BÁO CÁO LAB 3

Môn: An toàn mạng máy tính nâng cao

GVTH: Đỗ Thị Phương Uyên

Sinh viên thực hiện	**Sinh viên 1** MSSV: 21521182 Họ tên: Nguyễn Đại Nghĩa **Sinh viên 2** MSSV: 21521295 Họ tên: Phạm Hoàng Phúc **Sinh viên 3** MSSV: 21521848 Họ tên: Hoàng Gia Bảo **Sinh viên 4** MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	**NT534.O21.ATCL.1**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: Lab 1, Lab 2, Task 1 Lab 3 **[Sinh viên 2]**: Task 4, 5 Lab 3 **[Sinh viên 3]:** Task 6, 7 Lab 3 **[Sinh viên 4]:** Task 2, 3 Lab 3
Link Video thực hiện *(nếu có yêu cầu)*	

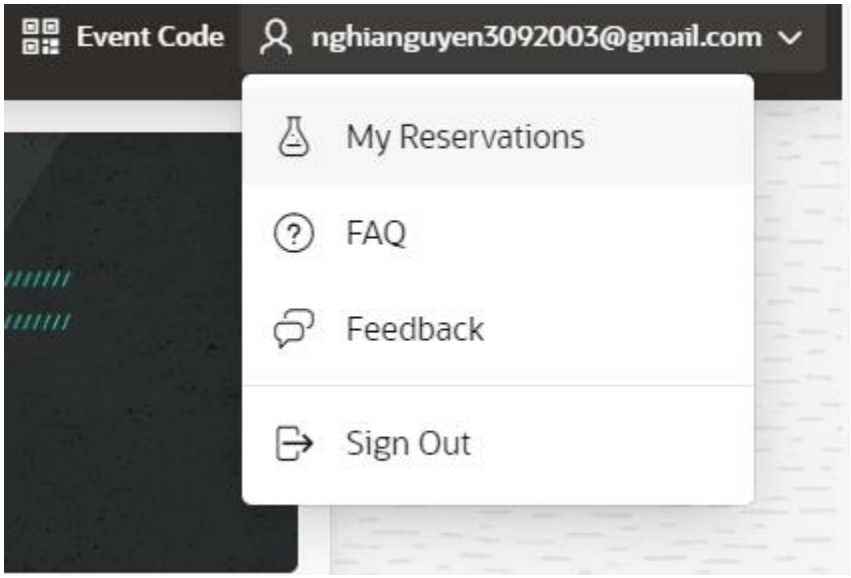
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	
Điểm tự đánh giá *(bắt buộc)*	9.5 /**10**

Lab 1: Environment Setup

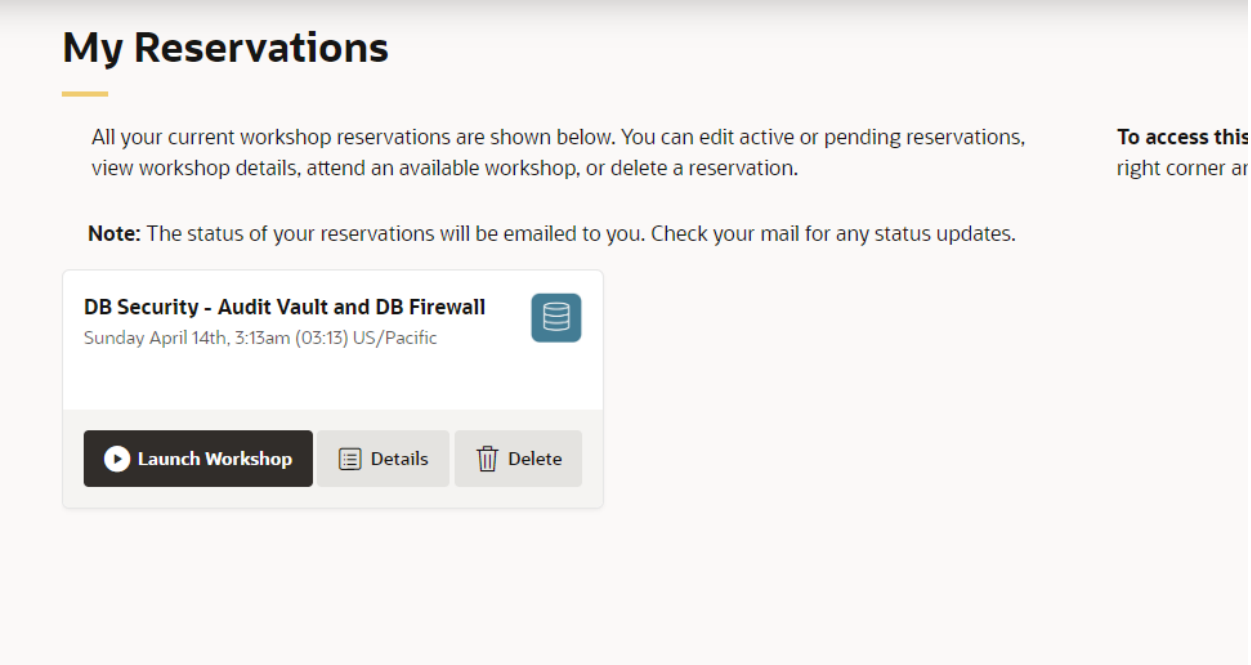
Task 1: Access the Graphical Remote Desktop:

Để hoàn thành lab 1 này, em sẽ thực hiện theo hướng dẫn với các bước như sau:

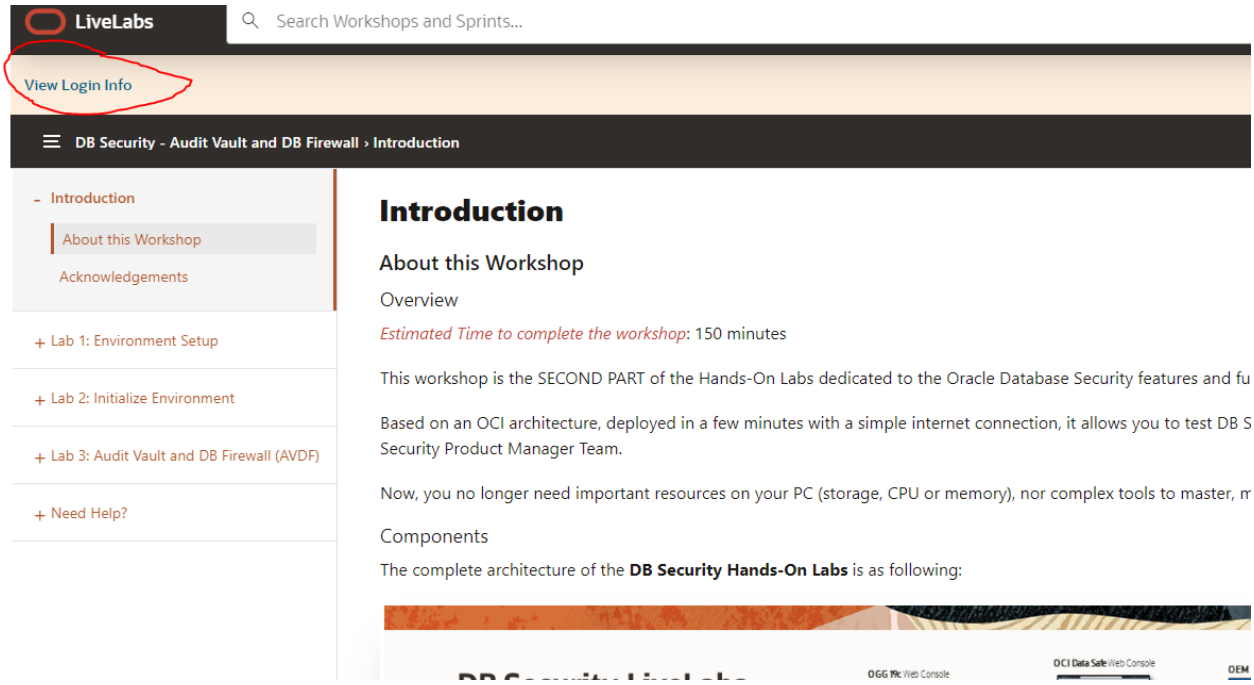
Truy cập vào mục "My Reservations":



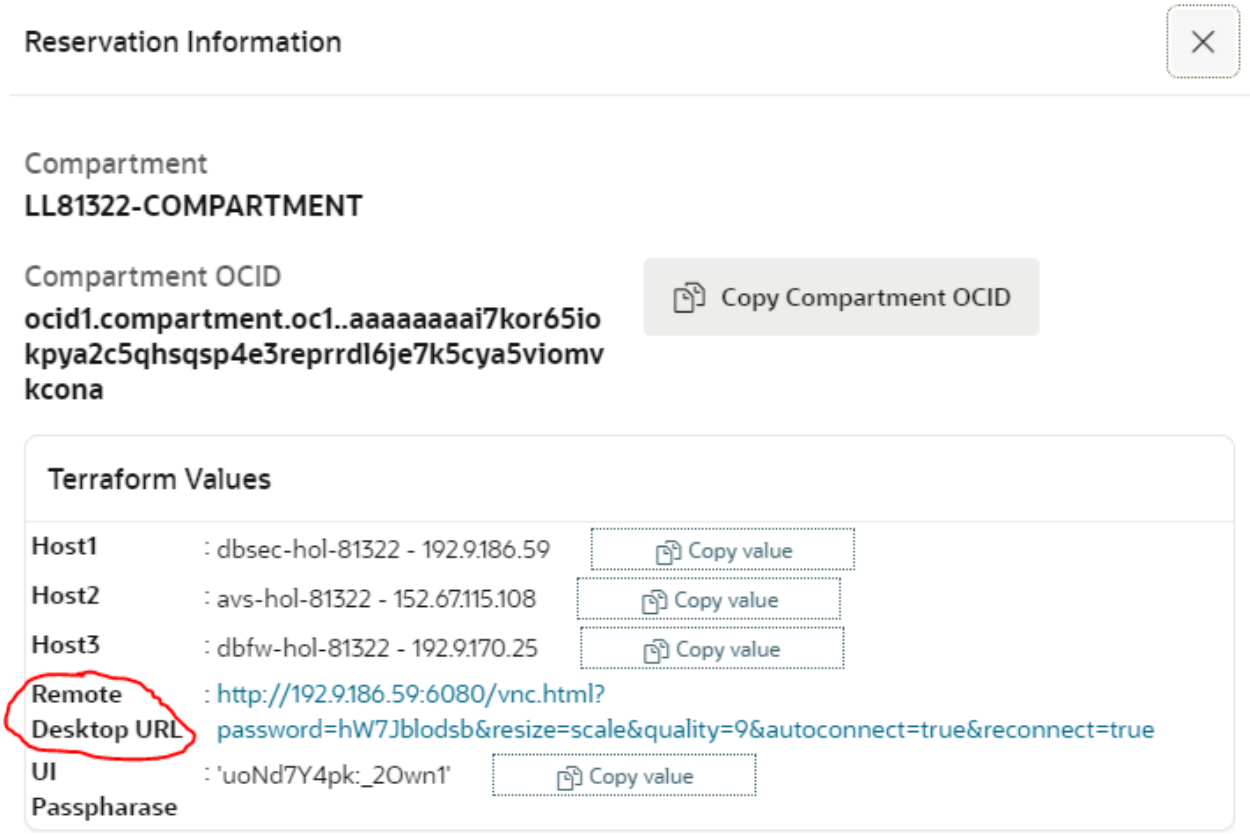
Màn hình như sau xuất hiện:



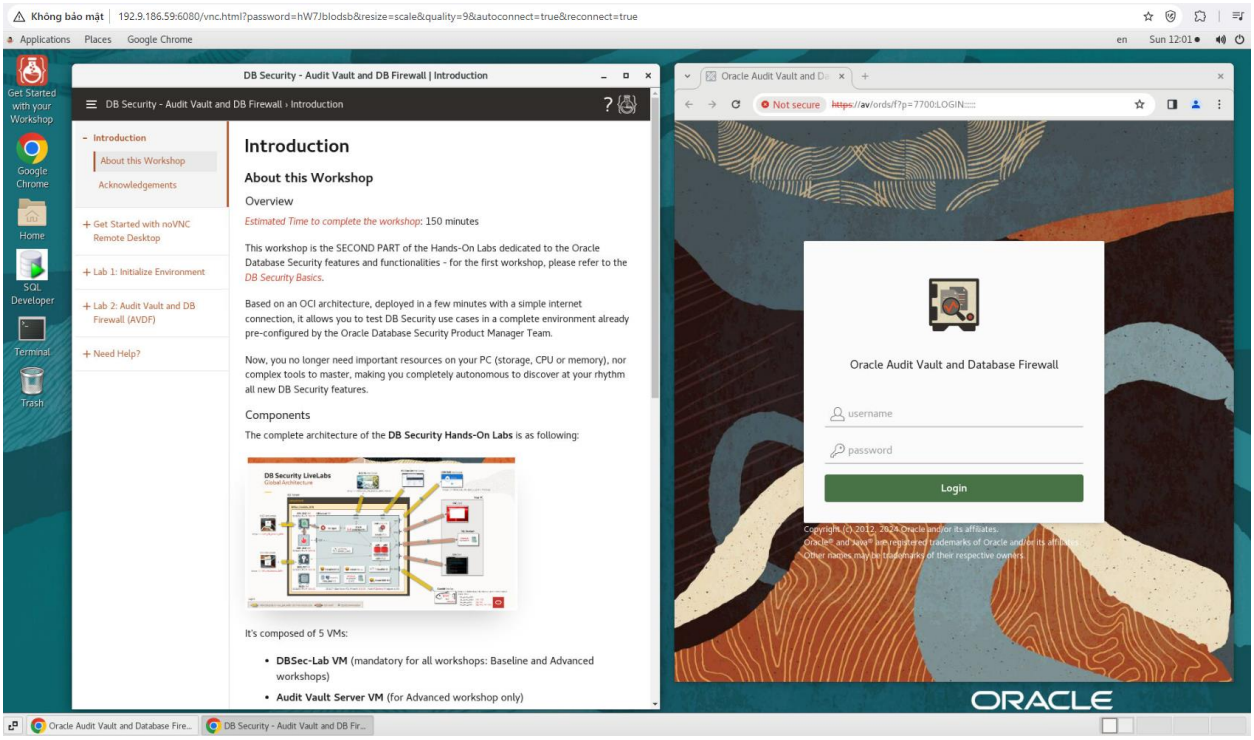
Kế đến là ấn vào nút "Launch Workshop" và chọn vào "View Login Info":



Rồi chọn vào "Remote Desktop URL":



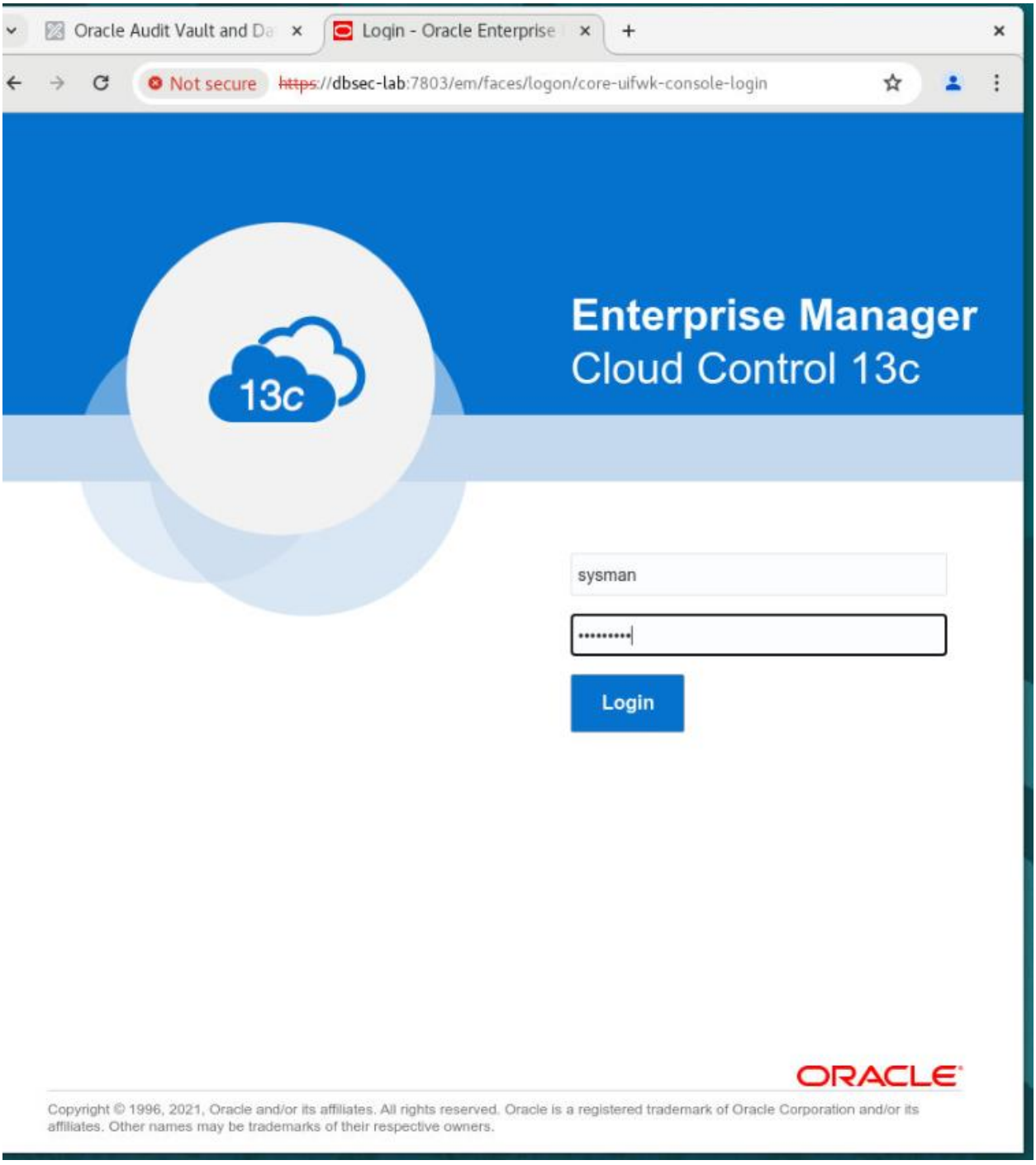
Kết quả nhận được:



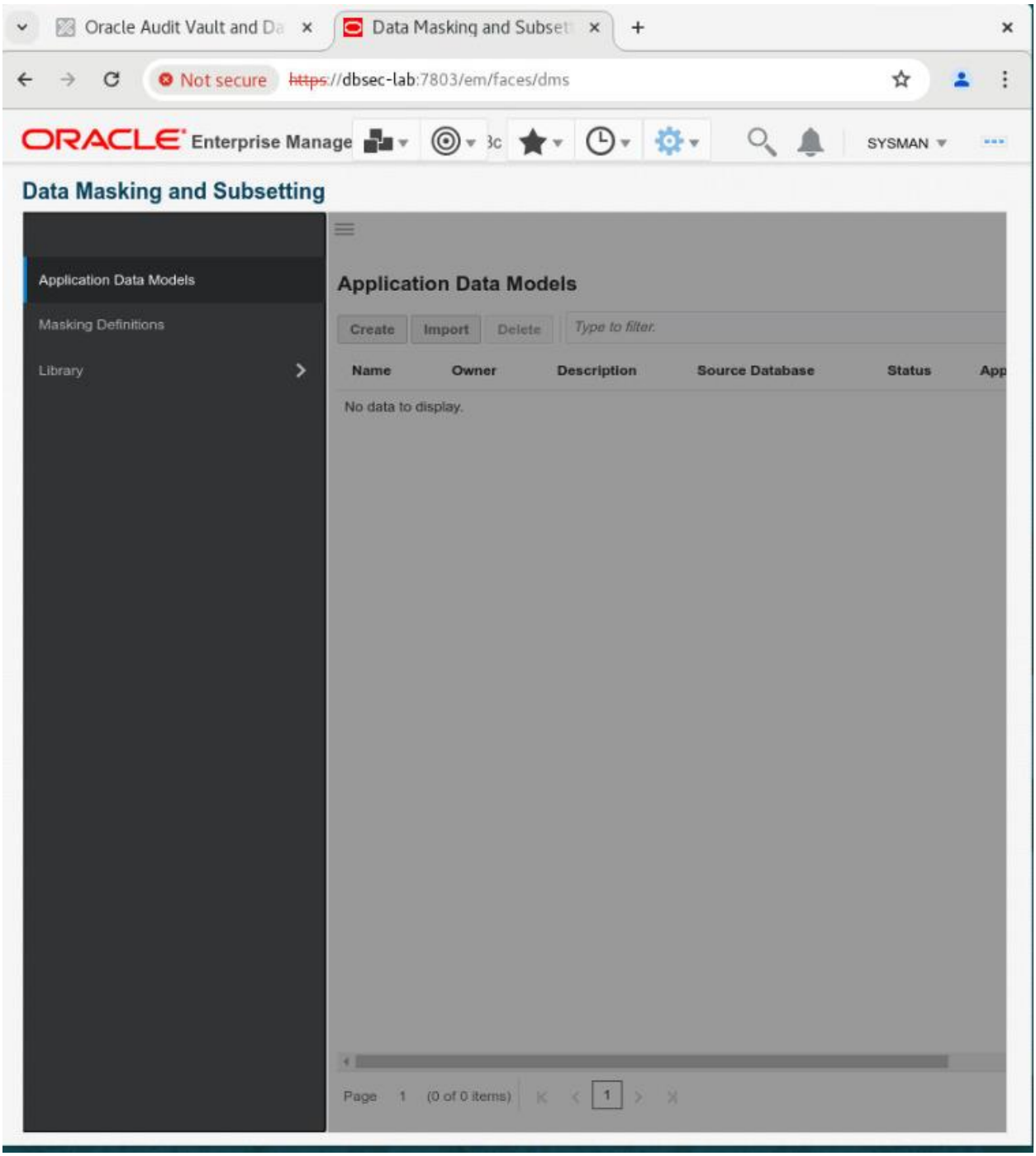
Lab 2: Initialize Environment

Task 1: Validate That Required Processes are Up and Running:

Em sẽ thực hiện đăng nhập vào Enterprise Manager với Username là sysman và Password là Oracle123:



Sau khi đăng nhập thành công, màn hình sau hiển thị:



Kế đến em thực hiện mở tab mới và chạy các đường dẫn sau để kiểm tra xem môi trường đã sẵn sàng chưa:

- PDB1

```
Prod: http://dbsec-lab:8080/hr_prod_pdb1
```
Copy

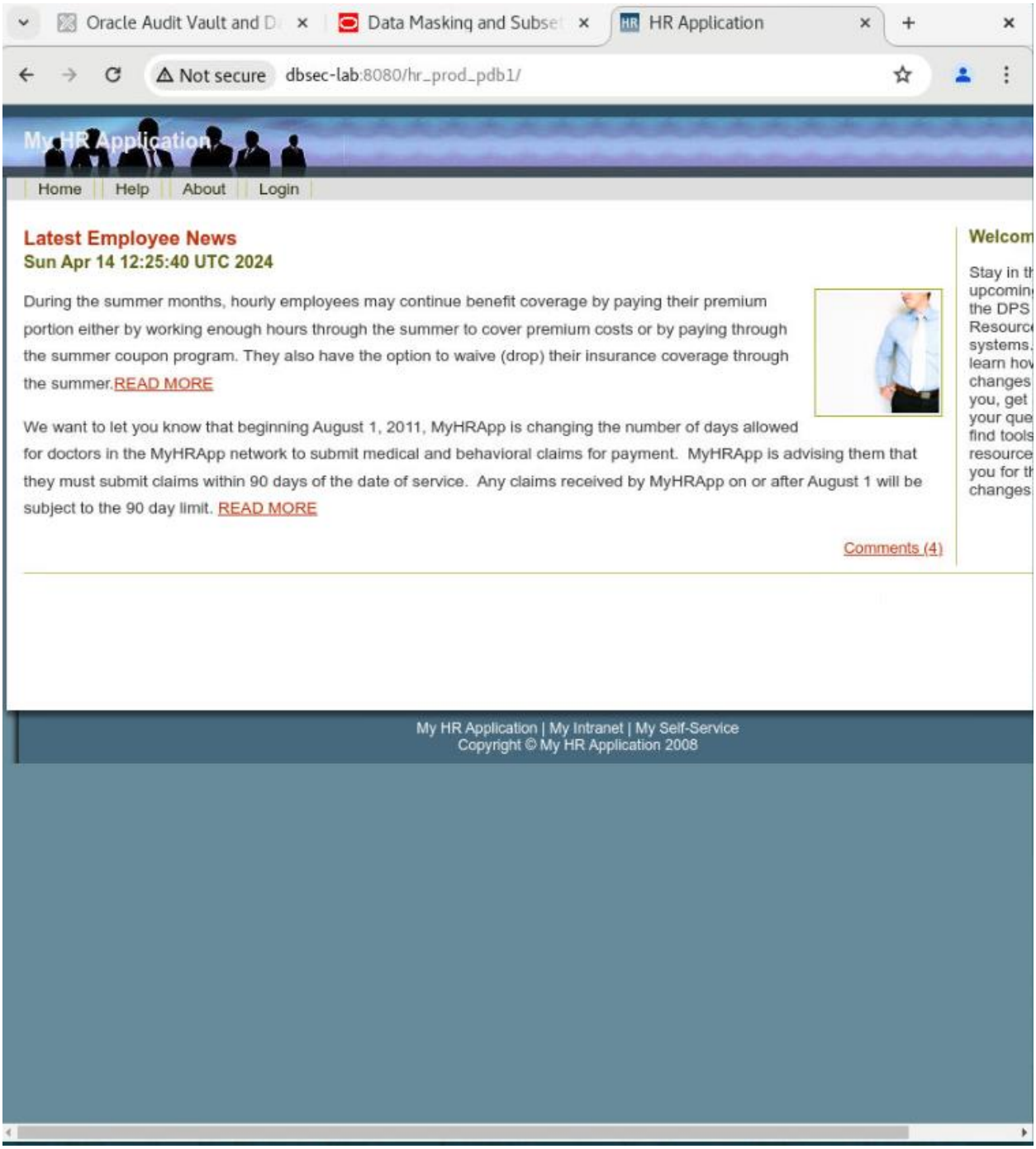
```
Dev: http://dbsec-lab:8080/hr_dev_pdb1
```
Copy

- PDB2

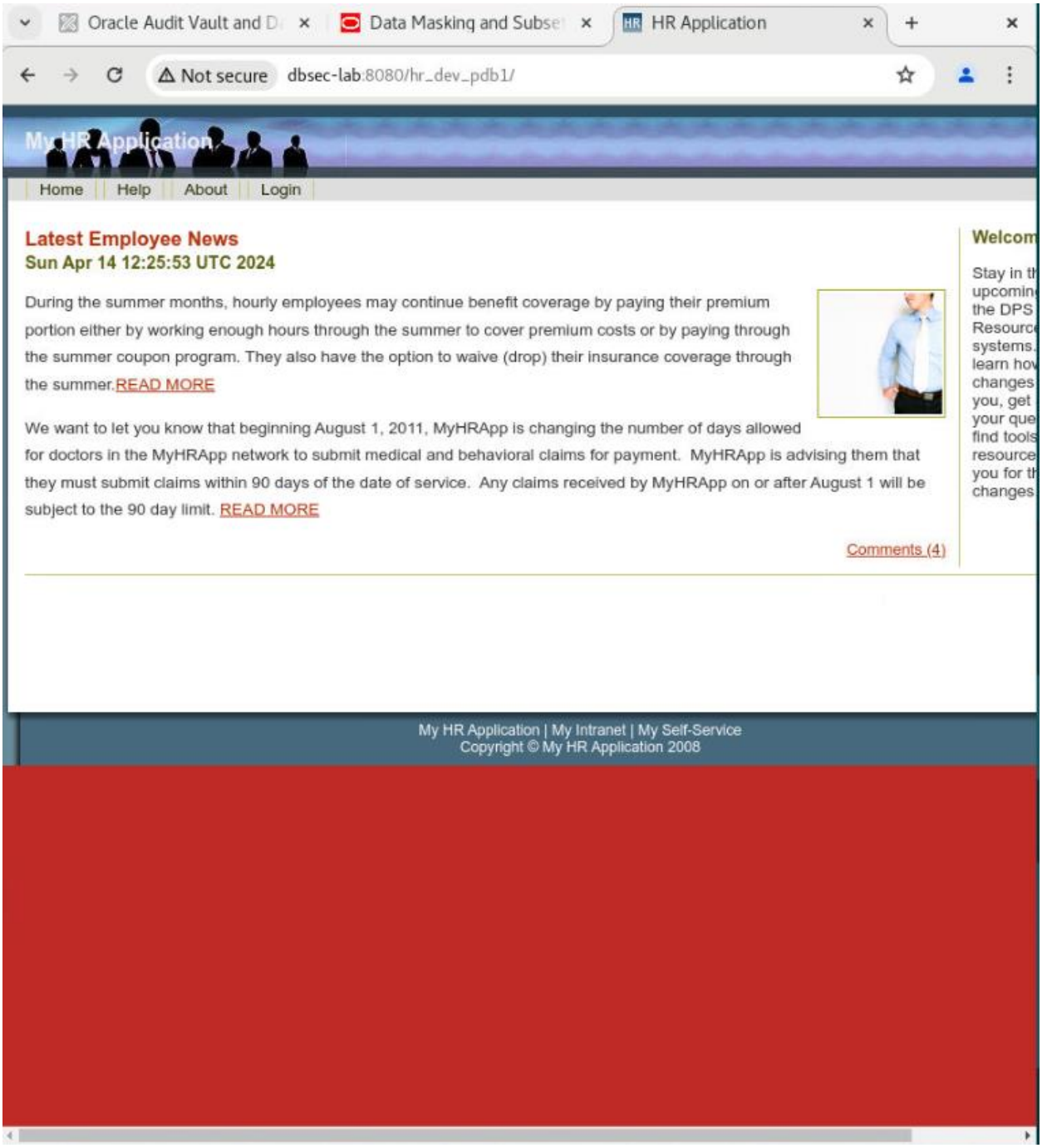
```
Prod: http://dbsec-lab:8080/hr_prod_pdb2
```
Copy

```
Dev: http://dbsec-lab:8080/hr_dev_pdb2
```
Copy

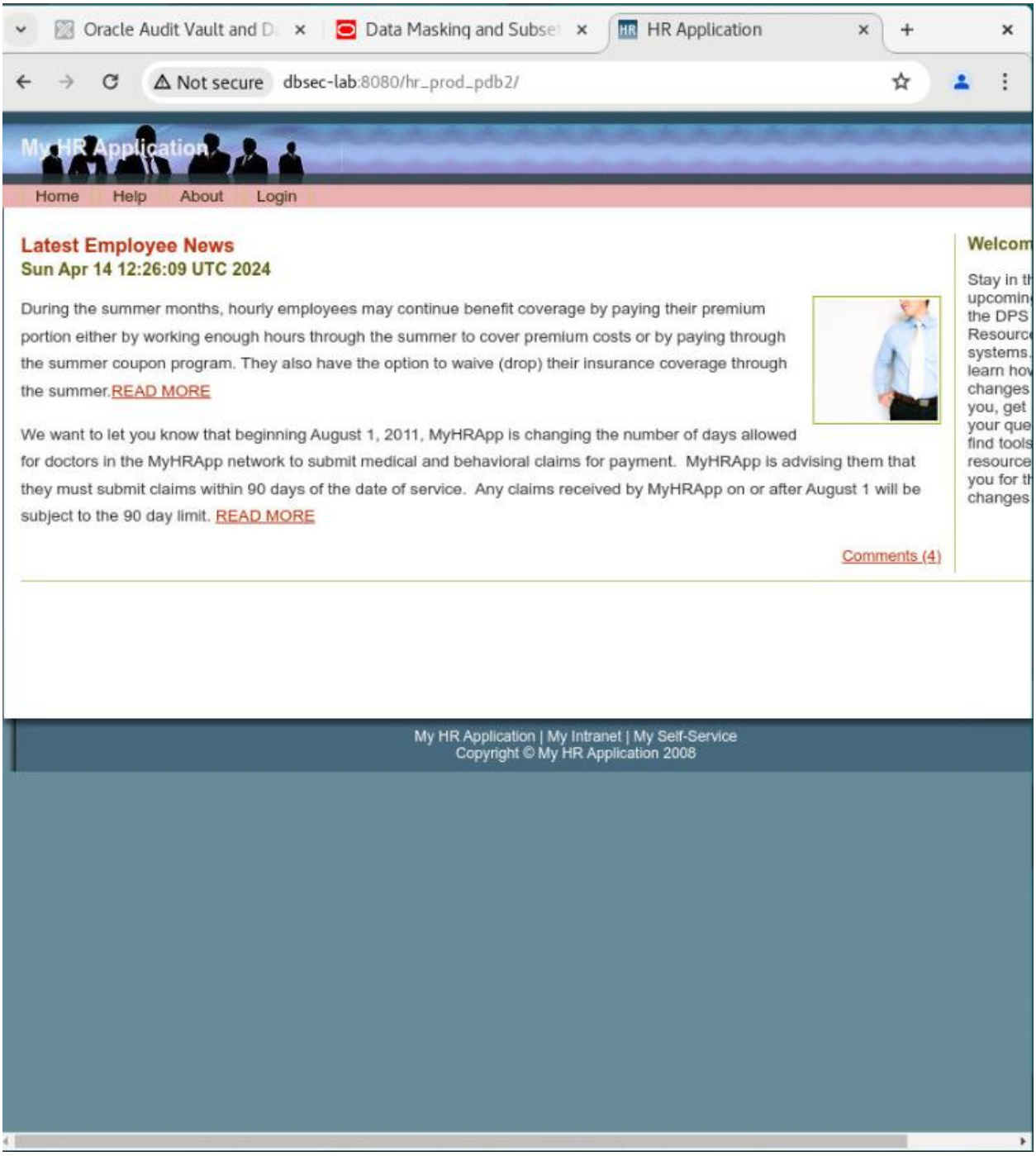
Với đường dẫn thứ nhất:



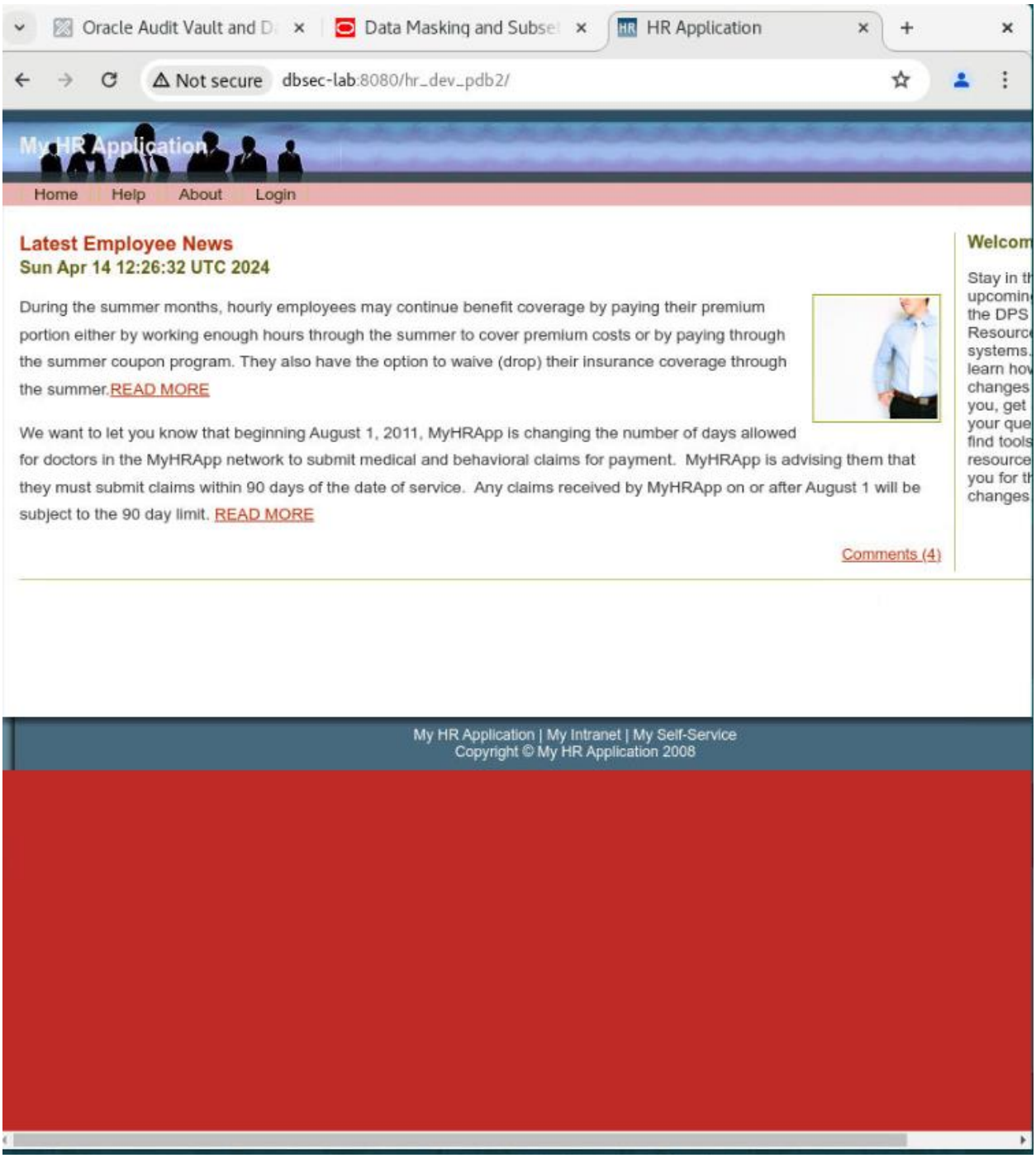
Đường dẫn thứ 2:



Đường dẫn thứ 3:



Đường dẫn thứ 4:



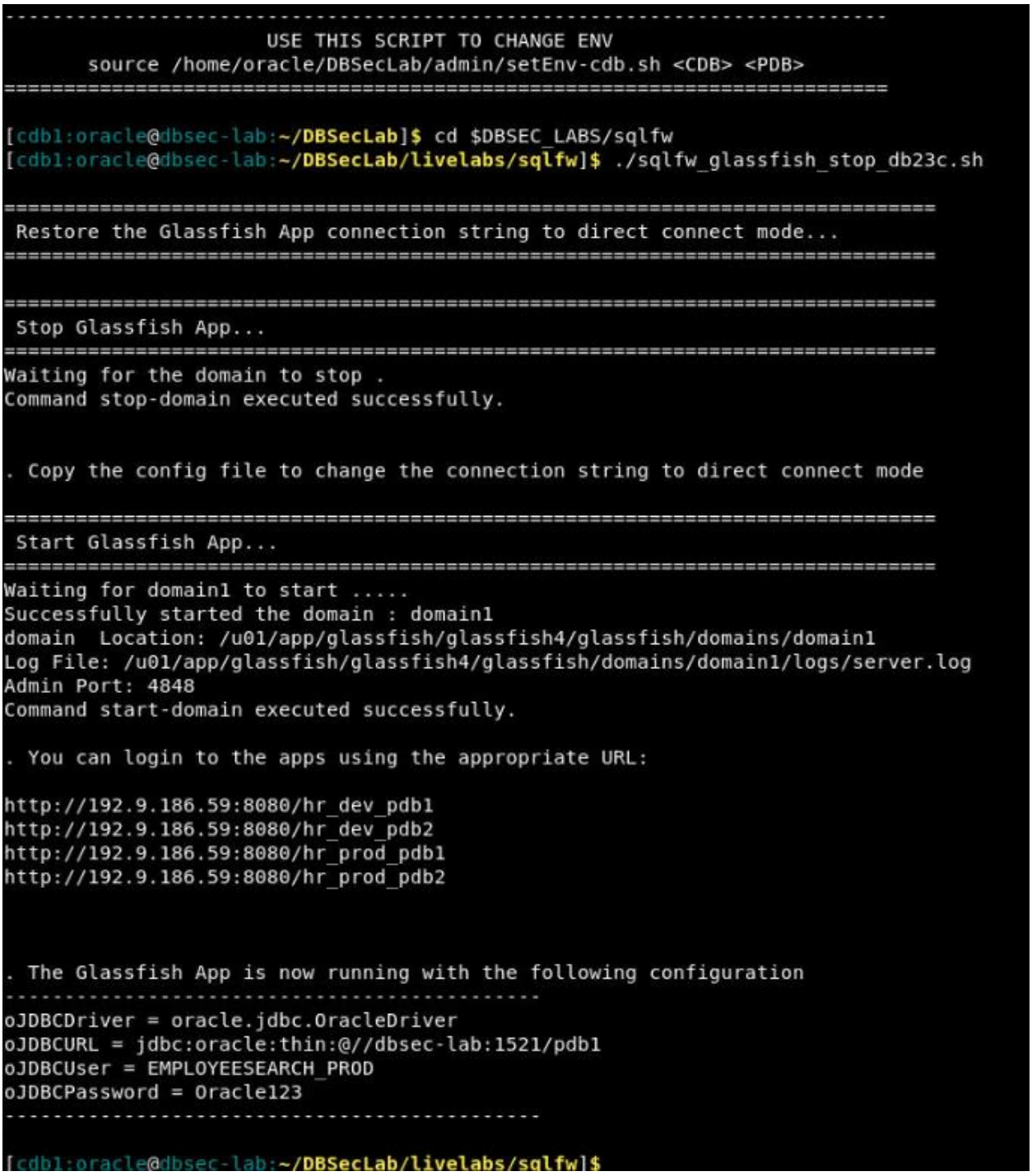
Qua các kết quả trên có thể thấy được rằng cả 4 đường dẫn đều chạy, có thể kết luận rằng môi trường đã sẵn sàng.

Task 2 - Set Glassfish to use pdb1 database in the dbseclab VM:

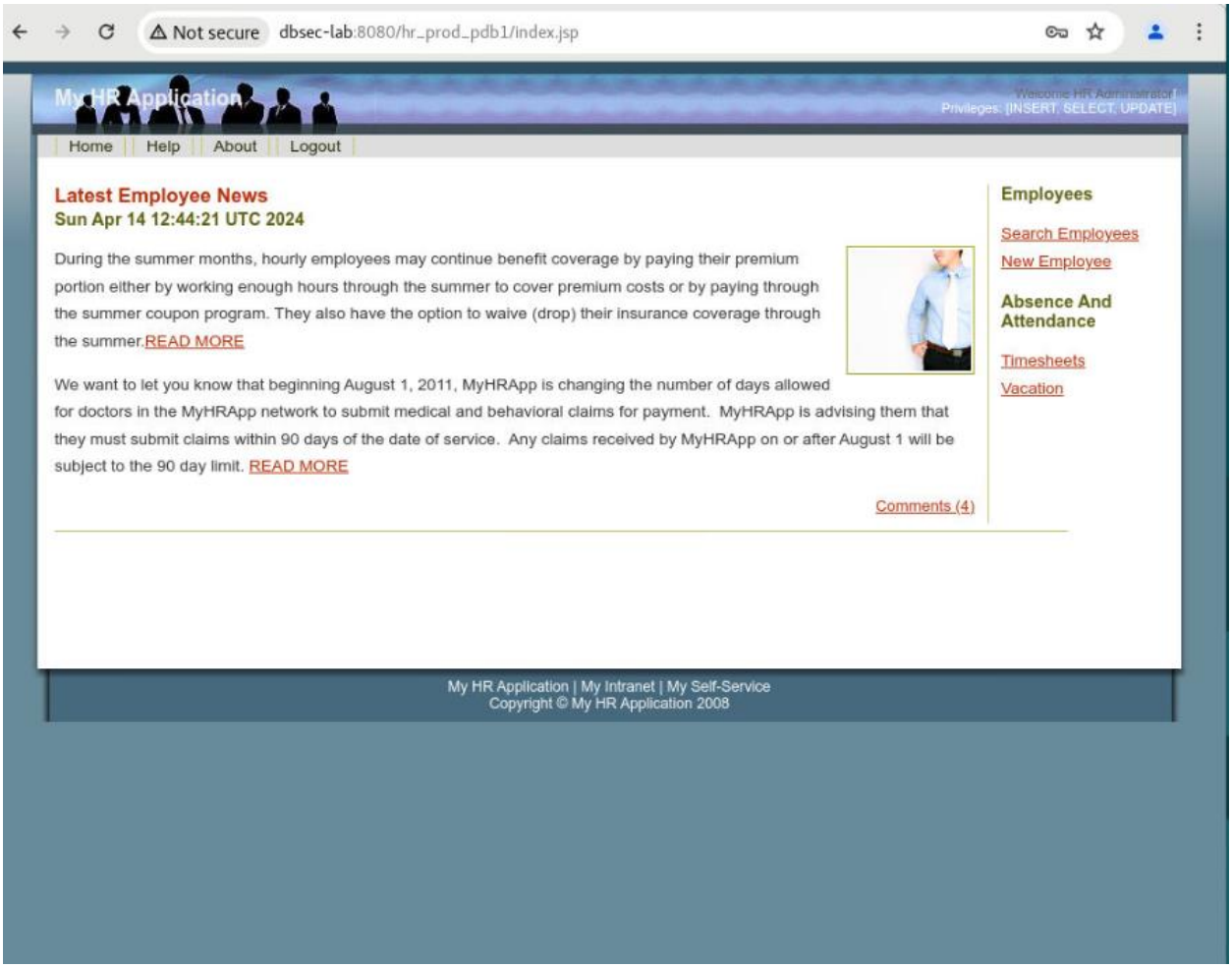
Bước đầu tiên em sẽ mở terminal lên và chạy lệnh "sudo su – oracle":

Sau đó đến đường dẫn "$DBSEC_LABS/sqlfw":

Chạy "./sqlfw_glassfish_stop_db23c.sh":

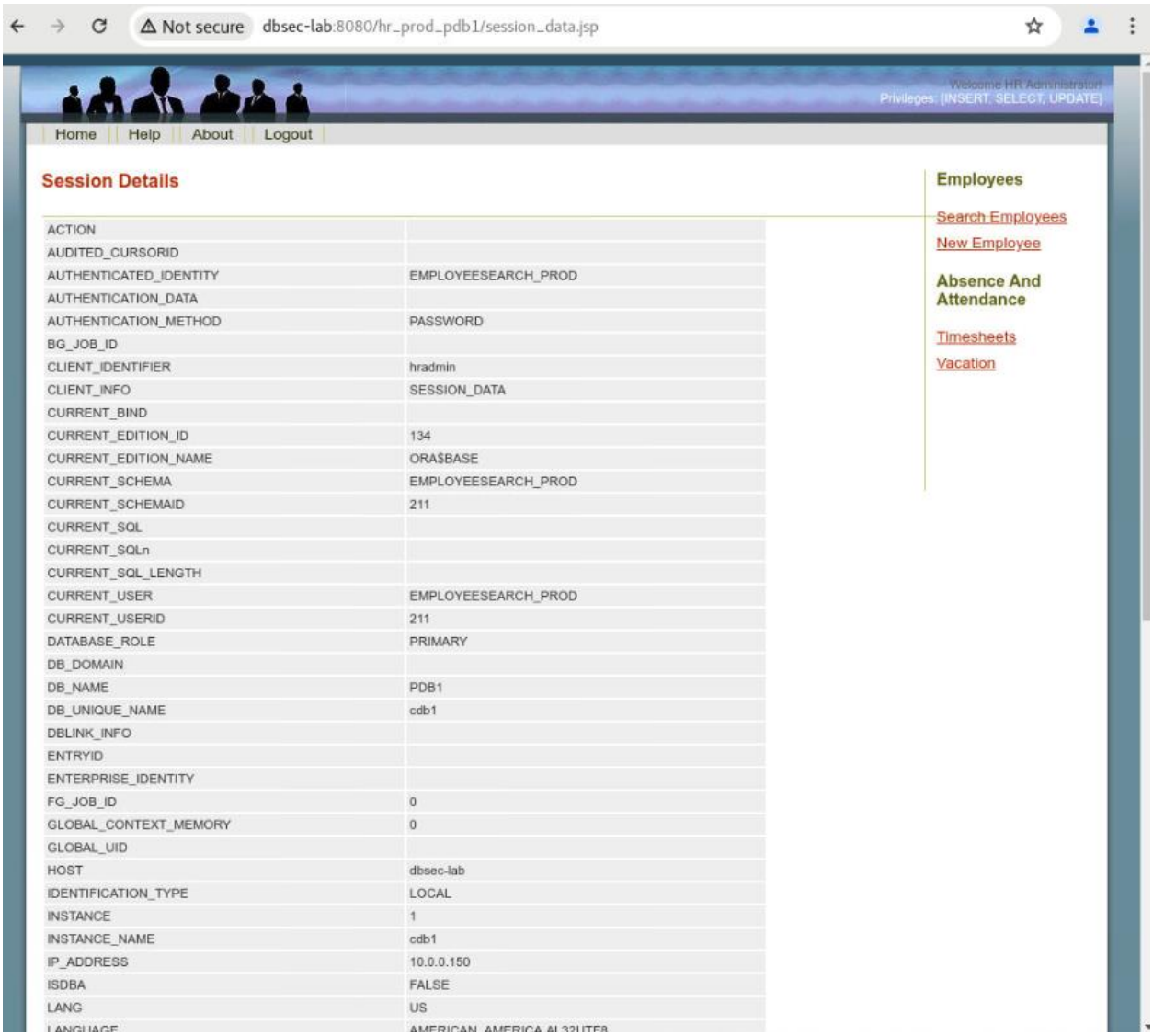


Tiếp đến em sẽ kiểm tra xem nó đã hoạt động đúng mong đợi chưa bằng cách truy cập vào url http://dbsec-lab:8080/hr_prod_pdb1 để kết nối đến Glassfish App. Rồi đăng nhập vào với username là “hradmin” và password là "Oracle123":



Sau khi đăng nhập xong thì màn hình như trên xuất hiện ra.

