[hw0x08] writeup

莊翔旭, woolninesun, b04902083

GhostGIF

主要利用 phar 反序列化的漏洞:
一開始 upload 部分，GIF 檢查只要在檔案前面加入 magic number `GIF87a` 就可以繞過 GIF 檢查，再使用 getsize 的 getimagesize() 來達到反序列化，就成拿到 flag。

ref: https://www.anquanke.com/post/id/159206