Proxy Logon

Tool sử dụng:

+ dnSpy

+ Visual Studio 2022

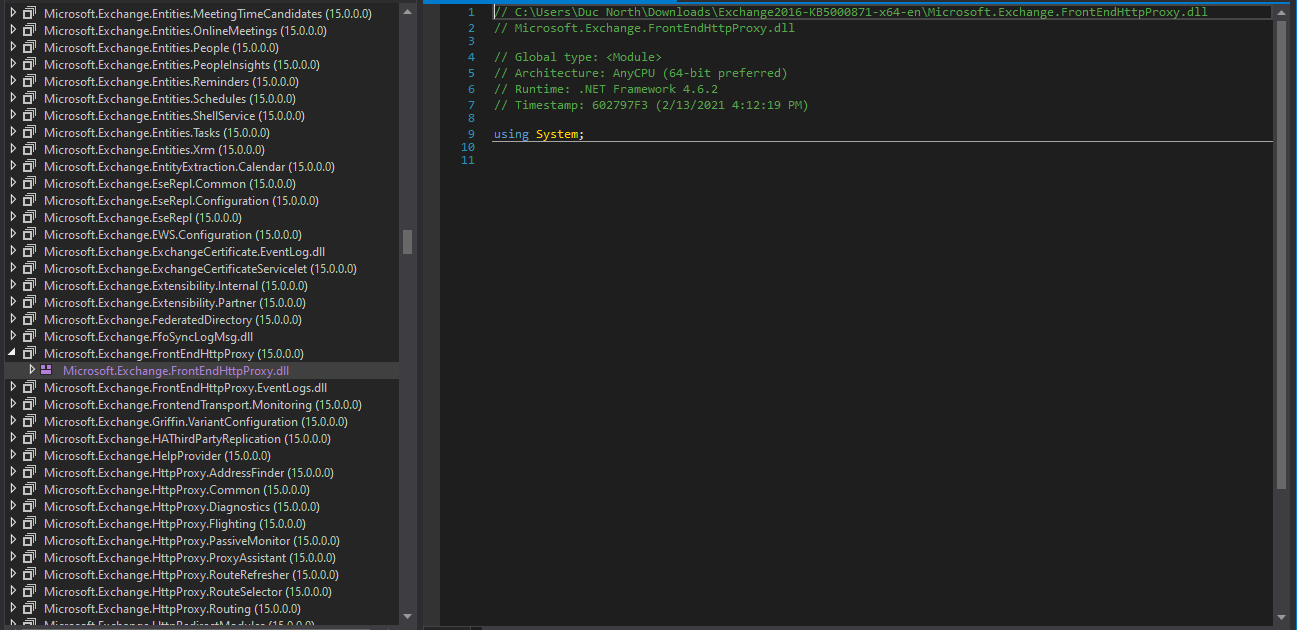
Giới Thiệu:

Proxy Logon là lỗ hổng xuất hiện trên Mircrosoft MailExchange cho phép kẻ tấn công có thể sử dụng để SSRF. Phiên bản được sủ dụng là Mcrosoft Exchange Server 2016 CU 18

Tổng quan

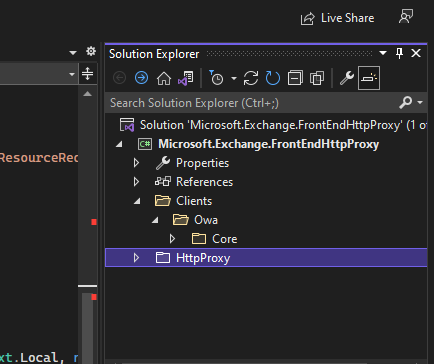
Lỗ hổng Proxy Logon được xác định là ở phần HttpProxy của hệ thống, do đó chúng ta sẽ đi vào phần FrontEndHttpProxy của hệ thống

Sau khi extract dữ liệu được lấy từ file smp của bản vá, chúng ta sử dụng dnSpy để xem dữ liệu trong đó. Vì đều được viết trên dotnet nên chúng ta cần sự hộ trợ từ Visual Studio để có thể complie ra file cs khiến cho việc tìm hiểu code trở nên dễ dàng (code sau khi được extract đều ở dạng assembly).

