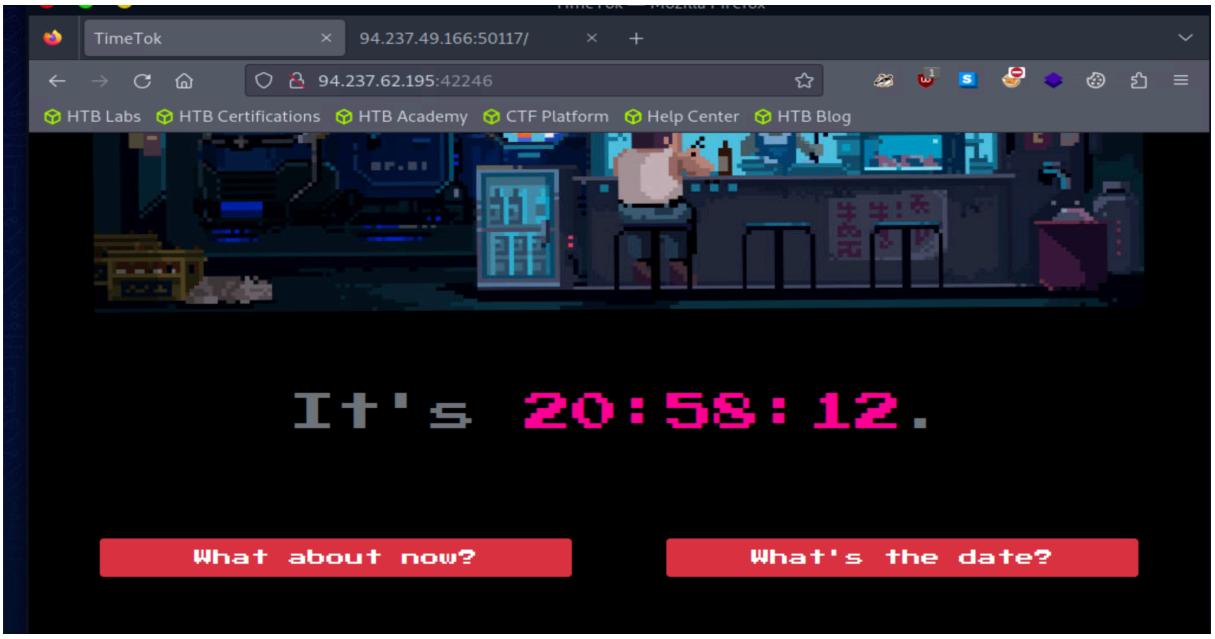
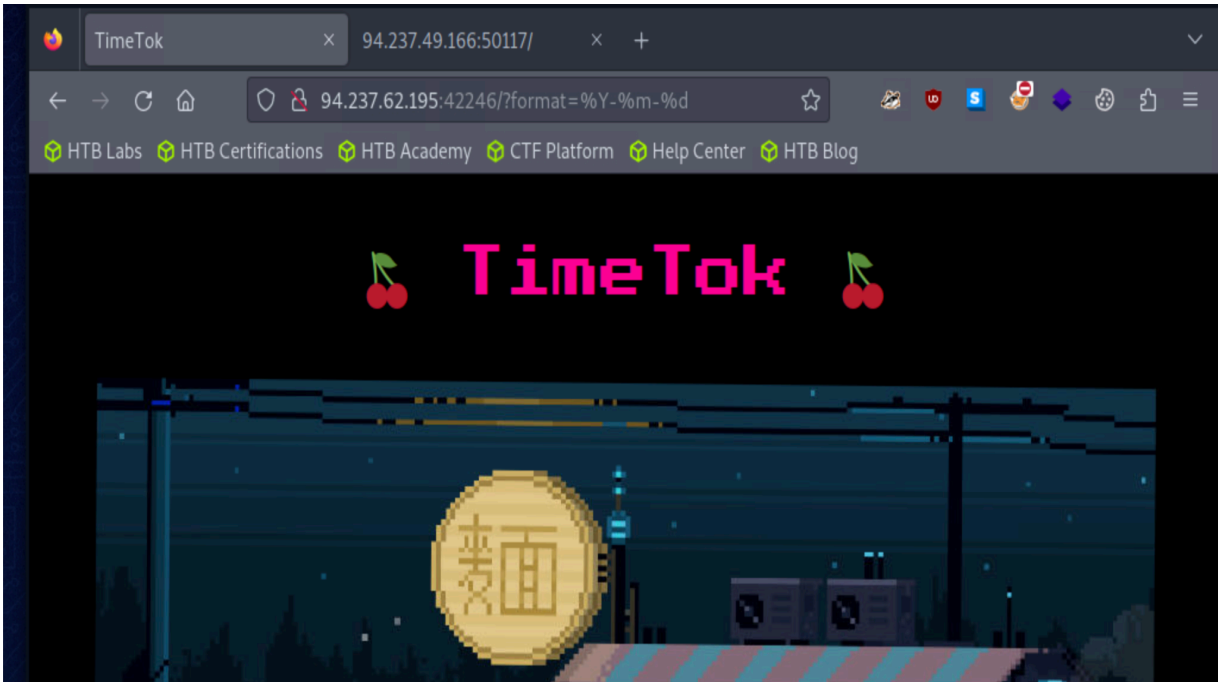
TimeTok Challenge

