



Server Bonsai Store

Partecipanti

Federico Risoli 307672

Descrizione del progetto

Il sito si presenta come un e-commerce dedicato alla vendita di bonsai attraverso cui un utente registrato può comprare le piante e avere accesso ad un'area riservata in cui può visualizzare i suoi ordini. Se l'utente è l'amministratore, ha accesso a funzionalità speciali, come ad esempio, degli insight che mostrano l'andamento delle vendite, i prodotti più acquistati e altre statistiche inerenti alle vendite

Un utente non registrato invece può solamente sfogliare il catalogo, ma non acquistare.

Gli acquisti sono simulati attraverso l'inserimento, in un form, delle informazioni della carta di credito.

Il sito verrà messo in sicurezza in HTTPS attraverso un certificato auto generato

Una volta acquistato il prodotto arriverà una mail di conferma.

Obiettivi

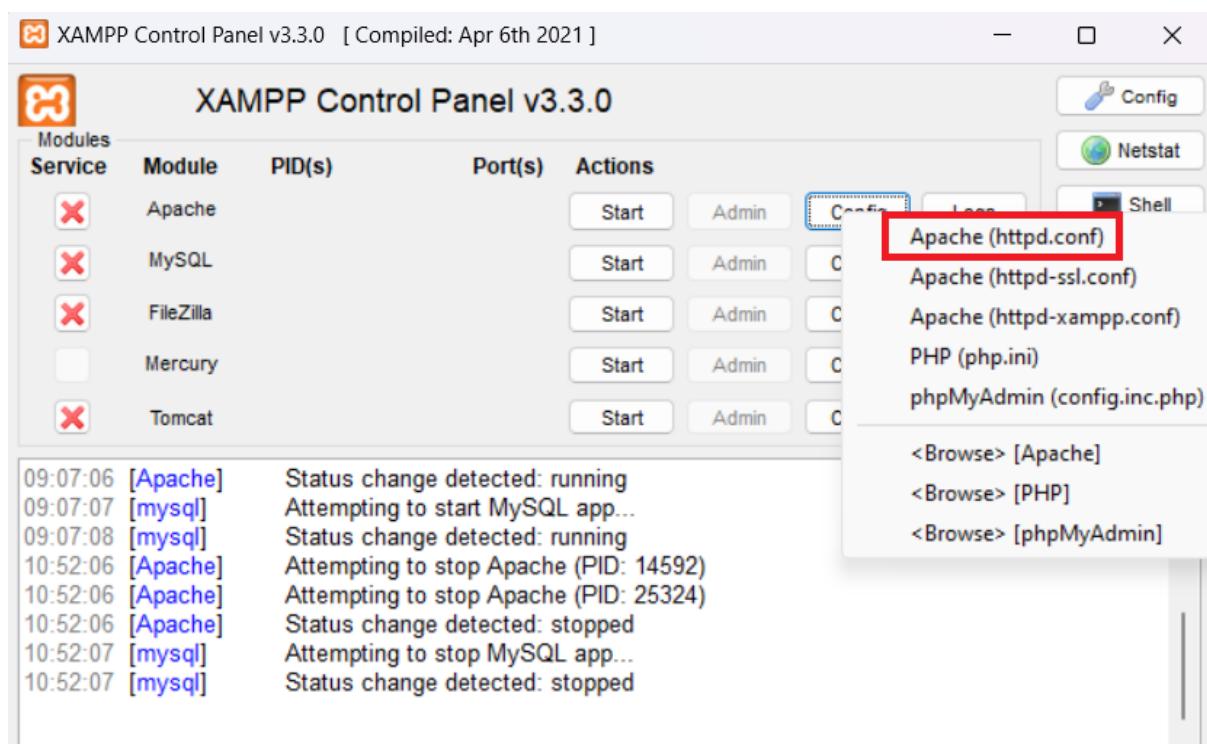
- Partendo da un sito esistente utilizzare virtual host name based
- Messa in sicurezza HTTPS attraverso certificati
- Invio mail di conferma dopo il pagamento
- Area ad accesso protetto (es. con autenticazione Basic) per qualche funzionalità particolare [Pagina insight.php riservata all'amministratore]

