مرکز صدور گواهی الکترونیکی پارس‌ساین

راهنمای نصب گواهی الکترونیکی SSL در Plesk

تدوین‌کننده: شرکت امن‌افزار گستر شریف

شماره سند.....SSW_UG_PKI_91174_1

تاریخ ۲۷/آذر/۱۳۹۱

نگارش ۱.۲

آدرس: تهران، خیابان آزادی، خیابان حبیب‌الله، خیابان قاسمی غربی، شماره ۳۷، طبقه پنجم

تلفن: ۲۰-۶۱۹۷۵۵۰۰ (۰۲۱) فاکس: ۶۶۰۹۰۲۹۹ (۰۲۱) **سایت اینترنتی**: www.parssignca.ir

حق طبع و نشر

فهرست مطالب

۱ مقدمه ۱

۲ فرضیات این سند ۲

۳ ایجاد درخواست امضای گواهی (CSR) و کلید خصوصی ۲

۴ پیکربندی پنل مدیریتی Plesk به منظور استفاده از گواهی SSL ۳

۴-۱ بررسی اختصاصی بودن آدرس IP وب‌سایت ۴

۴-۲ نصب کلید خصوصی، گواهی SSL، و زنجیره گواهی ۶

۵ بررسی صحت نصب گواهی SSL ۱۷

۶ مشکلات احتمالی پس از نصب گواهی ۱۸

۶-۱ عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وب‌سایت ۱۸

۶-۲ نمایش صفحه هشدار SSL در مرورگر ۲۰

۶-۳ نمایش صفحه دیگری به جای صفحه سایت ۲۲

۶-۴ نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر ۲۳

۷ پیوست ۲۴

۷-۱ رویه اختصاصی کردن آدرس IP وب‌سایت در Plesk ۲۴

۷-۲ نحوه بررسی pem بودن فرمت فایل کلید و تبدیل آن به فرمت PEM و حذف گذرواژه آن ۲۹

۷-۳ نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM ۳۱

۱ مقدمه

تأمین امنیت ارتباطات و تبادلات الکترونیکی در شبکه‌ها خصوصاً محیط اینترنت از جمله مسائل ویژه‌ای است که امروزه سازمان‌ها با آن مواجه هستند. به دلیل حساسیت امنیتی حجم قابل توجهی از این تبادلات در محیط وب، باید تدابیر امنیتی لازم در پروتکل‌ها و سرویس‌های مورد استفاده در این نوع ارتباطات اتخاذ گردد. پروتکل HTTP (که عموماً به عنوان پروتکل وب شناخته می‌شود) یکی از این پروتکل‌ها است که استفاده گسترده‌ای دارد. داده‌های HTTP به صورت ناامن روی شبکه منتقل می‌شوند؛ از این‌رو، داده‌هایی که بین سرویس‌دهنده[1] (سمت وب‌سایت) و سرویس‌گیرنده[2] (سمت کاربر وب‌سایت) مبادله می‌شود، توسط مهاجمین قابل مشاهده و حتی قابل تغییر هستند.

وب‌سایت‌هایی که اطلاعات مهم و محرمانه (مانند گذرواژه، شماره کارت اعتباری، اطلاعات بانکی، و دیگر اطلاعات خصوصی) با کاربران مبادله می‌کنند، نباید از پروتکل ناامن HTTP استفاده نمایند. نسخه امن‌شده این پروتکل به نام HTTPS، پرکاربردترین پروتکل امنیتی مبتنی بر رمزنگاری کلید عمومی است که در پیاده‌سازی این گونه وب‌سایت‌ها به کار می‌رود. این پروتکل مبتنی بر پروتکل SSL می‌باشد.

لازم به ذکر است، تأمین محرمانگی و عدم تغییر (جامعیت) اطلاعات تبادل‌شده بین کاربر و وب‌سایت تنها کاربرد HTTPS نیست. HTTPS برای جلوگیری از حملاتی مانند حمله فیشینگ مبتنی بر جعل سایت نیز استفاده می‌شود. در حمله مذکور، حمله‌کننده (مثلاً یک رقیب تجاری) با ایجاد یک وب‌سایت با ظاهری کاملاً مشابه سایت اصلی، کاربران آن سایت را به سایت جعلی هدایت کرده و امنیت آن‌ها را به مخاطره می‌اندازد؛ مثلاً اطلاعات کاربران را به سرقت برده یا در مورد آن‌ها اطلاعات جمع‌آوری می‌کند. در صورتی که از گواهی HTTPS استفاده شود، از این حمله جلوگیری می‌شود.

در پیکربندی وب‌سرور برای استفاده از HTTPS، از یک گواهی الکترونیکی SSL استفاده می‌شود. این گواهی باید توسط یک مرکز صدور گواهی الکترونیکی معتبر (مانند مرکز صدور گواهی الکترونیکی پارس‌ساین) صادر شده باشد تا کاربران بتوانند به آن اعتماد کرده و اطلاعات محرمانه خود را بر اساس این اعتماد، برای وب‌سایت ارسال نمایند.

---

[1] Server
[2] Client

در این سند، کلیه مراحل پیکربندی پنل مدیریتی Plesk 11 به منظور استفاده از گواهی الکترونیکی SSL در یک وب‌سایت توضیح داده شده است. لازم به ذکر است که نصب گواهی SSL در نسخه‌های قبلی Plesk نیز تقریباً مشابه رویه گفته شده در این سند می‌باشد.

۲ فرضیات این سند

در این سند، نحوه استفاده از گواهی الکترونیکی SSL ، بر اساس سناریوی فرضی زیر در نظر گرفته شده است:

«فرض می‌کنیم وب‌سایتی به آدرس www.mydomain.com و آدرس IP اختصاصی "۱۹۲.۱۶۸.۲۰۰.۱"، توسط نرم‌افزار Plesk مدیریت می‌شود. برای این وب‌سایت می‌خواهیم از مرکز صدور گواهی الکترونیکی پارس‌ساین، گواهی SSL درخواست نماییم. سپس، با استفاده از پنل Plesk گواهی صادرشده را به وب‌سایت تخصیص دهیم (آن را نصب نماییم)».

به منظور استفاده از این سند در سناریوی واقعی، باید به موارد زیر دقت نمایید:

- به جای آدرس www.mydomain.com، باید آدرس دقیق دامنه‌ای (وب‌سایتی) را وارد نمایید که برای آن گواهی SSL دریافت نموده‌اید.
- به جای آدرس IP فرضی "۱۹۲.۱۶۸.۲۰۰.۱"، آدرس IP واقعی وب‌سایت خود را قرار دهید.

۳ ایجاد درخواست امضای گواهی (CSR) و کلید خصوصی

برای دریافت گواهی الکترونیکی از مرکز صدور گواهی الکترونیکی پارس‌ساین، ابتدا باید یک درخواست امضای گواهی[1] (CSR) ایجاد نماییم. لازم به ذکر است که فیلدهای CSR باید طبق سیاست‌های مرکز صدور گواهی الکترونیکی پارس‌ساین تکمیل گردد. در غیر این صورت، مرکز صدور گواهی الکترونیکی پارس‌ساین برای آن CSR، گواهی الکترونیکی صادر نخواهد کرد.

با توجه به عدم تطابق فرایند ایجاد CSR در پنل مدیریتی Plesk با سیاست‌های زیرساخت کلید عمومی کشور و مرکز پارس‌ساین، توصیه می‌شود برای ایجاد CSR از نرم‌افزار ParsKey Utility استفاده نمایید.

[1] Certificate Signing Request (CSR)

برای دریافت این نرم‌افزار به بخش دانلود سایت مرکز پارس‌ساین به آدرس www.parssignca.ir مراجعه کنید. همچنین، برای دریافت سند "راهنمای ایجاد CSR با استفاده از نرم‌افزار Parskey Utility" به بخش راهنماها از سایت مراجعه نمایید. نحوه ایجاد CSR برای گواهی SSL، در بخش "پروفایل گواهی SSL" از سند مذکور تشریح شده است.

پس از ایجاد CSR و کلید خصوصی، فایل CSR باید به مرکز صدور گواهی الکترونیکی پارس‌ساین ارائه شود تا این مرکز گواهی SSL متناظر با فایل CSR را صادر نماید. دقت کنید برای صدور گواهی توسط مرکز صدور گواهی الکترونیکی پارس‌ساین، تنها به فایل CSR نیاز می‌باشد و نباید فایل کلید خصوصی به این مرکز ارائه شود.

نکته مهم: سرور از فایل کلید خصوصی برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌نماید. از این‌رو، در محافظت از این فایل دقت نمایید. در صورتی که این کلید در دسترس افراد غیرمجاز قرار گیرد، کلیه داده‌های رمزشده بین وب‌سایت و کاربران می‌تواند توسط این افراد رمزگشایی شود.

نکته مهم: بین CSR، کلید خصوصی (این کلید هنگام ایجاد CSR تولید می‌شود)، و گواهی الکترونیکی یک تناظر وجود دارد. از این‌رو، هر گواهی فقط با کلید خصوصی متناظر آن قابل استفاده است. چنانچه هنگام نصب گواهی روی سرور، فایل کلید خصوصی متناظر آن گواهی وجود نداشته باشد، گواهی روی سرور قابل نصب نخواهد بود.

۴ پیکربندی پنل مدیریتی Plesk به منظور استفاده از گواهی SSL

برای استفاده از گواهی الکترونیکی SSL در Plesk، باید مراحل زیر را انجام دهیم:

- بررسی اختصاصی بودن[1] آدرس IP وب‌سایت؛
- نصب کلید خصوصی، گواهی SSL و گواهی‌های مراکز صدور گواهی.

[1] Dedicated

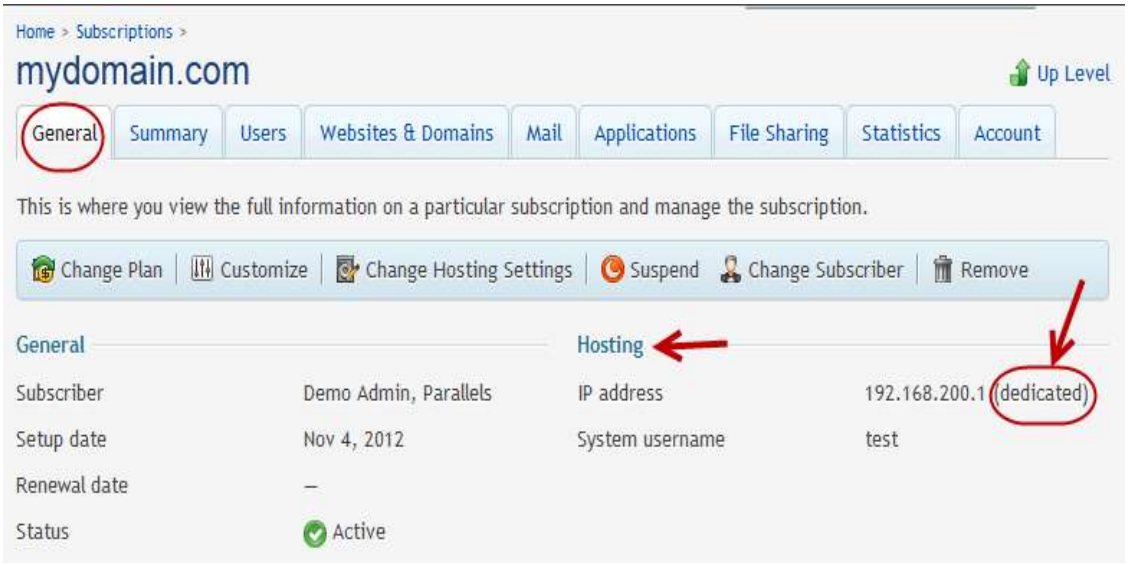
۱-۴ بررسی اختصاصی بودن آدرس IP وب‌سایت

قبل از نصب گواهی، باید از اختصاصی بودن آدرس IP وب‌سایت اطمینان حاصل نمایید. نحوه انجام این کار به صورت زیر می‌باشد:

۱. ابتدا به پنل مدیریتی Plesk خود Login می‌نماییم. از منوی سمت چپ، از بخش Hosting Services گزینه Domains را انتخاب می‌نماییم (شکل زیر).

