

مركز صدور گواهی الکترونيکی پارسساين

راهنمای نصب گواهی الکترونیکی SSL در SSL

تدوينكننده: شركت امنافزار گستر شريف

SSW_UG_PKI_91174_	شىمار <i>ە</i> سىند1_
۲۷/آذر / ۱۳۹۱	تاريخ
1.7	نگارش

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

تلفن: ۲۰–۶۱۹۷۵۵۰ (۲۱) فاکس: ۶۶۰۹۰۲۹۹ (۲۱) سایت اینترنتی: www.parssignca.ir

حق طبع و نشر

این سند در تاریخ ۱۳۹۱/۰۸/۱۶ توسط شرکت امنافزار گستر شریف به منظور تهیه بخشی از اسناد «مرکز صدور گواهی الکترونیکی پارسساین» تدوین گردیده است. تمامی حقوق این اثر متعلق به «شرکت امنافزار گستر شریف» میباشد و هرگونه نسخهبرداری از آن، اعم از کپی، نسخهبرداری الکترونیکی و یا ترجمه تمام یا بخشی از آن منوط به کسب اجازه کتبی از صاحب اثر است.

مطالب	ھرست	ف
-------	------	---

٠	مقد	۱
نميات اين سند۲	فرط	۲
ناد درخواست امضای گواهی (CSR) و کلید خصوصی۲	ايج	٣
لربندی پنل مدیریتی Plesk به منظور استفاده از گواهی SSL	پيک	۴
بررسی اختصاصی بودن آدرس IP وبسایت۴	1-4	
نصب کلید خصوصی، گواهی SSL و زنجیره گواهی۶	۲-۴	
سی صحت نصب گواهی SSL	برر	۵
کلات احتمالی پس از نصب گواهی	مشا	۶
عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وبسایت	۱-۶	
نمایش صفحه هشدار SSL در مرورگر	۲-۶	
نمایش صفحه دیگری به جای صفحه سایت	۳–۶	
نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر۲۳	4-9	
ست	پيو	۷
رویه اختصاصی کردن آدرس IP وبسایت در Plesk	۱–۷	
نحوه بررسی pem بودن فرمت فایل کلید و تبدیل آن به فرمت PEM و حذف گذرواژه آن۲۹	۲-۷	
نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM	۳-۷	

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 می شود) یکی از این پروتکلها است که استفاده گستردهای دارد. دادههای HTTP به صورت ناامن روی شبکه منتقل می شوند؛ از اینرو، دادههایی که بین سرویس دهنده (سمت وبسایت) و سرویس گیرنده (سمت کاربر وبسایت) مبادله می شود، 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 LSL میباشد.

لازم به ذکر است، تأمین محرمانگی و عدم تغییر (جامعیت) اطلاعات تبادل شده بین کاربر و وبسایت تنها کاربرد HTTPS نیست. HTTPS برای جلوگیری از حملاتی مانند حمله فیشینگ مبتنی بر جعل سایت نیز استفاده می شود. در حمله مذکور، حمله کننده (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 آن ها را به مخاطره می اندازد؛ مثلاً اطلاعات کاربران را به سرقت برده یا در مورد آن ها اطلاعات جمع آوری می کند. در صورتی که از گواهی HTTPS استفاده شود، از این حمله جلوگیری می شود.

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 پارس ساین) صادر شده باشد تا کاربران بتوانند به آن اعتماد کرده و اطلاعات محرمانه خود را بر اساس این اعتماد، برای وب سایت 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، 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 دامنه ای (وبسایتی) را وارد نمایید که برای آن گواهی SSL دریافت نموده اید.
 - به جای آدرس IP فرضی "I۹۲.۱۶۸.۲۰۰۱"، آدرس IP واقعی وبسایت خود را قرار دهید.

۳ ایجاد در خواست امضای گواهی (CSR) و کلید خصوصی

برای دریافت گواهی الکترونیکی از مرکز صدور گواهی الکترونیکی پارس ساین، ابتدا باید یک درخواست امضای گواهی (CSR) ایجاد نماییم. لازم به ذکر است که فیلدهای CSR باید طبق سیاستهای مرکز صدور گواهی الکترونیکی پارس ساین تکمیل گردد. در غیر این صورت، مرکز صدور گواهی الکترونیکی پارس ساین برای آن CSR، گواهی الکترونیکی صادر نخواهد کرد. با توجه به عدم تطابق فرایند ایجاد CSR در پنل مدیریتی Plesk با سیاستهای زیر ساخت کلید عمومی کشور و مرکز پارس ساین، توصیه می شود 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 می باشد 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 می شود)، 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 آدرس IP وبسایت؛
- نصب کلید خصوصی، گواهی SSL و گواهیهای مراکز صدور گواهی.

¹ Dedicated

© Copyright Amnafzar Co.

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
 ۱. ابتدا به پنل مدیریتی Domains خود انتخاب مینماییم (شکل زیر).

