



# Penetration Test Report

Mobile App 'DubMoney'  
of Dubius Payment Ltd.

**EXAMPLE**



# Contents

<b>i</b>	<b>List of changes</b>	<b>3</b>
<b>1</b>	<b>Contact persons</b>	<b>4</b>
1.1	Contact person Dubius Payment Ltd. . . . .	4
1.2	Contact person binsec GmbH . . . . .	4
1.3	About the pentester . . . . .	4
<b>2</b>	<b>Project overview</b>	<b>5</b>
2.1	Introduction . . . . .	5
2.2	Basic conditions . . . . .	5
2.3	Scope . . . . .	6
2.4	Performed tests . . . . .	7
<b>3</b>	<b>Management overview</b>	<b>9</b>
3.1	Summary . . . . .	9
3.2	List of findings . . . . .	10
<b>4</b>	<b>Technical report</b>	<b>11</b>
4.1	Installation of the mobile application on outdated operating systems . . . . .	11
4.2	Missing data deletion in case of multiple failed login attempts . . . . .	12
4.3	Missing memory release after data processing . . . . .	13
<b>5</b>	<b>Appendix A</b>	<b>14</b>
5.1	Classification details . . . . .	14
5.2	Procedure for mobile apps . . . . .	15
5.3	Risk assessment . . . . .	16
5.4	About the binsec GmbH . . . . .	18

## i List of changes

Version	Description	Author	Date
1.0	Report generation	Dominik Sauer	August 5, 2024
1.1	Quality Assurance	QA-Team	August 6, 2024

# 1 Contact persons

## 1.1 Contact person Dubius Payment Ltd.

Damian Westcott  
CEO

✉ d.westcott@dubius-payment.com

Dubius Payment Ltd.  
71 Peachfield Road  
SO53 4NE CHANDLER  
United States

## 1.2 Contact person binsec GmbH

Dominik Sauer  
Head of Penetration Testing

☎ +49 69247560713  
✉ ds@binsec.com

binsec GmbH  
Solmsstraße 41  
60486 Frankfurt am Main  
Germany

## 1.3 About the pentester

Since 2013, Mr. Dominik Sauer has been responsible for the management and implementation of penetration tests at binsec GmbH. He started his career while studying computer science at the Darmstadt University of Applied Sciences and ended his academic career with a very good master's degree in computer science with a specialization in IT security. He also holds the leading certifications in the field of penetration testing and has been an Offensive Security Certified Professional (OSCP) since 2013 and an Offensive Security Certified Expert (OSCE) since 2015.

In addition, he has been a lecturer for teaching at the Darmstadt University of Applied Sciences (HDA) and the TH Mittelhessen University of Applied Sciences (THM) since 2017. For example, he holds courses on penetration testing or digital forensics and supervises theses.

## 2 Project overview

### 2.1 Introduction

The Dubius Payment Ltd. had its mobile application 'DubMoney' subjected to a penetration test. In detail, customers can make transactions via the mobile app. The backend of the mobile application should not be tested because it has already been examined in a previous penetration test.

### 2.2 Basic conditions

The penetration test was conducted between July 29, 2024 and August 9, 2024 performed as an external grey box test, without using aggressive attacking techniques such as DDoS attacks. The complete classification is illustrated in chapter 5.1. The general pentest approach is described in chapter 5.2. All requests were executed from the following IP addresses:

#### IPv4

- » 185.156.254.128/25
- » 217.111.127.122/32
- » 162.55.59.194/32

#### IPv6

- » 2a07:a1c1:1:600::/63
- » 2001:920:1914:3464::/64

## 2.3 Scope

The following installation packages for Android and iOS were provided for the penetration test:

Operating system	Bundle ID	Version	Note
Android	dp.dub.dev	2.6.2 (Dev)	Root detection was implemented.
iOS	dp.dub.dev	2.6.2 (Dev)	Jailbreak detection was implemented.

