Penetration Testing Report

Prepared by: Sarang VP
Date: 03.10.2024

Table of Contents

---

1. Executive Summary

This report details the findings from the penetration test conducted on Tag Lah's web application. The test identified multiple vulnerabilities, including authentication bypass, CSRF vulnerabilities, file upload weaknesses, and IDOR vulnerabilities. Each vulnerability poses significant risks to user accounts and the integrity of the application.

2. Scope of Testing

The following components were included in the testing scope:

- User authentication mechanisms
- Password reset functionalities
- File upload features on the About-Us page
- User data access through the dashboard

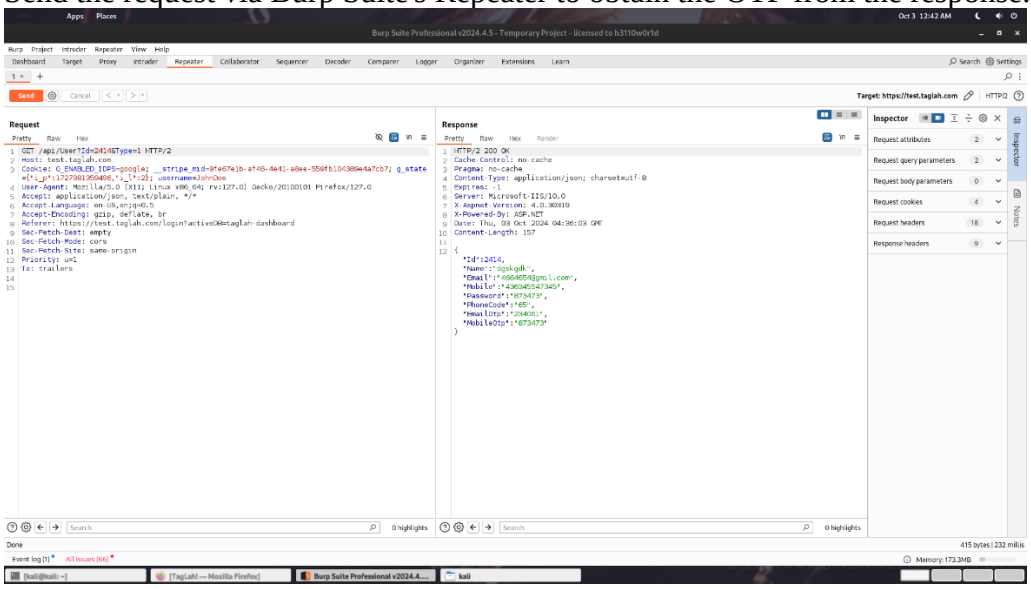
3. Vulnerabilities Identified

3.1 Authentication Bypass via OTP Verification

Description:
An attacker can bypass the OTP verification process to gain unauthorized access to user accounts.

Steps to Exploit:

1. Complete the account creation form to initiate OTP verification.
2. Intercept the OTP verification request using Burp Suite.
3. Send the request via Burp Suite's Repeater to obtain the OTP from the response.



Implications:
This vulnerability allows unauthorized access to user accounts without needing the password.

