Challenge: TimeKORP

Challenge Description :

Are you ready to unravel the mysteries and expose the truth hidden within Korp's digital domain? Join the challenge and prove your prowess in the world of cybersecurity. Remember, time is money, but in this case, the rewards may be far greater than you imagine.

Context :

- There is a Command injection Vulnerability in the web-application go and find it.

Notes :

- Tools:
    - BurpSuite - To intercept the http request and send forged ones.

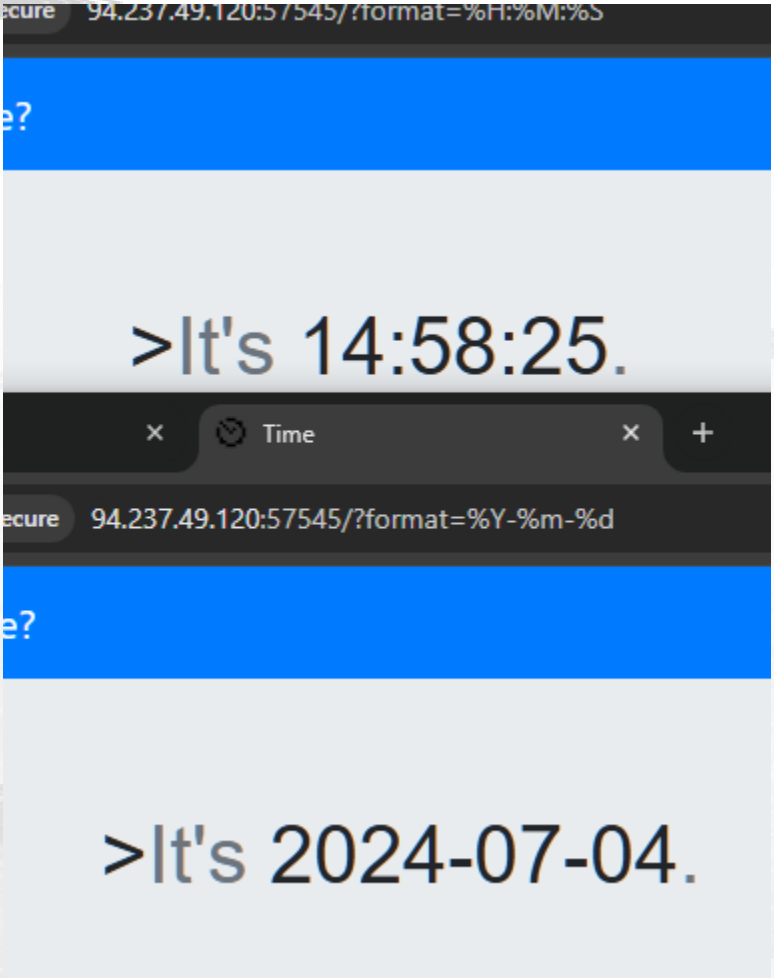
Flag :

- First Start the instance, go to the website and open the Inspect page, go to the elements tab and find what you can, as well as the elements page go to the network tab as well, you could find better results there.
- Looking at the source code we see that there is a url query that goes to " http://IP:PORT/?format=%H:%M:%S "

  There seems to be no input sanitation on the client-side, also as we don't get the source code for this one there might be input sanitation on the backend.

```
<body>
  <nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">
    <a class="navbar-brand mb-0" href="?format=%H:%M:%S">🕒 What's the time?</a>
    <div class="collapse navbar-collapse" id="navbarSupportedContent">
      <ul class="navbar-nav">
        <li class="nav-item">
          <a class="nav-link" href="?format=%Y-%m-%d">📅 What's the date? <span class="sr-only">(current)</span></a>
        </li>
      </ul>
    </div>
  </nav>
```

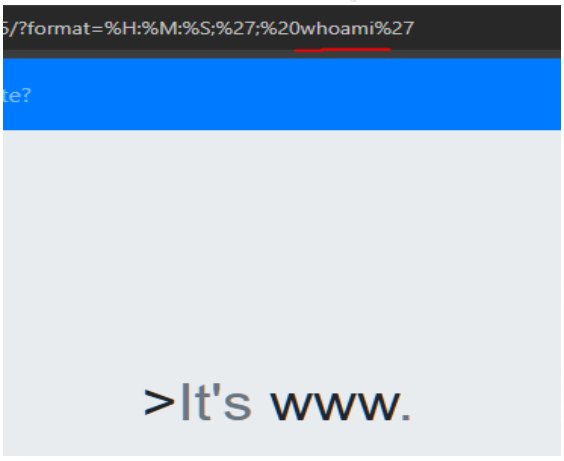
- Each Url query has a different format, one showing the time and one showing the data.



- To get shell / RCE on this we will try and run a command injection

  Example : '; id ' Or '; whoami '.

  We use single quotes to close the original string and start a new one, the semicolon to separate the command from the format, and then the Command to run.
- Running one of the Example command injections works but shows there isn't a proper user active.



- We can get the flag by just running : '; cat /flag '
- The flag is then obtained: HTB{1t_i5_t1m3_f0r_ult1m4t3_pwn4g3!}