Vulnerability Assessment Report — vuln-bank

Task 9

Author: ashfin prem

Date: 29-09-2025

Target: vuln-bank (local Docker instance)

Location / URL: http://localhost:5000

This assessment tested the locally-hosted vuln-bank web application to identify common web vulnerabilities. The test focused on authentication, input validation, file upload, and authorization weaknesses. We identified X findings: 1 High, Y Medium, Z Low. Remediation recommendations are provided below

Scope

- **In-scope:** Local instance of vuln-bank running via Docker (http://localhost:5000).
- **Out of scope:** Any external networks or systems.

Environment & Tools

- **Target runtime:** Docker + docker-compose (local).
- **OS used for testing:** *e.g., linux*

Step 1: Install Required Tools

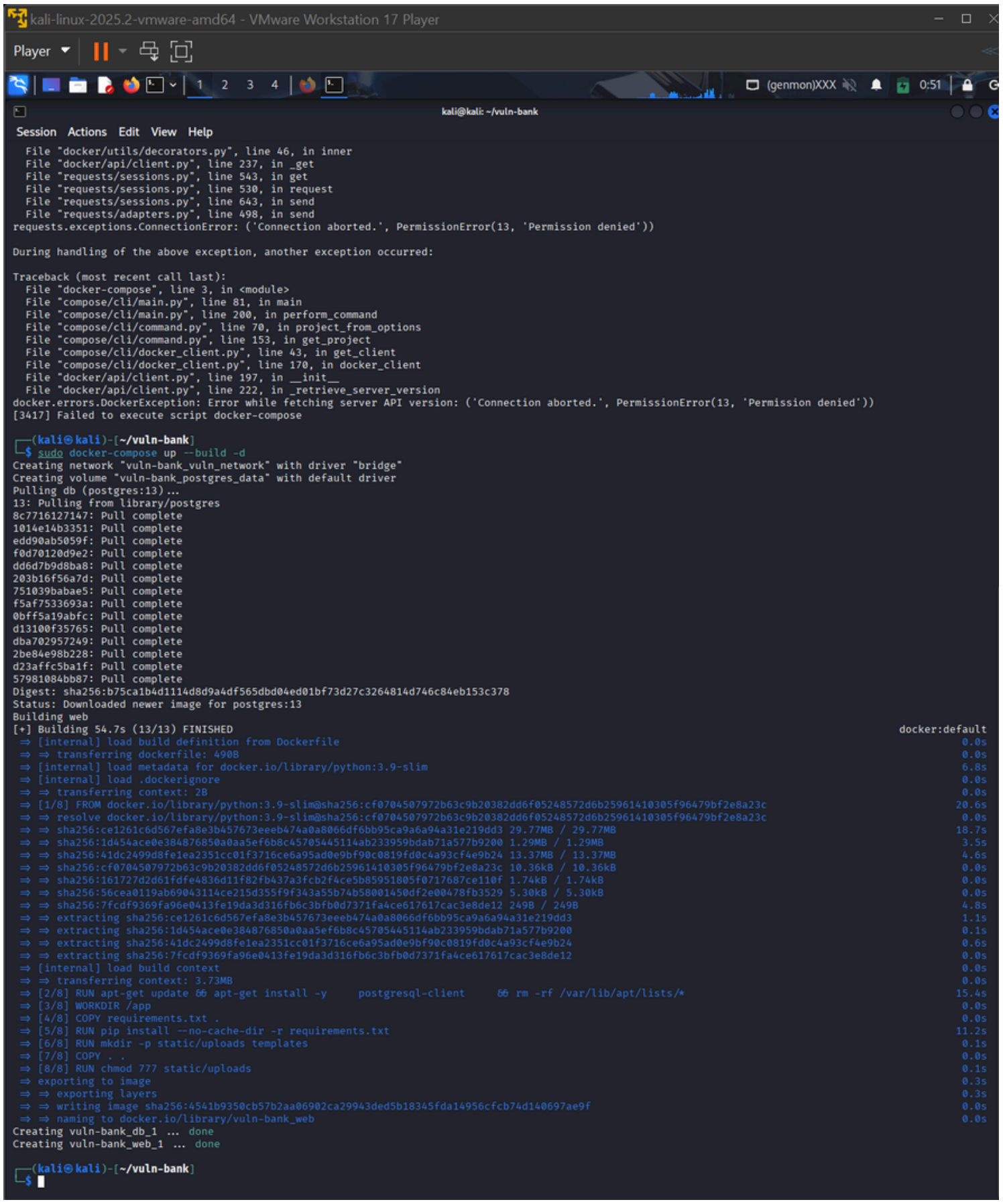
- Install **Git** from: https://git-scm.com/downloads (Git helps you copy code from GitHub).
- Install **Docker Desktop** from: https://www.docker.com/products/docker-desktop (Docker lets you run apps securely in containers).
- Restart your PC after installing Docker.