Configurazione

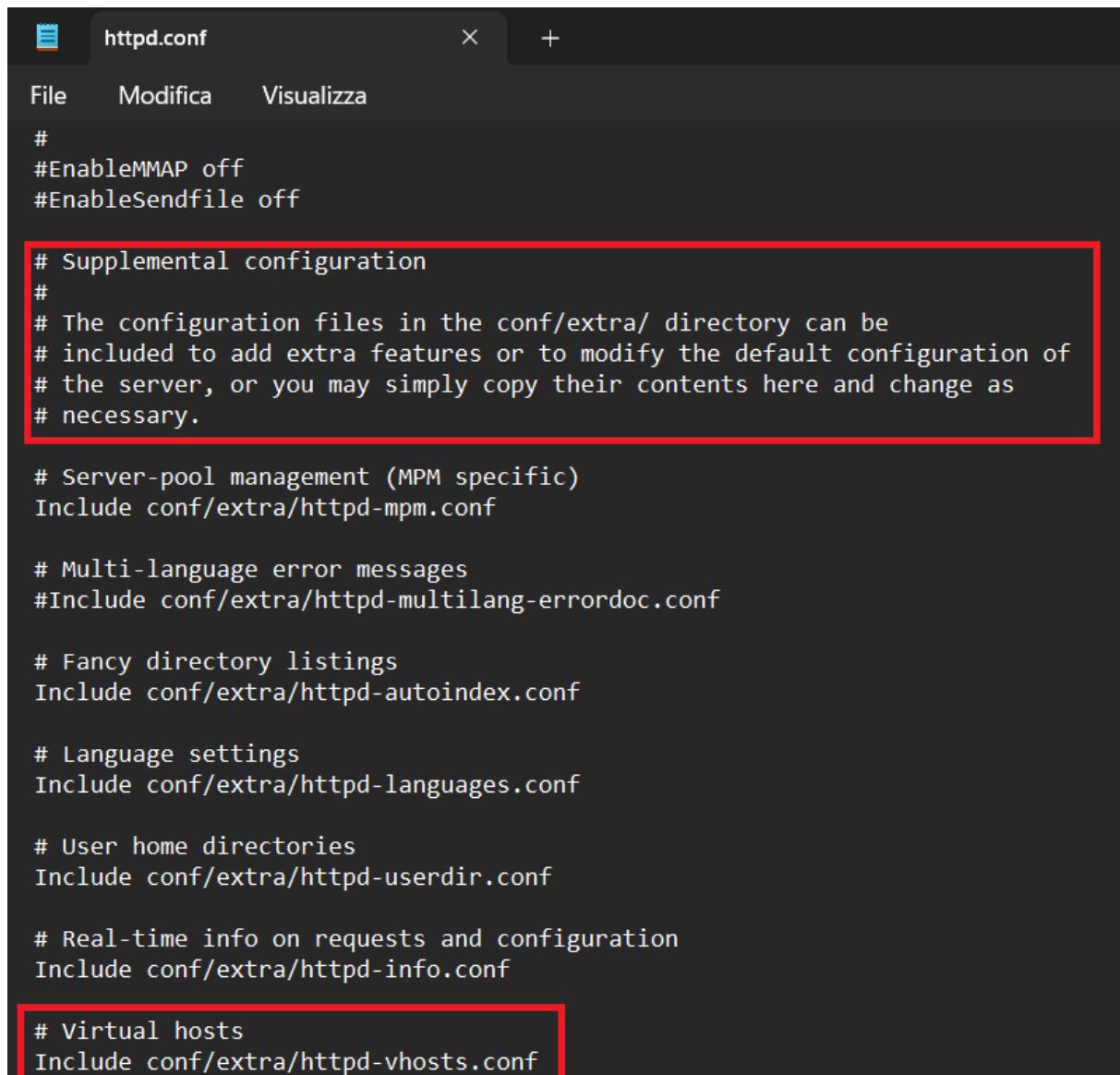
- Scaricare il sito di partenza (nel mio caso ho utilizzato il progetto del corso di "Basi di Dati e web" tenuto dal Prof. Cagnoni) al seguente link <https://github.com/FedericoRisoli/bdp>

nella repository è presente tutta la documentazione della struttura del sito e del database

- Assicurarsi il funzionamento del database e del codice php (l'ultimo commit era datato 23/3/2023)
- Modificato il file hosts al percorso C:\Windows\System32\drivers\etc inserendo 127.0.0.1 www.bonsai.com
- Aprendo il file di configurazione principale (httpd.conf) del server apache di xampp



