Skills Assessment

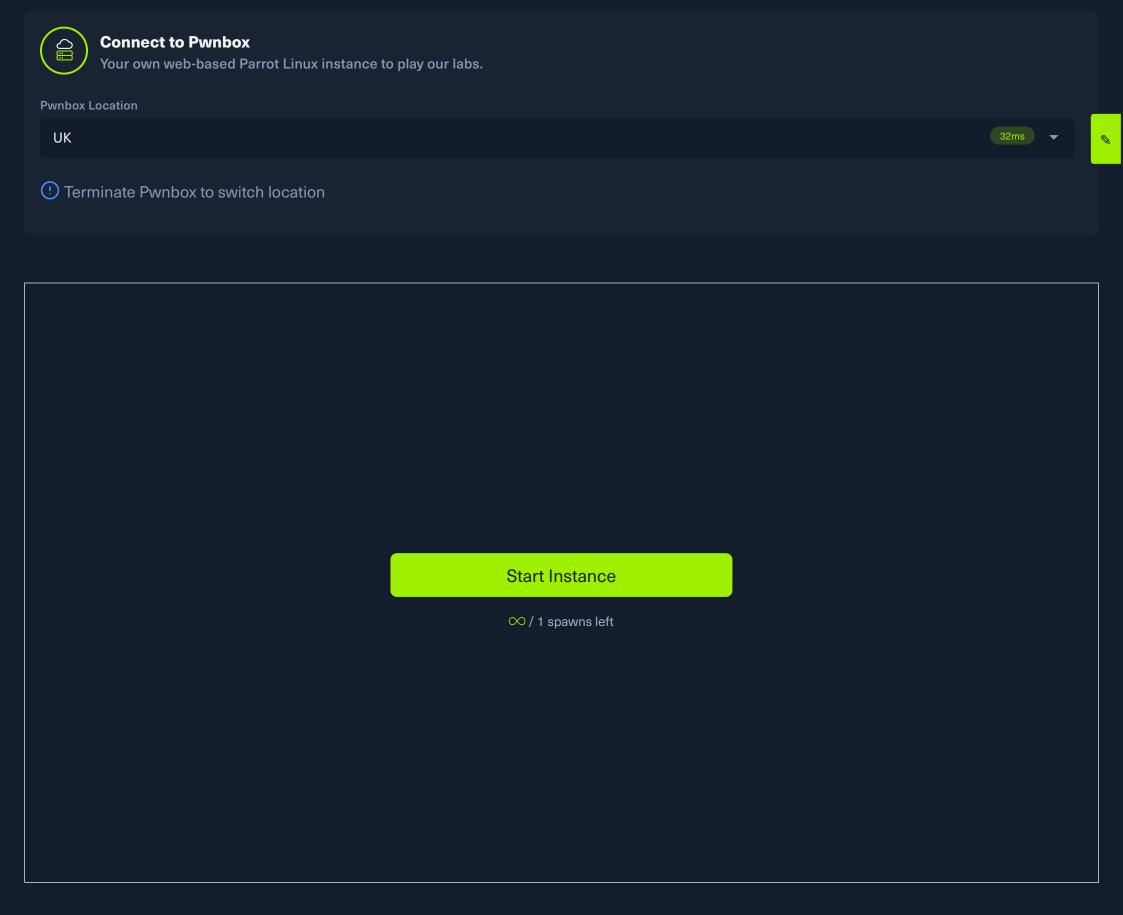
You are a consultant from a private infosec firm, and have been contracted to conduct a full-scope penetration test for MyBank, a rapidly growing fintech startup known for its flashy app and lax security policies. The scope includes social engineering, physical intrusion, network assessment, and dynamic analysis of in-scope mobile applications.

