|  |
| --- |
| ***File Upload*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| File Upload nedir ve Web for Pentester laboratuvarı üzerinde File Upload zafiyeti nasıl uygulanır bunun hakkında bilgi vereceğim. |

**30.07.2021**

***File Upload(Dosya yükleme)***

-Her web sitesinde mutlaka karşımıza çıkan,sunucuya dosya yüklemek için kullanılan bir uygulamadır.

-Web sitelerin upload bölümlerinde doğru filtreleme yapılmadığı zaman güvenlik açığı diyebileceğimiz durumlar oluşur.

-Örneğin bir web sitesinde kullanıcı profil resminin değiştirilmesi için konulan bir “File Upload” bölümü doğru şekilde yapılandırılmazsa,resim yerine zararlı dosya sisteme yüklenebilir.

-Bu sebeple File Upload bölümleri önce manuel olarak test edilmelidir.

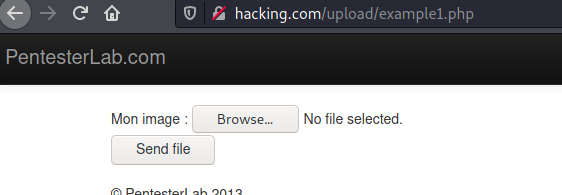
-File upload zafiyeti için WFP üzerinden 2 adet uygulama gerçekleştireceğiz.

**Uygulama 1 :** Temel Kullanım

- Birinci uygulamamızda .php uzantılı bir dosya bile rahat bir şekilde yüklenebiliyor.

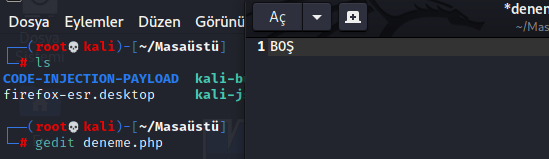


-Skipfish bu zafiyeti basit düzeyde bir zafiyet olarak yorumlamış.

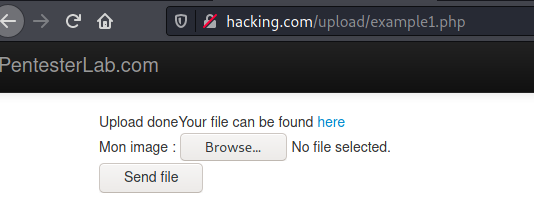


-Şimdi ise zafiyetimizin bulunduğu web sitesine bir göz atalım.Basit bir şekilde yükleme yapılıp dosya aktarımı yapılan bir sistemi var.

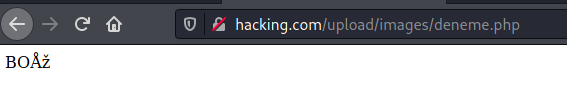
-Masaüstüne geçiş yapıyorum ve bir php dosyası oluşturuyorum.



-Php dosyasının içerisini boş bırakıyorum önce deneyeceğim karşı tarafa bir .php dosyası yüklenip yüklenemeyeceği.

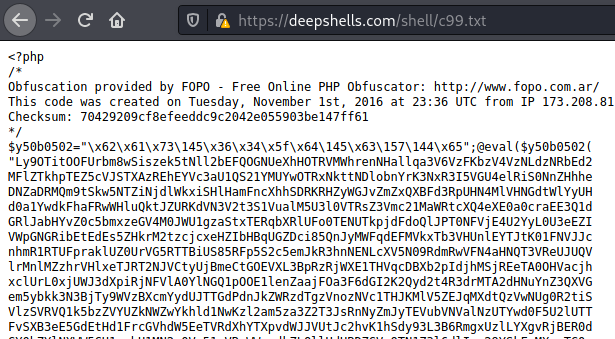


- Şimdi sırada deneme işlemi var.Başarılı bir şekilde gönderim sağlayabildim.



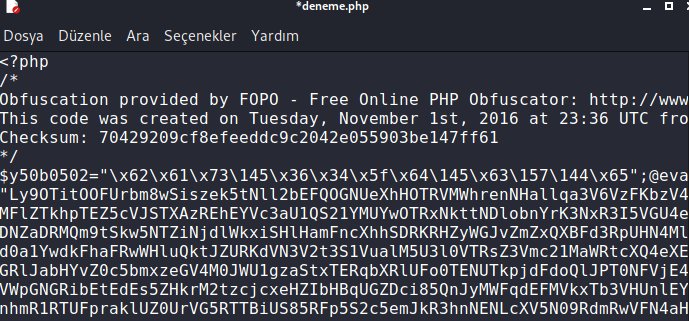
- Here butonuna basıp dosyayı başarılı bir şekilde upload ettiğimi teyit edebiliyorum.

-Şimdi ise sunucuya bir reverse php yükleyerek sunucuya sızma işlemini gerçekleştiricem.

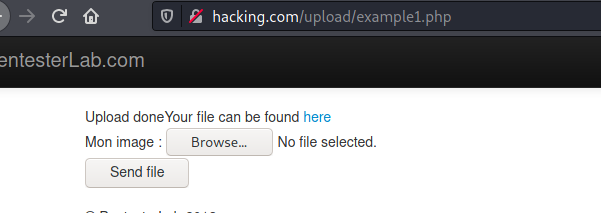


-Kali linuxta hazır olarak bulunan shell.php ile daha önce sızma işlemi yapmıştık fakat bu sefer internet üzerinden bir php dosyayı indirip o şekilde deneme yapmak istiyorum.

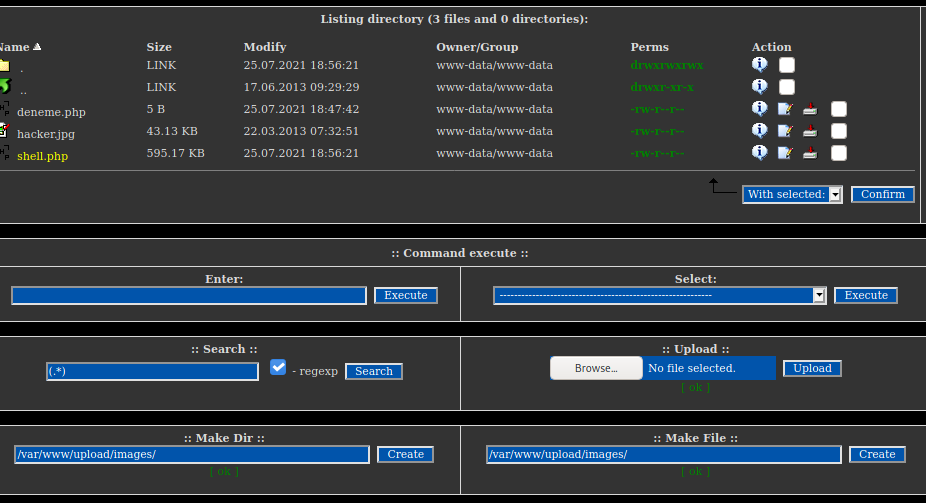
-Burada istediğimiz siteden indirme işlemi yapabiliriz tek yapmamız gereken diline dikkat etmek ben c99shell indiriyorum.Hem kullanışlı hemde yıllardır bilinen olduğu için onu indiriyorum.



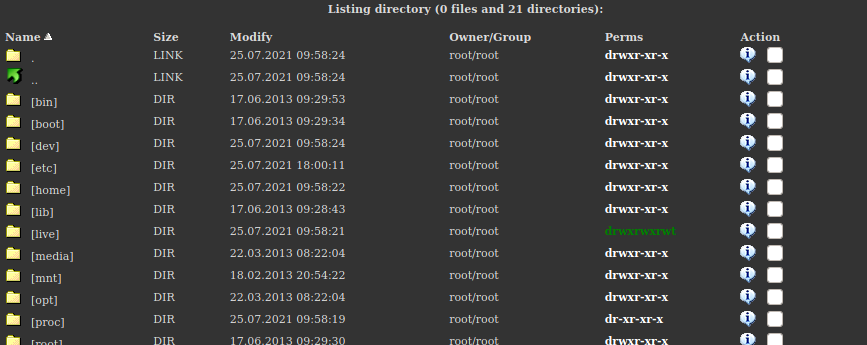
-Shell komutunu kopyalıyorum.Demin oluşturduğum deneme.php text'inin içine yapıştırıyorum.İsminide kaydettikten sonra ismini “Shell.php” olarak değiştiriyorum.



-Ardından zafiyetimin olduğu WFP kısmına geçiş yapıyorum ve bu .php dosyasını yüklüyorum.



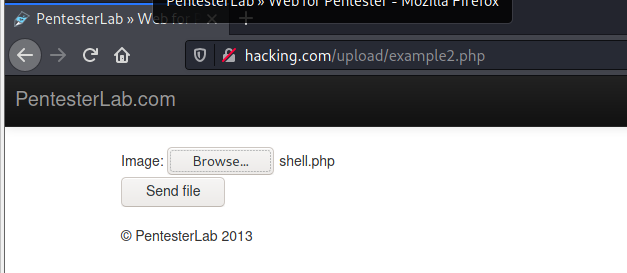
-Yükleme işleminden sonra here butonuna basarak bu sekmeye geçiş yapıyorum.Yüklemiş olduğum shellphp ile sunucuya başarılı bir şekilde sızdım artık istediğimi rahat bir şekilde yapabilirim.