The apps were installed on the following mobile devices:

Smartphone	OS version	Access authorization
Samsung Galaxy S9	Android 10	The device was rooted.
Pixel 6	Android 14	-
iPhones 12	iOS 16.5.1	A jailbreak was present on the end device.

In order to avoid disruptions in the production environment, the penetration test was carried out in the development environment. The following user accounts were created via the public registry to carry out the penetration test:

- » ds@binsec.com
- » ds+1@binsec.com
- » ds+2@binsec.com

## 2.4 Performed tests

The following pentest tasks were performed on the systems and applications described previously. This list was automatically generated by binsec GmbH's documentation tool.

### Target → Android-App: DubMoney

Result	Task: Reverse Engineering	Findings
✗	Identify required platform version	Page 11
✓	Check whether outdated software components are used by the app	-
✓	Reconstruction of the source code based on the APK	-
✓	Identification of the crypto algorithms used	-
✓	Android Root Detection Bypass	-
✓	Check if the application is debuggable	-
Result	Task: Platform Usage	Findings
✓	Identification of the permissions required by the app	-
✓	Verification that the app is prevented from running on a mobile device without a screen lock	-
✓	Checking whether screen overlay attacks are prevented	-
✓	Checking whether sensitive data is exposed via IPC mechanisms (Inter Process Communication)	-
Result	Task: Code Tampering	Findings
✓	Checking whether the server certificate of a remote endpoint is verified	-
✓	Checking whether JavaScript can be executed in WebViews	-
Result	Task: Data Storage	Findings
✓	Checking whether data backups contain sensitive information	-
✓	Checking whether screen capturing is prevented	-
✗	Checking whether the apps local storage is deleted after multiple failed login attempts	Page 12
✗	Checking the duration of sensitive data in memory	Page 13
✓	Checking whether sensitive data is displayed via the user interface	-
✓	Checking whether the keyboard cache for text input fields is disabled	-
✓	Checking whether sensitive data is written to application logs	-
✓	Checking whether sensitive data is stored insecurely	-

## Target → iOS-App: DubMoney

Result	Task: Reverse Engineering	Findings
✗	Identify required platform version	Page 11
✓	Check whether outdated software components are used by the app	-
✓	iOS Jailbreak detection bypass	-
✓	Identification of the crypto algorithms used	-
✓	Check if the application is debuggable	-
Result	Task: Platform Usage	Findings
✓	Checking whether third-party keyboards can be used	-
✓	Verification that the app is prevented from running on a mobile device without a screen lock	-
✓	Checking whether sensitive data is exposed via IPC mechanisms (Inter Process Communication)	-
Result	Task: Code Tampering	Findings
✓	Checking whether the server certificate of a remote endpoint is verified	-
✓	Checking whether JavaScript can be executed in WebViews	-
Result	Task: Data Storage	Findings
✓	Checking whether data backups contain sensitive information	-
✓	Checking whether screen capturing is prevented	-
✗	Checking whether the apps local storage is deleted after multiple failed login attempts	Page 12
✗	Checking the duration of sensitive data in memory	Page 13
✓	Checking whether sensitive data is displayed via the user interface	-
✓	Checking whether the keyboard cache for text input fields is disabled	-
✓	Checking whether sensitive data is written to application logs	-
✓	Checking whether sensitive data is stored insecurely	-



## 3 Management overview

### 3.1 Summary

The penetration test was conducted between July 29, 2024 and August 9, 2024. During it 6 vulnerabilities were identified which were combined into 3 findings and subjected to an initial risk assessment. As result there is no finding that requires immediate action and 2 findings that require action. The finding of category note is to be understood as a suggestion to increase the security level.

