- Filename: eccouncil-ceh31250-v10-15-1-1-sql_concepts.md
- Show Name: CEHv10 (312-50)
- Topic Name: SQL Injection
- Episode Name: SQL Concepts
- Description: In this episode, Daniel and Zach introduce you to a common and popular type of injection attack; the SQL Injection attack. Here they will start by explaining the why and how of a SQLi attack. Then they will dig into a web application to perform authentication bypass using SQLi and even look at the underlying code that allows for the issue to occur.

==

SQL Concepts

- **What is SQL Injection?**
    - Vulnerability in web applications from insecure coding practice that allows an attacker to...
        - Bypass authentication
        - Gain access to sensitive information
        - Modify or delete data
        - Create data
        - Execute remote code
    - **What issue allows for this?**
        - No data sanitization
    - **Which relational databases are vulnerable?**
        - ALL of them
    - **Can you show us how this works?**
        - Let's look at the bWAPP Login Form SQLi exercise
            - http://bwapp.com/bWAPP/sqli_3.php
            - Attempt to login
            - Inject SQL bypass
            - Explain why bypass works
                - Look at code for `sqli_3.php`