-İstediğim dizin üzerinde gezinti yapabilirim.

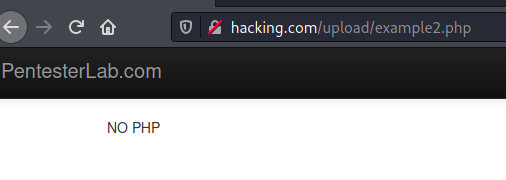
**Uygulama 2 :** Filtreleme atlatma

-Shell.php dosyasını bir önceki uygulamamızda nasıl indirdiğimizi göstermiştik ve karşı tarafa upload edip sunucu tarafına sızma işlemini başarılı bir şekilde tamamlamıştık.

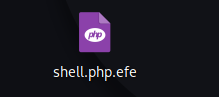


- Wfp üzerinde ki uygulama 2 üzerinde öncelikle php yükleme denemesi yapıyorum.

-Yükleme işlemini yaptım şimdi upload ediyorum.



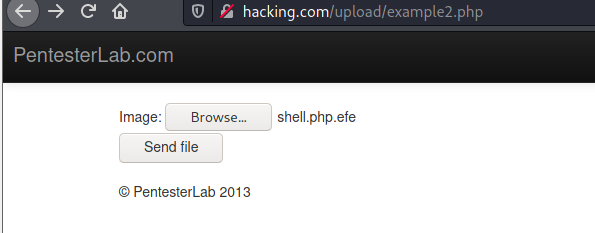
-Upload ettiğimde no.php hatası verdiğini görüyoruz.



-Bu yüzden .php uzantılı değil başka bir uzantı vermem gerekiyor.

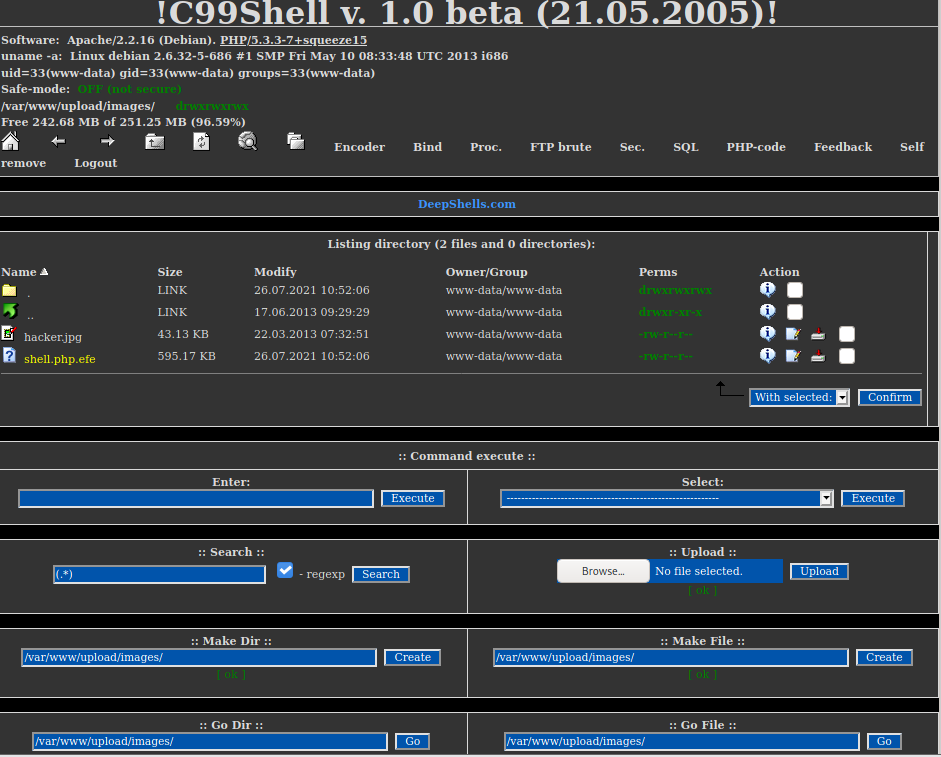
-Uzantının kullanılmayan bir uzantı olması gerekmelidir.

-Uzantısını ben efe olarak değiştirdim siz başka bir şeyde koyabilirsiniz.



-Şimdi ise uzantısını değiştirdiğim biçimde bir deneme yapmak istiyorum.Yükleme işlemini yaptım şimdi ise send edip deniyorum.

-Bu sefer hiçbir hata almadım başarılı bir şekilde gönderim yapabildim.Şimdi ise here butonu ile php dosyasını görüntülüyorum.



-Sisteme başarılı bir şekilde shell.php'yi yükledim ve sızma işlemini sağladım.Artık içeride istediğim işlemi gerçekleştirebilirim.