۲. در لیست نام وب‌سایت‌های موجود، روی نام وب‌سایتی که قرار است گواهی SSL برای آن نصب شود، کلیک می‌نماییم (شکل زیر).

۳. در منوی بالای صفحه، از بخش General در قسمت Hosting، آدرس IP وب‌سایت را در مقابل IP address مشاهده می‌کنیم. اگر کنار آدرس IP وب‌سایت، عبارت dedicated درج شده باشد (مانند شکل زیر)، آنگاه آدرس IP وب‌سایت اختصاصی خواهد بود. در غیر این صورت، آدرس IP وب‌سایت از نوع اشتراکی (shared) است. در صورتی‌که آدرس IP وب‌سایت اشتراکی باشد، پیش از نصب گواهی SSL در وب‌سایت، باید با مدیر سرور (هاستینگ) خود تماس حاصل نموده و یک آدرس IP اختصاصی برای وب‌سایت خود درخواست نمایید. پس از دریافت IP اختصاصی، تنظیمات مربوط به اختصاصی کردن آدرس IP در وب‌سایت را طبق بخش ۷-۱ از پیوست انجام می‌دهیم.



۲-۴ نصب کلید خصوصی، گواهی SSL، و زنجیره گواهی

پس از اطمینان از اختصاصی بودن آدرس IP، برای استفاده از گواهی SSL در وب‌سایت، باید کلید خصوصی، گواهی SSL، و زنجیره گواهی (بسته گواهی‌های مراکز صدورگواهی) در فرمت PEM را در Plesk نصب نماییم. فایل زنجیره گواهی "بسته (bundle) گواهی‌های مراکز صدور گواهی در فرمت PEM" را باید از بخش مخزن در سایت مرکز پارس‌ساین به آدرس www.parssignca.ir دریافت نمایید.

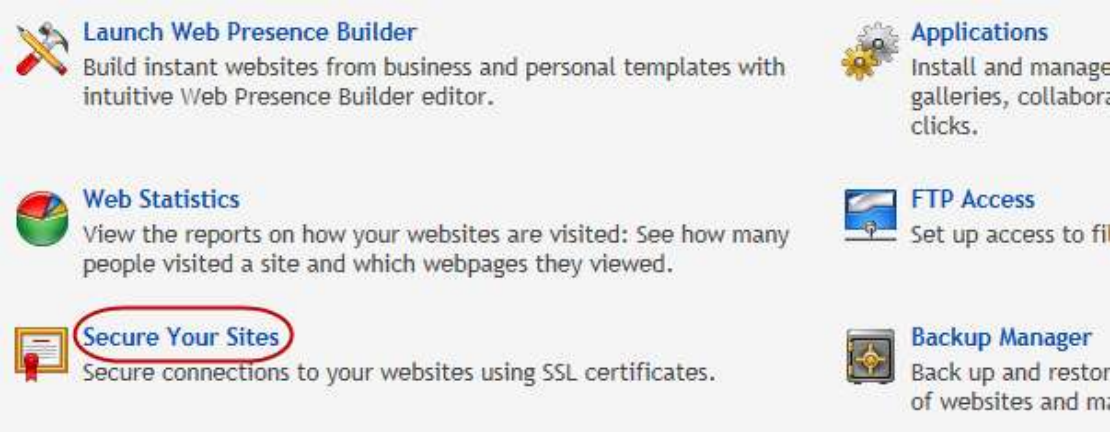
رویه نصب به صورت زیر می‌باشد:

۱. ابتدا به پنل مدیریتی Plesk خود Login می‌نماییم. از منوی سمت چپ، از بخش Hosting Services گزینه Domains را انتخاب می‌کنیم (شکل زیر).

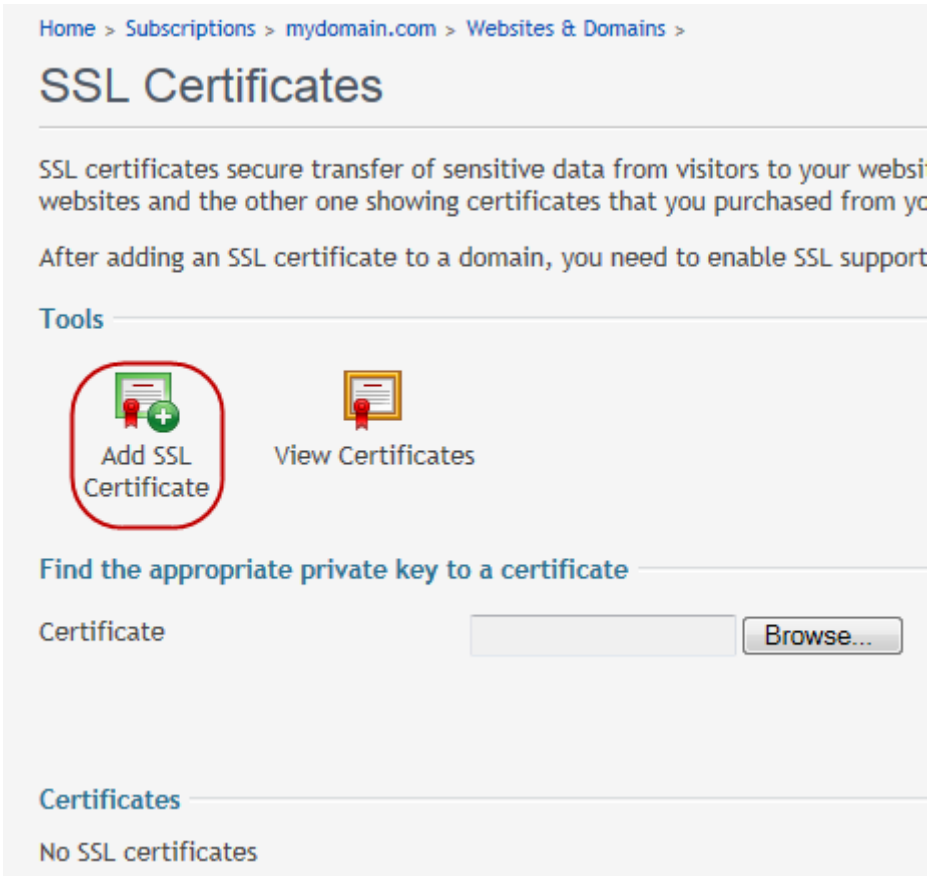
۲. در لیست نام وب‌سایت‌های موجود، روی نام وب‌سایتی که قرار است گواهی SSL برای آن نصب شود، کلیک می‌نماییم (شکل زیر).

۳. در منوی بالای صفحه، گزینه Websites & Domains را انتخاب می‌نماییم (شکل زیر).

۴. روی گزینه Secure Your Sites کلیک می‌نماییم (شکل زیر). دقن کنید، عدم وجود چنین گزینه‌ای در لیست، نشان‌دهنده عدم تخصیص آدرس IP اختصاصی (dedicated IP address) به وب‌سایت می‌باشد. در این صورت، باید طبق بخش ۷-۱ از پیوست، یک آدرس IP اختصاصی به وب‌سایت تخصیص داده شود.



۵. در صفحه SSL Certificates، ابتدا باید گواهی SSL صادر شده برای وب‌سایت را به لیست گواهی‌ها اضافه کنیم. برای این منظور، روی گزینه Add SSL Certificate کلیک می‌نماییم (شکل زیر).



۶. در صفحه Add SSL Certificate، از بخش Certificate، یک نام دلخواه برای گواهی SSL روبروی Certificate name وارد می‌کنیم. در شکل زیر نام انتخاب شده mydomain_cert می‌باشد.

۷. حال باید کلید خصوصی و گواهی‌ها را بارگذاری نماییم. دقت کنید کلید خصوصی در زمان ایجاد CSR تولید شده است. قبل از بارگذاری فایل‌های گواهی و کلید خصوصی، باید اطمینان حاصل کنیم که این فایل‌ها در فرمت PEM می‌باشند. همچنین، در صورتی که فایل کلید خصوصی دارای گذرواژه (پسورد) می‌باشد، ابتدا باید گذرواژه آن را حذف نماییم. نحوه بررسی pem بودن فایل کلید و حذف گذرواژه آن در بخش ۷-۲ از پیوست تشریح شده است. نحوه بررسی pem بودن فایل گواهی نیز در بخش ۷-۳ از پیوست آمده است.

به دو روش می‌توان کلید خصوصی، گواهی SSL وب‌سایت، و زنجیره گواهی را نصب کرد:

- **روش اول:** بارگذاری فایل‌های گواهی و کلید خصوصی از طریق بخش Upload certificate files؛
- **روش دوم:** وارد نمودن دستی محتویات فایل‌های گواهی از طریق بخش Upload certificate as text.

با استفاده از هر یک از روش‌های بالا می‌توانیم گواهی‌ها و کلید خصوصی را نصب نماییم. در ادامه، به توضیح هر دو روش می‌پردازیم.

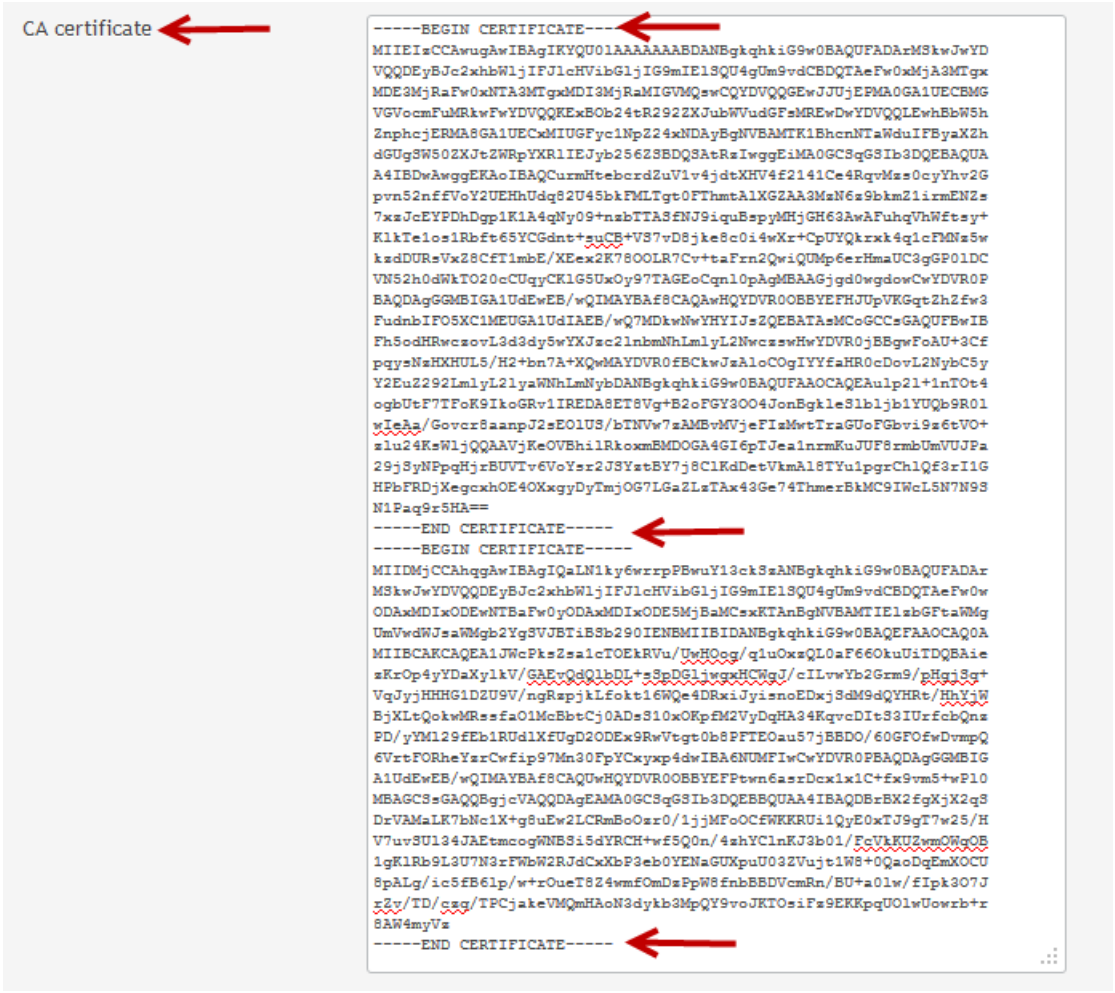
- **روش اول: بارگذاری فایل‌های گواهی و کلید خصوصی از طریق بخش Upload certificate files**:
  - توصیه می‌شود ابتدا پسوند فایل کلید را از pem. به key. تغییر دهید. برای بارگذاری کلید خصوصی، روبروی گزینه Private key، روی دکمه Browse کلیک نموده (مانند مرحله ۱ از شکل زیر) و در پنجره بازشده فایل کلید خصوصی را انتخاب می‌نماییم.
  - توصیه می‌شود ابتدا پسوند فایل گواهی را به crt. تغییر دهید. برای بارگذاری فایل گواهی SSL وب‌سایت، روبروی Certificate روی دکمه Browse کلیک نموده (مانند مرحله ۲ از شکل زیر) و فایل گواهی SSL را انتخاب می‌نماییم.
  - توصیه می‌شود ابتدا پسوند فایل زنجیره گواهی را به crt. تغییر دهید. برای بارگذاری فایل "زنجیره گواهی در فرمت PEM"، روی دکمه Browse، روبروی CA certificate کلیک نموده (مانند مرحله ۳ از شکل زیر) و در پنجره بازشده این فایل را انتخاب می‌نماییم.