Lúc này khi bấm vào dòng chữ "Welcome HR Administrator" ở bên góc phải trên cùng màn hình thì cửa sổ Session Details xuất hiện:



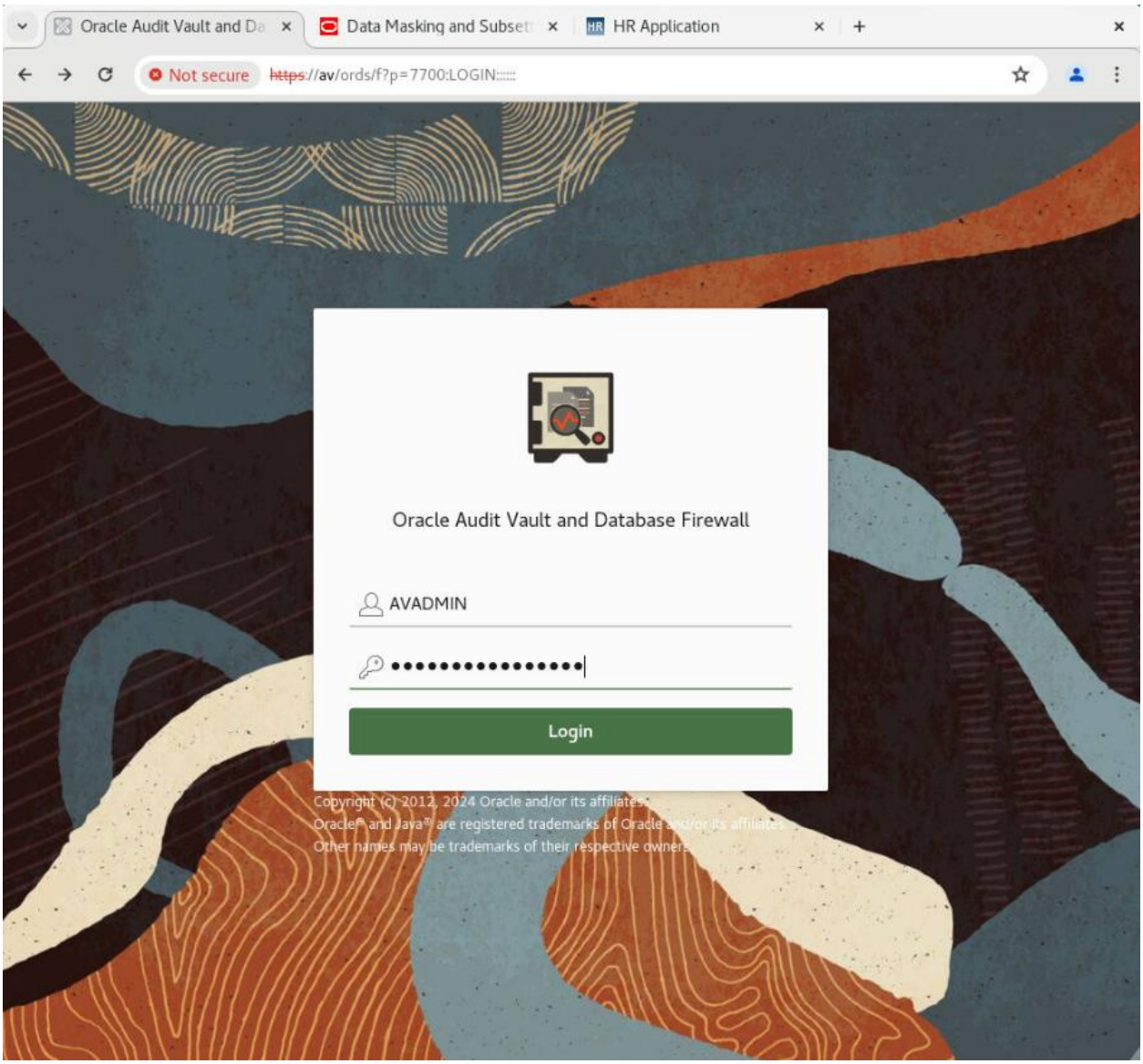
Lab 3: Audit Vault and DB Firewall (AVDF)

Task 1: Reset the randomly generated password:

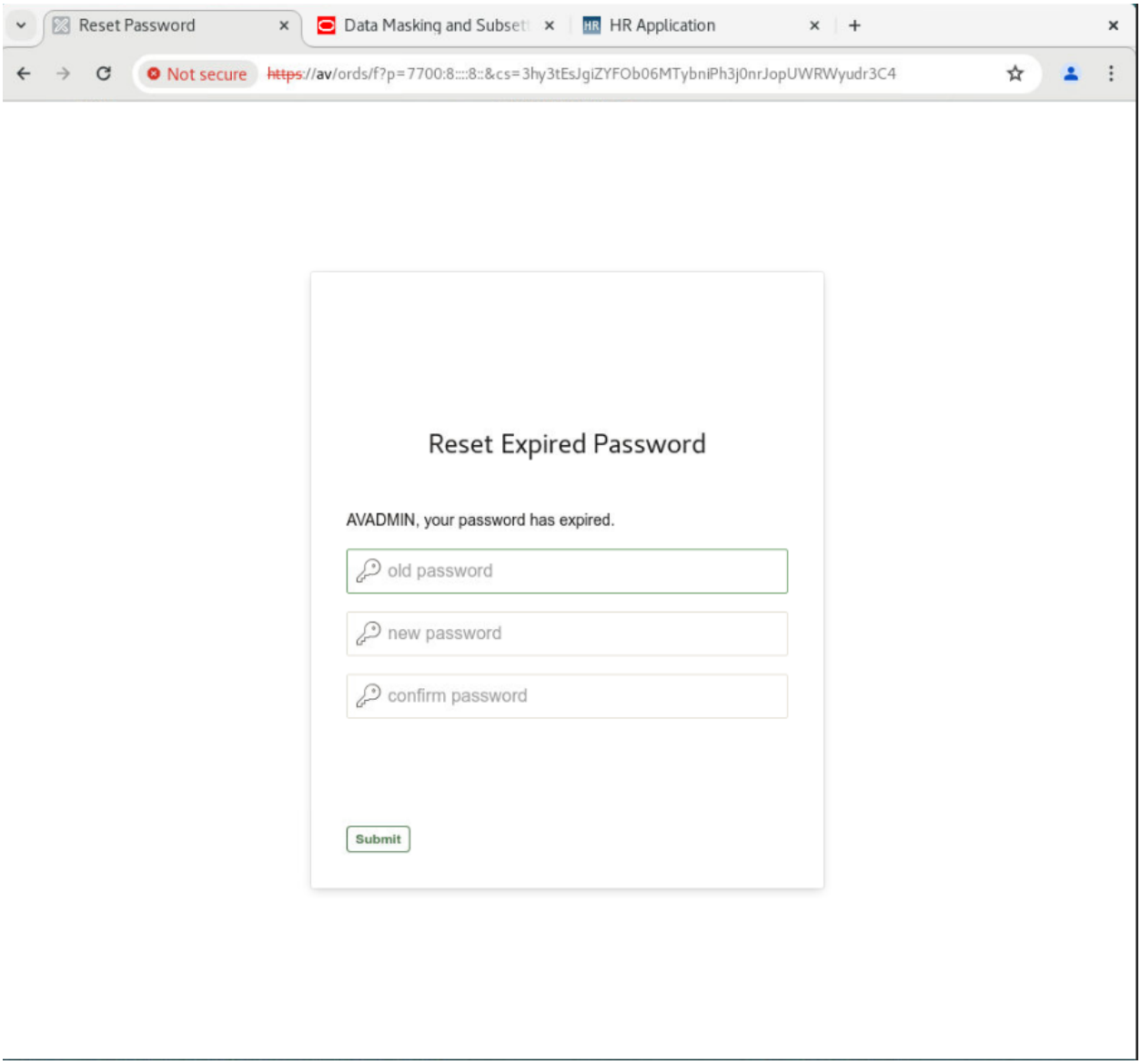
Bước đầu em sẽ truy cập đến đường dẫn "$DBSEC_LABS/avdf/avs" thông qua terminal:

Sau đó sẽ mở "$AVUSR_PWD" lên:

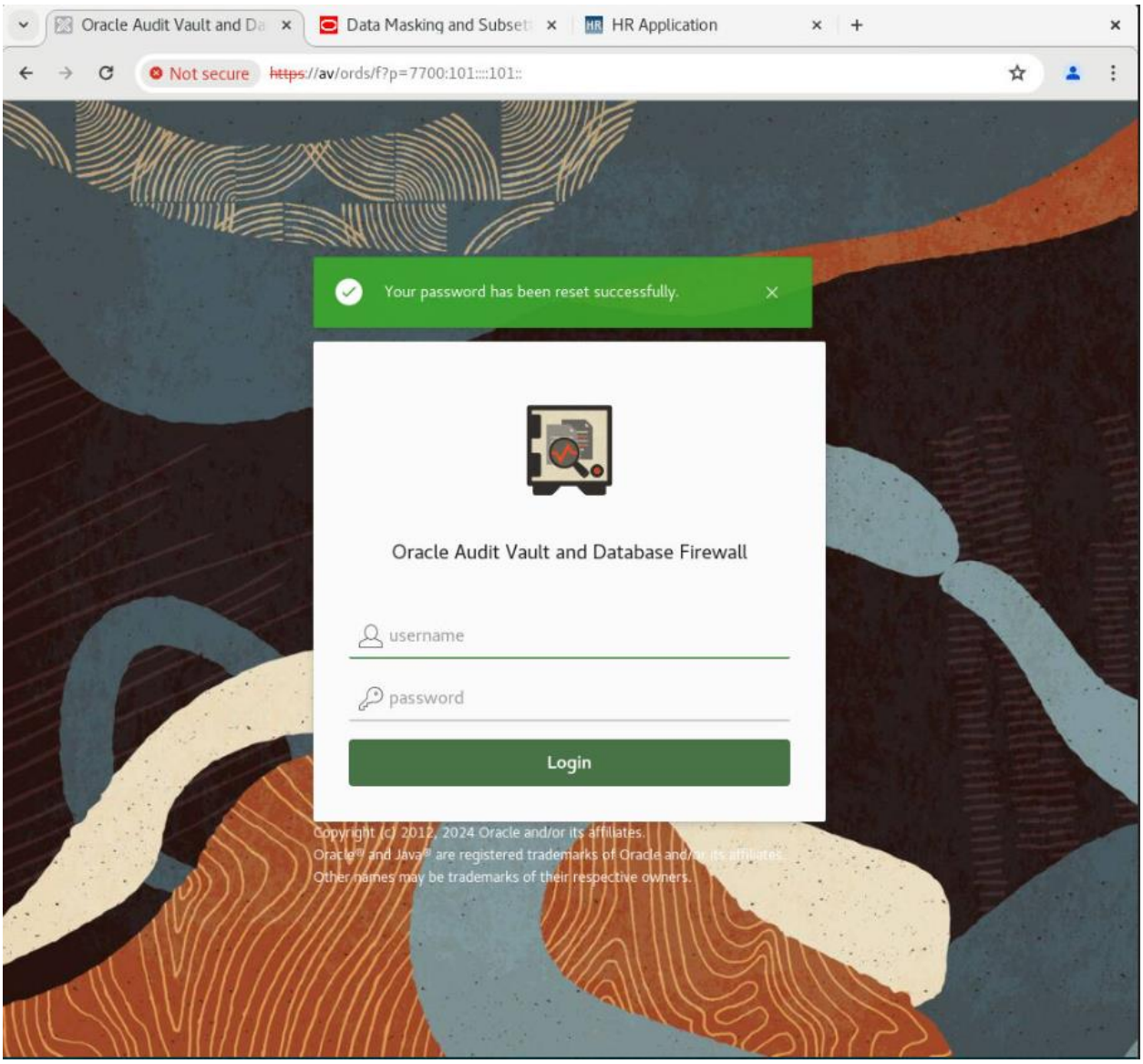
Kế tiếp em thực hiện truy cập đến https://av và đăng nhập với username là AVADMIN, password là password random vừa mở từ $AVUSR_PWD:



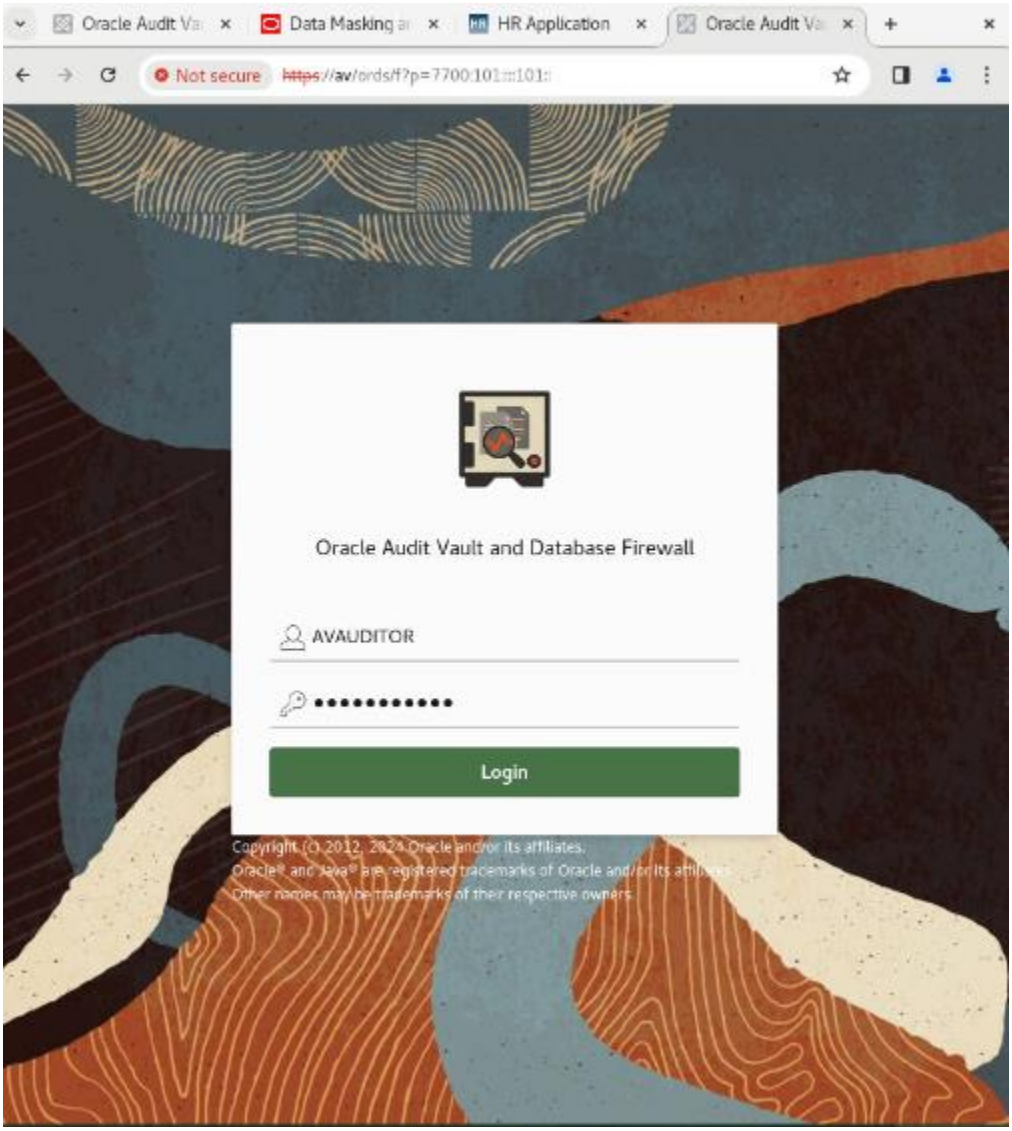
Sau khi đăng nhập xong, màn hình reset password hiện ra:



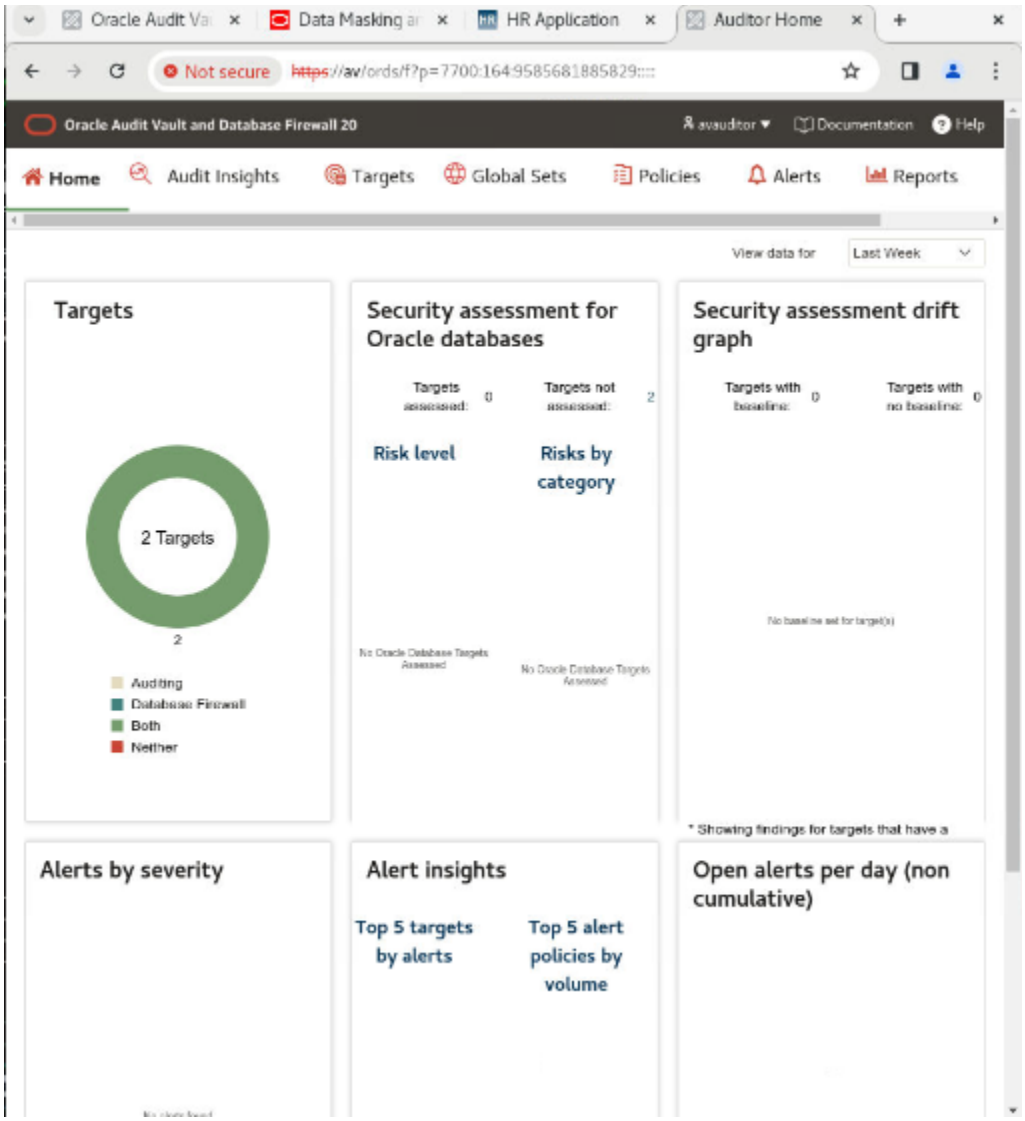
Em tiến hành đổi password và submit, kết quả nhận được là:



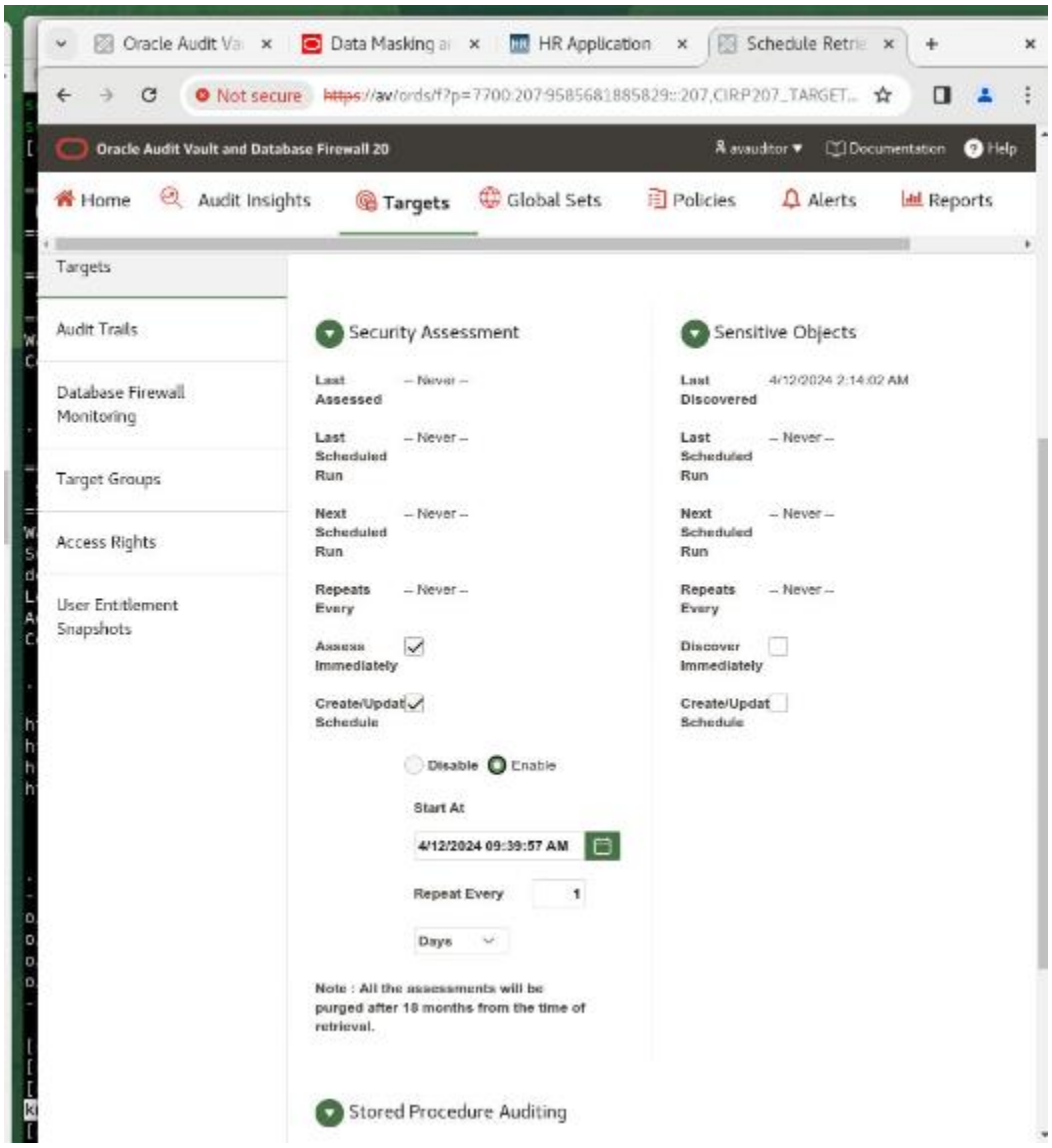
Task 2: Assess and Discover:



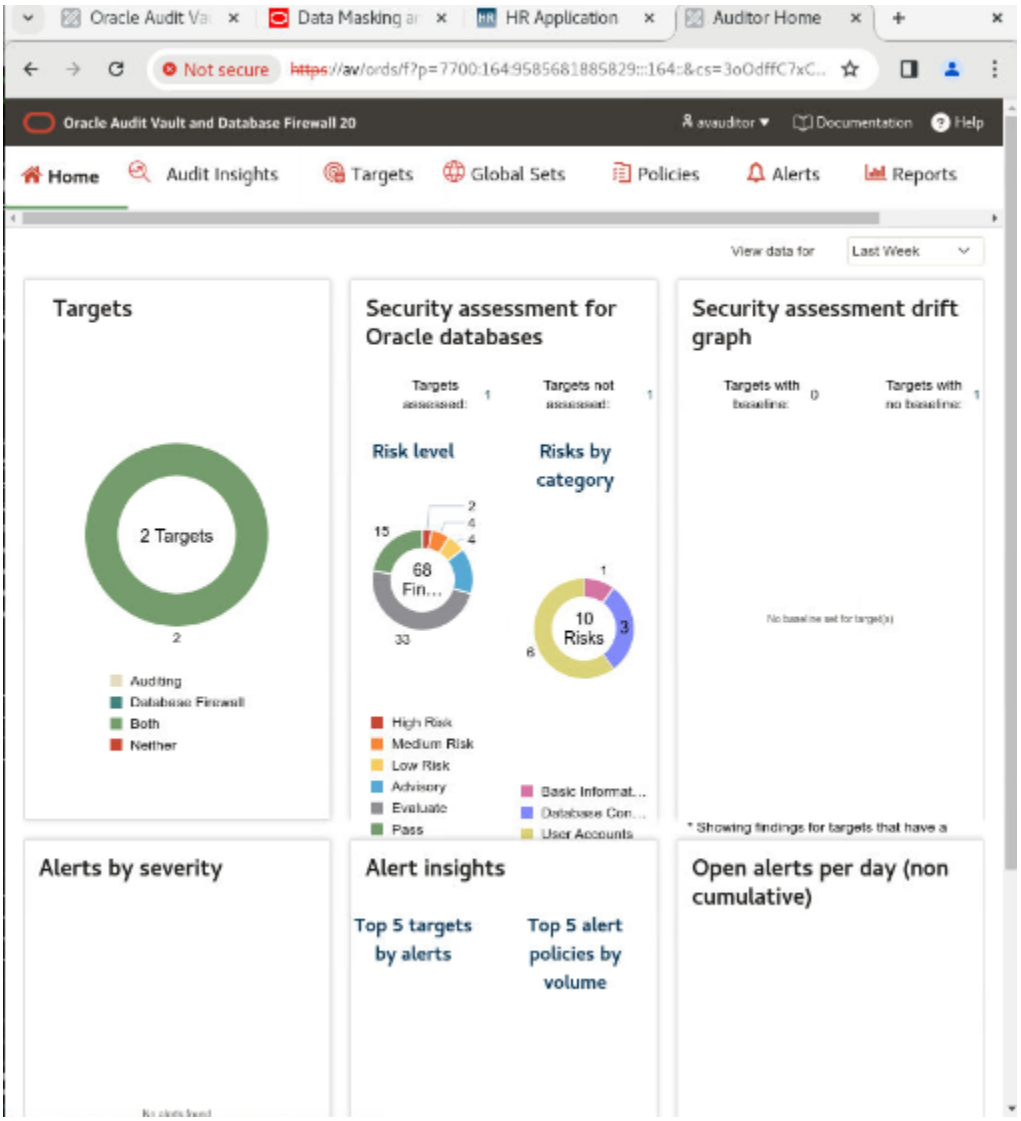
Login vào tài khoản AVAUDITOR bằng mật khẩu đã đổi ở task1



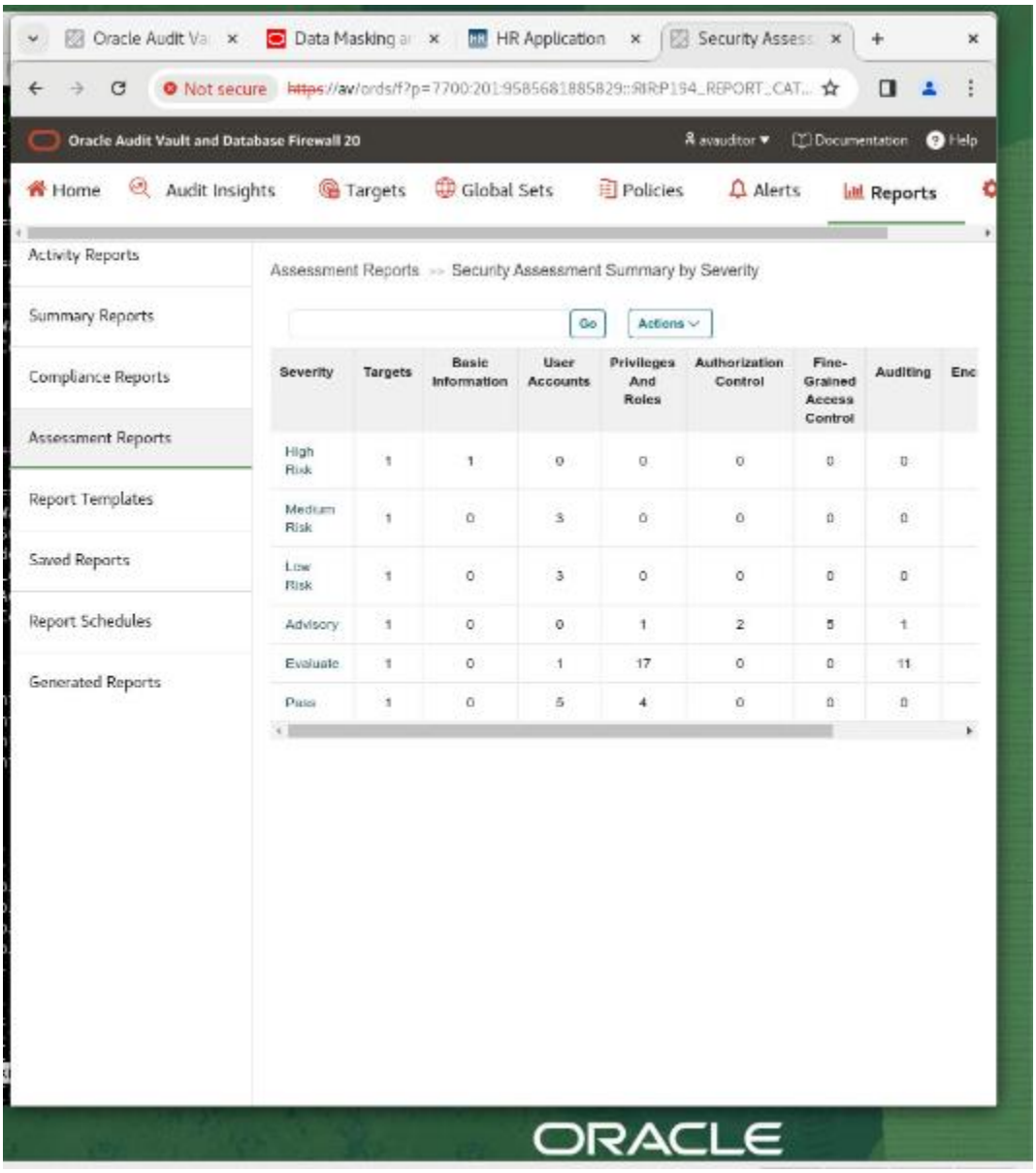
Màn hình home của tài khoản:



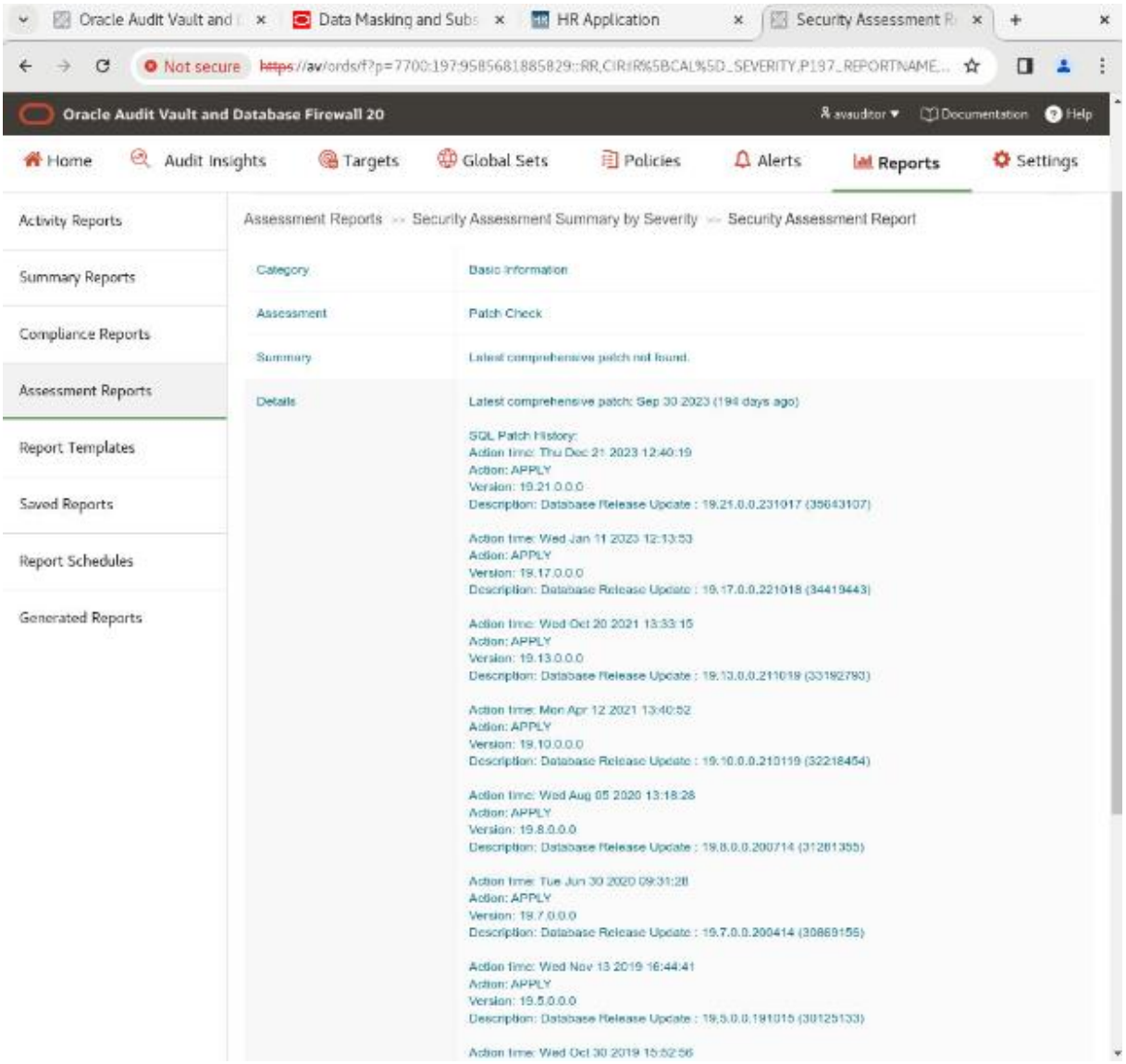
Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục Security Assesment và enable. Nhấn Save:



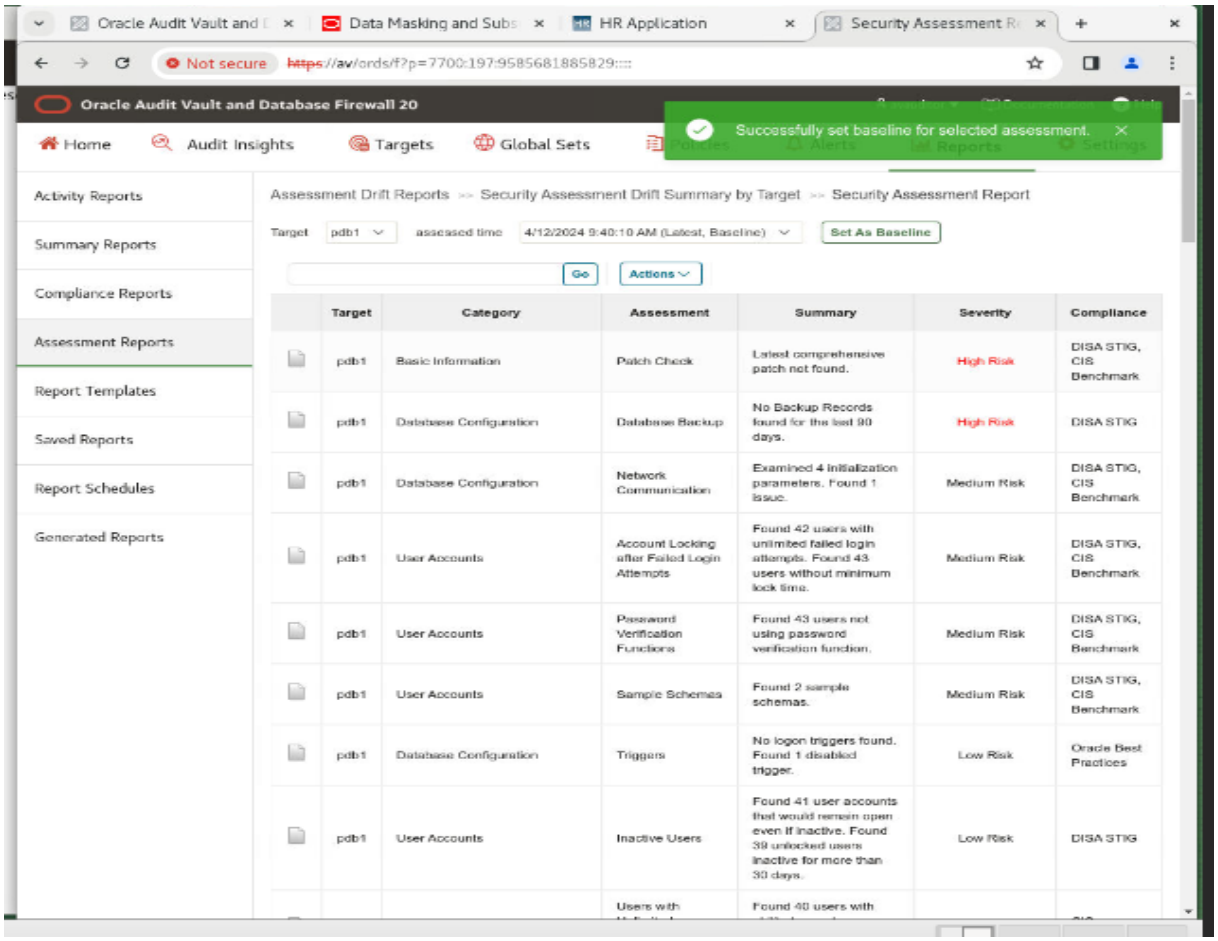
Quay lại Home, ta thấy phần Security Assessment đã có thêm các mục mới



Trong tab Report, click vào Security Assessment Summary by Serenity trong cột Assessment Report. Ta có thể thấy các risk với các mức độ báo động khác nhau.

