2D Life Write up

Writer : Sakuya Izayoi

1. Site map

Index.php	
	?p=pic
	?p=music
	?p=contact
	?p=secret_login

총 5개의 php파일로 이루어 져 있으며, pic, music, contact 기능은 본 문제와 크게 연관 없는 파일임.

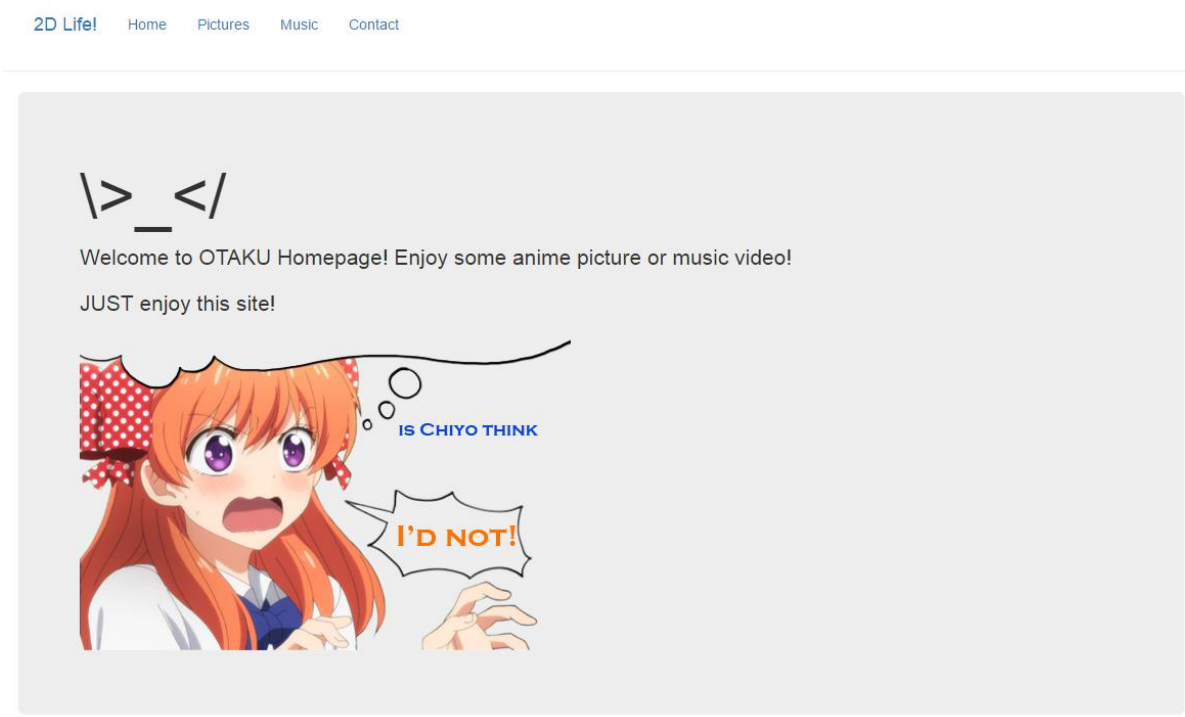
2. 문제 개요

?p=pagename 의 값을 보고 LFI로 시도 해 볼 수 있으나, 이것은 해당 문제와 연관이 없고, 해당 문제의 index.php?p=secret_login에서 SPY 계정으로 로그인 된 것을 F14G 계정으로 로그인하고 또한 DB에 저장된 F14G 계정의 certificate 값을 가져와서 해당 그림파일을 업로드 하면 플래그를 획득할 수 있는 문제이다.

3. 문제 구성 환경

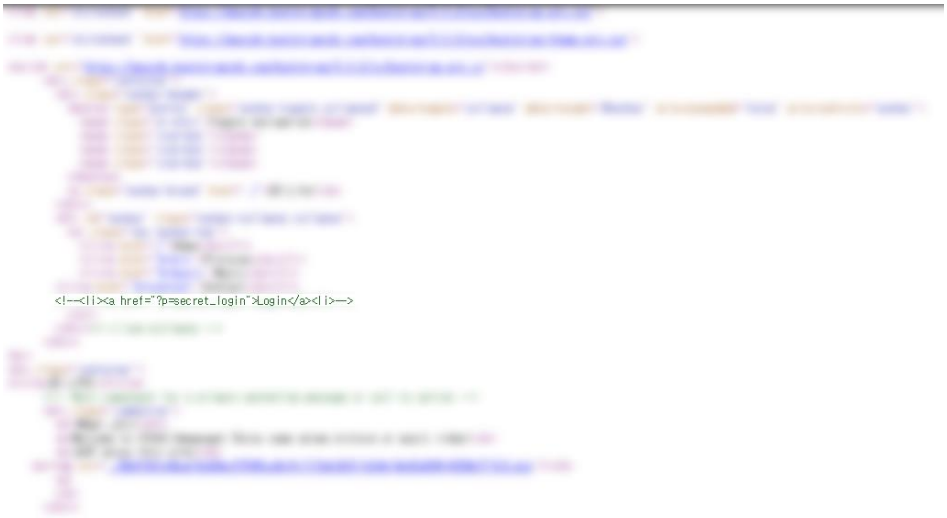
OS	Ubuntu 16.04
KERNEL	Linux ubuntu 4.4.0-59-generic #80-Ubuntu SMP Fri Jan 6 17:47:47 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
APACHE	Apache/2.4.18 (Ubuntu)
PHP	PHP 7.0.13-0ubuntu0.16.04.1
MYSQL	5.7.17-0ubuntu0.16.04.1

