe pour accéder à quelque chose. Les tokens de type matériel sont généralement de petits appareils portatifs qui contiennent des informations qui stockent des clés cryptographiques, des signatures numériques ou même des données biométriques par lesquelles on peut envoyer le numéro de clé généré à un système client. La plupart du temps, tous les tokens matériels ont une capacité d'affichage. Les jetons matériels comprennent un USB, un pass numérique, etc.

Désavantages :

1. Un jeton doit être transporté tout le temps.
2. Un logiciel spécial est nécessaire pour lire le jeton.
3. Toute personne qui a le jeton peut accéder aux informations, c'est-à-dire en cas de vol.

Authentification biométrique

Une authentification biométrique est la forme la plus avancée de l'authentification. Une authentification biométrique n'est rien d'autre que l'analyse des caractéristiques de l'utilisateur telles que l'empreinte digitale et la rétine des yeux qui sont stockées sous la forme d'une chaîne de caractères. Lorsque l'utilisateur essaie d'authentifier ses correspondances avec les données stockées, s'il y en a une, le système autorise l'utilisateur à entrer son mot de passe pour consulter les données demandées.

Désavantages :

1. L'authentification biométrique est pratique uniquement pour des applications limitées, car le système devient très lent pour un grand nombre d'utilisateurs.
2. Les empreintes digitales peuvent être prises sur une petite bande et peuvent être fournies pour le matériel.
3. Un matériel supplémentaire est nécessaire pour détecter les empreintes digitales et les rétines des yeux.

1.9.2 Comparaison entre l'utilisation d'un simple mot de passe et une authentification forte.

Méthode	Simple mot de passe	Authentification forte
Avantages	Largement utilisé et pris en charge par le plus grand nombre d'applications. Technologie facilement comprise par les utilisateurs	Authentification à deux facteurs compatibles avec l'infrastructure basée sur le mot de passe. Plus difficile à pirater.
Désavantages	S'appuie sur la protection de la personne et la gestion du secret.	Nécessite la possession de logiciels / matériel de production du mot de passe à usage unique ou l'accès à un canal secondaire pour sa transmission.
Vulnérabilités	Brute force. L'attaque « Man in the middle ». Phishing. Keystroke loggers(enregistreur de frappes au clavier).	L'attaque « Man in the middle ». Phishing (réduit par apport au simple mot de passe).
Domaine d'application	Environnements à risque inférieur. Aucune utilisation du réseau ou utilisation protégée du réseau.	Commerce en ligne. Sécurité des entreprises et des sociétés.

Figure 1 : Tableau d'étude comparative

1.10 Analyse

Le système d'authentification mobile à double facteurs est un système d'authentification innovant qui permet d'accéder aux ressources Web en utilisant une authentification forte via les téléphones portables personnels existants. Il est utilisé pour résoudre les défauts de sécurité de l'Internet et de l'Intranet sur le Web en demandant aux utilisateurs de s'authentifier en utilisant leurs téléphones portables personnels. L'enregistrement des utilisateurs doit se faire de manière sécurisée avant de pouvoir utiliser le système.

Il est conçu pour assurer la sécurité des applications Internet et Intranet basées sur le Web et nécessite que les utilisateurs s'authentifient avec deux critères uniques - un nom d'utilisateur et un mot de passe et un code qu'ils reçoivent uniquement pendant l'authentification (un mot de passe unique affiché au niveau de l'application) avant qu'ils ne soient autorisés à accéder à une ressource Web sécurisée. Avec la double authentification, on peut identifier les utilisateurs de manière positive et fournir des services facilement et de manière sécurisée à ces derniers, sans avoir besoin d'un système de sécurité supplémentaire. Les utilisateurs finaux peuvent profiter des avantages d'un processus très simple qui omet la nécessité de se souvenir de plusieurs mots de passe.

Chapitre 2 : Technologies, matériels utilisés et conception

2.1 Raspberry Pi

Figure 2 : Raspberry Pi 3 B

Le « Raspberry Pi » est un nano ordinateur de la taille d'une carte de crédit, avec un prix intéressant et une petite taille, le Raspberry est le produit idéal pour tester différentes choses.

Evidemment avec une petite taille, il ne faut pas s'attendre à de grandes performances, mais pour mettre en ligne des projets à montrer aux clients ou expérimenter une ou plusieurs variantes de systèmes d'exploitation c'est largement suffisant.

Cet ordinateur, vise à inciter l'apprentissage de la programmation informatique, il est aussi fourni nu dans le but de permettre l'utilisation de matériel de récupération et ainsi diminuer les coûts.

Le Raspberry peut être utilisé sans un écran, un clavier ou bien une souris, car sur certains systèmes d'exploitation le protocole SSH est présent et activé, ce qui permet de le contrôler à distance dès qu'il démarre. [1]

2.1.1 Configuration

- Carte mère Raspberry Pi 3 Type B
- Processeur intégré Quad-core ARM Cortex-A53 1.2 GHz (Broadcom BCM2837)
- RAM : 1024 Mo
- GPU Dual Core VideoCore IV Multimedia Co-Processor
- Lecteur de cartes Micro SD
- Ports : HDMI, 4x USB, RJ45, jack 3.5 mm, connecteurs pour APN et écran tactile
- Wi-Fi b/g/n et Bluetooth 4.1
- Support des distributions dédiées basées sur Linux et Windows 10

2.2 Ubuntu

Figure 3 : Logo Ubuntu

Vu sa côte de popularité, on ne le présente plus, on sait néanmoins que c'est un système d'exploitation open source développé par la société Canonical sur la base de la distribution Linux Debian. Son nom provient d'un ancien mot bantou qui signifie « je suis ce que je suis grâce à ce que nous sommes tous ».

Durant ce projet, on a utilisé Ubuntu pour sa fiabilité, sa richesse dans les bibliothèques et la disponibilité des packages correspondant à la configuration du modèle Raspberry utilisé (architecture ARM), il est aussi hautement personnalisable car tout est paramétrable avec plus ou moins d'efforts, une importante documentation est disponible (de source officielle ou venant de la communauté des utilisateurs), c'est

aussi un système très sécurisé où les droits des fichiers et applications sont mieux gérés.

Ubuntu offre beaucoup plus de stabilité dans les opérations aux utilisateurs que les autres systèmes Linux distribués librement, et cela en partie grâce à des similitudes de conception avec le système sorti dans le commerce.

Comparé à d'autres systèmes d'exploitation basés sur Linux, il contient les versions les plus stables de logiciels, ce qui réduit le risque de défaillance ou de plantage du système. [2]

2.3 Protocol SSH

Figure 4 : Schéma Protocol SSH.

Afin de pouvoir communiquer et travailler sur le Raspberry, on a privilégié l'usage du SSH.

Le protocole SSH (Secure Shell) a été mis au point en 1995 par le Finlandais Tatu Ylönen.

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

1. Les données circulantes entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut

lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

2. Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

L'établissement d'une connexion SSH se fait en plusieurs étapes :

1. Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
2. Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès. Il existe plusieurs méthodes :

1. La méthode la plus connue est le traditionnel mot de passe. Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisé et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide.
2. Une méthode moins connue mais plus souple est l'utilisation de clés publiques. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée. [3]

2.4 SMS Gateway

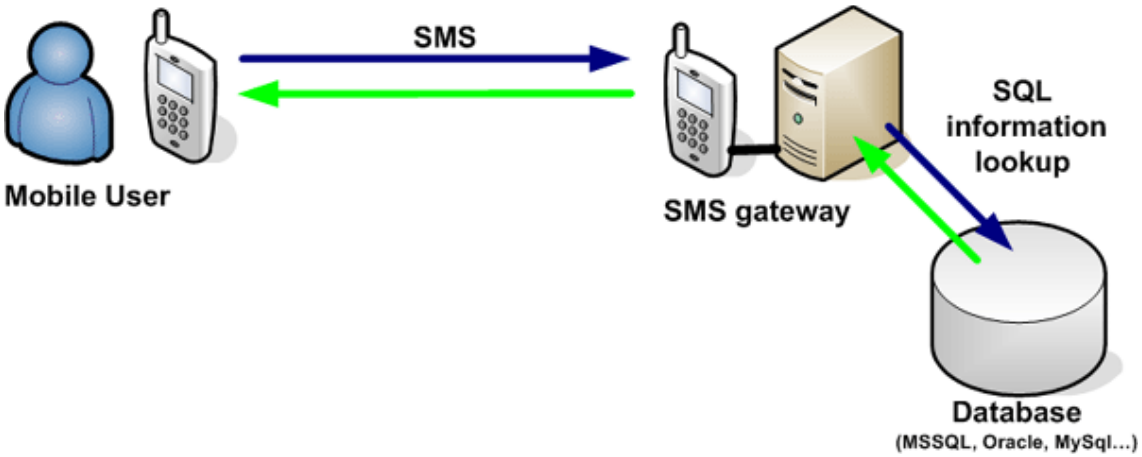


Figure 5 : Schéma Gateway SMS

La passerelle SMS est un périphérique ou un service offrant un transit SMS ; Transmettre des messages au trafic de réseau mobile à partir d'autres supports, ou vice versa, permettant la transmission ou la réception de messages SMS avec ou sans l'utilisation d'un téléphone mobile.

L'utilisation typique d'une passerelle serait de transmettre un courrier électronique simple à un destinataire de téléphone mobile. La passerelle SMS est le moyen le plus rapide et le plus fiable pour l'envoi de messagerie en masse / en vrac. Il traite avec le fournisseur de services mobiles et envoie des SMS avec l'identité de l'expéditeur en tant qu'identifiant et authentification textuelle. Ce système est développé pour améliorer la sécurité des utilisateurs de la passerelle.

La passerelle (gateway en anglais) reçoit les messages SMS dans un certain format et, basé sur le contenu des messages, les transfère à une application spécifique. En utilisant ce framework, des fonctionnalités additionnelles peuvent être ajoutées sans changer le code source de la passerelle, en fournissant une solution simple et évolutive pour l'ajout de service à un système déjà existant. Tout ce que doit faire l'administrateur système, c'est de fournir les informations nécessaires pour que le gateway sache où il doit faire suivre l'SMS.

Le système proposé récupère des informations à partir d'une base de données spécifique en fonction des informations fournies dans le SMS. De la même manière, une passerelle SMS peut être utilisée pour acheminer l'information vers différentes applications. Si le système sous-jacent est conçu correctement, une passerelle SMS

peut fournir une plate-forme omniprésente et facilement extensible pour fournir des services distants. [4]

2.5 Modem GSM

Figure 6 : Illustration modem GSM

Un modem GSM est un modem spécialisé qui accepte une carte SIM et opère sur un abonnement à un opérateur mobile, tout comme un téléphone portable. Du point de vue de l'opérateur mobile, un modem GSM ressemble à un téléphone mobile.

Lorsqu'un modem GSM est connecté à un ordinateur ou à un Raspberry, cela permet à ces derniers d'utiliser le modem GSM pour communiquer sur le réseau mobile. Alors que ces modems GSM sont les plus fréquemment utilisés pour fournir une connectivité Internet mobile, plusieurs d'entre eux peuvent également être utilisés pour envoyer et recevoir des messages SMS et MMS.

Un modem GSM peut être un modem dédié avec une connexion série, USB ou Bluetooth, ou il peut s'agir d'un téléphone mobile qui offre des capacités de modem GSM.

Les modems GSM peuvent être un moyen rapide et efficace de démarrer avec les SMS, car un abonnement spécial à un fournisseur de services SMS n'est pas nécessaire. Dans la plupart des régions du monde, les modems GSM sont une solution rentable pour recevoir des messages SMS, car l'expéditeur paie pour l’envoi des messages. [5]

2.6 Gammu

Figure 7 : Logo Gammu

Gammu est un utilitaire spécialisé dans l'envoi et la réception des SMS, il est compatible avec de nombreuses distributions du système UNIX ainsi que sur Windows, il offre de nombreux avantages, entre autres la possibilité d'y introduire quelques daemons (programmes démons) afin de pouvoir gérer ses SMS et écrire quelques scripts pour envoyer les SMS soit vers une plateforme externe, soit pour les stocker dans un fichier dans un répertoire donné. [6]

2.7 Deamon (démon)

Un daemon est un type de programme sur les systèmes d'exploitation de type Unix qui s'exécute de manière non structurée en arrière-plan, qui n'est pas sous le contrôle direct d'un utilisateur et est toujours en attente d'être activé par l'occurrence d'un événement ou d'une condition spécifique.

