**Lỗ hổng ProxyLogon**

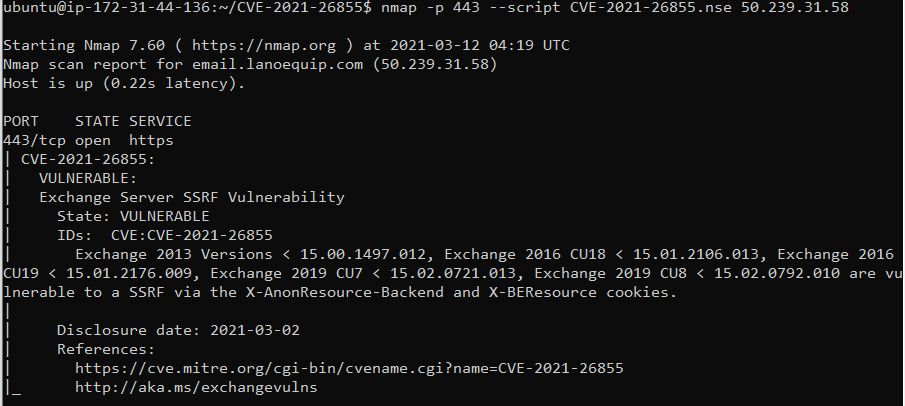
**Mô tả**

Lỗ hổng ProxyLogon có thể dẫn đến unauthen RCE trên hệ thống mail exchange. Đây lỗ hổng nghiêm trọng gây ảnh hưởng lớn đến một số lượng lớn các doanh nghiệp, tổ chức tại Việt Nam và toàn thế giới. Lỗ hổng này là 1 chain kết hợp của các lỗ hổng CVE-2021–26855: Mail Exchange Pre-Auth SSRF và CVE-2021–27065: Post-Auth arbitrary file write.

**Cách khai thác**

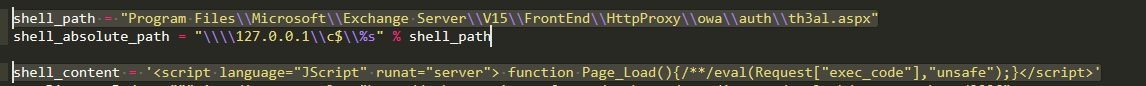
* Scan kiểm tra lỗ hổng, sử dụng script của Microsoft:

*https://github.com/microsoft/CSS-Exchange/blob/main/Security/src/http-vuln-cve2021-26855.nse*

