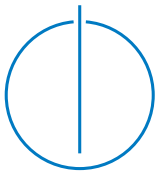
DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Report

Black Box Testing Report

Alexis Engelke, Johannes Fischer, Ralph Schaumann,
Saurabh Nawalgaria



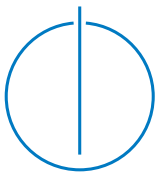
DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Report

Black Box Testing Report

Author:	Alexis Engelke, Johannes Fischer, Ralph Schaumann, Saurabh Nawalgaria
Team:	9
Lecture:	Secure Coding, Phase 2
Submission Date:	November 24, 2015



Executive Summary

Contents

1 Time Tracking

If a task is prefixed with (o), it refers to the Online Banking web application, if a task is prefixed with (s), the task refers only to the SecureBank web application.

Table 1.1: Time Tracking Table

Name	Task	Time
Alexis Engelke	Setting up LaTeX template	1
Alexis Engelke	(o) Analyzing XSS vulnerabilities using ZAP	2
Alexis Engelke	(o) Analyzing SQL injection vulnerabilities in the web interface using SQLmap	1.5
Alexis Engelke	(o) Analyzing SQL injection vulnerabilities in the file upload	2
Alexis Engelke	(o) Exploiting the TAN verification in the file upload	2
Alexis Engelke	Testing and Documenting Configuration and Deploy Management Testing	2
Alexis Engelke	Testing and Documenting Identity Management Testing	1
Foo	Fixing all issues	10

2 Vulnerabiliteis Overview

Through our testing, we identified the following vulnerabilities as the most critical for the Online Banking application and the SecureBank:

2.1 Online Banking

2.1.1 Stored XSS in Registration and Transaction Description

- Likelihood: high
- Implication: high
- Risk: high

With stored cross site scripting attacks it is possible to inject JavaScript code, which is run whenever an employee logs in and opens the list of unapproved accounts or transactions. It is also possible to inject script from other sites.

2.1.2 Missing check for amount in transactions from batch file

- Likelihood: medium
- Implication: high
- Risk: high

It is possible to get money from another client of the bank by filling in a negative number in the amount field of a transaction batch file. Therefore, one client can generate an infinite amount of money, while reducing the amount of money of other clients.

2.1.3 SQL injection in transaction batch file

- Likelihood: medium
- Implication: high

- Risk: high

The application is vulnerable to SQL injections in the transaction batch files. Therefore, it is possible to perform transactions while using any unused TAN in the system, which is not known to the attacker and might come from another client.

2.1.4 Some critical vulnerability

- Likelihood: high
- Implication: high
- Risk: high

The web application is vulnerable.

2.2 SecureBank

3 Tools

3.1 Zed Attack Proxy (ZAP)

TODO: Improve

- Stored XSS in Online Banking registration
- Basic SQL injection
  - In Online Banking: SQL injection in registration and login
- Reveal parts of the directory structure using forced browse
- In theory: buffer overflows, but none found

3.2 SQLmap

TODO: Improve

- SQL injection
  - In Online Banking: SQL injection in registration and login
  - In SecureBank: No SQL injection revealed

4 Detailed Report

4.1 Configuration and Deploy Management Testing

4.1.1 Test File Extensions Handling for Sensitive Information

Online Banking

Observation	We found various files which are served as plain text but are PHP source files. One of these files contains the credentials of the mail server. We were also able to download the compiled executable as well as the source code of the batch file parser.
Discovery	Using the OWASP ZAP tool, we used the forced browse functionality on `/InternetBanking/`. We received a list of files which were found using this tool, see below.
Likelihood	This can be tested by anyone who enters specific strings into the address bar of a browser. However, the likelihood of this vulnerability is much higher if the attacker uses specific tools which test specific paths systematically.
Impact	The attacker can get sensitive information, e.g. credentials to the mail server or the database. He can analyze the source of the parser and find vulnerabilies there.
Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Intigrity	No Impact
Availability	No Impact

TODO: Forced browsing results.