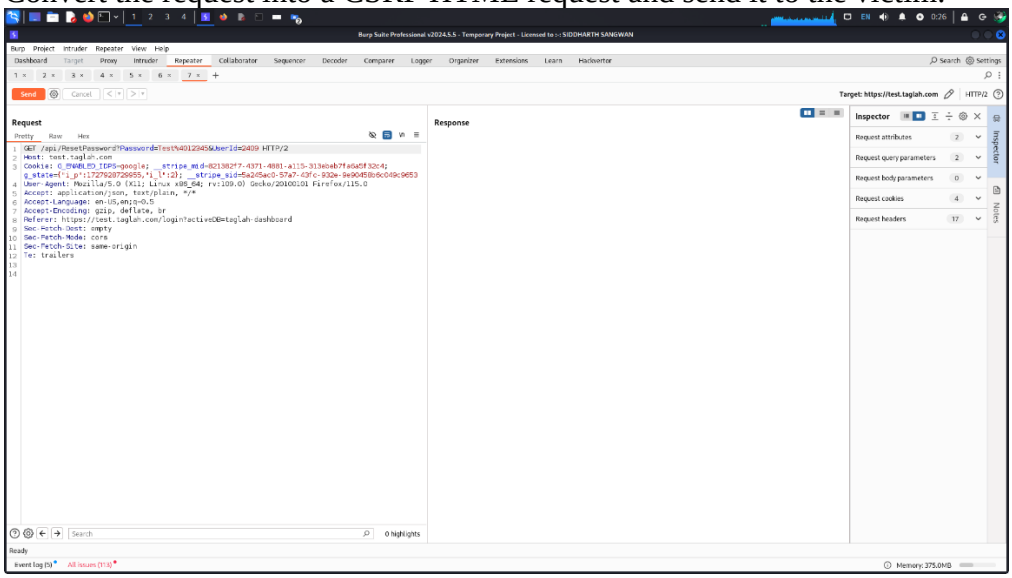
3.2 CSRF Vulnerability in Password Reset Functionality

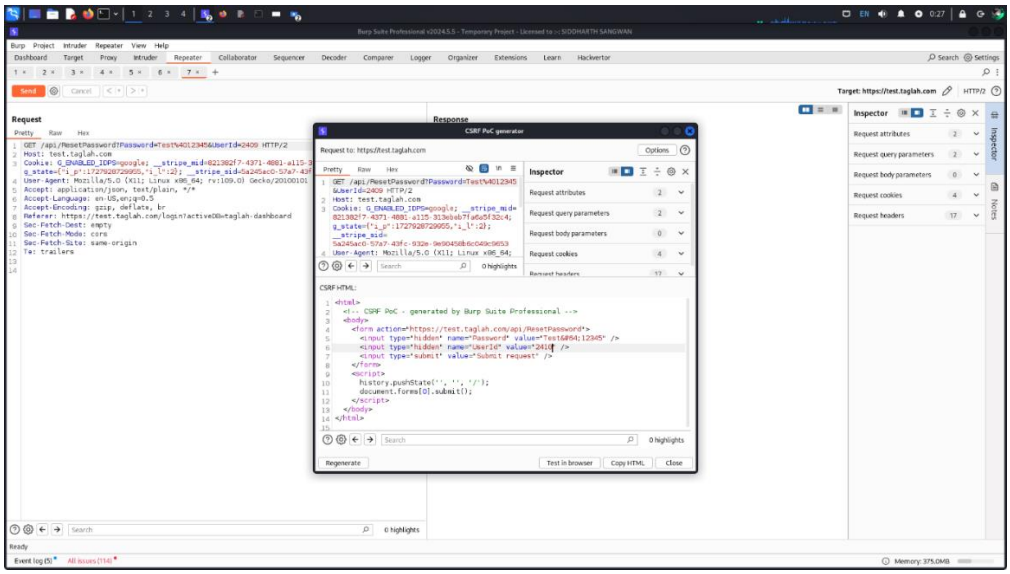
Description:
A CSRF vulnerability enables an attacker to change a user's password without their consent.

Steps to Exploit:

1. Capture the request for setting a new password using Burp Suite.
2. Modify the user ID and password in the captured request.

3. Convert the request into a CSRF HTML request and send it to the victim.





Implications:
An attacker could take control of any user account by changing passwords, leading to unauthorized access and potential data breaches.