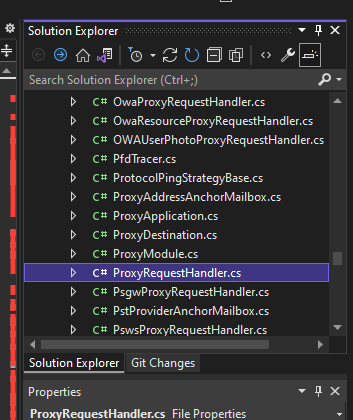


Sau khi extract chúng ta sẽ tìm đến thư mục Microsoft.Exchange.FrontEndHttpProxy.dll để tiến hành compile code.

Tiếp đó sử dụng Visual Studio để đọc code



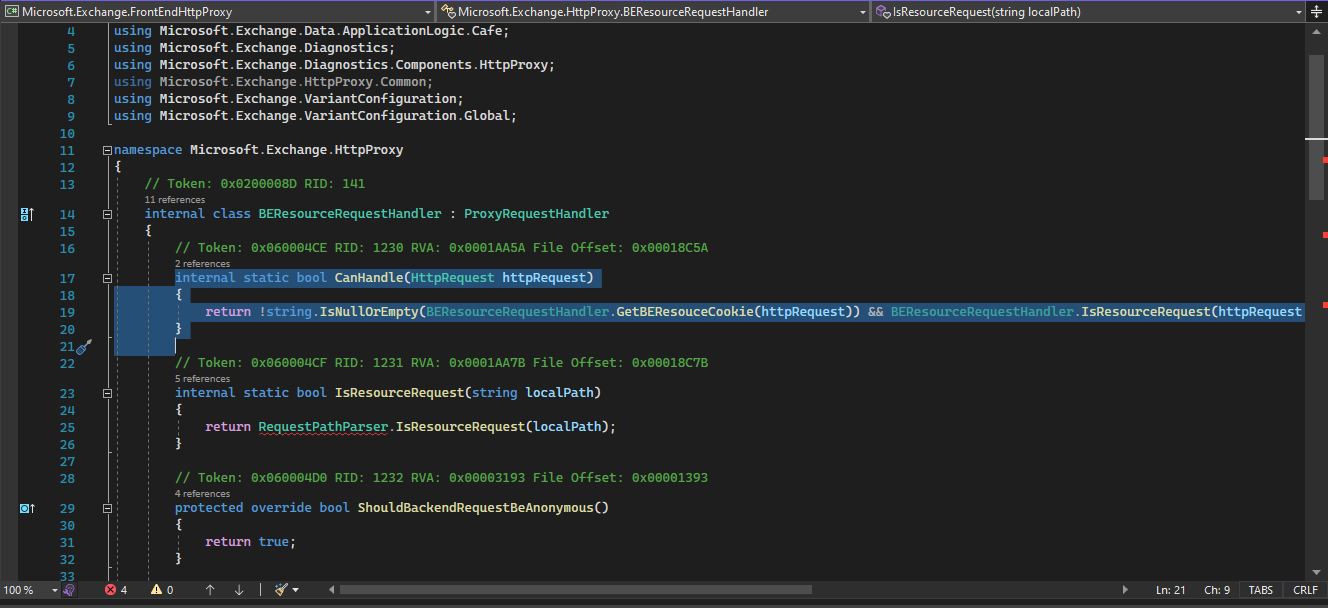
File code quan trọng cần tìm hiểu sẽ được nằm ở folder HttpProxy sau khi complie