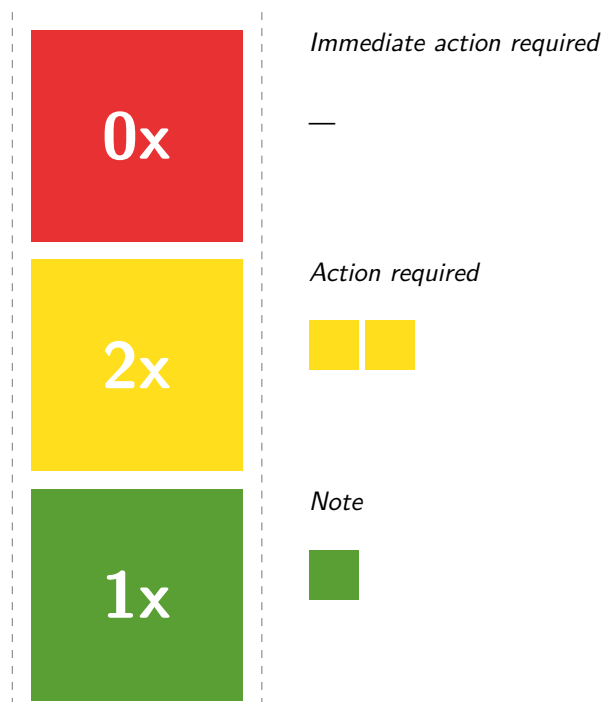











Fig. Risk Overview of Findings




Vulnerabilities in mobile data processing and storage were identified during the penetration test.

### 3.2 List of findings

- # 1  **Not fixed:** *Misconfiguration*  
 The mobile application supports operating systems that are no longer supplied with security updates by the manufacturer. See page 11.  
 **System:** Android, iOS
- # 2  **Not fixed:** *Data Storage*  
 The mobile application does not reset itself in case of multiple failed login attempts for the registered user account. See page 12.  
 **System:** Android, iOS
- # 3  **Not fixed:** *Misconfiguration*  
 The mobile app keeps sensitive data in memory longer than necessary, See page 13.  
 **System:** Android, iOS

## 4 Technical report

### 4.1 Installation of the mobile application on outdated operating systems

	action required
	Damage: high
	Occurrence: low

#### Finding #1

Not fixed

When developing iOS and Android apps, developers have the option of specifying which operating system versions are supported by their app. This is done via specific attributes in the configuration files of the respective app. For iOS apps, the minimum supported operating system version is defined in the 'Info.plist' with the 'MinimumOSVersion' attribute. For Android apps, this is determined in the 'AndroidManifest.xml' by the 'minSdkVersion' attribute. By setting these attributes, it can be ensured that the apps only run on operating system versions that are considered secure and have the APIs required by the app.

The Android and iOS version of the mobile app can run on outdated operating systems that no longer receive updates from the manufacturer:

```
minSdkVersion : '24
```

*Support of Android 7.0*

```
<key>MinimumOSVersion</key>
<string>12.0</string>
```

*Support of iOS 12*

In general, outdated operating systems may have known vulnerabilities. In addition, they no longer receive security updates and may not have up-to-date security features that protect against unauthorized access to sensitive app content.




#### Recommendation

In line with the end-of-life cycles of Android<sup>1</sup> and iOS<sup>2</sup>, only operating systems that receive security updates from the manufacturer should be supported.

<sup>1</sup><https://endoflife.date/android>

<sup>2</sup><https://endoflife.date/ios>

## 4.2 Missing data deletion in case of multiple failed login attempts

	action required
	Damage: medium
	Occurrence: medium

### Finding #2

Not fixed

According to security best practices, the data of a mobile application should be deleted or reset if an incorrect password for the registered user account is entered multiple times. During the penetration test, no counter could be determined that indicates how often an incorrect password can be entered in the mobile app 'DubMoney'. Instead, the data remained on the mobile device even after 15 incorrect login attempts.

### Recommendation

If the password is entered incorrectly several times, the mobile application should reset itself and the user's data on the mobile device should be deleted.