در پایان، از گوشه سمت راست این بخش، روی دکمه Send File (مانند مرحله ۴ از شکل زیر کلیک) می‌کنیم.

- **روش دوم: وارد نمودن دستی محتویات فایل‌های گواهی از طریق بخش Upload certificate as text:**
  - برای وارد کردن محتوای فایل کلید خصوصی، فایل کلید را با استفاده از نرم‌افزاری مانند Wordpad باز نموده و کل محتویات فایل، از جمله عبارات -----BEGIN RSA PRIVATE KEY----- و -----END RSA PRIVATE KEY----- را کپی و آن را درون جعبه متن مشخص‌شده در پنل Paste می‌نماییم (مانند شکل زیر).

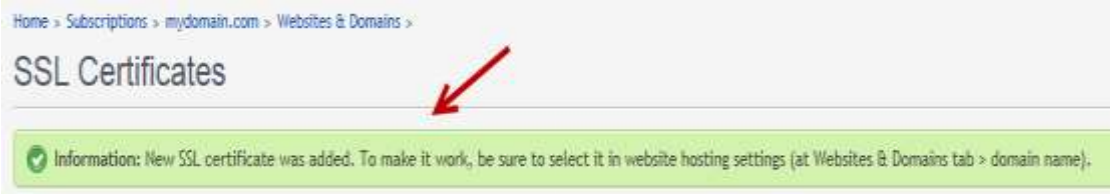
  - برای وارد نمودن فایل گواهی SSL وب‌سایت، آن را با استفاده از نرم‌افزاری مانند Wordpad باز نموده و کل محتویات فایل، از جمله عبارات -----BEGIN CERTIFICATE----- و -----END CERTIFICATE----- را کپی و آن را درون جعبه متن مشخص‌شده در پنل Paste می‌نماییم (مانند شکل زیر).

  - برای وارد نمودن فایل "زنجیره گواهی در فرمت PEM"، این فایل را با استفاده از نرم‌افزاری مانند Wordpad باز نموده و کل محتویات فایل را درون جعبه متن مشخص‌شده در پنل Paste می‌نماییم. دقت کنید باید کل محتویات فایل، از جمله عبارات -----BEGIN CERTIFICATE----- و -----END CERTIFICATE----- کپی شوند (شکل زیر).



حال از گوشه سمت راست، روی Send Text، مانند شکل زیر کلیک می‌نماییم.

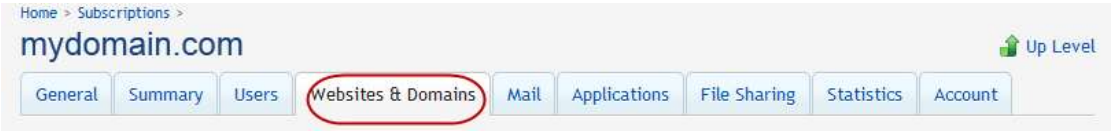
۸. پس از بارگذاری کلید خصوصی و گواهی‌ها به یکی از دو روش فوق، پیغامی به صورت شکل زیر ظاهر می‌شود که نشان‌دهنده اضافه‌شدن گواهی SSL به لیست گواهی‌های موجود می‌باشد.



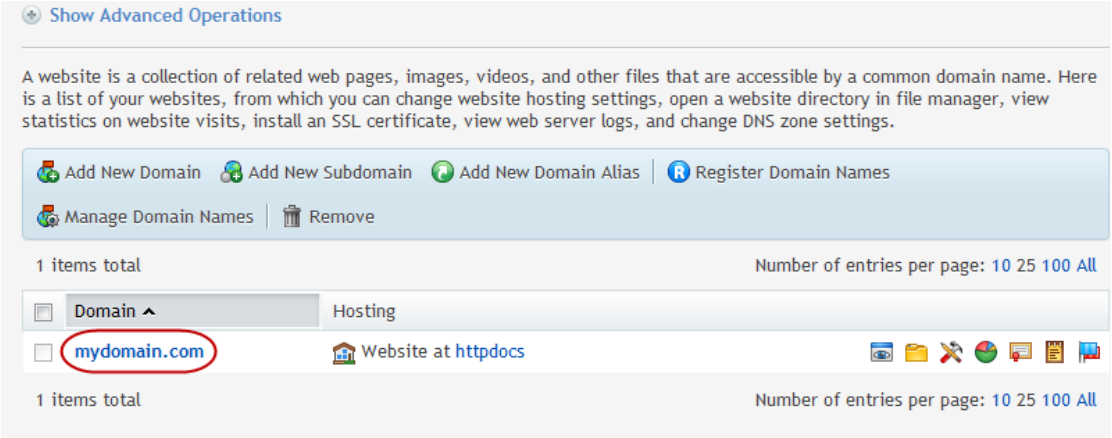
۹. در این مرحله باید گواهی SSL اضافه شده در Plesk را به وب‌سایت خود تخصیص دهیم. برای این منظور از منوی سمت چپ از بخش Hosting Services گزینه Domains را انتخاب می‌نماییم (شکل زیر).

۱۰. در لیست نام وب‌سایت‌های موجود، روی نام وب‌سایتی که قرار است گواهی SSL را برای آن نصب کنیم (mydomain.com)، کلیک می‌نماییم (شکل زیر).

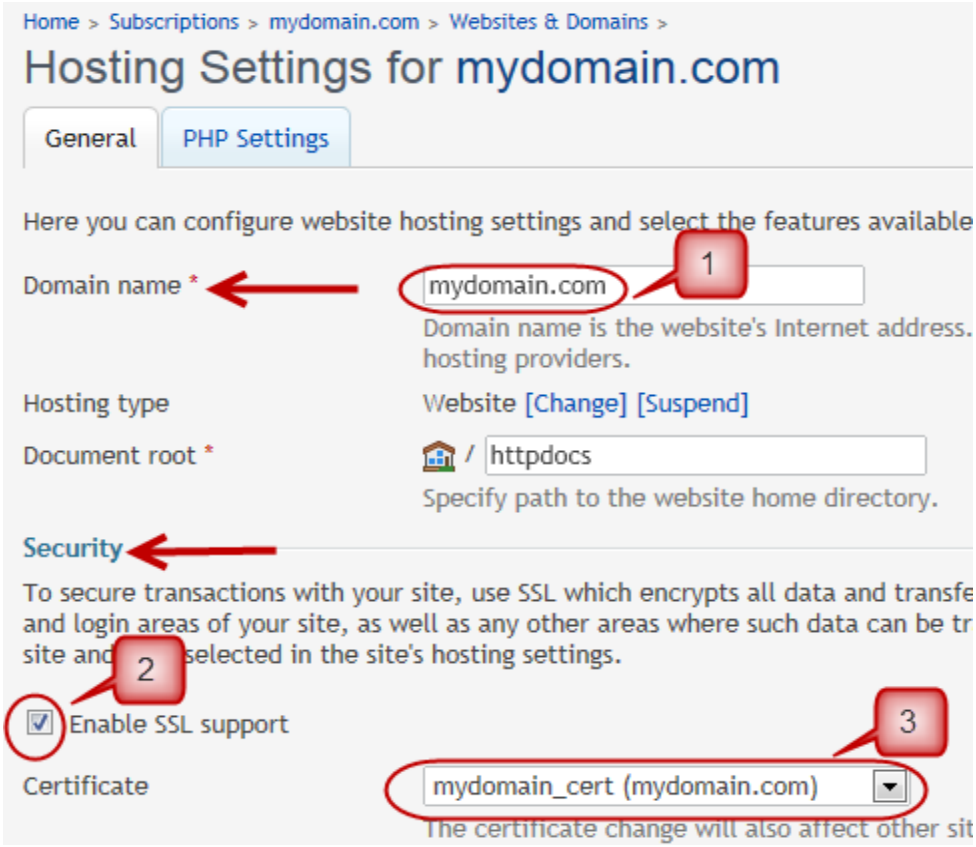
۱۱. در منوی بالای صفحه، گزینه Websites & Domains را انتخاب می‌کنیم (شکل زیر).



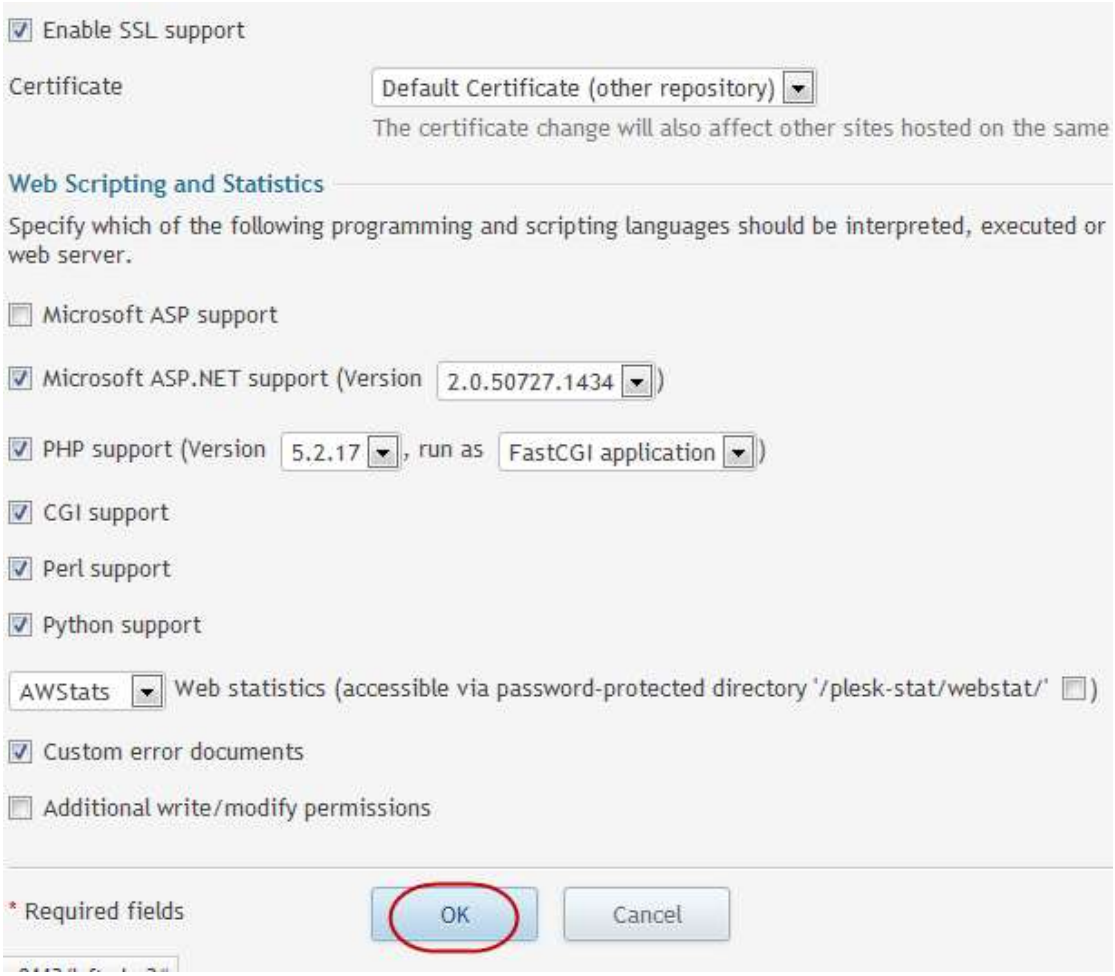
۱۲. در صفحه Websites & Domains، روی نام وب‌سایت در پایین صفحه کلیک می‌کنیم (شکل زیر).



۱۳.در صفحه Hosting Settings for mydomain.com، در سربرگ General، نام وب‌سایت باید همان نام پیش‌فرض آن یعنی وب‌سایتی که برایش گواهی SSL صادر شده، باشد (دقت نمایید، نام سایت را به صورت دقیق وارد نمایید). سپس در بخش Security، گزینه Enable SSL support را انتخاب می‌کنیم (تیک می‌زنیم). از قسمت Certificate، گواهی با نامی که در مرحله ۶ برای آن قرار دادیم (در مثال ما، mydomain_cert) را انتخاب می‌کنیم. همان‌طور که در شکل زیر ملاحظه می‌کنید در کنار نام گواهی، نام وب‌سایت متناظر آن (در مثال ما، mydomain.com) نیز درج شده است.

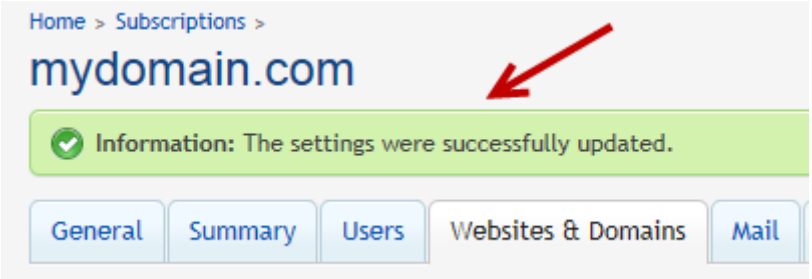


۱۴.پس از انجام تنظیمات لازم، روی دکمه OK در پایین صفحه کلیک می‌کنیم (شکل زیر).

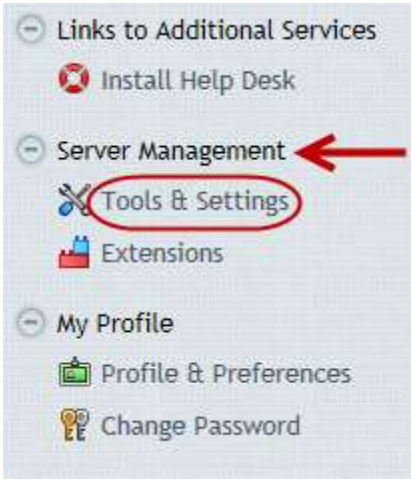


نکته: در شکل بالا، تکمیل گزینه‌های مرتبط با گواهی SSL عنوان شده است و سایر اطلاعات این بخش به نصب گواهی SSL در Plesk مربوط نمی‌باشد. به عبارت دیگر، شکل بالا به این معنا نیست که گزینه‌های نشان‌داده شده باید مانند شکل، فعال یا غیرفعال باشند.

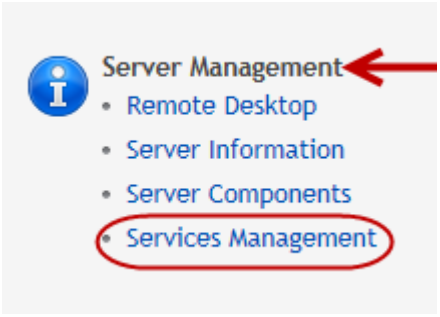
۱۵.پیغامی مبنی بر موفق بودن اعمال تغییرات جدید ظاهر می‌گردد (شکل زیر).



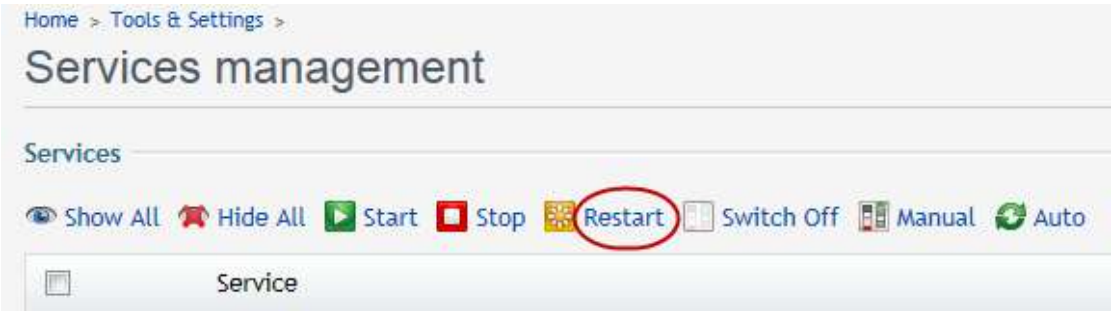
۱۶. پس از نصب گواهی SSL در وب‌سایت، برای فعال‌سازی گواهی SSL نصب شده، لازم است وب‌سرور restart گردد. در صفحه اصلی پنل، از منوی سمت چپ، در بخش Server Management روی گزینه Tools & Settings کلیک می‌کنیم (شکل زیر).



۱۷. در صفحه Tools & Settings، روی گزینه Services Management از بخش Server Management کلیک می‌کنیم (شکل زیر).



۱۸. در صفحه Services management، سرویس وب‌سرور را انتخاب نموده و روی گزینه Restart کلیک می‌کنیم (شکل زیر).



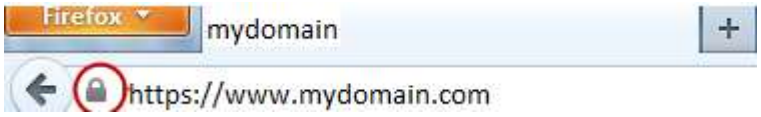
۵ بررسی صحت نصب گواهی SSL

برای برقراری ارتباط صحیح SSL میان مرورگر کاربر و وب‌سایت، کاربر وب‌سایت باید زنجیره گواهی را روی سیستم یا مرورگر خود نصب نماید. رویه این کار در سند «راهنمای نصب زنجیره گواهی» تشریح شده است. این سند را می‌توانید از بخش "راهنماها" در وب‌سایت مرکز پارس‌ساین به آدرس www.parssignca.ir دانلود و مطالعه نمایید. پس از نصب صحیح زنجیره گواهی، در نوار آدرس مرورگر، آدرس https://www.mydomain.com را وارد می‌نماییم (به جای www.mydomain.com باید آدرس دقیق سایت خود را وارد نمایید). نمایش علامت قفل به همراه عبارت https در نوار آدرس مرورگرها یکی از نشانه‌های صحیح بودن نصب گواهی SSL در وب‌سایت می‌باشد. نمایش علامت قفل در سه مرورگر Google Chrome، Internet Explorer، و Firefox به صورت زیر می‌باشد:

- **مرورگر Google Chrome**: در نوار آدرس (مطابق شکل زیر) قفل سبز رنگ در کنار عبارت سبز رنگ https ظاهر می‌شود.

- **مرورگر Internet Explorer**: علامت قفل در سمت راست نوار آدرس (شکل زیر) ظاهر می‌شود.

- **مرورگر فایرفاکس**: در نوار آدرس (مطابق شکل زیر) آیکن قفل کنار عبارت https ظاهر می‌شود.



برای اطمینان کامل از صحت نصب گواهی، در مرورگر خود روی علامت قفل کلیک نموده و روی لینک Certificate Information در Google Chrome، View Certificates در Internet Explorer، و More Information در Firefox کلیک نمایید. سپس اطمینان حاصل کنید که گواهی نشان‌داده شده، همان گواهی است که مرکز پارس‌ساین برای وب‌سایت شما صادر نموده است.

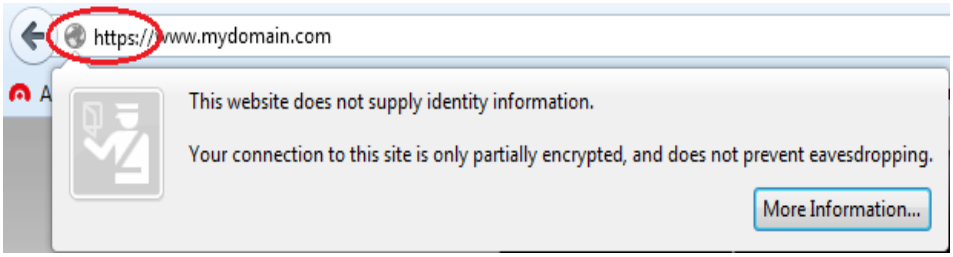
۶ مشکلات احتمالی پس از نصب گواهی

۶-۱ عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وب‌سایت

در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکل‌های زیر نمایش داده شود:

- **مرورگر Google Chrome**: در نوار آدرس مرورگر، علامت مثلث روی قفل کنار https نشان داده شود (مانند شکل زیر).

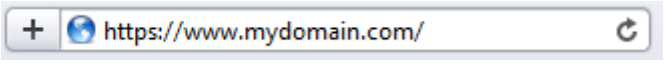
- **مرورگر Firefox**: در نوار آدرس مرورگر، علامت قفل کنار https ظاهر نشود (مانند شکل زیر).



- **مرورگر Intenet Explorer**: در پایین صفحه، پیامی مانند شکل زیر ظاهر گردد.

- **مرورگر Opera**: در نوار آدرس مرورگر، علامت Secure کنار https ظاهر نشود (مانند شکل زیر).

- **مرورگر Safari**: در انتهای نوار آدرس مرورگر، علامت قفل ظاهر نشود (مانند شکل زیر).



این مشکل معمولاً Mixed content warning نامیده می‌شود که ممکن است یک حمله‌کننده با استفاده از آن امنیت کاربران سایت شما را به مخاطره اندازد. این مشکل مربوط به گواهی SSL سایت نیست، بلکه به کد وب‌سایت یا تنظیمات سرور شما مربوط می‌باشد. دلیل مشکل این دلیل

است که در وب‌سایت شما از محتوای[1] ناامن استفاده شده است. مثال‌هایی از محتوای ناامن، عکس‌ها، اسکریپت‌ها، یا CSSهایی هستند که به طور ناامن (از طریق HTTP) در سایت شما بارگذاری می‌شوند. مرورگر از بارگذاری یا اجرای این محتواها جلوگیری می‌کند. به همین دلیل ممکن است CSS وب‌سایت شما بارگذاری نشده و ساختار وب‌سایت شما با HTTPS به هم بریزد، عکسی بارگذاری نشود، یا اسکریپتی اجرا نشود.

