SecureBank

Secure Coding – Team 8 – Phase 4

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

White Box Testing & Reverse Engineering of Team 4 - Online Banking

SecureBank

Online Banking Vulnerabilities

Name	Impact	Likelihood	CVSS Score	Phase
Sensitive Data Exposure	High	High	8.6	2
Weak Password Policy	High	High	8.3	2
Bypassing Session Management	High	High	9.8	2
Weak Lockout Mechanism	High	High	7.5	2
SQL Injection	High	High	7.5	2
Buffer Overflow in C	High	Medium	7.5	2

Sensitive Data Exposure

- Ranks in the list of top 10 vulnerabilities by OWASP
- No HTTPS
- Sensitive data is unencrypted over the HTTP channel and exposed to attack

Weak Password Policy

- No password policy during reset password. Password can even be set to blank.
- Weak cryptographic hash - Passwords stored in DB using md5

Bypassing Session Management Schema

- Ranks in the list of top 10 vulnerabilities by OWASP
- Cookie can be used to steal the session of any user account or the employee account and session can be hijacked.

Weak Lockout Mechanism

- An attacker can perform infinite attempts to login to the application.
- Increases the possibilities for Brute force attacks

SQL Injection

- Ranks in the list of top 10 vulnerabilities by OWASP
- No prepared statements in most queries
- User input is not validated/sanitized

Buffer Overflow in C

- Use of functions like strcpy, strcat and sprintf without checking lengths
- Results in overflow if string is long enough

Integer Overflow

- No checks during initialization of user account balance by Employee
- Example: Setting 111111111 results in 99999999.99

Live Demo