M10915027 石成峰 HW6

[Gopher POST]

1. 先使用file://協定查看source code，找到proxy.php是使用curl進行請求，還有flag.php需要內網存取。
2. 透過gopher://協定構造出發送POST及必要參數的TCP封包給內網，存取flag.php後得到flag。

[Cat]

1. Cat中反序列化後會執行system函數。
2. 執行反序列化的字串是session。
3. 可以構造Cat序列化後的物件，將本來的$sound覆蓋成想要執行的指令。
4. 將構造好的session進行base64\_encode後替換掉本來的session，達成RCE後找到flag。

[Rero Meme]

1. 查看原始碼找到有辦法觸發檔案操作進行反序列化，並且參數可以隨意控制的函數是lib.php中的is\_dir。
2. 建構一個phar檔，其中的meta-data是一個Meme class並在\_\_destruct後會用file\_put\_contents寫一個可以達成RCE的php。
3. 將檔案前面加上GIF89a通過GIF的判斷。
4. 上傳後清除session重新登錄，使用名稱讓is\_dir存取到phar檔案觸發反序列化，輸出php檔。
5. 直接存取可以RCE的php後找到flag。

[陸拾肆基底編碼之遠端圖像編碼器]

1. 先使用file://協定存取網頁的php，找到判斷網域的方法以及是使用curl進行請求。
2. 繼續使用file://協定往常用檔案中尋找線索，在/proc/net/tcp中看到一個可疑的27134 port。
3. 使用[::ffff:127.0.0.1]ipv6格式，讓回傳的第[0]個元素為[::ffff:127繞過判斷後往27134 port發送GET的請求。
4. 收到ERR wrong number of arguments for 'get' command的回覆，google後得知是redis的服務。
5. 使用gopher://協定構造出可以讓redis寫檔案的封包，將用來RCE的檔案寫在預設就可以被儲存的/tmp底下。
6. 使用....//繞過replace後讓include的page改為剛剛寫在/tmp下的php，達成RCE後找到flag。