Parallels Panel	
1 Home	
Hosting Services	
Customers	
Resellers	
Domains 🗲	-
Subscriptions	
Service Plans	

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

mydomain.com	😭 Website	Demo Admin, Parallels	Nov 4, 2012	-	0 B	0 B/month	View Site	Anage hosting
--------------	-----------	-----------------------------	-------------	---	-----	--------------	-----------	---------------

۳. در منوی بالای صفحه، از بخش General در قسمت Hosting، آدرس IP وبسایت را در مقابل IP address
 ۳. در منوی بالای صفحه، از بخش General در قسمت Hosting درج شده باشد (مانند IP address 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 میکادی یا وبسایت، باید از نوع اشتراکی باشد، پیش از نصب 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.

Home > Subsci mydon	riptions >	m						🔐 Up) Level
General	Summary	Users	Websites & Domains	Mail	Applications	File Sharing	Statistics	Account	
This is wher	e you view t Plan 🎹	he full info Customize	ormation on a particular e 🛃 Change Hosting S	subscrip Settings	otion and manag	e the subscripti	on. oscriber 🏦	Remove	1
General					Hosting ←	•			k
Subscriber			Demo Admin, Parallels		IP address		192.168.20	0.1 (dedica	ted)
Setup date			Nov 4, 2012		System usernan	ne	test	-	-
Renewal dat	e		5						
Status			🕙 Active						

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).

Parallels Panel	
Home	
Hosting Services	
S Customers	
& Resellers	
Domains	-
Subscriptions	
G Service Plans	

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



mydor	nain.co	m							😭 Up Level
General	Summary	Users	Websites & Domains	Mail	Applications	File Sharing	Statistics	Account	

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



Certificates

No SSL certificates

۶. در صفحه Add SSL Certificate، از بخش Certificate، یک نام دلخواه برای گواهی SSL روبروی.
۶. در صفحه Certificate می کنیم. در شکل زیر نام انتخاب شده mydomain_cert می باشد.



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 CSR که این فایلها در فرمت PEM می باشند. همچنین، در صورتی که فایل کلید خصوصی دارای گذرواژه (پسورد) می باشد، ابتدا باید گذرواژه آن را حذف نماییم. نحوه بررسی mem بودن فایل کلید و حذف گذرواژه آن در بخش ۷-۲ از پیوست تشریح شده است. نحوه بررسی mem بودن فایل گواهی نیز در بخش ۷-۳ از پیوست آمده است.

به دو روش می توان کلید خصوصی، گواهی SSL وبسایت، و زنیجره گواهی را نصب کرد:

- روش اول: بارگذاری فایل های 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.
 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 فایل های گواهی و کلید خصوصی از طریق بخش Upload certificate files:
- توصیه می شود 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 می نماییم.
- o توصیه می شود 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 می نماییم.
- توصیه می شود 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 می نماییم.

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

Upload certificate files <	•
Use this form to upload parts of the ce	rtificate (*.key, *.crt, *-ca.crt) that you
Private key *	Browse_
Certificate *	Browse_
CA certificate	Browse3
	Send File

- روش دوم: وارد نمودن دستی محتویات فایل های گواهی از طریق بخش Upload certificate as text:
- o 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 -----BEGIN RSA PRIVATE KEY
 و آن را درون جعبه متن مشخص شده در پنل Paste می نماییم (مانند شکل زیر).

Upload certificate as text 룾—	_	
Use this form to upload parts of the	certificate (*.key, *.crt, *-ca.crt) that you own, as a text. Copy the fi	iles content and
Private key *	BEGIN B3A PRIVATE KEY MIICXgIBAAKBgQC=Yw8tRFm8oPm8Gx+C+i2B5nNnliRNIzbQf2twxy9Bk=L3Imi4 tkdYf2r1+GNT7gg3+1W6fHpUNHWCo4SiGk18reQx3DR4bBoY5P/mjainUlEBq3 ucE92tesQ74sLnAA01XCWHtw0fkQyytugCANjfE4qj7DmfrGwcH88Vwg0QIDAQAB AgGAQ2E/8YjAlQDpV8m9N5Uuf+0GUgOCa7CMJcuBMxkfuUI4E8Wr33vtxKfrCcF oxN8MjnUgdyuh7hVcQPwsw5HMwqR5WirsB0mAKR2RMvQg37mDYeYTuvqNT7Yt5u 5/Yg1W+c3rQ2s2ZQfcAdqCLX92RTduMJdhfyL+TKochgCQODgtEUFtr8cHMX I+DAdeK08M82ot8/j4Gan409ca02K7i+WuEvEmYW1M7ax93ao/Jy2vV8dWAV70TU EyW6Kg1xAkEAx6VxBw8WgYN1r/rU0HWVRy4QAQKHch2q2hQd11YVFu1a7KFky hvLg+PsQ2jdm6MCDkByKcV1YQ1kyAcjdYQJBA1hD6eNydayaYmUuRLq3ArKVGNy qf3AugjJn3ybxixqfo505UX22Fb20ueik6d41NBwAuoQKLgW/Ps9Y+UY+DgEQQCI wirGw5bkcMWBxPrW1zRyR5nC+Ax10TxAB8A23fTP46iS047wNcyddBt8xTdSN1o0 02/Lh1RRLLk4L+Vxo2BAkEAp3Fa9hSgnLRuWRmk3jV3VNIJ4txofeNM02PAosa EvYDF1oxLHNctgIvVAnHpshw9HJXxw0wBmF/Qf290vUg== END B3A FRIVATE KEY	

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
 Paste می نماییم (مانند شکل زیر).