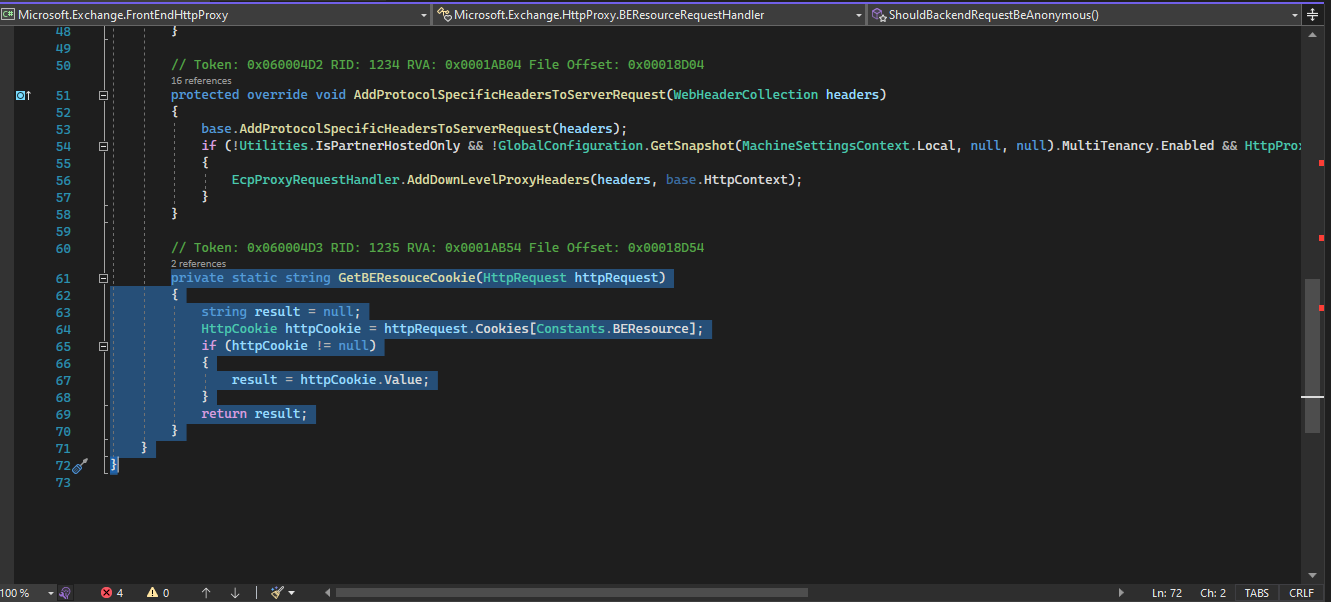
Truy cập folder HttpProxy vào tìm đến file .cs với tên ProxyRequestHandler

BEResourceRequestHandler là class sẽ được dùng vào việc handle các request có dạng resource (các file có đuôi .js, .css, …)

Việc xác định class này có thể handler request được hay không dựa vào method BEResourceRequestHandler.CanHandle()

