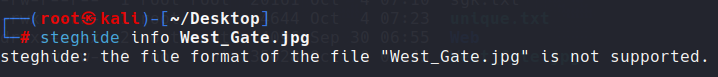
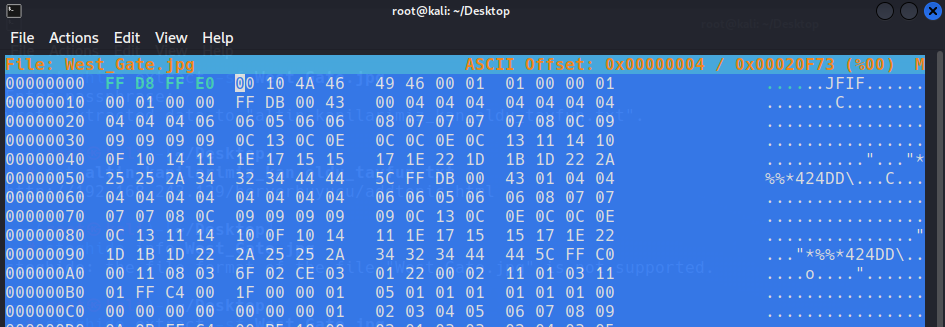
1. West.Gate.jgp adında bir jpg dosyası veriliyor ancak açmaya çalıştığımızda açılmıyor. Steghide info komutu ile baktığımızda dosya is not supported diyor.



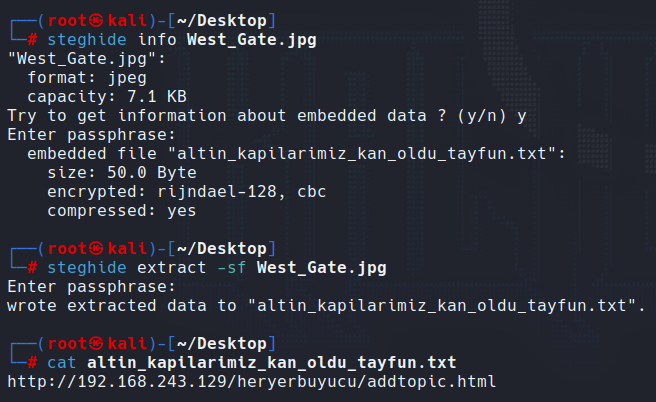
1. Dosyanın magic number jpg magic number’ından farklı. Bunun için dosyayı hexeditor ile açıp JPG için geçerli magic number’ı girdiğimizde dosya artık geçerli oluyor.



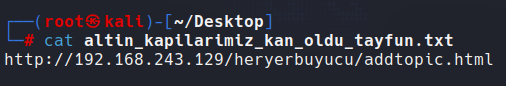
1. West\_Gate.jpg dosyasını açtığımızda görüntü bize Yüzüklerin Efendisi filminde geçen Moria Kapısını akla getirmektedir. Filmi bilmeyen bir kişi Google’da fotoğrafı aratırsa ipucu yakalayacaktır.



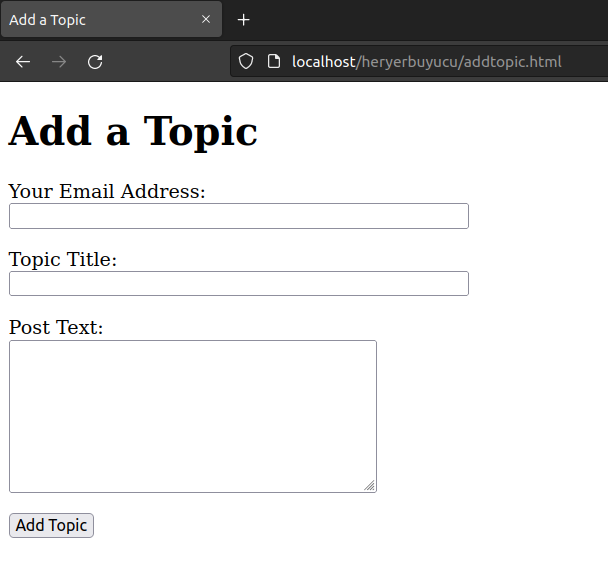
1. Terminalde bu dosyayı steghide aracı ile incelediğimizde içinde bir dosya olduğunu ve bunu çıkarmak için bir passphrase girmek gerektiğini görüyoruz. Görüntüdeki kapının üstünde Elfçe “Söyle, dost öyle gir” yazıyor. Filmde bu kapıyı açmak için Elfçe dost anlamına gelen “mellon” kelimesini söylemek gerekiyor.



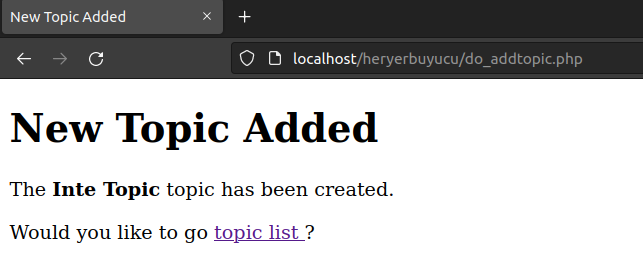
1. Bu anahtar kelimeyi girdiğimizde “altin\_kapilarimiz\_kan\_oldu\_tayfun.txt” adında bir text dosyası çıkıyor. Text dosyasında bir URL var.