Certificate *	BEGIN CERTIFICATE	
-	MIIDdjCCAt+gAwIBAgIBIzANBgkqhkiG9w0BAQUFADBJMQswCQYDVQQGEwJJUjEM	
	MAoGA1UEChMDYW1uMQwwCgYDVQQLEwNwa2kxHjAcBgNVBAMWFXJvb3Rfc2VsZ19z	
	aWduZWRfdGVzdDAeFw0xMjEwMzAyMDU1MjFaFw0xMzA4MjYyMDU1MjFaMFYxCzAJ	
	BgNVBAYTAklSMRkwFwYDVQQKExBOb24tR292ZXJubWVudGFsMREwDwYDVQQLEwhh	
	bW5hZnphcjEZMBcGA1UEAxMQd3d3Lm15ZG9tYW1uLmNvbTCBnzANBgkqhkiG9w0B	
	AQEFAAOBjQAwgYkCgYEArGMPLURZvKD5vBsfgvotgeZzZ5YkT3M20H9rcMcvQZLC	
	9yJouLZHWH9qyPhjRU2aUvtVren28izZx1gqOEohpNfK3kMdw0eG0qGOT/5o2op1	
	JRAat7nBPdrXs00+LC5wANNVw1h7cNH5EMsrboAgDY3xOKo+w5nxXFnB/PFcINEC	
	AwEAAaOCAV8wggFbMIH4BgNVHR8EgfAwge0wMaAvoC2GK2h0dHA6Ly93d3cucGFy	
	c3NpZ25jYS5pci9jbGFzczEvUFNfQ0FMMS5jcmwwgbeggbSggbGGgz5zZGFwOi8v	
	cGFyc3NpZ25jYS5pci9jbj1QYXJzU21nbiBQcm12YXR1IE1udGVybWVkzWF0ZSBC	
	cm9uemUgQ0EgLUcyK3N1cmlhbE51bWJ1cj02MTA1MzQ5NDAwMDAwMDAwMDAwNCxk	
	Yz1sZXZ1bDEsZGM9SW50ZXJtZWRpYXR1IENBLGRjPUcyLGM9aXI/Y2VydG1maWNh	
	dGVSZXZvY2F0aW9uTG1zdDtiaW5hcnkwQQYDVR0gBDowODA2BgdggmxlAQEBMCsw	
	KQYIKwYBBQUHAqEWHWh0dHBzOi8vd3d3LnBhcnNzaWduY2EuaXIvY3BzMBsGA1Ud	
	EQQUMBKCEHd3dy5teWRvbWFpbi5jb20wDQYJKoZIhvcNAQEFBQADqYEADuNOVm2c	
	ABDKmSuorwr0du6vLb+UTnrPcjmM8G+1zFN672qUcQjKZ7Zrhsr2jR1ec6CiimRD	
	eQCOoJ2wK4KUc7GvBLCbbiY6yx46DH64BXzyi6OzoUwKMbU2nHUrpUYk3WBHDjF1	
	h3xcvVM3w3FigNFZG1wwFN5V2JwjT605gkA=	
	END CERTIFICATE	

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 مشخص شده در پنل Paste می نماییم.
 دقت کنید باید کل محتویات فایل، از جمله عبارات -----BEGIN CERTIFICATE ----- و
 END CERTIFICATE----- کپی شوند (شکل زیر).