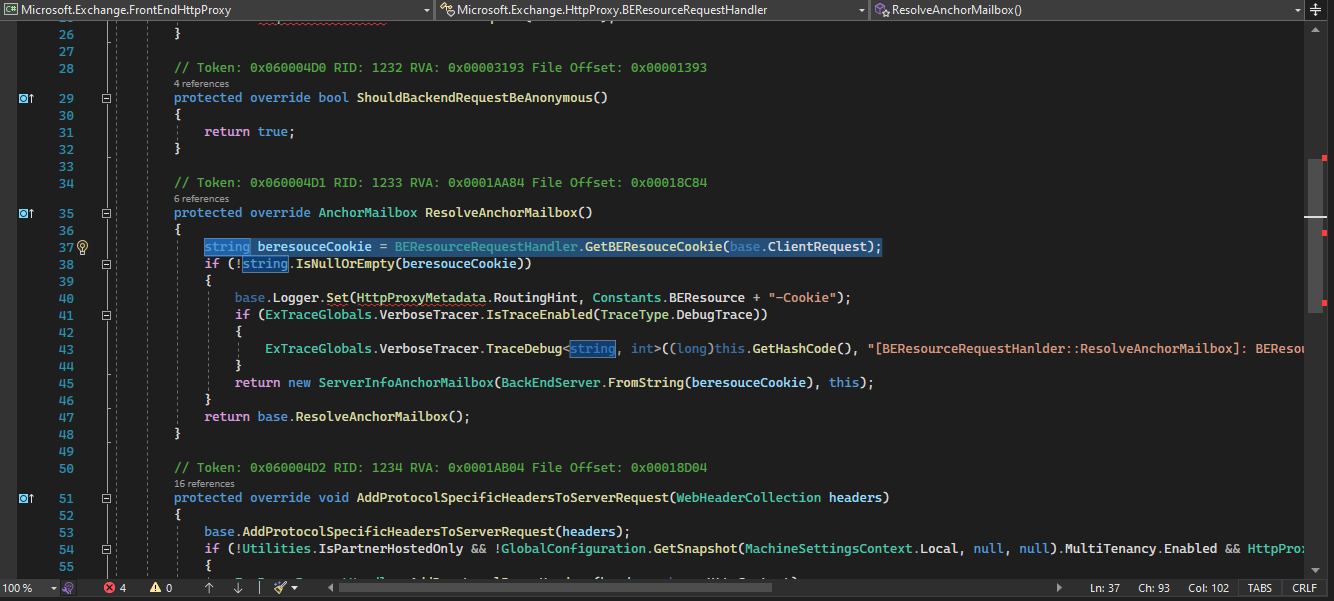


Đầu tiên là sẽ kiểm tra sự tồn tại của một cookie đặc biệt với method GetBEResouceCookie(). Method này sẽ lấy và trả về giá trị cookie “X-BEResource”

