lotto보고서

pwnable.kr에 있는 lotto문제를 풀어보았다. 기본적으로 lotto문제도 c소스를 주지만 나는 gdb사용법과 더불어 어셈블리어를 공부하고 있기 때문에 핸드레이 해보았다. 핸드레이 해본 소스는 아래와 같다.

```
int play()
{
	int v8, v18, v14;
	char v10[6];


	printf("Submit your 6 lotto bytes : ");
	fflush(stdout);
	v18 = read(0, submit, 6);
	puts("Lotto Start!");
	v14 = open("/dev/urandom", 0);
	if(v14 == -1)
	{
		puts("error. tell admin");
		exit(-1);
	}
	if(read(v14, v10[6], 6) != 6)
	{
		puts("error2. tell admin");
		exit(-1);
	}
	int v24 = 0;
	for(; v24 <= 5; v24++)
	{
		v10[v24] = (v10[v24] % 45) + 1;
	}
	close(v14);

	int v1c = 0, v20 = 0;

	for(v24 = 0;v24 <= 5; v24++){
		for(v1c = 0; v1c < 5; v1c++){
			if(v10[v24] == submit[v1c])
				v20++;
		}
	}
	if(v20 == 6)
	{
		system("/bin/cat flag");
	}
	else
	{
		puts("bad luck...")
	}
```

```
void help()
{
	puts("- nLotto Rule -");
	puts("nlotto is consisted with 6 random natural numbers less than 46");
	puts("your goal is to match lotto numbers as many as you can");
	puts("if you win lottery for *1st place*, you will get reward");
	puts("for more details, follow the link below");
	puts("http://www.nlotto.co.kr/counsel.do?method=playerGuide#buying_guide01\n");
	puts( "mathematical chance to win this game is known to be 1/8145060.");
}



int main()
{
	int = v4;

	while(1)
	{
		puts("- Select Menu -");
		puts("1. Play Lotto");
		puts("2. Help");
		puts("3. Exit");
		scanf("%d", &v4);

		if(v4 != 2)
		{
			if(v4 != 3)
			{
				if(v4 == 1)
				{
					play();
				}
				else
				{
					puts("invalid menu");
				}
			}
			else
			{
				puts("bye");

				return 0;
			}
		}
		else
		{
			help();
		}
	}
}
```

메인 함수를 보게되면 1번을 누르면 play함수를 열게 되는데 문제의 의도를 보면 6개의 문자열을 받아 비교하여 6개의 문자가 다맞으면 /bin/cat flag를 system함수로 열게된다.

근데 여기서 이상한 점을 발견하게되는데 핸드레이 한 위의 소스를 보면 빨간색으로 칠해 놓았다.

v10과 submit안에 있는 값을 비교하여 같으면 계속 반복하여 v20이 6이되어 /bin/cat flag이 실행되게 된다!!

또한 여기서 주의할 점이 있는데 lotto에서 받는 6개를 문자열로 받기 때문에 1~45의 숫자를 아스키코드로 넣어 줘야 한다.

그럼한번 직접 실행 해보도록 하겠다!

```
lotto@ubuntu:~$ ./lotto
- Select Menu -
1. Play Lotto
2. Help
3. Exit
1
Submit your 6 lotto bytes : !!!!!!
Lotto Start!
```

flag 파일을 읽을 수 있었다.