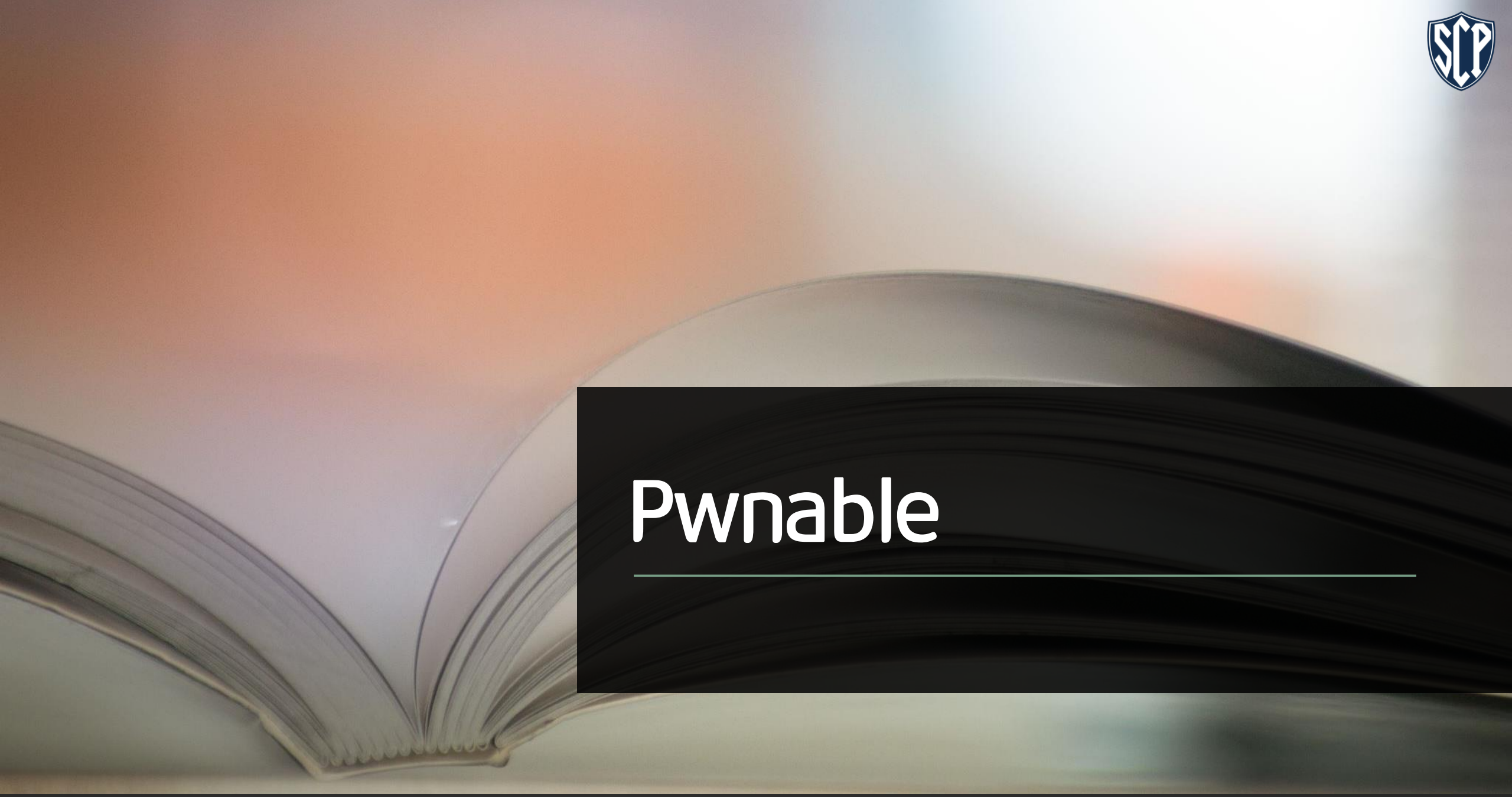
Pwnable Study

김수현

Contents



Pwnable

Pwnable

시스템 해킹이라고도 불리며,

OS 또는 프로그램의 취약점을 찾아 공격하여 관리자 권한 등을 얻어 시스템을 장악하는 것

FTZ

FTZ

Free Training Zone의 약자로써 해커스쿨에서 배포하는 워 게임

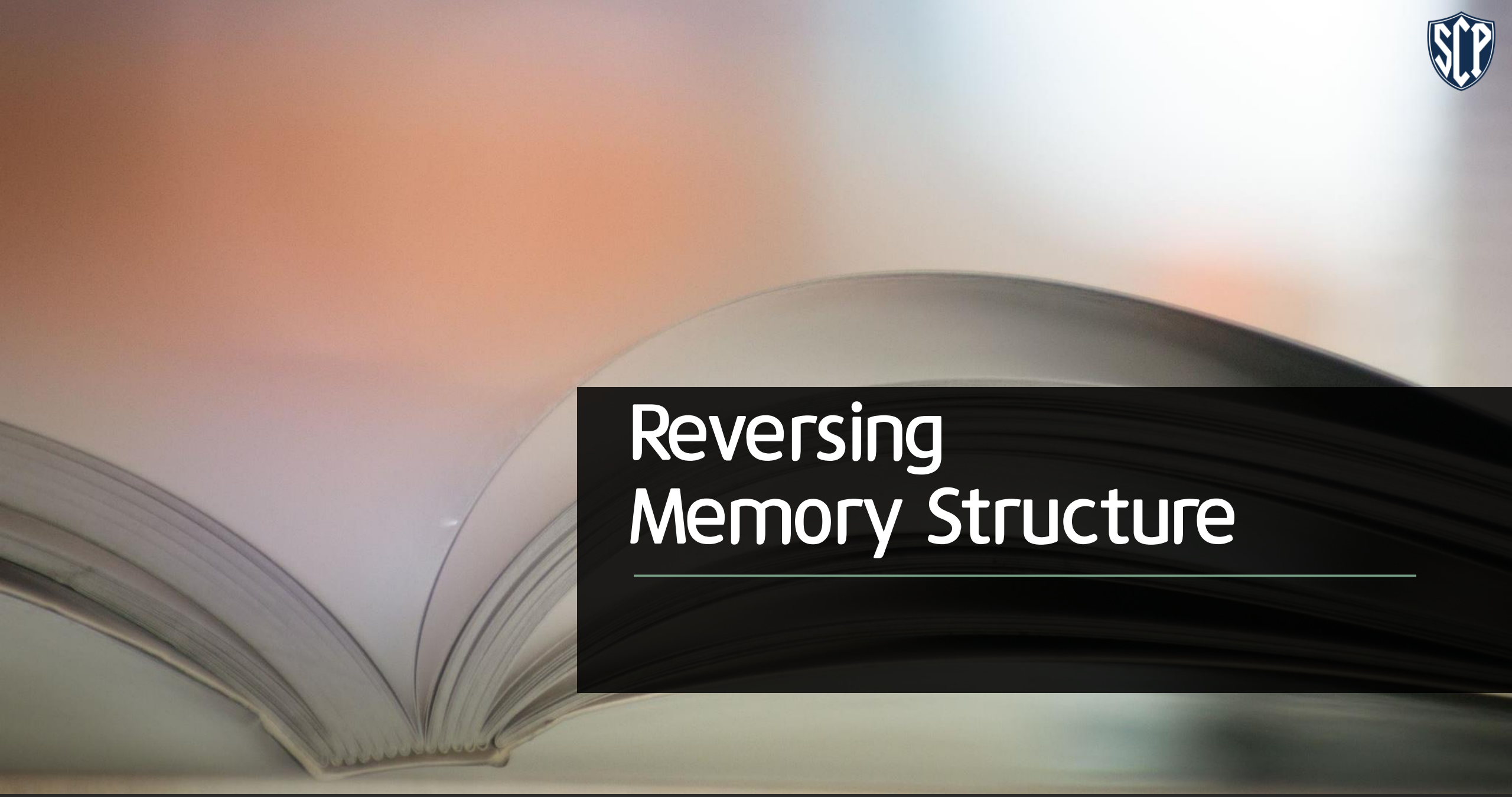
20 가지 문제와 여러 가지 시스템 해킹 기법을 무료로 트레이닝 할 수 있는 서버