È presente l'istruzione che reindirizza al file httpd-vhosts.conf nella cartella extra



```
# Supplemental configuration
#
# The configuration files in the conf/extra/ directory can be
# included to add extra features or to modify the default configuration of
# the server, or you may simply copy their contents here and change as
# necessary.

# Server-pool management (MPM specific)
Include conf/extra/httpd-mpm.conf

# Multi-language error messages
#Include conf/extra/httpd-multilang-errordoc.conf

# Fancy directory listings
Include conf/extra/httpd-autoindex.conf

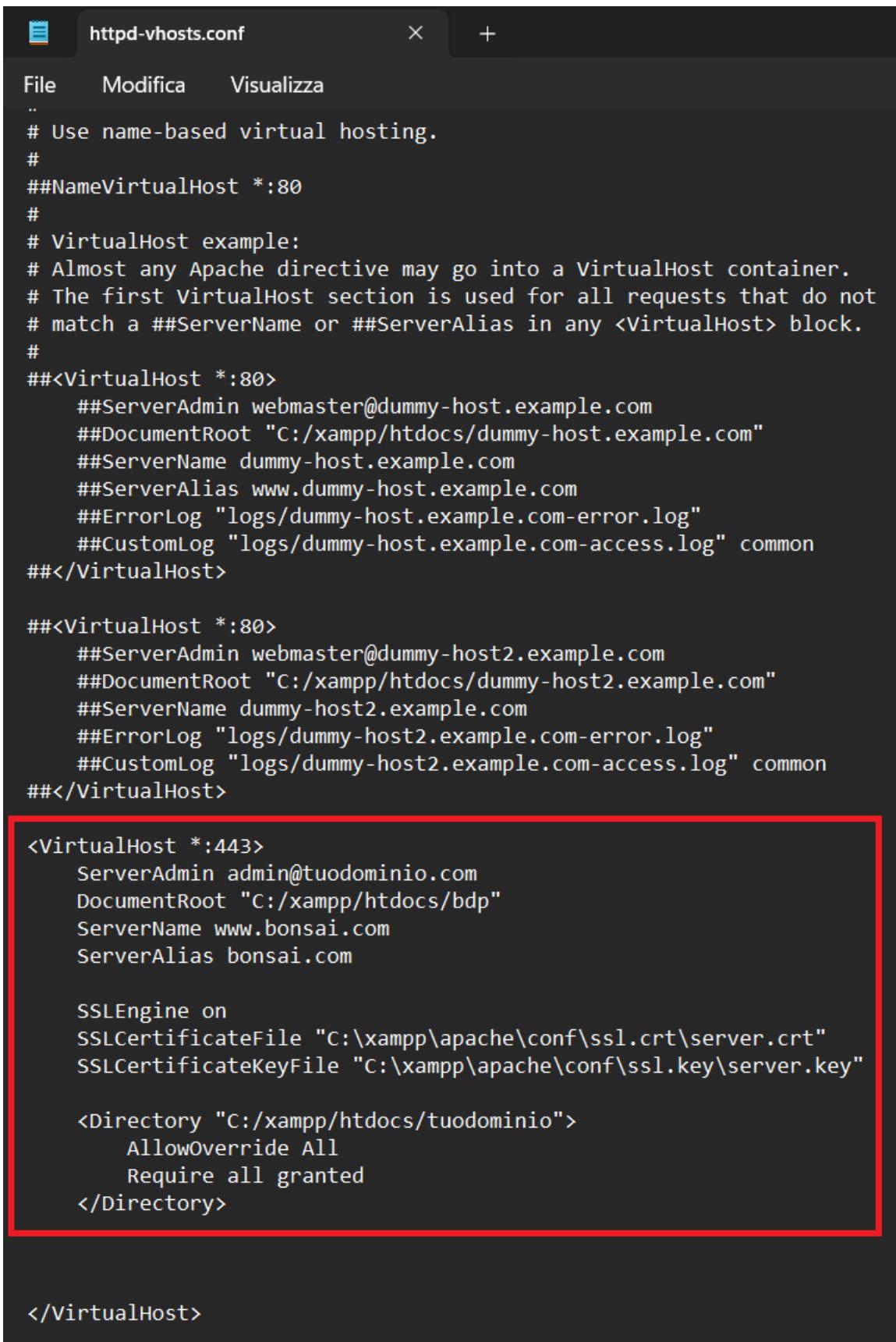
# Language settings
Include conf/extra/httpd-languages.conf

# User home directories
Include conf/extra/httpd-userdir.conf

# Real-time info on requests and configuration
Include conf/extra/httpd-info.conf

# Virtual hosts
Include conf/extra/httpd-vhosts.conf
```

