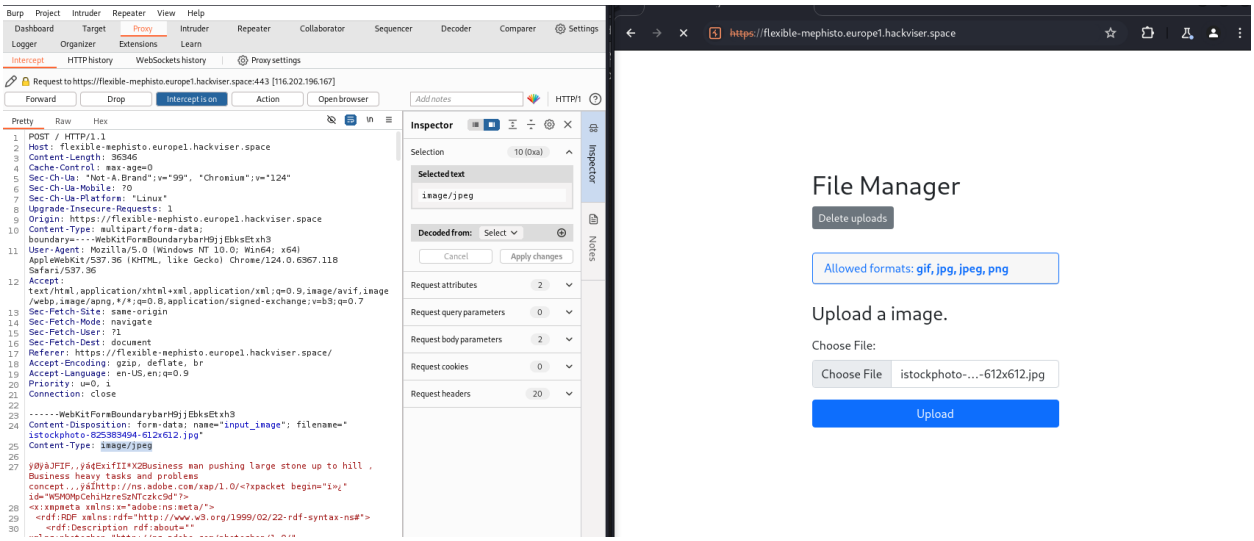
Unrestricted File Upload/ MIME Type Filter Bypass

Herkese selamlar bu yazımda Hackviser üzerinde bulunan Web security lablarından biri olan **Unrestricted File Upload/ Basic Unrestricted File Upload** çözümünü anlatacağım.

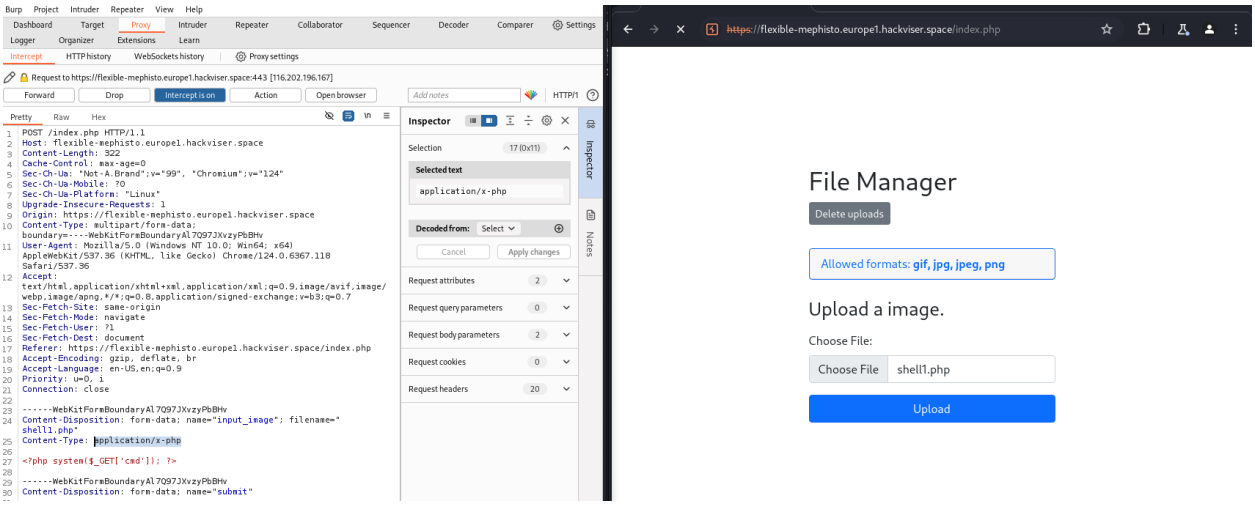
Bize verilen sitede çeşitli denemeler yaptıktan sonra bir sonuca varamıyorum.