FTZ 문제 구성

Level 01 ~ Level 08 → 리눅스 & 리눅스 기본 지식 / Write Up

Level 09 ~ Level 20 → BOF, FSB

FTZ Level 14



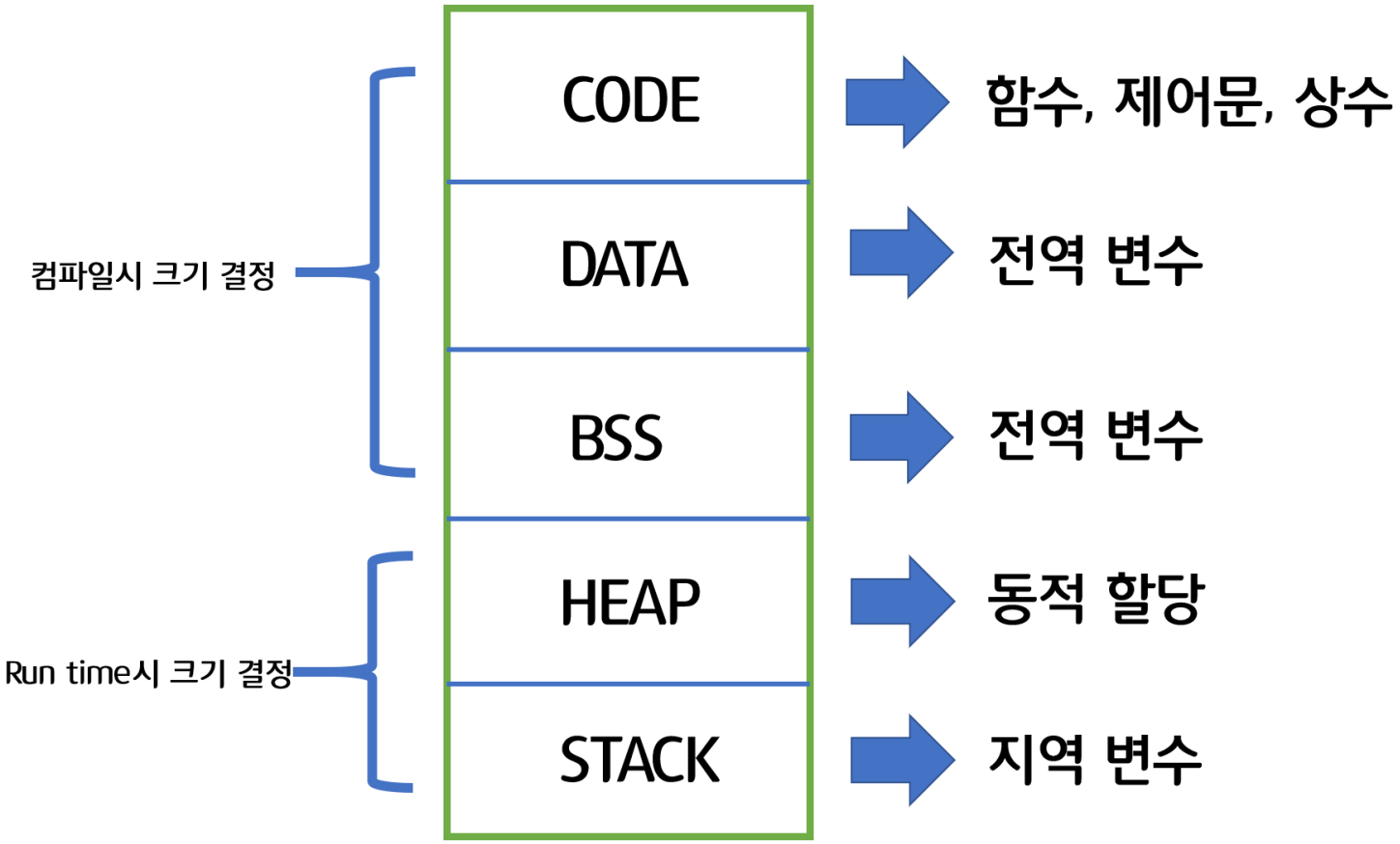
Reversing Memory Structure

Reversing

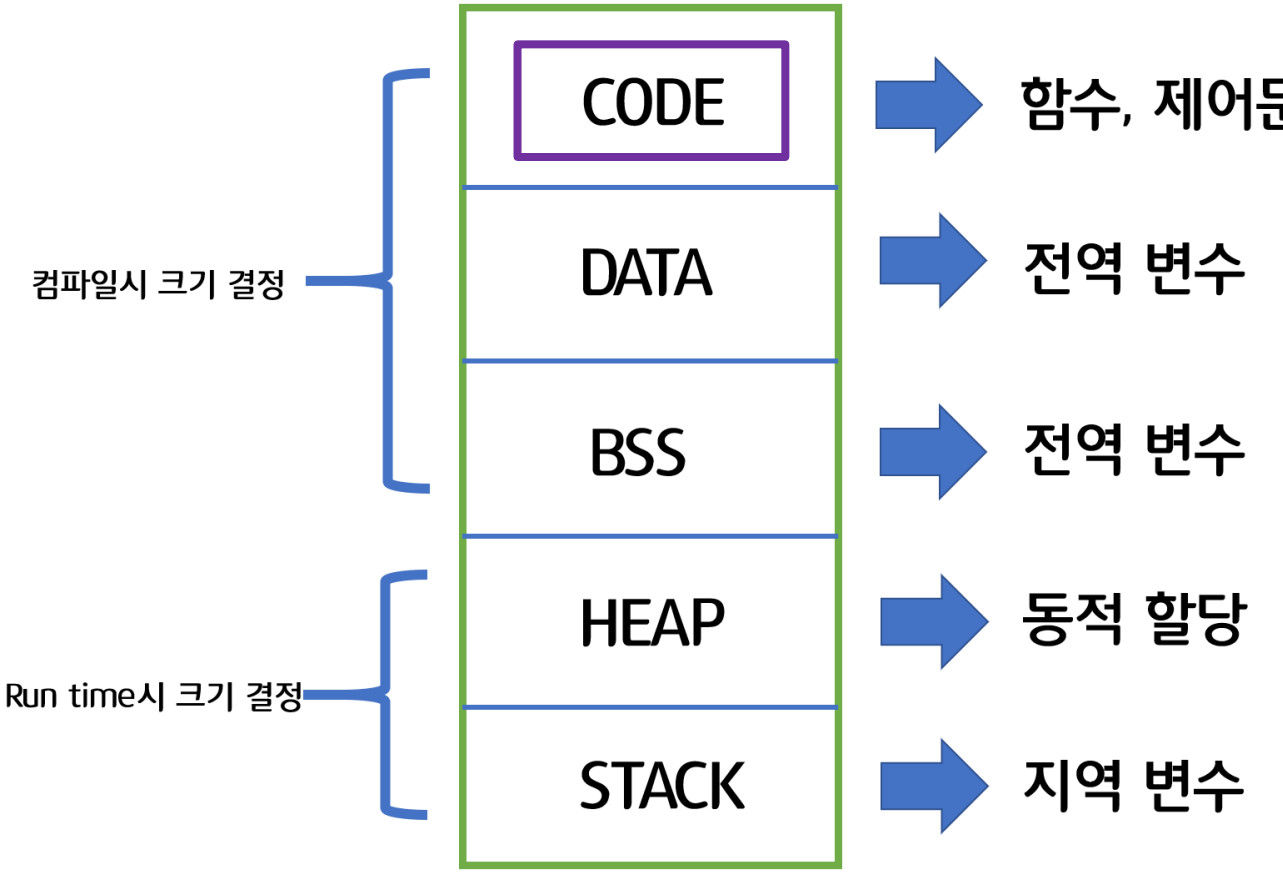