Les systèmes semblables à Unix exécutent souvent de nombreux démons, principalement pour répondre aux demandes de services provenant d'autres ordinateurs sur un réseau, mais aussi pour répondre à d'autres programmes et aux activités matérielles. Les exemples d'actions ou de conditions qui peuvent déclencher l'activité des démons sont une heure ou une date spécifique, le passage d'un intervalle de temps spécifié, une arrivée de fichier dans un répertoire particulier, la réception d'un courrier électronique ou une demande Web effectuée par une ligne de communication particulière. Il n'est pas nécessaire que l'auteur de l'action ou de l'état

soit conscient qu'un auditeur écoute, bien que les programmes exécutent souvent une action uniquement parce qu'ils sont conscients qu'ils susciteront implicitement un démon.

Les démons sont généralement instanciés en tant que processus. Un processus est une instance d'exécution (c'est-à-dire en cours d'exécution) d'un programme. Les processus sont gérés par le noyau (c'est-à-dire le noyau du système d'exploitation), qui attribue à chacun un numéro d'identification de processus unique (PID).

Il existe trois types de processus de base dans Linux : interactive, batch et daemon. Les processus interactifs sont exécutés de manière interactive par un utilisateur sur la ligne de commande (c'est-à-dire, le mode texte intégral). Les processus batch (par lots) sont soumis à une file d'attente de processus et ne sont pas associés à la ligne de commande ; Ils sont bien adaptés pour effectuer des tâches récurrentes lorsque l'utilisation du système est par ailleurs faible

Certains daemons sont lancés via des scripts init System V, qui sont des scripts (c'est-à-dire des programmes courts) qui s'exécutent automatiquement lorsque le système démarre. Ils peuvent survivre pour la durée de la session ou être régénérés à intervalles.

En plus d'être lancé par le système d'exploitation et par des programmes d'application, certains daemons peuvent également être démarrés manuellement. Les exemples de commandes qui lancent les démons incluent binlogd (qui enregistre les événements binaires sur les fichiers spécifiés), mysqld (serveur MySQL Database) et Apache (le serveur web Apache). [7]

2.8 WAMPSERVER

Figure 8 : Logo WampServer avec utilitaires inclus.

WampServer (anciennement WAMP5) est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement (sans avoir à se connecter à un serveur externe) des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant deux serveurs (Apache et MySQL), un interpréteur de script (PHP), ainsi que phpMyAdmin pour l'administration Web des bases MySQL.

Il dispose d'une interface d'administration permettant de gérer et d'administrer ses serveurs au travers d'un tray icon (icône près de l'horloge de Windows).

La grande nouveauté de WampServer 2 réside dans la possibilité d'y installer et d'utiliser n'importe quelle version de PHP, Apache ou MySQL en un clic. Ainsi, chaque développeur peut reproduire fidèlement son serveur de production sur sa machine locale. [8]

2.9 Organigramme du procédé d'identification

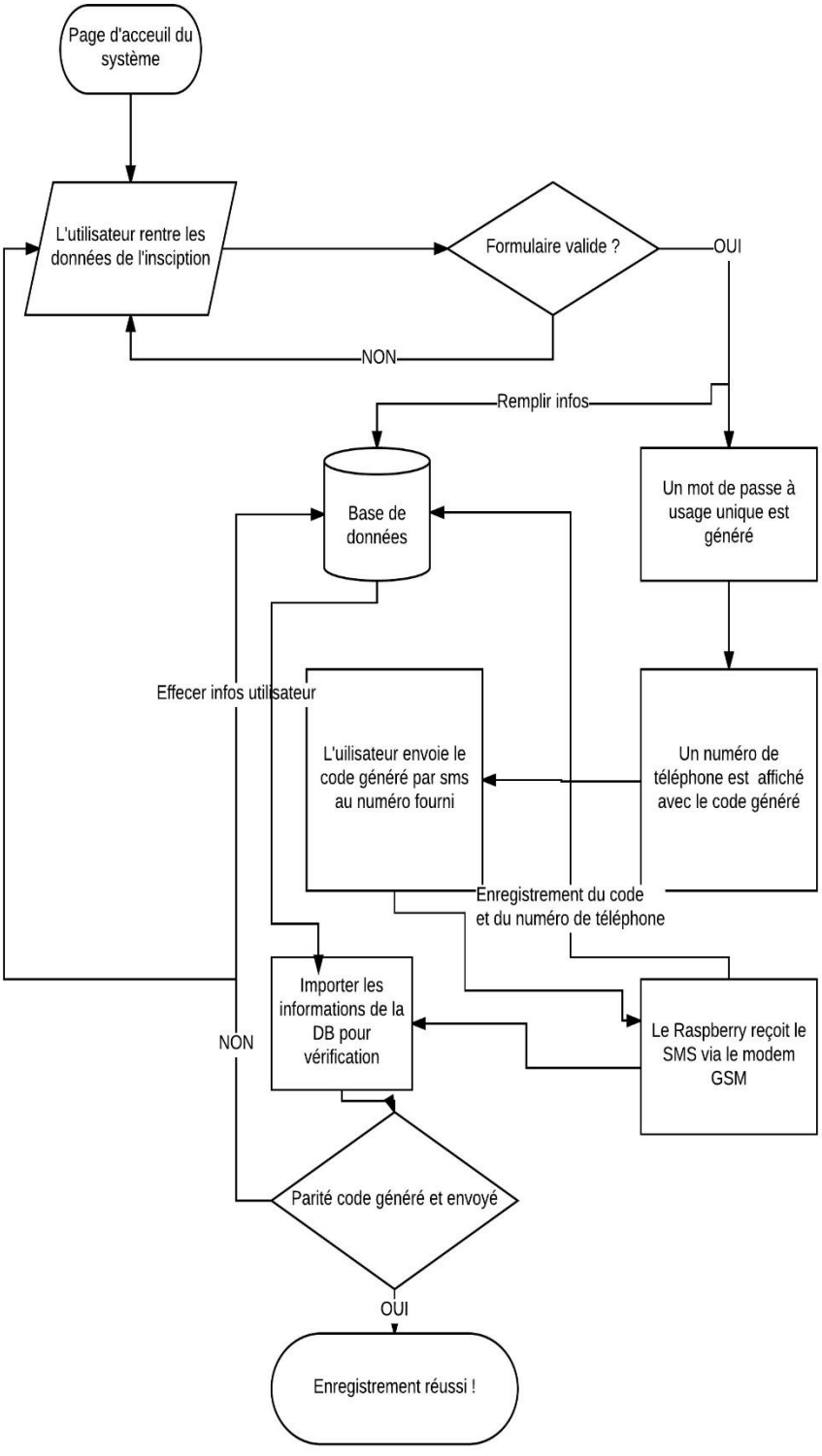


Figure 9 : organigramme du procédé de l'identification.

2.9.1 Description :

Tout d'abord, comme à chaque nouvelle inscription, il faut renseigner les informations nécessaires à cette dernière. Une fois cette étape terminée, la validité du formulaire est checkée via de simples tests de conformité préalablement mis en place.

Si le formulaire est valide, alors un mot de passe sous forme de code à usage unique est généré, et dans le même temps les informations déjà vérifiées sont stockées dans la base de données. Mais si en revanche, ce n'est pas le cas, l'utilisateur est redirigé vers le formulaire d'inscription pour vérifier les informations fournies.

Après succès de vérification, le code généré est affiché sur une nouvelle page, associé à un numéro de téléphone. L'utilisateur se charge ensuite d'envoyer le codé affiché au numéro de téléphone qui est aussi affiché à l'écran.

Ensuite, le Raspberry collecte les informations reçues pour les envoyer à la base de données pour comparer ces dernières avec les données collectées via le formulaire d'inscription.

Si les deux numéros de téléphone ainsi que les deux codes (généré et envoyé par sms) concordent, alors l'utilisateur est redirigé vers la dernière page web indiquant que l'inscription a correctement été effectuée. Sinon, dans le cas où soit les codes ou bien les numéros de téléphone ne concordent pas, par mesure de sécurité, l'utilisateur est redirigé vers le formulaire initial pour une vérification des informations, et les données qui ont été enregistrées sont effacées pour libérer l'espace occupé dans la base de données.

2.10 Diagramme de séquence

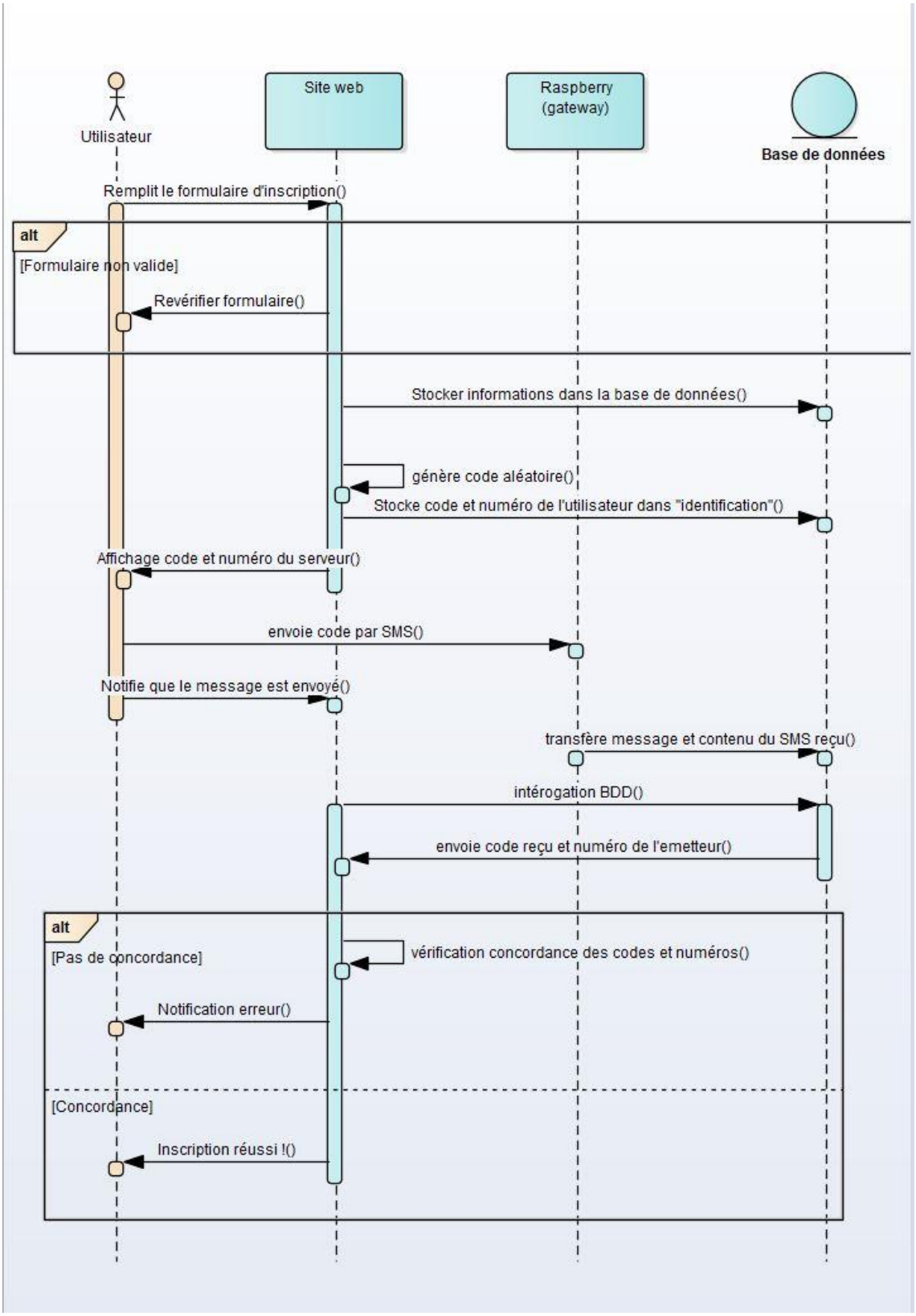


Figure 10 : DS du processus d'inscription.

