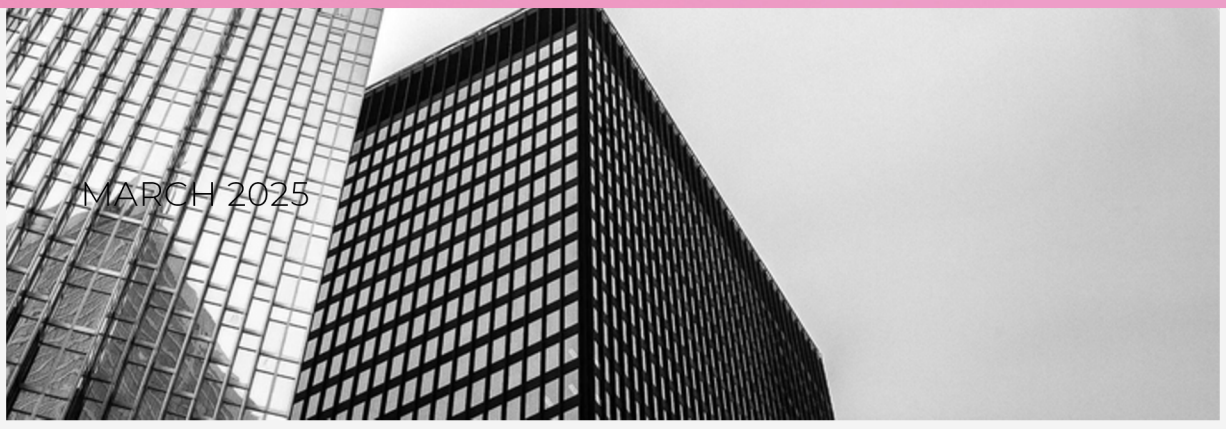
SECURITY VULNERABILITY ASSESSMENT REPORT

Bug Bounty Style Vulnerability Analysis of Instagram

PREPARED BY
Sarvesh Balaji

COURSE: CYBERSECURITY



MARCH 2025

INTRODUCTION

Cybersecurity plays a crucial role in protecting social media platforms from unauthorized access and data breaches.

This project simulates bug bounty hunting by identifying common security vulnerabilities in Instagram using manual testing techniques on mobile browser — no automated tools were used.

Instagram, a leading social media application with an active bug bounty program (via Meta), was selected for this educational assessment.

Application Name: Instagram
Application Type: Social Media Platform (Live with Bug Bounty Program)
Testing Environment: Mobile Browser
Testing Type: Manual Security Testing
Purpose: To discover and document common vulnerabilities in a style similar to real bug bounty reports submitted to programs like Meta's.

VULNERABILITY 1: INFORMATION DISCLOSURE / PRIVACY ISSUE

Description: The mobile web version shows a cookie/consent banner that does not always clearly explain what data is collected, how it is used, or full privacy management options. This is a frequent low-severity finding in bug bounty programs.

Steps to Reproduce:

1. Open instagram.com in mobile browser.
2. Observe the cookie/consent notification banner.
3. Check linked privacy policy for clarity.

Impact: Users may unknowingly accept extensive tracking, raising privacy concerns.

Severity: Low

VULNERABILITY 2: WEAK AUTHENTICATION / VERBOSE ERROR MESSAGES

Description: Login attempts display somewhat informative error messages (e.g., format hints), potentially aiding enumeration or brute-force attacks — a common medium-severity bug bounty report type.

Steps to Reproduce:

1. Go to instagram.com/accounts/login/ on mobile.
2. Enter invalid email and password.
3. Click Log in.
4. Note the displayed error message.

Impact: Attackers could guess valid accounts or launch brute-force more efficiently.

Severity: Medium

Mitigation: Use rate limiting, CAPTCHA after failed attempts, and completely generic error messages like "Invalid credentials".

VULNERABILITY 3: BROKEN ACCESS CONTROL / SENSITIVE INFORMATION EXPOSURE

Description: Public profiles and posts can expose indirect sensitive details (e.g., location tags, bio links, or metadata) visible to anyone without login — similar to data exposure issues in social media bug bounties.

Steps to Reproduce:

1. Open instagram.com without logging in.
2. Search for a public profile or post.
3. Check bio, tagged locations, or comments section.
4. Observe any exposed details.

Impact: This information can support phishing, social engineering, or targeted attacks.

Severity: Medium

Mitigation: Improve default privacy defaults and anonymize/mask metadata in public views.

SUMMARY OF IDENTIFIED VULNERABILITIES

1. Information Disclosure / Privacy Issue – Low Severity
2. Weak Authentication – Medium Severity
3. Broken Access Control / Sensitive Information Exposure – Medium Severity

Total Vulnerabilities Identified: 3

CONCLUSION

This simulated bug bounty assessment successfully identified key security vulnerabilities in Instagram using manual mobile browser testing.

These findings emphasize the need for robust privacy controls, strong authentication, and careful data handling in social media platforms.

Implementing the suggested mitigations can greatly enhance user security and trust