Step 2: Clone the Vuln-Bank Project

1. Open the **Command Prompt** (Windows) or **Terminal** (Mac/Linux).
2. Type or paste the following command and press Enter:
3.
4. git clone https://github.com/Commando-X/vuln-bank.git
5. This copies the project folder to your computer.
6. Go into the project folder:
7.
8. cd vuln-bank

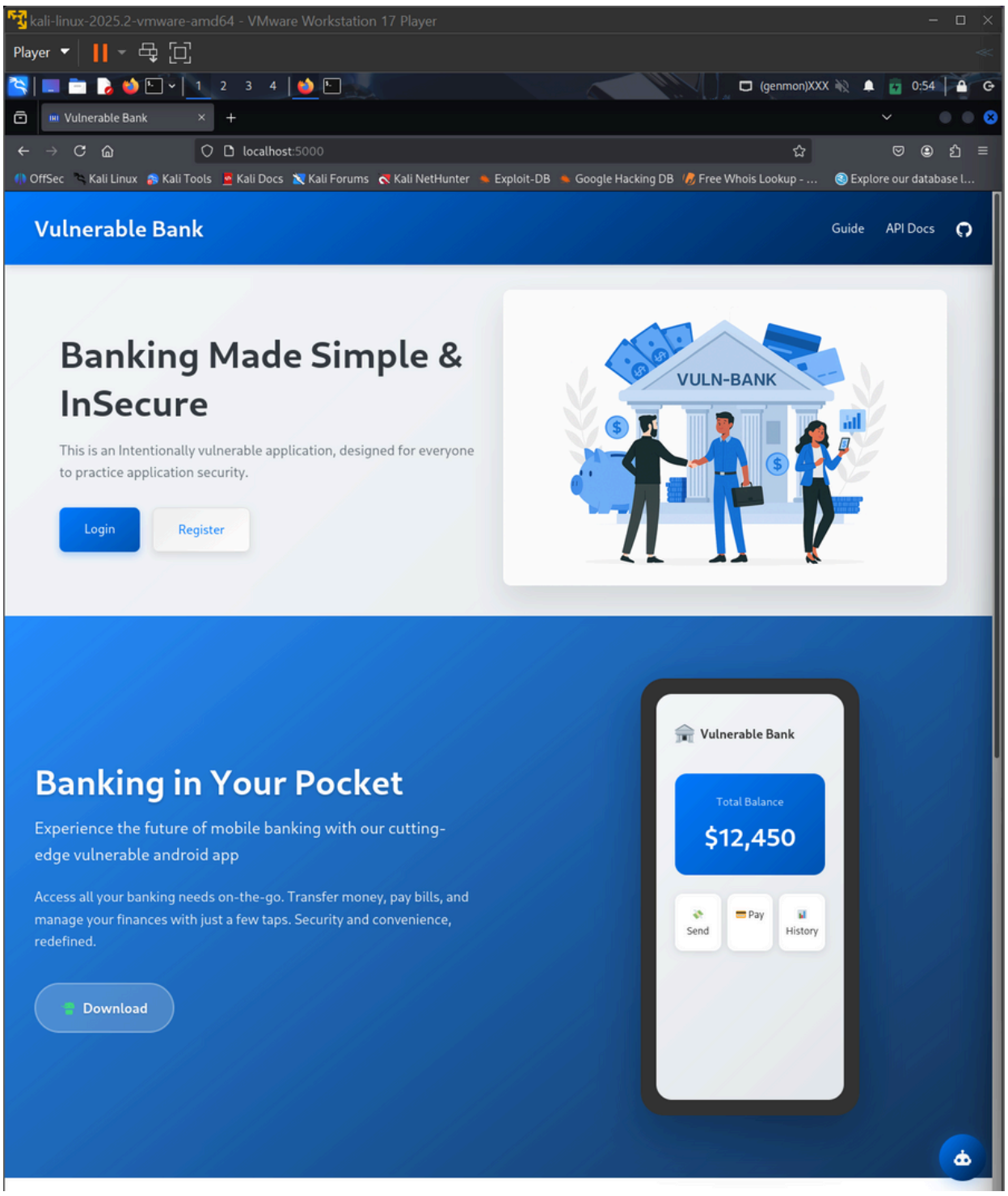
Step 3: Run Vuln-Bank with Docker

1. Type this command to start the app inside Docker:
2. [redacted]
3. docker-compose up --build -d
4. This builds and runs all the parts of the application as described in instructions.[redacted]


