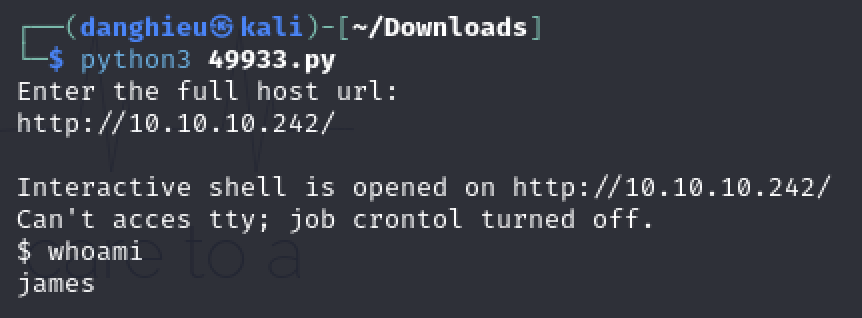
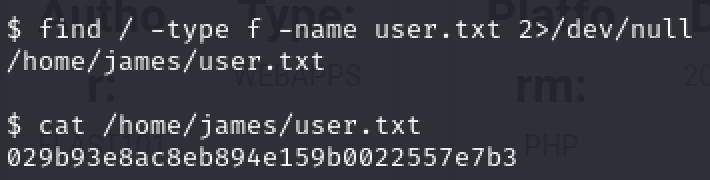


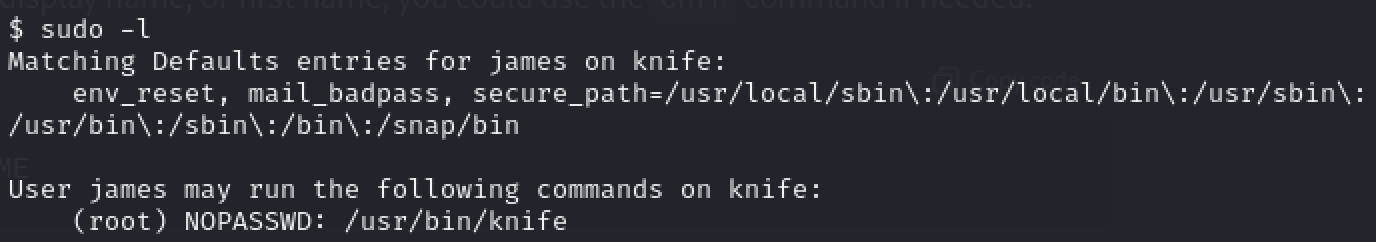
Ứng dụng web dùng PHP/8.1.0-dev

Chúng ta tìm được CVE có thể RCE bằng User-Agent





Cho phép ta chạy tệp nhị phân knife dưới quyền root



Chef Client là 1 công cụ chạy các Chef recipes trên 1 node. Nó lấy tệp cấu hình từ Chef Server (hoặc chạy trên local nếu Chef Zero được sử dụng)

Knife là 1 công cụ dòng lệnh tương tác với Chef Server. Knife quản lý cơ sở hạ tầng của Chef bao gồm cookbooks, nodes, environments và data bags.

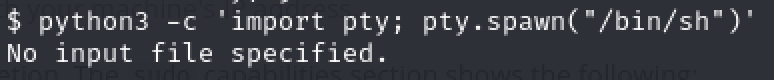
Người dùng james có trách nhiệm quản lý Chef Server

Nếu hacker chiếm quyền điều khiển Knife, hậu quả có thể rất nghiêm trọng vì Knife tương tác trực tiếp với Chef Server.

* Tải lên các cookbooks độc hại
* Điều chỉnh cấu hình Node
* Truy cập dữ liệu nhạy cảm
* Leo thang đặc quyền

Shell bạn lấy đc không có linh hoạt, không dùng được nhiều tính năng như di chuyển thư mục

Mình muốn bật interactive shell cũng không được



Thử reverse shell:

