



GOLIATH NATIONAL BANK

SECURE CODING

TEAM 12 - PHASE 5

MEMBERS

Alexander Lill Lorenzo Donini

Florian Mauracher Mahmoud Naser

USE-CASES AND VULNERABILITIES



USE-CASES PHASE 1

Usecase	Status
Customer / Employee registration (including sending e-mail with TANs)	WORKING
Customer / Employee login	WORKING
Customer / Employee logout	WORKING
Customer / Employee views bank account details of customer	WORKING
Customer / Employee views transaction history of customer	WORKING
Customer money transfer via HTML form (using TAN)	WORKING
Customer money transfer via uploading transaction batch file (using TAN)	WORKING
Employee approves transfers larger than 10.000 EUR	WORKING
Employee approves registration of customer or of other employee	WORKING
Customer / Employee downloads transaction history of customer as PDF	WORKING
Transaction verification page	WORKING
Search feature for user accounts	WORKING
Employee rejects transfers larger than 10.000 EUR	WORKING
Employee rejects registration of customer or of other employee	WORKING



USE-CASES PHASE 3

Usecase	Status
Password recovery	WORKING
Encrypted TAN generation and delivery via e-mail to customer	WORKING
Download of SCS after registration	WORKING
Transfer using SCS (Single transaction)	WORKING
Transfer using SCS (Batch transaction)	WORKING



VULNERABILITIES PHASE 1

Vulnerability	Status	Vulnerability	Status
Directory listing and file extension handling	FIXED	XSRF	FIXED
HTTPS	FIXED	Session timeout	FIXED
User registration process	PENDING	XSS	FIXED
Weak lockout mechanism	FIXED	SQL injection	FIXED
Bypassing authentication schema	FIXED	Command injection	FIXED
Weak passwords	FIXED	Integer overflow	FIXED
Bypassing authorization schema	FIXED	Business logic data validation	FIXED
Unsecure cookies	FIXED	Process timing	FIXED
Session fixation	FIXED	Application misuse	FIXED
Exposed session variables	FIXED	Upload of malicious files	FIXED
		Clickjacking	FIXED



VULNERABILITIES PHASE 3

Vulnerability	Status
File extension handling	FIXED
User registration process	FIXED
Error codes	FIXED
Weak SSL/TLS cipher	FIXED
Business logic data validation	FIXED
Application mis-use	FIXED





TOP SECURITY

FEATURES

The image features a large, bold, white watermark in the center that reads "TOP SECURITY FEATURES". The background is a dark, almost black, space-themed image showing stars and nebulae. Overlaid on this background is a massive amount of white assembly language code, which is completely illegible due to its size and complexity. The code appears to be a mix of game logic and security-related functions, possibly from a mod or a specific version of a game like Doom. The overall effect is one of a heavily secured or modified software system.

LESSONS LEARNED



COMMAND INJECTION IS EVIL!

The screenshot shows a web application interface for Goliath National Bank (GNB). The top navigation bar includes links for 'Overview', 'My Accounts', and 'Logout'. The main content area features the GNB logo ('GOLIATH NATIONAL BANK') and a welcome message: 'Welcome back, Robin Scherbatsky!'. Below this, a dropdown menu shows 'Selected account: 10000002'. On the left, a sidebar menu lists 'Account Overview', 'New transaction', 'New transaction (multiple)' (which is highlighted with an orange arrow), and 'Transaction History'. The main content area displays a terminal-like output of file upload results:

```
Fileupload successful!
total 216
drwxr-xr-x 28 lorenzodonini staff 952 Nov 19 17:35 .
drwxr-xr-x 12 lorenzodonini staff 408 Nov 19 00:51 ..
-rw-r--r--@ 1 lorenzodonini staff 6148 Oct 28 10:45 .DS_Store
-rw-r--r-- 1 lorenzodonini staff 9 Nov 2 12:39 .gitignore
drwxr-xr-x 10 lorenzodonini staff 340 Nov 19 00:51 accounts
-rw-r--r-- 1 lorenzodonini staff 1392 Oct 30 17:18 authentication.php
-rw-r--r-- 1 lorenzodonini staff 179 Nov 1 19:11 awesome_data.php
-rw-r--r-- 1 lorenzodonini staff 22333 Nov 2 22:39 bankfunctions.php
drwxr-xr-x 4 lorenzodonini staff 136 Nov 3 00:09 client
-rw-r--r-- 1 lorenzodonini staff 4676 Nov 19 17:35 dbheader.php
```



