Trên trình duyệt chỉ cho upload các file jpg , jpeg ,png

A screenshot of a computer

Description automatically generated

Ta thử upload 1 ảnh png tìm ra nơi chứa file ảnh là /profile\_images/

A computer screen shot of a computer

Description automatically generated

Và ta thấy giá trị accept đang không có giá trị .php nên ta không được phép chọn file php trên trình duyệt .

->Bypass bằng cách thêm giá trị .php vào giá trị của biến accept

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ta upload file WebShell.php lên và vào đường dẫn chứa file WebShell.php thực thi lệnh nhưng vẫn bị chặn bởi id=”error\_message”

A screen shot of a computer

Description automatically generated

Vượt qua bằng burpsuite

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

P/s: HTB{cl13n7\_51d3\_v4l1d4710n\_w0n7\_570p\_m3}

A screenshot of a computer screen

AI-generated content may be incorrect.

A computer screen with text on it

AI-generated content may be incorrect.

A computer screen shot of text

AI-generated content may be incorrect.

A blue line on a black background

AI-generated content may be incorrect.