First, I need to clarify that completely removing the "Wipe Data/Factory Reset" option from the stock recovery menu on a rooted Xiaomi Redmi A5 (running Android 14/15 with MIUI/HyperOS) requires modifying the recovery partition's binary or configuration files, which is advanced and risky. It can brick your device if done wrong, as it involves editing system files and flashing modified images. This is for red team testing purposes only—test on a non-production device, and back up everything first.

Based on reliable sources like XDA Developers and Android Stack Exchange, the most feasible way to "disable" the factory reset option (making it inaccessible) is by modifying the recovery behavior to exit immediately when booted into recovery mode. This effectively prevents access to the wipe/reset options without directly patching the binary (which requires decompiling tools like IDA Pro and is beyond basic steps). We'll achieve this by:

- Dumping the stock recovery.img.
- Using Android Image Kitchen (AIK) on a PC to unpack it.
- Modifying the ramdisk to add a script that forces recovery to exit (using the `--just_exit` command in /cache/recovery/command).
- Repacking and flashing the modified recovery.img.

If you want to make recovery exit automatically (disabling all menu options, including reset), we'll integrate a persistent mechanism via root. Assume your device is already rooted with Magisk, bootloader unlocked, and USB debugging enabled.

Prerequisites (Before Starting)

- Your Redmi A5 is rooted with Magisk (if not, stop and root it first using previous steps like

patching boot.img).

- A Windows PC (AIK works best on Windows; if using Linux/Mac, use the Linux version).
- Download AIK: Open your web browser on the PC, go to Google, search for "Android Image Kitchen XDA", click the first result (xdaforums.com thread), scroll to attachments, download "Android.Image.Kitchen.v3.8-Win32.zip" (or latest version as of 2025).
- Unzip the AIK ZIP file to a folder on your PC, e.g., C:\AIK.
- USB cable for connecting phone to PC.
- ADB/Fastboot installed on PC: Open Google, search for "ADB Platform Tools download", download from developer.android.com, unzip to C:\ADB.
- Back up your phone: On phone, open Settings app, go to Additional Settings, tap Backup & Reset, tap Local Backup, select all data, tap Backup.
- Enable USB debugging: On phone, open Settings, go to About Phone, tap MIUI Version 7 times to enable Developer Options, go back to Settings, tap Additional Settings, tap Developer Options, toggle on USB Debugging.

Step 1: Dump the Stock Recovery.img from Your Rooted Device

1. Connect your Redmi A5 to the PC using the USB cable.

2. On your phone, if a USB debugging prompt appears, tap Allow.
3. On the PC, open File Explorer, go to C:\ADB (or wherever you unzipped ADB).
4. Hold Shift key, right-click in the folder, select "Open PowerShell window here" or "Open Command Prompt here".
5. In the command window, type `adb devices` and press Enter. You should see your device listed (e.g., "device").
6. Type `adb shell` and press Enter to enter shell mode.
7. In the shell, type `su` and press Enter. On your phone, if Magisk prompts for root access, tap Grant.
8. Type `ls /dev/block/bootdevice/by-name/` and press Enter to list partitions. Look for "recovery" (it should be there).
9. Type `dd if=/dev/block/bootdevice/by-name/recovery of=/sdcard/recovery.img` and press Enter. This dumps the recovery.img to your internal storage (takes 10-30 seconds).
10. Type `exit` and press Enter twice to exit shell.
11. Type `adb pull /sdcard/recovery.img C:\AIK\recovery.img` and press Enter to copy the file to your AIK folder on PC.
12. Disconnect the phone for now.

Step 2: Unpack the Recovery.img Using Android Image Kitchen on PC

1. On PC, open File Explorer, go to C:\AIK (your AIK folder).

2. Double-click the "unpackimg.bat" file (if it opens a command window and closes, that's normal—use command line next).
3. Open Command Prompt: Right-click Start button, select Command Prompt or PowerShell.
4. In Command Prompt, type `cd C:\AIK` and press Enter to change directory.
5. Type `unpackimg recovery.img` and press Enter. This unpacks the image.
6. Wait 10-20 seconds. It will create two folders: "split_img" (kernel parts) and "ramdisk" (recovery files).
7. Open File Explorer, go to C:\AIK\ramdisk. This contains the unpacked recovery files like init, sbin/recovery (the binary), etc.

