Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Security Logging and Monitoring Failures

Bug Bounty Report- 08

IT23363366

TABLE OF CONTENT

Title 3

Scope & Objective 3

Enumeration and Reconnaissance 3

- Tools Used 3
- Steps Taken 3

Vulnerability Description 3

Affected Components 4

Impact Assessme 4

Proof of Concept (PoC) 4

- Check for Login and Error Handling 4
- Password Reset Handling 5
- Registration with Existing Email 6
- Monitoring and Alerting Mechanisms Review 7

Proposed Mitigation 8

Conclusion 9

References 9

1. Title

Report Title: Security Logging and Monitoring Failures
Reported By: Raahim Mahmooth
Platform: https://hackerone.com/
Tested on: Drawify.com

2. Scope & Objective

The goal of this report is to analyze the security logging and monitoring mechanisms of ***Drawify's*** web application, focusing on critical security events such as login attempts, failed logins, and password resets. The objective is to identify vulnerabilities related to insufficient logging, detection, monitoring, and response mechanisms that could lead to undetected breaches.

3. Enumeration and Reconnaissance

3.1 Tools Used

- Manual check, spying invalid credentials on critical systems.
- Burp Suite.

3.2 Steps Taken

3.2.1 Check if critical events are being logged:

Due to **a lack of access to developer or admin tools**, I am unable to verify whether critical events such as login failures or password reset attempts are logged properly.

3.2.2 Check for Login and Error Handling: (view poc)

I tested the login page for error handling and the exposure of sensitive data.

3.2.3 Review Monitoring and Alerting Mechanisms: (view poc)

I checked for any active monitoring mechanisms that could alert the system or admins to potential threats.

4. Vulnerability Description

The OWASP Top 10 2021 highlights the importance of detecting, escalating, and responding to active breaches through logging and monitoring mechanisms. Without sufficient logging and monitoring, breaches may go undetected, potentially leading to severe data breaches and system compromises. This vulnerability **relates to A9 of the OWASP Top 10**, focusing on failures to log and monitor critical system activities.

5. Affected Components

- Critical systems such as **login, password reset,** and **registration forms** were tested for logging and error handling vulnerabilities.

6. Impact Assessment

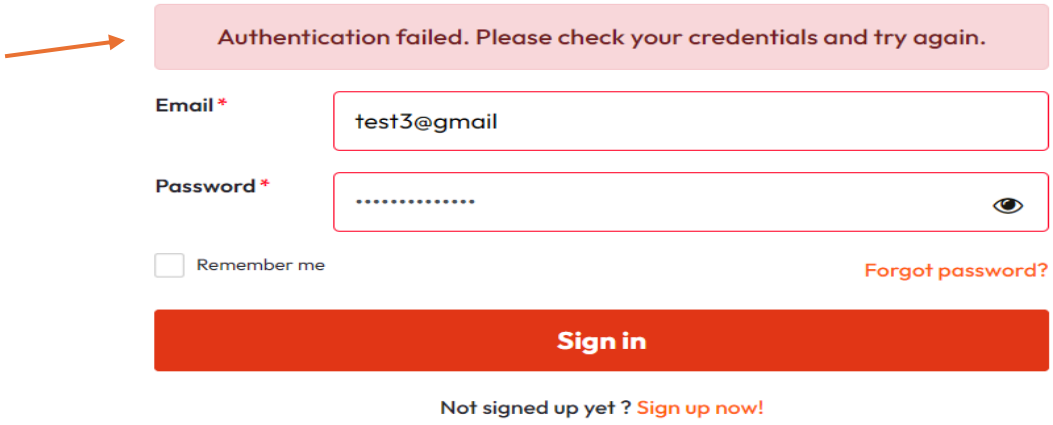
Common attack scenarios in this context often involve brute-forcing login credentials, exploiting weak or predictable tokens in password reset flows, and bypassing security measures due to insufficient logging and monitoring.

