FUTURE_CS_01

WEB APPLICATION SECURITY TESTING

TASK

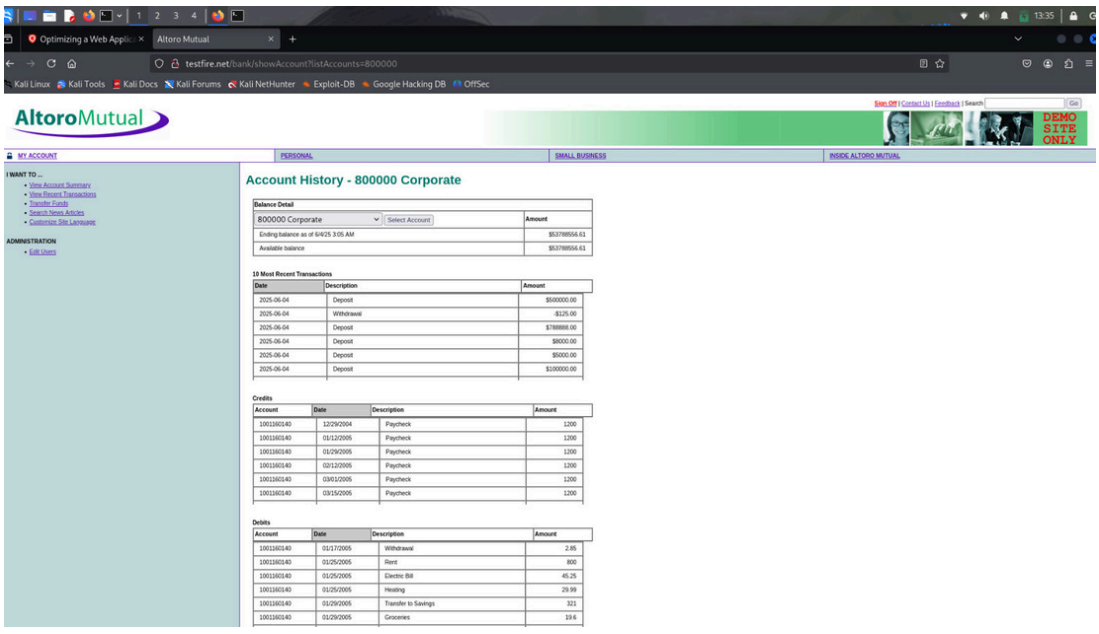
- Task: Conduct security testing on a sample web application to identify vulnerabilities like SQL injection, XSS, and authentication flaws.
- Skills Gained: Web application security, ethical hacking, penetration testing.
- Tools: OWASP ZAP, Burp Suite, SQLMap.
- Deliverable: A detailed security report with identified vulnerabilities and mitigation strategies.

TOOL USED & TARGET WEBSITE

- Burp Suite Community Edition
- Altoro Mutual Demo Banking Site - http://testfire.net

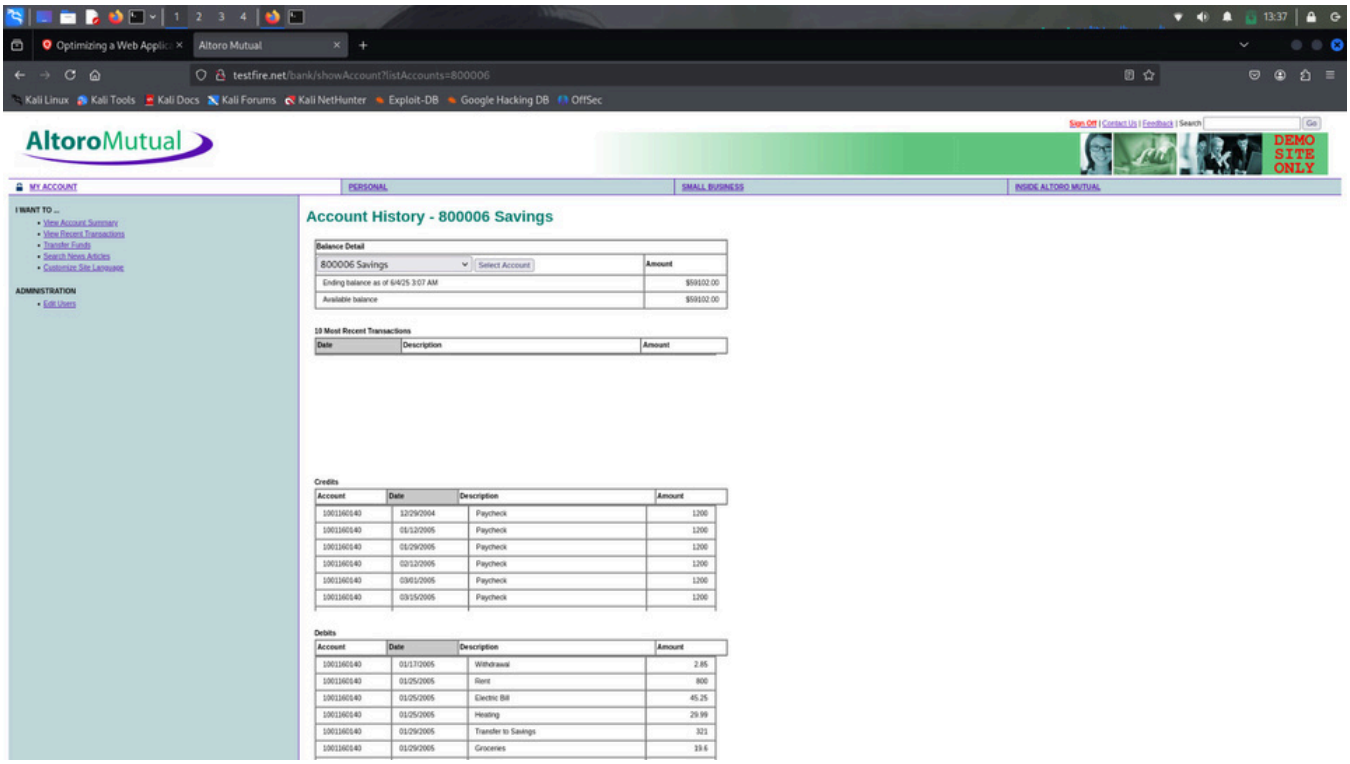
TESTING METHODOLOGY

- Configured browser to route traffic through Burp Suite proxy.
- Logged into the Altoro Mutual banking demo application.
- Intercepted account switching and balance viewing requests.
- Observed data exposures including account numbers, balances, and transactions.
- Performed passive scanning and observed insecure behavior in ID handling.



KEY FINDINGS

- **Insecure Direct Object Reference (IDOR)** - Account ID in the URL can be changed (e.g., 800000 -> 800006) to view data of other users.- Critical data like balances, debits, and credits are exposed.
- **Lack of Authorization Check** - There was no verification if the logged-in user has access to the requested account ID.
- **Sensitive Data Exposure** - The app returns full financial information without masking, including deposit and withdrawal history.
- **Missing Security Headers** - Burp Suite detected missing CSP, X-Frame-Options, and HSTS headers.



RECOMMENDATIONS

- Implement proper authorization checks before serving account data.
- Obfuscate or mask sensitive financial information where possible.
- Introduce secure session management and ID validation.
- Use security headers to protect against clickjacking and XSS.

CONCLUSION

The Altoro Mutual test application illustrates critical real-world vulnerabilities. Using Burp Suite, we identified several high-impact issues, including IDOR and data exposure. Fixing these will help reduce risk and improve the application's security posture.