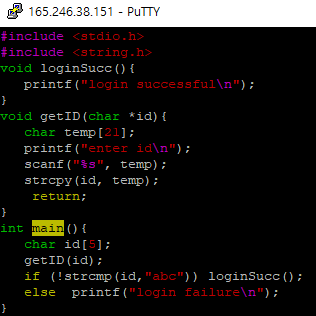
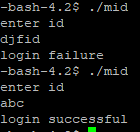
비밀번호 7451

1.

Stack buffer overflow 를 사용하여, loginSucc가 출력되는 시작점의 주소값을

Rtn addr 를 넣는 곳에 끼워 맞춰 넣어, 입력없이 로그인이 될 수 있도록 할 것 입니다.



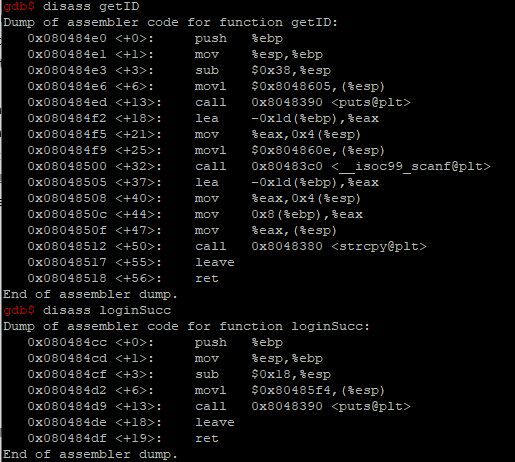


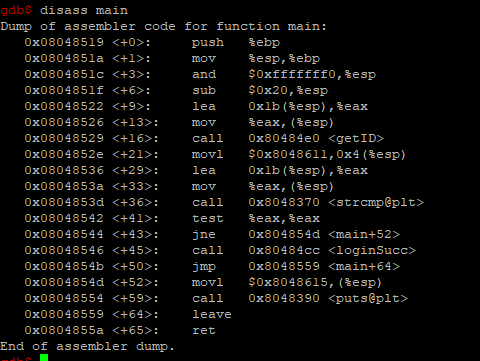
실행을 해보았습니다.





앞서 사용하였던 inp-write 파일을 변형하여 사용 할 것입니다.



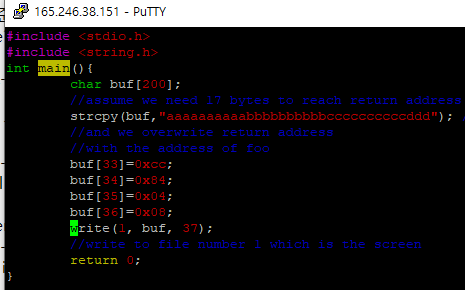


<loginSucc>를 호출하는 부분이 아래에서 6번쨰 줄에 있습니다.

Addr = [080484cc] 입니다.

Lea 0x1d 만큼의 공간과 push 이므로 29+4한 33에

loginSucc 의 시작 주소값을 넣어줍니다.

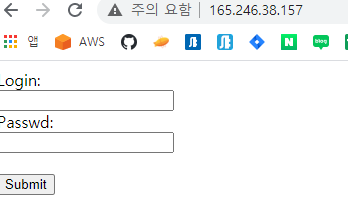


최종 mid-write.c 코드는 위와 같습니다.



결과가 출력되었습니다.

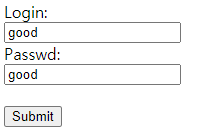
2.



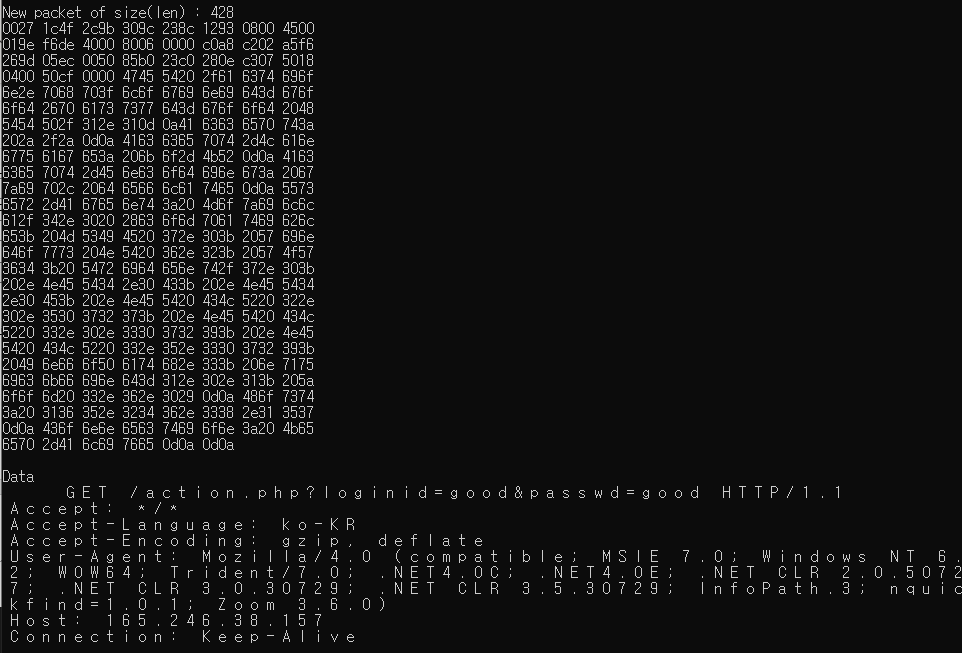
로그인 창입니다.