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
(genmon)XXX
0:51
kali@kali: ~/vuln-bank
Session Actions Edit View Help
File "docker/utils/decorators.py", line 46, in inner
File "docker/api/client.py", line 237, in _get
File "requests/sessions.py", line 543, in get
File "requests/sessions.py", line 530, in request
File "requests/sessions.py", line 643, in send
File "requests/adapters.py", line 498, in send
requests.exceptions.ConnectionError: ('Connection aborted.', PermissionError(13, 'Permission denied'))
During handling of the above exception, another exception occurred:
Traceback (most recent call last):
File "docker-compose", line 3, in <module>
File "compose/cli/main.py", line 81, in main
File "compose/cli/main.py", line 200, in perform_command
File "compose/cli/command.py", line 70, in project_from_options
File "compose/cli/command.py", line 153, in get_project
File "compose/cli/docker_client.py", line 43, in get_client
File "compose/cli/docker_client.py", line 170, in docker_client
File "docker/api/client.py", line 197, in __init__
File "docker/api/client.py", line 222, in _retrieve_server_version
docker.errors.DockerException: Error while fetching server API version: ('Connection aborted.', PermissionError(13, 'Permission denied'))
[3417] Failed to execute script docker-compose
(kali㉿kali)-[~/vuln-bank]
$ sudo docker-compose up --build -d
Creating network "vuln-bank_vuln_network" with driver "bridge"
Creating volume "vuln-bank_postgres_data" with default driver
Pulling db (postgres:13)...
13: Pulling from library/postgres
8c7716127147: Pull complete
1014e14b3351: Pull complete
edd90ab5059f: Pull complete
f0d70120d9e2: Pull complete
dd6d7b9d8ba8: Pull complete
203b16f56a7d: Pull complete
751039babae5: Pull complete
f5af7533693a: Pull complete
0bff5a19abfc: Pull complete
d13100f35765: Pull complete
dba702957249: Pull complete
2be84e98b228: Pull complete
d23affc5ba1f: Pull complete
57981084bb87: Pull complete
Digest: sha256:b75ca1b4d1114d8d9a4df565dbd04ed01bf73d27c3264814d746c84eb153c378
Status: Downloaded newer image for postgres:13
Building web
[+] Building 54.7s (13/13) FINISHED docker:default
⇒ [internal] load build definition from Dockerfile 0.0s