Dopodichè modificato il file httpd-vhosts.conf al percorso C:\xampp\apache\conf\extra in modo da configurare il server apache con virtual host name based



```
httpd-vhosts.conf
```

```
File Modifica Visualizza .. # Use name-based virtual hosting. # ##NameVirtualHost *:80 # # VirtualHost example: # Almost any Apache directive may go into a VirtualHost container. # The first VirtualHost section is used for all requests that do not # match a ##ServerName or ##ServerAlias in any <VirtualHost> block. # ##<VirtualHost *:80> ##ServerAdmin webmaster@dummy-host.example.com ##DocumentRoot "C:/xampp/htdocs/dummy-host.example.com" ##ServerName dummy-host.example.com ##ServerAlias www.dummy-host.example.com ##ErrorLog "logs/dummy-host.example.com-error.log" ##CustomLog "logs/dummy-host.example.com-access.log" common ##</VirtualHost> ##<VirtualHost *:80> ##ServerAdmin webmaster@dummy-host2.example.com ##DocumentRoot "C:/xampp/htdocs/dummy-host2.example.com" ##ServerName dummy-host2.example.com ##ErrorLog "logs/dummy-host2.example.com-error.log" ##CustomLog "logs/dummy-host2.example.com-access.log" common ##</VirtualHost> <VirtualHost *:443> ServerAdmin admin@tuodominio.com DocumentRoot "C:/xampp/htdocs/bdp" ServerName www.bonsai.com ServerAlias bonsai.com SSLEngine on SSLCertificateFile "C:\xampp\apache\conf\ssl.crt\server.crt" SSLCertificateKeyFile "C:\xampp\apache\conf\ssl.key\server.key" <Directory "C:/xampp/htdocs/tuodominio"> AllowOverride All Require all granted </Directory> </VirtualHost>
```

rendendo il sito raggiungibile tramite il dominio www.bonsai.com in localhost attraverso http

4. Ho generato chiave e certificato della CA

- a. Ho scaricato Openssl da questo link <https://wiki.openssl.org/index.php/Binaries>
- b. Attraverso il terminale ho generato la chiave con il comando
 - i. `openssl genrsa -des3 -out chiaveCA.key 2048`
- c. Successivamente ho creato il certificato auto firmato con la chiave privata creata qua sopra con il comando
 - i. `openssl req -x509 -new -nodes -key chiaveCA.key -sha256 -days 90 -out certificatoCA.crt`

Un certificato autofirmato è un certificato firmato con la propria chiave privata. Può essere utilizzato per crittografare i dati così come i certificati firmati da una CA

- d. Ho creato poi la chiave del server con il comando
 - i. `openssl genrsa -des3 -out server.key 2048`
- e. Crea il certificato auto firmato con la chiave privata
 - i. `openssl req -key server.key -new -x509 -days 365 -out server.crt`
- f. Ora è arrivato il momento di firmare il nostro CSR con la CA
 - i. Ho creato il file server.ext che contiene il seguente testo