- 리버스 + 엔지니어링의 합성어로 리버스 엔지니어링의 줄임 말

- **이진 코드로 되어있는 실행 파일을 분석하려는 행위이며, 소프트웨어를 분석학 동작을 해명해 나가는 행위**

- 원리를 이해하며 단점을 보완하고 새로운 아이디어를 추가하는 일련의 작업을 의미

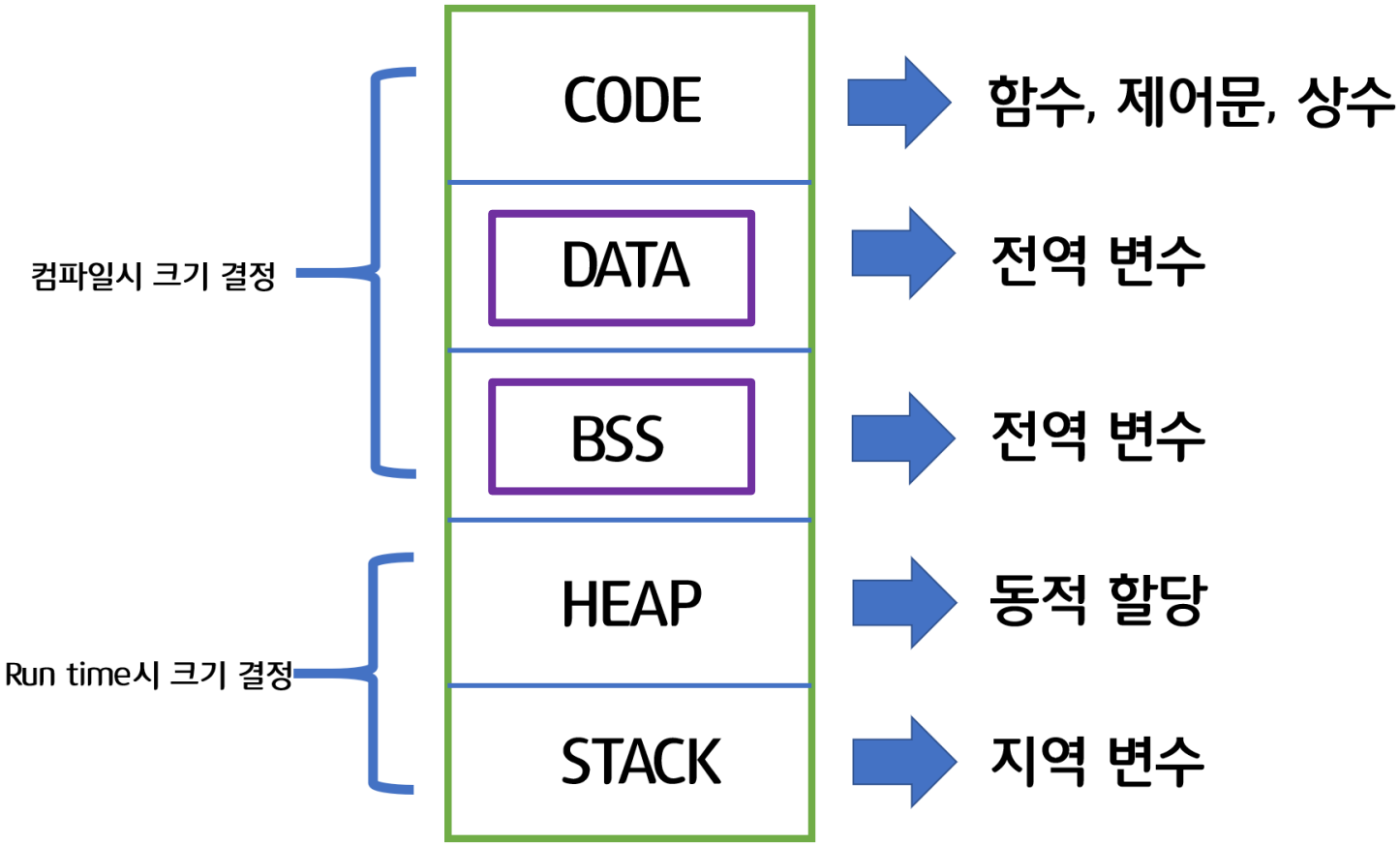


Memory Structure



CODE