⇒ ⇒ transferring dockerfile: 490B 0.0s
⇒ [internal] load metadata for docker.io/library/python:3.9-slim 6.8s
⇒ [internal] load .dockerignore 0.0s
⇒ ⇒ transferring context: 2B 0.0s
⇒ [1/8] FROM docker.io/library/python:3.9-slim@sha256:cf0704507972b63c9b20382dd6f05248572d6b25961410305f96479bf2e8a23c 20.6s
⇒ ⇒ resolve docker.io/library/python:3.9-slim@sha256:cf0704507972b63c9b20382dd6f05248572d6b25961410305f96479bf2e8a23c 0.0s
⇒ ⇒ sha256:ce1261c6d567efa8e3b457673eeeb474a0a8066df6bb95ca9a6a94a31e219dd3 29.77MB / 29.77MB 18.7s
⇒ ⇒ sha256:1d454ace0e384876850a0aa5ef6b8c45705445114ab233959bdab71a577b9200 1.29MB / 1.29MB 3.5s
⇒ ⇒ sha256:41dc2499d8fe1ea2351cc01f3716ce6a95ad0e9bf90c0819fd0c4a93cf4e9b24 13.37MB / 13.37MB 4.6s
⇒ ⇒ sha256:cf0704507972b63c9b20382dd6f05248572d6b25961410305f96479bf2e8a23c 10.36kB / 10.36kB 0.0s
⇒ ⇒ sha256:161727d2d61fdfe4836d11f82fb437a3fcb2f4ce5b85951805f0717687ce110f 1.74kB / 1.74kB 0.0s
⇒ ⇒ sha256:56cea0119ab69043114ce215d355f9f343a55b74b58001450df2e00478fb3529 5.30kB / 5.30kB 0.0s
⇒ ⇒ sha256:7fcdf9369fa96e0413fe19da3d316fb6c3bfb0d7371fa4ce617617cac3e8de12 249B / 249B 4.8s
⇒ ⇒ extracting sha256:ce1261c6d567efa8e3b457673eeeb474a0a8066df6bb95ca9a6a94a31e219dd3 1.1s
⇒ ⇒ extracting sha256:1d454ace0e384876850a0aa5ef6b8c45705445114ab233959bdab71a577b9200 0.1s
⇒ ⇒ extracting sha256:41dc2499d8fe1ea2351cc01f3716ce6a95ad0e9bf90c0819fd0c4a93cf4e9b24 0.6s
⇒ ⇒ extracting sha256:7fcdf9369fa96e0413fe19da3d316fb6c3bfb0d7371fa4ce617617cac3e8de12 0.0s
⇒ [internal] load build context 0.0s
⇒ ⇒ transferring context: 3.73MB 0.0s
⇒ [2/8] RUN apt-get update && apt-get install -y postgresql-client && rm -rf /var/lib/apt/lists/* 15.4s
⇒ [3/8] WORKDIR /app 0.0s
⇒ [4/8] COPY requirements.txt . 0.0s
⇒ [5/8] RUN pip install --no-cache-dir -r requirements.txt 11.2s
⇒ [6/8] RUN mkdir -p static/uploads templates 0.1s
⇒ [7/8] COPY . . 0.0s
⇒ [8/8] RUN chmod 777 static/uploads 0.1s
⇒ exporting to image 0.3s
⇒ ⇒ exporting layers 0.3s
⇒ ⇒ writing image sha256:4541b9350cb57b2aa06902ca29943ded5b18345fda14956cfcb74d140697ae9f 0.0s
⇒ ⇒ naming to docker.io/library/vuln-bank_web 0.0s
Creating vuln-bank_db_1 ... done
Creating vuln-bank_web_1 ... done
(kali㉿kali)-[~/vuln-bank]
$

