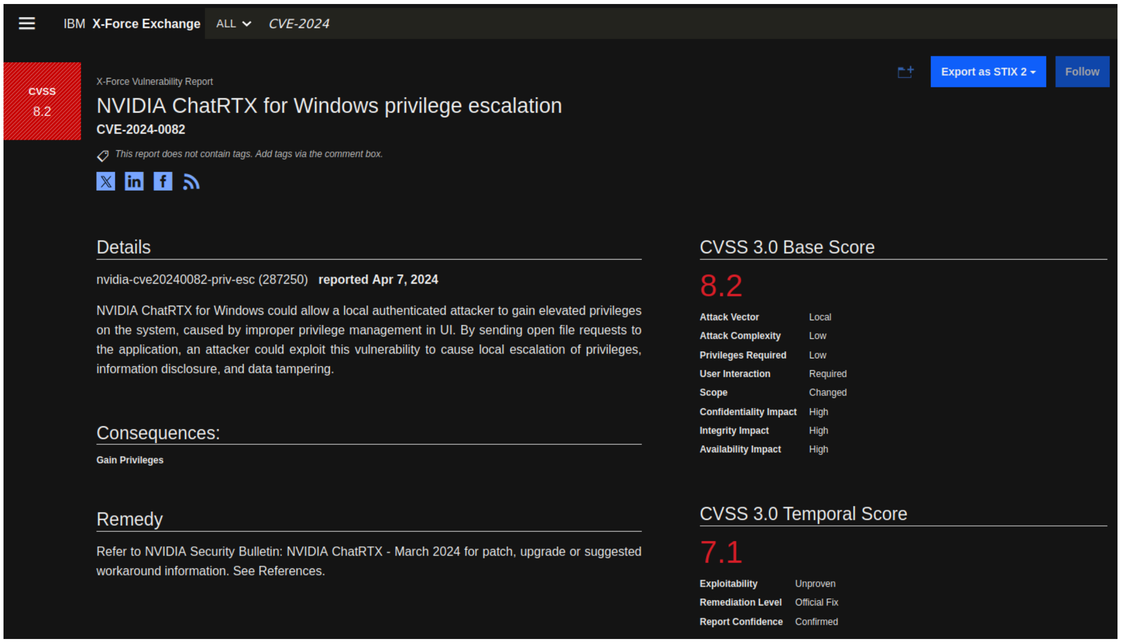
For this final project, I will demonstrate my ability to protect SecureBank from vulnerabilities and enhance its security posture.

Task 1/4: Identify a vulnerability using IBM XForce Exchange

Here is a recently identified vulnerability in the IBM X-Force Exchange CVE-2024-0082



X-Force Vulnerability Report

NVIDIA ChatRTX for Windows privilege escalation

CVE-2024-0082

This report does not contain tags. Add tags via the comment box.

Details

nvidia-cve20240082-priv-esc (287250) **reported Apr 7, 2024**

NVIDIA ChatRTX for Windows could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper privilege management in UI. By sending open file requests to the application, an attacker could exploit this vulnerability to cause local escalation of privileges, information disclosure, and data tampering.

Consequences:

Gain Privileges

Remedy

Refer to NVIDIA Security Bulletin: NVIDIA ChatRTX - March 2024 for patch, upgrade or suggested workaround information. See References.

CVSS 3.0 Base Score

8.2

Attack Vector	Local
Attack Complexity	Low
Privileges Required	Low
User Interaction	Required
Scope	Changed
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High