CA certificate	BEGIN CERTIFICATE	
-	MIIEIzCCAwugAwIBAgIKYQU01AAAAAABDANBgkqhkiG9w0BAQUFADArMSkwJwYD	
	VQQDEyBJc2xhbWljIFJlcHVibGljIG9mIElSQU4gUm9vdCBDQTAeFw0xMjA3MTgx	
	MDE3MjRaFw0xNTA3MTgxMDI3MjRaMIGVMQswCQYDVQQGEwJJUjEPMA0GA1UECBMG	
	VGVocmFuMRkwFwYDVQQKExB0b24tR292ZXJubWVudGFsMREwDwYDVQQLEwhBbW5h	
	ZnphcjERMA8GA1UEC*MIUGFyc1NpZ24*NDAyBgNVBAMTK1BhcnNTaWduIFByaXZh	
	dGUgSW50ZXJtZWRpYXR1IEJyb256ZSBDQSAtRzIwggEiMA0GCSqGSIb3DQEBAQUA	
	A4IBDwAwggEKAoIBAQCurmHtebcrdZuV1v4jdtXHV4f2141Ce4RqvMzs0cyYhv2G	
	pvn52nffVoY2UEHhUdq82U45bkFMLTgt0FThmtAlXGZAA3MzN6z9bkmZ1irmENZs	
	7xzJcEYPDhDgp1K1A4qNy09+nzbTTASfNJ9iquBspyMHjGH63AwAFuhqVhWftsy+	
	KlkTelos1Rbft65YCGdnt+suCB+VS7vD8jke8c0i4wXr+CpUYQkrxk4q1cFMNz5w	
	kzdDURsVxZ8CfT1mbE/XEex2K7800LR7Cv+taFrn2QwiQUMp6erHmaUC3qGP01DC	
	VN52h0dWkT020cCUgvCK1G5Ux0v97TAGEoCgn10pAgMBAAGigd0wgdowCwYDVR0P	
	BAODAGGGMBIGA1UdEwEB/wOIMAYBAf8CAOAwHOYDVR0OBBYEFHJUpVKGgtZhZfw3	
	FudnbIF05XC1MEUGA1UdIAEB/w07MDkwNwYHYIJsZOEBATAsMCoGCC=GAOUFBwTB	
	Fh5odHBwcsovL3d2du5wYXJzc2lnbmNhJmluL2NwcsswHwYDVR0+BBcwFoAU+2Cf	
	noveNetXHUL5/H2+bn73+XOwM3VDVB0fBCtwJa31oCOgIVVfsHD0xDowI2NwbC5*	
	V2P. 22021 - 1 - 1 21 MAR A WART DANE - b - b - CO-OF 3 OF 3 OF 3 OF 3 - 21 + 1 - 70 + 4	
	ogbut:/irokyikogkviikLukoLibyg+bzorgi3004JonbgkleSibijbiiugbykui	
	WIERE/GOVCTOREDUCES/DINVW/ERADOWVJETIEMWEITRGOOTGDV19202000	
	ziu24KswijQQAAvjKeOVBhilRkoxmBMDOGA4G16pTJeainrmkuJUF8rmBUmVUJPa	
	29JSyNPpdnjrBUVIV6Vorsr2JSiztBi/jBCIKdDetVkmAl8Trulpdrch10f3r11G	
	HPbrRDjXegcxhOE4OXxgyDyTmjOG7LGa2LzTAx43Ge74ThmerBkMC91WcL5N7N9S	
	N1Paq9r5HA==	
	END CERTIFICATE	
	BEGIN CERTIFICATE	
	MIIDMjCCAhqgAwIBAgIQaLN1ky6wrrpPBwuY13ckSzANBgkqhkiG9w0BAQUFADAr	
	MSkwJwYDVQQDEyBJc2xhbWljIFJlcHVibGljIG9mIE1SQU4gUm9vdCBDQTAeFw0w	
	ODAxMDIxODEwNTBaFw0yODAxMDIxODE5MjBaMCsxKTAnBgNVBAMTIE1zbGFtaWMg	
	UmVwdWJsaWMgb2YgSVJBTiBSb290IENBMIIBIDANBgkqhkiG9w0BAQEFAAOCAQ0A	
	MIIBCAKCAQEA1JWcPksZsa1cTOEkRVu/UwHOog/q1uOxsQL0aF660kuUiTDQBAie	
	zKrOp4yYDaXy1kV/GAEvQdQ1bDL+sSpDG1jwgxHCWgJ/cILvwYb2Grm9/pHgjSg+	
	VqJyjHHHG1DZU9V/ngRzpjkLfokt16WQe4DRxiJyisnoEDxjSdM9dQYHRt/HhYjW	
	BjXLtQokwMRssfa01McBbtCj0ADsS10xOKpfM2VyDqHA34KqvcDItS3IUrfcbQnz	
	PD/yYM129fEb1RUd1XfUgD20DEx9RwVtgt0b8PFTE0au57jBBD0/60GF0fwDvmpQ	
	6VrtFORheYzrCwfip97Mn30FpYCxyxp4dwIBA6NUMFIwCwYDVR0PBAQDAgGGMBIG	
	A1UdEwEB/wQIMAYBAf8CAQUwHQYDVR00BBYEFPtwn6asrDcx1x1C+fx9vm5+wP10	
	MBAGCS=GAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQDBrBX2fqXjX2q3	
	DrVAMaLK7bNc1X+g8uEw2LCRmBoOgr0/1jjMFoOCfWKKRUi1QyE0xTJ9gT7w25/H	
	V7uvSUl34JAEtmcogWNBSi5dYRCH+wf5Q0n/4zhYClnKJ3b01/FcVkKUZwmOWgOB	
	1gK1Rb9L3U7N3rFWbW2RJdCxXbP3eb0YENaGUXpuU03ZVujt1W8+0OaoDgemXOCU	
	8phLg/ic5fB61p/w+rOueT8Z4wmfOmDgPpW8fnbBBDVcmRn/BU+=01w/fTnb207J	
	rZu/TD/cgg/TPCisteVMOmHAoN2dutb2MpOY9voJKTOsiFg9EKKpgHO1wHowrbtr	
	RAWAmuVa	
	END CERTIFICATE	

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

Upload certificate as text

Use this form to upload parts of the certificate (*.key, *.crt, *-ca.crt) that you own, as a text. Copy the files content and paste into an appropriate field.