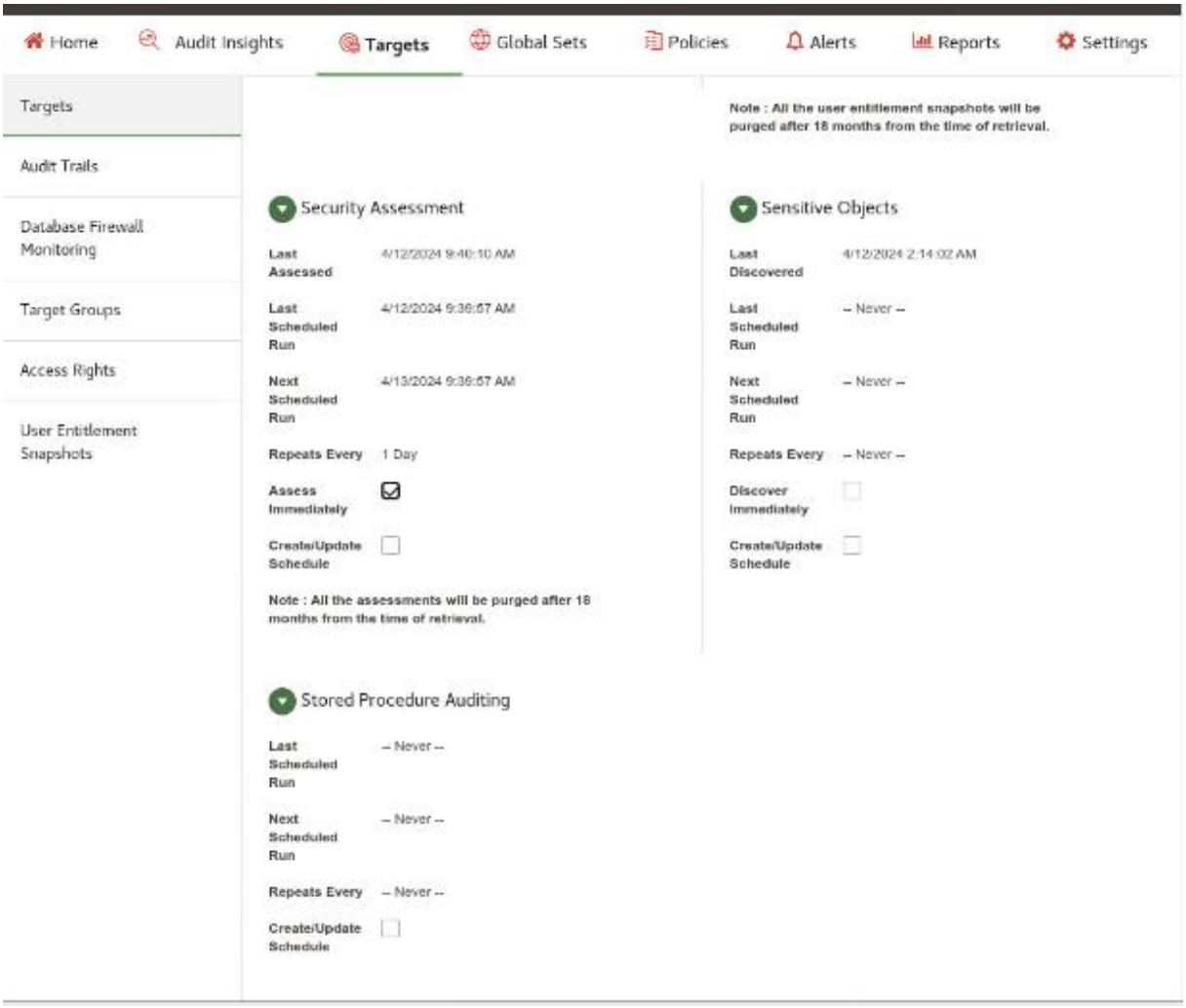


VD: High risk assessments

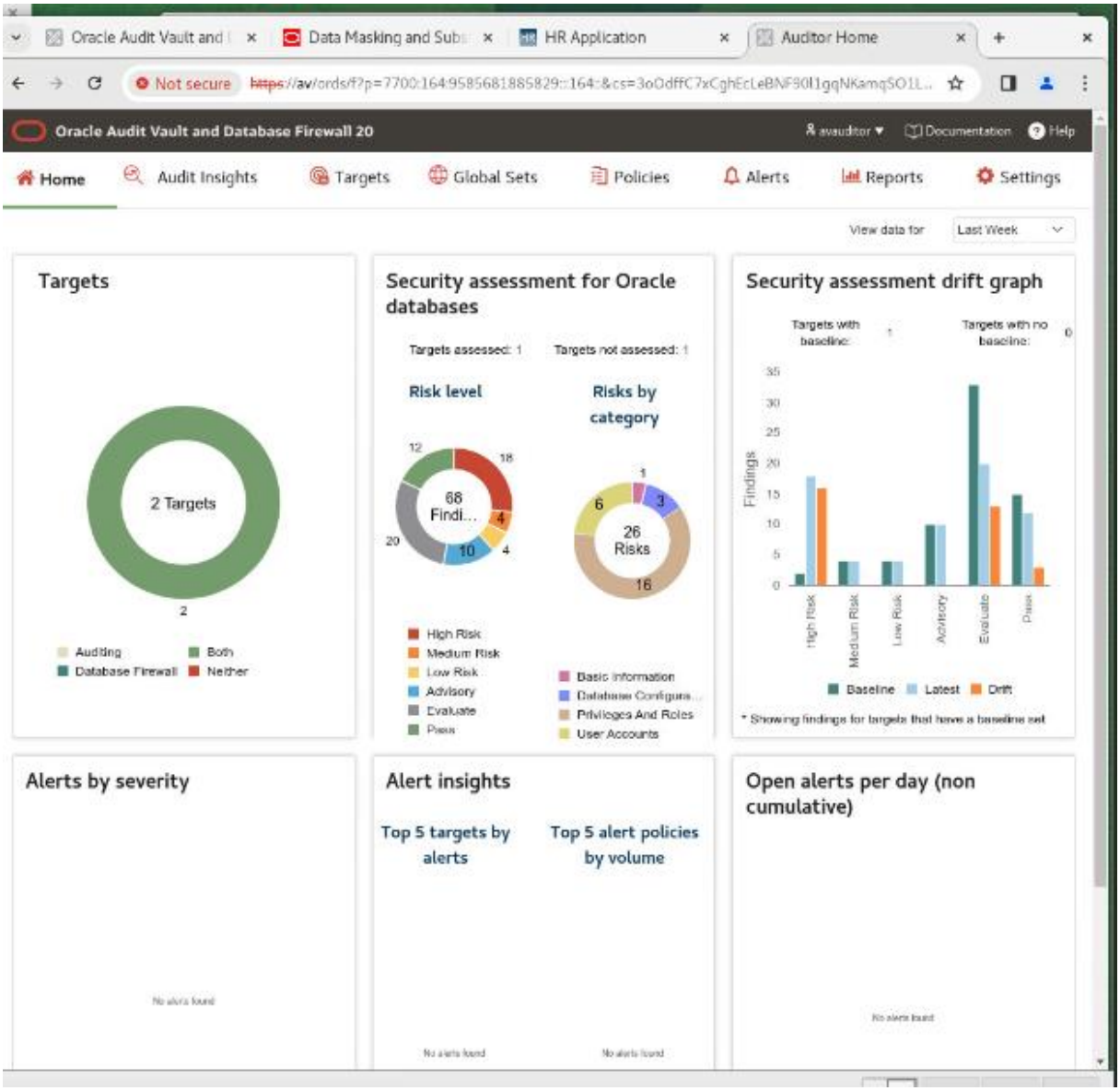


Trong mục Target with no baseline ở Home, ta chọn pdb1 để set baseline.

Tạo drift cho pdb1



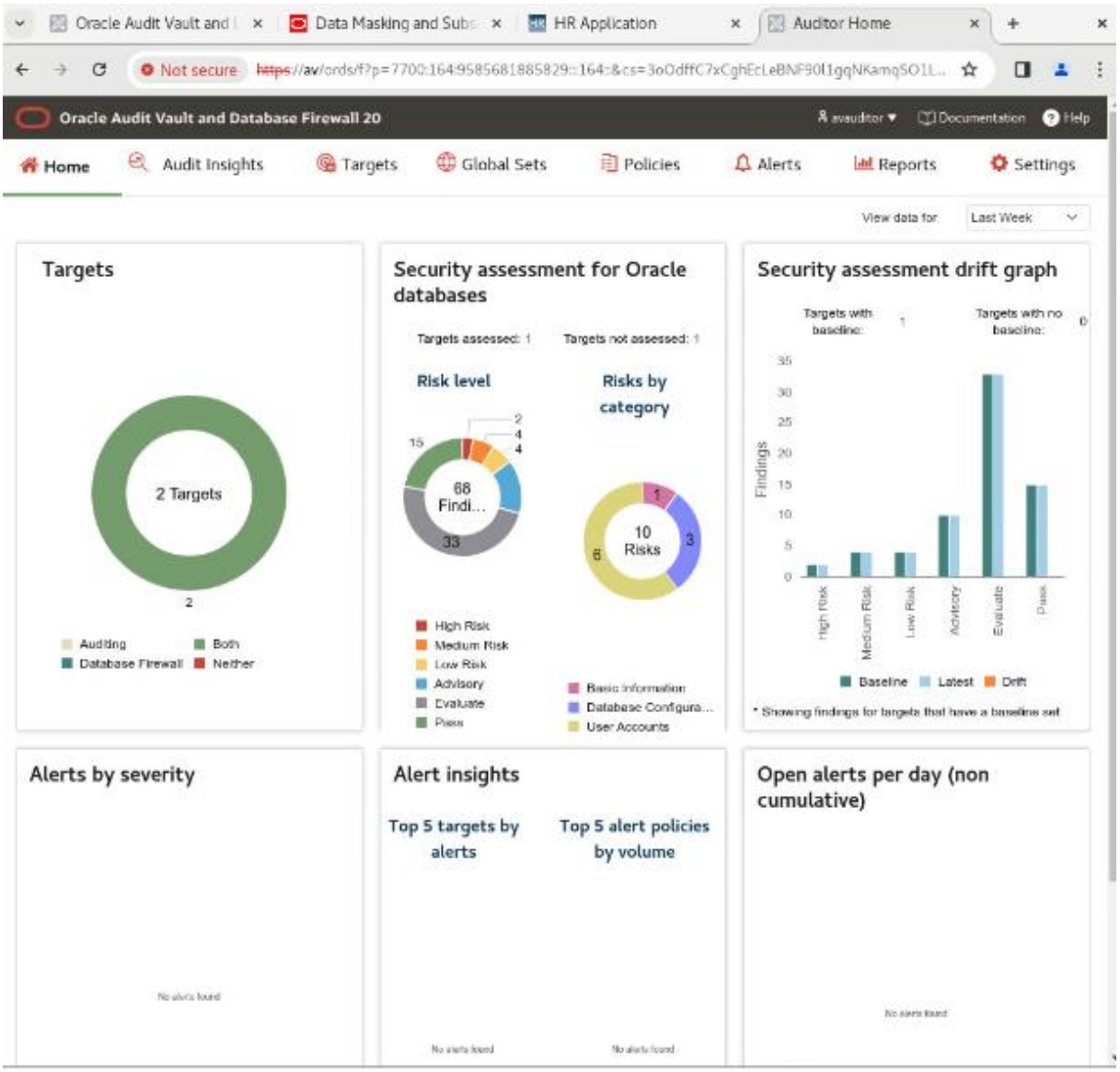
Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào ô Assess Imediately trong mục Security Assesment và enable. Nhấn Save



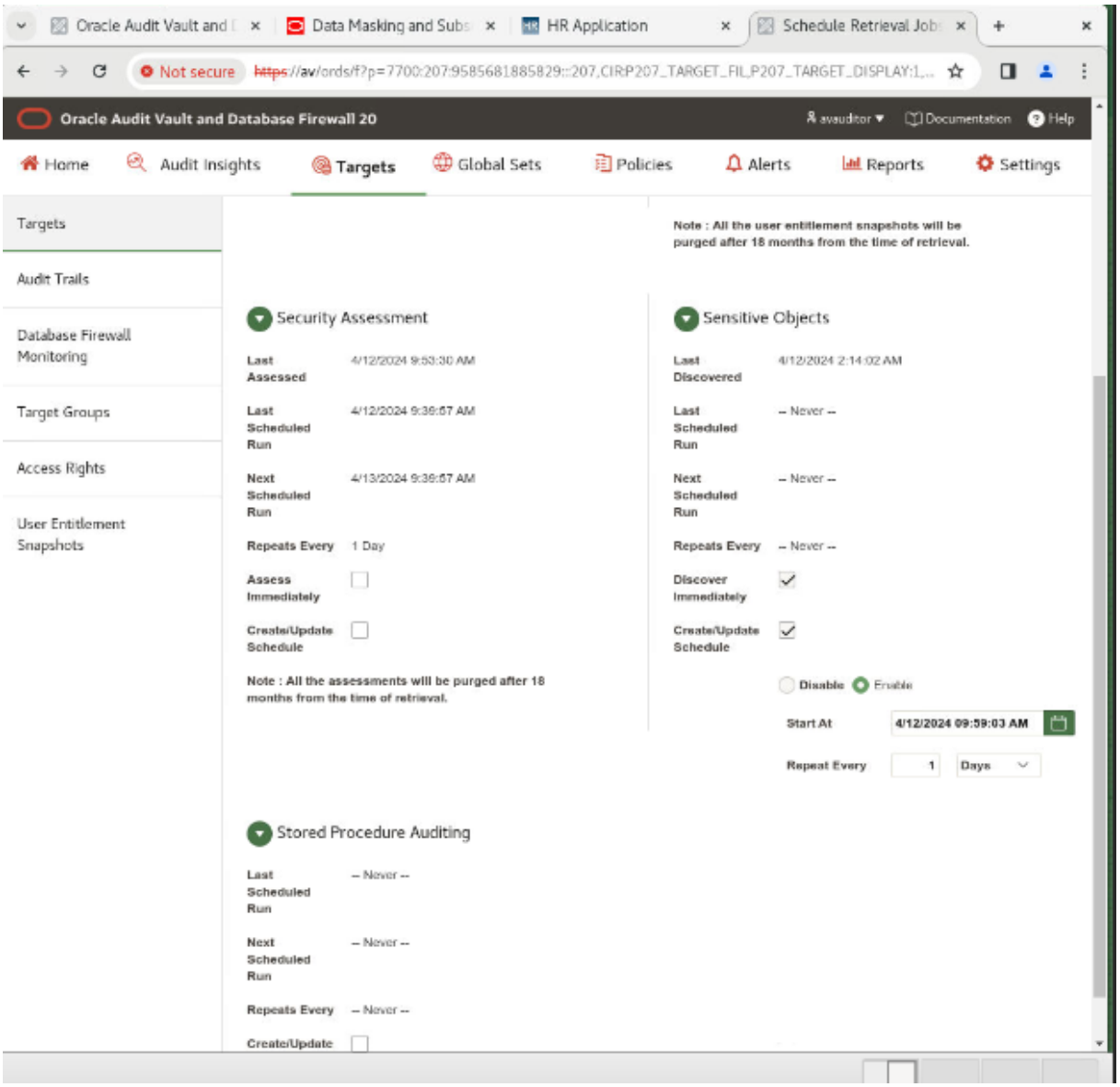
Ta thấy rằng mục Target with baseline đã chuyển thành 1 với dữ liệu thống kê cho pdb1

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_mitigate-risk.sh pdb1

================================================================================
 Mitigate the drift risk on pdb1...
================================================================================