برای کشف محتوای ناامن، می‌توانید از قابلیت Web Developer Toolbar در اغلب مرورگرها استفاده کنید. کشف محتوای ناامن با استفاده از مرورگرهای رایج معمولاً به صورت زیر می‌باشد:

- **مرورگر Google Chrome و Internet Explorer**: فشردن کلید F12 و مشاهده خطاها در بخش Console.
- **مرورگر Firefox**: فشردن کلیدهای Ctrl + Shift + K و مشاهده خطاهای Mixed Content.

پس از کشف محتوای ناامن، آن‌ها را از طریق HTTPS بارگذاری نموده و در صورت عدم امکان بارگذاری با استفاده از HTTPS، آن‌ها را از وب‌سایت خود حذف نمایید. در زیر چند سناریو از محتوای ناامن توصیف شده است.

- برای مثال، فرض کنید CSS سایت به صورت http://www.mydomain.com/templates/mycss.css در صفحه سایت فراخوانی شده باشد. در این صورت، به دلیل استفاده از http (به جای https) این محتوا توسط مرورگر ناامن تشخیص داده شده و بارگذاری نمی‌شود (در نتیجه ساختار سایت بهم می‌ریزد). بنابراین توصیه می‌شود به جای استفاده از آدرس‌های قطعی (hardcoded) برای عکس‌ها، CSS، و اسکریپت‌های سایت، از روش‌هایی مانند آدرس‌های نسبی، توابع (مثلاً ()include)، یا هر روش دیگری استفاده نمایید که با استفاده از آن بتوان محتوا را با استفاده از https بارگذاری نمود. در صورتی که از روشی مانند آدرس‌دهی نسبی استفاده کنید اما مشکل همچنان باقی باشد، مشکل مربوط به تنظیمات SSL در سرور شما می‌باشد.
- در برخی موارد، ممکن است آدرس عکس، CSS، یا اسکریپت با https باشد اما مرورگر آن را بارگذاری نکند. این مشکل معمولاً به این دلیل است که مثلاً CSS با آدرس https://mydomain.com/templates/mycss.css (یعنی بدون www) فراخوانی شده است اما

[1] Content

آدرس درج شده در گواهی سایت، با www است. در این مثال، راه حل این است آدرس https به طور دقیق و طبق آنچه در گواهی SSL سایت درج‌شده وارد شود.

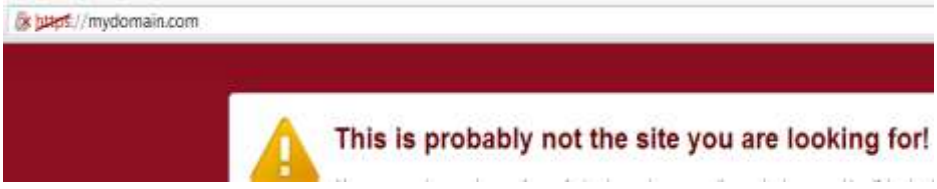
- مثال دیگر از محتوای ناامن، استفاده از اسکریپت‌هایی است که با استفاده از http اطلاعاتی را از سایت ما برای سایت دیگری (مثلاً برای یک سایت ثبت آمار کاربران) ارسال می‌کنند. همچنین، اسکریپت‌ها، عکس‌ها، و غیره که از سایت دیگر به صورت http در سایت ما بارگذاری می‌شوند. مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری می‌کند. در صورتی که امکان بارگذاری این محتواها از طریق https وجود ندارد، آن‌ها از وب‌سایت خود حذف نمایید. روش دیگر این است که دو صفحه مجزا، یکی برای http و یکی برای https طراحی کنید؛ در صفحه مربوط به http، همه محتوای مورد نظر را قرار دهید اما در صفحه https، محتوای ناامن را حذف کنید. سپس در تنظیمات SSL روی سرور، درخواست‌های SSL را به آدرس صفحه https ارجاع دهید. راه‌حل دیگر این است که به جای دریافت محتوا (مثلاً عکس) از سایت دیگر، محتوا را از سایت مذکور دریافت و در منابع سایت خود قرار دهید. سپس به طور محلی آن‌ها را فراخوانی/بارگذاری کنید.
- در برخی موارد، ممکن است محتوا از سایت دیگر و با https فراخوانی شود، اما توسط مرورگر بارگذاری نشود. این مشکل معمولاً دلایل مختلفی می‌تواند داشته باشد که همگی بستگی به سرویس HTTPS سایت ارسال‌کننده محتوا دارد. مثلاً ممکن است گواهی SSL آن سایت، برای مرورگر مورد اعتماد نباشد. برای حل این مشکل، وضعیت سرویس HTTPS سایت ارسال‌کننده را بررسی نمایید.

۲-۶ نمایش صفحه هشدار SSL در مرورگر

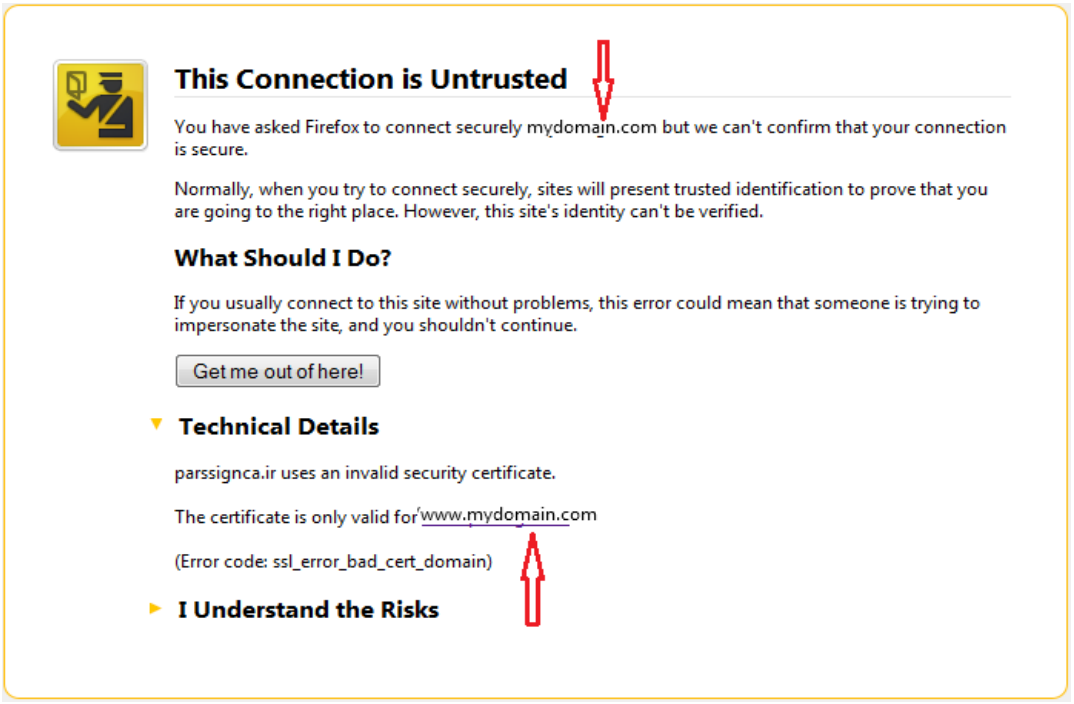
در حالت کلی این گونه هشدارها را به دقت مطالعه نموده و دلیل آن را بررسی نمایید.

در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکل‌های زیر نمایش داده شود:

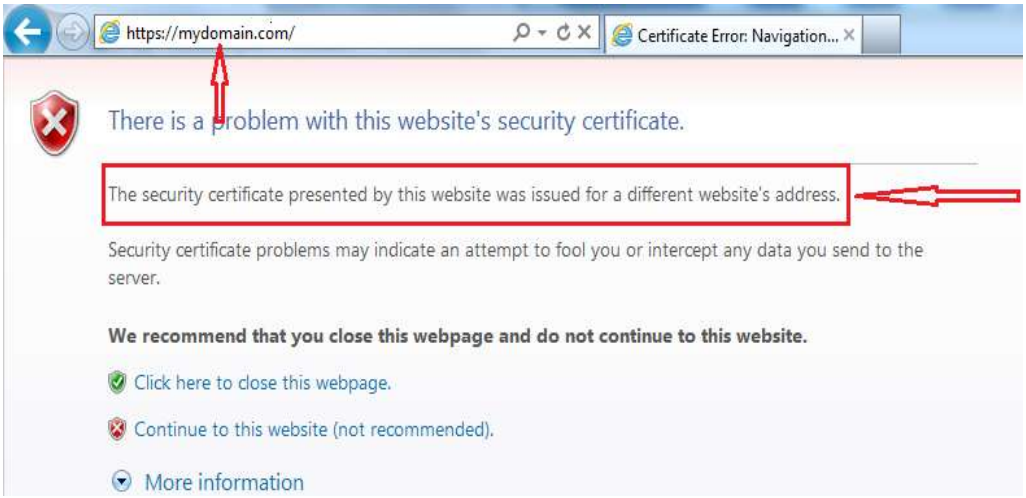
- **مرورگر Google Chrome**: پیام زیر نمایش داده شود.



- **مرورگر Firefox**: پیام زیر نمایش داده شود.



- **مرورگر Internet Explorer**: پیام زیر نمایش داده شود.



دلیل مشکل فوق این است که آدرس سایت را بطور دقیق وارد ننموده‌اید. در زیر، چند سناریو که منجر به چنین خطایی می‌شوند آورده شده است:

- اگر گواهی برای www.mydomain.com صادر شده باشد اما آدرس https://mydomain.com (یعنی بدون www) را در مرورگر وارد نمایید، با صفحه خطای فوق مواجه می‌شوید. برای رفع این مشکل، یا باید همیشه آدرس دقیق وارد شود یا راه‌حل بهتر اینکه در تنظیمات سرور خود، آدرس

https://mydomain.com را به https://www.mydomain.com (یعنی با آدرس دقیق) تغییر مسیر دهید (redirect نمایید).

- ممکن است یک سایت، به چند دامنه (مثلاً mydomain.com و mydomaint.ir) تخصیص داده شده باشد. مثلاً اگر گواهی سایت برای www.mydomain.com صادر شده باشد اما آدرس https://www.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می‌شوید. در صورتی که برای یک سایت چند دامنه وجود داشته باشد اما گواهی شما فقط برای یک دامنه صادر شده باشد، باید از مرکز صدور گواهی درخواست گواهی SAN نمایید. کاربرد گواهی SAN برای استفاده از یک گواهی برای چندین دامنه است.
- ممکن است برای یک سایت فقط یک دامنه وجود داشته باشد اما در آن دامنه، زیردامنه[1] نیز وجود داشته باشد (مثلاً mail.mydomain.com). حال اگر آدرس https://mail.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می‌شوید. در صورتی که بخواهید برای زیردامنه خود نیز از HTTPS استفاده نمایید، باید یک گواهی مجزا برای این زیر دامنه درخواست نمایید. در صورتی که بخواهید فقط از یک گواهی برای یک دامنه و تمام زیردامنه‌هایش استفاده کنید، می‌توانید درخواست گواهی Wildcard نمایید.

توجه: ممکن است صفحه‌های هشدار مشابه دیگری با دلایل خاص خود وجود داشته باشد که معمولاً مربوط به پیکربندی سرور شما می‌باشد. در صورت مواجهه با چنین خطاهایی، آن‌ها را به دقت مطالعه نموده و با انجام تنظیمات لازم روی سرور، آن‌ها رفع نمایید.

