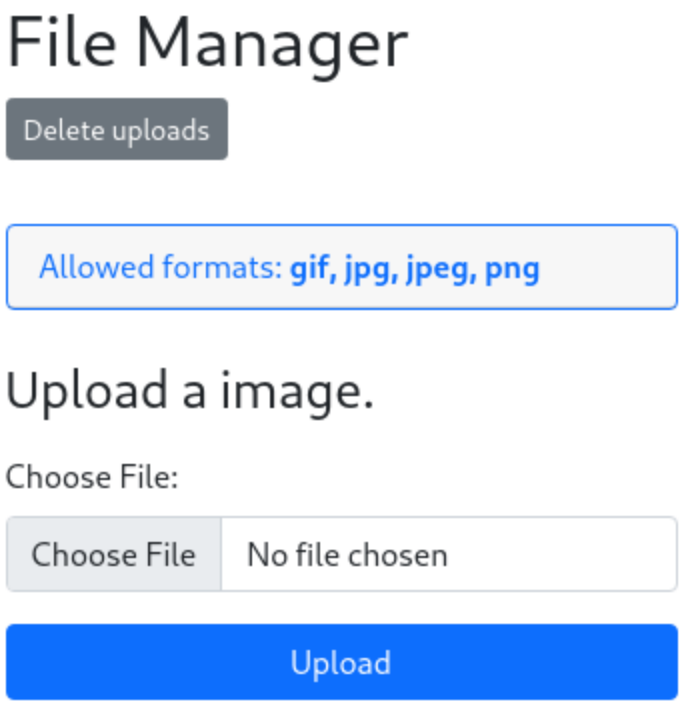
Unrestricted File Upload/ File Signature Filter Bypass

Öncelikle steye gittiüimizde bizi aşağıdaki gibi bir dosya yükleme ekranı karşılıyor.



Buraya çeşitli denemeler yaptıktan sonra başarılı bir sonuca ulaşamıyorum.

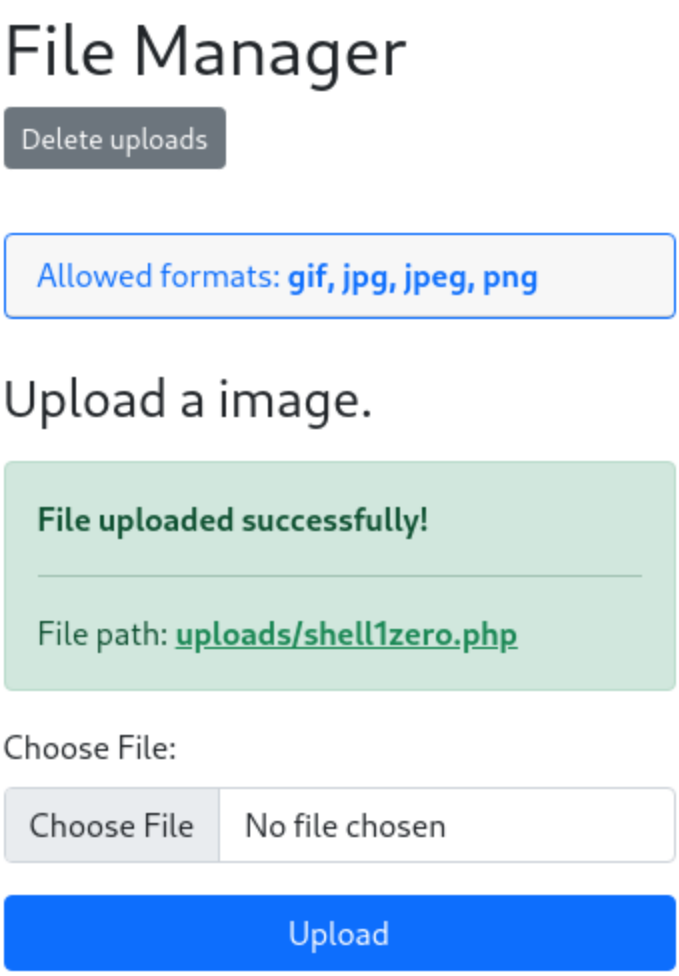
Aklıma soru da ipucu olarak da verilen magic bytes geliyor. Ve bunun için internette araştırma yapmaya başlıyorum.

https://medium.com/@wakedxy/bypassing-file-upload-restriction-using-magic-bytes-ae59fb5bb383