Revoke succeeded.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

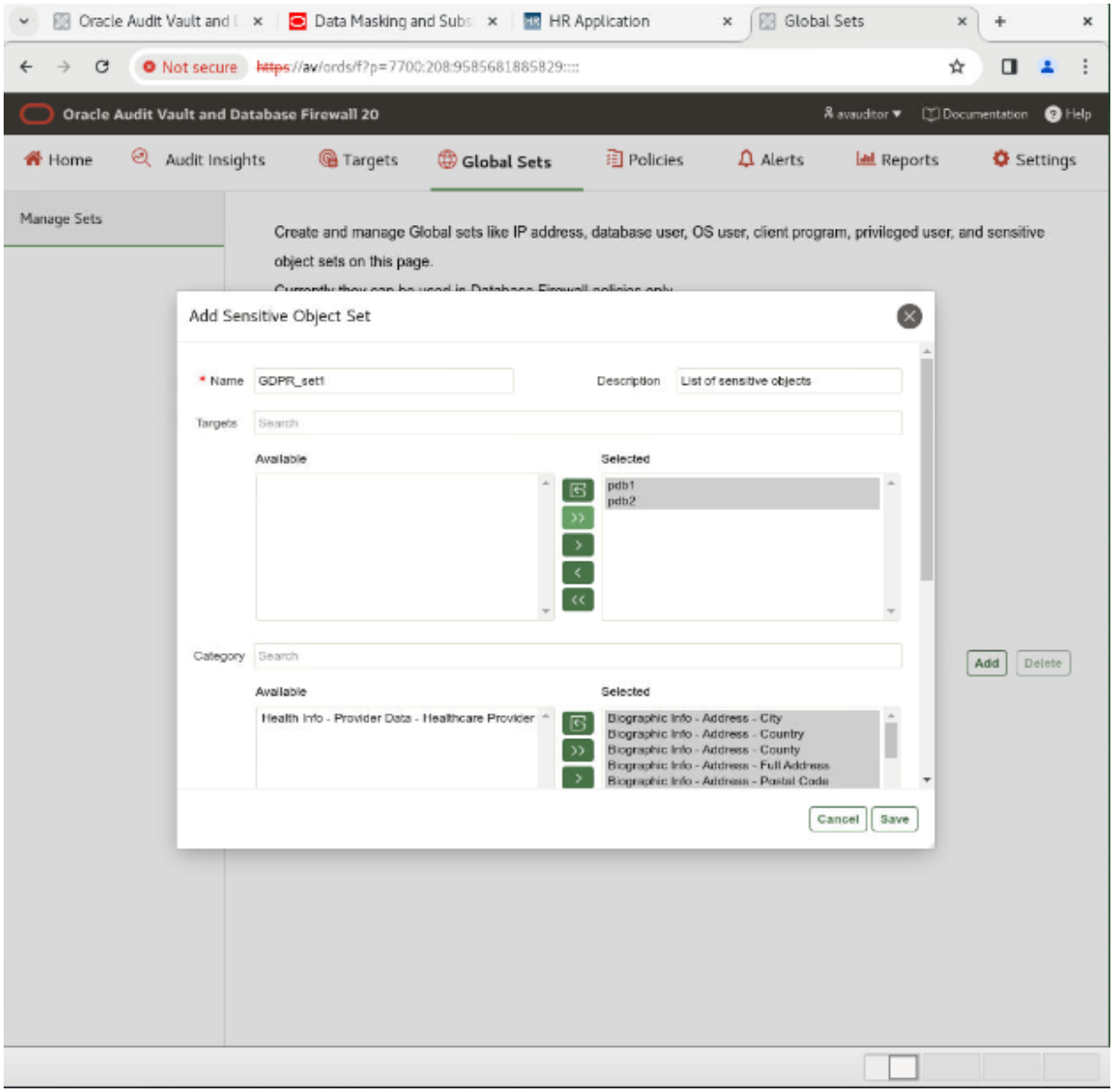
Giảm độ risk của drift trên pdb1



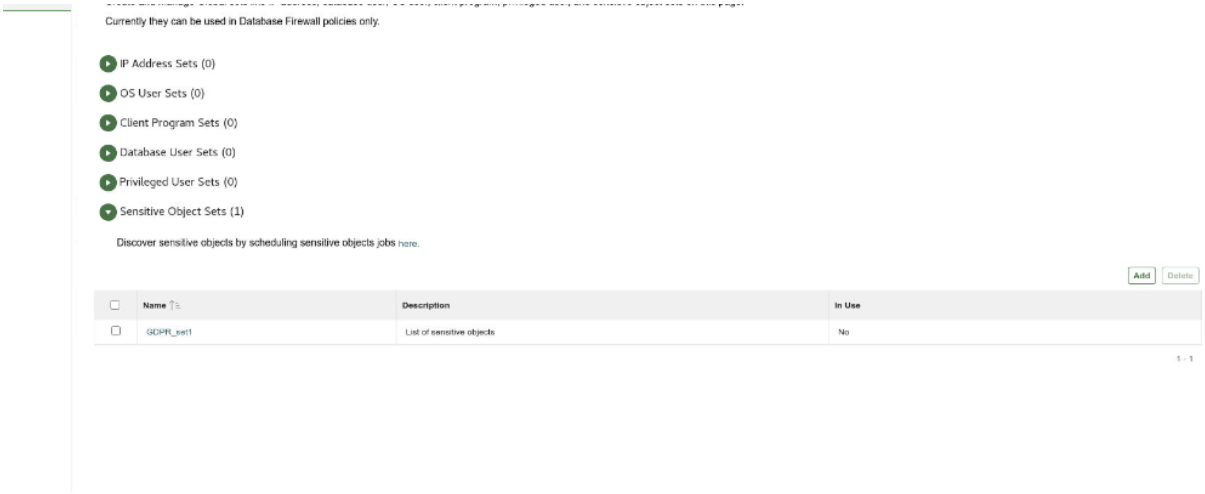
Kết quả sau khi giảm độ risk của drift trên pdb1



Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **Sensitive Objects** và enable. Nhấn Save

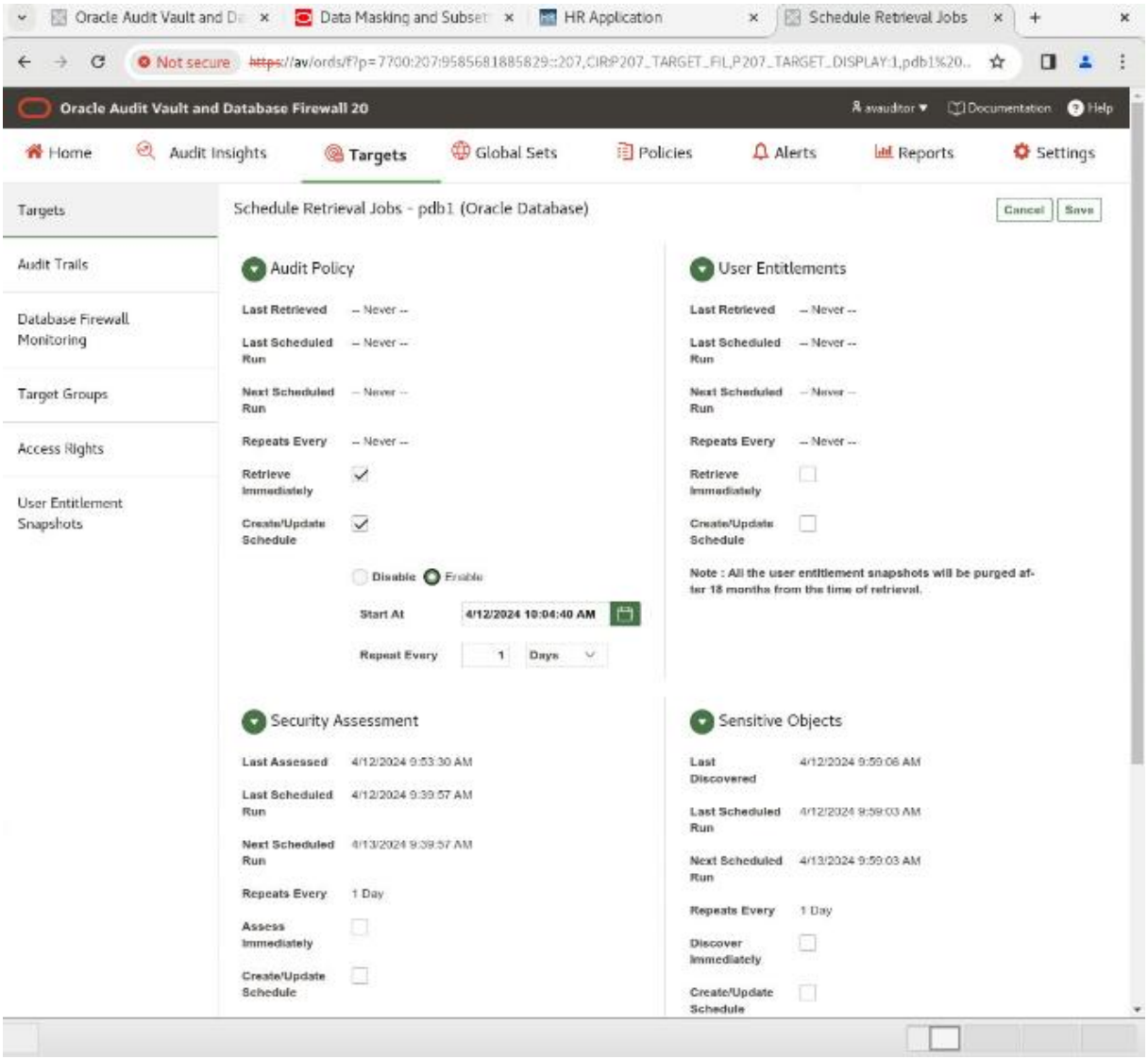


Trong tab Global Sets, click vào hành **Sensitive object sets** để mở rộng. Chọn add. Đặt tên, mô tả và chọn cả 2 pdb1 và pdb2. Nhấn Save

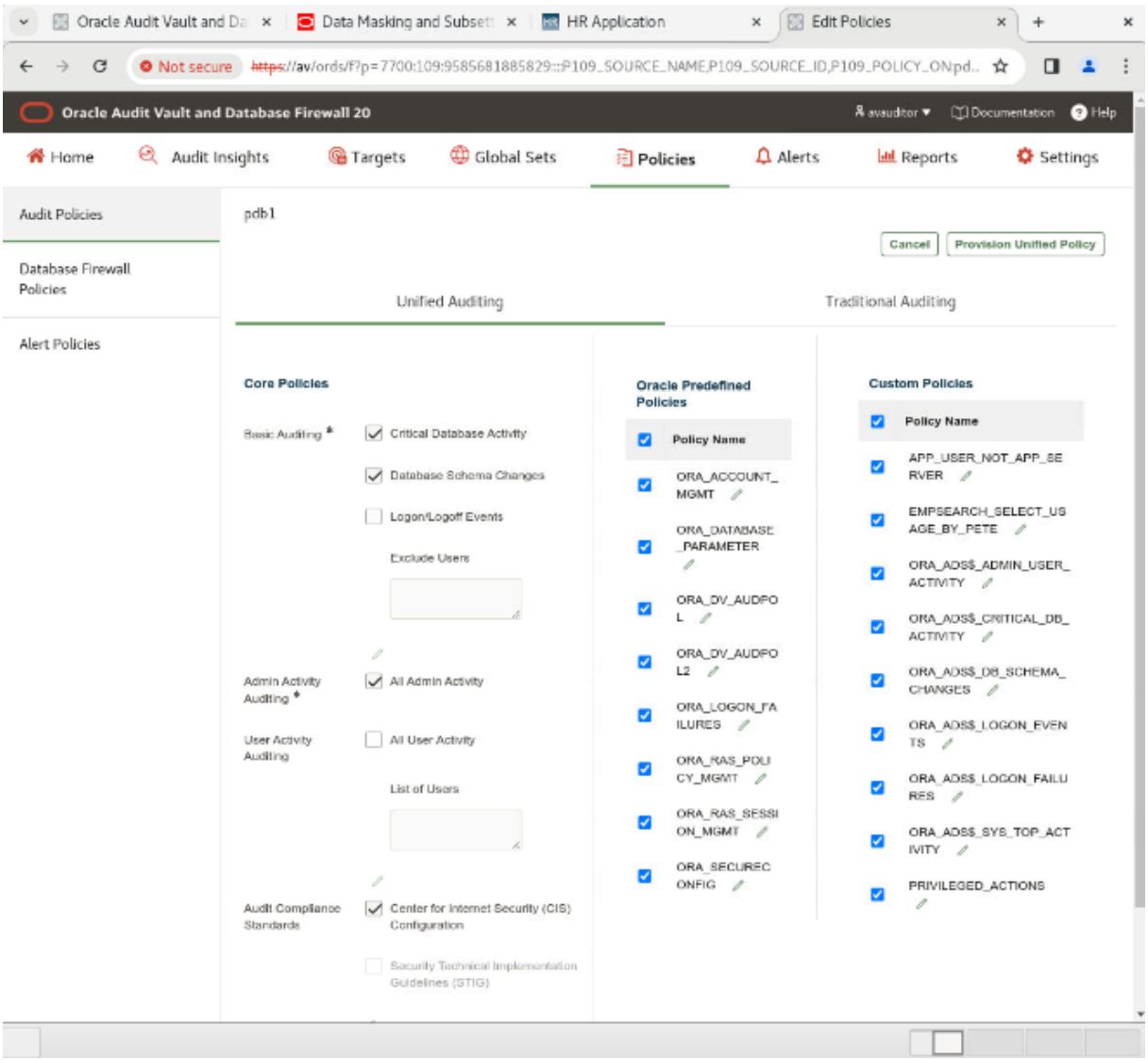


Kết quả sau khi tạo sets

Task3: Audit and Monitor:



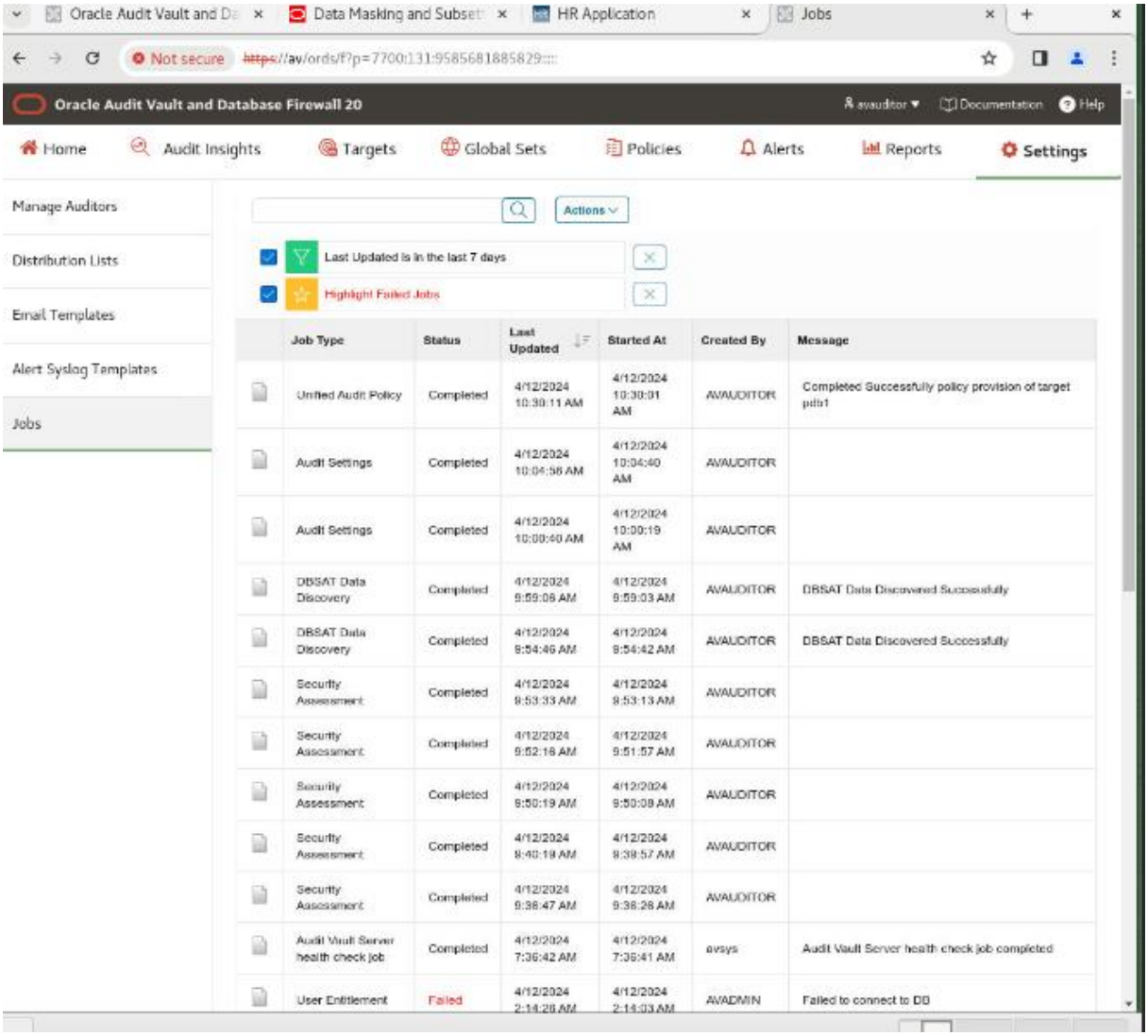
Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **Audit Policy** và enable. Nhấn Save