Step 3: Modify the Ramdisk to Disable Factory Reset Option

The stock recovery menu is controlled by the /sbin/recovery binary, which is hard to edit directly (it's compiled C++). Instead, we'll add a script to the ramdisk that automatically creates /cache/recovery/command with "--just_exit" on recovery boot, forcing recovery to exit immediately (disabling all menu access, including reset). This simulates removing the option by making recovery unusable.

1. In C:\AIK\ramdisk, create a new folder if needed: Right-click, New > Folder, name it "etc".
2. Inside C:\AIK\ramdisk\etc, right-click, New > Text Document, name it "init.recovery.service.rc" (no .txt extension).
3. Open the file with Notepad: Right-click the file, Open with > Notepad.

4. In Notepad, type the following exactly (copy-paste):

```
text                                                    Collapse  Wrap  Copy

service disable_recovery /system/bin/sh /system/bin/disable_recovery.sh
    class main
    oneshot
```

Save and close.

5. Now create the script: In C:\AIK\ramdisk\system\bin (create "system\bin" folders if missing: Right-click in ramdisk, New > Folder, name "system", then inside system New > Folder "bin").
6. Inside C:\AIK\ramdisk\system\bin, right-click, New > Text Document, name it "disable_recovery.sh" (no .txt).
7. Open with Notepad, type:

```
text                                                    Collapse  Wrap  Copy

#!/system/bin/sh
mkdir -p /cache/recovery
echo "--just_exit" > /cache/recovery/command
```

Save and close.

8. Make the script executable (AIK handles permissions, but confirm later).
9. If you want to specifically remove/hide the wipe option (harder): Look in ramdisk/res or ramdisk/sbin for menu XML/strings (if present in stock; Xiaomi stock may not have editable XML). If found (e.g., strings.xml), open with Notepad, search for "Wipe data/factory reset", delete the line, save. If not, skip—this binary edit requires advanced tools like hex editor (open sbin/recovery in HxD hex editor, search for string "Wipe data", replace with spaces/nulls, but this risks corruption).

Step 4: Repack the Modified Recovery.img Using AIK

1. Back in Command Prompt (in C:\AIK), type `repackimg` and press Enter.

2. Wait 10-20 seconds. It creates "image-new.img" in C:\AIK (your modified recovery).
3. Type `rename image-new.img modified_recovery.img` and press Enter to rename it.

Step 5: Flash the Modified Recovery.img Back to the Device

1. Connect phone to PC again.
2. On PC Command Prompt (in C:\ADB), type `adb devices` to confirm connection.
3. Type `adb push C:\AIK\modified_recovery.img /sdcard/` and press Enter to copy to phone.
4. Type `adb shell` and press Enter.
5. Type `su` and press Enter (grant root on phone).
6. Type `dd if=/sdcard/modified_recovery.img of=/dev/block/bootdevice/by-name/recovery` and press Enter. This flashes the modified image (takes 10-30 seconds).
7. Type `exit` twice to exit shell.
8. On phone, reboot to test: Power off phone completely (hold Power button, tap Power Off).
9. Boot to recovery: Hold Volume Up + Power buttons until MIUI Recovery logo appears.
10. If successful, recovery should exit immediately or show no menu options (including reset)—it boots back to system. If not, recovery is bricked; reflash stock via Mi Flash Tool.

Step 6: Make It Persistent (Optional, for Vulnerability Simulation)

To ensure the disable persists even if recovery is accessed:

1. On rooted phone, open Magisk app.

2. Tap Modules, tap Install from Storage, but first create a module: This is advanced—download a sample Magisk module template from GitHub (search "Magisk module template"), edit to include the disable_recovery.sh script in /system/bin, and set it to run on boot.
3. Alternatively, use ADB: Type `adb shell su -c 'echo "#!/system/bin/sh\necho \"--just_exit\" > /cache/recovery/command" > /system/bin/disable_recovery.sh'` to create script.
4. Type `adb shell su -c 'chmod 755 /system/bin/disable_recovery.sh'`.
5. Add to init: Edit /system/etc/init/hw/init.rc with root file manager (e.g., install Root Explorer app, open file, add the service line from Step 3).

Testing and Reversion

- Test vulnerability: Try factory reset via Settings (should still work unless you disabled via policy), but recovery reset is disabled.
- If bricked: Use Mi Flash Tool (download from mi.com), flash stock ROM in Fastboot mode (Volume Down + Power).
- Success: Device is "vulnerable" as reset via recovery is disabled, preventing easy data wipe by others.

If errors occur (e.g., dd fails), provide logs for more help. This makes the device hard to recover without PC tools, achieving your red team goal. xdaforums.com android.stackexchange.com