۶-۳ نمایش صفحه دیگری به جای صفحه سایت

برای استفاده از HTTPS برای یک دامنه (وب‌سایت)، باید یک آدرس IP اختصاصی (Dedicated IP Address) به آن دامنه تخصیص داده شود (رویه تخصیص IP اختصاصی در بخش ۷-۱ توضیح داده شده است). در صورتی که آدرس IP سایت با سایت‌های دیگر به اشتراک گذاشته شده باشد (Shared باشد)، هنگام درخواست HTTPS، سرور معمولاً صفحه پیش‌فرض Plesk یا صفحه دیگری را نشان می‌دهد (زیرا نمی‌تواند تشخیص دهد چه سایتی را برگرداند).

[1] Subdomain

۴-۶ نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر

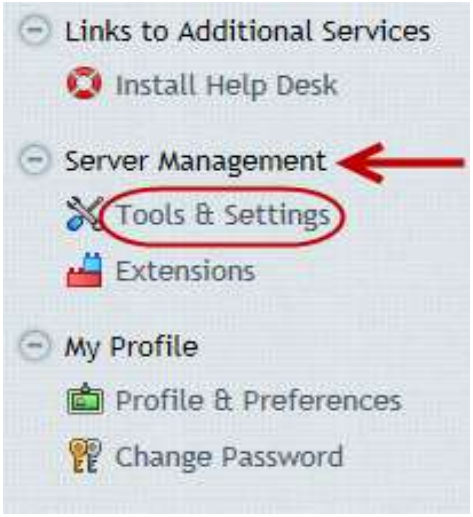
این مشکل مربوط به گواهی SSL سایت نیست، زیرا گواهی صادرشده توسط مرکز میانی پارس‌ساین از استانداردی (استاندارد X.509) تبعیت می‌کند که وابسته به مرورگر یا سیستم‌عامل خاصی نیست. این مشکل معمولاً به دلیل استفاده از مرورگر یا سروری است که بروزرسانی نشده است. در صورتی که مرورگر و سرور هر دو به روز باشد، مشکل در تنظیمات SSL سرور است.

۷ پیوست

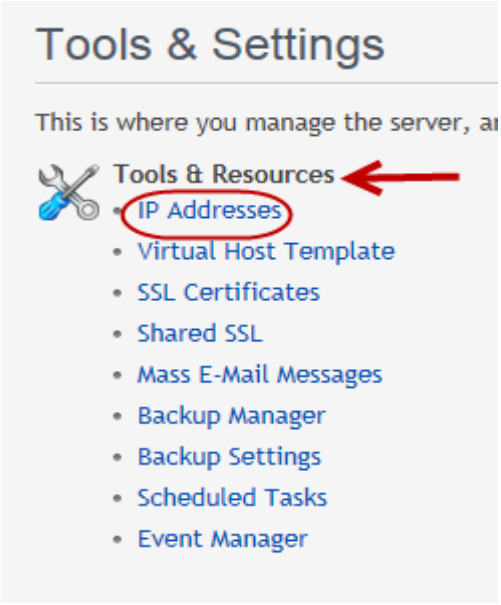
۷-۱ رویه اختصاصی کردن آدرس IP وب‌سایت در Plesk

پس از دریافت آدرس IP اختصاصی برای وب‌سایت خود، باید تنظیمات لازم برای تخصیص این آدرس IP به وب‌سایت را در Plesk انجام دهیم. برای این منظور باید مراحل زیر را طی نماییم:

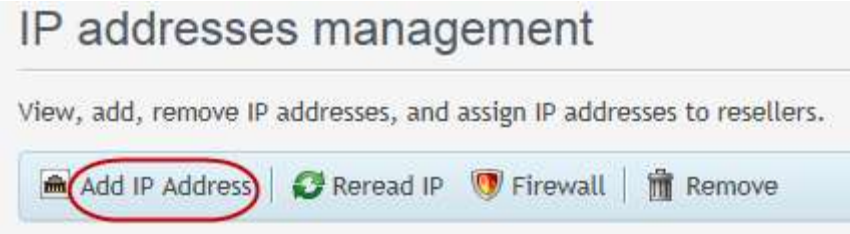
۱. ابتدا به پنل مدیریتی Plesk خود Login می‌نماییم. از منوی سمت چپ، در بخش Server Management روی گزینه Tools & Settings کلیک می‌کنیم (شکل زیر).



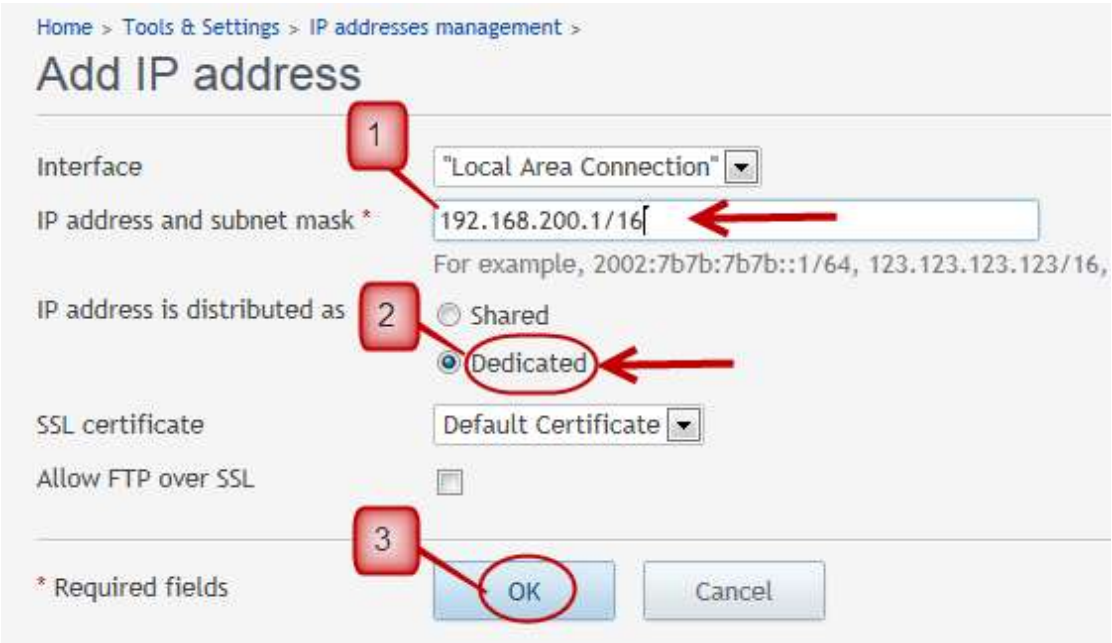
۲. در صفحه Tools & Settings، از بخش Tools & Resources گزینه IP Addresses را انتخاب می‌کنیم (شکل زیر).



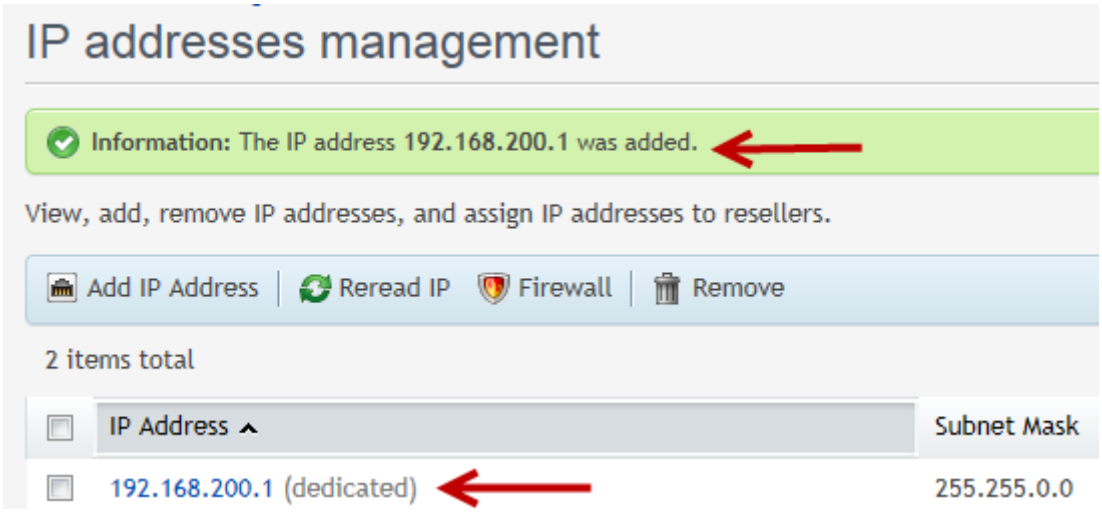
۳. در صفحه IP addresses management گزینه Add IP Address را انتخاب می‌کنیم (شکل زیر).



۴. در صفحه Add IP address باید آدرس IP اختصاصی و Subnet mask را که از مدیر سرور (هاستینگ) دریافت نموده‌ایم در مقابل IP address and subnet mask وارد نماییم. برای مثال، در شکل زیر فرض می‌کنیم آدرس IP اختصاصی وب‌سایت 192.168.200.1 باشد و ۱۶ بیت از آدرس IP برای زیرشبکه در نظر گرفته شده باشد. IP address and subnet mask را به دو صورت 192.168.200.1/16 یا 192.168.200.1/255.255.0.0 می‌توان وارد نمود. سپس در بخش IP address is distributed as گزینه Dedicated را انتخاب و روی دکمه OK کلیک می‌کنیم.



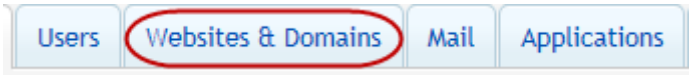
۵. در صفحه IP addresses management پیغامی مبنی بر اضافه شدن آدرس IP جدید به لیست آدرس‌های IP موجود، نمایش داده می‌شود و آدرس IP اختصاصی جدید نیز در لیست آدرس‌ها به صورت (dedicated) قرار می‌گیرد (شکل زیر).



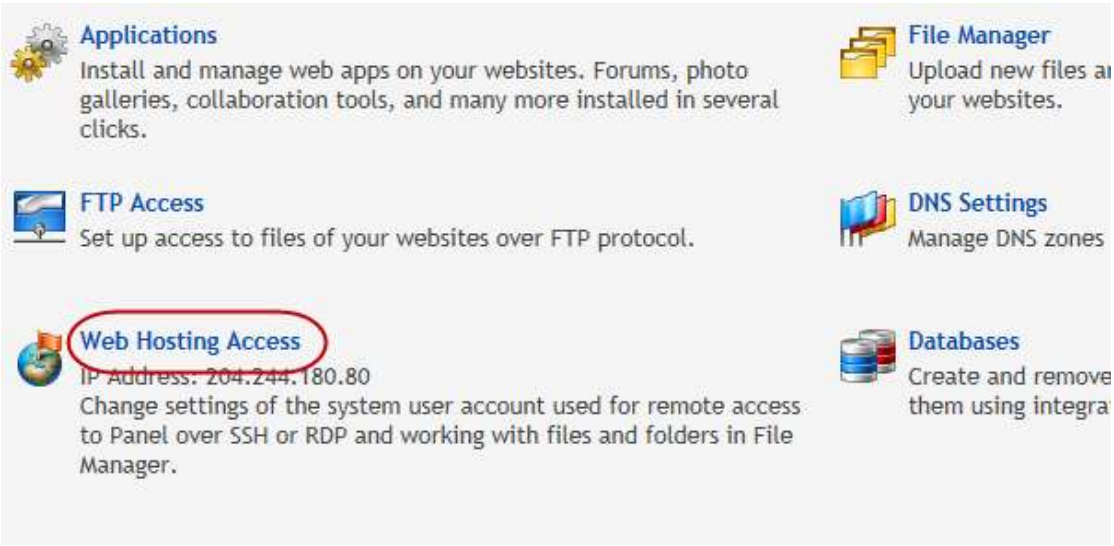
۶. حال باید آدرس IP اختصاصی را به وب‌سایت خود تخصیص دهیم. برای این منظور، از منوی سمت چپ، در بخش Hosting Services گزینه Domains را انتخاب می‌کنیم (شکل زیر).