4. 풀이

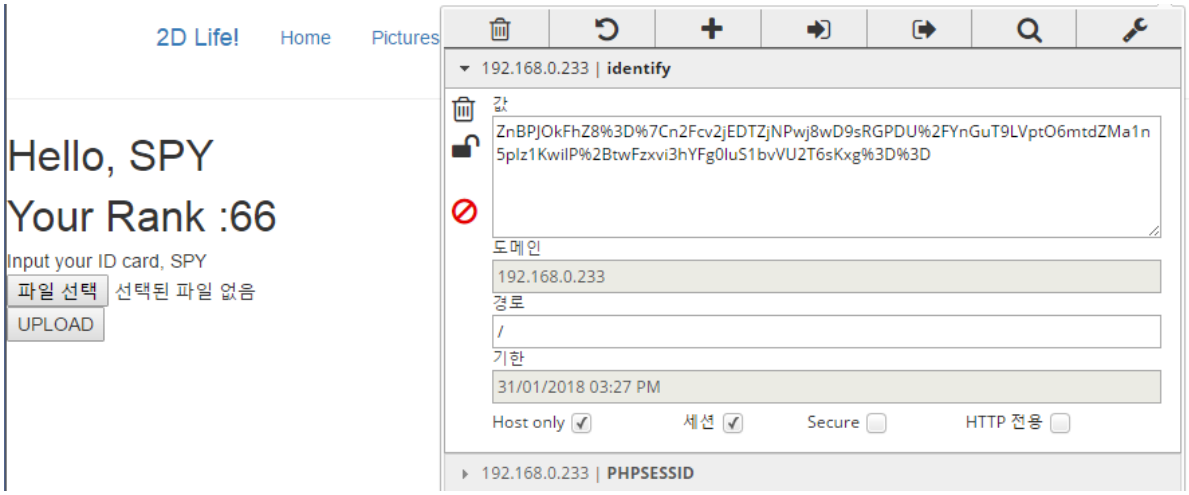


해당 문제의 페이지에 접속하게 되면 Home, Pictures, Music, Contact의 4개의 목록이 보이고 해당 페이지를 둘러보다 보면 별 기능이 없 없다는 것 알게 된다.

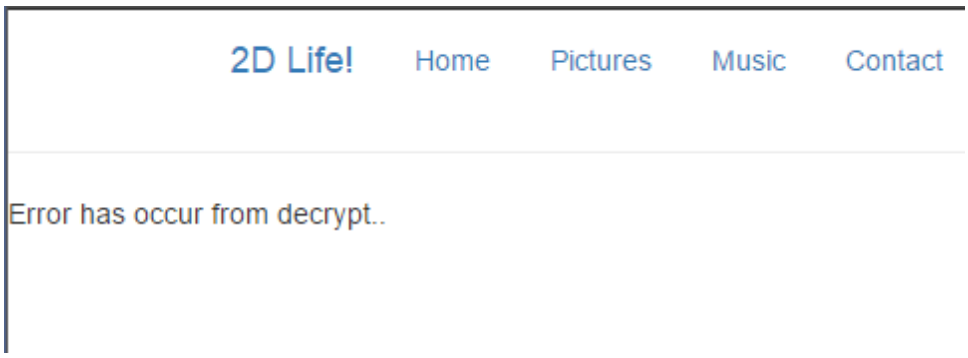
게시된 4개의 페이지 어느 곳에서든 소스코드를 보면 아래와 같은 주석을 발견 할 수 있다.



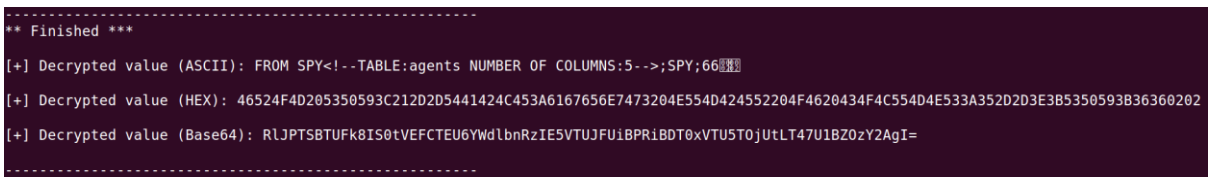
?p=secret_login을 보면 이미 SPY로 로그인 된 것을 볼 수 있다.



이미 로그인 된 이 값은 쿠키 identify 를 복호화 하여 나온 값이라는 것을 어림잡아 짐작할 수 있다. |(0x7c) 값을 기준으로 앞부분이 IV, 뒷부분이 Encryption 에 해당하는 것을 알 수 있고 해당 쿠키 값을 조작하다 보면 아래와 같은 에러 메세지를 발견 할 수 있다.