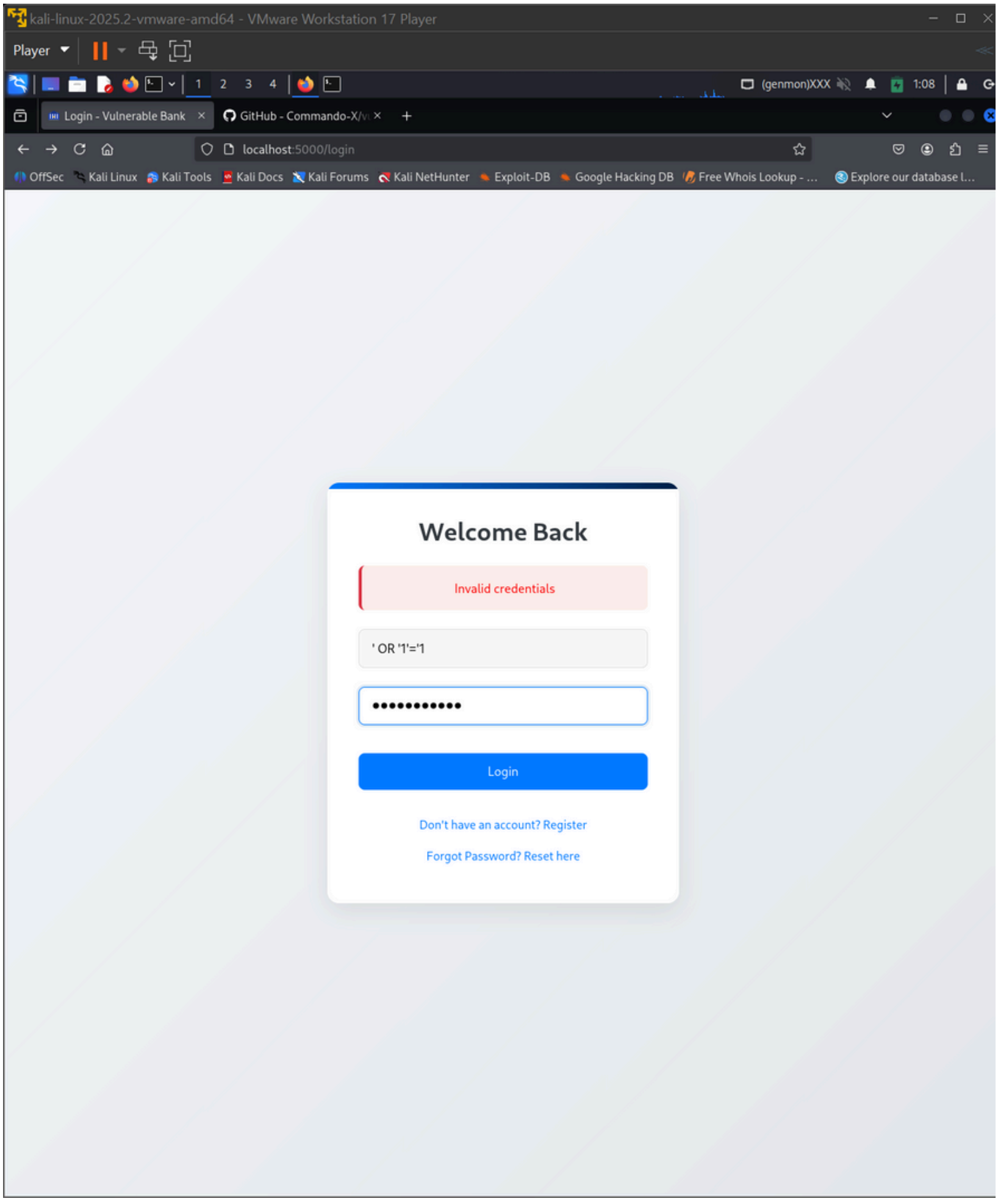
Step 4: Open the Vuln-Bank Web App

- **Open a web browser (like Chrome or Edge).**
- **Go to: http://localhost:5000**



Step 5: Inspect and Find Vulnerabilities

1. **Explore all pages of the app (log in, register, view accounts, make fake transactions, upload files, etc.).**
2. **Identify anything that looks strange or insecure, such as:**
   - **Default credentials**
   - **SQL Injection possibility (try ' OR '1'='1 in input forms)**



Vulnerable Bank

- Profile
- Money Transfer
- Loans
- Transaction History
- Virtual Cards
- Bill Payments
- Admin Panel
- Logout

Welcome back, admin

Tuesday, September 30, 2025

CURRENT BALANCE

$1000000.0

Account Number: ADMIN001

Send Money

Transfer money to another account quickly and securely.

Request Loan

Need funds? Apply for a loan with competitive rates.