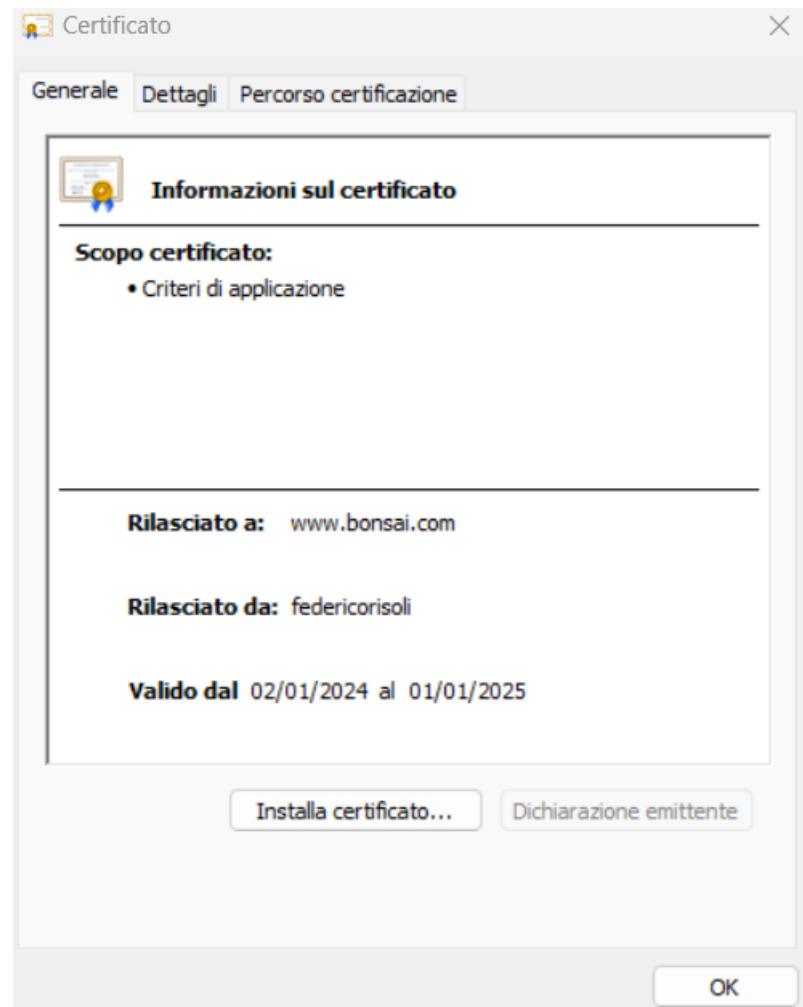

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 =
www.bonsai.com
```
- g. A questo punto si può quindi firmare il nostro CSR (server.csr) con il certificato CA e la sua chiave privata con il comando
 - i. `openssl x509 -req -CA certificatoCA.crt -CAkey chiaveCA.key -in server.csr -out server.crt -days 365
-CACreateserial -extfile server.ext`

Ho dovuto utilizzare il comando `openssl rsa -in server.key -out server-no-pass.key` per togliere la password dalle chiavi in quanto (dopo svariati tentativi) ho scoperto che windows non supporta l'immissione di password nella procedura di creazione del certificato

se tutto è andato a buon fine otterremo l'output