SecureBank

Observation	We found some HTML snippets, which do not contain any sensitive information, and the compiled executable of the transaction file parser.
Discovery	Using the OWASP ZAP tool, we used the forced browse functionality on `/seccoding-2015/`. We received a list of files which were found using this tool, see below.
Likelihood	This can be tested by anyone who enters specific strings into the address bar of a browser. However, the likelihood of this vulnerability is much higher if the attacker uses specific tools which test specific paths systematically.
Impact	The attacker only has access to the parser executable, which might contain information about the database connection. He can analyze the parser and find vulnerabilies there.
Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Intigrity	No Impact
Availability	No Impact

TODO: Forced browsing results.

Comparison

The web application of the SecureBank discloses less sensitive information. However, both applications disclose information which should not be available to unauthorized persons.

4.1.2 Test HTTP Methods

Online Banking

Observation	The server responded that the method `POST`, `GET`, `OPTIONS` and `HEAD` are supported.
Discovery	We submitted the request `OPTIONS / HTTP/1.1` to the server via NetCat on port 80.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	The server responded that the method `POST`, `GET`, `OPTIONS` and `HEAD` are supported.
Discovery	We submitted the request `OPTIONS / HTTP/1.1` to the server via NetCat on port 80.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

There are no significant differences between both applications.

4.1.3 Test HTTP Strict Transport Security

Online Banking

Observation	The server did not send any `Strict-Transport-Security` header.
Discovery	Executing the command `curl -s -D- http://vm/InternetBanking/ | grep Strict` resulted in no results.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	The server did not send any `Strict-Transport-Security` header.
Discovery	Executing the command `curl -s -D- http://vm/InternetBanking/ | grep Strict` resulted in no results.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

There are no significant differences between both applications.

4.1.4 Test RIA cross domain policy

Online Banking

Observation	No cross domain policy files were found.
Discovery	We scanned the traffic using ZAP.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	No cross domain policy files were found.
Discovery	We scanned the traffic using ZAP.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

There are no significant differences between both applications.

4.2 Identity Management Testing

4.2.1 Test Role Definitions

Online Banking

Observation

We found the following functionality for the different roles:

	Client	Employee
View own account	×	×
View own transaction history	×	–
Create new transactions	×	–
View account and transaction history of clients and employees	–	×
Change account details and balance of clients and employees	–	×
Approve transactions	–	×
Approve registrations of clients and employees	–	×

We noticed that there are links to view the transaction history and change the account balance of employees, too.

Discovery

We gathered the information by exploring the web application interface manually.

Impact

n/a

Likelihood

n/a

CVSS

n/a

SecureBank

Observation We found the following functionality for the different roles:

	Client	Employee
View own account	×	–
View own transaction history	×	–
Create new transactions	×	–
View account and transaction history of clients	–	×
Approve transactions	–	×
Approve registrations of clients and employees	–	×

Discovery We gathered the information by exploring the web application interface manually.

Impact n/a

Likelihood n/a

CVSS n/a

Comparison

The SecureBank web application does not offer a possibility for an employee to change the account balance of a client. However, the Online Banking application allows to view the transaction history and change the account balance also for employees, which have no account. This behaviour might be confusing.

4.2.2 Test User Registration Process

Online Banking

Observation	For registration, a username, an e-mail address, a password and whether the registrant is a client or an employee are needed. Anyone can register for access. The registration has to be approved by an employee before the registrant can use the account. A person can register only one time with the same e-mail address. However, a person can register many times with the same username. (The activation of such an account fails with a database error.) We could not find out, whether the registrants are verified personally before the approval.
Discovery	We tried to register several accounts with the same e-mail address and/or username using the web application.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	For registration, the full name, an e-mail address, a password and whether the registrant is a client or an employee are needed. Anyone can register for access. The registration has to be approved by an employee before the registrant can use the account. A person can register only one time with the same e-mail address. We could not find out, whether the registrants are verified personally before the approval.
Discovery	We tried to register several accounts with the same e-mail address and/or names using the web application.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

The Online Banking web application allows the double-registration of the same username at first, it only fails at the activation. This behaviour is confusing. Also, the application should ask for the full name be able to verify the name. Otherwise, there are no significant differences between both applications.