2.10.1 Description :

Dans ce diagramme de séquence, on détaille tout le processus, les tâches et actions effectuées par les différents acteurs pour le bon fonctionnement de notre système.

Le premier acteur, l'utilisateur de notre système se charge de remplir le formulaire d'inscription, c'est alors qu'intervient notre page web via un script PHP, pour vérifier les informations contenues dans le formulaire, si celles-ci ne sont pas valides, le site web renvoie une demande à l'utilisateur afin que ce dernier puisse revérifier les informations entrées.

Ce stade une fois dépassé, le site web stocke les données collectées dans la base de données, et génère ensuite un code aléatoire qui sera utilisé par la suite.

Le site web affiche ensuite à l'utilisateur, le code précédemment généré auquel il associe un numéro de téléphone correspondant à la carte SIM contenue dans notre Raspberry.

L'utilisateur prend alors son téléphone, et envoie le code qui lui est affiché à l'écran au numéro de téléphone indiqué sur la page web, le SMS sera destiné au Raspberry, une fois l'opération accomplie, il notifie le site web qu'il a bien effectué l'opération demandée, en cliquant sur le bouton adéquat.

C'est à ce stade qu'intervient le Raspberry, en effet, après avoir reçu le SMS, la gateway envoie les données reçues à la base de données, c'est à dire le SMS ainsi que le numéro de téléphone de l'émetteur du message.

Le site web effectue ensuite une interrogation de la base de données, pour y recueillir les informations concernant le message reçu par le Raspberry et procède à la vérification de conformité des informations récoltées d'une part, via le formulaire d'inscription, et d'autre part, par le biais du Raspberry.

Si les codes et numéros concordent, le site web notifie à l'utilisateur que l'inscription est réussie, sinon une erreur lui est notifiée, et le processus doit être recommencé.

Chapitre 3 : mise en place du système.

3.1 Installation et configuration de WampServer

On commence tout d'abord par télécharger et installer WampServer, on choisit aussi un port spécifique pour que les machines externes arrivent à communiquer avec ce dernier.

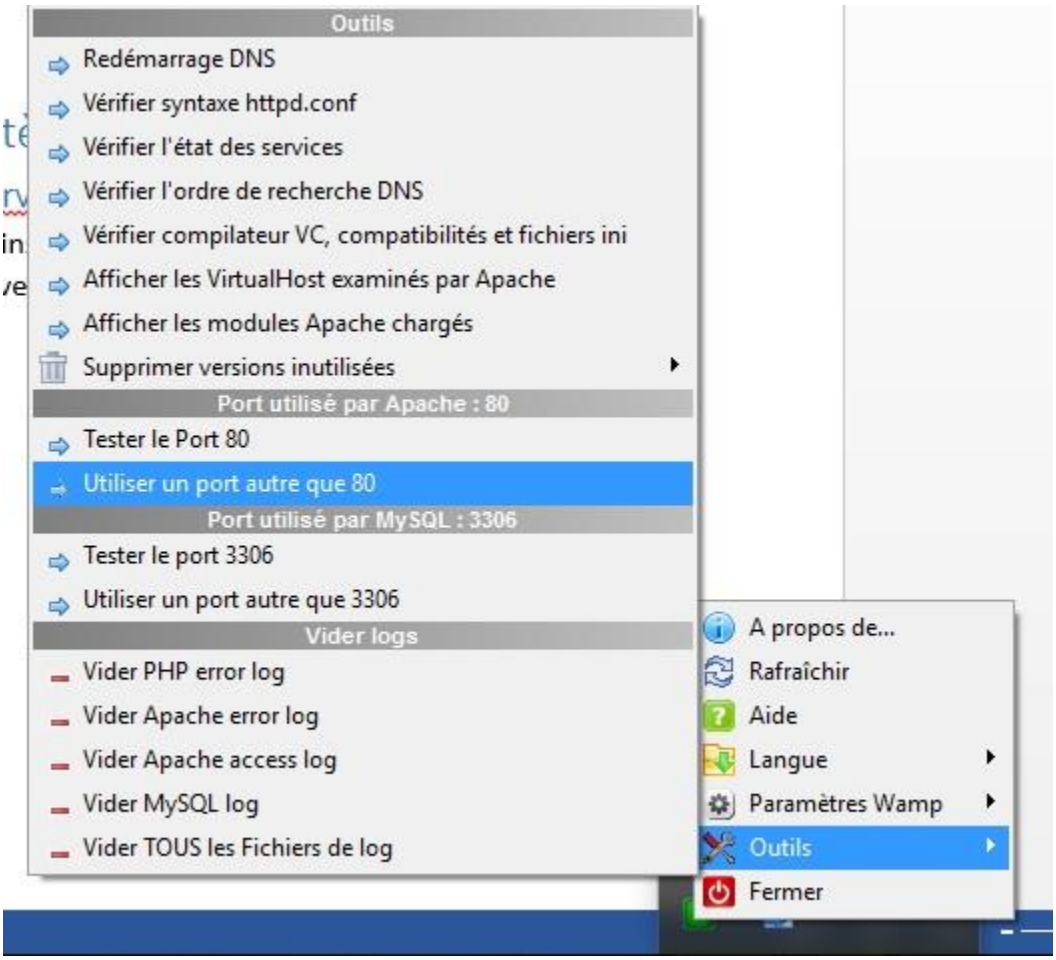


Figure 11 : Spécification du port WampServer.

On configure ensuite le serveur en créant un compte, avec un certain niveau d'accès selon le niveau d'habilitation, on aura ainsi la possibilité de créer une base de données pour l'application.

Dans le cadre de ce projet, WampServer a été installé sur Windows, mais il est aussi possible de le mettre en place sur les distributions Linux à l'aide de LampServer, qui est dédié spécialement à celles-ci.

3.2 Création d'une base de données adéquate pour l'application

Tout d'abord, on a créé une base de données nommée « projet » qu'on va utiliser durant ce projet, on a ensuite créé les tables nécessaires pour la bonne tenue du projet comme c'est indiqué ci-dessous.

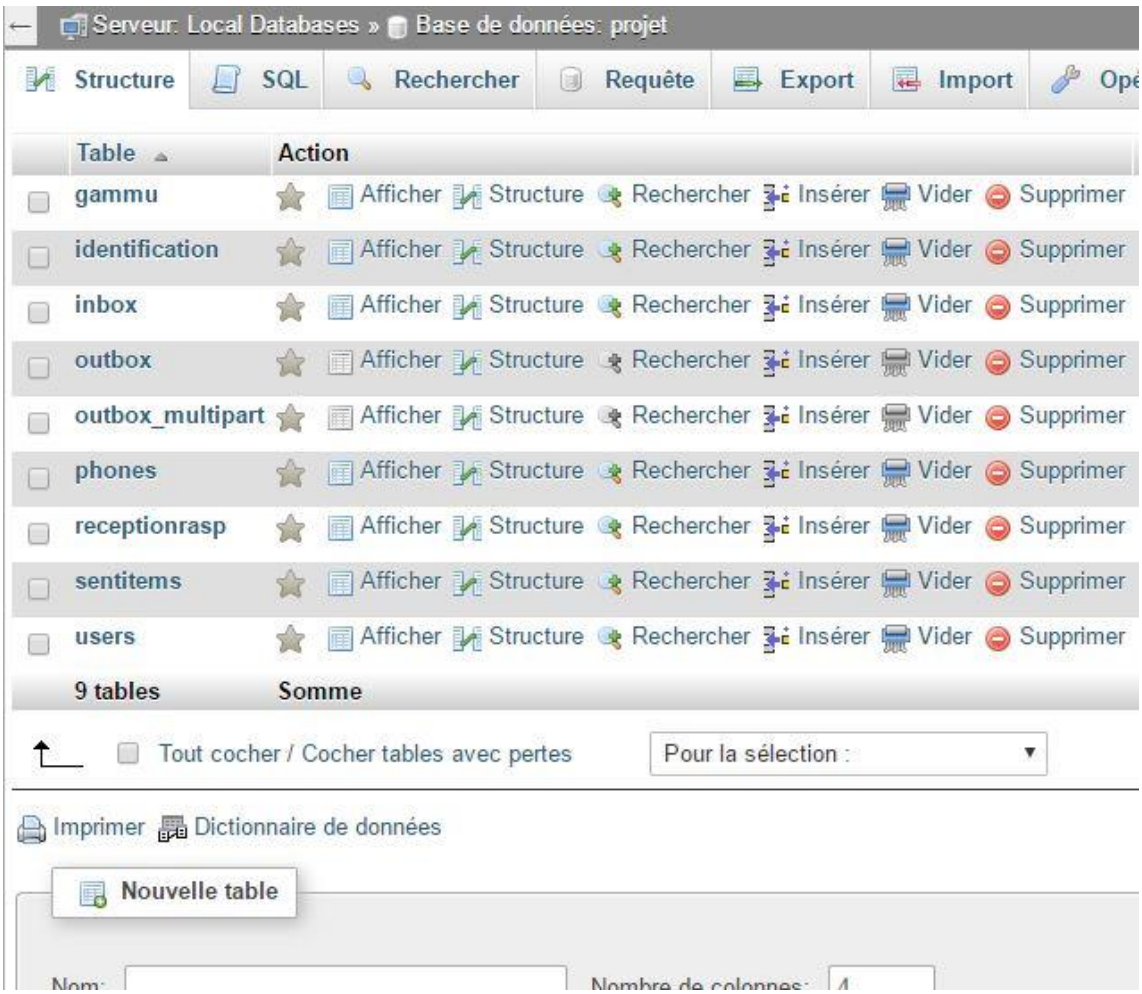


Figure 12 : Base de données serveur.

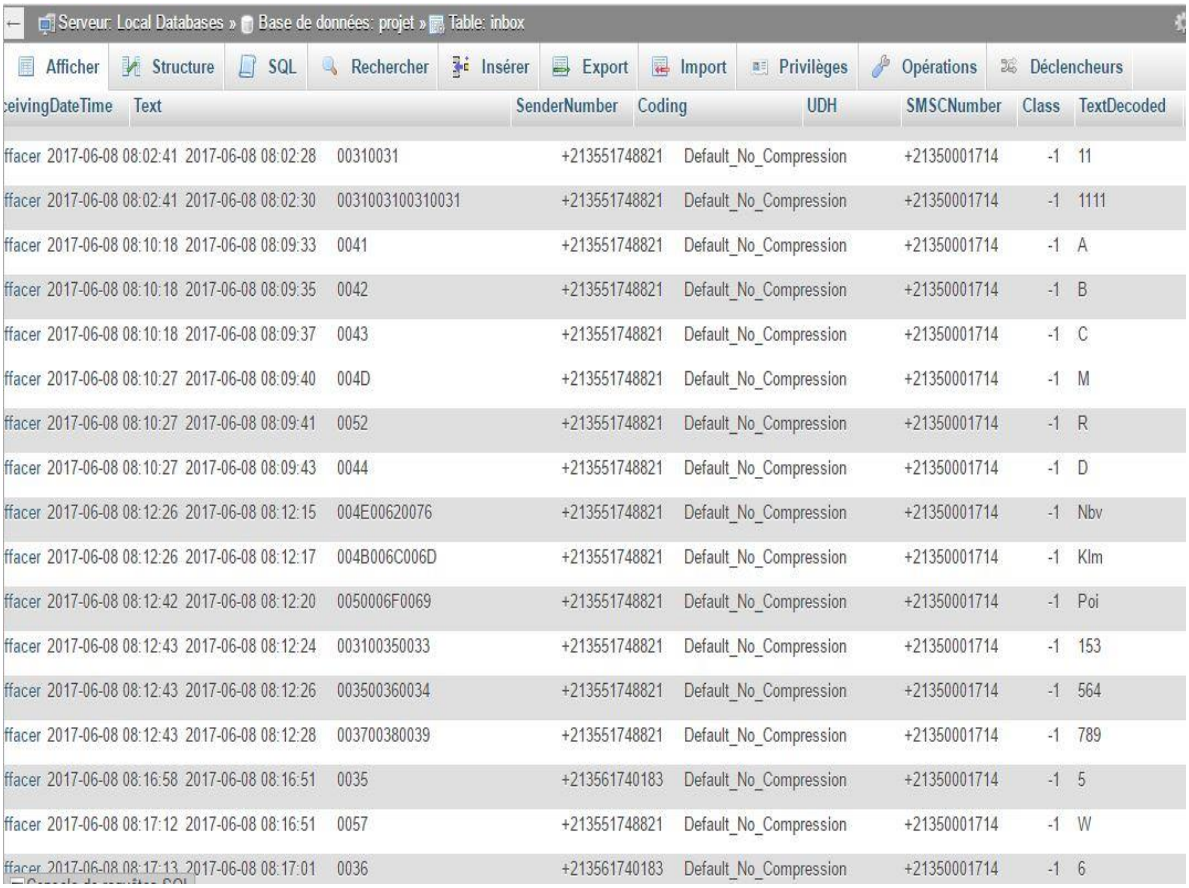
Les tables qui nous intéressent spécialement ici sont les tables suivantes :

1. Inbox
2. Identification
3. Users

Ces trois tables sont en effet les éléments clés de la base de données, les autres tables présentes sont nécessaires au bon fonctionnement de l'utilitaire Gammu qu'on verra par la suite.