PROJECT MANAGEMENT

- Applications like Trello make life easier
- Agile programming FTW



**APPLY SOFTWARE DESIGN
PRINCIPLES FROM THE BEGINNING!**



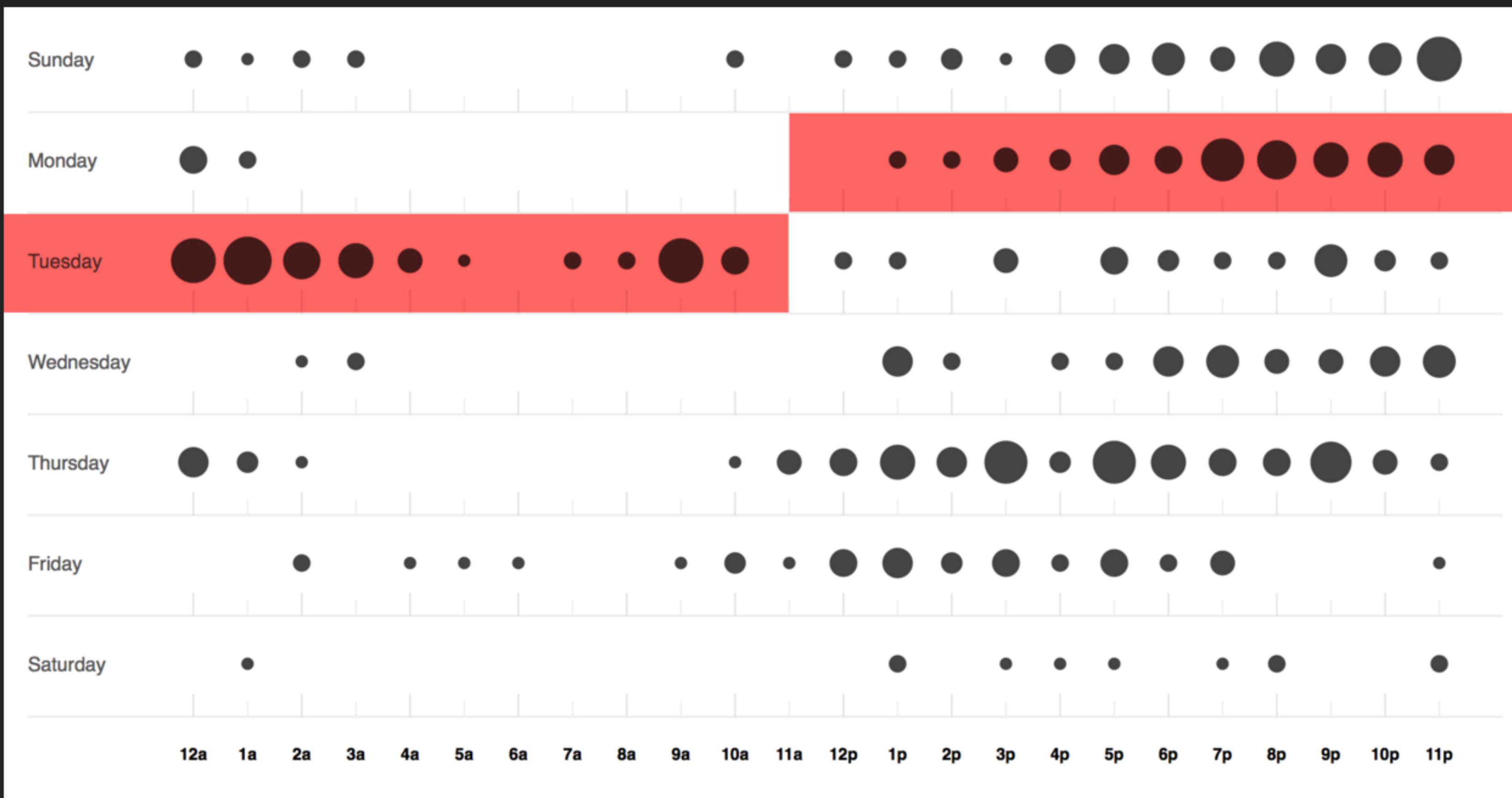
TESTING IN TARGET ENVIRONMENT
IS IMPORTANT

&

AUTOMATED TESTING IS AWESOME



TIME MANAGEMENT?



TEAMWORK



THIS PROJECT IN NUMBERS...

Party pizzas & takeouts	360€
Total amount of commits	460+
Average hours of work per phase	120
Exchanged group messages	3000+
Trello cards	70+
Lame jokes	countless
Days since the beginning of the project	102



DO YOU THINK YOUR APPLICATION IS SECURE?



DO YOU THINK YOUR APPLICATION IS SECURE?



**WOULD YOU PUT YOUR OWN MONEY
IN THE BANK BUILT BY YOUR TEAM?**



CHALLENGE ACCEPTED.



**THANKS FOR YOUR
ATTENTION!**