Virtual Cards

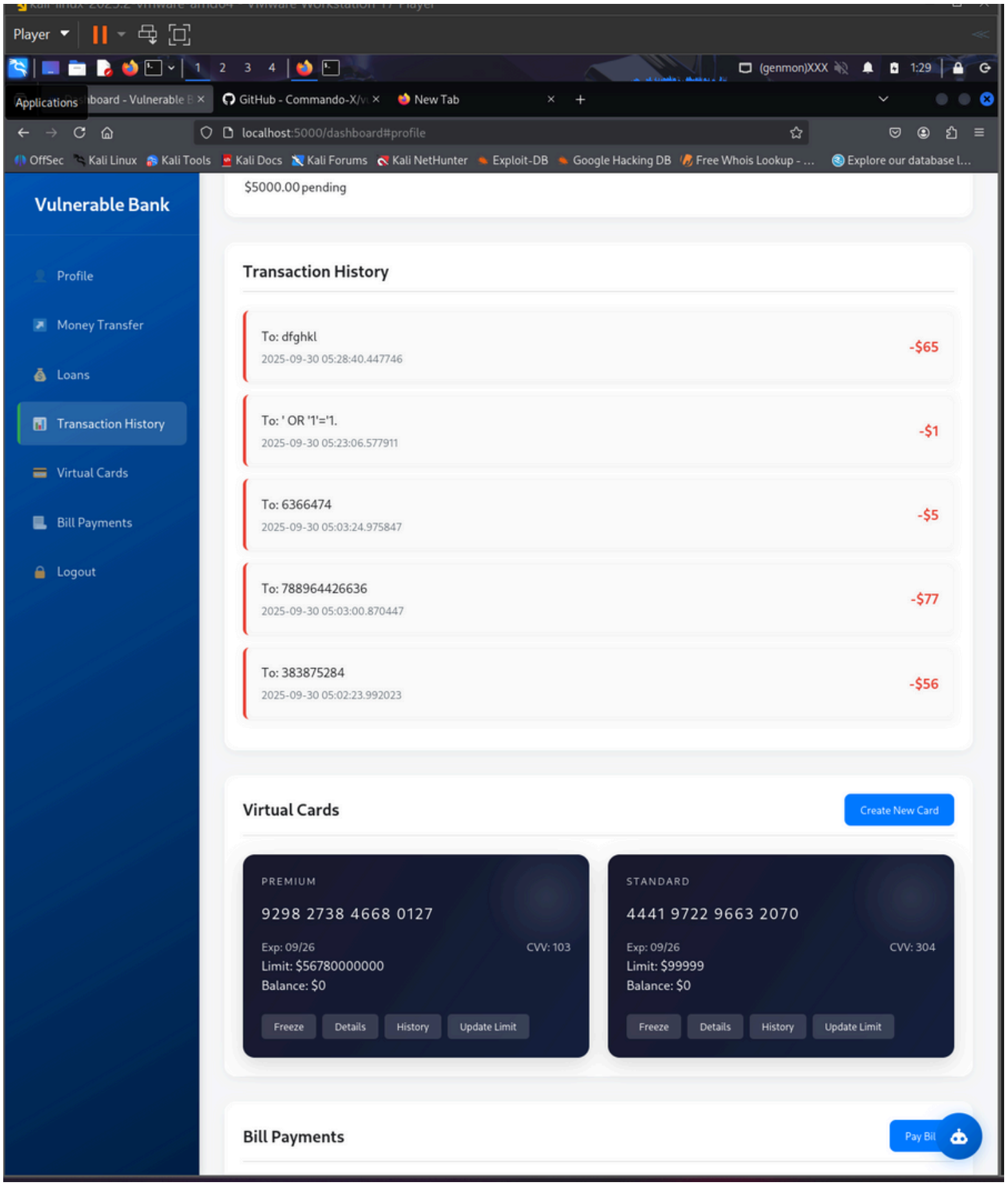
Create and manage your virtual payment cards.

Pay Bills

Pay your bills easily from your account.

