SUBMITTED BY: IQRA JAWAD AHMAD

TASK: COOKIE SESSION HIJACKING

1. Scope and Objective

The test was limited to:

- Accessing the user's Duolingo account via a valid session cookie.
- Observing available account features after cookie-based login.
- Documenting steps taken for educational and mitigation purposes.

No changes were made to the account, no personal data was downloaded, and no third-party accounts were targeted.

2. Methodology

The following methodology was used during the test:

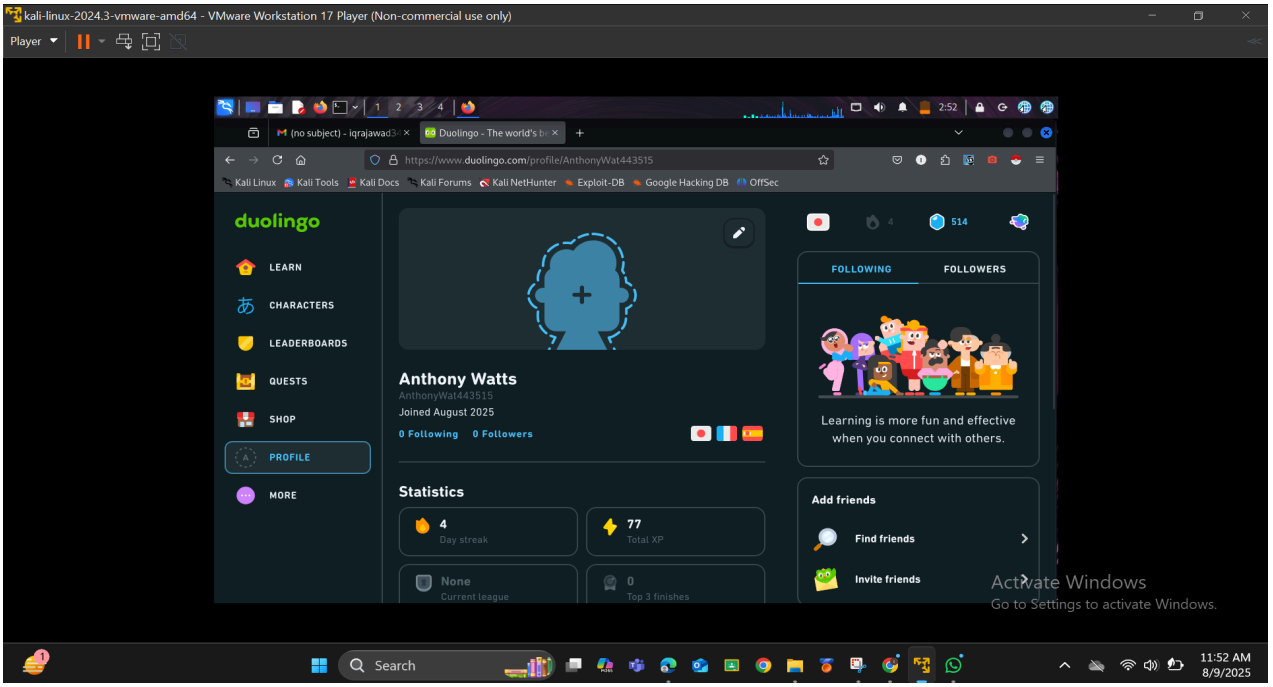
1. **Session Cookie Acquisition**
   I got the valid session cookie for Duolingo from the EduTecHack website.
2. **Testing Environment**
   - **Operating System:** Kali Linux 2024.3 (VMware Workstation 17 Player)
   - **Browser:** Firefox (with Cookie-Editor extension)
3. **Session Injection Process**
   - The existing cookies in Firefox for `duolingo.com` were deleted.
   - The provided session cookie was imported using Cookie-Editor.
   - The Duolingo site was refreshed.
4. **Result**
   The browser was logged in to the user account without entering any credentials, confirming that the session cookie alone was sufficient for account access.