```
Certificate request self-signature ok ,O=bonsaienterprise, CN=www.bonsai.com
```

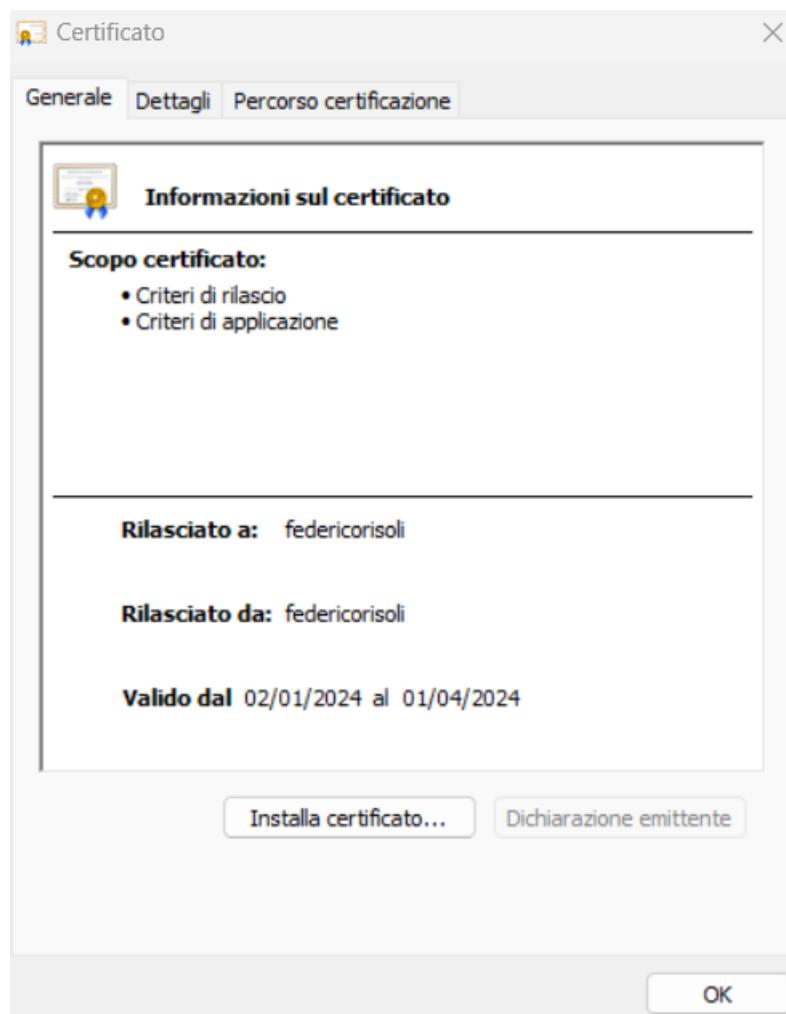
e il file server.crt



il procedimento ha creato questi file

certificatoCA.crt	02/01/2024 13:49	Certificato di sicur...	2 KB
certificatoCA.srl	02/01/2024 14:35	File SRL	1 KB
chiaveCA.key	02/01/2024 13:43	File KEY	2 KB
server.crt	02/01/2024 14:35	Certificato di sicur...	2 KB
server.csr	02/01/2024 14:35	File CSR	2 KB
server.ext	02/01/2024 14:33	File EXT	1 KB
server.key	02/01/2024 14:38	File KEY	2 KB

mentre il file certificatoCA.crt contiene



Ora bisogna inserire la CA appena creata nelle autorità di certificazione radice attendibile
Attraverso **Microsoft Management Console**

Console1 - [Radice console\Certificati (computer locale)\Autorità di certificazione radice attendibili\Certificati]

File Azione Visualizza Preferiti Finestra ?

Radice console

- > Certificati - Utente corrente
- > Certificati (computer locale)
 - Personale
 - Autorità di certificazione radice
 - Certificati
 - Attendibilità per l'organizzazione
 - Autorità di certificazione intermedia
 - Autori attendibili
 - Certificati non disponibili nell'elenco
 - Autorità di certificazione radice di confidenzialità
 - Persone attendibili
 - Emissenti per autenticazione digitale
 - Radici versione di anteprima
 - Radici di prova
 - AAD Token Issuer
 - eSIM Certification Authorities
 - ISG Trust
 - Autorità di certificazione OEM elettronica
 - Radici attendibili Passpoint
 - Desktop remoto
 - Richieste di registrazione dei certificati
 - Radici attendibili smart card
 - Autorità di installazione app in piattaforma
 - Dispositivi attendibili
 - Windows Live ID Token Issuer
 - WindowsServerUpdateServices

Rilasciato a Emesso da Data scadenza Scopi designati

Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Autenticazione d...
Certum CA	Certum CA	11/06/2027	Autenticazione d...
Certum Trusted Network CA	Certum Trusted Network CA	31/12/2029	Autenticazione d...
Certum Trusted Network CA 2	Certum Trusted Network CA 2	06/10/2046	Autenticazione d...
Class 3 Public Primary Certificate...	Class 3 Public Primary Certification Authority	02/08/2028	Autenticazione d...
COMODO RSA Certification Authority	COMODO RSA Certification Authority	19/01/2038	<Tutti>
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Timestamp
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10/11/2031	Autenticazione d...
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	15/01/2046	Firma codice, Tim...
DigiCert Global Root CA	DigiCert Global Root CA	10/11/2031	Autenticazione d...
DigiCert Global Root G2	DigiCert Global Root G2	15/01/2038	Autenticazione d...
DigiCert Global Root G3	DigiCert Global Root G3	15/01/2038	Autenticazione d...
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	10/11/2031	Autenticazione d...
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15/01/2038	Autenticazione d...
DST Root CA X3	DST Root CA X3	30/09/2021	Autenticazione d...
Entrust Root Certification Authority	Entrust Root Certification Authority	27/11/2026	Autenticazione d...
Entrust Root Certification Authority	Entrust Root Certification Authority	07/12/2030	Autenticazione d...