- **Brute Force Attacks:** If login attempts are not logged properly, attackers can repeatedly try different username and password combinations to gain unauthorized access.
- **Token Prediction and Reset Abuse:** Attackers can exploit weak or predictable tokens used in password reset flows to take over user accounts.
- **Account Enumeration:** Insufficient error handling can lead to attackers determining which usernames exist in the system, increasing the success rate of targeted attacks.
- **Denial of Service (DoS) Attacks:** The lack of monitoring or an account lockout mechanism allows attackers to flood the system with repeated failed login attempts, potentially leading to denial of service or unauthorized access.

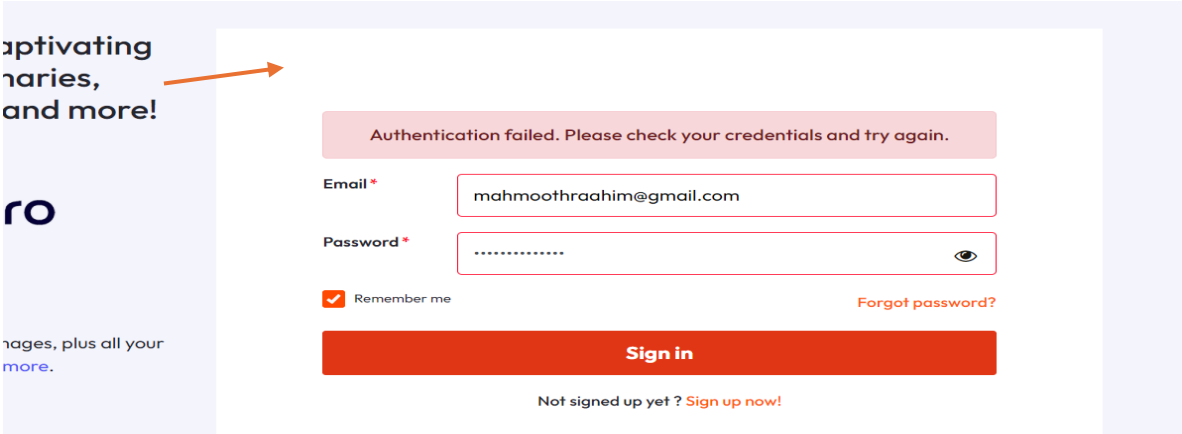
7. Proof of Concept (PoC)

Check for Login and Error Handling:

- I tested the login form with an **invalid password using the email** `test3@gmail.com` and received a generic "Authentication failed" message.



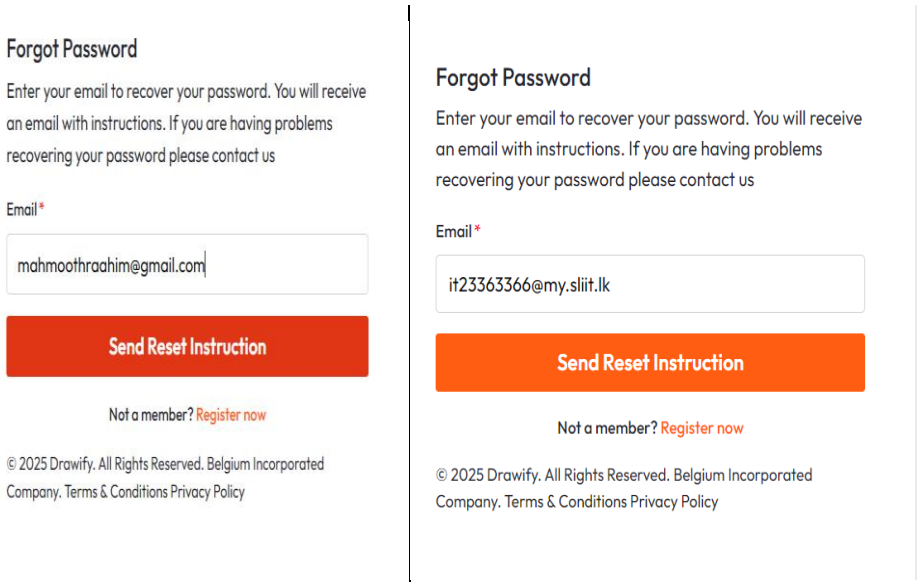
- I also tested with a **valid email** (`mahmoothraahim@gmail.com`) but an invalid password, and the **response was the same**.