3.2.1 Table « inbox »

Cette table contient comme son nom l'indique toutes les informations reçues par le Raspberry quand un SMS arrive (l'identité de l'émetteur, le contenu du message, date et heure…etc).


Serveur: Local Databases » Base de données: projet » Table: inbox

Afficher | Structure | SQL | Rechercher | Insérer | Export | Import | Privilèges | Opérations | Déclencheurs

eivingDateTime	Text	SenderNumber	Coding	UDH	SMSCNumber	Class	TextDecoded
ffacer 2017-06-08 08:02:41	2017-06-08 08:02:28 0031003100310031	+213551748821	Default_No_Compression		+21350001714	-1	1111
ffacer 2017-06-08 08:10:18	2017-06-08 08:09:33 0041	+213551748821	Default_No_Compression		+21350001714	-1	A
ffacer 2017-06-08 08:10:18	2017-06-08 08:09:35 0042	+213551748821	Default_No_Compression		+21350001714	-1	B
ffacer 2017-06-08 08:10:18	2017-06-08 08:09:37 0043	+213551748821	Default_No_Compression		+21350001714	-1	C
ffacer 2017-06-08 08:10:27	2017-06-08 08:09:40 004D	+213551748821	Default_No_Compression		+21350001714	-1	M
ffacer 2017-06-08 08:10:27	2017-06-08 08:09:41 0052	+213551748821	Default_No_Compression		+21350001714	-1	R
ffacer 2017-06-08 08:10:27	2017-06-08 08:09:43 0044	+213551748821	Default_No_Compression		+21350001714	-1	D
ffacer 2017-06-08 08:12:26	2017-06-08 08:12:15 004E00620076	+213551748821	Default_No_Compression		+21350001714	-1	Nbv
ffacer 2017-06-08 08:12:26	2017-06-08 08:12:17 004B006C006D	+213551748821	Default_No_Compression		+21350001714	-1	Klm
ffacer 2017-06-08 08:12:42	2017-06-08 08:12:20 0050006F0069	+213551748821	Default_No_Compression		+21350001714	-1	Poi
ffacer 2017-06-08 08:12:43	2017-06-08 08:12:24 003100350033	+213551748821	Default_No_Compression		+21350001714	-1	153
ffacer 2017-06-08 08:12:43	2017-06-08 08:12:26 003500360034	+213551748821	Default_No_Compression		+21350001714	-1	564
ffacer 2017-06-08 08:12:43	2017-06-08 08:12:28 003700380039	+213551748821	Default_No_Compression		+21350001714	-1	789
ffacer 2017-06-08 08:16:58	2017-06-08 08:16:51 0035	+213561740183	Default_No_Compression		+21350001714	-1	5
ffacer 2017-06-08 08:17:12	2017-06-08 08:16:51 0057	+213551748821	Default_No_Compression		+21350001714	-1	W
ffacer 2017-06-08 08:17:13	2017-06-08 08:17:01 0036	+213561740183	Default_No_Compression		+21350001714	-1	6

Figure 13 : Structure table Inbox.

3.2.2 Table « users »

Cette table est remplie par la première page contenant le formulaire d'inscription, qui, une fois terminé et validé, envoie les données listées ci-dessous vers la table.

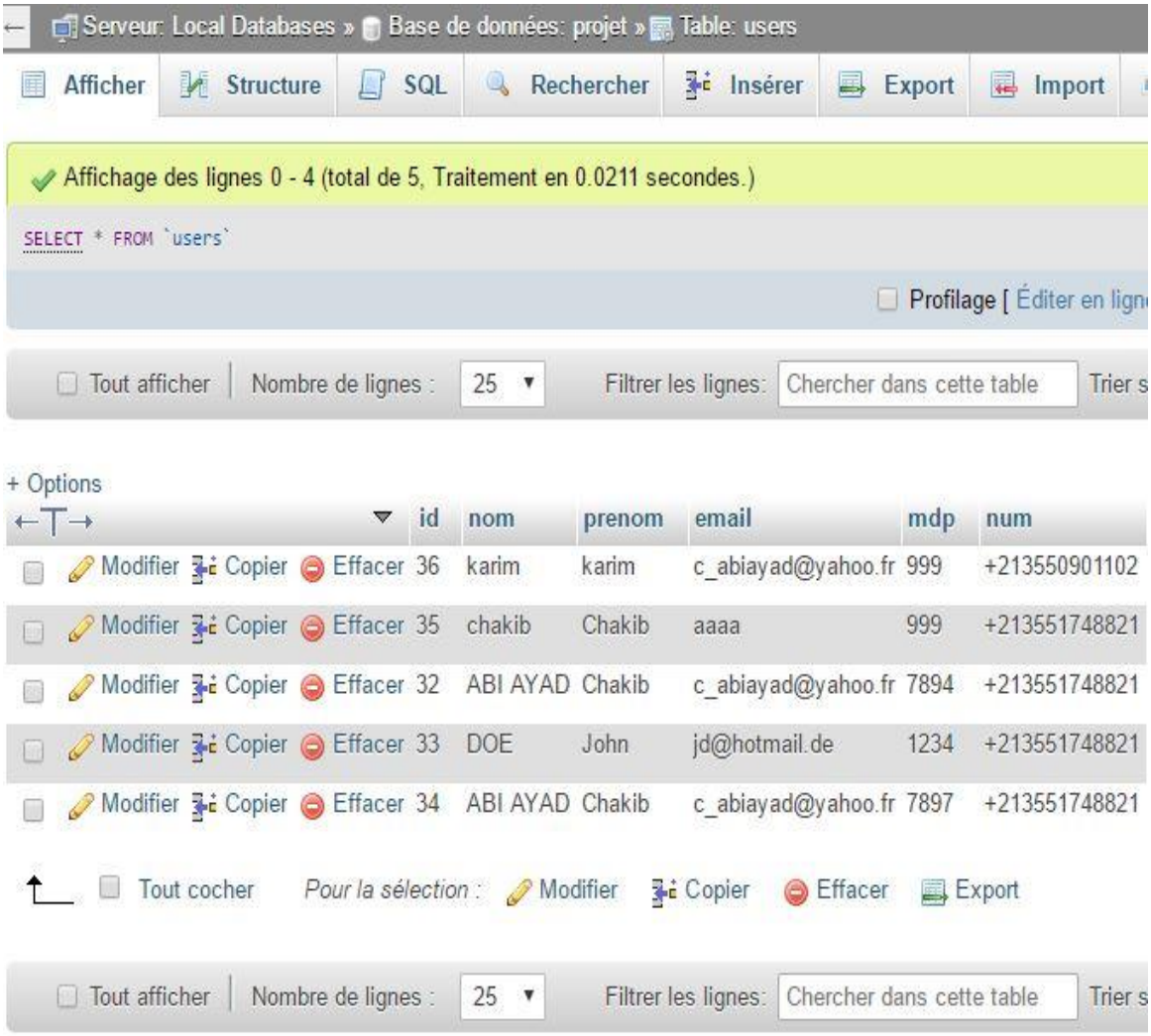


Figure 14 : Structure table "Users".

3.2.3 Table « identification »

Après s'être enregistré, le numéro de téléphone entré par l'utilisateur ainsi que le code qui a été généré par l'application sont stockés dans cette table, ainsi on pourra comparer ces données avec la table « inbox »

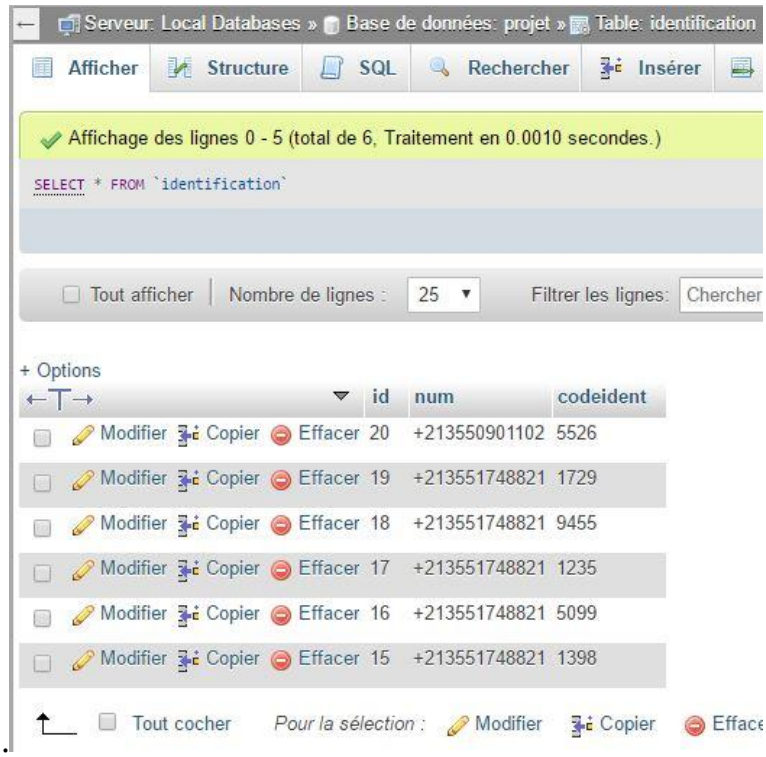


Figure 15 : Structure table "Identification"

3.2.4 Structure de la base de données

On obtient ainsi la structure suivante (les tables pertinentes) :

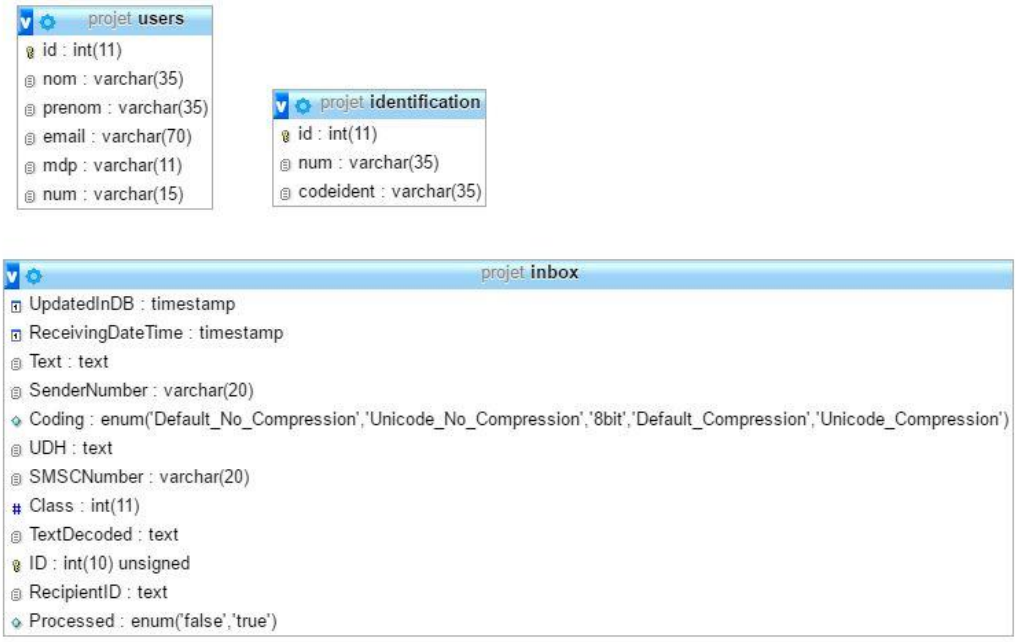


Figure 16 : Structure base de données.

