

Esoteric web vulnerabilities assignment

For this assignment you will need to solve 4 ctf challenges related to the lecture. The challenges are heavily inspired by challenges present at TDC NET CTF 2023, which writeups do exist for.

The challenges are the following:

Name	Location	Bot knows this as
Polyglots	http://188.166.21.120:11000	http://polyglots.local
Css-injection	http://188.166.21.120:12000	http://css-injection.local
Cachepoison	http://188.166.21.120:13000	http://cachepoison.local
Hostheader	http://188.166.21.120:14000	*Not applicable*

Additionally there is a xss bot on <http://188.166.21.120:10000> that you can ask to visit links, please note the bot knows the websites as another hostname.

The challenges will reset every 10 minutes.

For each challenge, you must get the flag and document the steps you took to get it.

Tools that should help you edit web requests (you can pick 1):

Burpsuite

Postman

Caido

Tools for logging outbound http requests

<https://webhook.site>

digital ocean instance with `python3 -m http.server`