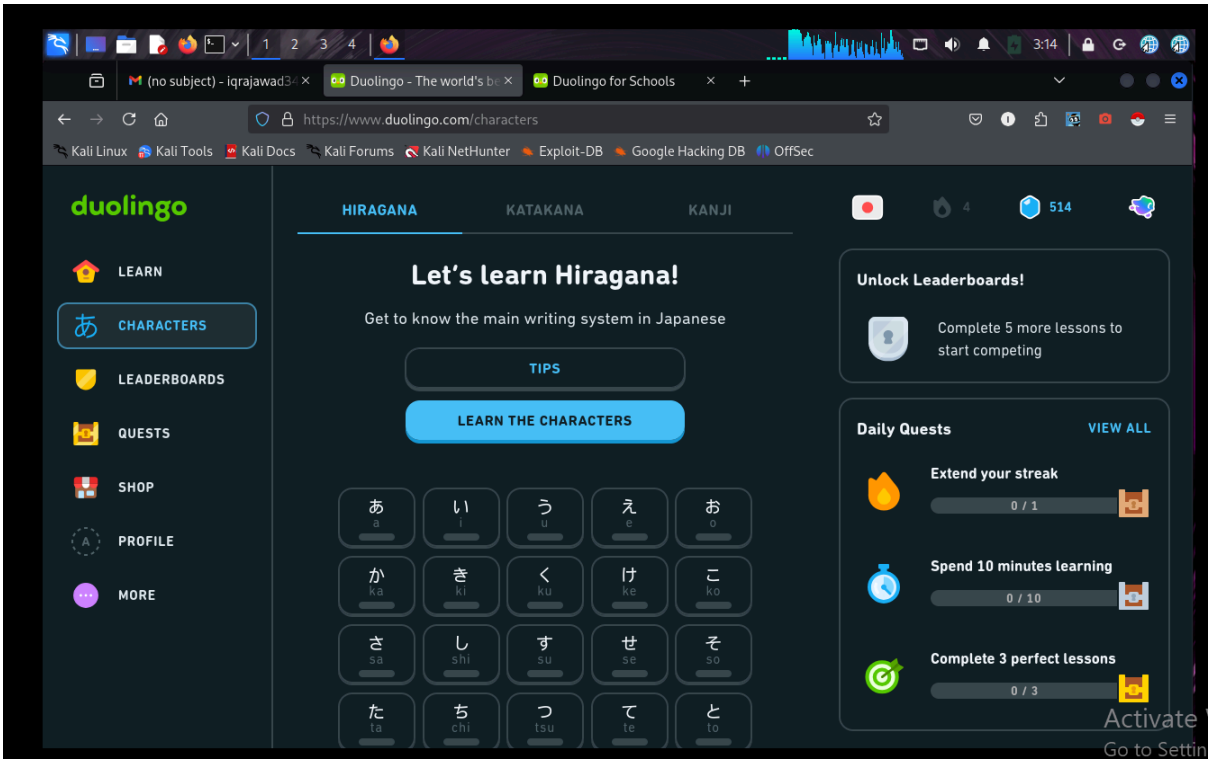
3. Findings

- **Vulnerability:** Session hijacking via a valid session cookie.
- **Impact:** Any attacker with access to an unexpired session cookie could bypass the login process entirely, impersonating the user.
- **Risk Level:** Sensitive user data and account control can be compromised.

4. Evidence

A screenshot from the test environment shows the Duolingo profile of the account owner accessed solely using the imported session cookie.
Duolingo profile after successful session cookie injection.





5. Recommendations

To mitigate session hijacking risks, the following measures are advised:

1. **Use Secure & HttpOnly Flags:** Ensure cookies are transmitted only over HTTPS and are inaccessible to JavaScript.

2. **Implement Short Session Lifetimes:** Invalidate session cookies after a short idle time.

3. **Revalidate on Sensitive Actions:** Require password re-entry or 2FA for sensitive operations.

4. **Enable IP & Device Binding:** Tie sessions to the user's IP/device and flag anomalies.

5. **Educate Users:** Encourage logging out from public/shared devices and avoiding insecure networks.

6. Conclusion

This controlled demonstration showed that with a valid session cookie, it is possible to bypass authentication on Duolingo. Real-world attackers could exploit such vulnerabilities to compromise user accounts. The platform should implement stricter session management and security policies to safeguard against such threats.