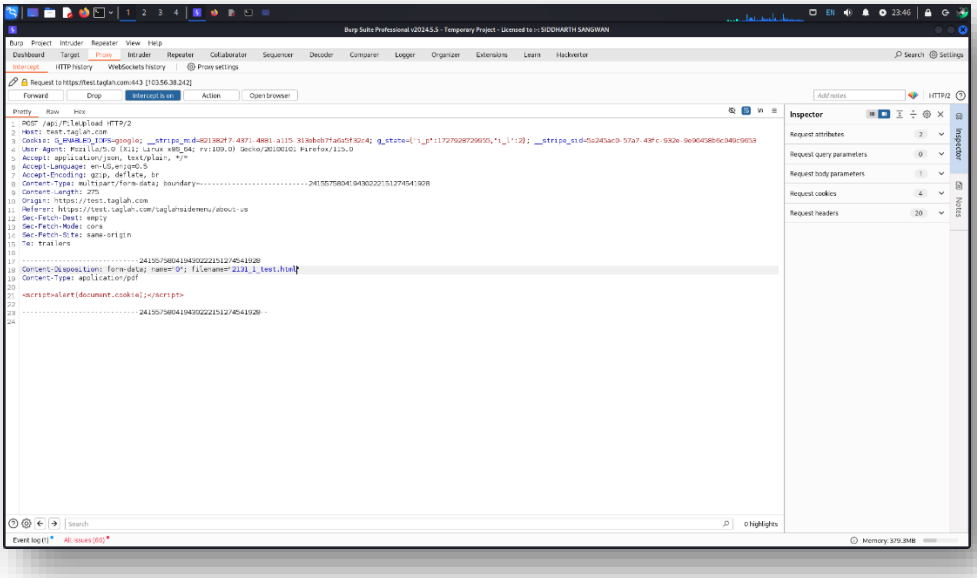
3.3 File Upload Vulnerability in PDF Upload Parameter

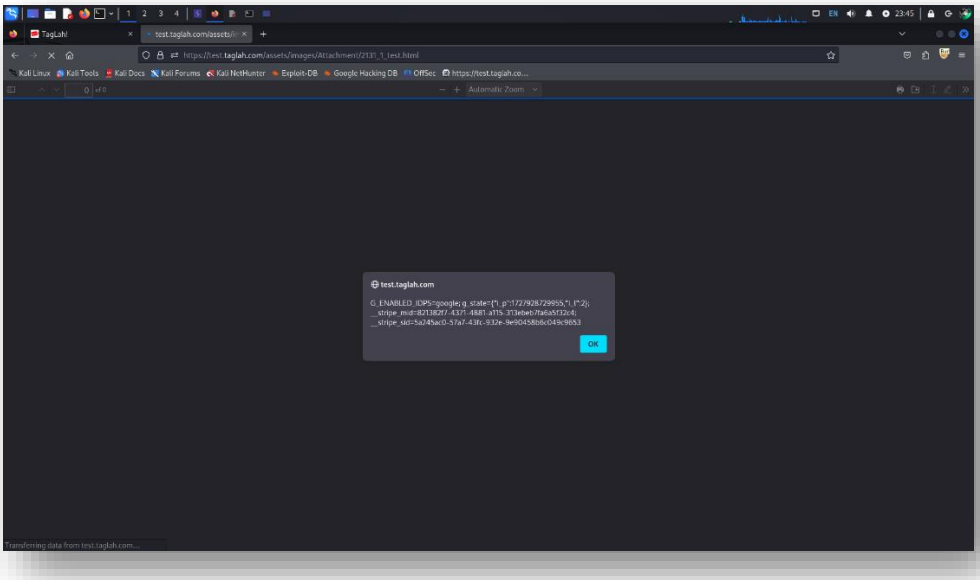
Description:
A vulnerability allows the upload of malicious HTML files disguised as PDFs.

Steps to Exploit:

1. Create a new card and navigate to the About-Us page.
2. Create a malicious HTML payload saved as `.html.pdf`.

3. Intercept the file upload request and modify file extenction it to upload the malicious file.
4. Execute the payload by accessing the uploaded file.