4.2.3 Test Account Provisioning Process

Online Banking

Observation	There is no way to change the role of a user. Account requests (both, client and employee) must be approved by an employee.
Discovery	We followed the links in the user interface and tried to login as a non-verified user.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	There is no way to change the role of a user. Account requests (both, client and employee) must be approved by an employee.
Discovery	We followed the links in the user interface and tried to login as a non-verified user.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

There are no significant differences between both applications.

4.2.4 Testing for Account Enumeration and Guessable User Account

Online Banking

Observation	There are no differences in the servers response for not activated accounts, valid usernames and invalid usernames.
Discovery	We tested the login for activated and non-activated accounts, existing and not-existing usernames and valid or invalid passwords.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	There are no differences in the servers response for not activated accounts, valid usernames and invalid usernames.
Discovery	We tested the login for activated and non-activated accounts, existing and not-existing usernames and valid or invalid passwords.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

There are no significant differences between both applications.

4.2.5 Testing for Weak or unenforced username policy

Online Banking

Observation	We were not able to find a username policy.
Discovery	We tested various usernames.
Impact	n/a
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	The username has to be a valid e-mail address of the client/employee. There is no policy regarding the e-mail address.
Discovery	We tested valid and invalid e-mail addresses.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

The only difference between the applications is that the Online Banking application uses usernames, which might have less correlation to the user than the e-mail address.

4.3 Authentcation Testing

4.3.1 Testing for Credentials Transported over Encrypted Channel

TODO!

Online Banking

Observation	
Discovery	
Impact	
Likelihood	n/a
CVSS	n/a

SecureBank

Observation	
Discovery	
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

4.3.2 Testing for default credentials

We decided to not test for default credentials, because we are working with custom software and therefore assume that all users and administrators choose secure passwords.

4.3.3 Testing for Weak lock out mechanism

Online Banking

Observation	We were not able to find any lock out mechanism. Therefore, brute force attacks on passwords are possible.
Discovery	We entered a valid username and incorrect passwords 10 times, and always got the error message about an incorrect password. Afterwards, we were able to log in with a correct password.
Impact	An attacker can brute-force the password of any user and therefore take the user over.
Likelihood	High
Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Intigrity	Low
Availability	No Impact

SecureBank

Observation	We were not able to find any lock out mechanism. Therefore, brute force attacks on passwords are possible.
Discovery	We entered a valid username and incorrect passwords 10 times, and always got the error message about the failed login. Afterwards, we were able to log in with a correct password.
Impact	An attacker can brute-force the password of any user and therefore take the user over.
Likelihood	High
Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Intigrity	Low
Availability	No Impact

Comparison

Both applications do not provide any lock out mechanism.

4.3.4 Testing for bypassing authentication schema

Online Banking

Observation	We were able to bypass the authentication schema via a SQL injection. This gave us the ability to login as any user without knowing the password.
Discovery	Using the fuzzer `jbrofuzz / SQL Injection` of ZAP on the username field of the login page, we were able to login as `admin` or another user without knowing the password. We had no success with direct page requests, modifiying the session ID and parameter modification.
Impact	An attacker can take over a user without knowing the valid access credentials.
Likelihood	High
Access Vector	Network
Access Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Intigrity	Low
Availability	No Impact

SecureBank

Observation	We were not able to bypass the authentication schema.
Discovery	Using the fuzzer `jbrofuzz / SQL Injection` of ZAP and SQLmap on the username field of the login page, we were not able to find SQL injection vulnerabilities to bypass the authentication schema. We also had no success with direct page requests, modifiying the session ID and parameter modification.
Impact	n/a
Likelihood	n/a
CVSS	n/a

Comparison

The Online Banking web application provides a way to bypass the authentication schema via SQL injection. The SecureBank application does not offer such vulnerabilities.

Acronyms

TUM Technische Universität München.