GETTING STARTED
WebApp CVEs

Common Vulnerabilities and Exposures (CVE) is a list of all publicly disclosed vulnerabilities. In this section, we will take a look at how to search for a publicly available exploit for a vulnerability and use it to compromise the target machine.

What will you learn?

- Searching for publicly available exploits
- Understanding the root cause of vulnerabilities
- Exploiting a vulnerability and compromising the target machine

References:
1. Common Vulnerability and Exposures (https://cve.mitre.org/cve/)
2. Exploit DB (https://www.exploit-db.com/)

Labs:

- Rails DoubleTap RCE
    - Objective: Exploit the Remote Code Execution vulnerability and execute arbitrary commands on the target machine.
- Laravel Unserialize RCE
    - Objective: Exploit the Insecure Deserialization vulnerability and execute arbitrary commands on the target machine.
- Vulnerable File Upload Widget
    - Objective: Exploit the arbitrary file upload vulnerability and execute arbitrary commands on the target machine.
- CVE-2018-7600
    - Objective: Exploit the Remote Code Execution vulnerability and execute arbitrary commands on the target machine.

More labs for this topic are available in the Web app CVEs section. The links to the subsection are mentioned below:
- CVE 2020
- CVE 2019
- CVE 2018
- CVE 2017
- CVE 2016
- Older CVEs