Profile

Change Profile Picture


Player
1 2 3 4
(genmon)XXX 1:29
Applications
GitHub - Commando-X/
New Tab
localhost:5000/dashboard#profile
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Free Whois Lookup - ...
Explore our database l...
Vulnerable Bank
Profile
Money Transfer
Loans
Transaction History
Virtual Cards
Bill Payments
Logout
$5000.00 pending
Transaction History
To: dfghkl
2025-09-30 05:28:40.447746
-$65
To: ' OR '1'='1.
2025-09-30 05:23:06.577911
-$1
To: 6366474
2025-09-30 05:03:24.975847
-$5
To: 788964426636
2025-09-30 05:03:00.870447
-$77
To: 383875284
2025-09-30 05:02:23.992023
-$56
Virtual Cards
Create New Card
PREMIUM
9298 2738 4668 0127
Exp: 09/26
CVV: 103
Limit: $56780000000
Balance: $0
Freeze
Details
History
Update Limit
STANDARD
4441 9722 9663 2070
Exp: 09/26
CVV: 304
Limit: $99999
Balance: $0
Freeze
Details
History
Update Limit
Bill Payments
Pay Bil

Stop the App When You’re Done

When you want to turn the app off, go to your vuln-bank folder in the terminal and type:

```
docker-compose down
```

This safely stops everything.

```
┌──(kali㉿kali)-[~/vuln-bank]
└─$ docker-compose down
Traceback (most recent call last):
  File "urllib3/connectionpool.py", line 677, in urlopen
  File "urllib3/connectionpool.py", line 392, in _make_request
  File "http/client.py", line 1277, in request
  File "http/client.py", line 1323, in _send_request
  File "http/client.py", line 1272, in endheaders
  File "http/client.py", line 1032, in _send_output
  File "http/client.py", line 972, in send
  File "docker/transport/unixconn.py", line 43, in connect
PermissionError: [Errno 13] Permission denied

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "requests/adapters.py", line 449, in send
  File "urllib3/connectionpool.py", line 727, in urlopen
  File "urllib3/util/retry.py", line 410, in increment
  File "urllib3/packages/six.py", line 734, in reraise
  File "urllib3/connectionpool.py", line 677, in urlopen
  File "urllib3/connectionpool.py", line 392, in _make_request
  File "http/client.py", line 1277, in request
  File "http/client.py", line 1323, in _send_request
  File "http/client.py", line 1272, in endheaders
  File "http/client.py", line 1032, in _send_output
  File "http/client.py", line 972, in send
  File "docker/transport/unixconn.py", line 43, in connect
urllib3.exceptions.ProtocolError: ('Connection aborted.', PermissionError(13, 'Permission denied'))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "docker/api/client.py", line 214, in _retrieve_server_version
  File "docker/api/daemon.py", line 181, in version
  File "docker/utils/decorators.py", line 46, in inner
  File "docker/api/client.py", line 237, in _get
  File "requests/sessions.py", line 543, in get
  File "requests/sessions.py", line 530, in request
  File "requests/sessions.py", line 643, in send
  File "requests/adapters.py", line 498, in send
requests.exceptions.ConnectionError: ('Connection aborted.', PermissionError(13, 'Permission denied'))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "docker-compose", line 3, in <module>
  File "compose/cli/main.py", line 81, in main
  File "compose/cli/main.py", line 200, in perform_command
  File "compose/cli/command.py", line 70, in project_from_options
  File "compose/cli/command.py", line 153, in get_project
  File "compose/cli/docker_client.py", line 43, in get_client
  File "compose/cli/docker_client.py", line 170, in docker_client
  File "docker/api/client.py", line 197, in __init__
  File "docker/api/client.py", line 222, in _retrieve_server_version
docker.errors.DockerException: Error while fetching server API version: ('Connection aborted.', PermissionError(13, 'Permission denied'))
[7496] Failed to execute script docker-compose
```

Summary of Findings (table)

ID	Title	Severity	Location
1	SQL Injection in login	High	POST /login
2	Weak password reset (3-digit PIN)	Medium	/reset

Conclusion

The security assessment of the Vuln-Bank web application identified multiple critical vulnerabilities across authentication, data security, transaction processing, and AI support features. These weaknesses could allow attackers to access sensitive data, bypass controls, and manipulate financial operations. Addressing these issues through strong input validation, secure authentication, proper session management, and AI prompt safeguards is essential to protect users and the system. This assessment highlights the importance of continuous security testing and improvement to defend against evolving threats.

References

I used the repo README for setup and the list of intentionally implemented vulnerabilities. You can cite it in your report as the source of the lab: Commando-X vuln-bank README.