WeParser Web CTF Writeup

Recon and Initial Steps

- Register a user account on the WeParser website and log in.
- After logging in, you will be redirected to a dashboard page, e.g., http://127.0.0.1:5000/dashboard?user_id=125.
- The dashboard contains chat messages hinting that the **super user/admin** has user_id=0.

IDOR for Privilege Escalation

- Perform an **Insecure Direct Object Reference (IDOR)** attack by changing the URL parameter:

text

http://127.0.0.1:5000/dashboard?user_id=0

- Visiting this page reveals a **beta access token** for the XML parser feature.

Using the Beta Access Token

- Use the obtained beta access token to activate Beta Features.
- Access the "Checkout New Feature" button on the dashboard; this brings up an XML parser interface.

XXE Attack for Flag Retrieval

- The XML parser includes a clear hint that you should try an **XXE (XML External Entity) attack**.
- On the "Input XML" area, use the following payload to read the flag.txt file:

xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///flag.txt" >]>
<foo>&xxe;</foo>
```

Outcome

- Submitting this payload causes the server to parse the XML, read from flag.txt, and display the file contents (the flag) in the output box.
- DJSISACA{XX3_A$D_1D0r_f4r_th3_w1n_33inwueb}