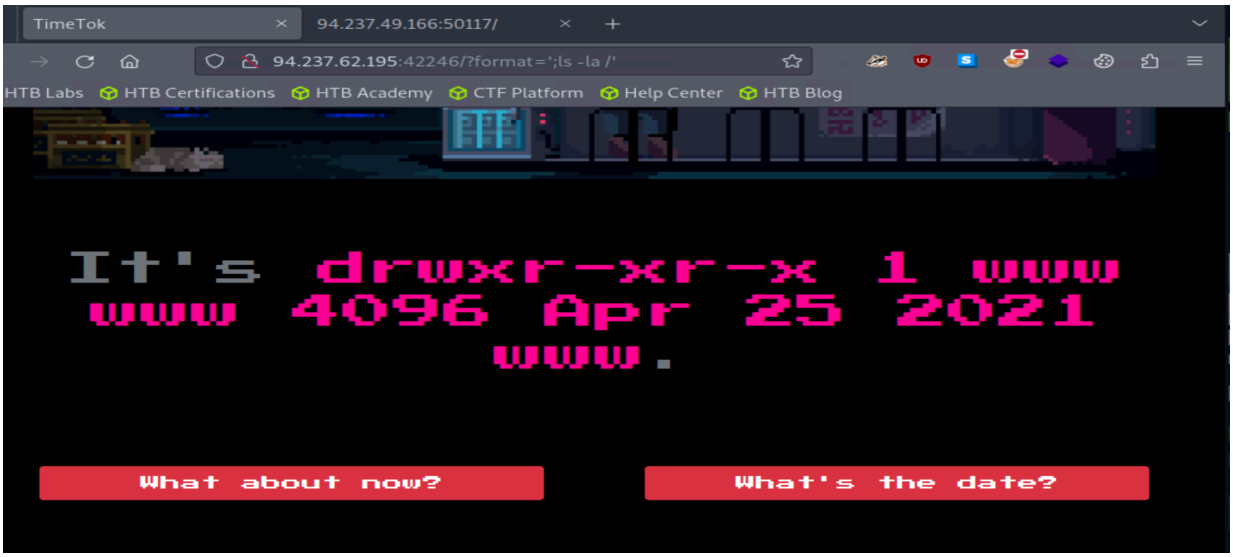
Step1: First visited http://94.237.62.195:42246/



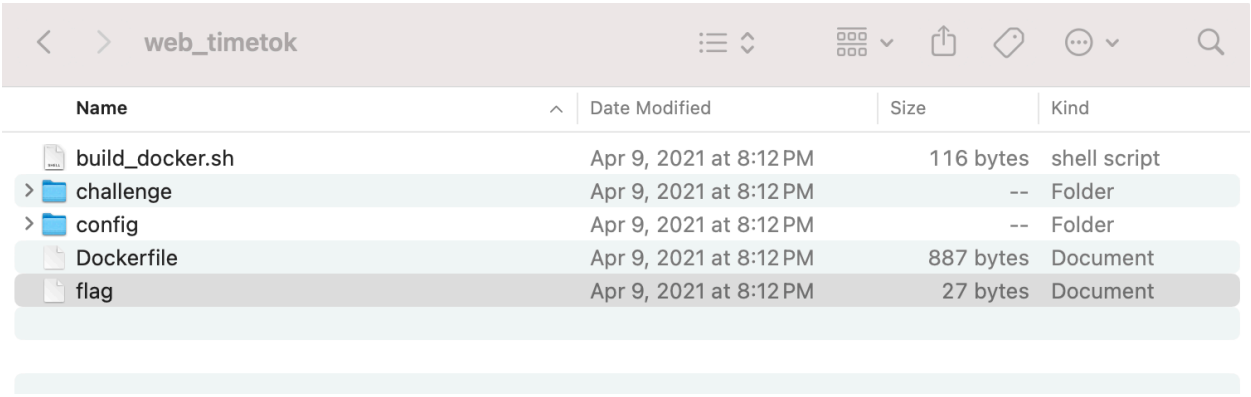
Step2: Then clicked on “What`s the date?” and found the ‘format’ parameter in the URL as shown in the below.



Step3: Then injected a command as the value of format parameter which disclosed the directories and files.



Step4: Then exploited and found the whole path and files (/www/views/index.php). But we didn't any flag in any directory. Then looked at the files which are provided to us to assist. That contained config file, so it might be the file of timetok web, where found "flag" file in root mentioned as test flag.



Step5: Hence, tried **cat /flag** which gave us the flag as shown in the below.

Risk mitigation strategy for command injection:

1. Input validation or sanitization
2. Using input whitelisting filter of allowed input specifications
3. Providing least privileges to files access
4. Parameterized commands
5. Avoiding shell or command execution by user-controlled input.
6. Code to control the content being displayed on the website as result to avoid disclosing irrelevant data.