- Filename: eccouncil-ceh31250-v10-14-1-4-common_web_app_threats_pt4.md
- Show Name: CEHv10 (312-50)
- Topic Name: Hacking Web Applications
- Episode Name: Common Web App Threats Pt.4
- Description: In this episode, Daniel and Zach walk you through the plethora of threats geared toward Web Applications. Here they will demonstrate how Cross-Site Scripting(XSS) can be used to execute arbitrary code and Social Engineering attacks. Then they discuss the issues of using known dangerous components (demonstrating the Shellshock vulnerability) and allowing for Indirect Object References(IDOR).

==========

Common Web App Threats Pt.4

- Cross-Site Scripting
    - Reflected
    - Stored
    - DOM
        - The target's browser does all the script rendering
            - Isn't rendered by either the...
                - Database
                - Web Server
        - **DEMO: DVWA**
            1. Choose language setting and submit
            2. In Address bar add XSS alert after Language type
            3. Get alert pop up
            4. Inspect element of Language and see how XSS has become apart of the Language type (injected into the DOM)
- Known Vulnerable Components
    - Heartbleed
    - Drupalgeddon
    - Shellshock (DEMO)
- Indirect Object Reference (IDOR)
    - bWAPP movie tickets