Graphical user interface, text, application

Description automatically generated

Lâu lắm rồi mk mới quay trở lại và bài hn mk chọn là 1 bài vừa mới đc ra mắt là “Cyber Heroes”. Bắt đầu thôi

1. Dò quét

rustscan -b 500 -a 10.10.232.174

A screenshot of a computer

Description automatically generated with low confidence

nmap -sC -sV -v -p 22,80 10.10.232.174 -Pn

Text

Description automatically generated

Vẫn là 2 cổng quen thuộc là 80 và 22

1. Enum

Graphical user interface, text, application

Description automatically generated

Và đây là login page:

A screenshot of a computer

Description automatically generated

Nhìn giao diện ntn, mới đầu mk đoán khả năng là người ta dùng CMS nhưng sau 1 hồi xem xét thì ko phải, chỉ là giao diện đẹp thui :))). Test qua 1 vài default credentials (admin:admin, admin:password,…) cho lỗi như sau:

Graphical user interface, application

Description automatically generated

Nhìn như thế này (Theo suy đoán khả năng website là dùng javascript-ajax để check login) nên mk kiểm tra luôn source code thì ôi thôi, thật bất ngờ

Text, letter

Description automatically generated

Đến đây chúng ta có được username và password. Username là "h3ck3rBoi" và password là

A screenshot of a computer

Description automatically generated with low confidence

Sau đó thì login vào và lấy flag thôi.