Layer7 Internal CTF

선린인터넷고등학교
문시우 (751 pts)

CHALLENGES

MISC

Knock, Knock! (1 pts)

WEB

Simple Login (100 pts)

Welcome to DB (200 pts)

Google Hacking (200 pts)

FORENSIC

Man In The Middle (50 pts)

Chrome’s footprint (100 pts)

CRYPTO

Layer7’s Letter (100 tps)

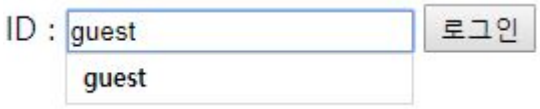
Knock, Knock! (1 pts)

```
FLAG IS LCTF{Hello_Layer7!}
```

You solved this challenge.

간단한 mic check 문제다.
LCTF{Hello_Layer7!}

Simple Login (100 pts)



guest로 로그인해보면 user_info라는 쿠키가 생성된다.
user_info를 보면 {“id”:”guest”}를 base64로 7번 인코딩한 값이라는 걸 알 수 있다.
{“id”:”admin”}을 base64로 7번 인코딩해서 user_info에 넣어주면 플래그가 나온다.

user_info=Vm1wS05HSXlUWGhVV0d4VllUSlNjVlZzV2t0V1ZscHlWMjVrVkUxWGVlcFdiVEZ
lWVcxS1NHVklj%0ARmhoTW1oUVdWUkdZVmRlVmtWUwpiRlpYVm10WmVsWlZXa1pQV
mtKU1VGUXdQUW89

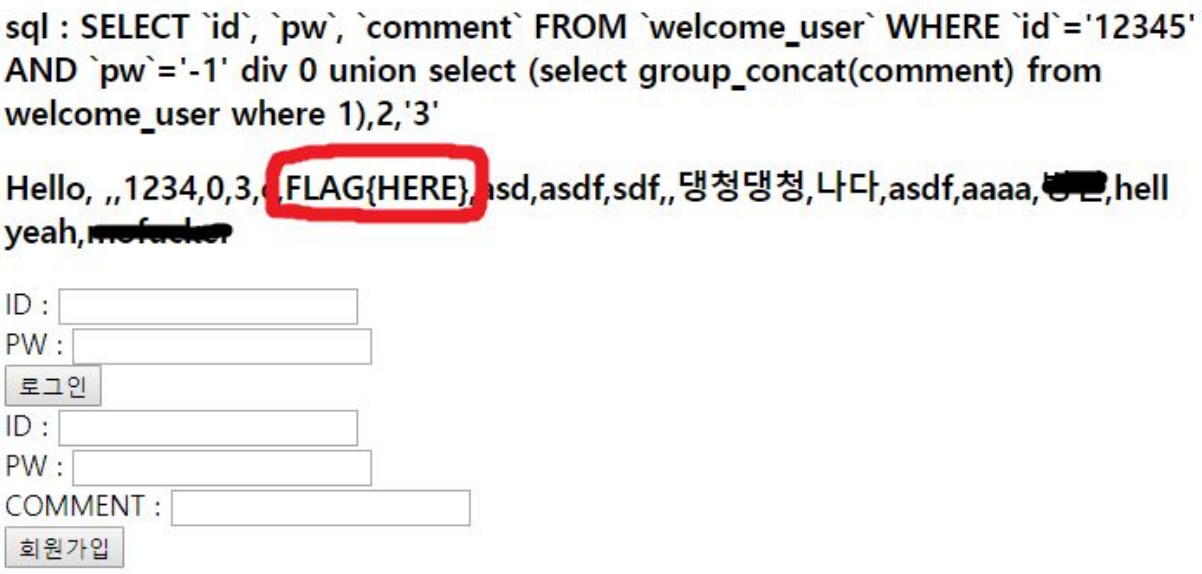
FLAG{Hello_Layer7!}

Welcome to DB (200 pts)

> 관리자가 숨겨둔 플래그를 읽으세요!
> Link

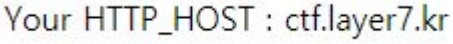
필터링은 딱히 없는 것 같다.
그냥 바로 union select로 플래그를 추출했다.
(테이블 이름은 문제에서 쿼리 자체를 보여주기 때문에 알 수 있다.)

payload
id : 12345
pw : -1' div 0 union select (select group_concat(comment) from welcome_user where 1),2,'3



FLAG{HERE}

Google Hacking (200 pts)



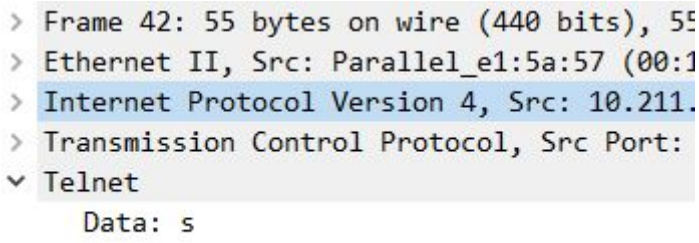
http host를 조작해서 구글 도메인으로 바꾸면 된다.
이런 간단한 것을 도구 문제로 굉장히 오래걸렸다.

