Stage I:

1. 概要

   CVE 編號：CVE-2025-22974

   類型：SQL Injection

   簡述：SeaCMS（PHP-based CMS）在 phome.php 組件內，DoTranExecSql 參數存在 SQL 注入漏洞；透過該參數的未妥善處理，遠端攻擊者可構造惡意輸入以影響 SQL 執行流程，進而達到讀寫資料庫或進一步的遠端代碼執行

   嚴重性：CVSS Version 3.x 給予他 9.8（Critical）高分

   影響範圍：SeaCMS v13.2 及之前版本

   影響：攻擊者可能藉此執行任意 SQL 查詢、竄改或外洩資料庫資料、甚至在特定情況下達成遠端代碼執行與取得後臺存取權限，導致服務破壞、資料外洩或持久化後門等後果

2. 如何重現漏洞環境

   A. 平台和版本

   - VM : Virtualbox Ubuntu 22.04.5
   - Network : Nat
   - Docker : Docker 28.2.2, Docker-compose 1.29.2
   - Images : php 7.4-apache, mysql 5.7
   - SeaCMS : 13.2

   B. 專案結構

   ```
   SEACMS_LAB/
       apache_log/
           access.log
           error.log
           other_vhosts_access.log
       seacms/
       docker-compose.yml
   ```

   C. 環境建構步驟

   1. 在 terminal 執行

      ```
      cd ~/seacms_lab
      sudo docker-compose up -d –build
      ```

   2. 在瀏覽器開啟 http://localhost:8080/jxpsl5
   3. 利用帳號 admin 密碼 1234 登入後台並且取得 session

cookie

3. 如何準備重現 exploit

    A. 建立 Baseline，先取得正常請求的行為與日誌，之後才看得出異常差異

    B. 進行非破壞性輸入處理探測，證明 DoTranExecSql 參數會被程式接收並進入後端流程

    C. 在 VM 內檢視程式碼內，進一步證明 phome.php 確實接收該參數並帶到後端流程

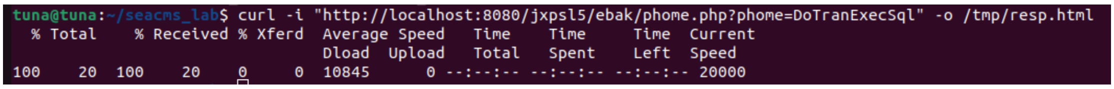
Stage II:

Trial i:

- Result: Success

- Description: 以非破壞性請求觸發 endpoint：

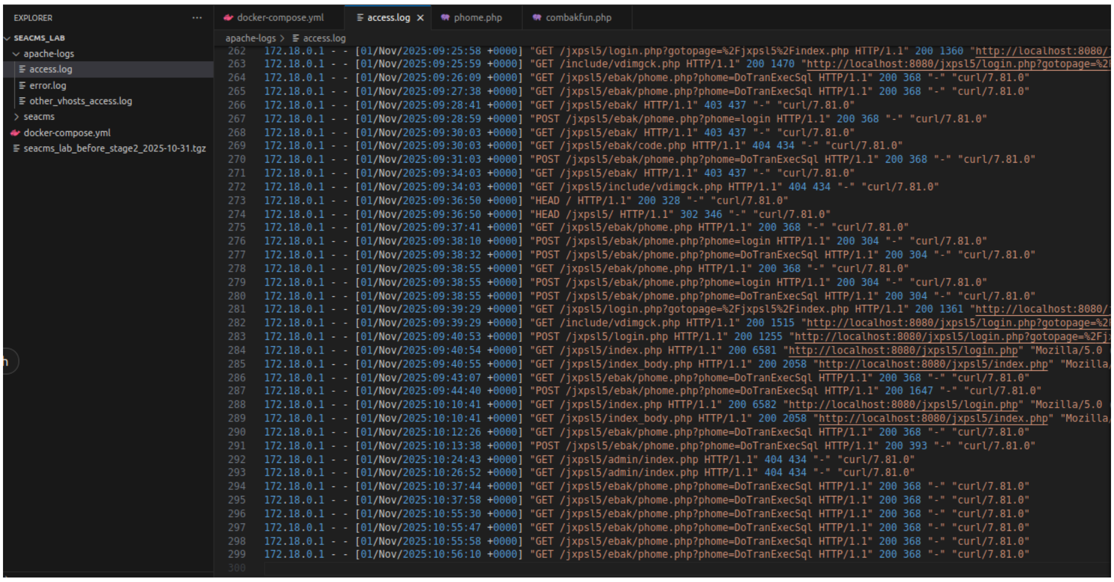
curl -i "http://localhost:8080/jxpsl5/ebak/phome.php?phome=DoTranExecSql" -o /tmp/resp.html



```
tuna@tuna:~/seacms_lab$ curl -i "http://localhost:8080/jxpsl5/ebak/phome.php?phome=DoTranExecSql" -o /tmp/resp.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    20  100    20    0     0  10845      0 --:--:-- --:--:-- --:--:-- 20000
```