### 4.3 Missing memory release after data processing



note

Damage: warning

Occurrence: low

### Finding #3

Not fixed

According to security best practices, sensitive data should only be kept in memory as long as necessary. Although the password is no longer required by the mobile application after a user logs in, it could be found in main memory despite 5 minutes of user inactivity on the app homescreen:

```
# memory search "54 65 73 74 31 32 33 34 21 61 62 63 64"
Searching for: 54 65 73 74 31 32 33 34 21 61 62 63 64
137b0da8 54 65 73 74 31 32 33 34 21 61 62 63 64 00 00 Test1234!abcd...
137b0db8 98 e7 78 79 00 00 00 00 00 00 00 00 00 00 00 ...xp.....
137b0dc8 58 6a 80 79 00 00 00 00 02 00 00 00 08 ff ba 70 Xj.p.....
Pattern matched at 1 addresses
```

Successful search for user password 'Test1234!abcd'

```
Using USB device `iPhone`
Agent injected and responds ok!
```

```
(object)inject(:ipn, v1.11.a)
```

Runtime Mobile Exploration  
by: @leonjza from @sensepost

```
# memory search "54 65 73 74 31 32 33 34 21 61 62"
```

```
# memory search "54 65 73 74 31 32 33 34 21 61"
Searching for: 54 65 73 74 31 32 33 34 21 61 62
```

```

Searching for: 54 65 73 74 31 32 33 34 21 61 62
12bde6820 54 65 73 74 31 32 33 34 21 61 62 63 64 00 00 ed Test1234abcd...
12bde6830 1b cb af fb a1 25 00 00 00 00 00 00 00 00 00 00 .....%.....
12bde6840 7c fa 35 81 82 00 00 00 00 67 68 82 82 00 00 00 .....5.....g.....
20808c850 54 65 73 74 31 32 33 34 21 61 62 63 64 00 00 00 Test1234abcd...
20808c890 1f 64 65 2d 44 45 2d 28 75 75 6c 6c 29 2d 30 2d ..de-DE-(null)-0-
20808c8a0 59 4f 54 48 4f 55 54 2d 44 65 66 61 75 6c 74 73 WITHOUT-Defaults

Pattern matched at 2 addresses

```

Successful search for user password 'Test1234!abcd'

The RAM analysis was performed for both Android and iOS using the runtime mobile exploration toolkit 'objection'<sup>3</sup>, which requires administrative access to the mobile devices.

## Recommendation

The data objects should be overwritten after processing and then deleted.

