Sorunun çözümü için ilk aşamada sistemin ne yaptığını anlamak gerekiyor. Sistemde kullanılan teknoloji RIPS. Ne olduğuna kısaca göz atalım:

"RIPS - A static source code analyser for vulnerabilities in PHP scripts"

Biz bir dizin veriyoruz, bu program sayesinde o dizindeki (hatta alt dizinlerdeki) zafiyetleri bulabiliyoruz. Amacımız sistemdeki flag'i bulup basmak olduğu için ilk aşamada File Inclusion(Dosya Dahil Etme) zafiyetlerinin olduğu php dosyalarını incelemeye başladım.

leakscan.php, function.php, main.php gibi zafiyet içeren birçok dosyayı inceledim ama dikkatimi çeken kısım function.php dosyası oldu. "Sorry, no files included" hatası alıyordum. Sonrasında bu dosyaya parametre vermeyi denedim.

http://webloadbalancer-1838688779.eu-west-1.elb.amazonaws.com:9090/windows/function.php?file= şeklinde parametreleri denemeye başladım. İlk olarak mevcut dizinde flag.txt dosyası olup olmadığına bakmak için flag.txt dosyasını parametre olarak verdim. http://webloadbalancer-1838688779.eu-west-1.elb.amazonaws.com:9090/windows/function.php?file=flag.txt

Bu sürede üst dizinlere de çıkmayı denedim. ../../../ kullanımı ile root dizinine kadar çıkıp ardından flag.txt'yi bulmayı amaçladım.

Bu süre zarfında farklı farklı dizinler denedim, az önceki hatadan farklı olarak "Sorry, wrong file included" hatası aldım. Doğru yerdeydim fakat uygun dizini bir türlü bulamıyordum.

Birçok denemeden sonra sadece bir üst dizine bakayım diye düşündüm ve http://webloadbalancer-1838688779.eu-west-1.elb.amazonaws.com:9090/windows/function.php?file=../flag.txt 'yi denedim ve flag değerini elde ettim.