回應內容為 HTTP/1.1 200 並顯示"ERROR! LOGIN PLEASE!"，代表程式路徑可被成功存取，但此動作需要登入才會執行上傳或 SQL 處理。

- Reason: Apache access log 記錄該請求並回傳 200，證明該功能端點存在且可到達。但伺服器進一步拒絕未授權操作（需要登入），說明尚有權限檢查或 session 機制存在。



```
172.18.0.1 - - [01/Nov/2025:09:25:58 +0000] "GET /jxpsl5/login.php?gotopage=%2Fjxpsl5%2Findex.php HTTP/1.1" 200 1360 "http://localhost:8080/
172.18.0.1 - - [01/Nov/2025:09:25:59 +0000] "GET /include/vdimgck.php HTTP/1.1" 200 1470 "http://localhost:8080/jxpsl5/login.php?gotopage=%2
172.18.0.1 - - [01/Nov/2025:09:26:09 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:27:38 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:28:41 +0000] "GET /jxpsl5/ebak/ HTTP/1.1" 403 437 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:28:59 +0000] "POST /jxpsl5/ebak/phome.php?phome=login HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:30:03 +0000] "GET /jxpsl5/ebak/ HTTP/1.1" 403 437 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:30:03 +0000] "GET /jxpsl5/ebak/code.php HTTP/1.1" 404 434 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:31:03 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:34:03 +0000] "GET /jxpsl5/ebak/ HTTP/1.1" 403 437 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:34:03 +0000] "GET /jxpsl5/include/vdimgck.php HTTP/1.1" 404 434 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:36:50 +0000] "HEAD / HTTP/1.1" 200 328 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:36:50 +0000] "HEAD /jxpsl5/ HTTP/1.1" 302 346 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:37:41 +0000] "GET /jxpsl5/ebak/phome.php HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:38:10 +0000] "POST /jxpsl5/ebak/phome.php?phome=login HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:38:32 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:38:55 +0000] "GET /jxpsl5/ebak/phome.php HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:38:55 +0000] "POST /jxpsl5/ebak/phome.php?phome=login HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:38:55 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:39:29 +0000] "GET /jxpsl5/login.php?gotopage=%2Fjxpsl5%2Findex.php HTTP/1.1" 200 1361 "http://localhost:8080/
172.18.0.1 - - [01/Nov/2025:09:39:29 +0000] "GET /include/vdimgck.php HTTP/1.1" 200 1515 "http://localhost:8080/jxpsl5/login.php?gotopage=%2
172.18.0.1 - - [01/Nov/2025:09:40:53 +0000] "POST /jxpsl5/login.php HTTP/1.1" 200 1255 "http://localhost:8080/jxpsl5/login.php?gotopage=%2Fj
172.18.0.1 - - [01/Nov/2025:09:40:54 +0000] "GET /jxpsl5/index.php HTTP/1.1" 200 6581 "http://localhost:8080/jxpsl5/login.php" "Mozilla/5.0
172.18.0.1 - - [01/Nov/2025:09:40:55 +0000] "GET /jxpsl5/index_body.php HTTP/1.1" 200 2058 "http://localhost:8080/jxpsl5/index.php" "Mozilla
172.18.0.1 - - [01/Nov/2025:09:43:07 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:09:44:40 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 1647 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:10:41 +0000] "GET /jxpsl5/index.php HTTP/1.1" 200 6582 "http://localhost:8080/jxpsl5/login.php" "Mozilla/5.0
172.18.0.1 - - [01/Nov/2025:10:10:41 +0000] "GET /jxpsl5/index_body.php HTTP/1.1" 200 2058 "http://localhost:8080/jxpsl5/index.php" "Mozilla
172.18.0.1 - - [01/Nov/2025:10:12:26 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:13:38 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 393 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:24:43 +0000] "GET /jxpsl5/admin/index.php HTTP/1.1" 404 434 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:26:52 +0000] "GET /jxpsl5/admin/index.php HTTP/1.1" 404 434 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:37:44 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:37:58 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:30 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:47 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:58 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:56:10 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
```