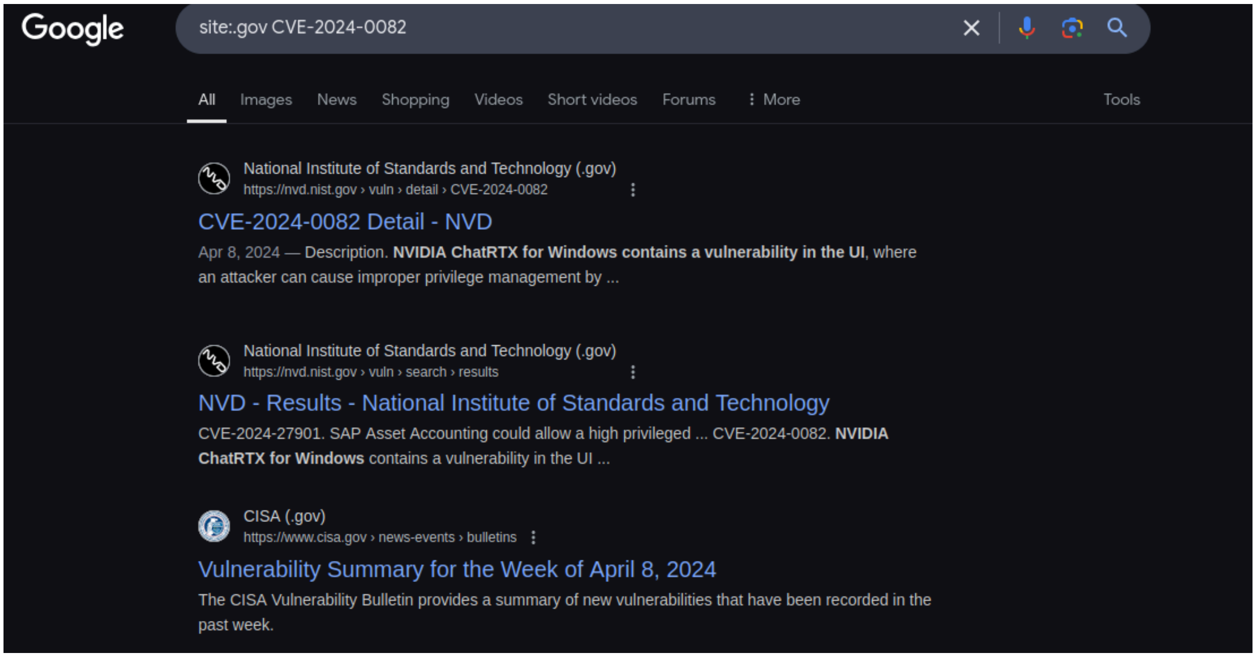
CVSS 3.0 Temporal Score

7.1

Exploitability	Unproven
Remediation Level	Official Fix
Report Confidence	Confirmed

Task 2/4: Investigate vulnerability using Google Dorking Commands

By using Google Dorking techniques I can quickly gather more information about this vulnerability such as using the search “site: CVE-2024-0082” to only find websites containing this information. However, I would prefer to only find government affiliated websites for more trusted information so I will further specify this search to “site:.gov CVE-2024-0082” to only show the websites with a .gov extension.



site:.gov CVE-2024-0082

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2024-0082

CVE-2024-0082 Detail - NVD

Apr 8, 2024 — Description. **NVIDIA ChatRTX for Windows contains a vulnerability in the UI**, where an attacker can cause improper privilege management by ...

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › search › results

NVD - Results - National Institute of Standards and Technology

CVE-2024-27901. SAP Asset Accounting could allow a high privileged ... CVE-2024-0082. **NVIDIA ChatRTX for Windows** contains a vulnerability in the UI ...

CISA (.gov)
https://www.cisa.gov › news-events › bulletins

Vulnerability Summary for the Week of April 8, 2024

The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded in the past week.

Task 3/4: Create a penetration testing plan following the given prompts

Prompt 1

Scenario: You are in a meeting with SecureBank's IT team to discuss the penetration test. The team includes the IT manager, the network administrator, and a security officer. They provide you with an overview of their infrastructure, which includes external web applications, internal databases, and a mix of on-premises and cloud-based services.

Question: What should you include in the scope?

Answer: Include all systems, networks, and applications.

Justification: When considering that SecureBank infrastructure includes external web applications, internal databases, and a mix of on-premises and cloud-based services it would be wise to include all systems, networks, and applications. It is more secure to have a comprehensive scope, as you don't want to create unintended vulnerabilities on unfocused aspects.

Prompt 2

Scenario: You are required to define the primary objectives of the penetration test. The IT team has expressed concerns about recent phishing attacks and regulatory compliance requirements

Question: Which objective should be prioritized for the penetration test based on the IT team's concerns?

Answer: Focus on compliance with industry standards.

Justification: As the IT team's expressed concern is about recent phishing attacks and regulatory compliance requirements, the correct answer is to focus on compliance with industry standards as they will likely also have the latest protections against phishing attacks. Wile identifying all possible vulnerabilities or testing incident response capabilities are important goals, they aren't the clearest path to our primary concern.

Prompt 3

Scenario: You have to establish the rules of engagement for the penetration test. However, the IT team is concerned about potential disruptions to business operations.

Question: What approach will you take to minimize disruptions while conducting the penetration test?

Correct answer: Notify staff that the test will be conducted after business hours.

Justification: When performing the penetration test after business hours, it will apply a minimum amount of potential disruptions when compared to the other options.

Prompt 4

Scenario: You begin the Discovery phase to gather information about the target systems. However, the IT team has provided you with limited information about their network topology.

