

Forum: [Hack Forums](#)

Thread: [THE MOST EXTENSIVE MYSQL DEFENSE AND COUNTERRECON CHEATSHEET EVER](#)

Clumsy - December 4, 2025, 11:53 am

SERVER ENUMERATION AND DISCOVERY

SHOW DATABASES

SHOW SCHEMAS

SHOW TABLES

SHOW TABLE STATUS

SHOW VARIABLES

SHOW GLOBAL VARIABLES

SHOW SESSION VARIABLES

SHOW STATUS

SHOW GLOBAL STATUS

SHOW SESSION STATUS

SHOW PROCESSLIST

SHOW FULL PROCESSLIST

SHOW OPEN TABLES

SHOW ENGINES

SHOW STORAGE ENGINES

SHOW CHARACTER SET

SHOW COLLATION

SHOW INDEX FROM anytable

SHOW EVENTS

SHOW TRIGGERS

SHOW PROCEDURE STATUS

SHOW FUNCTION STATUS

SHOW CREATE DATABASE dbname

SHOW CREATE TABLE tablename

SHOW CREATE TRIGGER name

SHOW CREATE VIEW name

SHOW CREATE PROCEDURE name

SHOW CREATE FUNCTION name

SHOW CREATE EVENT name

SHOW GRANTS

SHOW GRANTS FOR user@host

SHOW PRIVILEGES

SHOW PLUGINS

SHOW PROFILE

SHOW PROFILES

SHOW MASTER STATUS

SHOW REPLICA STATUS

SHOW BINLOG EVENTS

SHOW BINARY LOGS

SHOW VARIABLES LIKE secure_file_priv

SHOW VARIABLES LIKE log_bin

SERVER STATE CONTROL AND RESET

FLUSH PRIVILEGES
FLUSH TABLES
FLUSH HOSTS
FLUSH LOGS
FLUSH STATUS
FLUSH DES_KEY_FILE
FLUSH ENGINE LOGS
FLUSH OPTIMIZER_COSTS

DATABASE CREATION AND CONTROL

CREATE DATABASE dbname
CREATE DATABASE dbname CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci
DROP DATABASE dbname
ALTER DATABASE dbname UPGRADE DATA DIRECTORY NAME
ALTER DATABASE dbname CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci

USER AND ACCESS MANAGEMENT

CREATE USER user@host IDENTIFIED BY password
DROP USER user@host
ALTER USER user@host IDENTIFIED BY newpass
SET PASSWORD FOR user@host
ACCOUNT LOCK user@host
ACCOUNT UNLOCK user@host
RENAME USER old@host TO new@host
GRANT ALL PRIVILEGES ON db to user@host WITH GRANT OPTION
GRANT SELECT INSERT UPDATE DELETE ON db to user@host
GRANT PROCESS ON to user@host
GRANT REPLICATION SLAVE ON to user@host
GRANT REPLICATION CLIENT ON to user@host
REVOKE ALL PRIVILEGES FROM user@host
REVOKE GRANT OPTION FROM user@host

TABLE MANAGEMENT AND SCHEMA CONTROL

RENAME TABLE a TO b
ALTER TABLE tablename ADD COLUMN col type
ALTER TABLE tablename DROP COLUMN col
ALTER TABLE tablename MODIFY COLUMN col type
ALTER TABLE tablename CHANGE old new type
ALTER TABLE tablename ENGINE engine
CHECK TABLE tablename
OPTIMIZE TABLE tablename
ANALYZE TABLE tablename
REPAIR TABLE tablename
TRUNCATE TABLE tablename
DROP TABLE tablename

DATA OPERATIONS AND FORENSIC REVIEW

SELECT FROM tablename
SELECT COUNT(*) FROM tablename
SELECT DISTINCT col FROM tablename
SELECT col FROM tablename ORDER BY col ASC
SELECT col FROM tablename LIMIT number
SELECT FROM tablename WHERE col LIKE pattern

SELECT FROM tablename WHERE col IN set
SELECT FROM tablename WHERE col BETWEEN a AND b
SELECT FROM tablename WHERE col REGEXP regex
UPDATE tablename SET col=value WHERE condition
DELETE FROM tablename WHERE condition
INSERT INTO tablename (a,b) VALUES (x,y)

JOIN AND UNION DETECTION AND ANALYSIS

SELECT a.x b.y FROM t1 a INNER JOIN t2 b ON a.id=b.id
SELECT a.x b.y FROM t1 a LEFT JOIN t2 b ON a.id=b.id
SELECT a.x b.y FROM t1 a RIGHT JOIN t2 b ON a.id=b.id
SELECT col FROM t1 UNION SELECT col FROM t2
SELECT col FROM t1 UNION ALL SELECT col FROM t2

INDEX CONTROL AND PERFORMANCE SAFETY

CREATE INDEX idx ON tablename (col)
DROP INDEX idx ON tablename
ALTER TABLE tablename ADD INDEX idx (col)
ALTER TABLE tablename DROP INDEX idx
EXPLAIN SELECT query
EXPLAIN ANALYZE SELECT query

BACKUP AND RESTORE

mysqldump full backup
mysqldump table backup
mysqldump routine backup
mysql restore plaintext
mysql restore selective