federicorisoli	federicorisoli	01/04/2024	<Tutti>
GlobalSign	GlobalSign	18/03/2029	Autenticazione d...
GlobalSign	GlobalSign	10/12/2034	Autenticazione d...
GlobalSign Code Signing Root R...	GlobalSign Code Signing Root R45	18/03/2045	Firma codice
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Autenticazione d...
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	29/06/2034	Autenticazione d...
Go Daddy Root Certificate Authority	Go Daddy Root Certificate Authority	01/01/2038	Autenticazione d...
GTS Root R4	GTS Root R4	22/06/2036	Autenticazione d...
ISRG Root X1	ISRG Root X1	04/06/2035	Autenticazione d...

Azioni

- Certificati
- Altre azioni

L'archivio Autorità di certificazione radice attendibili contiene 58 certificati.

a questo punto il sito si presenta in questo modo

Guarda 'Lezioni di Bonsai'

bonsai.com

La connessione è sicura

Cookie e dati dei siti

Impostazioni sito

www.bonsai.com/index.php

Ficus Bonsai PROMO -10% 22.5 \$

Olivio Bonsai PROMO -10% 31.5 \$

Olmo Bonsai 15 \$

Quercia Bonsai 120 \$

Accedi Registrati

Visualizzazione del certificato: www.bonsai.com

Generali Dettagli

Rilasciato a

Nome comune (CN)	www.bonsai.com
Organizzazione (O)	bonsaienterprise
Unità organizzativa (OU)	<Non incluso nel certificato>

Emesso da

Nome comune (CN)	federicorisoli
Organizzazione (O)	fede
Unità organizzativa (OU)	<Non incluso nel certificato>

Periodo di validità

Emesso in data	martedì 2 gennaio 2024 alle ore 14:35:32
Scade in data	mercoledì 1 gennaio 2025 alle ore 14:35:32

Impronte SHA-256

Certificato	c813a1db15301c5902284f20655e3a35bd738c3b80f1da5ba0db223c88f892df
Chiave pubblica	ef9389d3157188c5db0f9ab04c288f559bd68f0bea9b57fae185611dfe7eac5b

Mail di conferma

1. Ho creato un account google chiamato **progettiuniversita9@gmail.com** da utilizzare come mailer
2. Nelle impostazioni dell' account Google ho attivato l'autenticazione a due fattori
3. In questo modo si "sblocca" l'opzione password per le app e ne ho creata una in modo da poterla utilizzare con PHPmailer
4. Ho scaricato e installato Composer dal seguente link <https://getcomposer.org/download/>
5. In alternativa può essere scaricato da Github PHPmailer al seguente link <https://github.com/PHPMailer/PHPMailer/tree/master>
6. e installato attraverso il comando `composer require phpmailer/phpmailer`
7. Ho successivamente modificato il database in quanto non era presente il campo mail negli utenti

The screenshot shows the phpMyAdmin interface for the 'bonsaistore' database. The 'utenti' table is selected. The 'mail' column for rows a, b, and c is highlighted with a red box. The table data is as follows:

	username	password	nome	cognome	datanascita	indirizzo	mail
a	a	a	a	a	2003-04-10	a	a@mail.com
b	b	b	b	b	2003-04-01	b	fede8906@gmail.com
c	123456	c	c	ciao	2005-01-01	c	federico.risoli@studenti.unipr.it

Ho modificato le pagine php di conseguenza e attraverso il form di pagamento nella pagina **pagamento.php** tramite un action passo le informazioni alla pagina che processa il pagamento simulato e attraverso il seguente codice manda la mail automatica di conferma all'indirizzo di posta elettronica che l'utente aveva inserito in fase di registrazione [tramite una variabile session]

