

Retail Mobile Application Penetration Testing

Project overview



20 days

For testing



3

Certified ethical
hackers



1

Mobile Application



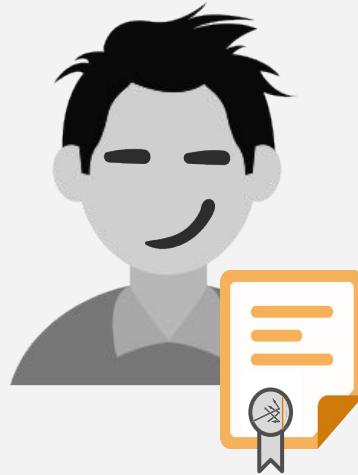
GRAY BOX

Penetration testing

Project Challenge

Technical Goals

- Test Mobile Application with initial access (unprivileged user profile) from attackers' perspective
- Detect and give recommendations on fixing security issues to protect sensitive data, users' money and company reputation



Business Goals

- Evaluate current level of mobile application and platform security
- Identify gaps in current cybersecurity posture and check IT environment for weaknesses
- Provide an accurate evaluation of the security level after remediation phase

Mobile Application overview

iOS & Android cross platform app

Integrations with **Banking Systems**

Production environment with more than 100 000 users

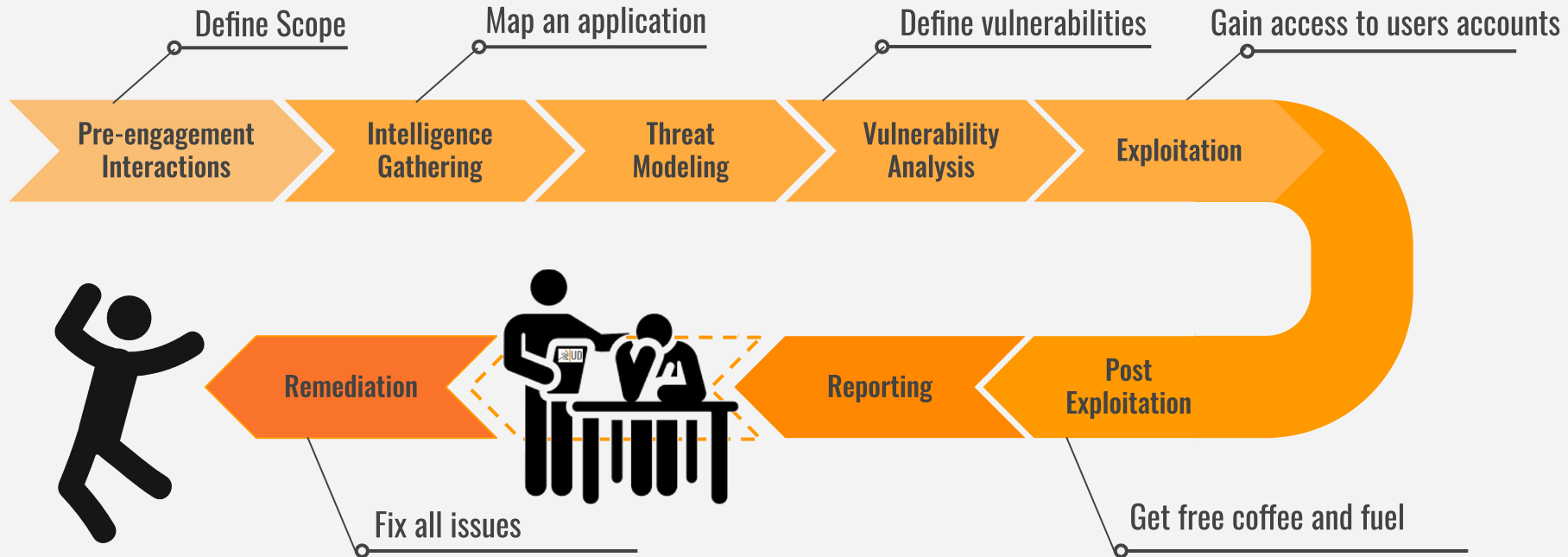


Manage your **bonus points**: accumulate, spend, share

Pay for fuel and coffee on gas stations

Review bonus system partners, **news and updates**

Project Planning and Goals



Found vulnerabilities by severity

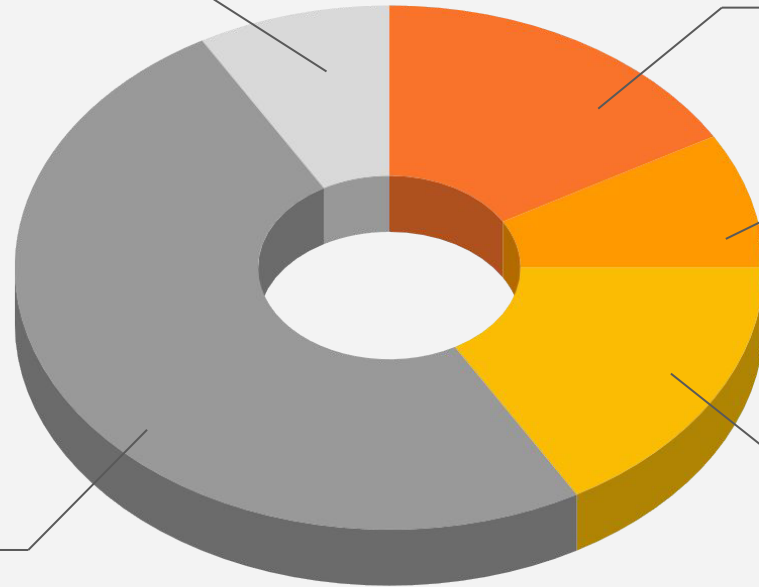