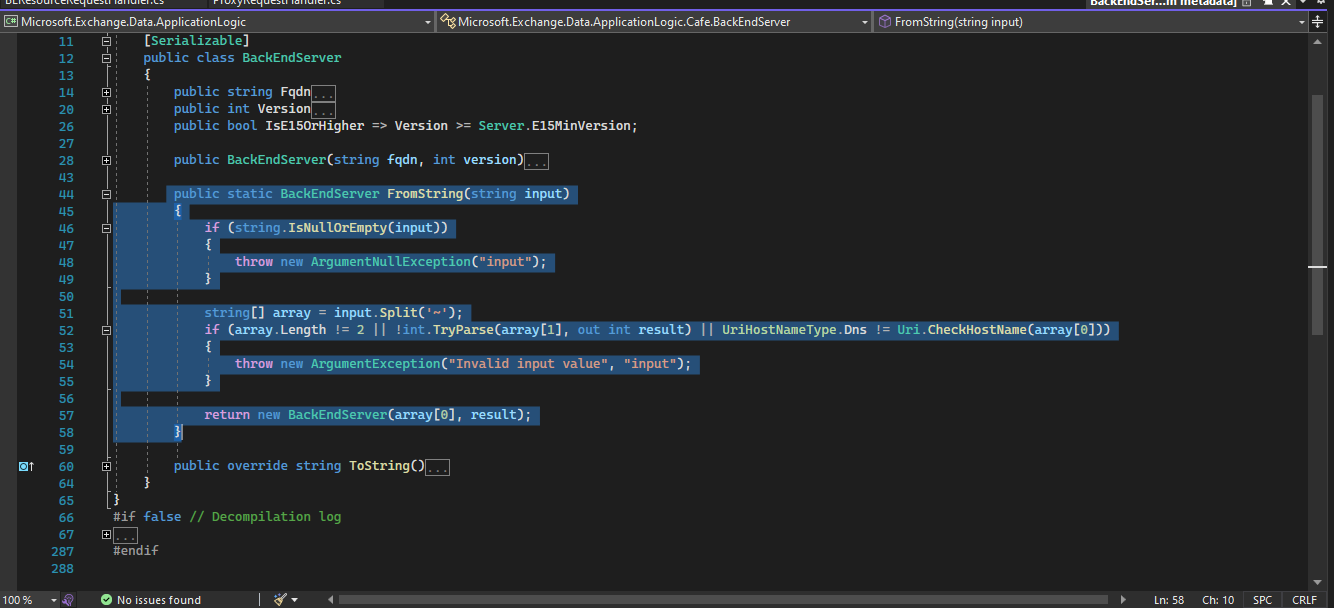


Tiếp sau đó, BEResourceRequestHandler.IsResourceRequest() sẽ kiểm tra xem URL request có đuôi dạng các file resource hay không.

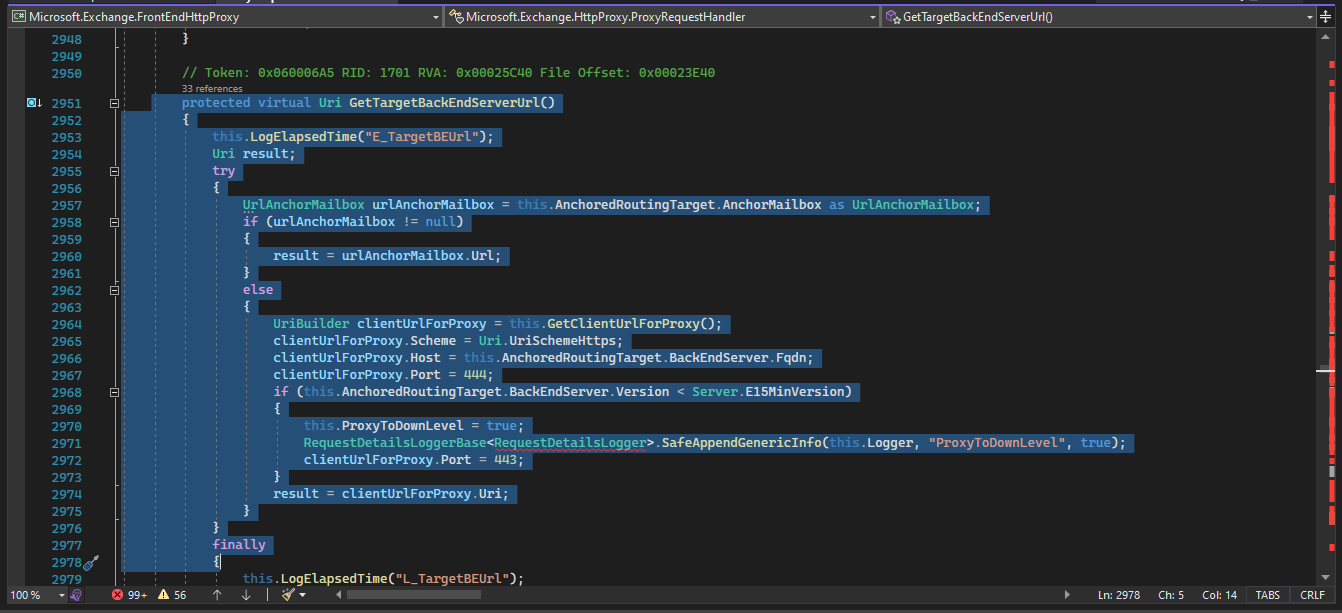
Giá trị “X-BEResource” sau đó tiếp tục được truyền vào BackEndServer.FromString() để xác định BackEnd Server cho request này.



Phía backend sẽ xử lý code như sau



Tại ProxyRequestHandler.BeginProxyRequest() sẽ gọi tới GetTargetBackEndServerUrl() để xác định uri sắp được forward tới (chức năng đúng như tên của Class luôn). Method GetTargetBackEndServerUrl() có nội dung như sau:



Chức năng này sẽ xây dựng lại url và được forward lại vào phía backend.