165.246.38.157 and port 80 을 통해 이로 다니는 데이터를 캐치하려고 합니다.

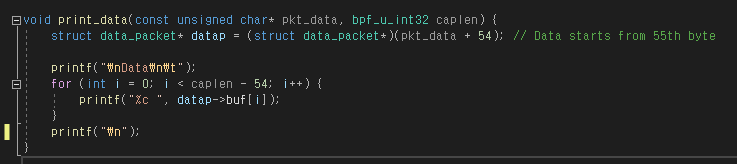


good / good 을 넣어 data패킷 부분을 확인해 보았습니다.



G E T / a c t i o n . p h p ? l o g i n i d = g o o d & **p a s s w d = g o o d** H T T P / 1 . 1

이 부분이 비밀번호를 가지고 있는 것을 확인했습니다.



즉, 위 부분을 수정하여,

Passwd= ~ http 사이의 값을 가져올 수 있도록 하면

비밀번호를 캐치할 수 있게됩니다. 저는 우선,

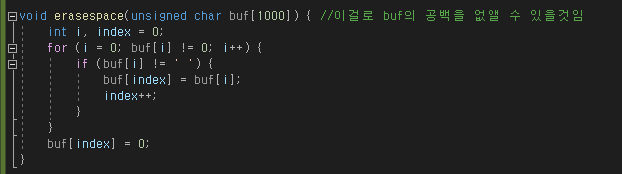
1) 위 데이터부분 값들의 공백을 없앤다.

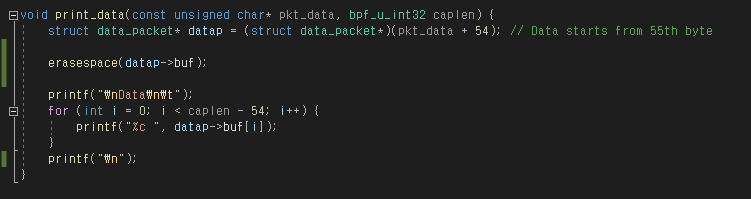
2) 데이터 전체를 끝까지 확인해보며 ‘passwd=’ 인 곳을 찾는다.

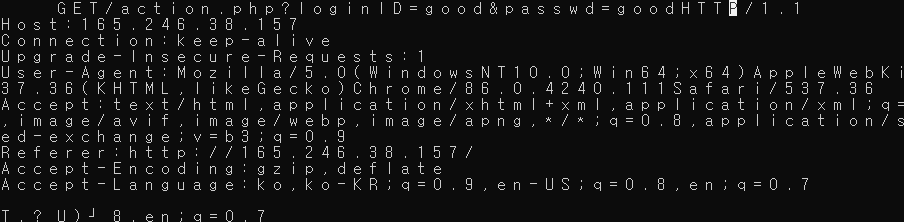
또한, ‘http’ 인곳을 찾는다.

3)그사이의 값을 출력하도록 한다.