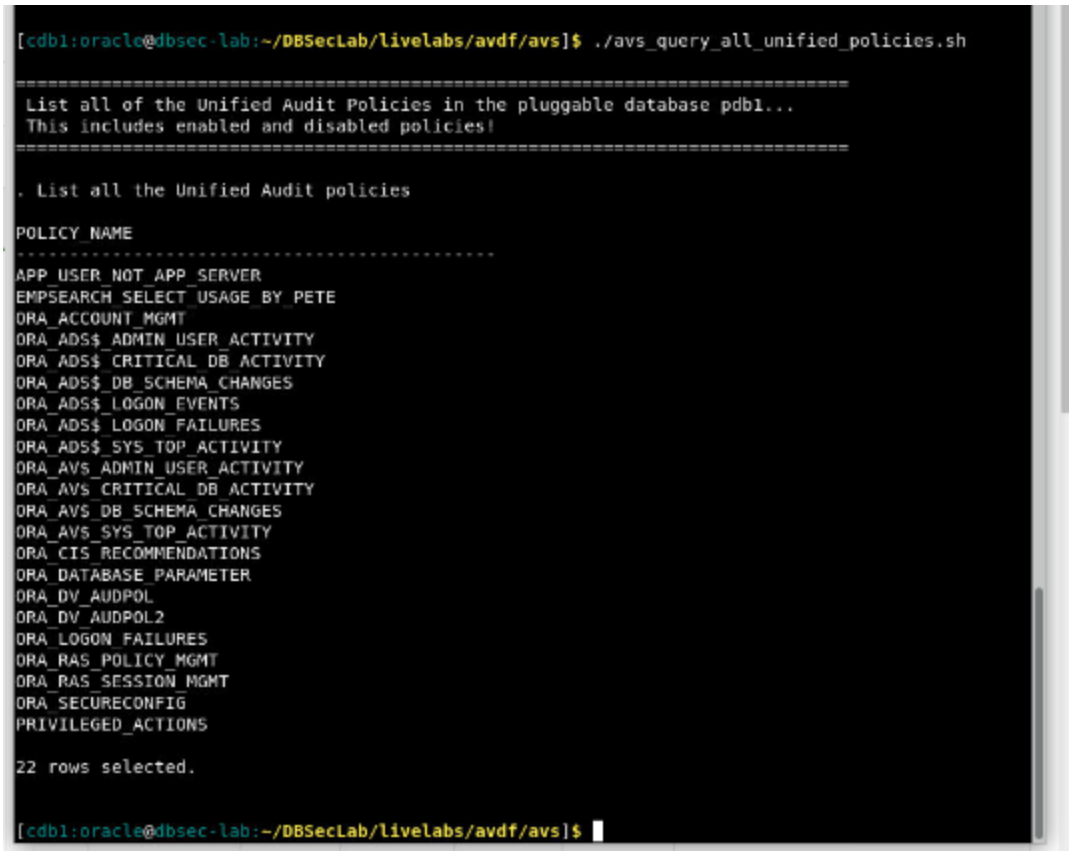
Trong Tab Policies, mục Audit Policies, click các mục:

- *Critical Database Activity*
- *Database Schema Changes*
- *All Admin Activity*
- *Center for Internet Security (CIS) Configuration*

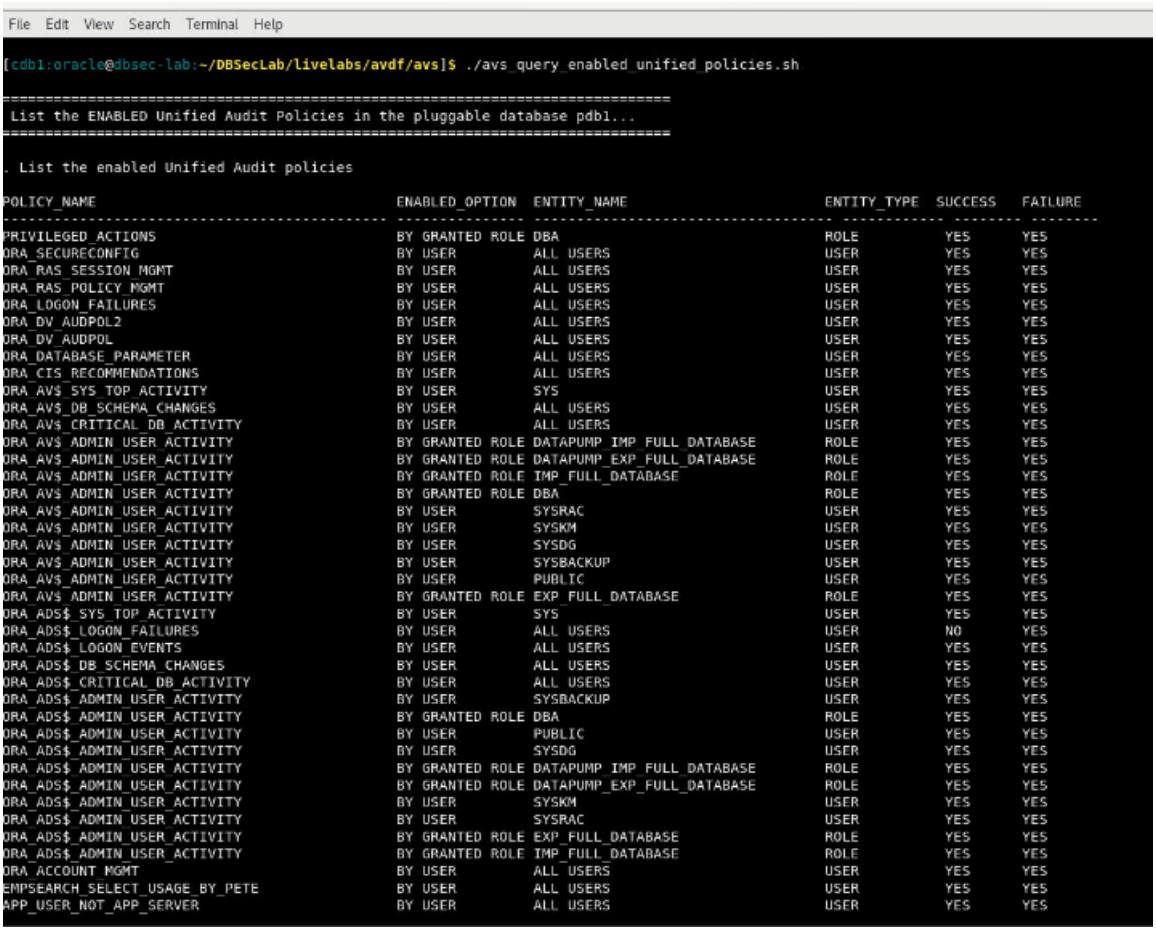
Nhấn **Provision Unified Policy**



Kiểm tra trong mục Setting, trong mục Jobs ta có thể thấy một job tên **Unified Audit Policy** đã hoàn thành ở trên đầu

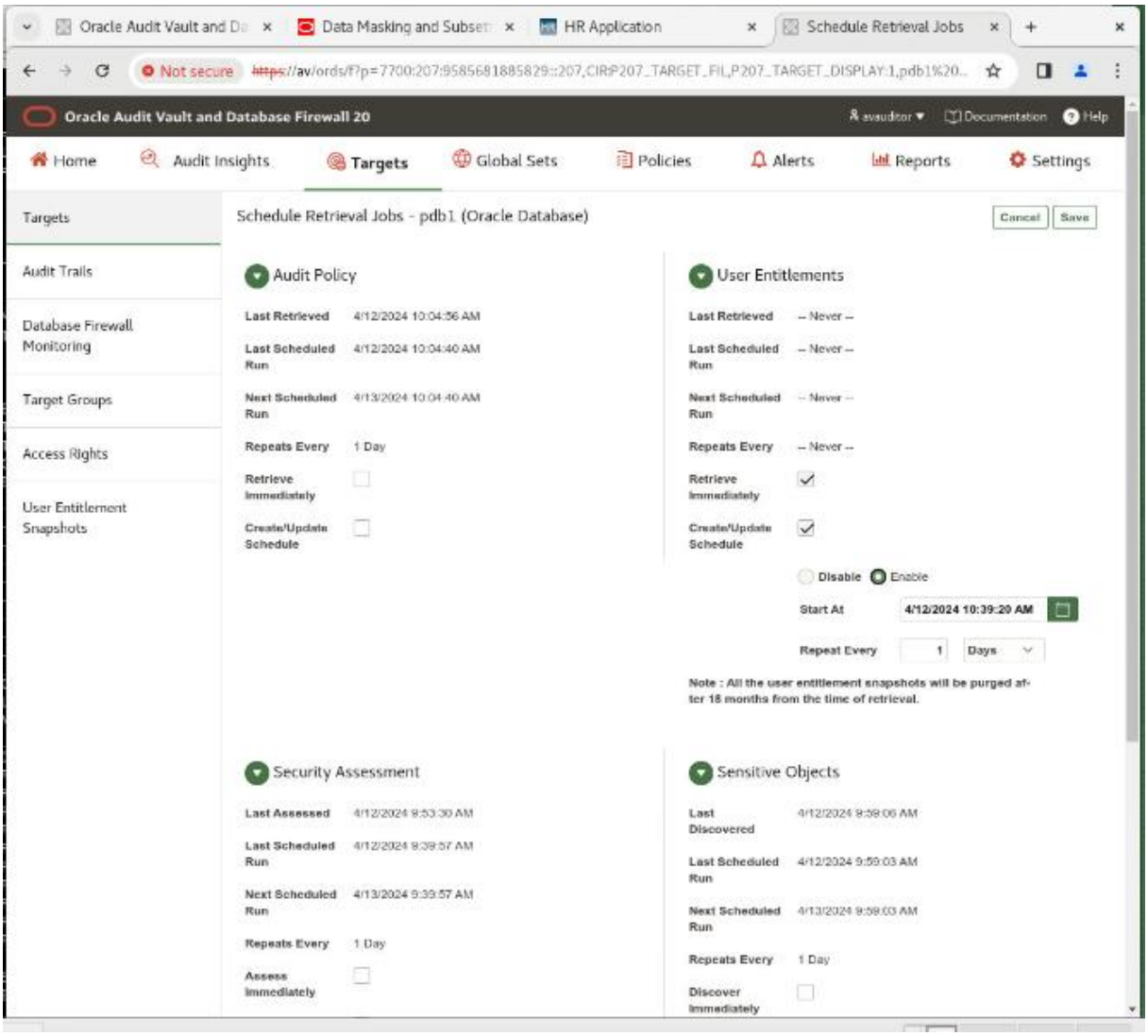


Kiểm tra các Unified Audit Policies sử dụng **SQL*Plus**

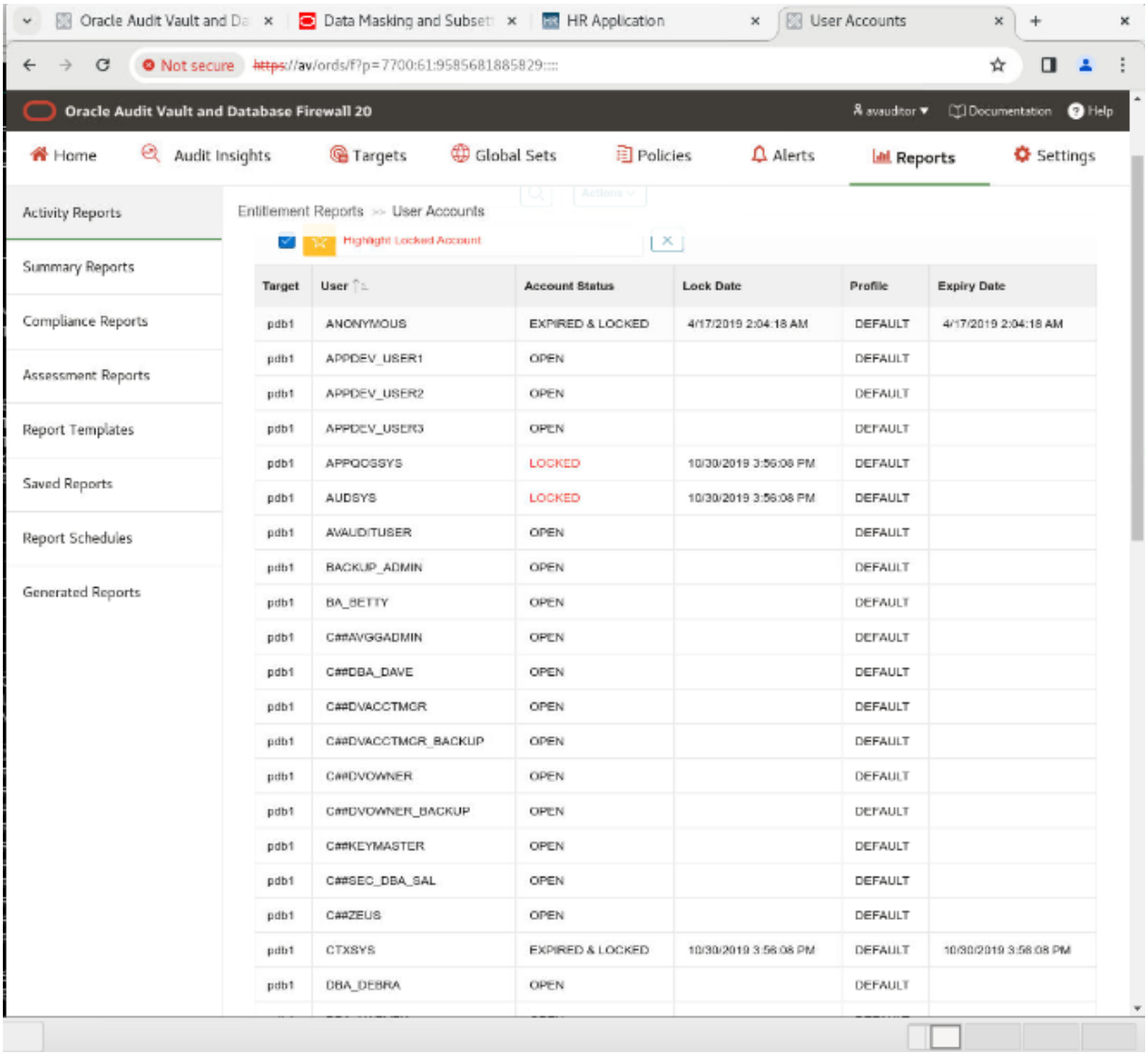


```
File  Edit  View  Search  Terminal  Help

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_query_enabled_unified_policies.sh

================================================================================
 List the ENABLED Unified Audit Policies in the pluggable database pdb1...
================================================================================

. List the enabled Unified Audit policies

POLICY_NAME                                ENABLED_OPTION  ENTITY_NAME                      ENTITY_TYPE  SUCCESS   FAILURE
------------------------------------------ --------------- -------------------------------- ------------ --------- ---------
PRIVILEGED_ACTIONS                         BY GRANTED ROLE DBA                              ROLE         YES       YES
ORA_SECURECONFIG                           BY USER         ALL USERS                        USER         YES       YES
ORA_RAS_SESSION_MGMT                       BY USER         ALL USERS                        USER         YES       YES
ORA_RAS_POLICY_MGMT                        BY USER         ALL USERS                        USER         YES       YES
ORA_LOGON_FAILURES                         BY USER         ALL USERS                        USER         YES       YES
ORA_DV_AUDPOL2                             BY USER         ALL USERS                        USER         YES       YES
ORA_DV_AUDPOL                              BY USER         ALL USERS                        USER         YES       YES
ORA_DATABASE_PARAMETER                     BY USER         ALL USERS                        USER         YES       YES
ORA_CIS_RECOMMENDATIONS                    BY USER         ALL USERS                        USER         YES       YES
ORA_AV$_SYS_TOP_ACTIVITY                   BY USER         SYS                              USER         YES       YES
ORA_AV$_DB_SCHEMA_CHANGES                  BY USER         ALL USERS                        USER         YES       YES
ORA_AV$_CRITICAL_DB_ACTIVITY               BY USER         ALL USERS                        USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE       ROLE         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE       ROLE         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE IMP_FULL_DATABASE                ROLE         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DBA                              ROLE         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSRAC                           USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSKM                            USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSDG                            USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSBACKUP                        USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         PUBLIC                           USER         YES       YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE EXP_FULL_DATABASE                ROLE         YES       YES
ORA_ADS$_SYS_TOP_ACTIVITY                  BY USER         SYS                              USER         YES       YES
ORA_ADS$_LOGON_FAILURES                    BY USER         ALL USERS                        USER         NO        YES
ORA_ADS$_LOGON_EVENTS                      BY USER         ALL USERS                        USER         YES       YES
ORA_ADS$_DB_SCHEMA_CHANGES                 BY USER         ALL USERS                        USER         YES       YES
ORA_ADS$_CRITICAL_DB_ACTIVITY              BY USER         ALL USERS                        USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY USER         SYSBACKUP                        USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY GRANTED ROLE DBA                              ROLE         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY USER         PUBLIC                           USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY USER         SYSDG                            USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE       ROLE         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE       ROLE         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY USER         SYSKM                            USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY USER         SYSRAC                           USER         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY GRANTED ROLE EXP_FULL_DATABASE                ROLE         YES       YES
ORA_ADS$_ADMIN_USER_ACTIVITY               BY GRANTED ROLE IMP_FULL_DATABASE                ROLE         YES       YES
ORA_ACCOUNT_MGMT                           BY USER         ALL USERS                        USER         YES       YES
EMPSEARCH_SELECT_USAGE_BY_PETE             BY USER         ALL USERS                        USER         YES       YES
APP_USER_NOT_APP_SERVER                    BY USER         ALL USERS                        USER         YES       YES
```

Kiểm tra các Unified Audit Policies đã được bật.



Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **User Entitlements** và enable. Nhấn Save



Trong tab Reports, ở phần **Entitlement Reports,** nhấn vào **User Accounts.** Ở phần label chọn Latest và chọn tất cả Target Name, sau khi nhấn Go ta sẽ có được danh sách user entitlement.