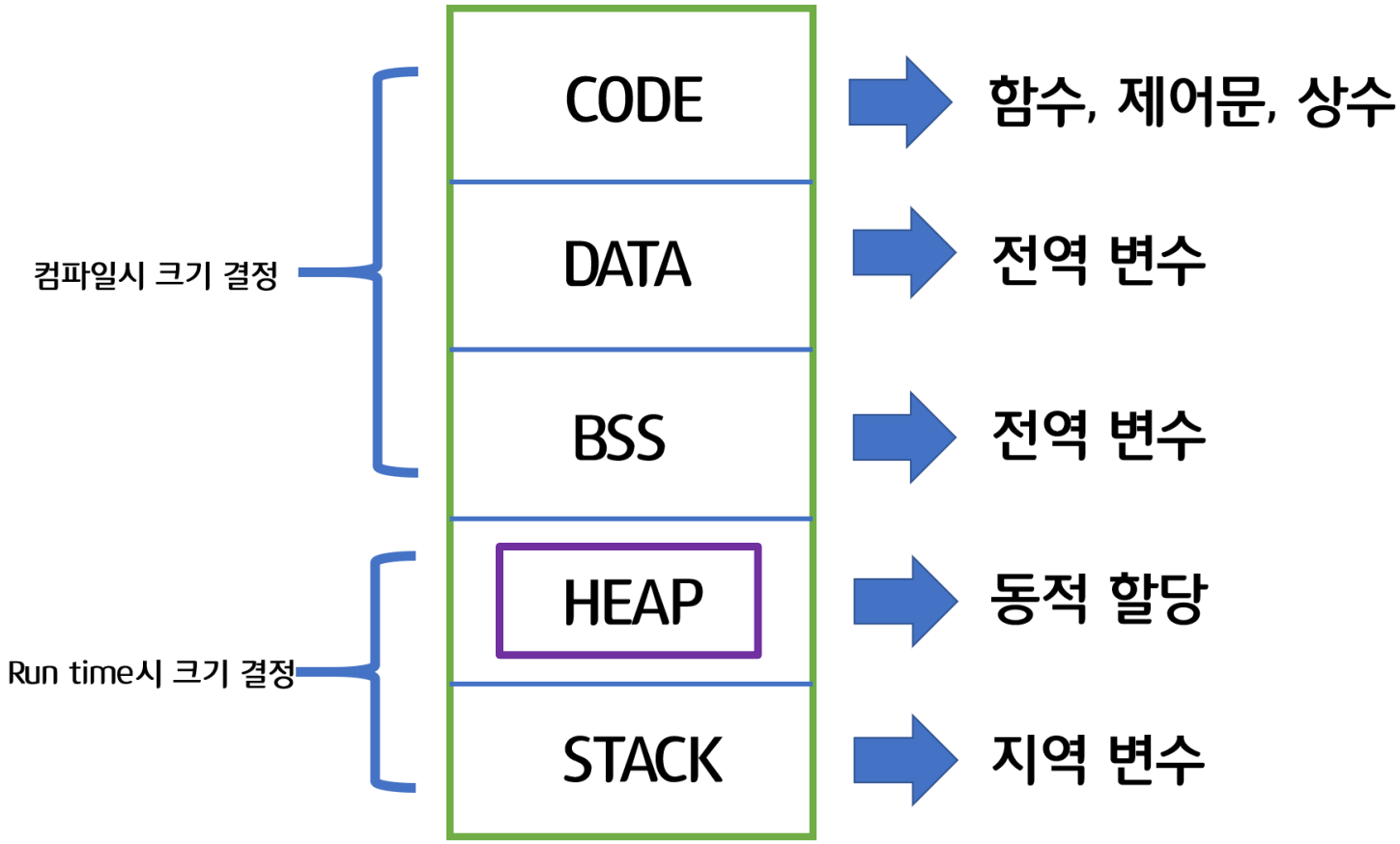
프로그램 소스코드 저장



DATA & BSS

전역변수 (Global), 정적변수 (Static),
배열 (array), 구조체 (Structure) 등
저장

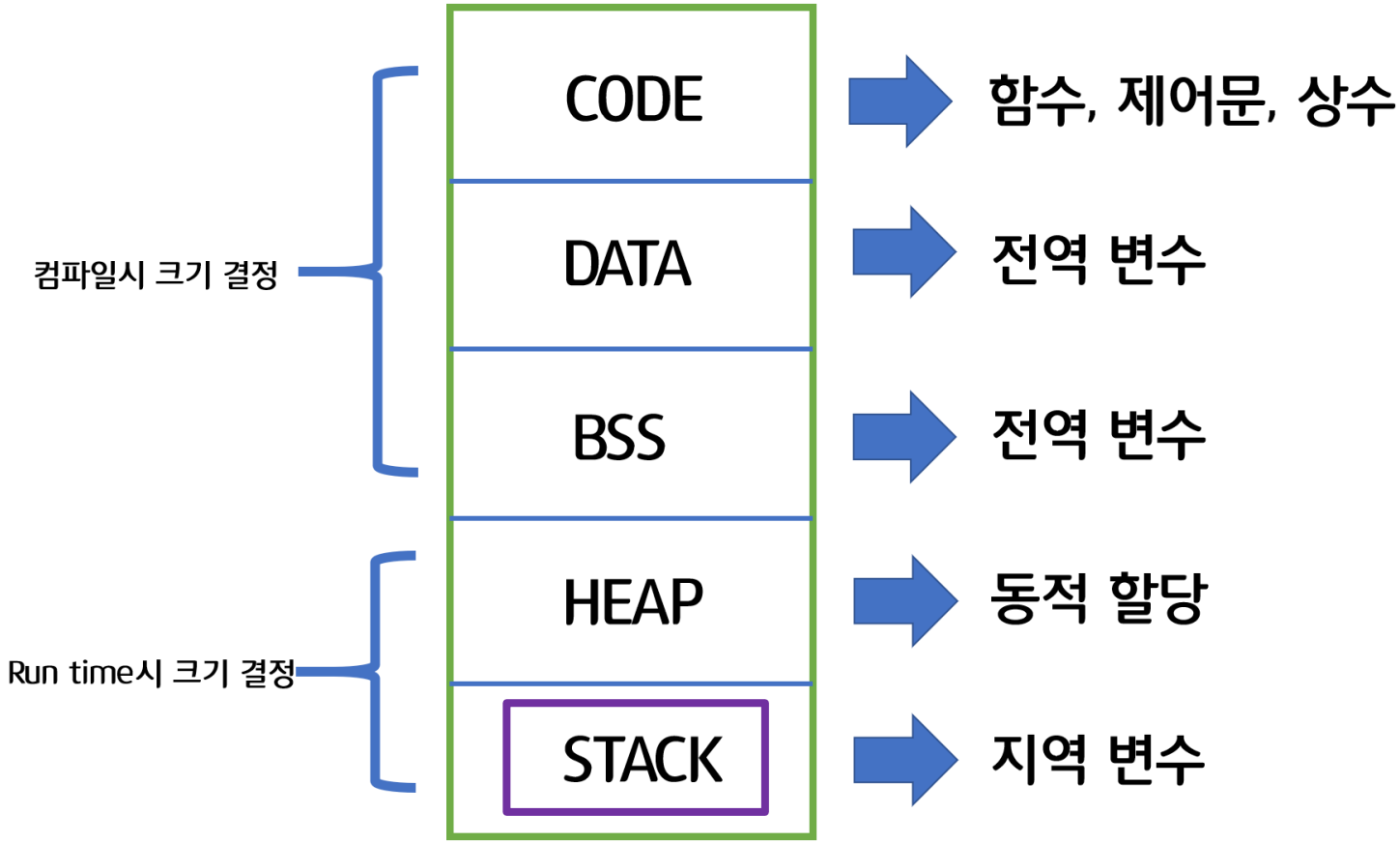
초기화 된 데이터는 data 영역,
초기화 되지 않은 데이터는
BSS 영역에 저장