GET /ctf/Google.php HTTP/1.1
Host : google.co.kr

Man In The Middle (50 pts)

> 패킷을 도청했다. 텔넷 아이디와 비밀번호를 알아내자!
> 플래그 : (id)_(pw) md5 해쉬값
> 예) id가 a, pw가 b 이면 md5("a_b")
> Link

Link를 들어가면 dump.pcapng를 다운받을 수 있다.
와이어샤크로 열어서 확인해보면 한눈에 보기 쉬운 패킷 캡쳐 기록을 볼 수 있는데
프로토콜이 TELNET인 부분을 자세히 보면 아이디와 비밀번호를 알 수 있다.



ID : sprout
PW : AhhA1

플래그는 (id)_(pw) 형식을 md5로 해시한 값이므로
“sprout_AhhA1”를 md5로 해시하면 FC7C8E3C021EC827012745815EF7371D.

flag : FC7C8E3C021EC827012745815EF7371D

Chrome's footprint (100 pts)

> 누군가 크롬으로 불법 사이트에 접근했다. 사이트명과 아이디, 비밀번호를 알아내자!
> 플래그 : (id)_(pw)_(url) md5 해쉬값
> 예) id가 a, pw가 b, url이 c면 md5("a_b_c")
> Link

Link를 들어가면 History 파일을 다운받을 수 있다.
History 파일은 sqlite sql 파일이다.
sqlite로 열어보면 여러 테이블이 보이는데 그 중 urls 테이블을 확인해보면
사이트 접속 기록이 많이 보인다.

그 중 아이디, 비밀번호가 보이는 url을 확인 할 수 있다.

http://lol.kr/?id=admin&pw=1234

ID : admin
PW : 1234
URL : lol.kr

admin_1234_lol.kr 도 해보고
admin_1234_http://lol.kr/ 도 해보고
admin_1234_http://lol.kr/?id=admin&pw=1234 도 해봤는데 안됐다.

다른 URL도 (예 : 토렌트 킴, 토사랑) 다 해봤지만, 인증이 모두 안된다.
그래서 운영진 측에 문의해보니 정답으로 인정해주었다.

flag : 437E2B64C357898C14B09A1AB07EFA21

Layer7's Letter (100 pts)

> 바다에서 주운 편지다. 해독해보자.
> Link

Shal7 ohz illu dpao aol zjovvs zpujl 2001, dolu Zbuspu Pualyula Opno Zjovvs dhz klzpnuhalk hz aol mpyza PA johyhjalypzapj opno zjovvs pu Zlvbs. Zabkluaz dov hyl pualylzalk pu zljbypaf hyl ibpskpun h jsbi, huk pu aol yhyl hylhz vm ohjrpun, lhjo vaoly ohz olswlk lhjo vaoly huk ohz zabkplk zljbypaf. Aol zfzalthapj jbyypjbsbt huk aol whzzpvu vm aol jsbi tltilyz huk aol zluzl vm ylzwvuzpipspaf ohcl jvuaypibalk av aol opzavyf vm 17 flhyz. Aol Dvysk Dhy Aluupz Johtwpvuzopwz, ovzalk if aol Dvysk'z Tvza Dhualk if Klhao huk Klmluzl Tpupzayf, hyl wbispzolk pu chypvbz mplskz, pujsbkpun aol Pualyuhapvuhs Ohjrpun Jvumlylujl, vynhupglk if aol Pualyuhapvuhs Ohjrpun Jvumlylujl, huk wbispzopun pu chypvbz mplskz, pujsbkpun jvtwbalyz, Dli wvyahsz, huk ltilkklk mvythaz. Avkhf dl ohcl opkklu h mshn. MSHN{Shfly7_pz_nvvkkkkkkkkk}

마지막에 있는 MSHN{Shfly7_pz_nvvkkkkkkkkk}가 뭔가 의심스럽다.
MSHZ -> FLAG 각 알파벳의 아스키코드 간격을 보니 7씩 차이가 난다.
예 : ord('M') = 77 , ord('F') = 70

MSHN{Shfly7_pz_nvvkkkkkkkkk} 에서 각 문자 아스키 값을 7씩 빼보면
FLAG{La_er7_is_goodddddddddd} 가 되는데 La_er7에서 언더바는 게싱으로 맞추면 된다.

FLAG{Layer7_is_goodddddddddd}

이번 내부 대회에서는 다양한 분야를 풀어보았다.
재밌는 문제가 많았고 성적도 괜찮게 나와서 좋은 기억으로 남는 대회일 것 같다.