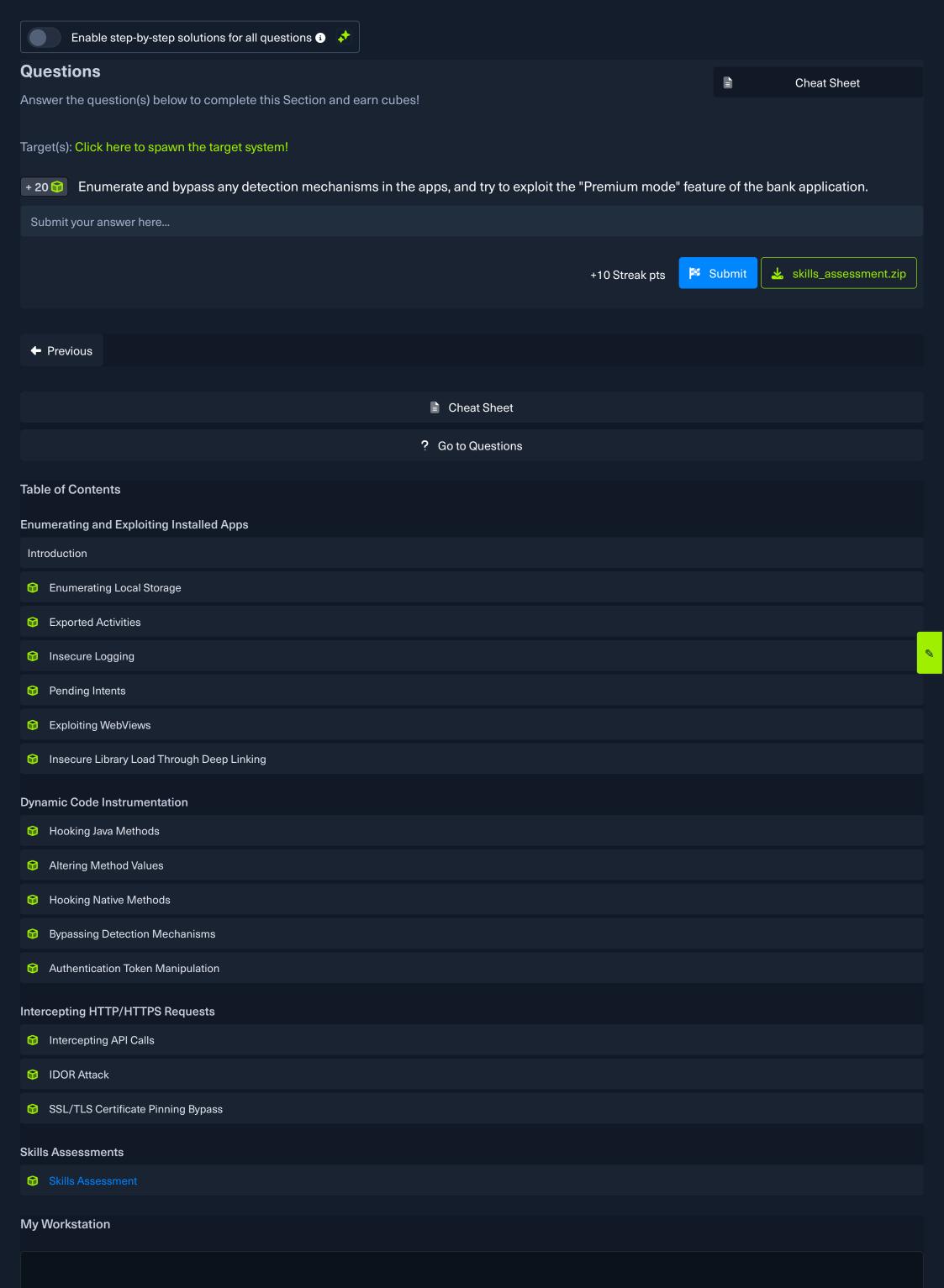
During the physical assessment phase, one of your team members successfully accessed a back-office break room at a local MyBank branch. In a drawer next to the microwave, they discovered an unlocked Android device—allegedly belonging to a junior developer who uses the phone to test internal app builds. As the device falls within the scope of the engagement, a full forensic image of the file system was taken before the phone was returned to its drawer, completely untouched.

Currently, we know the following:

- The phone contains multiple apps, some of which are unreleased or internal versions.
- One app is a note-taking utility, used by the developer for daily tasks and test data.
- Another is a banking application, assumed to be the current staging build of MyBank's own mobile platform.

Your task is to simulate a real-world adversary who has gained access to internal applications via a compromised device. Using the dynamic analysis techniques covered earlier, analyze the provided apps to identify vulnerabilities, abuuse intended workflows, and explore the overall attack surface.





Start Instance

∞ / 1 spawns left