Private key *	BEGIN R3A PRIVATE KEY	
-	MIICXgIBAAKBgQCsYw8tRFm8oPm8Gx+C+i2B5nNnliRNIzbQf2twxy9BksL3Imi4	
	tkdYf2rI+GNFTZpS+1Wt6fbyLNnHWCo4SiGk18reQx3DR4bSoY5P/mjainUlEBq3	
	ucE92tesQ74sLnAA01XCWHtw0fkQyytugCANjfE4qj7DmfFcWcH88Vwg0QIDAQAB	.
	AcGAQZE/8YjA1QUpV8m9N5Uuf+0GUg0Ca7CMJcuBMxkfuUI4E8Wrr33vfxKfrCcF	
Certificate *	BEGIN CERTIFICATE	
	MIIDdiCCAt+gAwIBAgIBIgANBgkghkiG9w0BAOUFADBJMOgwCOYDVOOGEwJJUjEM	
	MAoGA1UEChMDYW1uMOwwCgYDVOOLEwNwa2kxHiAcBgNVBAMWFXJvb3Rfc2VsZ19z	
	aWduZWRfdGVzdDAeFw0xMjEwMzAvMDU1MjFaFw0xMzA4MjYvMDU1MjFaMFYxCzAJ	*
	BoNVBAYTAk13MRkwFwYDVOOKExBOb24tR292ZXJubWVudGFsMREwDwYDVOOLEwhh	
CA certificate	BEGIN CERTIFICATE	
art der en loade	MILEIzCCAwugAwIBAgIKYOU01AAAAAABDANBgkghkiG9w0BAOUFADArMSkwJwYD	
	VOODEvBJc2xhbWljIFJlcHVibGljIG9mIElSOU4gUm9vdCBDOTAeFw0xMjA3MTgx	-
	MDE3MjRaFw0xNTA3MTgxMDI3MjRaMIGVMOswCOYDVOOGEwJJUjEPMA0GA1UECEMG	*
	VGVocmFuMRkwFwYDVOOKEwB0b24tB2922XJubWVudGF=MREwDwYDVOOLEwbBbW5b	
	s	end Text

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.

Home > Subscriptions > mydomain.com > Websites & Domains > SSL Certificates	
Information: New SSL certificate was added. To make it work, be sure to select it in website hosting settings (at Websites & Domains tab > domain name).	
. در این مرحله باید گواهی SSL اضافه شده در Plesk را به وبسایت خود تخصیص دهیم. برای این	٩
منظور از منوی سمت چپ از بخش Hosting Services گزینه Domains را انتخاب مینماییم (شکل	
زير).	

Parallels Panel	
1 Home	
Hosting Services	
& Customers	
& Resellers	
@ Domains	-
Subscriptions	
G Service Plans	

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).

mydomain.com	😭 Website	Demo Admin, Parallels	Nov 4, 2012	-	0.1	8 0 8	/month	View Site	A Manag	ge hosting
يم (شكل زير).	خاب میکن	را انت	Websites	&	Domains	گزينه 8	بىفحە،	بالاي م	منوى	۱۱. در
Home > Subscriptions > mydomain.com	n								🔒 Up Le	evel
General Summary	Users Webs	ites & Dor	mains Mail	Арр	lications Fi	ile Sharing	Statistic	Accour	nt	

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

Show Advanced Operations						
A website is a collection of related web pages, images, videos, and other files that are accessible by a common domain name. Here is a list of your websites, from which you can change website hosting settings, open a website directory in file manager, view statistics on website visits, install an SSL certificate, view web server logs, and change DNS zone settings.						
🛃 Add New Domain 🛛 🔏 Add New	🐻 Add New Domain 🛛 😪 Add New Subdomain 🕡 Add New Domain Alias 🛛 🚯 Register Domain Names					
🧔 Manage Domain Names 🛛 🍿 Remove						
1 items total		Number of entries per page: 10 25 100 All				
Domain 🔺	Hosting					
mydomain.com	🕋 Website at httpdocs	🔤 🖴 🔆 🗳 🗐				
1 items total		Number of entries per page: 10 25 100 All				

۱۳.در صفحه General، نام وبسایت باید همان نام وبسایت باید همان نام پیش فرض 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 می کنیم (تیک می زنیم). از قسمت Certificate، گواهی با نامی که در مرحله ۶ برای آن قرار دادیم (در مثال ما، (تیک می زنیم). از انتخاب می کنیم. همان طور که در شکل زیر ملاحظه می کنید در کنار نام گواهی، از می می نیم در مثال ما، می نیم می نیم می نیم می نیم انتخاب می کنیم (تیک می زنیم). از انتخاب می کنیم در مده با نامی که در مرحله ۶ برای آن قرار دادیم (در مثال ما، از می می نیم). می کنید در کنار نام گواهی، با نامی که در مرحله می کنید در کنار نام گواهی، نام وبسایت متناظر آن (در مثال ما، می کنیم) نیز درج شده است.

