SecureBank

Secure Coding – Team 8 – Phase 2

Swathi Shyam Sunder, Vivek Sethia,
Mai Ton Nu Cam, Korbinian Würl

SecureBank

BANK-APP Vulnerabilities

Name	Impact	Likelihood	CVSS Score
Weak Authorization Mechanism	High	High	8.1
Static Session ID	High	High	4.8
Command Injection	High	High	9.8
Buffer Overflow	High	High	7.9
SQL Injection	High	High	7.9
Directory Index	High	High	7.9
Reflected & Stored XSS	High	High	7.9
Weak Lockout Mechanism	High	High	7.5

Live Demo

Weak Authorization Mechanism

- A normal user can access the list of all the users.
- He can perform operations like approval/rejection of transactions

Static Session ID

- The session id is not unset when the user logs out.
- New session id is not generated on login ,if session id already exists.

  Tools - EditThisCookie (Chrome Extension)

Command Injection

- During file upload , filenames can be manipulated to upload files over the server.

  Example: test;touch mytest.txt;.txt

Buffer Overflow

- When a file with huge data is uploaded, then application crashes since memory is not allocated.

  Tools used - Burp Suite

SQL Injection

- Ranks in the list of top 10 vulnerabilities by OWASP.
- While performing a transaction, it possible to inject SQL in the recipient field.

    Tools used - SQLmap

Directory Listing

- The entire directory listing of the application is visible.

  Tools used - Nikto

Reflected and Stored XSS

- Ranks in the list of top 10 vulnerabilities by OWASP.
- Stored XSS is detected in all pages with forms such as Login and New Transaction.
- Refelcted XSS can be observed in View User page by manipulating the URL.

Weak Lockout Mechanism

- A attacker can try infinite number of times to login into the application.
- The same behavior can be observed in New Transaction.

Insecure Direct Object References

- Ranks in the list of top 10 vulnerabilities by OWASP.
- A customer can gain unauthorized access to transactions of all other customers by modifying the URL in Transactions page.

Sensitive Data Exposure

- Ranks in the list of top 10 vulnerabilities by OWASP.
- Cookie can be used to steal the session of any user account or the administrator account. Hence sensitive data information is easily leaked.

Tools - EditThisCookie (Chrome Extension)

Missing Function Level Access Control

- Ranks in the list of top 10 vulnerabilities by OWASP.
- A customer can view all the transactions of the bank which should be seen only by authorized personnel.