Network Security - Project2

0656510 蔡孟谷

1. 透過網站根目錄下的「robots.txt」這個檔案，我們可以發現除了 blog 本身之外，還有其他三個檔案。
   - ✓ phpMyAdmin_NS_pRojEct_2017/：phpMyAdmin 的路徑
   - ✓ backup.tar.gz：透過瀏覽器，可以直接下載到這個檔案，解壓縮之後，發現內容為該 blog 的原始碼。
   - ✓ blog/memorandum.txt：無法直接透過瀏覽器存取該檔案，但嘗試一下之後發現，可以下載到一個名為「blog/.memorandum.txt.swp」的暫存檔，內容被編碼且加密過。
2. 先透過「cat memorandum.txt.swp | base64 --decode」這條指令來 decode base64 的編碼，再透過 XOR Cracker (https://wiremask.eu/tools/xor-cracker/)這個線上工具來解密，會得到兩個可能的結果，其中一個看起來比較像是正常的文件，打開來看發現，該文件內寫著 phpMyAdmin 的帳密。

```
2016.01.13
phpMyAdmin Account & Password
Account: BobIsGod
Password: preventativescrediblescuffed
```

3. 透過這組帳密，就可以順利登入 phpMyAdmin 了，進到「ns2017fall_Bob」這個資料庫後發現，在「posts」這張資料表裡，存有著所有文章的資料，也可以看到被鎖起來的文章的密碼。

	id	title	content	password
編輯 複製 刪除	1	Sugar - Maroon 5	I'm hurting, baby, I'm broken down I need your lo...	NULL
編輯 複製 刪除	2	You're beautiful	My life is brilliant. My life is brilliant. My...	NULL
編輯 複製 刪除	3	おだ のぶなが	Oda Nobunaga (織田 信長 About this sound Oda Nobunaga ...	NULL
編輯 複製 刪除	4	山本五十六	山本 五十六（やまもと いそろく、1884年（明治17年）4月4日 - 1943年（昭和18年）4月...	NULL
編輯 複製 刪除	5	This is not what you're looking for...	Not this post... Please try another post...	NULL
編輯 複製 刪除	6	Fake stay night saying	People die if they are killed!! <img src="http:...	NULL
編輯 複製 刪除	7	My Lovely Girlfriend!!	236GZfZOSQTlmYrqGe44Nm4teDiTmCjlW0aW3QWeskX/NB3Jyt...	44f37c5442cd34cf

4. 若是將這組密碼直接輸入到網站以進行驗證，並沒有辦法成功解鎖文章，仔細研究了一下從「backup.tar.gz」這個檔案裡所取得的網站的原始碼之後發現，原來網站會先將我們的輸入送給 functions.php 裡的「my_own_hash」這個函式進行處理，如果 hash 出來的結果和資料庫裡所儲存的密碼相同，則會呼叫「decrypt_content」這個函式來進行解鎖，因此，我們需要想辦法生出一組 input，讓它 hash 出來的值，會等於資料庫裡所儲存的密碼的值。

5. 在「my_own_hash」這個函式裡，有著兩組 magic number，將其丟進去 google 之後發現，原來這裡所使用的，是一種名為「MySQL323」的 hash 函式，透過 MySQL323 Collider 這套工具 (https://tobtu.com/mysql323.php)，我們可以很方便地找到一組會產生相同雜湊值的輸入，下圖紅框裡，就是我們所需要的輸入的值。

```
star096374@star096374-VirtualBox:~/Network_Security/project2/MySQL323_Collider$
./mysql323collider64 -h 44f37c5442cd34cf -m 2048 -t 1
Initializing...
Took 14.74 sec
2.488 Pp/s [100.0%]
44f37c5442cd34cf:227a5f67215b3c64484e66405c:"z_g![<dHNf@\

Crack time:    256.106 seconds
Average speed: 2.466 Pp/s
```

6. 將該輸入丟到網站進行驗證之後發現，我們終於順利解鎖文章並取得原圖了！

My Lovely Girlfriend!!

This is my lovely girlfriend(This is the answer for project1! Congraz!):

「What have you learned?」

1. 「robots.txt」這個檔案，原本是用來告訴爬蟲機器人不要存取目錄底下的哪些檔案，但也有可能導致目錄底下的一些敏感資料的路徑被他人得知。
2. 備份檔案或暫存檔案，如果沒有適當的拒絕他人存取或刪除，可能會導致網站的原始碼或是其他的敏感資料洩漏，進而增加被攻擊成功的風險。
3. 儘管敏感資料的內容有做過加密，但使用的卻是很簡單的 xor 加密的方式，被破解之後，敏感資料就真的洩漏了。
4. 在 phpMyAdmin 的資料庫裡，儘管還有另外使用 hash 的方式來做保護，但使用的卻是會產生碰撞的 hash 函式，透過工具找到能夠產生相同 hash 值的 input 之後，文章內容就被他人得知了。

「How to prevent or patch these vulnerabilities?」

1. 不要將敏感資料放在網站根目錄底下供他人存取，如此一來，「robots.txt」也就不會洩漏敏感資料的路徑。
2. 要特別注意備份檔案或暫存檔案，有時候這些檔案，會導致敏感資料意外地被洩漏出去。
3. 加密的方式不能太過簡單，否則儘管有加密，還是很容易被他人破解。
4. 使用的 hash 函式也不能太容易被反推或產生碰撞，否則也很有可能會成為被他人攻擊的弱點之一。