1 Informational

2 Critical

1 High

2 Medium

6 Low



Hacking Scenario: account takeover & funds usage



Attacker...

... gets **list of Users** utilizing an User Enumeration vulnerability...



... checks if user account has **credit card** assigned...



... gains **access to user's account** utilizing vulnerability in password reset functionality ...



... STEALS user's **private data and money** from assigned credit card



Free coffee and fuel



Using found security issues **UnderDefense** Penetration Testing Team was able to collect information about existing users, perform attacks on users' profiles to obtain access to them.

After a compromise of **user's account** we could pay for coffee and fuel with bonuses and also what's more critical with a **debit card** attached to the account.



Project Artifacts

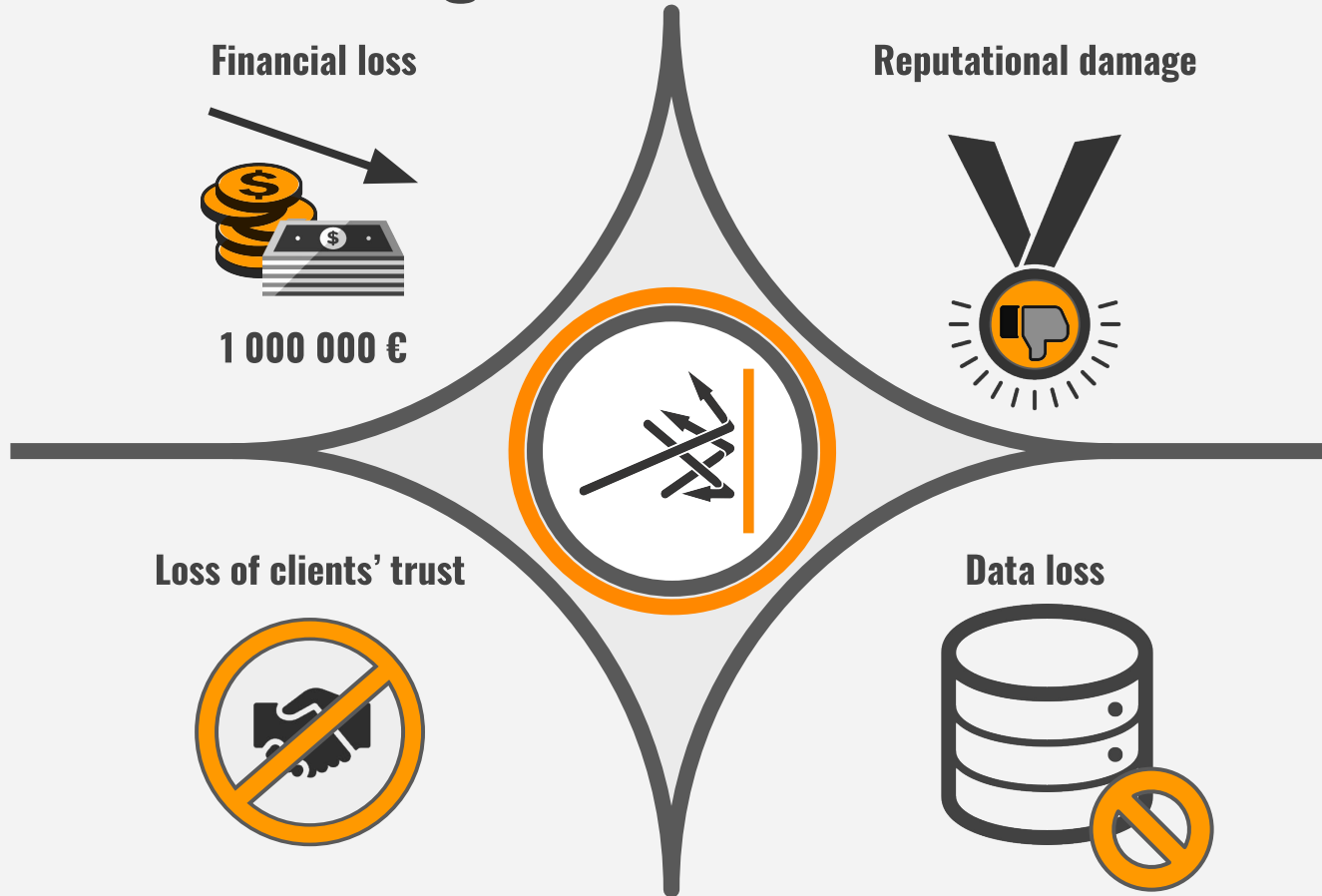
Found **passwords** to profiles

```
Can't login to XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
Found phone with pin 1337: XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
Found phone with pin 1337: XXXXXXXXXXXY  
Can't login to XXXXXXXXXXXX  
Can't login to XXXXXXXXXXXX  
....
```

