

# CPTC Week 3 Homework

## Web Apps

### Part 1: Questions (50pts)

- (40pts) Compare and contrast your choice of any 2 (or more) web app injection techniques. You may choose from the list below, or pick your own. Some things to think about are:
  - Prerequisites
  - Tooling/techniques used
  - Impact
  - Remediations

SQL Injection	Cross Site Scripting	Server Side Template Injection
Mass Assignment	LDAP Injection	Command Injection

- (10pts) You come across a PHP web application that is vulnerable to local file inclusion. You have determined that the web application is run under the context of the account `www-data`. What is one of the possible steps forward in this assessment? Please include your reasoning behind this approach.

### Part 2: Lab (50pts)

- (40pts) Complete the OWASP Top 10 TryHackMe room.  
(<https://tryhackme.com/room/owasptop10>)
- (10pts) Pick a vulnerability in the TryHackMe room that you found particularly interesting. Write a finding block to explain that vulnerability as if you were a professional penetration tester. Use these example reports that have finding blocks to design your own finding block. Ensure your finding block is designed well. [https://github.com/globalcptc/report\\_examples](https://github.com/globalcptc/report_examples).

## Deliverables

- Submit a PDF with all of the following:
  - Answers to all the questions
  - Screenshots showing full completion of the TryHackMe room
  - Your finding block for your vulnerability
- Make sure all sections and images are readable and labeled.
- Name the file with the following format: `FirstLast_CPTCHomework3.pdf`

If you are trying out for the team, make sure you submit your PDF in Canvas.