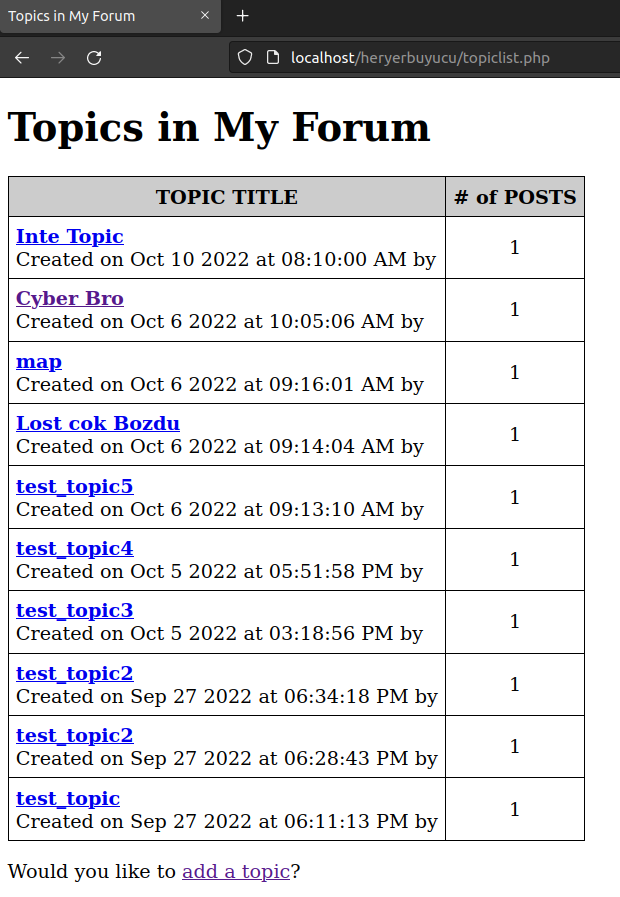
1. URL’i ziyaret ettiğimizde bir Post uygulaması bizi karşılıyor.



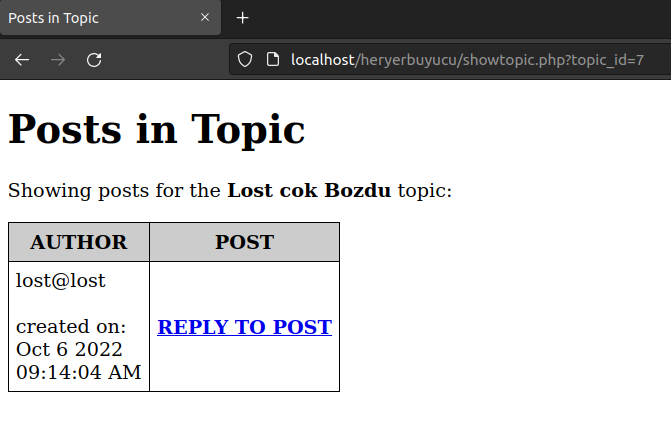
1. Bir post ekliyoruz.



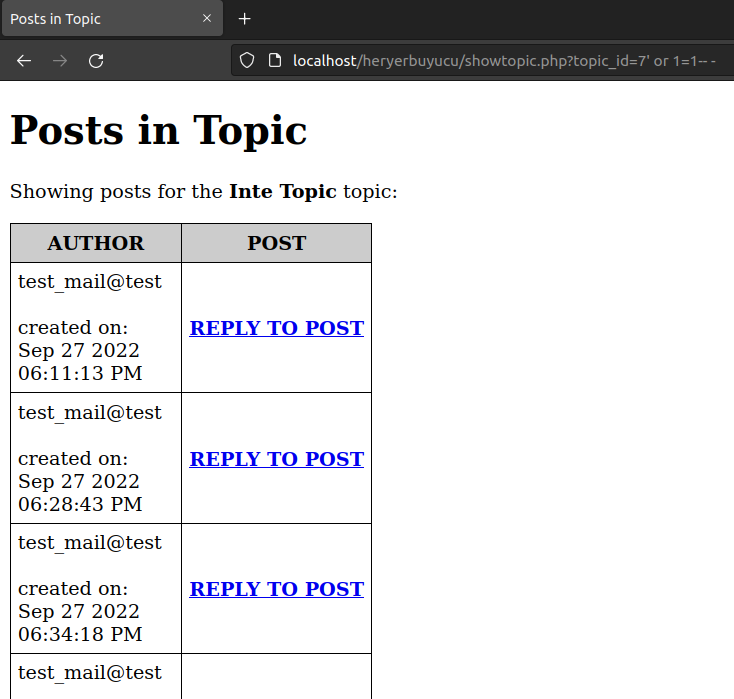
1. Sonrasında post başlıklarının bulunduğu sayfaya gidiyoruz.