Trial ii:

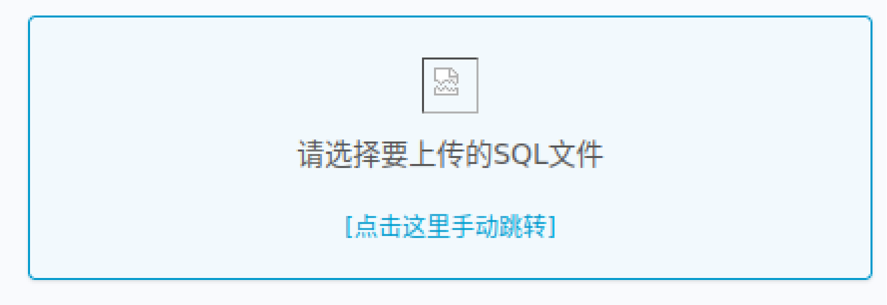
- Result: Partial Success

- Description: 上傳空檔以觸發上傳處理流程

用已登入 session（PHPSESSID）呼叫上傳端點並上傳空檔：

```
PHPSESSID="7cb9aac5c39d17d80c59999f59ae08b6"
touch /tmp/empty.sql
curl -b "PHPSESSID=${PHPSESSID}" -F "file=@/tmp/empty.sql"
"http://localhost:8080/jxpsl5/ebak/phome.php?phome=DoTranExecSql" -o
/tmp/resp_upload.html -s -w "\nHTTPSTATUS:%{http_code}\n"
```

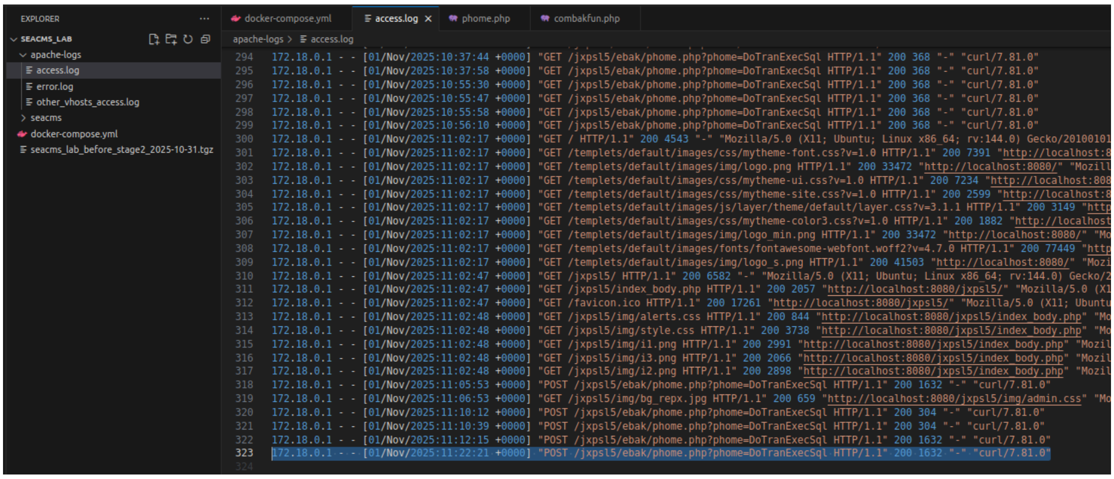
回應 HTTPSTATUS:200，response body 顯示「请选择要上传的 SQL 文件」並自動跳回，表示伺服器已經進入上傳處理邏輯但因檔案內容/格式不符而中止。



请选择要上传的SQL文件

[点击这里手动跳转]