3.3 Implémentation des pages web

3.3.1 Index.php

Cette première page, considérée comme page d'accueil contient le formulaire d'inscription composé du nom, prénom, email, mot de passe et confirmation du mot de passe et le numéro de téléphone.

Le formulaire est doté de la méthode « POST » qui envoie les informations remplies vers la page « add.php »

A noter que sur cette page, une fonction Javascript intitulée « validatePassword » est présente pour contrôler et vérifier la parité des deux mots de passes entrés qui sont notés « mdp » et « confirm_mdp »

3.3.2 Add.php

La page « add.php » récupère les informations reçues par le formulaire contenu dans la page « index.php ». Elle insère ensuite ces données, dans la base de données après s'être connectée à la base de données et affiche à l'utilisateur que les informations ont bien été entrées dans la base de données et le redirige vers la page, ou bien qu'il manque certaines informations s'il y a un problème avec les données reçues et le redirige vers la page « index.php ».

3.3.3 Appel.php

Les lignes de code de cette page permettent de générer un code aléatoire de 4 chiffres qui va être affiché à l'utilisateur (voir figure ci-dessous), et de le stocker ensuite avec le numéro de téléphone de l'utilisateur qui a été entré dans le formulaire et qu'on a récupéré grâce à une session ouverte dans la page « add.php »

```php
<?php
  session_start();
  if (isset($_SESSION['num']))
    {
        $num=$_SESSION['num'];
        $codeident=1000 + mt_rand(0, 8999);  //générer un code aléatoire
        echo $num;
        $_SESSION['codeident'] = $codeident;
        try
            {
             $base = new PDO('mysql:host=localhost;dbname=projet;charset=utf8', 'ident', '');
            }
        catch(Exception $e)
            {
                    die('Erreur : '.$e->getMessage());
            }

        // On ajoute une entrée dans la table identification
        try {
        $req = $base->prepare('INSERT INTO identification(num,codeident) VALUES(:num, :codeident)');
        $req->execute(array(
                            'num' => $num,
                            'codeident' => $codeident,
                            ));
            }
        catch(Exception $e)
            {
                    die('Erreur : '.$e->getMessage());
            }

    }
```

Figure 17 : partie code appel.php

3.3.4 Wait.php

Cette page s'affiche à l'utilisateur après qu'il ait envoyé le SMS au modem GSM, elle permet d'indiquer à l'utilisateur que la vérification est en cours, et qu'il doit patienter

quelques secondes pendant que le Raspberry reçoit le SMS et stocke les informations reçues dans la table correspondante qui est « inbox ».

3.3.5 Success.php

Cette dernière page s'occupe de la conformité du code généré au préalable avec le code envoyé par l'utilisateur qu'on récupère avec une simple requête SQL après s'être connecté à la base de données (on s'y connecte à chaque fois pour éviter les problèmes de déconnexion subite), et l'on fait de même pour le numéro de téléphone.

Deux messages d'alertes sont également présents pour notifier l'utilisateur de la réussite ou bien de l'échec de l'inscription.

3.4 Configuration du Raspberry

3.4.1 Installation du système d'exploitation

On commence tout d'abord par décompresser un fichier .img compatible avec le Raspberry, dans le cadre de ce projet on a décidé d'installer sur la Raspberry une distribution Linux Ubuntu à l'aide de l'utilitaire Rufus.

Une fois l'opération finie, on démarre le système puis le configure en activant le protocole SSH au démarrage du système pour qu'on puisse communiquer avec le Raspberry depuis n'importe quelle machine ou périphérique dans le réseau, et pour cela on doit exécuter les commandes suivantes

1. # sudo update-rc.d ssh defaults
2. # sudo systemctl enable ssh.service

3.5 Accès au Raspberry et configuration du modem GSM

Une fois l'installation finie, on se connecte au Raspberry grâce à Putty, un client SSH léger dans lequel on saisit l'adresse réseau du Raspberry comme suit :

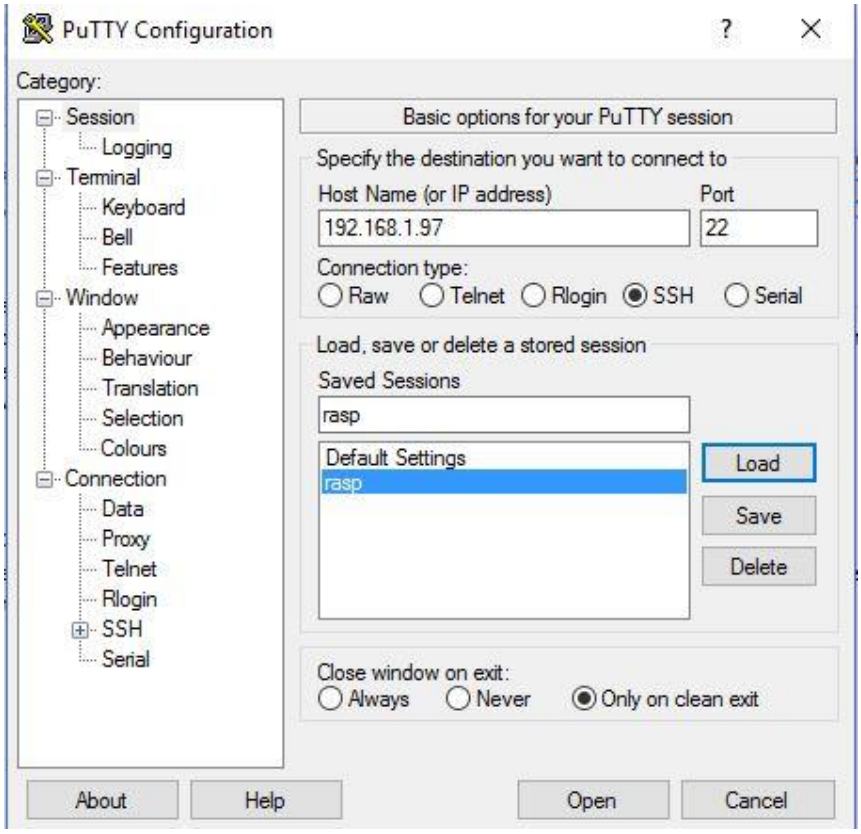


Figure 17 : Connexion distante via protocol SSH.

Après avoir cliqué sur « Open », une fenêtre s'ouvre demandant de saisir le nom d'utilisateur et mot de passe pour se connecter au Raspberry.

On connecte maintenant le modem GSM par USB au Raspberry et on vérifie qu'il est bien connecté à l'aide de la commande « lsusb » :

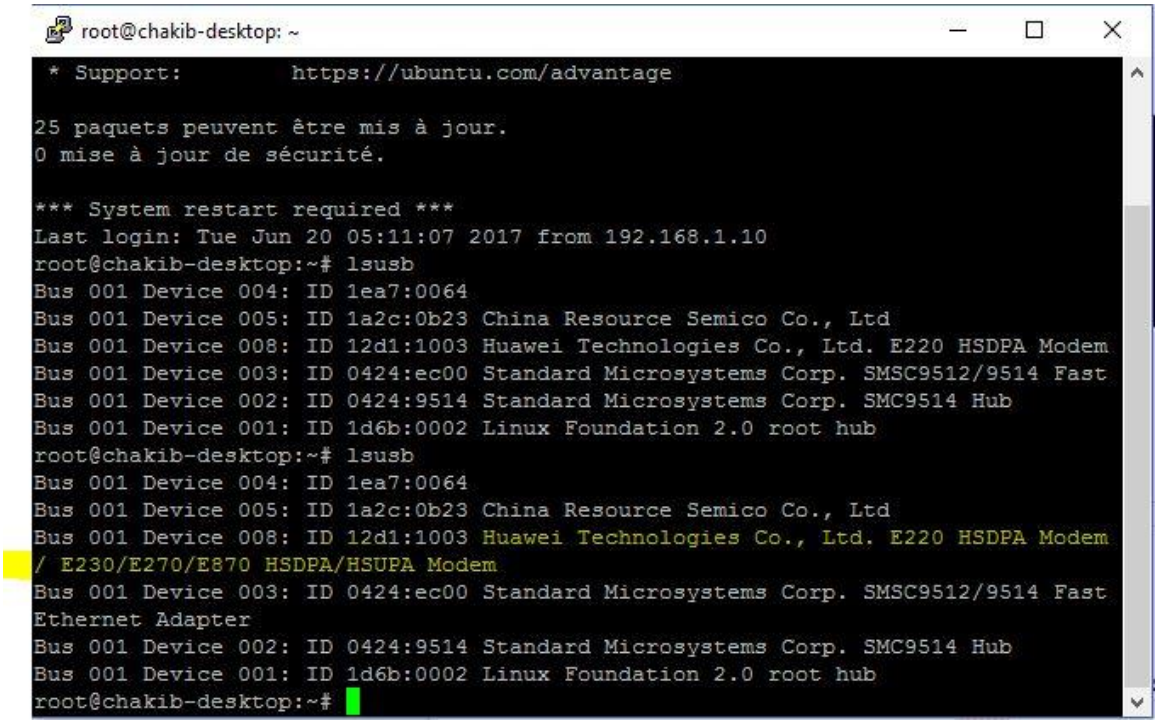


Figure 19 : Liste périphériques USB connectés.