Home > Subscriptions > mydomain.co	m > Websites & Domains > or mydomain.com
General PHP Settings	
Here you can configure website	hosting settings and select the features available
Domain name * 🗲 🗕	Domain name is the website's Internet address. hosting providers.
Hosting type	Website [Change] [Suspend]
Document root *	fraction for the second
Security	
To secure transactions with your and login areas of your site, as v site and 2 selected in the site	site, use SSL which encrypts all data and transfe vell as any other areas where such data can be tr e's hosting settings.
Enable SSL support	3
Certificate	mydomain_cert (mydomain.com)
	The certificate change will also affect other sit

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

📝 Enable SSL	support
Certificate	Default Certificate (other repository) 💌
	The certificate change will also affect other sites hosted on the same
Web Scripting	g and Statistics
Specify which web server.	of the following programming and scripting languages should be interpreted, executed or
Microsoft A	ASP support
📝 Microsoft A	ASP.NET support (Version 2.0.50727.1434)
PHP suppor	rt (Version 5.2.17 , run as FastCGI application)
CGI suppor	t
Perl suppor	t
V Python sup	port
AWStats 💌	Web statistics (accessible via password-protected directory '/plesk-stat/webstat/' 🗐)
🔽 Custom err	or documents
🔲 Additional	write/modify permissions
* Required fiel	lds OK Cancel
مات این بخش	نکته : در شکل بالا، تکمیل گزینههای مرتبط با گواهی SSL عنوان شده است و سایر اطلا [۔]
معنا نیست که	به نصب گواهی SSL در Plesk مربوط نمیباشد. به عبارت دیگر، شکل بالا به این ا
	گزینههای نشانداده شده باید مانند شکل، فعال یا غیرفعال باشند.
	۱۵.پیغامی مبنی بر موفق بودن اعمال تغییرات جدید ظاهر میگردد (شکل زیر).
	Home > Subscriptions >
	mydomain.com
	Information: The settings were successfully updated.

General Summary Users Websites & Domains Mail

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 می کنیم (شکل زیر).



IV. در صفحه Tools & Settings، روی گزینه Services Management از بخش Tools & Settings.

کلیک میکنیم (شکل زیر).



۱۸. در صفحه Services management، سرویس وبسرور را انتخاب نموده و روی گزینه Restart کلیک



© Copyright Amnafzar Co.

Service

۵ بررسی صحت نصب گواهی SSL

برای برقراری ارتباط صحیح SSL میان مرور گر کاربر و وبسایت، کاربر وبسایت باید زنجیره گواهی را روی سیستم یا مرور گر 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 مرور گر، www.parssignca.ir دانلود و مطالعه نمایید. پس از نصب صحیح زنجیره گواهی، در نوار آدرس مرور گر، آدرس https://www.mydomain.com را وارد مینماییم (به جای www.mydomain.com باید آدرس <u>دقیق</u> سایت خود را وارد نمایید). نمایش علامت قفل به همراه عبارت shttps در نوار آدرس مرور گرها <u>یکی</u> از نشانههای صحیح بودن نصب گواهی SSL در وبسایت میباشد. نمایش علامت قفل در سه مرور گر Firefox به صورت زیر میباشد:

 مرور گر Google Chrome: در نوار آدرس (مطابق شکل زیر) قفل سبز رنگ در کنار عبارت سبز رنگ https ظاهر می شود.



۶ مشکلات احتمالی پس از نصب گواهی

۸–۶ 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:

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

/ mydomain	×
$\label{eq:constraint} \boldmath ${\ensuremath ${\ensur$	https://www.mydomain.com

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

+ ttps://	ww.mydomain.com
	This website does not supply identity information.
	Your connection to this site is only partially encrypted, and does not prevent eavesdropping.
	More Information

مرور گر 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).

+ > 2 - 🚯 https://www.mydomain.com/

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

+ 🔄 https://www.mydomain.com/

این مشکل معمولاً Mixed content warning نامیده می شود که ممکن است یک حمله کننده 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 می باشد. دلیل مشکل این دلیل

Ċ

۱۸

است که در وبسایت شما از محتوای ناامن استفاده شده است. مثالهایی از محتوای ناامن، عکسها، اسکریپتها، یا CSSهایی هستند که به طور ناامن (از طریق HTTP) در سایت شما بارگذاری می شوند. مرورگر از بارگذاری یا اجرای این محتواها جلوگیری می کند. به همین دلیل ممکن است CSS وبسایت شما بارگذاری نشده و ساختار وبسایت شما با HTTP به هم بریزد، عکسی بارگذاری نشود، یا اسکریپتی اجرا نشود. برای کشف محتوای ناامن، می توانید از قابلیت Toolbar در اغلب مرورگرها