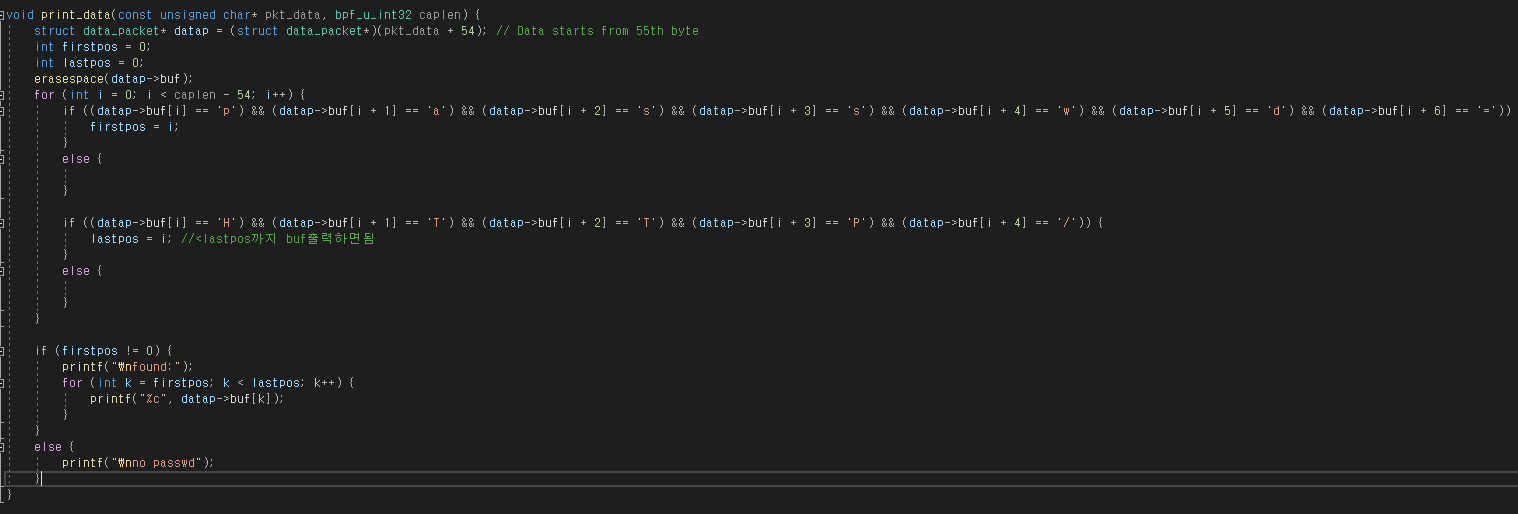
이 flow로 문제를 해결하도록 하겠습니다. ( 혹시 비밀번호가 http이거나 passwd 일경우에는 cover가 불가능하지만, 우선 생각나는 방법이 위의 방법이라 사용하도록 하겠습니다.)







간격이 사라졌습니다.



void print\_data(const unsigned char\* pkt\_data, bpf\_u\_int32 caplen) {

struct data\_packet\* datap = (struct data\_packet\*)(pkt\_data + 54); // Data starts from 55th byte

int firstpos = 0;

int lastpos = 0;

erasespace(datap->buf);

for (int i = 0; i < caplen - 54; i++) {

if ((datap->buf[i] == 'p') && (datap->buf[i + 1] == 'a') && (datap->buf[i + 2] == 's') && (datap->buf[i + 3] == 's') && (datap->buf[i + 4] == 'w') && (datap->buf[i + 5] == 'd') && (datap->buf[i + 6] == '=')) {

firstpos = i;

}

else {

}

if ((datap->buf[i] == 'H') && (datap->buf[i + 1] == 'T') && (datap->buf[i + 2] == 'T') && (datap->buf[i + 3] == 'P') && (datap->buf[i + 4] == '/')) {

lastpos = i; //<lastpos까지 buf출력하면됨

}

else {

}

}

if (firstpos != 0) {

printf("\nfound:");

for (int k = firstpos; k < lastpos; k++) {

printf("%c", datap->buf[k]);

}

}

else {

printf("\nno passwd");

}

}

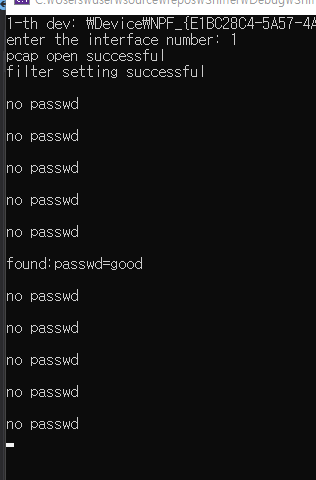
각 datap->buf[] 값을 for문을 돌려 확인하며,

Passwd= 를 찾은 지점의 첫부분,

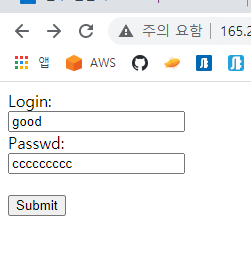
HTTP/를 찾은 지점의 첫부분을 구해

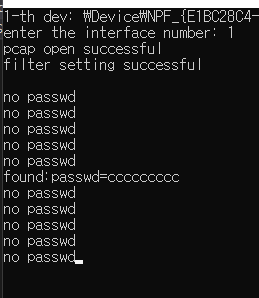
그 사이 값이 있으면, 비밀번호 이므로 그 값을 출력해주고,

없을 시에는 nopasswd 를 출력하도록 하였습니다.



결과입니다.





간격을 조절해주었고, 결과가 잘 출력되는 것을 확인하였습니다.