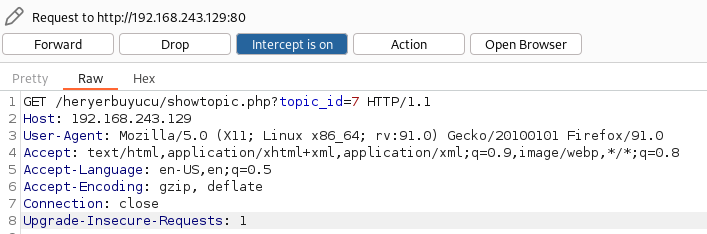
1. Bir post’u görüntülediğimizde URL’de topic\_id parametresi dikkatimizi çekiyor.



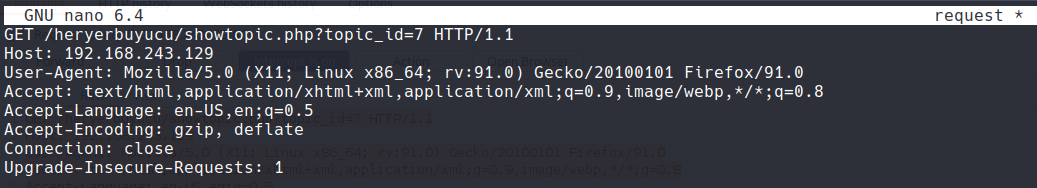
1. Bu parametreye SQL Injection denediğimizde (7‘ or 1=1-- - gibi bir payload) bütün postların listelendiğini görüyoruz.



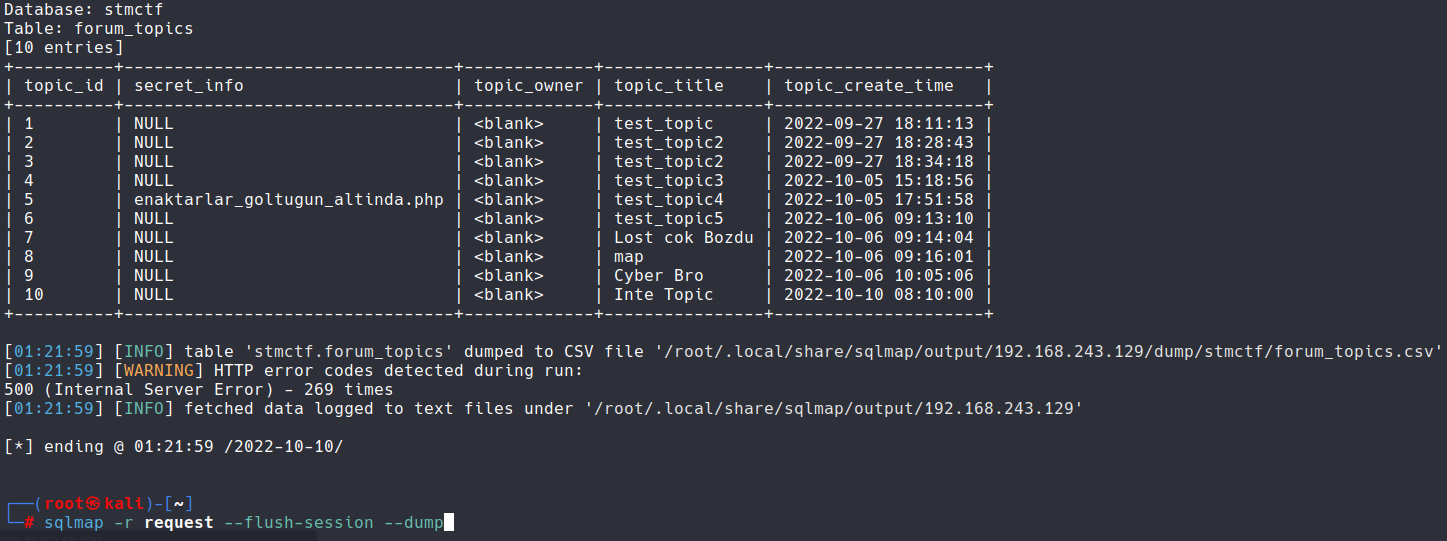
1. Sorguyu otomatize etmek için SQLMap aracını kullanacağız. Bunun için istek paketini SQLMap’e vermek gerekiyor. İstek paketini Burp aracı ile yakalıyoruz.



1. İsteği kopyalayıp bir dosyaya kaydediyoruz.



1. İsteği kaydettiğimiz dosyayı SQLMap’e veriyoruz ve SQLMap ile veritabanını dump’lıyoruz.



1. Dump edilen verilerde “secret\_info” adında bir kolonda “enaktarlar\_goltugun\_altinda.php” adında bir veri dikkatimizi çekiyor. Bu directory’e gittiğimizde flag elde edilmiş olunuyor.