Question: Which approach will be most effective for gathering information?

Correct answer: C: Use a combination of automated and manual techniques

Justification: Using a combination of automated tools (like Nmap and Nessus) and manual techniques will provide the most comprehensive and diverse amount of data.

Promt 5

Scenario: You have identified several vulnerabilities and are ready to exploit them. The vulnerabilities include an outdated web server, weak passwords, and an unpatched database.

Question: Which approach will you take to exploit the identified vulnerabilities?

Correct answer: B: Exploit the highest severity vulnerabilities first

Justification: Exploiting the highest severity vulnerabilities first is better as they are the most potentially damaging to your asset and organization.

Prompt 6

Scenario: You now have to compile your findings and provide recommendations. Your audience includes technical staff and the executive leadership.

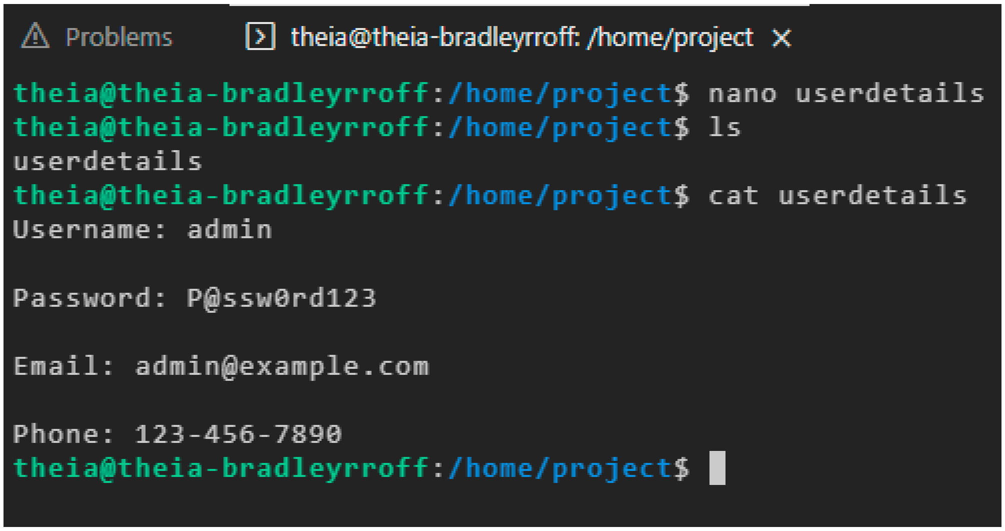
Question: What is the most effective way to present your findings?

Correct answer: C: Create a detailed technical report and an executive summary

Justification: It would be best to provide a detailed technical report and executive summary to please both parties. This would provide the technical data for the IT and offer an overview for decision makers.

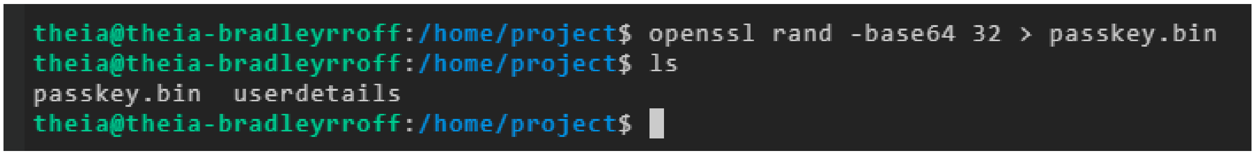
Task 4/4: Securing information using symmetric encryption

To begin I use the nano command to create a userdetails file containing an example admin account details for symmetric encryption.