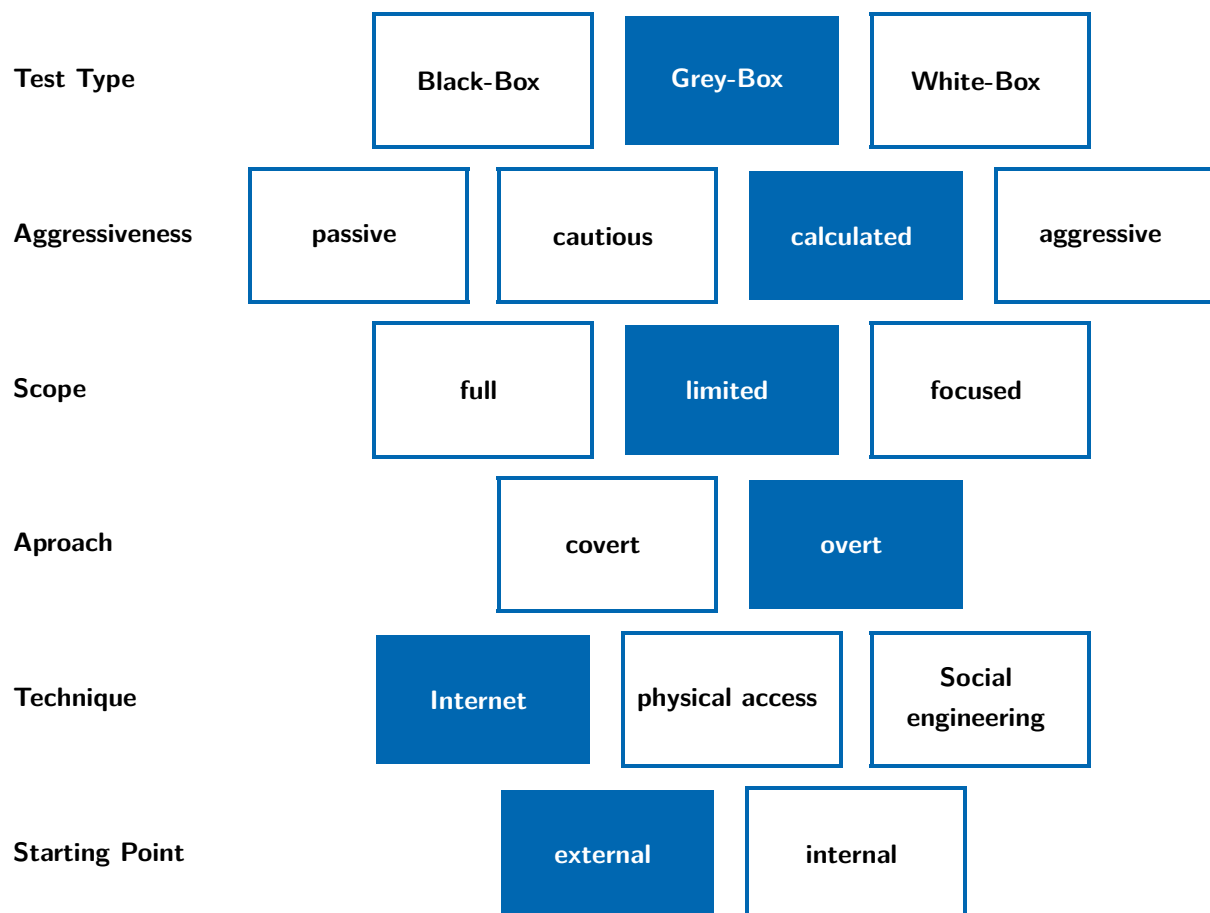
<sup>3</sup><https://github.com/sensepost/objection>

## 5 Appendix A

### 5.1 Classification details

In cooperation with Dubius Payment Ltd., the following classification variant was agreed as the approach: The penetration test was performed as an external grey box test, without using aggressive attacking techniques such as DDoS attacks.

Pursuant to the study “Implementation Concept for Penetration Tests“ by the German Federal Office for Information Security (BSI), binsec GmbH used the following classification for this penetration test:



## 5.2 Procedure for mobile apps

The test method used by binsec GmbH for mobile applications is based on the OWASP Mobile Application Security Testing Guide and the OWASP Mobile TOP 10. The Open Web Application Security Project (OWASP) is currently the world's largest non-profit organisation, the objective of which is to increase the security of applications. The OWASP Mobile Top 10 includes the ten most critical vulnerabilities in mobile applications. According to the current release from 2024, one of the most common vulnerabilities is the insecure storage of sensitive data, such as user passwords in a configuration file. Unless otherwise requested, we also include the APIs of a mobile application in our penetration test.

### Methods of approach

The methodical test approach of binsec GmbH is roughly divided into the following test phases. Within the test phases, the mobile application is examined for the vulnerabilities of the OWASP Mobile TOP 10. Various analysis tools are used during the pentest, as well as intensive manual testing. The exact course of the penetration test depends heavily on the characteristics of the respective application and is based on the approach a real attacker would take. In order to gain full control over the communication and access to the data storage, we try to circumvent protection mechanisms such as an implemented jailbreak/root detection or HTTP pinning of public keys:

1. Setting up a test environment
2. Reverse engineering & manipulation of the source code
3. Verification of the platform usage
4. Secure data storage & communication
5. Checking the server-side protection mechanisms

## 5.3 Risk assessment

Binsec GmbH considers the term “risk” to mean a combination of the probability of occurrence of a vulnerability (or the likelihood of its exploitation) and the possible extent of damage. The probability of occurrence or the probability of exploitation of a security gap in IT systems essentially depends on these factors:

- How easily can the vulnerability be identified? (Visibility)
- Are there any exploits for this vulnerability available, or is the attacker required to have a certain level of knowledge to exploit them? (Exploitability)
- Does the exploitation require special rights? (Privilege Escalation)
- Is a combination with other security holes required? (Vulnerability Chaining)
- Is human interaction necessary for the vulnerability? (Social Engineering)

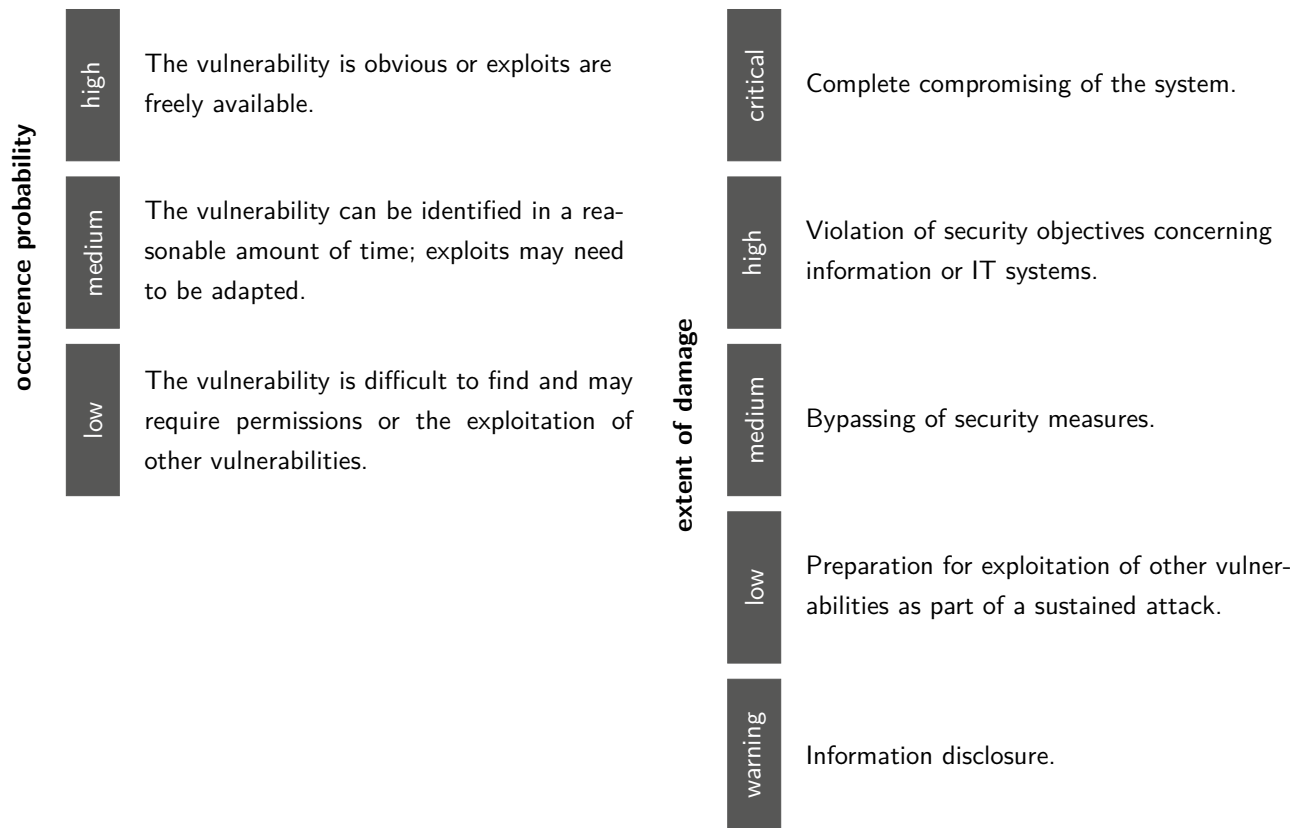
The following classifications are decisive for the possible extent of damage:

1. Financial damage
2. Complete compromising of the system
3. Violation of security objectives related to data or user accounts:
  - a) Confidentiality
  - b) Availability
  - c) Integrity
4. Bypassing of security measures
5. Information disclosure

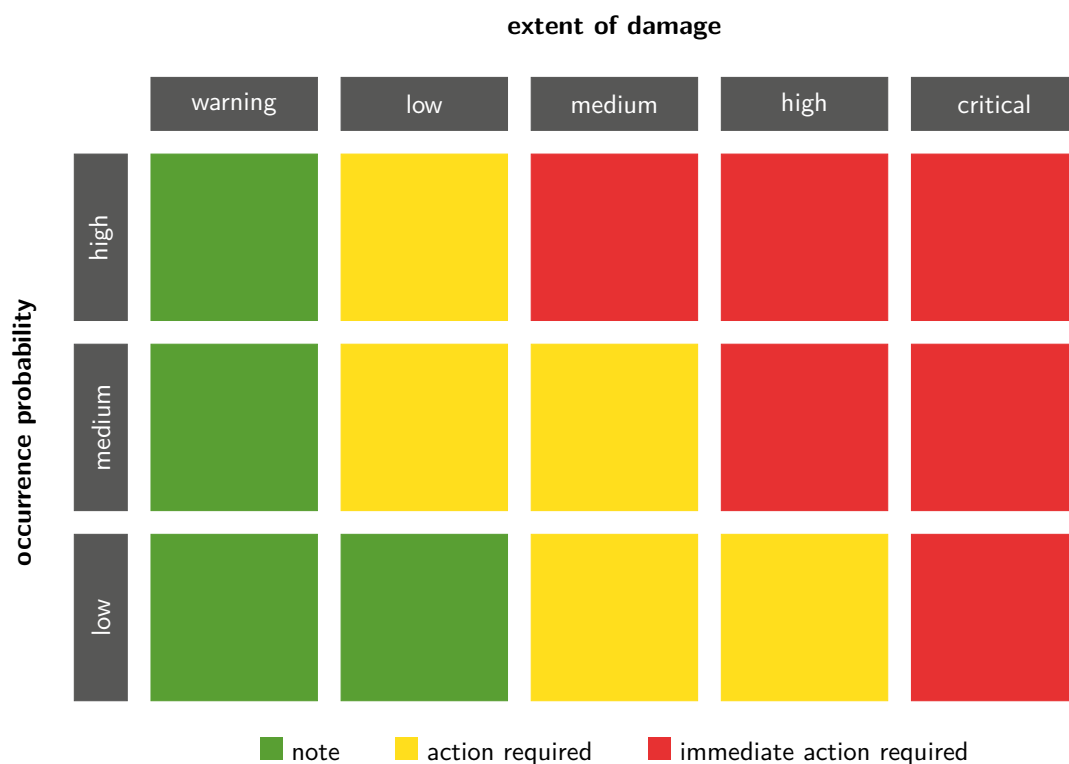
Taking into account both the probability of occurrence and the potential extent of damage, the penetration tester makes a subjective assessment of the risk for each vulnerability found. We recommend taking an own assessment of the vulnerabilities.



The assessment is subject to the following classification:



The risk classification entails a priority for action.



## 5.4 About the binsec GmbH

We are a company that specializes in IT penetration testing, located at Frankfurt am Main, Germany. Since 2013, carrying out technical security analyses of IT infrastructures, web applications, APIs, mobile apps (Android / iOS), etc. has been the core of our daily work. As an owner-managed company, the long-term satisfaction of our customers is of great importance. The certifications of our employees, the teaching activities at universities and our pentesting experience speak for themselves.



binsec GmbH  
Solmsstraße 41  
60486 Frankfurt am Main  
Germany

✉ info@binsec.com  
☎ +49 69 2475607-0

Managing Director: Patrick Sauer  
Authorised Officers: Dominik Sauer, Florian Zavatzki

Commercial Register: Frankfurt a.M. HRB 97277  
VAT ID no.: DE290966808