۷. در لیست نام وب‌سایت‌های موجود، روی نام دامنه‌ای که قرار است گواهی SSL برای آن نصب شود (در مثال ما، mydomain.com)، کلیک می‌کنیم (شکل زیر).

۸. در منوی بالای صفحه، گزینه Websites & Domains را انتخاب می‌کنیم (شکل زیر).

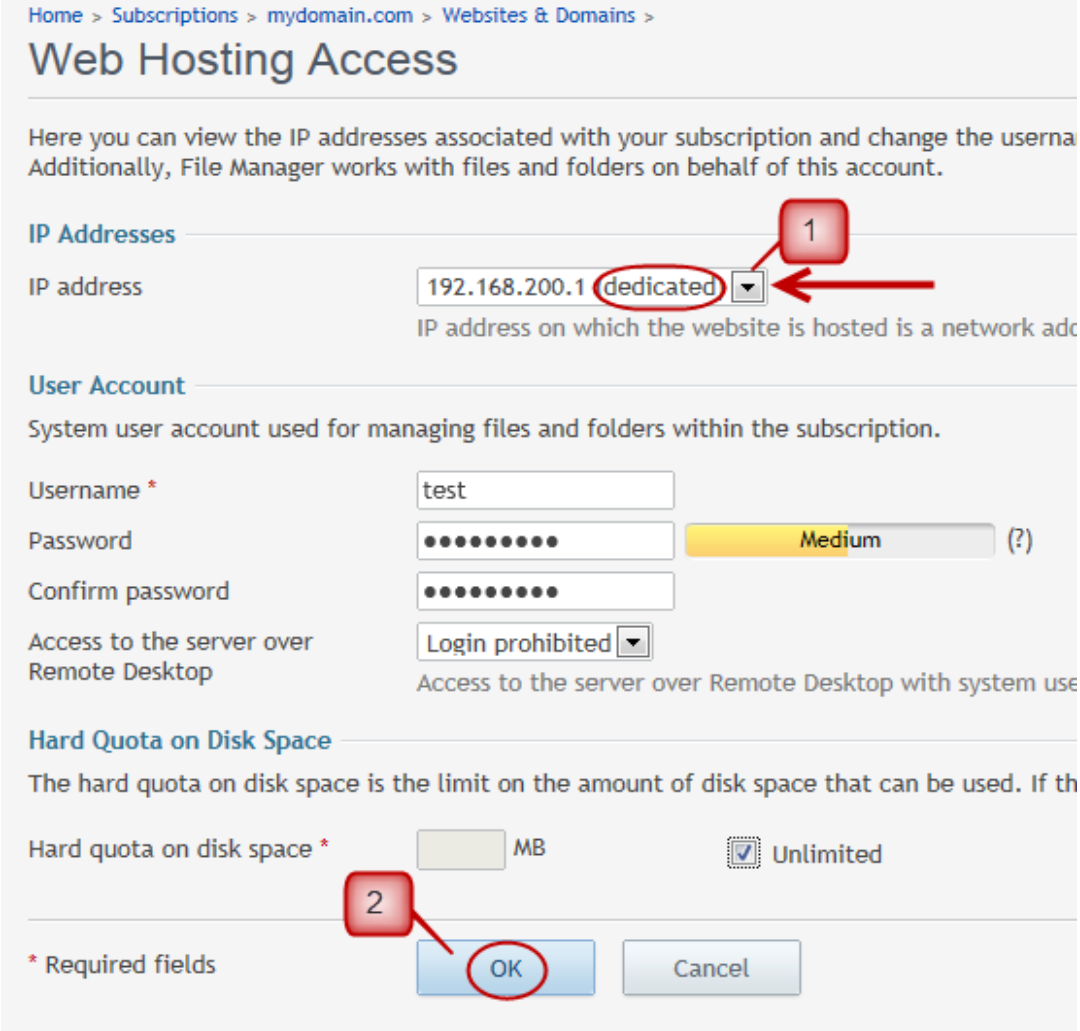


۹. در لیست Websites & Domains، روی گزینه Web Hosting Access کلیک می‌کنیم (شکل زیر).

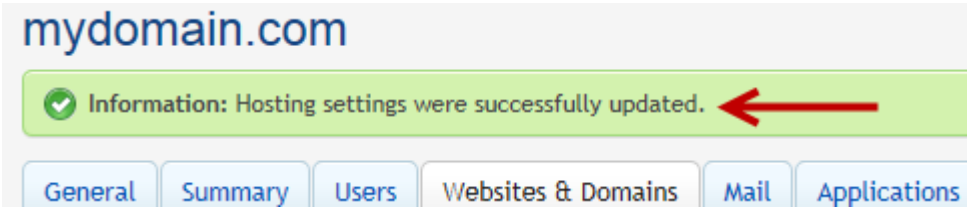


۱۰.در صفحه Web Hosting Access، از لیست آدرس‌های IP موجود مقدار IP address را آدرس IP اختصاصی که از مدیر سرور (هاستینگ) دریافت نموده‌ایم، انتخاب می‌کنیم. دقت کنید که در کنار آدرس IP انتخاب شده حتماً عبارت (dedicated) وجود داشته باشد. سپس روی گزینه OK کلیک می‌کنیم (شکل زیر).

نکته: اطلاعات دیگری مانند گزینه‌های User Account در این بخش وجود دارد. این تنظیمات مربوط به گواهی SSL نمی‌شود. به عبارت دیگر، شکل زیر به این معنا نیست که گزینه‌های نشان‌داده شده باید مانند شکل فعال/غیرفعال باشند.



۱۱. پیغامی مبنی بر موفق بودن اعمال تنظیمات جدید ظاهر می‌شود.



۲-۷ نحوه بررسی pem بودن فرمت فایل کلید و تبدیل آن به فرمت PEM و حذف گذرواژه آن

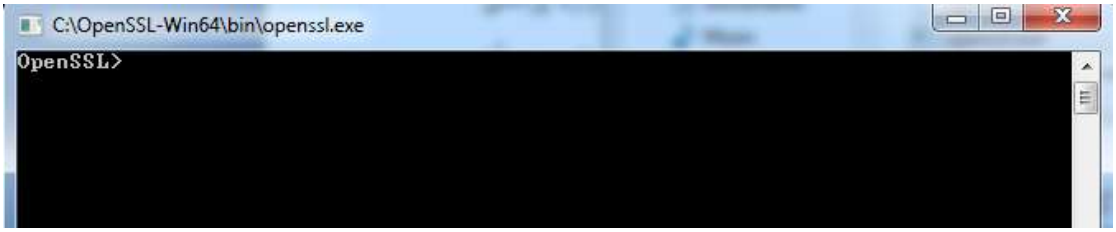
برای بررسی pem بودن فرمت فایل کلید خصوصی، آن را با یک ویرایشگر متن باز WordPad باز می‌کنیم. در صورتی که فایل با عبارت -----BEGIN RSA PRIVATE KEY----- شروع و به -----END RSA PRIVATE KEY----- ختم شده باشد، فرمت فایل از نوع PEM می‌باشد.

نکته: در صورتی که CSR با نرم‌افزار ParsKey Utility تولید شده باشد، فایل کلید در فرمت PEM می‌باشد.

در صورتی‌که فرمت فایل کلید خصوصی PEM نباشد، برای تبدیل آن به فرمت PEM مراحل زیر را باید انجام دهیم:

۱. به وب‌سایت مرکز پارس‌ساین به آدرس www.parssignca.ir مراجعه نموده و نرم‌افزار OpenSSL را دانلود و روی سیستم خود نصب می‌نماییم. این نرم‌افزار معمولاً در سیستم‌های لینوکسی نصب شده وجود دارد.

۲. اگر نسخه تحت ویندوز OpenSSL را نصب کرده باشیم، به مسیر نصب OpenSSL رفته (در ویندوز 7 ۶۴ بیتی، C:\OpenSSL-Win64 مسیر نصب پیش‌فرض می‌باشد) و وارد پوشه bin می‌شویم. در پوشه bin، فایل اجرایی OpenSSL به نام openssl.exe وجود دارد. این فایل را اجرا می‌کنیم تا صفحه اجرایی نرم‌افزار OpenSSL به شکل زیر ظاهر گردد.



روبروی عبارت OpenSSL> در پنجره فوق، دستور زیر را وارد می‌کنیم:

```
rsa -in mydomain.key -out mydomain_new.key -outform PEM
```

لازم به ذکر است که اگر با ترمینال لینوکس کار می‌کنیم، فرمان زیر را به جای دستور فوق باید وارد نماییم:

```
openssl rsa -in mydomain.key -out mydomain_new.key -outform PEM
```

در دستور بالا، فایل mydomain.key، فایل کلید خصوصی اصلی است که می‌خواهیم آن را به فرمت PEM تبدیل نماییم. فایل mydomain_new.key، فایل کلید خصوصی جدید در فرمت PEM است که با اجرای دستور ایجاد می‌شود.

لازم به ذکر است که برای هر یک از فایل‌های فوق، باید مسیر دقیق آن‌ها را در دستور وارد کنیم. برای مثال، در صورتی که فایل mydomain.key در درایو D و پوشه keys قرار داشته باشد و بخواهیم فایل mydomain_new.key نیز در همین مسیر ذخیره شود، دستور به صورت زیر خواهد بود:

```
rsa -in d:\keys\mydomain.key -out d:\keys\mydomain_new.key
 -outform PEM
```

اگر با ترمینال لینوکس کار می‌کنیم، فرض می‌کنیم فایل mydomain.key در مسیر /home/keys قرار داشته باشد و می‌خواهیم فایل mydomain_new.key نیز در همین مسیر ذخیره شود. در این‌صورت، دستور زیر را وارد می‌نماییم:

```
openssl rsa -in /home/keys/mydomain.key -out
/home/keys/mydomain_new.key
```

نکته: در صورتی که هنگام ایجاد CSR، برای فایل کلید، گذرواژه تعیین کرده باشیم، هنگام نصب گواهی روی سرور با استفاده از پنل مدیریتی Plesk باید گذرواژه آن را حذف نموده و فایل کلیدی بدون گذرواژه ایجاد کنیم (دلیل این کار، عدم پشتیبانی پلسک از کلید دارای گذرواژه است). رویه این کار به صورت زیر می‌باشد:

در صفحه اجرایی نرم‌افزار OpenSSL، دستور زیر را وارد نمایید:

```
rsa -in mydomain.key -out mydomain_passless.key
```

لازم به ذکر است که اگر با ترمینال لینوکس کار می‌کنیم، دستور زیر را باید وارد نماییم:

```
openssl rsa -in mydomain.key -out mydomain_passless.key
```

با اجرای دستور بالا، از شما خواسته می‌شود که گذرواژه کلید خصوصی را وارد نمایید که باید گذرواژه انتخاب‌شده برای کلید هنگام ایجاد CSR را وارد کنید. در دستور بالا، فایل mydomain.key، فایل کلید خصوصی است که می‌خواهیم گذرواژه آن را حذف کنیم. فایل mydomain_passless.key، فایل کلید خصوصی جدید است که با اجرای دستور ایجاد می‌گردد و در آن گذرواژه حذف شده است.