❖ **No specific error messages were being returned for invalid credentials. This helps avoid user enumeration**.

Password Reset Handling:

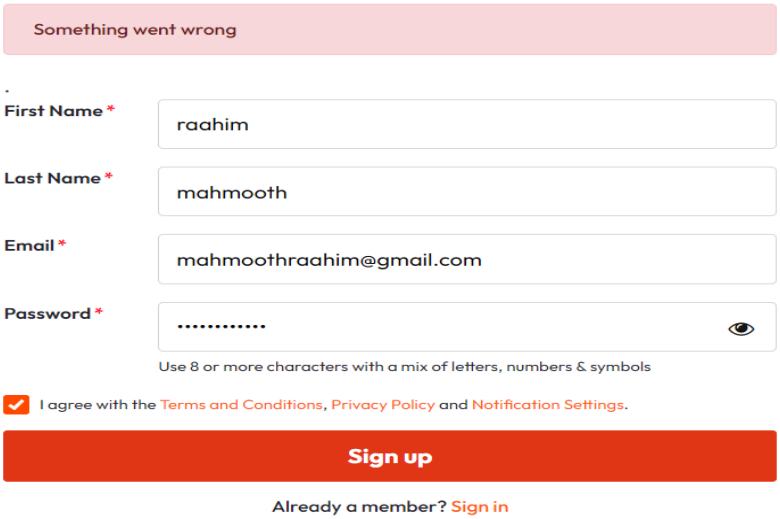
- When testing the password reset for the email *`mahmoothraahim@gmail.com`*, the **response led to the homepage** after submitting the request. However, **only valid emails received the reset link**.
- Testing with **an invalid email** (`it23363366@my.sliit.lk`) **resulted** in **no feedback** or **reset link**



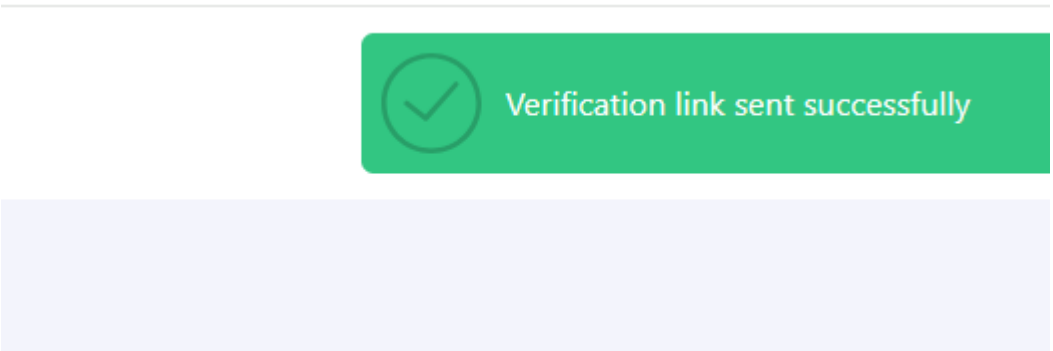
❖ **It demonstrating minimal error information returned to the user.**

Registration with Existing Email:

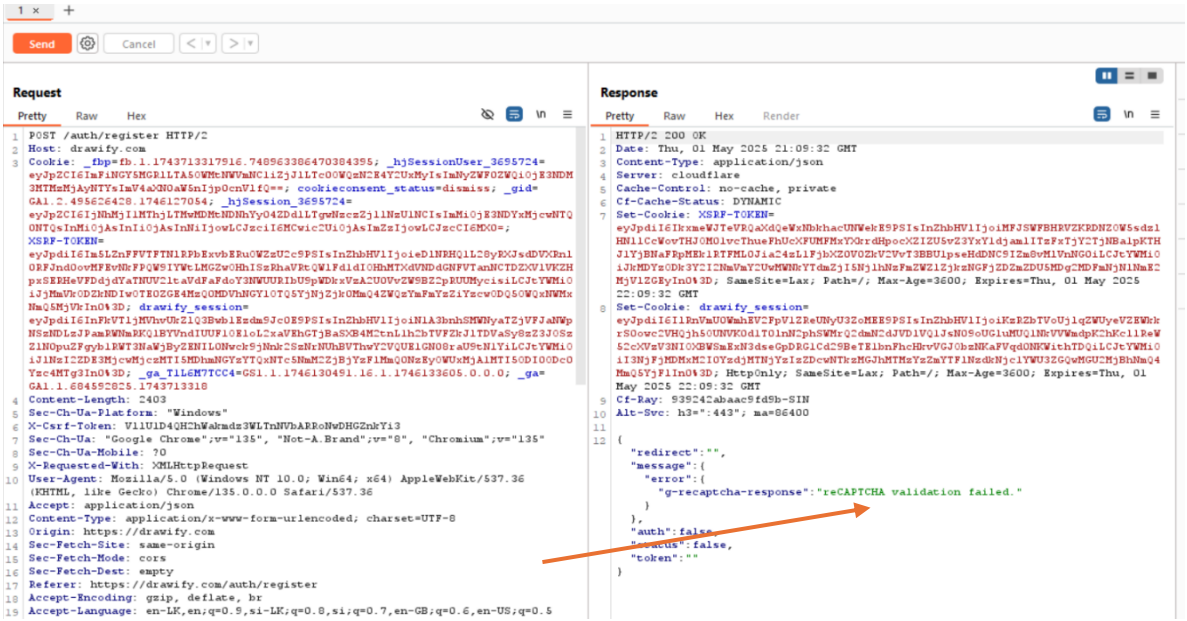
- I attempted to register with an existing email address (`mahmoothraahim@gmail.com`) and received a generic error message "Something went wrong," indicating good error handling. However, this could still be susceptible to user enumeration because ***"Email already exists***" versus "***Something went wrong.***" Were seems to similar errors, only **valid email** will resulting "***Something went wrong***" in the system



- Non existing emails are resulting by sending the verification link to Non existing emails, this sense possible user enumeration



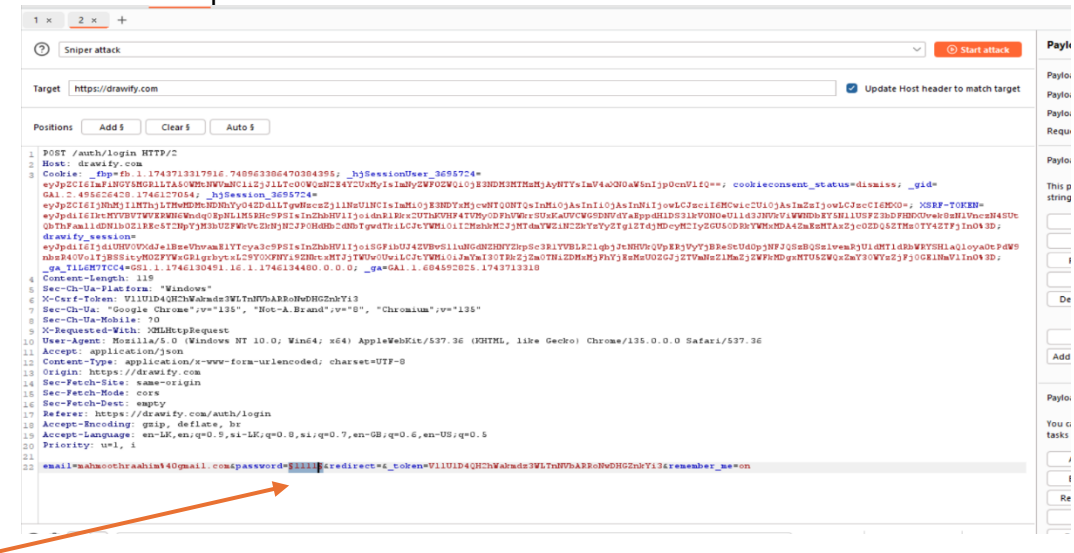
- Mean time open the burp and capture the submit form and tried to enumerate the email filed to identify potential valid emails