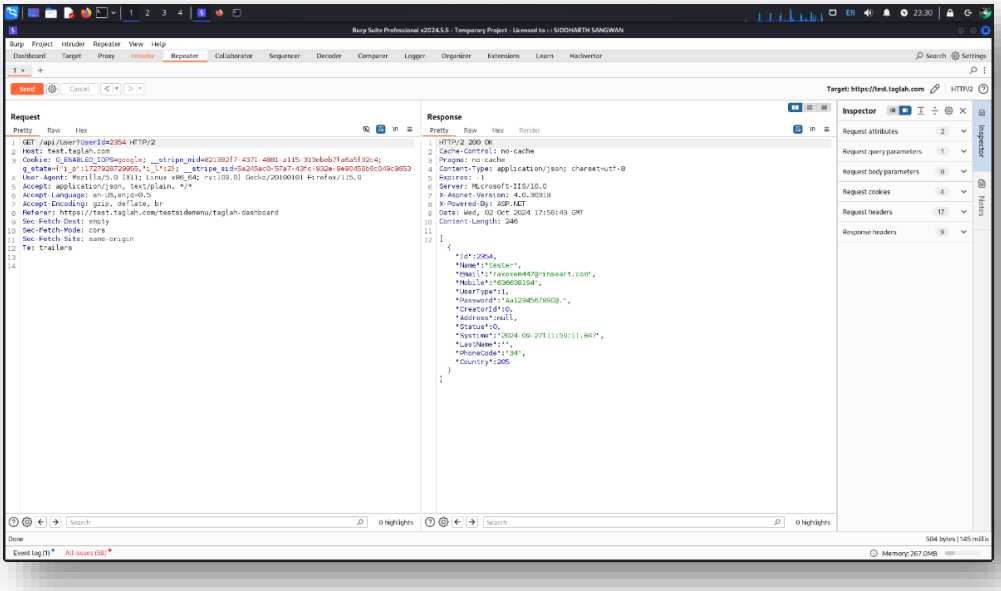
Implications:
This vulnerability can lead to XSS attacks, code injection, malware distribution, and unauthorized access to sensitive data.

3.4 Insecure Direct Object Reference (IDOR) Vulnerability

Description:
An IDOR vulnerability allows an attacker to access user details by manipulating the 'id' parameter in requests.

Steps to Exploit:

1. Capture the request for the dashboard that contains the 'id' parameter.
2. Bruteforce the 'id' parameter with various values to retrieve user details from the database.



Implications:
An attacker can access sensitive information of registered users, potentially leading to data leaks and privacy violations.

4. Severity Table

Vulnerability	Severity Level	Description
Authentication Bypass via OTP Verification	Critical	Allows unauthorized access to user accounts without passwords.
CSRF Vulnerability in Password Reset Functionality	High	Enables attackers to change user passwords without consent.
File Upload Vulnerability in PDF Upload Parameter	High	Permits the upload of malicious files, leading to XSS and other attacks.
Insecure Direct Object Reference (IDOR) Vulnerability	High	Allows unauthorized access to sensitive user details.

5. Recommendations

5.1 For Authentication Bypass via OTP Verification

- **Fix the OTP Verification Process:** Ensure OTPs are not sent in plain text. Use hashing or encryption methods for verification.
- **Implement Rate Limiting and IP Blocking:** Prevent brute-force attacks on OTP verification.
- **Adopt Secure Authentication Mechanisms:** Consider multi-factor authentication (MFA) or passwordless authentication.

5.2 For CSRF Vulnerability

- **Implement CSRF Protection:** Use token-based and header-based validation to secure requests.
- **Enhance Password Reset Process:** Employ a token-based system to verify user identity during password resets.
- **Validate User Input:** Implement thorough validation and sanitization to protect against CSRF attacks.

5.3 For File Upload Vulnerability

- **Implement File Type Validation:** Validate file types server-side to restrict uploads to allowed formats.
- **Utilize Secure File Upload Mechanisms:** Leverage libraries or frameworks that provide built-in file validation.
- **Sanitize User Input:** Protect against malicious data injection throughout the file upload process.
- **Use a Web Application Firewall (WAF):** Detect and block malicious file uploads.

5.4 For IDOR Vulnerability

- **Implement Access Controls:** Ensure that users can only access their own data by validating user permissions for each request.
- **Use Secure Coding Practices:** Apply best practices to prevent direct object reference vulnerabilities, such as using unique identifiers or tokens.
- **Regularly Review Access Logs:** Monitor access patterns to identify potential exploitation attempts.

6. Conclusion

The penetration test revealed critical vulnerabilities that could have significant implications for TAGLAH s security posture. Immediate remediation of the identified issues is recommended to enhance the security of the application and protect user data.

Prepared by:
Sarang VP