이를 통해 Oracle padding attack 임을 짐작 할 수 있고, 성공적인 공격을 위해 평문을 먼저 알아야 할 필요가 있다. 해당 공격에 가장 자주 쓰이는 padbuster 툴을 돌리면 아래와 같은 평문을 획득할 수 있다



;(semicolon)을 기점으로 2 번째 값과 3 번째 값이 출력됨을 알 수 있다.

또한 해당 정보를 통해 Table 이 agents 라는 것과 컬럼이 총 5 개 있다는 것을 알 수 있고 이를 통해 sql injection 으로 DB 내부에 있는 값들을 획득해야 한다.

하지만 컬럼명을 뽑아내기 위한 information_Schema 와 같은 주요 DB 들이 필터링으로 막혀있고, 이를 우회하기 위해 union 을 통한 sql injection 을 시도한다.

SPY 와 같이 ID 가 적혀있는 란에는 '(single quote)가 필터링 되어 있음을 알 수 있고, ₩(backslash)등을 통해 escape 한다고 하더라도 자세한 쿼리 구성을 알 수 없으므로 66 이 적혀있는 곳에 injection 을 시도한다. 변조해서 넣을 평문은 아래와 같다

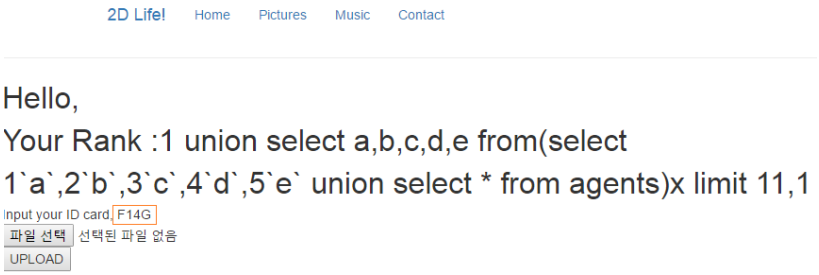
```
;;1 union select a,b,c,d,e from(select 1`a`,2`b`,3`c`,4`d`,5`e` union select * from agents)x limit 11,1
```

툴을 돌려서 나온 결과값은 다음과 같다

```
------------------------------------------------------------
** Finished ***

[+] Encrypted value is: 0OWmIoAQ07rLzvWgTaJVTrZ9lZDhC%2BF0v1F9RaAAAAAAA%3D%3D
------------------------------------------------------------
```

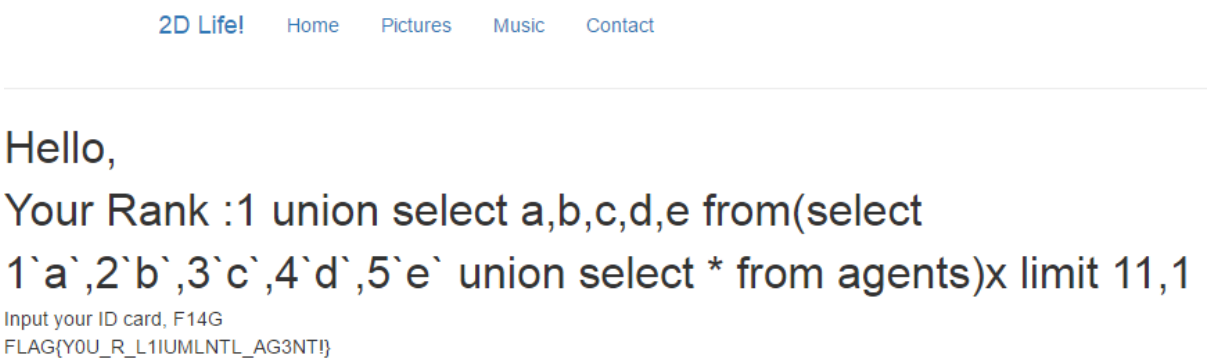

```
------------------------------------------------------------
** Finished ***

[+] Encrypted value is: 0OWmIoAQ07rLzvWgTaJVTrZ9lZDhC%2BF0v1F9RaFpXUcqKR12fb1W%2BSO27jb5UE2r7jJTs944fRYywDh4T6reCf5Fs%2FqC6BrnOZGt6yw6%2Fs9qileuRqrRSsi%2F82h8TwEs6EF17nCphlkAAAAAAAAAAA%3D%3D
------------------------------------------------------------
```


해당 값은 암호문이므로, IV 를 제외한 암호문만 변경해 주면 아래와 같이 F14G 로 로그인 된 것을 볼 수 있다



해당 쿼리문을 조금만 더 응용하면 F14G 의 certificate 를 획득 할 수 있으며

해당 주소로 들어가면 QR code 파일을 하나 얻을 수 있다. 다시한번 F14G 로 로그인 한 후, 파일을 업로드 하면 해당 문제의 Flag 값을 얻을 수 있다.



FLAG : FLAG{Y0U_R_L1IUMLNTL_AG3NT!}

EOF