استفاده کنید. کشف محتوای ناامن با استفاده از مرورگرهای رایج معمولاً به صورت زیر میباشد:

- مرور گر Google Chrome و Internet Explorer: فشردن کلید F12 و مشاهده خطاها در بخش Console.
- مرور گر 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.
- CSS مثال، صورت سايت کنید فرض • برای به 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 نمی شود (در نتیجه ساختار سایت بهم میریزد). بنابراین توصیه می شود به جای استفاده از آدرس های قطعی (hardcoded) برای عکس ها، CSS، و اسکرییت های 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 آدرس دهی نسبی استفاده کنید اما مشکل همچنان باقی باشد، مشکل مربوط به تنظیمات SSL در سرور شما ميباشد.
- 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

¹ Content

© Copyright Amnafzar Co.

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 اسکرپیتهایی است که با استفاده از http اطلاعاتی را از سایت ما برای سایت دیگری (مثلاً برای یک سایت ثبت آمار کاربران) ارسال میکنند. همچنین، اسکرپیتها، عکسها، و غیره که از سایت دیگر به صورت http در سایت ما بارگذاری می شوند. مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری میکند. در صورتی که امکان بارگذاری این محتواها از طریق http وجود ندارد، آنها از وب سایت خود حذف نمایید. روش دیگر این است که دو صفحه مجزا، یکی برای http و یکی برای http طراحی کنید؛ در صفحه مربوط به در تنظیمات SSL روی سرور، در خواستهای SSL را به آدرس صفحه همجوای ناامن را حذف کنید. سپس در تنظیمات LSS روی سرور، در خواستهای LSS را به آدرس صفحه ور از از سایت مذکور در تنظیمات LSS روی سرور، در خواستهای کاک را به آدرس صفحه در از سایت مذکور در میگر 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:

مرور گر Google Chrome: پیام زیر نمایش داده شود.



• مرور گر Firefox پیام زیر نمایش داده شود.

You have asked Firefox to connect securely mydomain.com but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
parssignca.ir uses an invalid security certificate.
The certificate is only valid for' <u>www.mydomain.c</u> om
(Error code: ssl_error_bad_cert_domain)
I Understand the Risks



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
 اگر گواهی برای را در مرورگر وارد نمایید، با صفحه خطای فوق مواجه می شوید. برای رفع این
 مشکل، یا باید همیشه آدرس دقیق وارد شود یا راه حل 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
 می شوید. 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 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' نیز وجود داشته باشد (مثلاً mail.mydomain.com). حال اگر آدرس https://mail.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می شوید. 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، می توانید درخواست گواهی لیاید.

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 نمی تواند تشخیص دهد چه سایتی را برگرداند).

© Copyright Amnafzar Co.

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.

√ پيوست

Plesk رویه اختصاصی کردن آدرس IP وبسایت در IP

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 & Resources، از بخش Tools & Resources گزینه IP Addresses را انتخاب می کنیم

(شكل زير).

Tools & Settings This is where you manage the server, an Tools & Resources IP Addresses Virtual Host Template SSL Certificates Shared SSL Mass E-Mail Messages Backup Manager Backup Settings Scheduled Tasks Event Manager

۳. در صفحه Add IP Address گزینه Add IP Address را انتخاب می کنیم (شکل زیر).
 ۳. IP addresses management
 View, add, remove IP addresses, and assign IP addresses to resellers.
 Add IP Address
 IP Reread IP
 IP Firewall

۴. در صفحه Add IP address را که از مدیر سرور IP اختصاصی و Subnet mask را که از مدیر سرور (هاستینگ) دریافت نموده ایم در مقابل IP address and subnet mask وارد نماییم. برای مثال، در شکل زیر فرض می کنیم آدرس IP اختصاصی وب سایت 192.168.200.1 باشد و ۱۶ بیت از آدرس IP شکل زیر فرض می کنیم آدرس IP اختصاصی وب سایت IP address and subnet mask رای زیر فرض می کنیم آدرس IP اختصاصی وب سایت 192.168.200.1 باشد و ۱۶ بیت از آدرس IP برای زیر شبکه در نظر گرفته شده باشد. ۱۹۵۸ می توان وارد نمود. سپس در بخش رای در بخش IP address and subnet mask می توان وارد نمود. سپس در بخش IP address and subnet می کنیم.

