Team 20

Presented by

Simon Barth
Bharti Munjal
Michael Remmler

Use Cases From Phase 1	Implemented?
Customer / Employee registration (including sending e-mail with TANs)	YES
Customer / Employee login	YES
Customer / Employee logout	YES
Customer / Employee views bank account details of Customer	YES
Customer / Employee views transaction history of Customer	YES
Customer money transfer via HTML form (using TAN)	YES
Customer money transfer via uploading transaction batch file (using TAN)	YES
Employee approves transfers larger than 10.000 EUR	YES
Employee approves registration of Customer or of other employee	YES
(optional) Customer / Employee downloads transaction history of Customer as PDF document	YES
Vulnerabilities from Phase 1	**Fixed?**
Reflected Cross Site Scripting	YES
SQL Injection	YES
Clickjacking	YES
Session Timeout	YES

Use Cases from Phase 3	Implemented?
Encrypted TAN delivery by email	YES
Download of SCS	YES
Transfer money using SCS	YES
Customer/Employee Password Recovery	YES
Employee able to initialize balance	YES
Transactions only to existing Accounts	YES
Account Number and amount visible to customer	YES
Batch Transfer allow multiple transfer	YES
All required fields shown in transaction history	YES
Vulnerabilities from Phase 3	**Fixed?**
Weak change and forgot password policy	YES
Upload of unexpected file type	YES
Weak browser cache policy	YES

Security Features
Session Timeout
Account validation email
Locking of account if multiple unsuccessful attempts are made (brute force protection)
Ensuring Strong password
HTTPS, no browser cache, cookie protection
CSRF protection in forms
Clickjacking Protection (Frame-breaking script and X-Frame-Options)
Obfuscated C++

Lessons Learned
Knowledge about vulnerability types like CSRF, XSS and SQL injection
Small vulnerabilities can compromise the whole system
Getting crypto right is hard
Some languages are hard to handle and are easily used in a wrong way
Changing the basic architecture takes up lots of time
Never trust user input
Investigate third party components thoroughly before deciding to use them

Additional Features

Migration to phpsec
“Change Password” functionality
“Remember Me” option

Thank You