HEAP

크기가 변함,
프로그래머의 필요에 따라 할당하여 사용 할 수 있음

위에서부터 아래로 채워 짐



STACK

크기가 변함, 지역변수 저장

스택에는 여러개의 스택 프레임 존재

커널영역을 침범하지 않도록
+
데이터 용량의 불확실성을 가짐

-> 따라서 아래서부터 채움

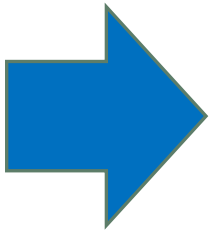
HEAP & STACK Overflow

HEAP Overflow

- heap 영역이 stack 영역 침범

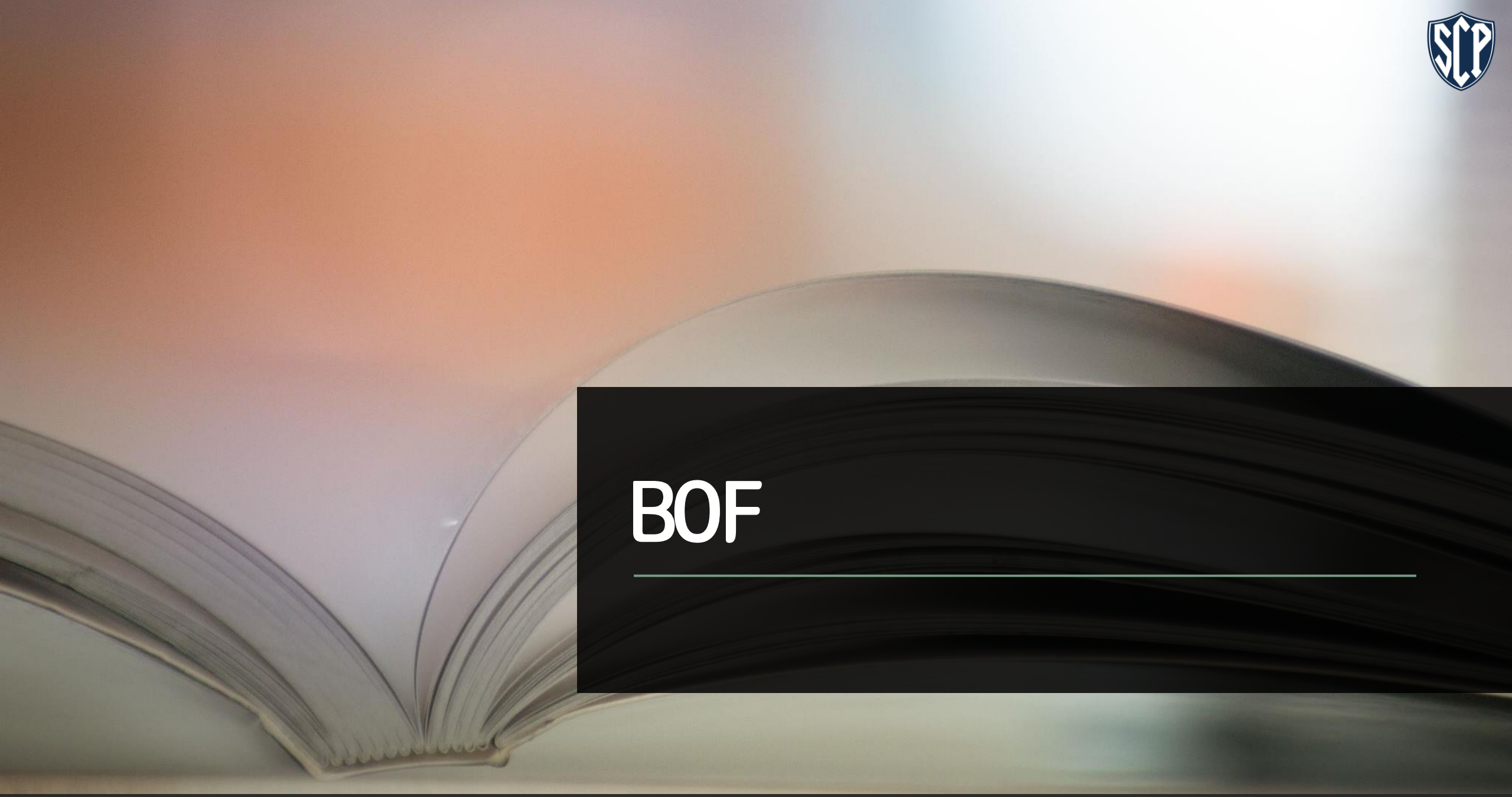
STACK Overflow

- stack 영역이 heap 영역 침범



HEAP & STACK 영역이 서로 반대로 채워지기 때문에
서로의 영역을 침범 할 수 있음

이를 이용해 공격 가능



BOF

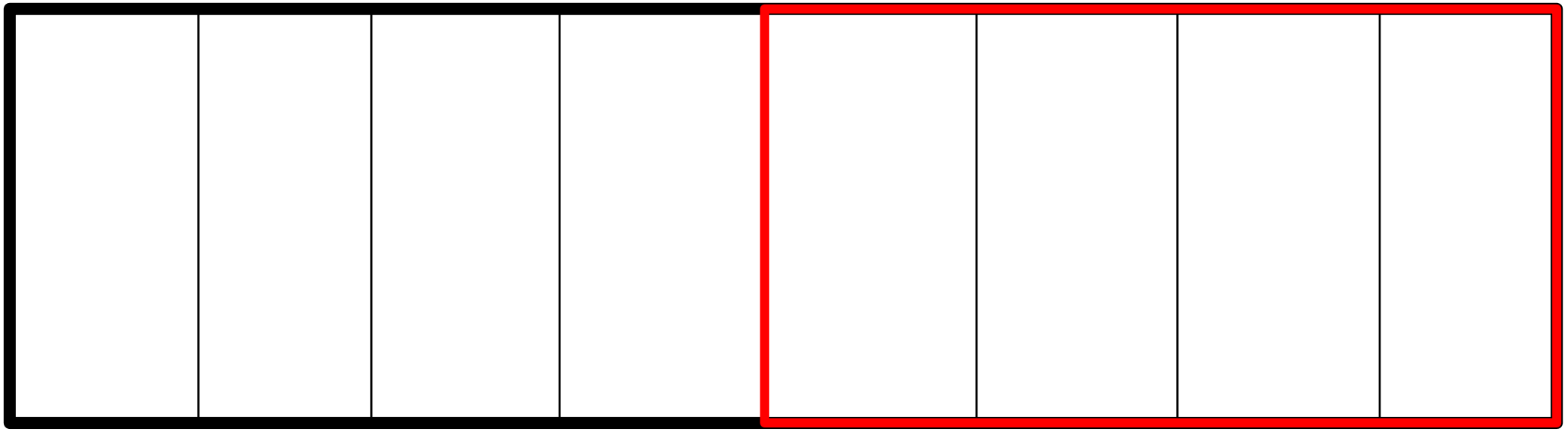
Buffer Overflow

- 버퍼를 넘치게 하는 것을 의미

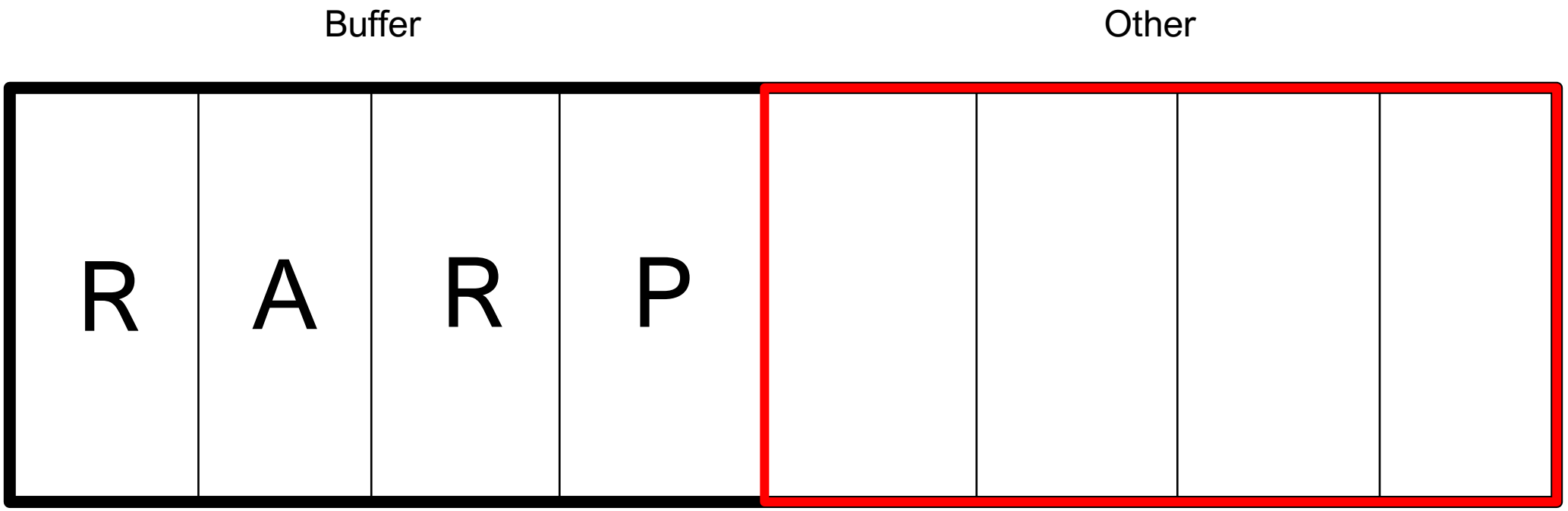
- 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소를 조작해 궁극적으로 해커가 원하는 코드를 실행 하는 것

Buffer Overflow

R A R P S Buffer Other

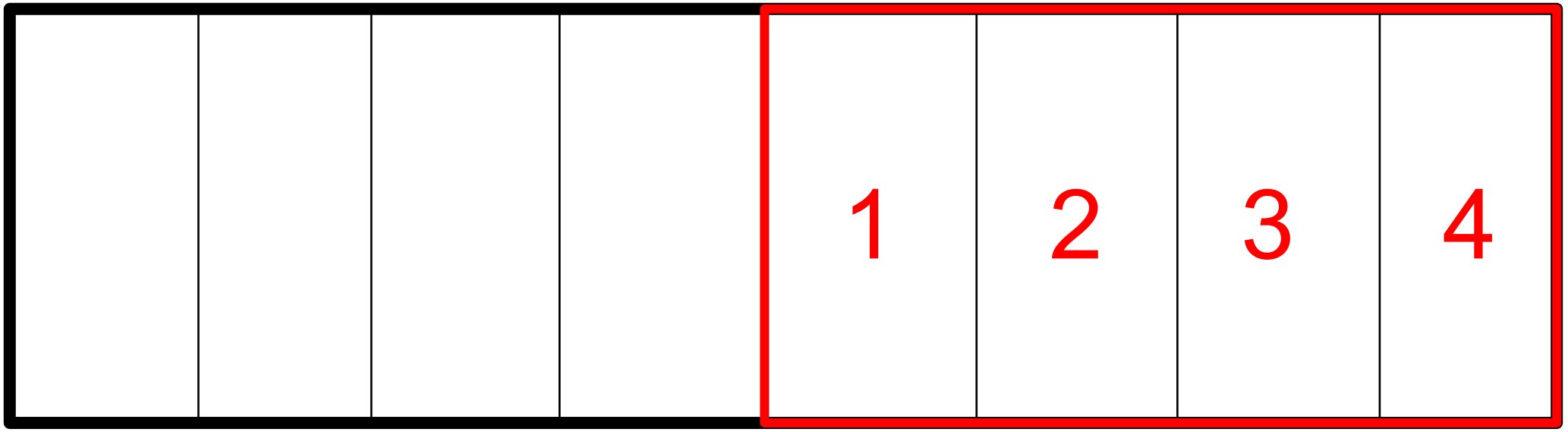


Buffer Overflow

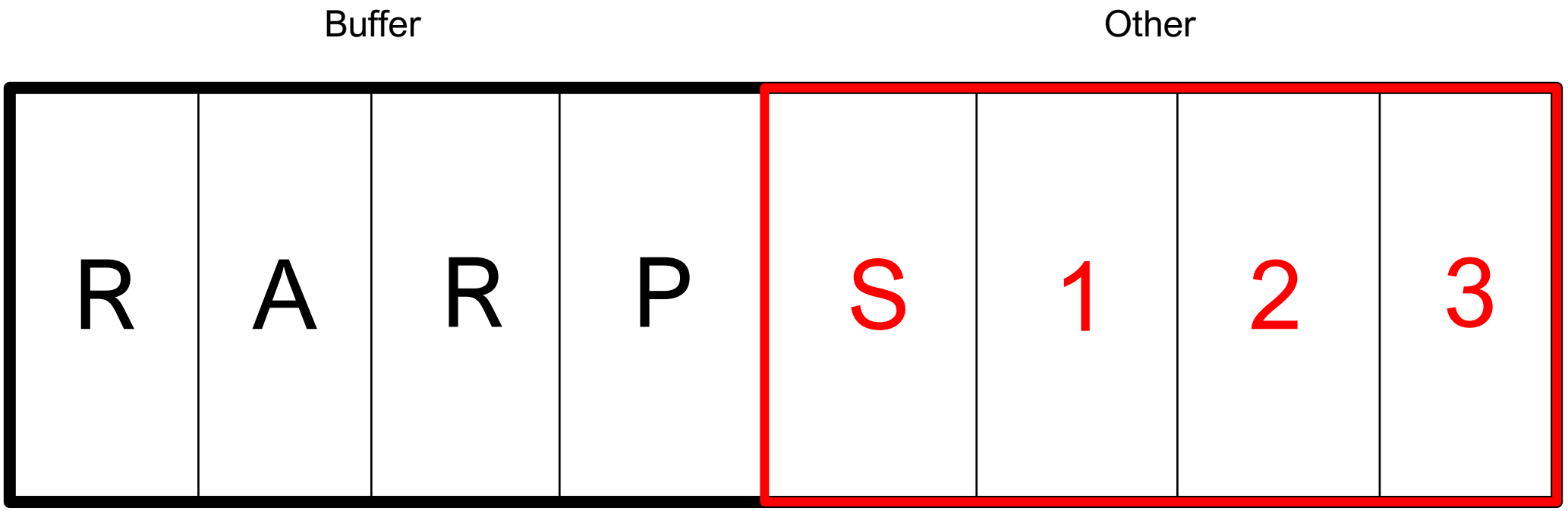


Buffer Overflow

R A R P S Buffer Other