3.6 Installation et configuration de Gammu

On procède maintenant à l'installation de Gammu avec le service daemon (démon) qui permet de connecter des scripts daemon avec l'utilitaire Gammu lui-même

Une fois l'installation terminée, on doit identifier le port qui est réservé au modem GSM, en exécutant la commande suivante : « dmesg »

Une fois le port identifié on configure Gammu à l'aide de la commande « gammu–config »

Une fois accédé à la configuration, on sélectionne le bon port ainsi que les données correspondantes à la carte SIM, puis on sélectionne « save » pour sauvegarder les modifications. Avant de continuer on vérifie que le système est bien configuré à

l'aide de la commande « gammu –identify »

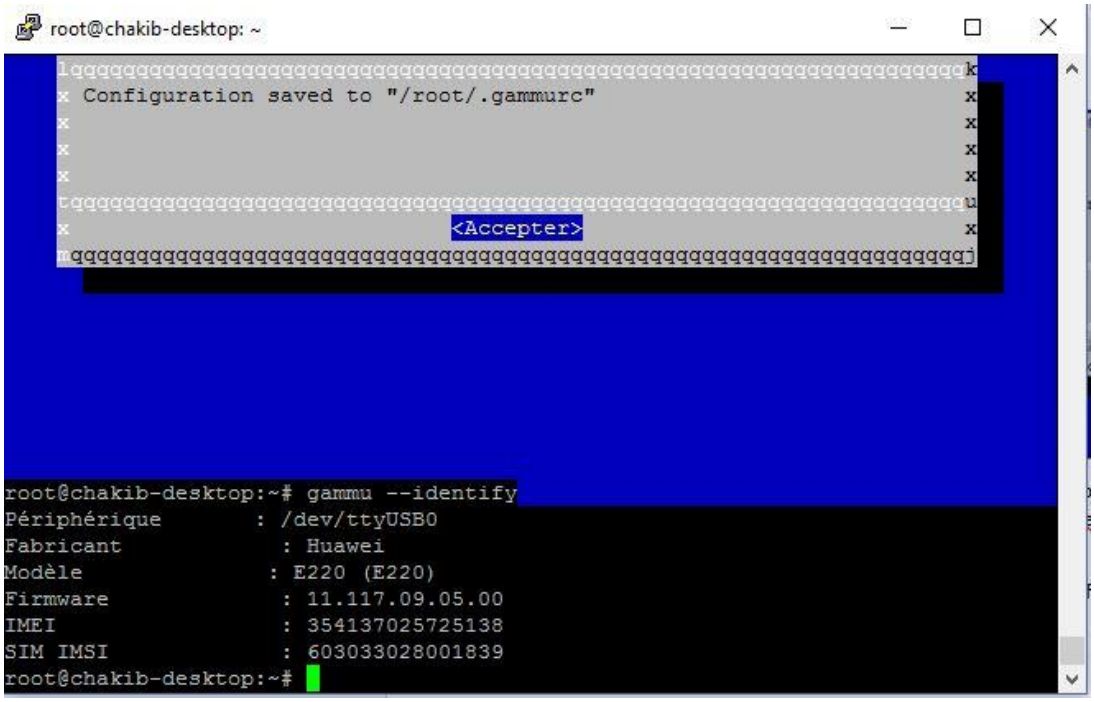


Figure 20 : Identification du modem GSM.

On peut attester grâce à la figure ci-dessus que le modem GSM est bien configuré et que Gammu fonctionne parfaitement, et est prêt à servir.

3.7 Mise en place du daemon

Maintenant qu'on a tout le dispositif prêt et fonctionnel, on s'attaque à la partie daemon, qui est la plus importante, pour cela, on commence par mettre en place un fichier de configuration

```
[gammu]
device = /dev/ttyUSB0
#model = 6110
connection = at19200
#synchronizetime = yes
#logfile = gammulog # this is not used at all in SMSD mode
#logformat = textall
#use_locking = yes
#gammuloc = gammu.us
#startinfo = yes



[smsd]

service= Mysql
# PIN for SIM card
PIN = 1234
# File
logfile = smsdlog
# Amount of information being logged, each bit mean one level
debuglevel = 0

# Commication frequency settings
commtimeout = 30
sendtimeout = 30
#receivefrequency = 0
```

Figure 21 : fichier de configuration du daemon P1.

```
#deliveryreport = no
#deliveryreportdelay = 10

# Ignoring broken SMSC
#skipsmscnumber = +48602123456
phoneid = Huawei

# Database backends congfiguration
user = rasp
password =
pc = 192.168.1.8
# pc can also contain port or socket path after colon (eg. localhost:/path/to/socket)
database = projet

# DBI configuration
#driver = native_mysql
# driverspath = /usr/lib/dbd/
# Database directory for sqlite
# dbdir = /var/lib/smsd

# Files backend configuration
#inboxpath = /var/spool/sms/inbox/
#outboxpath = /var/spool/sms/outbox/
#sentsmspath = /var/spool/sms/sent/
#errorsmspath = /var/spool/sms/error/
#inboxformat = unicode
#transmitformat = auto
#outboxformat = detail
```

Figure 22 : Fichier de configuration du daemon P2.

Sur ce fichier, on a défini l'ID du modem GSM, le service de stockage du sms (mysql), pour que les SMS reçus soient directement stockés dans la base de données précédemment créée.

3.8 Multiplier les modems GSM

Une fois un daemon configuré, on peut reproduire la même chose en insérant un autre modem GSM qu'on peut différencier avec le premier grâce aux ports utilisés par les modems (figure ci-dessous), une fois le deuxième modem inséré, il suffit de créer et remplir le même fichier de configuration, à deux différences près :

1. Le port dans lequel le modem a été identifié.
2. Le nom de l'ID, car il est unique à chaque modem, sinon on ne pourra pas faire la différence entre eux au niveau de la base de données

Comme cela, on a la possibilité de recevoir plus de SMS en même temps, ce qui rend le système beaucoup plus performant et capable de gérer un grand nombre d'inscriptions en même temps.

3.9 Lancement du démon

Le lancement du daemon se fait par une seule ligne de commande :

« gammu-smsd -c /chemin/fichier_de_configuration_créé -d»

Qui une fois exécutée active le daemon à l'aide du fichier de configuration à chaque démarrage du Raspberry, et ceci grâce au « -d » qui veut dire « daemonize », qui en français veut dire « démonisé », entre autres, le service se lancera immédiatement, et aussi à chaque démarrage du système.

3.10 Fonctions supplémentaires

Il existe plusieurs fonctions qu'on peut exploiter, comme par exemple l'envoi des SMS depuis le Raspberry, si par exemple une entreprise en question choisit d'envoyer des SMS à ses clients pour une raison tierce, grâce à la commande suivante qu'on peut aussi mettre dans un script donné : `echo "message" | gammu sendsms TEXT « numéro du destinataire »`

Chapitre 4 : Déroulement du processus d’inscription et récapitulatif

Dans ce dernier chapitre on va voir comment se passe le processus d'inscription de l'utilisateur pas à pas, on commence d'abord par remplir le formulaire d'inscription :

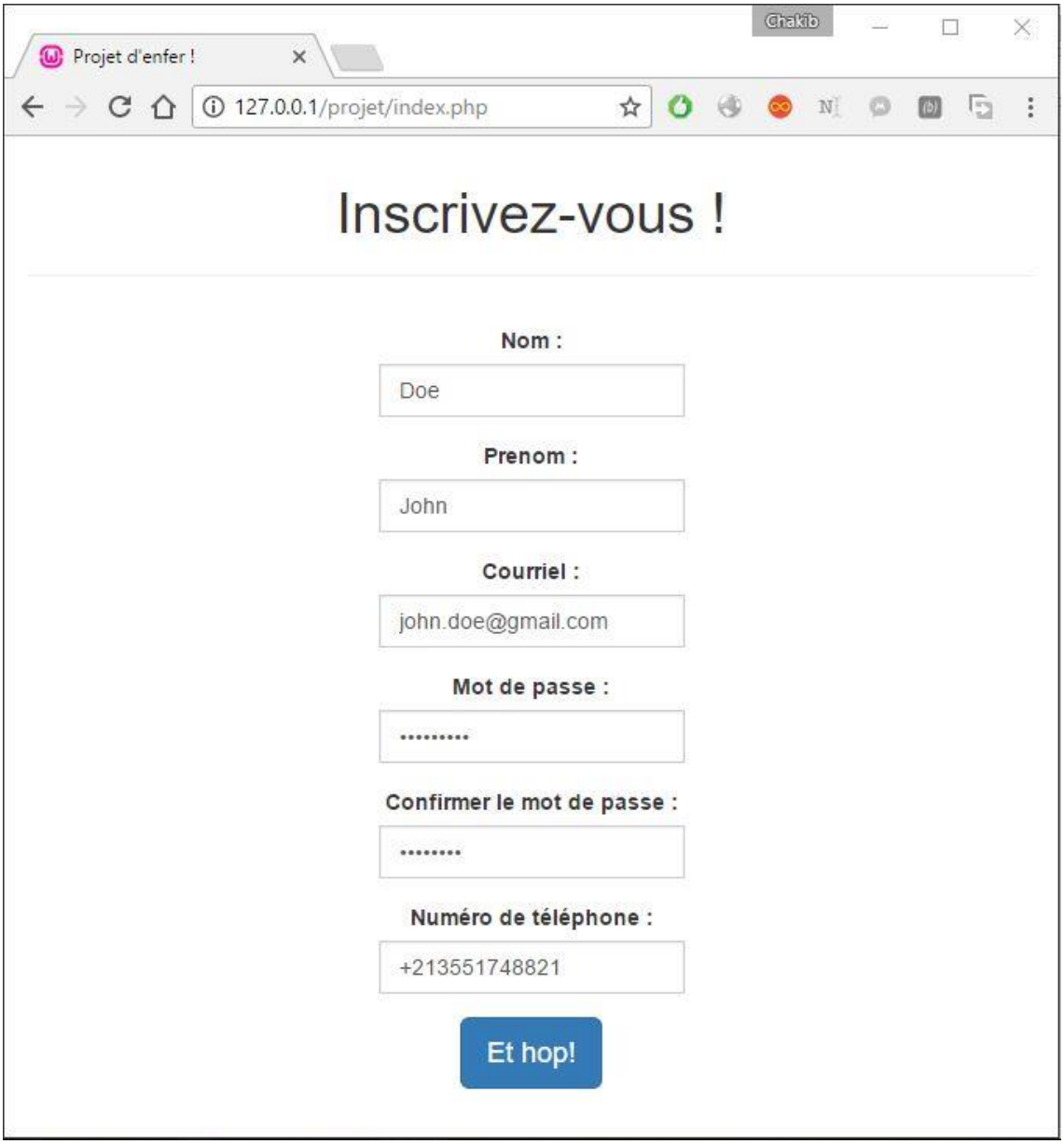


Figure 23 : Index.php

Après avoir cliqué sur « Et hop ! » on est redirigé vers la page « add.php » qui affiche ceci :

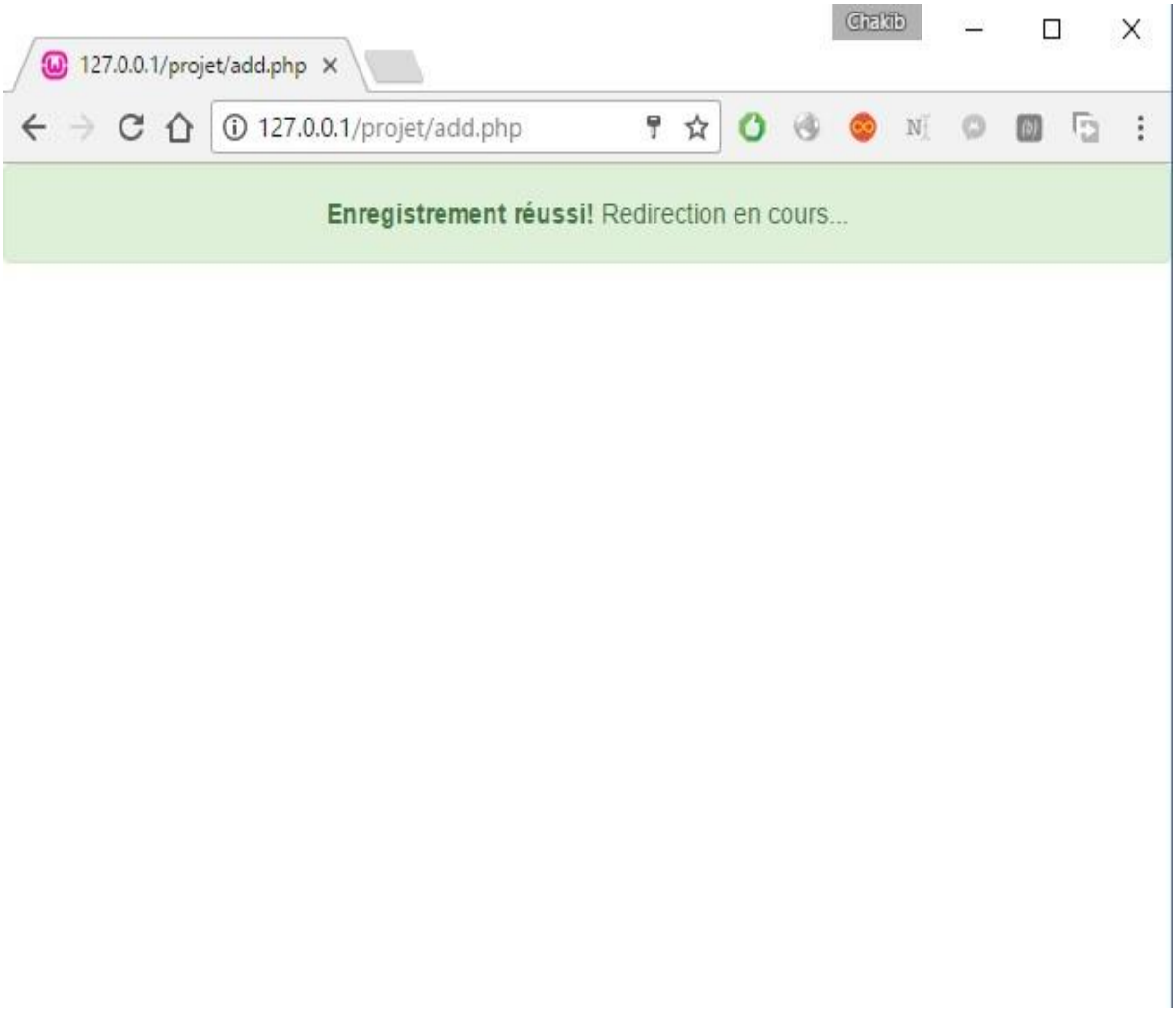


Figure 24 : add.php

Si l'utilisateur se trompe et ne remplit pas tout le formulaire un message d'erreur s'affiche comme ceci :