TRANSACTIONS AND DAMAGE MITIGATION

START TRANSACTION
SAVEPOINT name
ROLLBACK TO name
COMMIT
ROLLBACK

ROUTINES, FUNCTIONS, AND ATTACK SURFACE CONTROL

DELIMITER //
CREATE PROCEDURE name begin end //
DELIMITER
DROP PROCEDURE name
CREATE FUNCTION name returns type begin end
DROP FUNCTION name
ALTER ROUTINE name COMMENT text
SHOW CREATE PROCEDURE name
SHOW CREATE FUNCTION name

VIEWS AND SECURITY DEFINERS

CREATE VIEW vname AS select
DROP VIEW vname
ALTER VIEW vname AS select
CHECK OPTION for view consistency
SQL SECURITY DEFINER review

SQL SECURITY INVOKER review

TRIGGERS AND INJECTION SURFACE CONTROL

CREATE TRIGGER trig BEFORE INSERT ON tablename FOR EACH ROW begin end
CREATE TRIGGER trig AFTER INSERT ON tablename FOR EACH ROW begin end
DROP TRIGGER trig
SHOW TRIGGERS
VERIFY DEFINER for triggers
VERIFY unintended data flows

EVENT SCHEDULER COUNTER-INTEL

CREATE EVENT ev ON SCHEDULE EVERY 1 MINUTE DO query
ALTER EVENT ev ON COMPLETION PRESERVE
DROP EVENT ev
SHOW EVENTS
Audit any unexpected scheduled events
Audit any definers on events

REPLICATION SECURITY AND FORENSICS

CHANGE MASTER TO parameters
RESET MASTER
RESET SLAVE
START SLAVE
STOP SLAVE
SHOW SLAVE STATUS
SHOW REPLICA STATUS
GTID monitoring
Relay log validation
Replication channel integrity checks

LOGGING AND FORENSIC COLLECTION

SET GLOBAL general_log ON
SET GLOBAL general_log OFF
SET GLOBAL slow_query_log ON
SET GLOBAL slow_query_log OFF
SET GLOBAL log_output TABLE
SET GLOBAL log_output FILE
SELECT FROM mysql.general_log
SELECT FROM performance_schema.events_statements_history
SELECT FROM performance_schema.threads
SELECT FROM performance_schema.accounts
Audit queries containing suspicious patterns
Audit metadata enumeration patterns

AUDIT FOR POSSIBLE ABUSE ATTEMPTS

SELECT FROM mysql.general_log WHERE argument LIKE system keyword
SELECT FROM mysql.general_log WHERE argument LIKE load keyword
SELECT FROM mysql.general_log WHERE argument LIKE information schema
SELECT FROM mysql.general_log WHERE argument LIKE select from mysql
SELECT * FROM information_schema.user_privileges ORDER BY grantee
SELECT user host plugin FROM mysql.user
Audit users with wildcard hosts
Audit users with FILE privilege

Audit users with SUPER privilege

HARDENING MODULE ALL LEVELS

- Disable remote root entirely
- Force TLS and modern ciphers
- Force strong authentication plugin
- Disable anonymous accounts
- Restrict FILE operations
- Set secure_file_priv
- Disable LOCAL INFILE
- Disable symbolic links
- Enforce strict SQL mode
- Enforce full mode set
- Disable old password protocol
- Enable audit plugin when possible
- Set binary log integrity checks
- Set maximum connection rate limits
- Enable firewall rules by host
- Segment database network
- Disable performance schema visibility for untrusted users
- Disable INFORMATION_SCHEMA visibility
- Disable EVENT SCHEDULER unless required
- Disable SUPER privileges for all apps
- Disable DEFINER routines unless necessary
- Use SELinux or AppArmor confinement
- Encrypt data at rest
- Encrypt backups
- Passphrase protect keysets
- Do not store credentials in scripts
- Use hardware key token for master passwords

INTRUSION DETECTION AND REALTIME MONITORING

- Monitor unknown DEFINER routines
- Monitor unknown scheduled events
- Monitor new replication users
- Monitor new grants
- Monitor failed logins
- Monitor long running queries
- Monitor sleep based timing probes
- Monitor metadata enumeration spikes
- Monitor sudden table scans
- Monitor replication desync
- Monitor binary log removals
- Monitor plugin installation
- Monitor UDF creation attempts
- Monitor temp table abuse
- Monitor large UNION or JOIN scans

FORENSIC CHECKLIST

- Compare grants with baseline
- Compare mysql.user structure with baseline
- Hash all tables and detect drift
- Review binary logs for suspicious writes

- Review general logs for enumeration
- Review slow logs for timing probes
- Review schema for unauthorized changes
- Export performance schema state
- Snapshot disk and RAM
- Quarantine server
- Rotate all credentials
- Rebuild from trusted image if compromised

MILITARY TIER ZERO TRUST DB MODEL

- No implicit trust from networks
- Every user role constrained
- Every query inspectable
- Every administrative session logged
- No wildcard hosts
- No legacy auth
- No unaudited routines
- No uncontrolled events
- No insecure replication
- No exposed metadata
- No plaintext backups
- No unnecessary plugins