Çeşitli uzantılı dosyaların içeriğine php kodu gömmeme rağmen herhangi bir sonuca ulaşamıyorum.

Ardından dosyayı değitşirmek yerine isteği değiştirmek aklıma geliyor ve isteği incelemeye başlıyorum

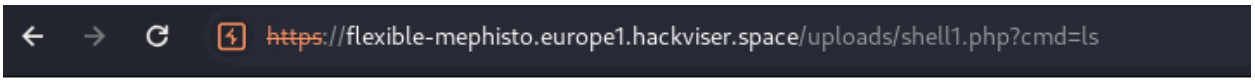


Bu kısımda “Content Type” kısmı dikkatimi çekiyor .jpg uzantılı bir dosya yüklediğim zaman Content Type image/jpeg oluyor.



PHP shell dosyası yüklediğimde ise Content Type application/x-php oluyor. Burada Content Type ı image/jpeg yapıp gönderiyorum. ve Başarılı bir şekilde yüklendi mesajını görüyorum.

Test etmek için ls komutunu kullanıyorum ve başarılı bir şekilde çalışıyor.



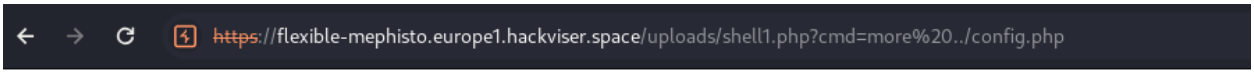
shell1.php

Bulunduğum dizinde birşey bulamadığım için üst dizine bakıyorum.

assets config.php delete.php index.php uploads

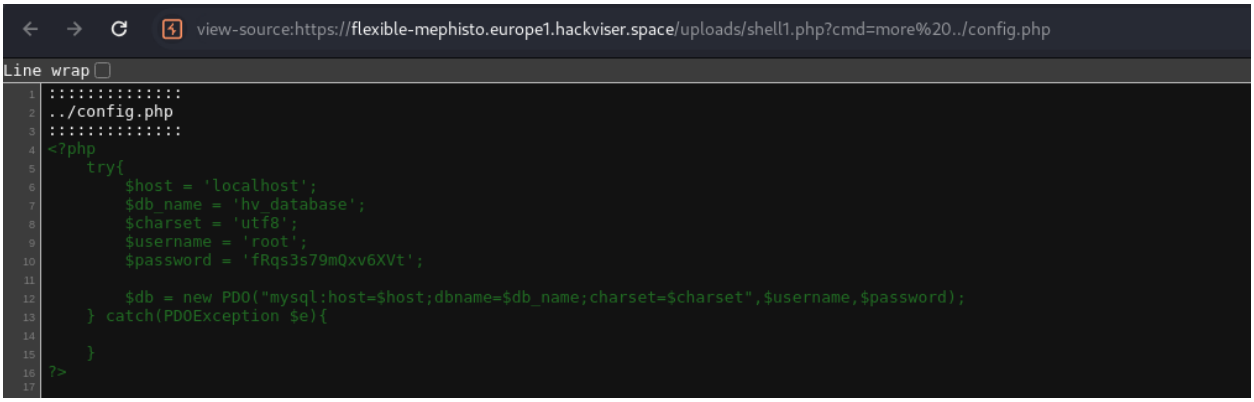
Ve aradığım config.php dosyasını burada buluyorum.

cat komutunu kullandığım zaman dosyayı yazdıramıyorum. bende more komutunu deniyorum.



:::::::::::::: ../config.php ::::::::::::::

Görünürde birşey yok ama kaynak koduna baktığım zaman aradığım şeyi orada buluyorum



Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.