

Lâu lắm rồi chưa viết bài, hn mk trở lại với 1 bài trên HTB có tên là “Busqueda”. Bắt đầu thôi

1. **Dò quét**

*rustscan -b 500 -a 10.10.11.208*

Text

Description automatically generated

Vẫn 2 là port quen thuộc là 22 và 80. Chi tiết hơn xem nó ntn

*nmap -p 22,80 -sC -sV -v -T4 10.10.11.208 -Pn*

Text

Description automatically generated

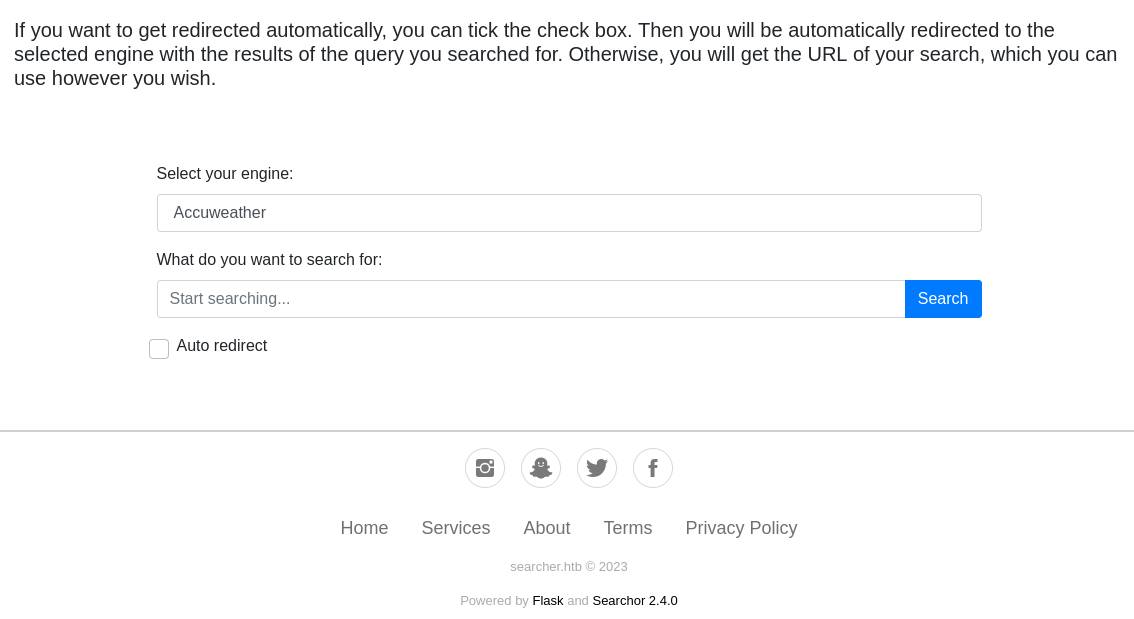
Với kết quả này thì biết được là backend đang dùng ngôn ngữ Python

1. **Enum**

Một số câu hỏi cần trả lời mk thường đặt ra: Tech mà target sử dụng? OS, Web server, CMS/Framework sử dụng – ngôn ngữ lập trình – sử dụng lib/dependency/package nào? Phiên bản của nó là bao nhiêu? Website có những chức năng gì? Chúng ta có thể inject vào đâu (URL/Form Input, cookie,…) ? Target có để lộ thông tin gì không (creds, source code, hidden file/folder/ parameter/domain,…) ?…..Càng nhiều câu hỏi đặt ra thì khi trả lời được => giúp chúng ta có thể xác định chính xác lỗi.

Graphical user interface, text, application, email

Description automatically generated



Chú ý đến dòng “Powered by Flask and Searchor 2.4.0” => phải tra cứu ngay về Flask và Searchor 2.4.0

Graphical user interface, text, application

Description automatically generated

Trên phiên bản 2.4.0, dev họ dùng 1 hàm rất nguy hiểm là eval(), cho phép attacker có thể RCE. Từ bản 2.4.2 thì lỗi này được fix.

Graphical user interface, text, application, email

Description automatically generated

Vất vả lắm mk mới tìm được PoC để khai thác (ngồi search trên Google mãi ko ra, mk chuyển qua Search Engine khác là Bing mới tìm ra được)

Graphical user interface, text, application, email

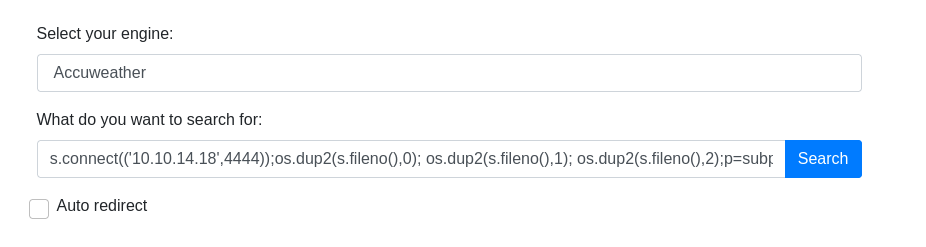
Description automatically generated

1. **Exploitation**

Tiến hành lắng nghe kết nối đến:

Text

Description automatically generated

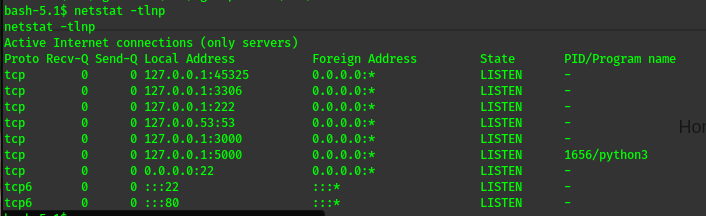


Và đây là kết quả. Chúng ta có được shell của user ”svc”

Text

Description automatically generated

1. **Leo thang**



Graphical user interface, application

Description automatically generated

Tại port 3000 đang chạy Gitea Version: 1.18.0+rc1. Bản này khá mới nên ko có lỗi. Mk có chuyển qua brute force tìm password (với username là “cody” và “administrator”) nhưng ko thành công. Tìm Repo thì cũng ko có cái Repo nào để tận dụng.

Chuyển qua port 3306 cũng chẳng khá khẩm hơn.

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

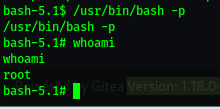
Với loạt lệnh là kết quả trả về, mk nghĩ tới hướng liên quan đến docker và git. Có điều là khi chạy docker thì dính permission còn hướng git thì ko có thông tin gì có thể tận dụng được. Đến đây hơi bí nên ra ngoài làm cốc nước cho thoải mái đầu óc.

Đến đây thì mk trở lại với những hướng cơ bản: sudo permission, SUID, cron, kernel,.….Và kết quả thật bất ngờ.

Text

Description automatically generated

“/usr/bin/bash” => ko ngờ lại đơn giản đến thế mà mk lại suy nghĩ cực kỳ phức tạp



Đến đây là thành công rồi. Tạm biệt !!!