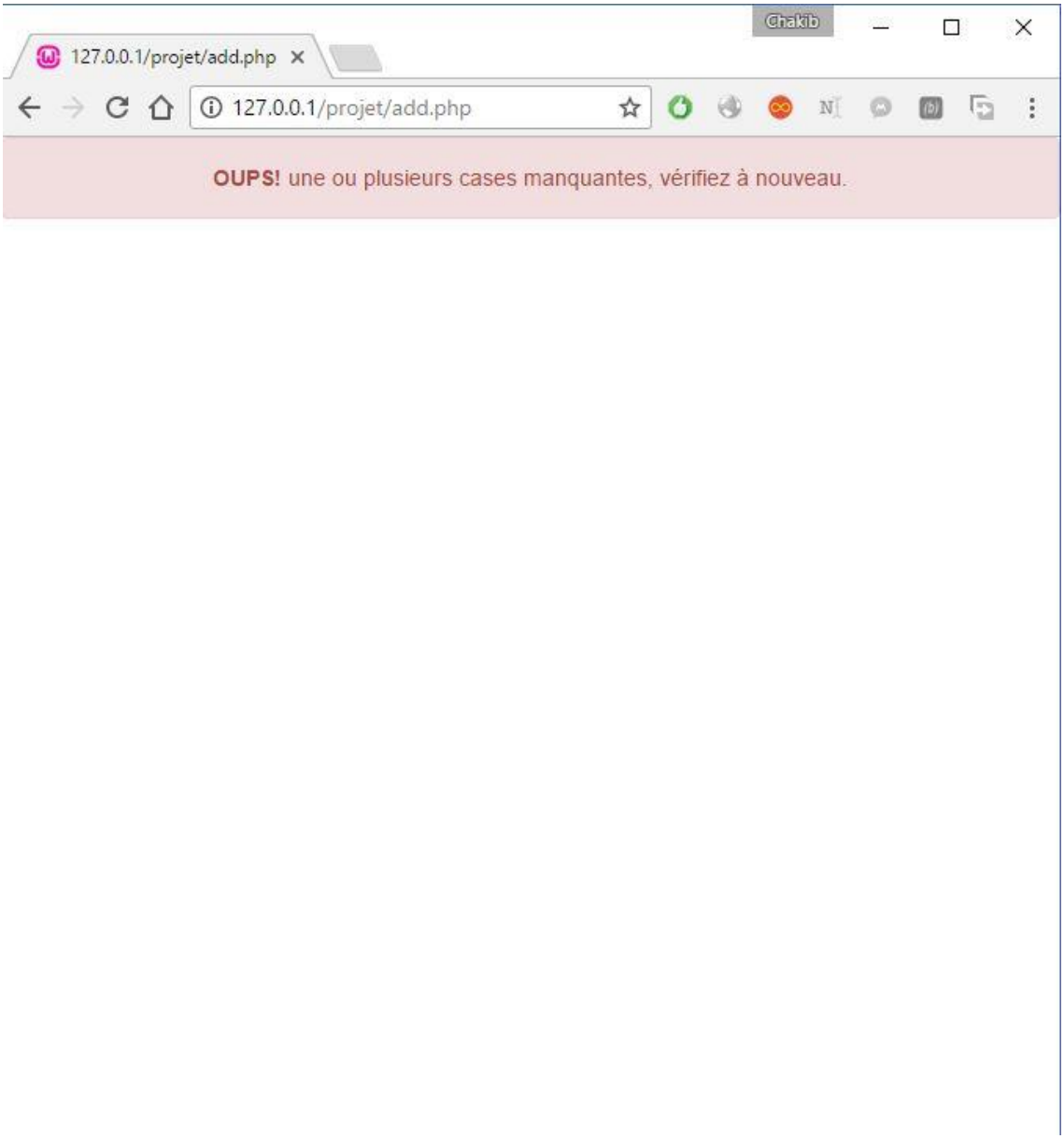


Figure 25 : add.php (erreur).

Une fois l'enregistrement réussi, et les informations transmises à la base de données, on est redirigé vers la page « appel.php » dans laquelle il est demandé d'envoyer le code par SMS au numéro affiché :

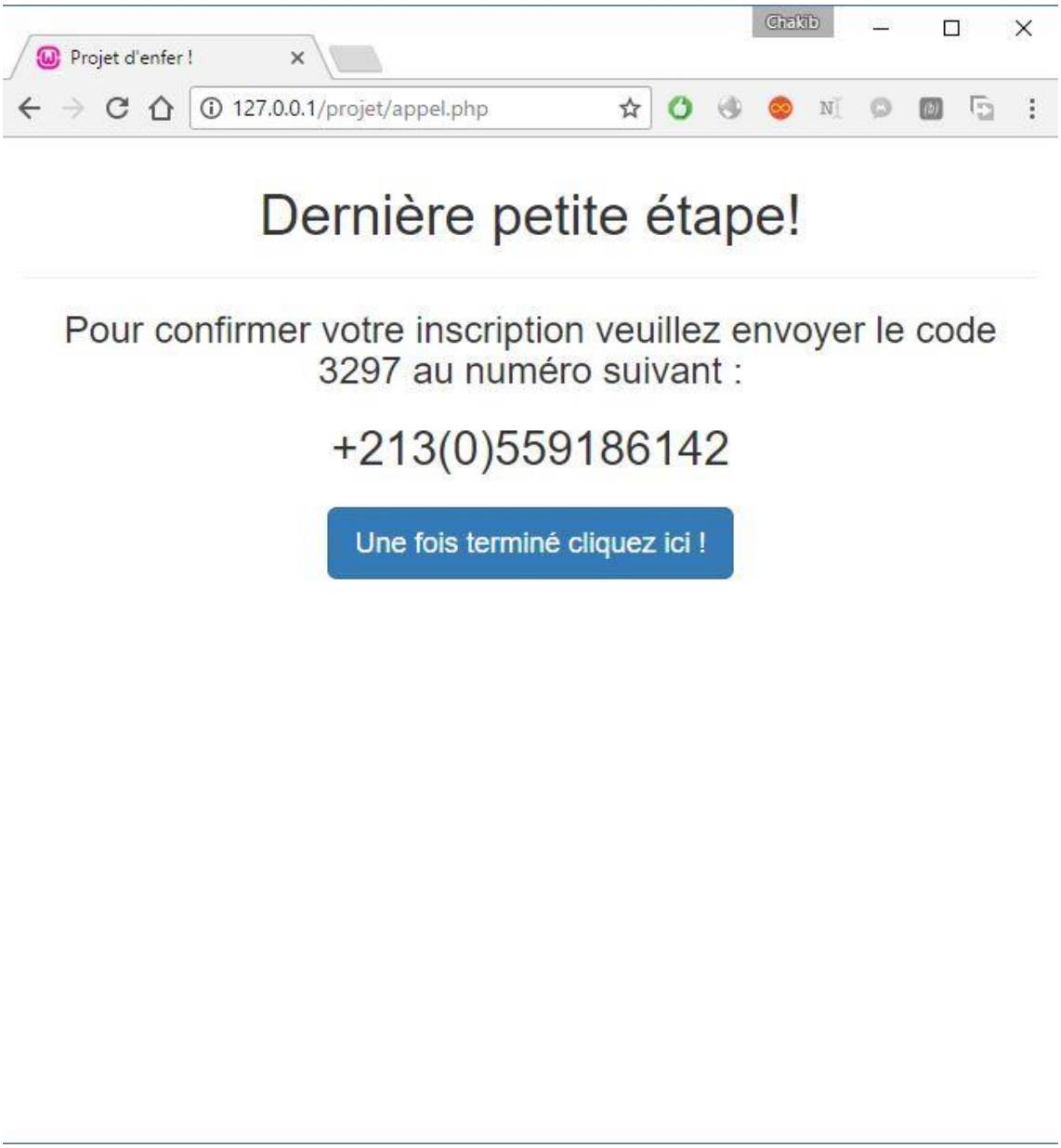


Figure 26 : appel.php

L'utilisateur doit maintenant envoyer le code suivant par SMS au numéro également affiché, puis cliquer sur le bouton.

Après cette opération l'utilisateur est redirigé vers la page « success.php », qui, si le code n'est pas bien envoyé au numéro affiché on obtient le résultat suivant :

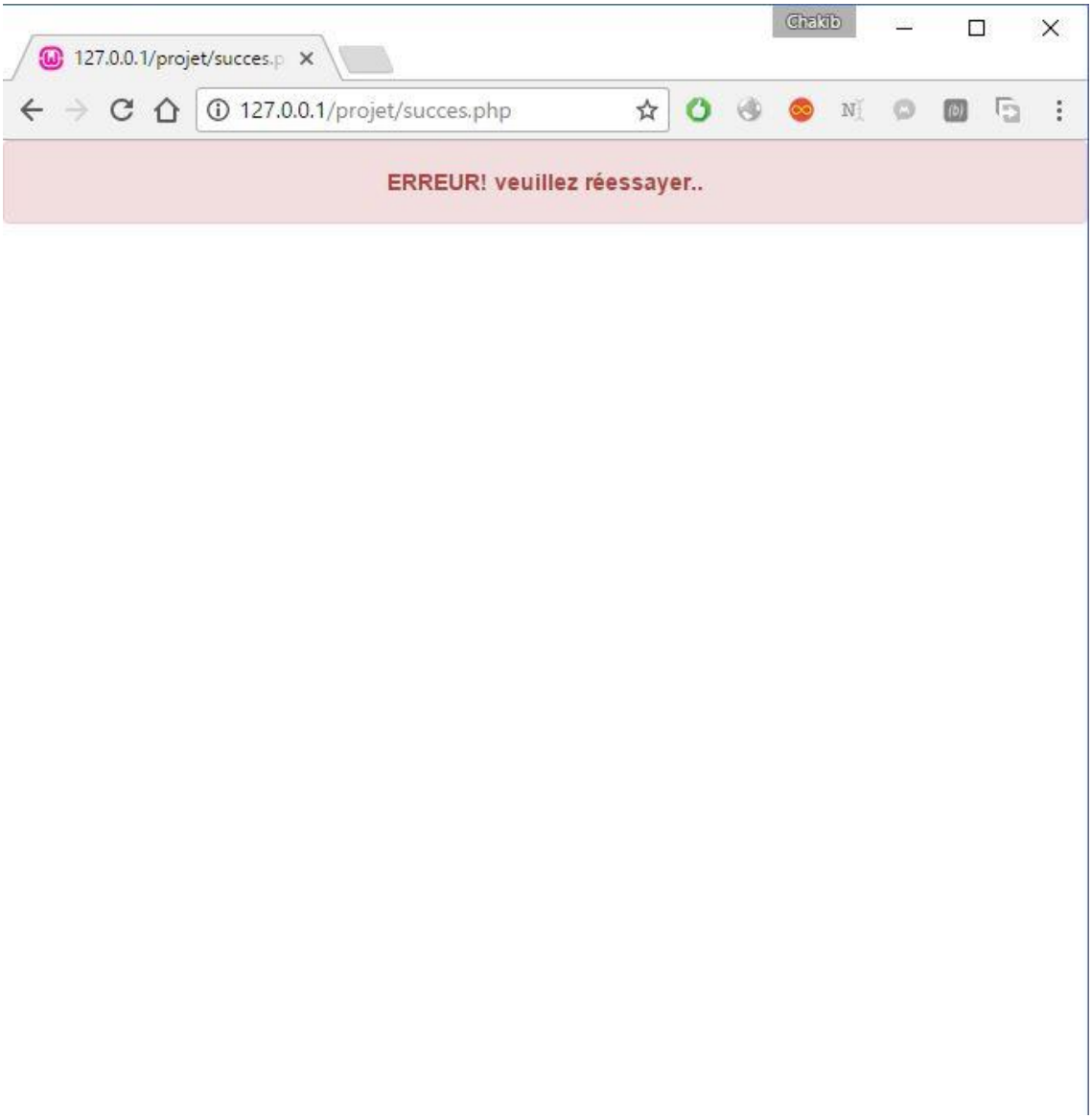


Figure 27 : success.php (erreur).