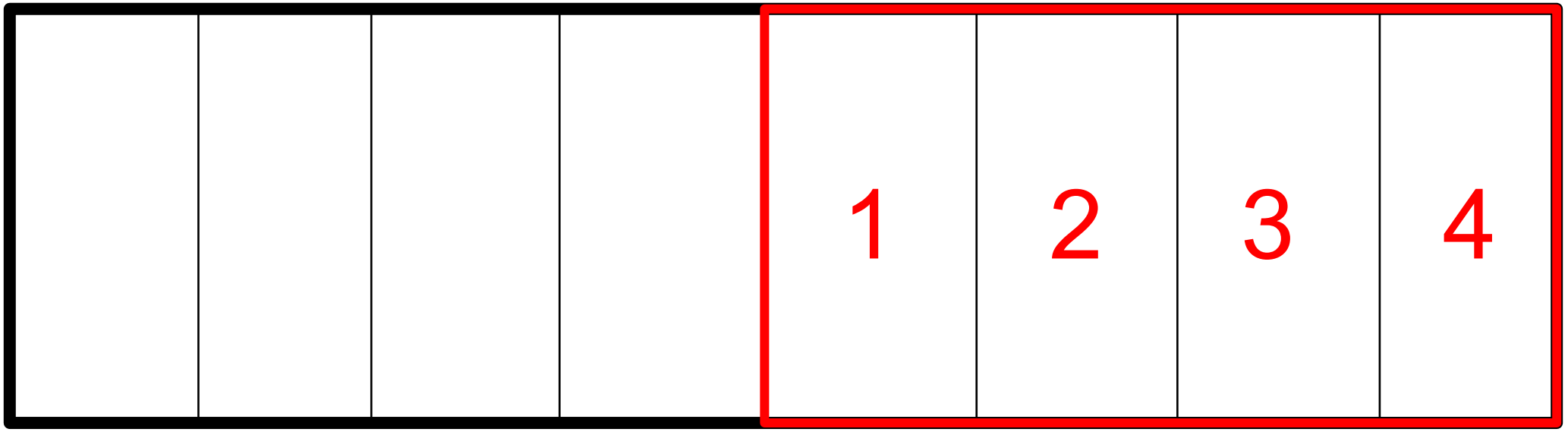


Buffer Overflow



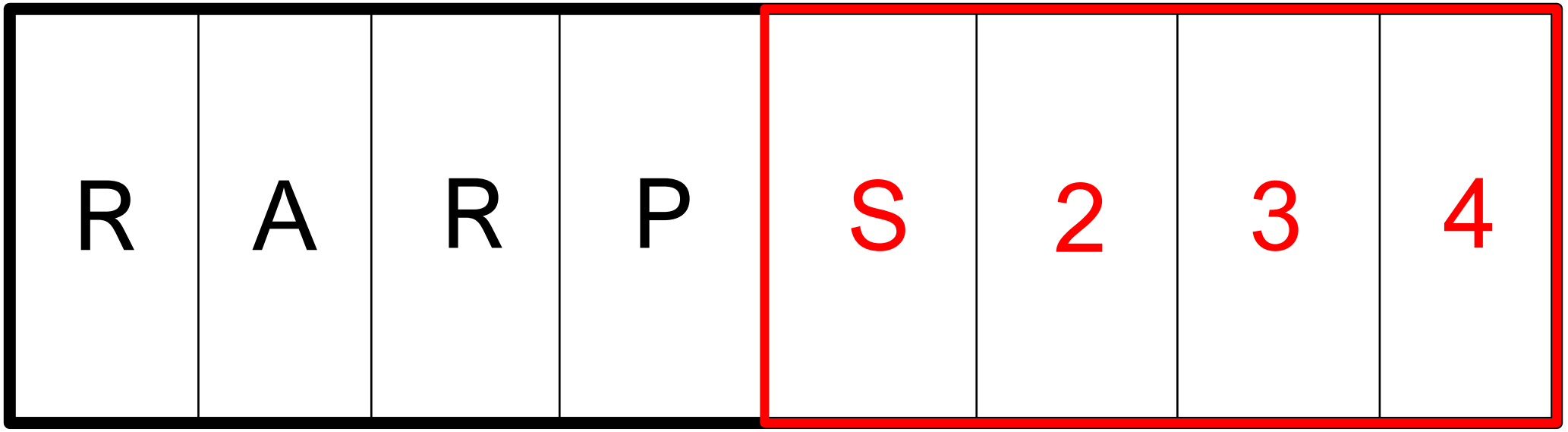
Buffer Overflow

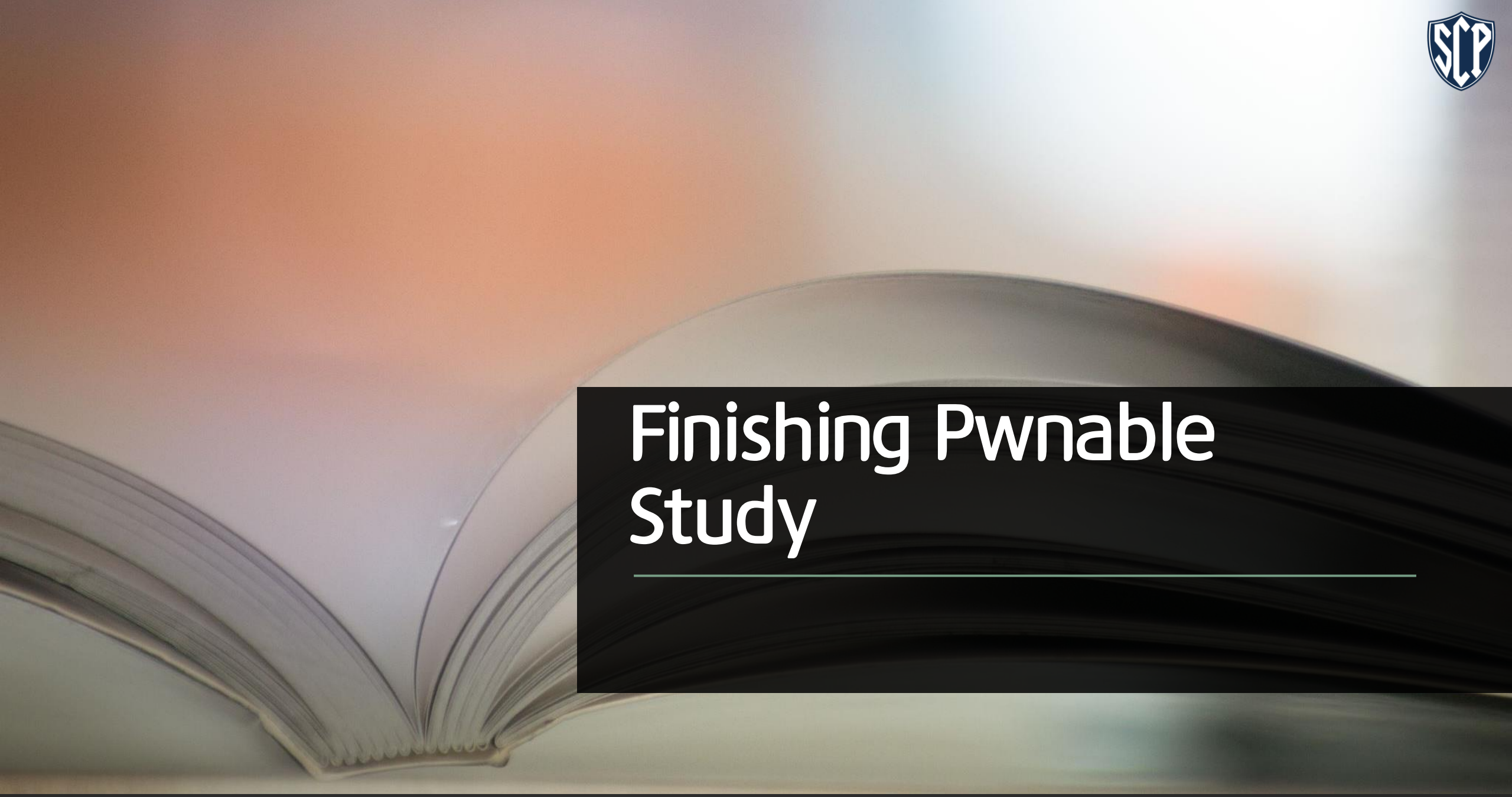
R A R P S Buffer Other



Buffer Overflow