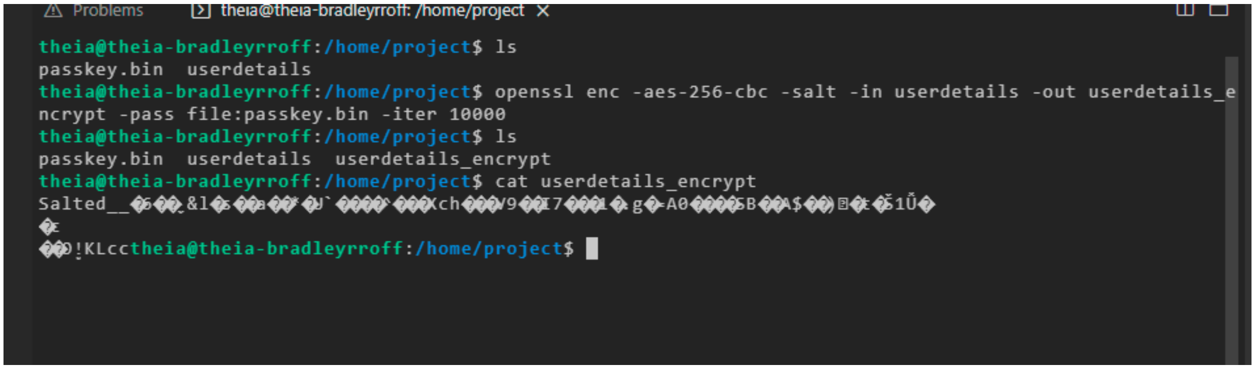
```
theia@theia-bradleyrroff:/home/project$ nano userdetails
theia@theia-bradleyrroff:/home/project$ ls
userdetails
theia@theia-bradleyrroff:/home/project$ cat userdetails
Username: admin

Password: P@ssw0rd123

Email: admin@example.com

Phone: 123-456-7890
theia@theia-bradleyrroff:/home/project$ 
```

Using openssl I create a random encryption key for AES encryption, storing it into the “passkey.bin” file.



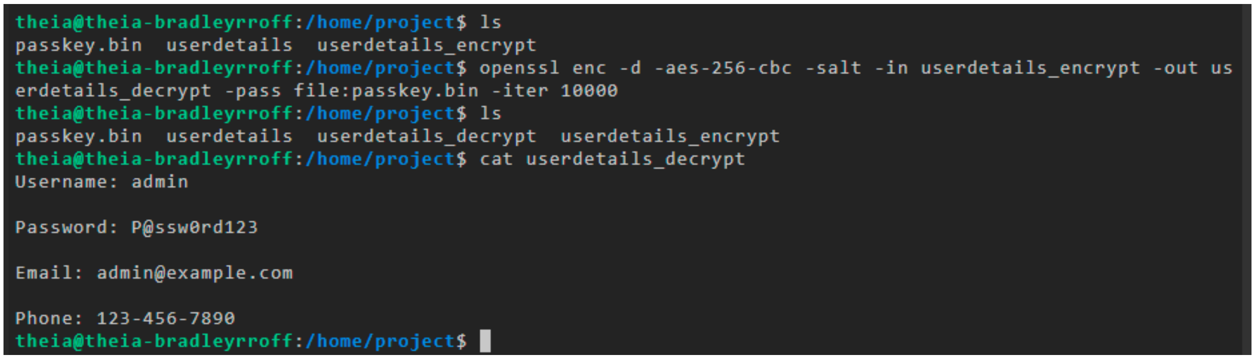
```
theia@theia-bradleyrroff:/home/project$ openssl rand -base64 32 > passkey.bin
theia@theia-bradleyrroff:/home/project$ ls
passkey.bin  userdetails
theia@theia-bradleyrroff:/home/project$ 
```

Using my generated AES key, I encrypt the contents of the “userdetails” file and save it into the encrypted file “userdetails_encrypt”. I then cat the encrypted file to check if the encryption was successful.



```
theia@theia-bradleyrroff:/home/project$ ls
passkey.bin  userdetails
theia@theia-bradleyrroff:/home/project$ openssl enc -aes-256-cbc -salt -in userdetails -out userdetails_e
ncrypt -pass file:passkey.bin -iter 10000
theia@theia-bradleyrroff:/home/project$ ls
passkey.bin  userdetails  userdetails_encrypt
theia@theia-bradleyrroff:/home/project$ cat userdetails_encrypt
Salted__�6��&l�s��a��*�J`����^���Xch���V9��I7���1�.g�-A0����5B��A$��)⊡�ε�5̆1Ů�
�ε
��D!KLcctheia@theia-bradleyrroff:/home/project$ 
```

I then decrypt the file using the private key and -d tag, saving it to userdetails_decrypt



```
theia@theia-bradleyrroff:/home/project$ ls
passkey.bin  userdetails  userdetails_encrypt
theia@theia-bradleyrroff:/home/project$ openssl enc -d -aes-256-cbc -salt -in userdetails_encrypt -out us
erdetails_decrypt -pass file:passkey.bin -iter 10000
theia@theia-bradleyrroff:/home/project$ ls
passkey.bin  userdetails  userdetails_decrypt  userdetails_encrypt
theia@theia-bradleyrroff:/home/project$ cat userdetails_decrypt
Username: admin

Password: P@ssw0rd123

Email: admin@example.com

Phone: 123-456-7890
theia@theia-bradleyrroff:/home/project$ 
```