CTF hw8

b05902127 劉俊緯

Ghost GIF

FLAG{phar_ez_ez}

- 首先，看到src.php本身就有自定義magic function，並且觀察這個magic function的__destruct的upload，就知道可以搞事了。如果你可以控制了這個function，你就可以在某個資料夾做任意寫入。
- 至於要如何創造出這個一個物件，就必須，就要歸功於getimgsize這類跟file有關的函數，都會因為phar這個偽協議而做parsing。
- 所以如果要觸發用getimgsize用phar做一個object，那麼就必須要上傳一些phar file到遠端上，再讓它去讀這個被放在遠端的phar code。
- 製作出一個會產生某object的code，直接寫一個php，用phar相關的api就可以了。需要注意的兩點是：開頭必須是gif的magic string，還有一般php server預設phar是read only，要自己設定把它調開。
- 如何遠端上傳這份code，並且知道這份code位在何方？這件事不需要做什麼race condition，因為網頁本身就有這個功能讓你使用。
- 將phar file上傳後，再用getsize觸發，就可以用phar產生出一個FileManager的object了。
- 既然可以用phar的FileManager，此時就把你的phar利用setMetadata一個自己參數定義個FileManager(把mode改成upload，name改成你要upload的path，content改成一個web shell)，再用getimgsize去處發，如此一來你就有一個web shell了。
- 有了webshell後就一切好辦，慢慢搜flag在那就可以了。