SecureBank

Secure Coding – Team 8 – Phase 5

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

SecureBank

Use Cases: Phase 1

- ✔ Customer/Employee registration (including sending e-mail with TANs)
- ✔ Customer/Employee login
- ✔ Customer/Employee logout
- ✔ Customer/Employee views bank account details of Customer
- ✔ Customer/Employee views transaction history of Customer
- ✔ Customer money transfer via HTML form (using TAN)
- ✔ Customer money transfer via uploading transaction batch file (using TAN)
- ✔ Employee approves transfers larger than 10.000 EUR
- ✔ Employee approves registration of Customer or of other employee
- ✔ Customer/Employee downloads transaction history of Customer as PDF document

Use Cases: Phase 3

- ✔ Employee initializes the Account Balance of a Customer
- ✔ Customer receives TANs in a password protected PDF via Email
- ✔ Customer / Employee recovers forgotten password via Email
- ✔ Download of SCS after registration
- ✔ Customer money transfer via HTML form (using TAN from SCS)
- ✔ Customer money transfer via uploading transaction file (using TAN from SCS)

Use Cases: Phase 3 - Fixes

- ✔ Use of HTTPS
- ✔ Directory traversal/File include
- ✔ Weak lockout mechanisms
- ✔ Weak password policy
- ✔ Session fixation
- ✔ XSS
- ✔ Stack traces
- ✔ Business logic data validation
- ✔ CSRF
- ✔ Clickjacking
- ✔ Buffer overflow

Use Cases: Phase 5 - Fixes

- ✔ Guessable User Account
- ✔ Weak SSL/TLS Ciphers
- ✔ SCS stack traces
- ✔ Cookie secure flag
- ✔ Buffer overflow in C
- ✘ Error Codes

Security Features (1)

Countermeasures against

- SQL Injection: User input sanitization
- Privilege Escalation:
  - Consistent checks for privilege
  - Page-access independent of user input
- XSS: User input sanitization

Security Features (2)

- CSRF: Unique CSRF tokens for every request
- Insecure Channel: Use of HTTPS and HSTS header
- Session Fixation:
  - Session timeout
  - PHP cookie with secure and httponly flag
- Brute Force: Lockout mechanism

Security Features (3)

- File Attacks: Proper validation of uploaded files
- Traversal Attacks: Disabled directory listing
- Clickjacking: X-Frame-Options header

Lessons Learned

- Good architecture -> easier to fix things
- Vulnerabilities hide in small details
- No project is too small for some kind of task management

SecureBank is very secure!

Sign up now and get 10.000€!