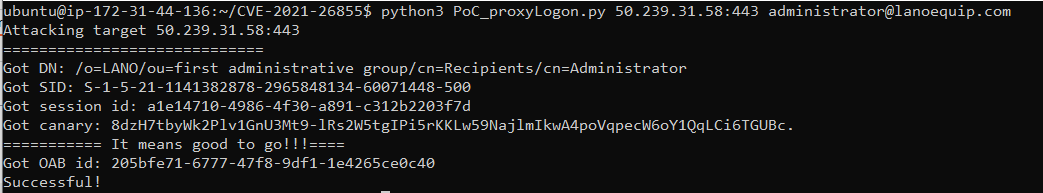


*Sử dụng nmap để kiểm tra khả năng dính lỗ hổng CVE-2021–26855 của target*

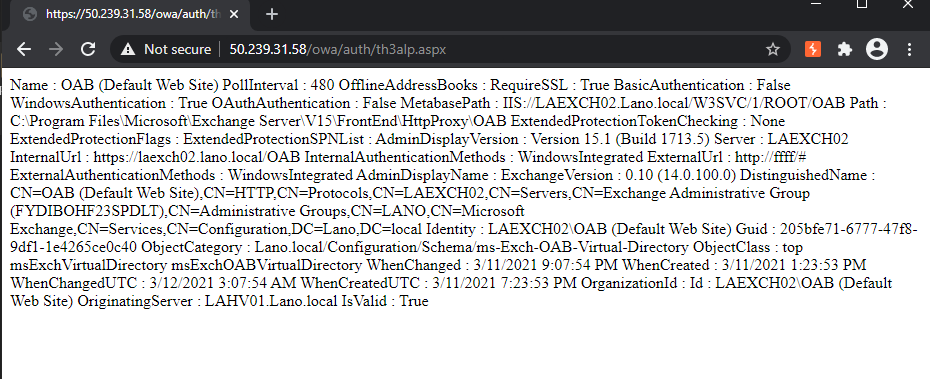
* Code shell sẽ được upload lên server

****

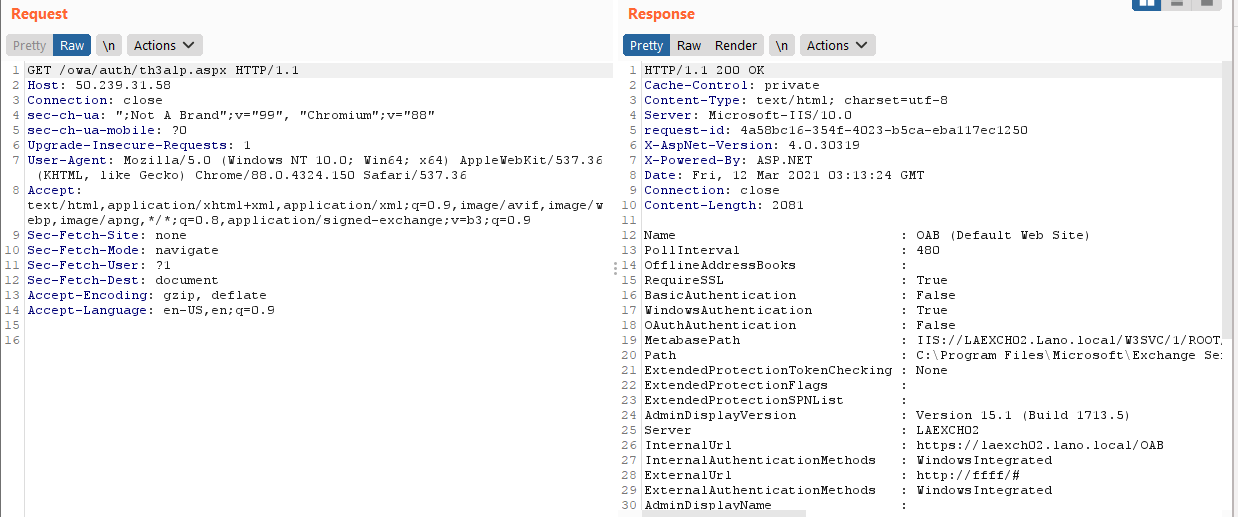
*Nơi chứa file shell (shell\_path) và code file shell (shell\_content) và sẽ upload lên server*



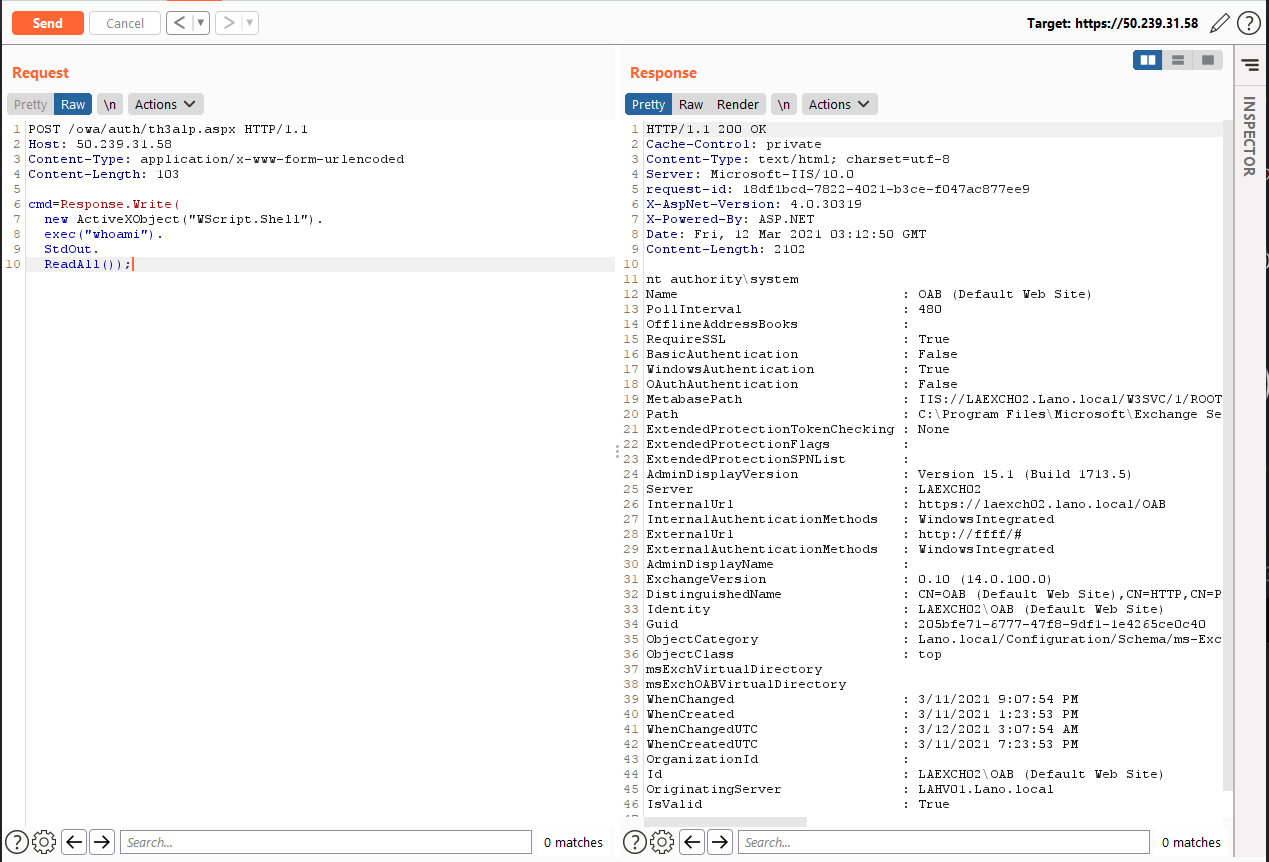
*Chạy file PoC và upload shell thành công*



*Kiểm tra file shell (th3alp.aspx) đã upload lên server*

**

*Dùng Burpsuite bắt request chứa file shell (th3alp.apsx) đã được upload*



*Repeater đổi method GET sang POST và chỉnh sửa phần body để execute command*