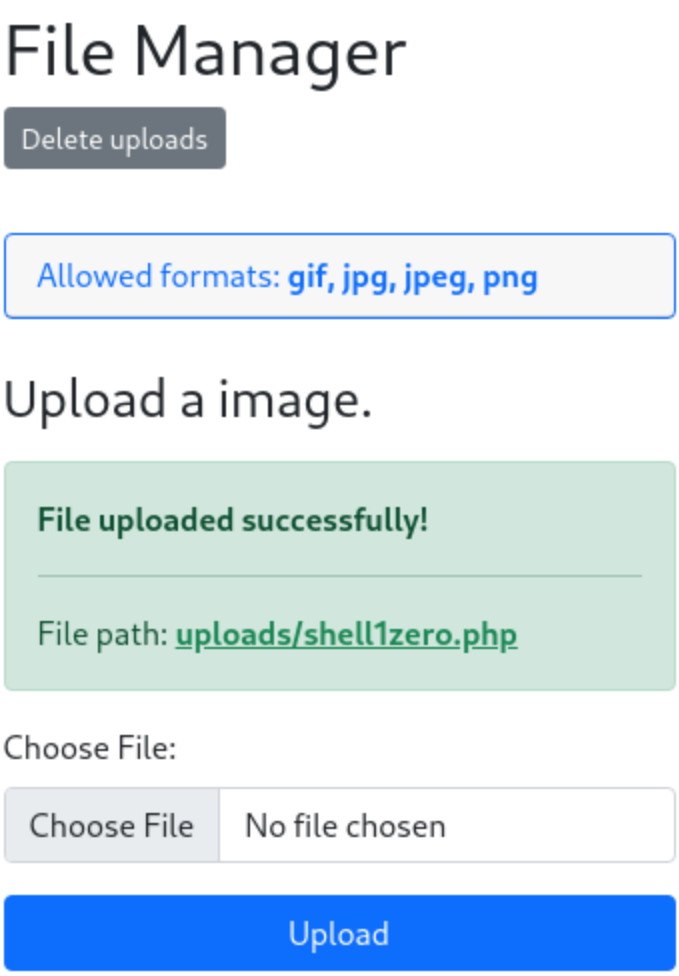
Araştırma yaparken bu yazıya denk geliyorum.

Burada GIF87a kullanarak bypass yapabileceğimi görüyorum.

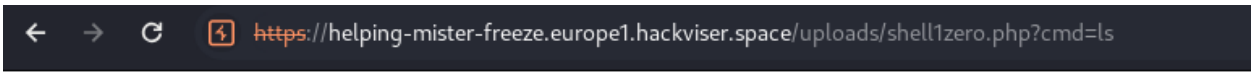
Aşağıdaki gibi bir payload hazırlayarak bunu göndermeyi deniyorum.



Ve başarılı bir şekilde dosyayı yükleeybildik.

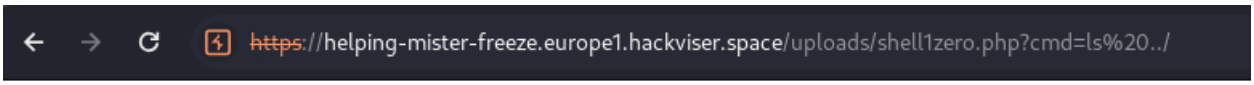


Sırada ise test etme kısmı var.



GIF87a shell1zero.php

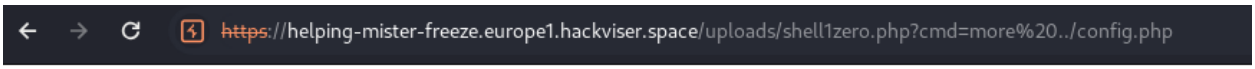
Ve başarılı bir şekilde çalıştı.



GIF87a assets config.php delete.php index.php uploads

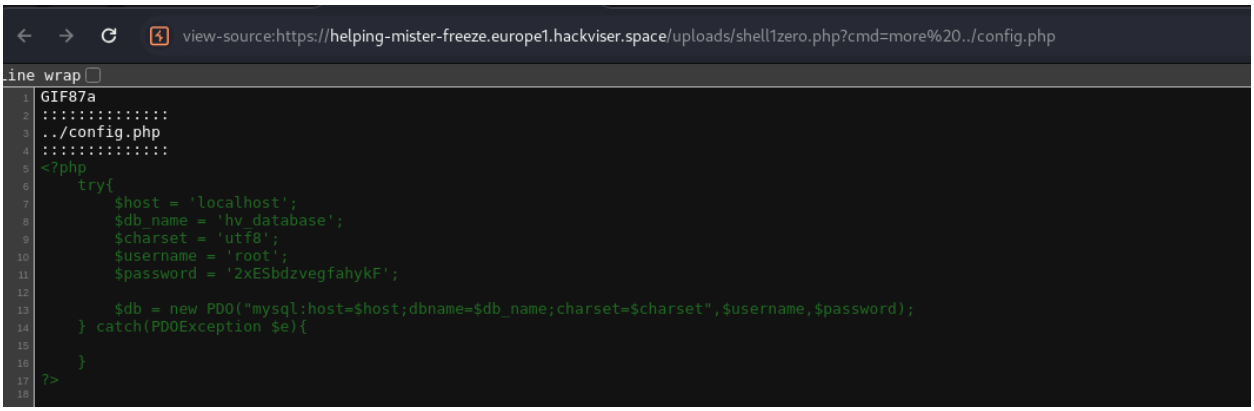
bu şekilde config.php dosyasını da bulduk.

Sırada ise içeriğini okumak var tahmin edeceğiniz gibi cat yine çalışmıyor bizde more komutunu kullanıyoruz.



GIF87a :::::::::::::: ../config.php ::::::::::::::

Sırada ise tekrardan kaynak koduna bakmak var.



Ve bu soruyu da böylece çözmüş olduk.

Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.