DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Secure Coding - Phase 2

Blackbox Testing Report

Team 12
Alexander Lill
Lorenzo Donini
Florian Mauracher
Mahmoud Naser

Executive Summary

1 DogeBank- Team 27

2 Goliath National Bank- Team 12

3 Comparison

Contents

1 Timetracking

User	Task	Time
Alexander Lill	Example	2h
Lorenzo Donini	Example	2h
Florian Mauracher	Example	2h
Mahmoud Naser	Example	2h

2 Vulnerabilities Overview

2.1 DogeBank

2.2 Goliath National Bank

2.3 Comparison

3 Detailed Report

3.1 Tools description

3.2 Configuration and Deploy Management Testing

3.2.1 Test File Extensions Handling for Sensitive Information (OTG-CONFIG-003)

	DogeBank
Observation	observation text
Discovery	discovery text
Likelihood	likelihood text
Implication	implication text
CVSS	av ac pr ui s c i a

	Goliath National Bank
Observation	observation text
Discovery	discovery text
Likelihood	likelihood text
Implication	implication text
CVSS	av ac pr ui s c i a

3.2.2 Test HTTP Methods (OTG-CONFIG-006)

3.2.3 Test HTTP Strict Transport Security (OTG-CONFIG-007)

3.2.4 Test RIA cross domain policy (OTG-CONFIG-008)

3.3 Identity Management Testing

3.3.1 Test Role Definitions (OTG-IDENT-001)

3.3.2 Test User Registration Process (OTG-IDENT-002)

3.3.3 Test Account Provisioning Process (OTG-IDENT-003)

3.3.4 Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004)

3.3.5 Testing for Weak or unenforced username policy (OTG-IDENT-005)

3.4 Authentication Testing

3.4.1 Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)

3.4.2 Testing for default credentials (OTG-AUTHN-002)

3.4.3 Testing for Weak lock out mechanism (OTG-AUTHN-003)

3.4.4 Testing for bypassing authentication schema (OTG-AUTHN-004)

3.4.5 Test remember password functionality (OTG-AUTHN-005)

3.4.6 Testing for Browser cache weakness (OTG-AUTHN-006)

3.4.7 Testing for Weak password policy (OTG-AUTHN-007)

3.4.8 Testing for Weak security question/answer (OTG-AUTHN-008)

3.4.9 Testing for weak password change or reset functionalities (OTG-AUTHN-009)

3.4.10 Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)

3.5 Authorization Testing

3.5.1 Testing Directory traversal/file include (OTG-AUTHZ-001)

3.5.2 Testing for bypassing authorization schema (OTG-AUTHZ-002)

3.5.3 Testing for Privilege Escalation (OTG-AUTHZ-003)

3.5.4 Testing for Insecure Direct Object References (OTG-AUTHZ-004)

3.6 Session Management Testing

3.6.1 Testing for Bypassing Session Management Schema (OTG-SESS-001)

3.6.2 Testing for Cookies attributes (OTG-SESS-002)

3.6.3 Testing for Session Fixation (OTG-SESS-003)

3.6.4 Testing for Exposed Session Variables (OTG-SESS-004)

3.6.5 Testing for Cross Site Request Forgery (OTG-SESS-005)

3.6.6 Testing for logout functionality (OTG-SESS-006)

3.6.7 Test Session Timeout (OTG-SESS-007)

3.6.8 Testing for Session puzzling (OTG-SESS-008)

3.7 Data Validation Testing

3.7.1 Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)

3.7.2 Testing for Stored Cross Site Scripting (OTG-INPVAL-002)

3.7.3 Testing for HTTP Verb Tampering (OTG-INPVAL-003)

3.7.4 Testing for HTTP Parameter pollution (OTG-INPVAL-004)

3.7.5 Testing for SQL Injection (OTG-INPVAL-005)

3.7.6 Testing for LDAP Injection (OTG-INPVAL-006)

3.7.7 Testing for ORM Injection (OTG-INPVAL-007)

3.7.8 Testing for XML Injection (OTG-INPVAL-008)

3.7.9 Testing for SSI Injection (OTG-INPVAL-009)

3.7.10 Testing for XPath Injection (OTG-INPVAL-010)

3.7.11 IMAP/SMTP Injection (OTG-INPVAL-011)

3.7.12 Testing for Code Injection (OTG-INPVAL-012)

Testing for Local File Inclusion
Testing for Remote File Inclusion

3.7.13 Testing for Command Injection (OTG-INPVAL-013)

3.7.14 Testing for Buffer overflow (OTG-INPVAL-014)

Testing for Heap overflow
Testing for Stack overflow
Testing for Format string

3.7.15 Testing for incubated vulnerabilities (OTG-INPVAL-015)

3.7.16 Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)

3.8 Error Handling

3.8.1 Analysis of Error Codes (OTG-ERR-001)

3.8.2 Analysis of Stack Traces (OTG-ERR-002)

3.9 Cryptography

3.9.1 Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001)

3.9.2 Testing for Padding Oracle (OTG-CRYPST-002)

3.9.3 Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)

3.10 Business Logic Testing

3.10.1 Test Business Logic Data Validation (OTG-BUSLOGIC-001)

3.10.2 Test Ability to Forge Requests (OTG-BUSLOGIC-002)

3.10.3 Test Integrity Checks (OTG-BUSLOGIC-003)

3.10.4 Test for Process Timing (OTG-BUSLOGIC-004)

3.10.5 Test Number of Times a Function Can be Used Limits (OTG-BUSLOGIC-005)

3.10.6 Testing for the Circumvention of Work Flows (OTG-BUSLOGIC-006)

3.10.7 Test Defenses Against Application Mis-use (OTG-BUSLOGIC-007)

3.10.8 Test Upload of Unexpected File Types (OTG-BUSLOGIC-008)

3.10.9 Test Upload of Malicious Files (OTG-BUSLOGIC-009)

3.11 Client Side Testing

3.11.1 Testing for DOM based Cross Site Scripting (OTG-CLIENT-001)

3.11.2 Testing for JavaScript Execution (OTG-CLIENT-002)

3.11.3 Testing for HTML Injection (OTG-CLIENT-003)

3.11.4 Testing for Client Side URL Redirect (OTG-CLIENT-004)

3.11.5 Testing for CSS Injection (OTG-CLIENT-005)

3.11.6 Testing for Client Side Resource Manipulation (OTG-CLIENT-006)

3.11.7 Test Cross Origin Resource Sharing (OTG-CLIENT-007)

3.11.8 Testing for Cross Site Flashing (OTG-CLIENT-008)

3.11.9 Testing for Clickjacking (OTG-CLIENT-009)

3.11.10 Testing WebSockets (OTG-CLIENT-010)

3.11.11 Test Web Messaging (OTG-CLIENT-011)

3.11.12 Test Local Storage (OTG-CLIENT-012)