لازم به ذکر است که برای هر یک از فایل‌های فوق، باید مسیر دقیق آن‌ها را در دستور وارد نماییم. برای مثال، در صورتی که فایل mydomain.key را در درایو D و پوشه keys قرار داده باشیم و

می‌خواهیم فایل mydomain_passless.key نیز در همین مسیر ذخیره شود، دستور به صورت زیر خواهد بود:

```
rsa -in d:\keys\mydomain.key -out d:\keys\mydomain_passless.key
```

اگر با ترمینال لینوکس کار می‌کنیم، فرض می‌کنیم فایل mydomain.key در مسیر /home/keys قرار داشته باشد و بخواهیم فایل mydomain_passless.key نیز در همین مسیر ذخیره شود. در این‌صورت، دستور زیر را وارد می‌کنیم:

```
openssl rsa -in /home/keys/mydomain.key -out
/home/keys/mydomain_passless.key
```

۳-۷ نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM

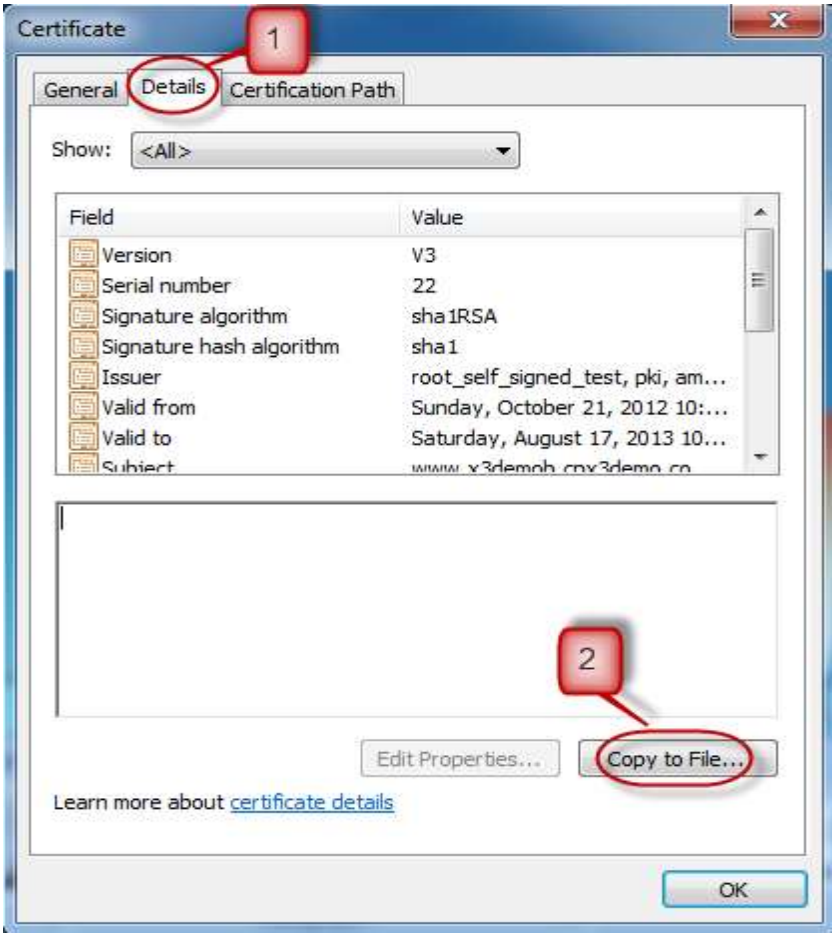
از روی پسوند گواهی، نمی‌توان به PEM بودن فرمت فایل گواهی پی برد. برای بررسی PEM بودن گواهی، آن را با یک ویرایشگر متن (نرم‌افزار WordPad در ویندوز و cat در لینوکس) باز می‌نماییم. در صورتی که فایل با عبارت -----BEGIN CERTIFICATE----- شروع و به -----END CERTIFICATE----- ختم شده باشد، فرمت فایل از نوع PEM می‌باشد.

در صورتی که فرمت گواهی PEM نباشد، به یکی از دو روش زیر می‌توانیم، آن را تبدیل به یک گواهی با فرمت PEM نماییم:

- **روش اول:** در ویندوز می‌توانیم عمل تبدیل فرمت را به صورت زیر انجام دهیم:

۱. ابتدا فایل مورد نظر را باز می‌نماییم. برای این کار، روی فایل گواهی دابل‌کلیک نموده، سپس در پنجره ظاهرشده روی دکمه Open کلیک می‌نماییم.

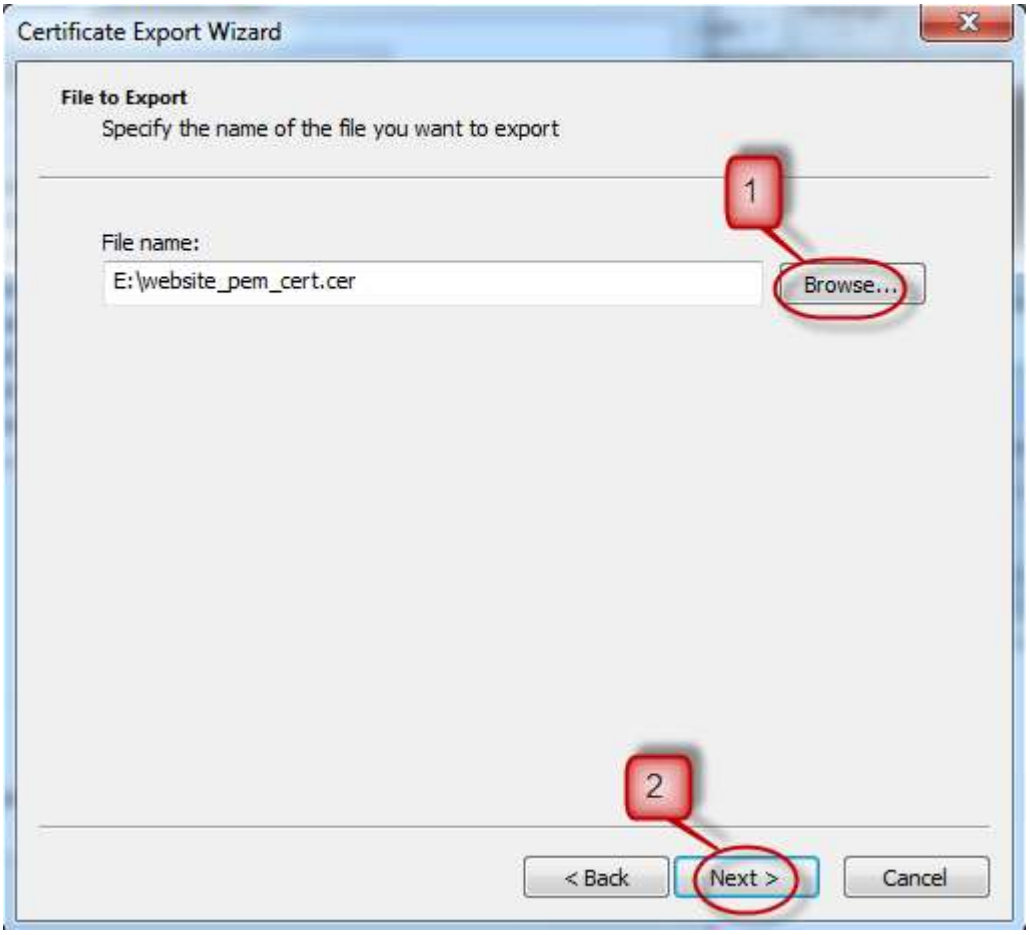
۲. در پنجره بازشده، در سربرگ Details روی دکمه Copy to Files کلیک می‌نماییم (مانند شکل زیر).



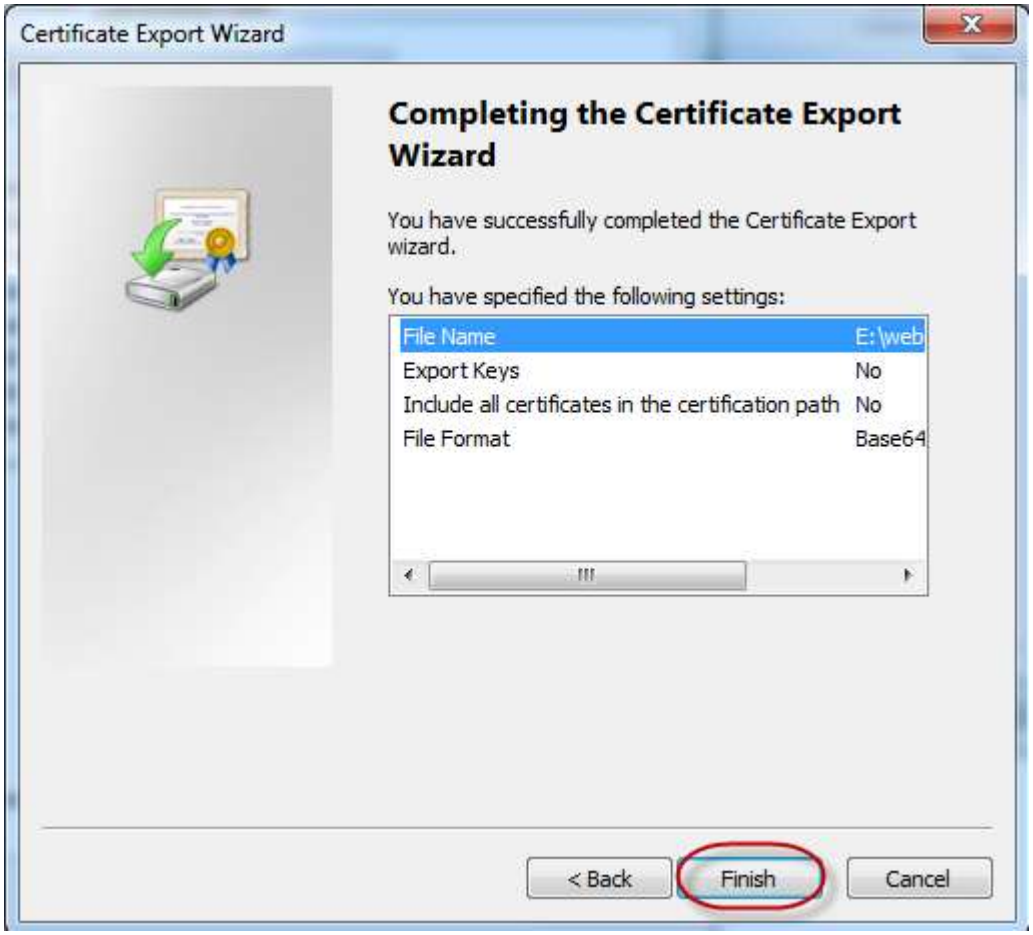
۳. در پنجره Certificate Export Wizard روی Next کلیک می‌نماییم (مانند شکل زیر).

۴. در پنجره Export File Format در بخش Select the format you want to use گزینه Base-64 encoded X.509 (.CER) را انتخاب نموده، سپس روی Next کلیک می‌کنیم (مانند شکل زیر).

۵. در پنجره File to Export برای انتخاب مسیر ذخیره فایل با فرمت PEM، روی Browse کلیک می‌نماییم. پس از انتخاب نام و مسیر ذخیره فایل، روی Next کلیک می‌نماییم (مانند شکل زیر).



۶. در پنجره Completing the Certificate Export Wizard روی Finish کلیک می‌نماییم (مانند شکل زیر).



۷. پنجره زیر ظاهر می‌گردد که نشان‌دهنده ایجاد موفقیت‌آمیز یک گواهی جدید با فرمت PEM می‌باشد. در این پنجره روی OK کلیک می‌نماییم.

- **روش دوم:** با استفاده از نرم‌افزار OpenSSL در لینوکس (که معمولاً بطور پیش‌فرض روی سیستم‌های لینوکس وجود دارد)، می‌توانیم عملیات تبدیل را انجام دهیم. بدین‌منظور، دستور زیر را در ترمینال لینوکس وارد می‌نماییم:

```
openssl x509 -inform der -in www.mydomain.com.cer -out
www.mydomain.com.crt
```

در دستور بالا، www.mydomain.com.cer فایل گواهی ورودی در فرمت DER است و فایل www.mydomain.com.crt فایل گواهی خروجی در فرمت PEM است. لازم به ذکر است در این دستور، باید آدرس دقیق فایل‌های مذکور را وارد نماییم. مثلاً اگر گواهی‌ها را در دایرکتوری /home/certs/ ذخیره می‌کنیم، دستور به صورت زیر خواهد بود:

```
openssl x509 -inform der -in /home/certs/www.mydomain.com.cer
 -out /home/certs/www.mydomain.com.crt
```