Ou bien sinon si le code est bien envoyé au numéro affiché on obtient le résultat suivant :

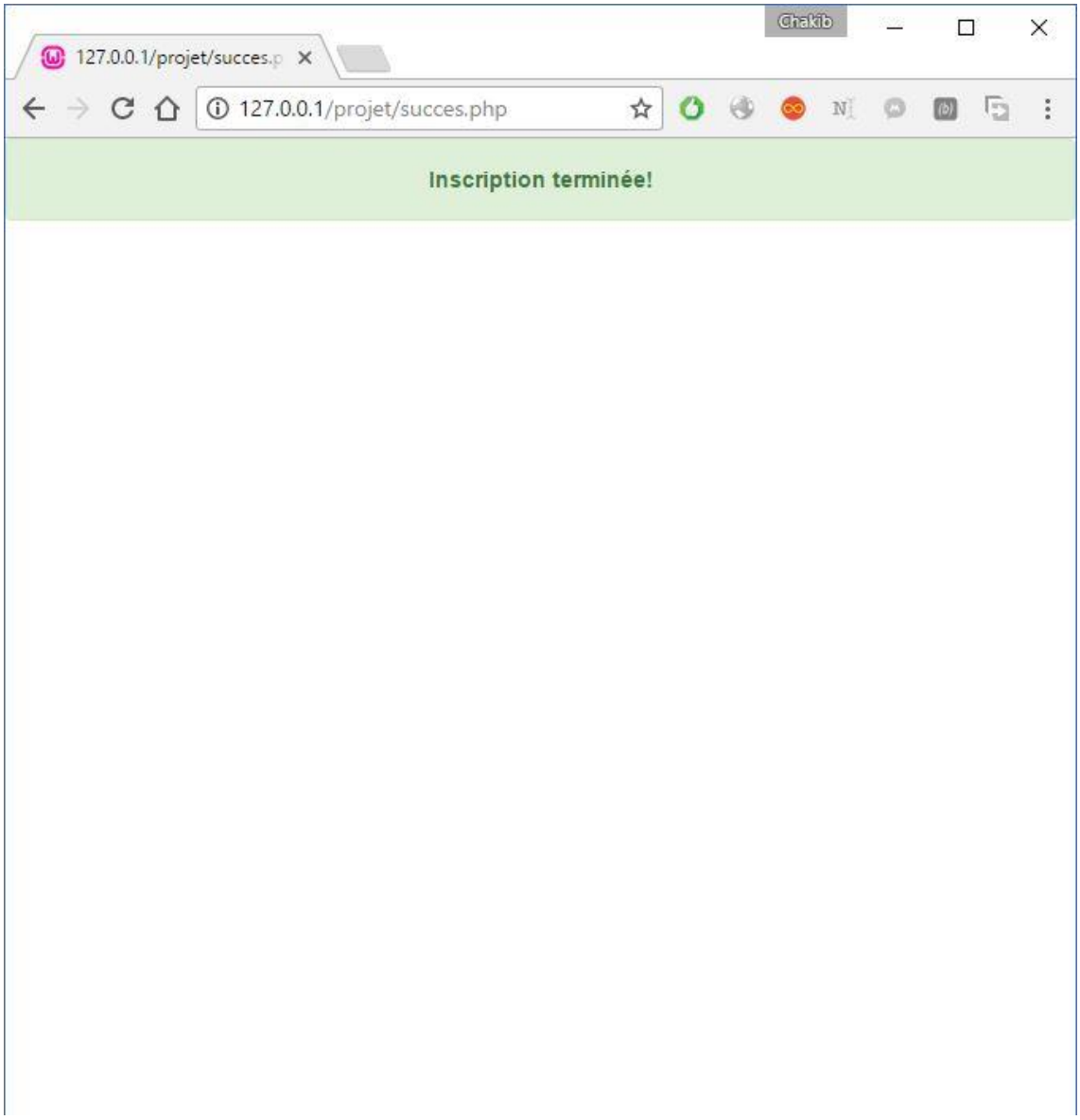


Figure 28 : success.php (réussite).

4.1 Récapitulatif

On a d'abord installé et mis en place WampServer sur le PC qui est considéré comme le serveur de ce système, s'en est suivi la mise en place de la base de données ainsi que des tables adéquates pour ce projet.

Ensuite, on a implémenté les pages web pour permettre à l'utilisateur de faire son inscription en utilisant notamment le framework CSS « bootstrap » pour personnaliser les boutons et le formulaire d'inscription entre autres.

Enfin on a mis en place le gateway SMS sur le Raspberry, puis configuré le daemon pour qu'il puisse être actif en continue et toujours en attente de nouveaux SMS pour qu'il les envoie à la base de données du serveur.

Conclusion générale

L’objectif du projet était d'étudier et de mettre en œuvre la méthode d'authentification forte et ses avantages par rapport au système d'authentification simple. La première étape a été l'analyse où on a étudié les systèmes d'authentification traditionnels et comment les mots de passe sont compromis dans de tels systèmes et ce qui peut être fait pour nier les facteurs qui les composent. Ceci a été suivi par l'étude des limites des systèmes d'authentification mobile à deux facteurs. Une fois que les éléments ci-dessus ont été achevés, l'accent a été mis sur la mise en œuvre de la méthode d'authentification à deux facteurs.

On a aussi mis en place une application web permettant aux utilisateurs de s’inscrire avec une double authentification, ce qui rend leurs comptes plus sécurisés, et cela grâce à la mise en place d’un gateway GSM via un Raspberry et un modem GSM avec une carte SIM.

On a expérimenté beaucoup de manières de concevoir ce système, on a à mi-chemin, eu quelques petits obstacles qu’on a pu surmonter grâce à de nombreuses heures de recherches sur internet.

L’objectif du projet pour étudier et mettre en œuvre une méthode d'authentification forte a été réussi et la fonctionnalité mise en œuvre a été fonctionnelle de manière satisfaisante.

5. Perspectives

Une fois ce système finalisé, on a pu se projeter et imaginer quelques nouveaux builds, des builds axés sur deux points principaux :

5.1 La sécurité

Tout système mis en place, doit assurer une certaine sécurité vis-à-vis de ses utilisateurs pour contrer d'éventuelles attaques subies après son déploiement.

C'est pour cela qu'une mise à l'épreuve des capacités du système est prévue afin de pouvoir anticiper toute attaque DOS, ou encore, le chiffrement des données après qu'elles soient entrées par les différents utilisateurs qui interagissent avec le système.

5.2 L'aspect visuel

Comme dans chaque partie web d'un système, le côté web du système dont on dispose doit être revisité afin de pouvoir couvrir toutes les difficultés que peuvent rencontrer les utilisateurs en interagissant avec les pages web mises à disposition par le système.

5.3 Réduire le délai de traitement

Après plusieurs tests concluants, il s'avère qu'en changeant de matériel, on peut avoir un temps de réponse beaucoup plus court, et un traitement encore plus rapide, comme par exemple en remplaçant de Raspberry 3 B, par un le dernier Raspberry commercialisé (Raspberry 4), ou bien en s'équipant de modules GSM plus rapides et plus modernes.

Références bibliographiques

[1] : Raspberry Pi 3 [En ligne]. Disponible sur : https://www.elektor.fr/raspberry-pi-3-model-b

[2] : Ubuntu [En ligne]. Disponible sur : http://amaizo.info/2012/06/06/ubuntu-je-suis-parce-que-nous-sommes/9588

[3] : Protocole SSH [En ligne]. Disponible sur : https://www.lemagit.fr/definition/SSH-Secure-Shell

[4] : Gateway SMS [En ligne]. Disponible sur : https://www.techopedia.com/definition/2978/sms-gateway

[5] : Modem GSM [En ligne]. Disponible sur : https://gsm-domotique.com/tag/modem-gsm-c-quoi/

[6] : Gammu [En ligne]. Disponible sur : https://doc.ubuntu-fr.org/gammu

[7] : SMS daemon [En ligne]. Disponible sur : https://fr.wammu.eu/smsd/

[8] : WampServer [En ligne]. Disponible sur : https://www.supinfo.com/articles/single/1577-wampserver

[a] : Authentification à double facteurs [En ligne]. Disponible sur : https://storedsafe.com/assets/twofactorstoredsafe-a4.pdf

Résumé

Face à l'évolution croissante des technologies et de la naissance d'une forte dépendance à internet, nos informations personnelles deviennent de plus en plus sensibles, et la nécessité de préserver ces dernières est devenue plus qu'évidente.

Pour cela, on a mis au point un système de sécurité basé sur l'authentification à double facteur. En effet, à chaque inscription ou bien enregistrement où un utilisateur est amené à saisir un mot de passe, un code à usage unique lui est délivré, pour qu'il puisse l'envoyer à notre serveur, via le numéro de téléphone avec lequel il s'était préalablement inscrit.

Afin d'y parvenir, nous avons mis en place un côté serveur, où on trouve une base de données qui récolte comme son nom l'indique, les données qui nous proviennent des pages web générées et remplies par les différents utilisateurs, et d'un autre côté une gateway GSM, qui reçoit les SMS provenant des utilisateurs.

Abstract

Faced with the increasing evolution of technologies and the emergence of a strong dependence on the internet, our personal information is becoming more and more sensitive, and the need to preserve it has become more than obvious.

For this, we put a security system based on dual factor authentication. Indeed, each registration or registration where a user is required to enter a password, a single-use code is issued to him, so that he can send it to our server, via the phone number with which he had previously registered.

In order to achieve this, we have set up a server side, where we find a database that collects as its name indicates, the data that comes from the web pages generated and filled by the different users, and from another side a GSM gateway, which receives SMS from users.

ملخص

في مواجهة التطور المتزايد للتقنيات وظهور االعتماد القوي على االنترنت ، أصبحت معلوماتنا الشخصية أكثر حساسية ، وأصبحت الحاجة إلى الحفاظ عليها أكثر من واضحة.

لهذا الغرض ، تم تطوير نظام أمان يعتمد على مصادقة عامل مزدوج. في الواقع ، كل تسجيل يُطلب من المستخدم إدخال كلمة مرور ، يتم إصدار رمز لالستخدام مرة واحدة ، حتى يتمكن من إرسالها إلى خادمنا ، عبر رقم الهاتف الذي معه قد سجل سابقا.

ولتحقيق ذلك ، أنشأنا جانب الخادم ، حيث نجد قاعدة بيانات تجمع كما يشير اسمها ، والبيانات التي تأتي من صفحات الويب التي تم إنشاؤها وملؤها من قبل مختلف المستخدمين ، ومن جانب آخر بوابة ، والذي يتلقى الرسائل القصيرة من المستخدمين.