```

<?php
require 'vendor/autoload.php';
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\SMTP;
use PHPMailer\PHPMailer\Exception;
require 'C:\xampp\htdocs\bdp\vendor\phpmailer\phpmailer\src\Exception.php';
require 'C:\xampp\htdocs\bdp\vendor\phpmailer\phpmailer\src\PHPMailer.php';
require 'C:\xampp\htdocs\bdp\vendor\phpmailer\phpmailer\src\SMTP.php';

//altro codice

else if($operation=="comprato"){
    //id usr idprod, data
    $name= $_SESSION["usr"];
    $data = date("Y-m-d");
    $prodotto = $_SESSION['idprod'];
    $prezzo = $_POST['prezzo'];

    $compro="INSERT INTO `acquisti`(`id`, `usr`, `idprod`, `data`, `prezzo`)
    //eseguo la query
    // Prepara i dettagli dell'ordine per l'email
    $nomeProdotto=$_POST['nome']; // Recupera il nome del prodotto
    $prezzo = $_POST['prezzo']; // Recupera il prezzo del prodotto
    $mail=$_SESSION["mail"];//recupera mail utente

    //Load Composer's autoloader
    require 'vendor/autoload.php';
}

```

```

//password dell'account google oich jhsj jutv zkdb
//Create an instance; passing `true` enables exceptions
$mail = new PHPMailer(true);

try {
    //Server settings
    $mail->SMTPDebug = 0;                                         //Enable verbose de
    $mail->isSMTP();                                              //,
    $mail->Host         = 'smtp.gmail.com';                      //Se
    $mail->SMTPAuth    = true;                                     //,
    $mail->Username     = 'progettiuniversita9@gmail.com';      //
    $mail->Password     = 'oichjhsijutvzkdb';                   //
    $mail->SMTPSecure  = PHPMailer::ENCRYPTION_STARTTLS;;        //
    $mail->Port         = 587;                                     //,
    //Recipients
    $mail->setFrom('progettiuniversita9@gmail.com', 'no-reply Bonsai');
    $mail->addAddress($_SESSION["mail"]);                         //Add a recipient

    //Content
    $mail->isHTML(true);                                         //Set er
    $mail->Subject = 'Bonsai Order Confirmation!';
    $mail->Body    = "<div style='font-family: Brush Script MT, sans-serif; font-size: 16px; color: #FCA311;'><b>Conferma Ordine</b>
<h1 style='font-size: 20px; color: #FCA311;'><b>Conferma Ordine</b>
<p>Grazie per aver acquistato su Bonsai Store!</p>
<p style='color: #607466;'><b>Prodotto:</b> {$nomeProdotto}</p>
<p style='color: #607466;'><b>Prezzo:</b> €{$prezzo}</p>
<p>Il prodotto arriverà in 3 giorni lavorativi</p>
</div>";

    $mail->send();
    echo "<script>alert('La conferma dell'\\'ordine è stata inviata');";
} catch (Exception $e) {
    echo "<script>alert('L'email non è stata inviata. Errore: {$mail->ErrorInfo}');";
}
}

```

Ottenendo in questo modo la mail automatica



no-reply Bonsai Confir... 12:13 (23 minuti fa)

a me ▾

•••

Conferma Ordine

Grazie per aver acquistato su Bonsai Store!

Prodotto: Ficus Bonsai

Prezzo: €22.5

Il prodotto arriverà in 3 giorni lavorativi

Protezione pagina riservata all'amministratore

1. Ho scelto la pagina Insight.php in quanto è l'unica funzionalità particolare del sito dedicata all'amministratore

```
if (!isset($_SERVER['PHP_AUTH_USER']) || !isset($_SERVER['PHP_AUTH_PW'])) {
    header('WWW-Authenticate: Basic realm="Area Protetta"');
    header('HTTP/1.0 401 Unauthorized');
    exit;
} else {
    $username = $_SERVER['PHP_AUTH_USER'];
    $password = $_SERVER['PHP_AUTH_PW'];

    if ($username != 'admin' || $password != 'admin') {
        header("Location: logged.php?auth=failed");
        exit;
    }
}
```

Attraverso questo codice

- Controllo se le credenziali dell'utente (`PHP_AUTH_USER` e `PHP_AUTH_PW`) sono state impostate.

(Queste sono le credenziali inviate dall'utente attraverso l'autenticazione HTTP Basic.)

- Se le credenziali non sono impostate, il server invia un `WWW-Authenticate` che fa apparire una finestra di autenticazione nel browser dell'utente. Dopodiché, manda un header di stato `401 Unauthorized`
- Successivamente verifica le credenziali, se sono corrette allora l'amministratore avrà accesso alla pagina altrimenti verrà reindirizzato tramite una funzione alla pagina precedente senza più il permesso di accedere alla pagina protetta (le credenziali vengono richieste se si esce e rientra nel browser o se si cancellano i dati di navigazione)