Home > Tools & Settings > IP address	ses management >
Interface	"Local Area Connection" 💌
IP address and subnet mask *	192.168.200.1/16
IP address is distributed as 2	For example, 2002:7b7b:7b7b::1/64, 123.123.123.123/16, Shared Oedicated
SSL certificate	Default Certificate 💌
Allow FTP over SSL	
* Required fields	OK Cancel

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

IP addresses management	
Summation: The IP address 192.168.200.1 was added.	
View, add, remove IP addresses, and assign IP addresses to resellers.	
📾 Add IP Address 🤣 Reread IP 🛛 🕅 Firewall 🎁 Remove	
2 items total	
IP Address A	Subnet Mask
192.168.200.1 (dedicated)	255.255.0.0
ی IP اختصاصی را به وبسایت خود تخصیص دهیم. برای این منظور، از منوی سمت	 حال باید آدرس
Hosting Services گزینه Domains را انتخاب میکنیم (شکل زیر).	چپ، در بخش
Parallels Panel Home Hosting Services Customers Resellers Domains Subscriptions Service Plans	
ببسایتهای موجود، روی نام دامنهای که قرار است گواهی SSL برای ان نصب شود mydomain.co)، کلیک میکنیم (شکل زیر).	 ۷. در لیست نام و ۳. (در مثال ما، m)
mydomain.com	ite 📮 Manage hosting



IP address مقدار IP address از لیست آدرسهای IP موجود مقدار IP address را آدرس IP میکنیم. دقت کنید که در کنار 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 نمی شود. به عبارت دیگر، شکل زیر به این معنا نیست که گزینههای نشانداده شده باید به مانند شکل فعال/غیرفعال باشند.

Home > Subscriptions > mydomain.com > Websites & Domains >

Web Hosting Access

Here you can view the IP addresses associated with your subscription and change the userna Additionally, File Manager works with files and folders on behalf of this account.

IP Addresses	1
IP address	192.168.200.1 (dedicated)
	IP address on which the website is hosted is a network add
User Account	
System user account used for mar	naging files and folders within the subscription.
Username *	test
Password	Medium (?)
Confirm password	•••••
Access to the server over Remote Desktop	Login prohibited Access to the server over Remote Desktop with system use
Hard Quota on Disk Space	a limit on the amount of dick space that can be used. If th
The hard quota on disk space is th	le unit on the amount of disk space that can be used. If th
Hard quota on disk space *	MB Unlimited
2	
* Required fields	Cancel
ى شود.	 پیغامی مبنی بر موفق بودن اعمال تنظیمات جدید ظاهر م
mydomain.com	
Information: Hosting set	tings were successfully updated.
General Summary U	sers Websites & Domains Mail Applications

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 میباشد.

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

در صورتی که 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 روشه ۶۴ بیتی، OpenSSL-Win64 می رفته. در پوشه ۶۴ می می اشد) و وارد پوشه bin می شویم. در پوشه bin می فایل اجرایی OpenSSL به نام openssl.exe وجود دارد. این فایل را اجرا می کنیم 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 ذكر است كه اگر با ترمينال لينوكس كار مىكنيم، فرمان زير را به جاى دستور فوق بايد وارد نماييم: 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 می شود.

لازم به ذکر است که برای هر یک از فایل های 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 /home/keys در مسیر mydomain.key اگر با ترمینال لینوکس کار میکنیم، فرض میکنیم فایل mydomain_new.key در مسیر ذخیره شود. در قرار داشته باشد و میخواهیم فایل mydomain_new.key نیز در همین مسیر ذخیره شود. در این صورت، 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 می باشد:

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:

 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

PEM نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM

از روی پسوند گواهی، نمی توان 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 می نماییم. در صورتی که فایل با عبارت -----BEGIN CERTIFICATE----- شروع و به -----END CERTIFICATE می باشد.

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

- روش اول: در ویندوز می توانیم 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).

ield	Value
Version	V3
Serial number	22
Signature algorithm	sha 1RSA
Signature hash algorithm	sha1
Issuer	root_self_signed_test, pki, am
Valid from	Sunday, October 21, 2012 10:
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Cabuday, Ave. at 17, 2012 10
Valid to	Saturday, August 17, 2013 10
Valid to	Saturday, August 17, 2013 10



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

۶. در پنجره Export File Format در بخش Select the format you want to use گزینه (مانند Next) کلیک می کنیم (مانند Next) کلیک می کنیم (مانند شکل زیر).

Expo	rt File Format Certificates can be exported in a variety of file formats
2	certificates can be exported in a variety of the formats.
1	Select the format you want to use:
	DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Microsoft Serialized Certificate Store (.SST)
earr	n more about <u>certificate file formats</u>

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

×
port
Browse
2
< Back (Next >) Cancel

۶. در پنجره Completing the Certificate Export Wizard روی Finish کلیک می نماییم (مانند شکل



۷. پنجره زیر ظاهر می گردد که نشاندهنده ایجاد موفقیت آمیز یک گواهی جدید با فرمت PEM می باشد. در این پنجره روی OK کلیک می نماییم.

Certificate Ex	port Wizard
The export	was successful.
	ОК

• روش دوم: با استفاده از نرمافزار OpenSSL در لینوکس (که معمولاً بطور پیش فرض روی سیستمهای لینوکس وجود دارد)، میتوانیم عملیات تبدیل را انجام دهیم. بدین منظور، 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، DER است و فایل گواهی ورودی در فرمت DER است و فایل www.mydomain.com.cer فایل گواهی خروجی در فرمت PEM است. لازم به ذکر است در این دستور، باید آدرس دقیق فایل های مذکور را وارد نماییم. مثلاً اگر گواهی ها 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