R A R P S Buffer Other





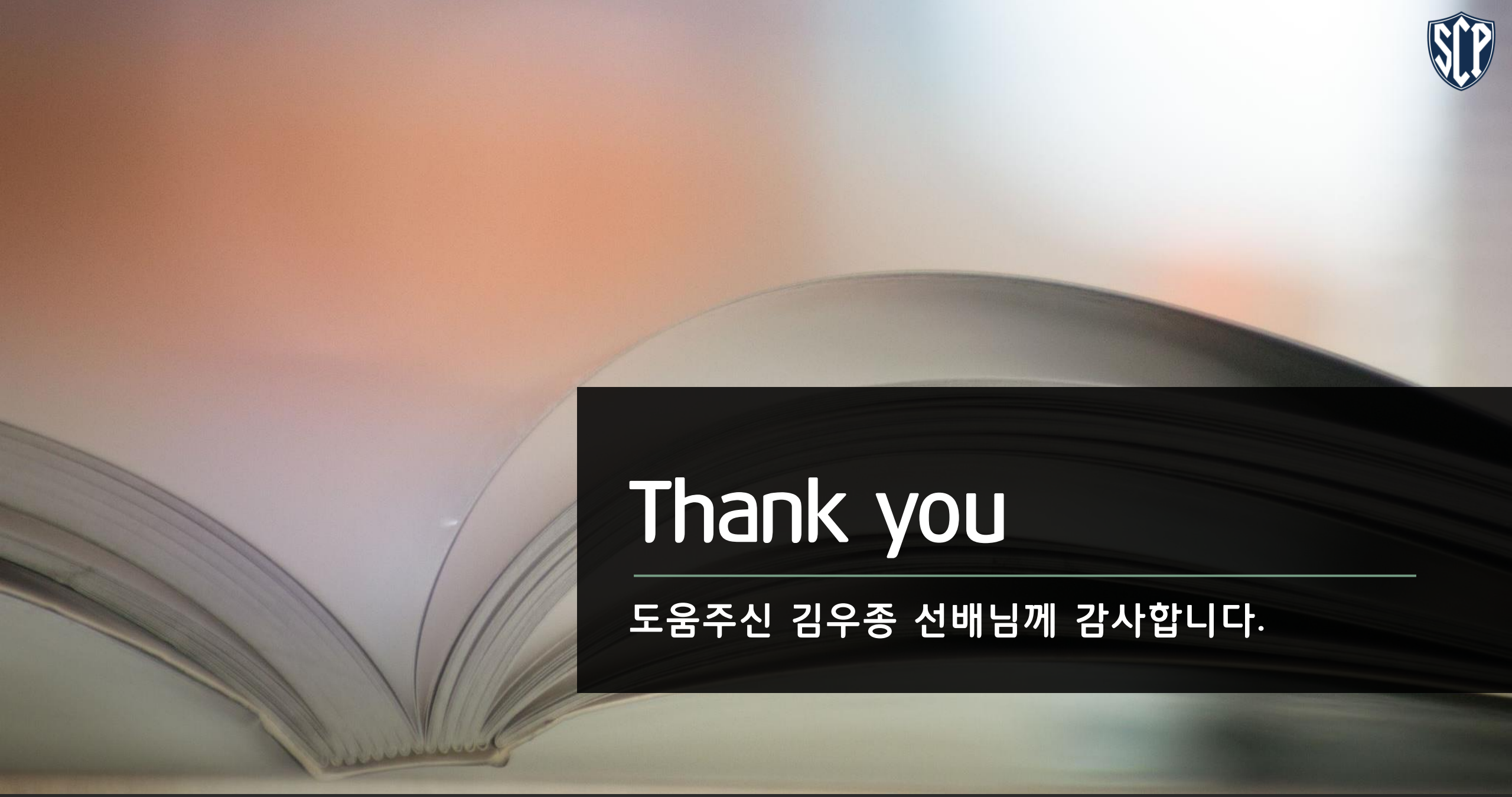
Finishing Pwnable Study

Finishing Pwnable Study

!! 메모리 구조 !!

!! 리버싱 !!

포기하지않고 인내를
가지고 천천히 계속



Thank you

도움주신 김우종 선배님께 감사합니다.