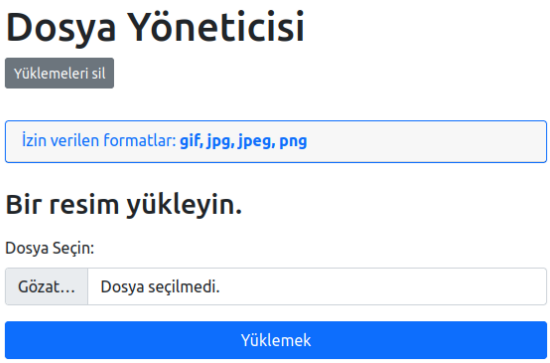
3. File Upload

File Upload Nedir;kullanıcıların web uygulamasına dosya yüklemesine olanak tanıyan bir işlevdir. Bu özellik, kötü niyetli kullanıcıların zararlı dosyalar yükleyerek sistemde güvenlik açıklarına neden olmasına yol açabilir.
Nasıl Önlenir;File upload işlemlerini önlemek için yalnızca belirli dosya türlerine (örneğin, .jpg, .png) ve maksimum boyut sınırına izin verilmelidir; ayrıca yüklenen dosyalar güvenli bir dizine kaydedilmeli ve dosya içeriği, uzantısı ile tutarlılığı kontrol edilerek zararlı yazılımların yüklenmesi engellenmelidir.

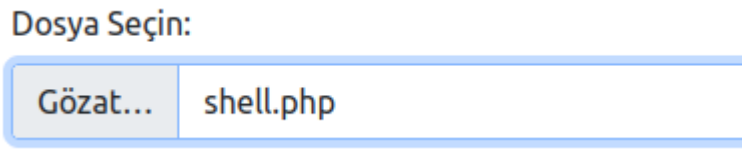
3.1 Basic File Upload

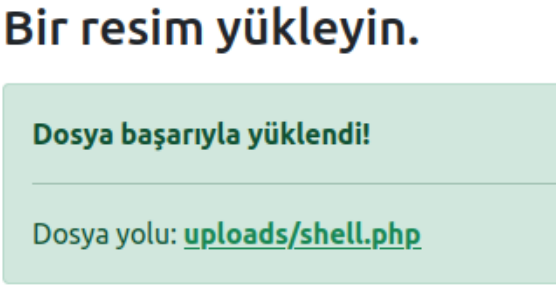
ÇÖZÜM

Karşımızda ki web adresimiz bu



İzin verilen formatlar belirtilmiş, ancak acaba yazılımcı filtreleme, yapmış mı test edelim.

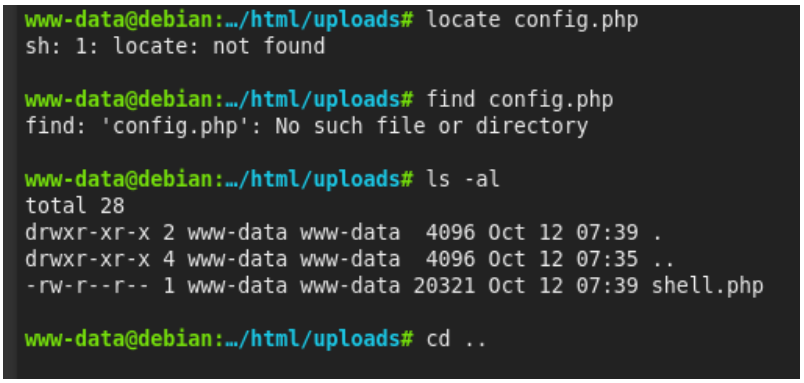




Evet yüklendi hatta , yazılımcının burada ki bir hatası ise dosya yolunu vermesi , çünkü biz php betiğini çalıştırırsak bu betil shelle ulaşıp shelli açıyor. Eğer bunu random bir isimle ve farklı bir dizin adıyla ve üstüne erişim kısıtlaması getirseydi urlden dosyamıza gitmeyi. Belki ulaşamicak veya başka bir bypasslama yöntemlerine başvurucaktık.

Ve shell.php ye gittiğmizde bizi karşılayan ekran bu;

Buraya komutlarımızı yazabiliriz.
Şimdi ise makinenin bizden istediği soruya bakalım. Config.php dosyasında ki veritabanı şifresi ne diye soruyor.



Burada dosya araması yapıyorum nerede diye , gizli dosyaları inceliyorum ancak bulamıyorum ama bir üst dizine gittiğimde görüyorum.

Cat ile okuyalım.

Ve cevaba ulaştık.
Soru: Config.php dosyası içerisinde ki veritabanı şifresi nedir?
Cevap: 8jv77mvXwR7LVU5v