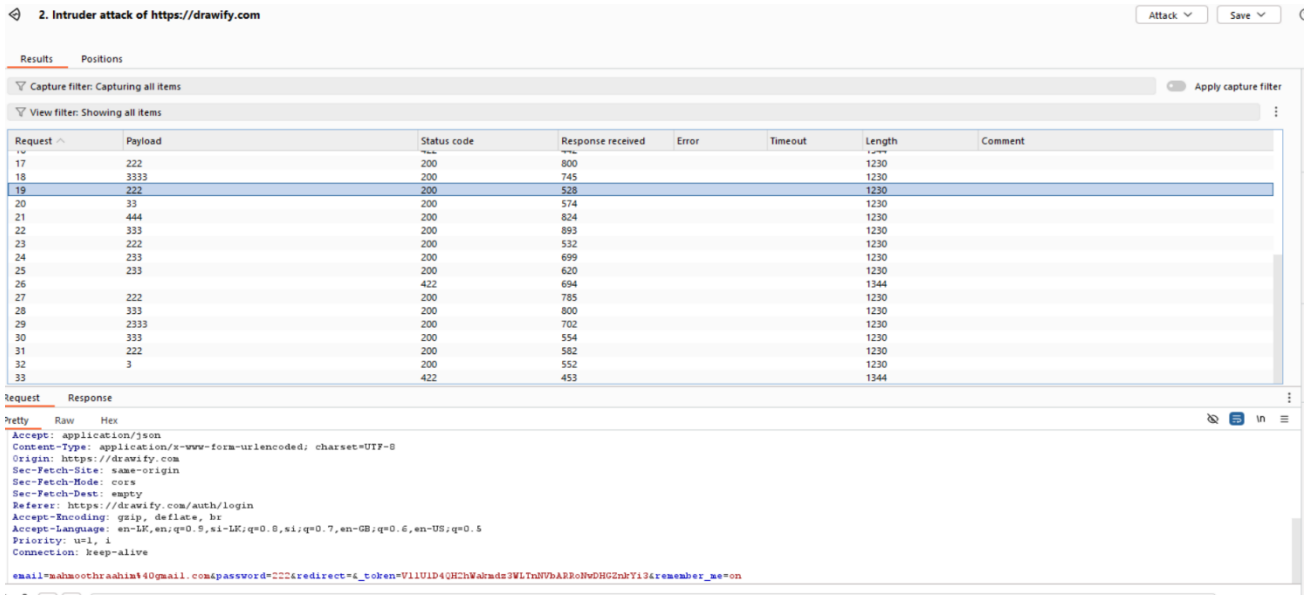


- **But the cool part here is registration form enforces reCAPTCHA, with token validation on every submission. Ensuring mitigation against brute-force or automated enumeration**.

Monitoring and Alerting Mechanisms Review:

- I used Burp Suite to capture login attempts with valid usernames and brute-forced my password using an annual password list. To identify is there any alerting or lockout mechanism in place





After this…

- Ensuring the **system did not have an account lockout mechanism** or **alerting via email**, but since this **is not a critical system like a banking application**, the lack of these features is acceptable for this context.

8. Proposed Mitigation

To mitigate this vulnerability, the following measures should be taken:

- Ensure all login, access control, and server-side input validation failures are logged with sufficient user context to identify suspicious or malicious activities. Logs should be stored for long enough to support forensic analysis if needed.
- Ensure that logs are generated in a format that log management systems can easily parse and analyze.
- Encode log data correctly to prevent injection attacks or other manipulations of the logging or monitoring systems.
- Implement audit trails for high-value transactions with integrity controls to prevent tampering or deletion.
- Establish effective monitoring and alerting mechanisms to detect and respond to suspicious activities quickly.
- Adopt an incident response and recovery plan, such as the NIST 800-61r2 framework, for improved security management.

9. Conclusion

The lack of proper logging and monitoring in this system exposes it to various security risks, such as brute-force attacks and token prediction exploitation. While some good error-handling practices are in place, there are still areas for improvement, particularly in ensuring all critical security events are properly logged and monitored for early breach detection and response.

10. References

- *OWASP A9: Security Logging and Monitoring Failures*