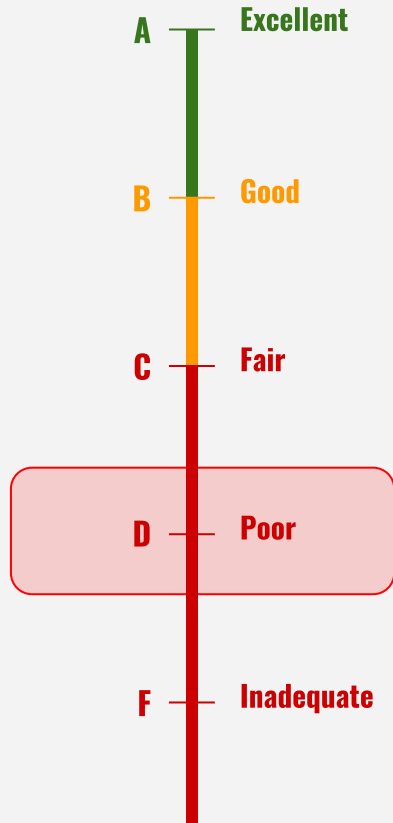
Liters of **coffee and fuel**



Business risks mitigated

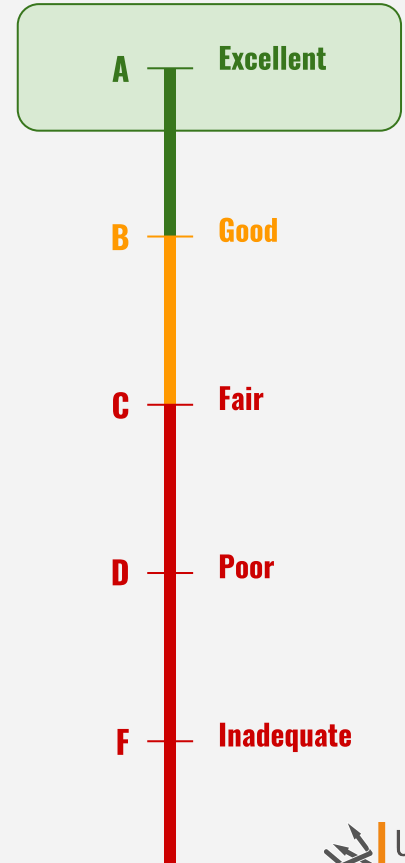


Project Results



UnderDefense has delivered a comprehensive report covering all found vulnerabilities and providing recommendations on the best ways of mitigation

At the end our client was able to meet **the highest** level of compliance and regulation standards, develop better **security** practices and get a big logo on the board assuring customers in a good security posture.



Thank you!



Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau

Tel: (852) 2893 8860
Email: sales@version-2.com.hk

Taiwan

Tel: (886) 02 7722 6899
Email: sales@version-2.com.tw

Singapore, Malaysia & SEA

Tel: (65) 6296 4268
Email: sales@version-2.com.sg