- Reason: Apache access.log 記錄該請求



```
172.18.0.1 - - [01/Nov/2025:10:37:44 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:37:58 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:30 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:47 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:55:58 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:10:56:10 +0000] "GET /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 368 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET / HTTP/1.1" 200 4543 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:144.0) Gecko/20100101
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/css/mytheme-font.css?v=1.0 HTTP/1.1" 200 7391 "http://localhost:8
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/img/logo.png HTTP/1.1" 200 33472 "http://localhost:8080/" "Mozill
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/css/mytheme-ui.css?v=1.0 HTTP/1.1" 200 7234 "http://localhost:808
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/css/mytheme-site.css?v=1.0 HTTP/1.1" 200 2599 "http://localhost:8
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/js/layer/theme/default/layer.css?v=3.1.1 HTTP/1.1" 200 3149 "http
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/css/mytheme-color3.css?v=1.0 HTTP/1.1" 200 1882 "http://localhost
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/img/logo_min.png HTTP/1.1" 200 33472 "http://localhost:8080/" "Mo
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/fonts/fontawesome-webfont.woff2?v=4.7.0 HTTP/1.1" 200 77449 "http
172.18.0.1 - - [01/Nov/2025:11:02:17 +0000] "GET /templets/default/images/img/logo_s.png HTTP/1.1" 200 41503 "http://localhost:8080/" "Mozi
172.18.0.1 - - [01/Nov/2025:11:02:47 +0000] "GET /jxpsl5/ HTTP/1.1" 200 6582 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:144.0) Gecko/2
172.18.0.1 - - [01/Nov/2025:11:02:47 +0000] "GET /jxpsl5/index_body.php HTTP/1.1" 200 2057 "http://localhost:8080/jxpsl5/" "Mozilla/5.0 (X1
172.18.0.1 - - [01/Nov/2025:11:02:47 +0000] "GET /favicon.ico HTTP/1.1" 200 17261 "http://localhost:8080/jxpsl5/" "Mozilla/5.0 (X11; Ubuntu
172.18.0.1 - - [01/Nov/2025:11:02:48 +0000] "GET /jxpsl5/img/alerts.css HTTP/1.1" 200 844 "http://localhost:8080/jxpsl5/index_body.php" "Mo
172.18.0.1 - - [01/Nov/2025:11:02:48 +0000] "GET /jxpsl5/img/style.css HTTP/1.1" 200 3738 "http://localhost:8080/jxpsl5/index_body.php" "Mo
172.18.0.1 - - [01/Nov/2025:11:02:48 +0000] "GET /jxpsl5/img/i1.png HTTP/1.1" 200 2991 "http://localhost:8080/jxpsl5/index_body.php" "Mozil
172.18.0.1 - - [01/Nov/2025:11:02:48 +0000] "GET /jxpsl5/img/i3.png HTTP/1.1" 200 2066 "http://localhost:8080/jxpsl5/index_body.php" "Mozil
172.18.0.1 - - [01/Nov/2025:11:02:48 +0000] "GET /jxpsl5/img/i2.png HTTP/1.1" 200 2898 "http://localhost:8080/jxpsl5/index_body.php" "Mozil
172.18.0.1 - - [01/Nov/2025:11:05:53 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 1632 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:11:06:53 +0000] "GET /jxpsl5/img/bg_repx.jpg HTTP/1.1" 200 659 "http://localhost:8080/jxpsl5/img/admin.css" "Mo
172.18.0.1 - - [01/Nov/2025:11:10:12 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:11:10:39 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 304 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:11:12:15 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 1632 "-" "curl/7.81.0"
172.18.0.1 - - [01/Nov/2025:11:22:21 +0000] "POST /jxpsl5/ebak/phome.php?phome=DoTranExecSql HTTP/1.1" 200 1632 "-" "curl/7.81.0"
```

Trial iii:

- Result: Success

- Description: 上傳非破壞性檔案

以管理員 PHPSESSID 登入後，上傳一個不含 SQL 內容的檔案：

```
PHPSESSID="7cb9aac5c39d17d80c59999f59ae08b6"
printf "harmless test file\n" > /tmp/harmless.sql
curl -b "PHPSESSID=${PHPSESSID}" -F "file=@/tmp/harmless.sql" "http://localhost:8080/jxpsl5/ebak/phome.php?phome=DoTranExecSql" -o /tmp/resp_upload.html
```

回應 HTTP 200，頁面顯示「文件上传失败，请检查 tmp 目录权限」，表示伺服器已嘗試存取上傳檔案但寫入失敗。

- Reason: 此結果證明 phome.php?phome=DoTranExecSql 在登入狀態下會進入 Ebak_DoTranExecSql()上傳邏輯；若 tmp 目錄具寫入權限且內容含 SQL，程式將直接執行該 SQL。權限錯誤訊息反而佐證了漏洞函式被觸發且有檔案存取行為。