

KTD-008 - Let's Encrypt SSL Sertifikası Kurulumu ve HTTPS Yapılandırması

Bu doküman Nginx Proxy Manager kullanarak Let's Encrypt SSL sertifikası almayı, HTTPS yapılandırmasını, Force SSL, HTTP/2 ve HSTS ayarlarını ve sertifika doğrulama adımlarını anlatır.

1. SSL Sertifikası Nedir?

SSL sertifikası istemci ile sunucu arasındaki iletişimi şifreler.

2. HTTPS Neden Önemlidir?

HTTPS veri güvenliği, kullanıcı güveni ve modern web standartları için gereklidir.

3. Let's Encrypt

Ücretsiz ve otomatik yenilenebilir SSL sertifikası sağlayan bir sertifika otoritesidir.

4. Ön Gereksinimler

- Domain doğru VPS IP adresine yönlenmeli
- 80 ve 443 portları açık olmalı
- Nginx Proxy Manager çalışıyor olmalı

5. SSL Sekmesi

Hosts → Proxy Hosts → Domain → Edit → SSL

6. Yeni Sertifika Talebi

SSL Certificate: Request a new SSL Certificate

Domainler:

- kemaltokmak.com
- www.kemaltokmak.com

7. E-posta ve Kullanım Şartları

Geçerli bir e-posta adresi girin ve Let's Encrypt kullanım şartlarını kabul edin.

8. Force SSL

HTTP isteklerini otomatik olarak HTTPS'e yönlendirir.

9. HTTP/2

Performans için HTTP/2 desteğini etkinleştirin.

10. HSTS

HTTPS kullanımını zorunlu kılar. Yapılandırma tamamlandıktan sonra etkinleştirilmesi önerilir.

11. curl ile Kontrol

```
curl -I http://kemaltokmak.com  
curl -I https://kemaltokmak.com
```

12. Tarayıcı Kontrolü

Adres çubuğunda kilit simgesinin görüldüğünü doğrulayın.

13. Sertifika Yenileme

`docker logs nginx-proxy-manager`

`certbot renew --dry-run`

14. Sorun Giderme

DNS kayıtlarını, 80/443 portlarını, Proxy Host ayarlarını ve Nginx Proxy Manager loglarını kontrol edin.

15. Özet

SSL sertifikası almayı, HTTPS yapılandırmasını ve sertifika doğrulamasını öğrendik.

Öğrenilen Komutlar

- `curl -I http://kemaltokmak.com`
- `curl -I https://kemaltokmak.com`
- `docker logs nginx-proxy-manager`
- `certbot renew --dry-run`