Account Enumeration Vulnerability: `MAXIMA Eesti app (iOS/Android)`

Gregor Eesmaa
gregor.eesmaa@ut.ee
University of Tartu

June 21, 2025

1 Introduction

Account enumeration is a security vulnerability enabling attackers to determine if specific user accounts exist on a service. The vulnerability usually lies in the account registration functionality of a service, where an error message is returned, indicating that a user with the specified account identifier is already registered. However, an online service can also leak this information in other, more subtle ways, which are often overlooked by software developers. For example, even without a direct message, small visual differences in responses, or slight variations in how the server behaves (like the exact data returned) for existing versus non-existing accounts, can still reveal if an account is registered.

On 2025-06-18, we reassessed `MAXIMA Eesti app (iOS/Android)` and found that **the service is still vulnerable to account enumeration**.

If the account identifier of an online service is personal data (e.g. email address, personal code etc), then the fact, whether it is associated to an account, is also considered personal data. Any disclosure of personal data to third parties without a legal basis constitutes a data breach [1].

We advise you to investigate the potential data breach, and notify the supervisory authority and the affected data subjects, if necessary. Detailed guidelines for mitigating this type of flaw are available in [2].

2 Vulnerabilities Found

We tested the login form, password reset form, account registration form and email change form of `MAXIMA Eesti app (iOS/Android)`. No issues appeared on the login form, password reset form and email change form. However, we identified security issues on the account registration form. Same vulnerabilities were found on iOS and Android. The vulnerabilities found are described in more detail in subsections below.

2.1 Account Registration Form

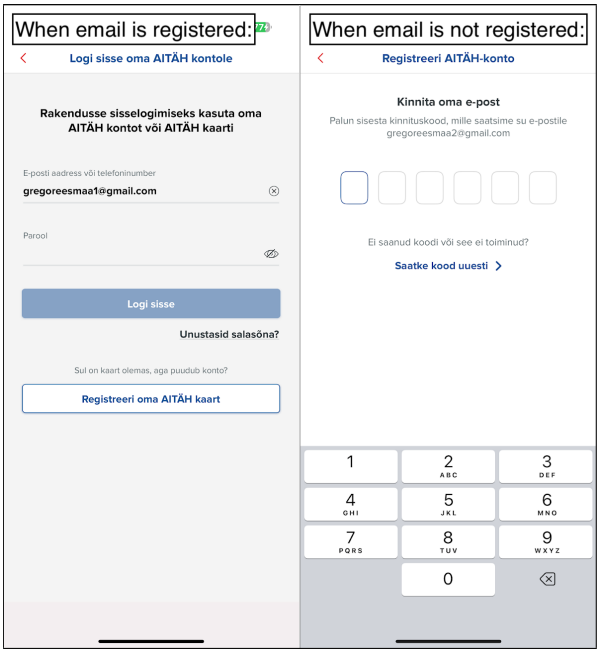

Figure 1: The vulnerability in the account registration form

The account registration form is susceptible to account enumeration attacks. This is because when the provided email address is already taken, the resulting view appears visually different, compared to when the email is not taken (see Figure 1).

It is also crucial to eliminate any side-channels that an attacker could exploit to differentiate between account existence and non-existence. For example, the response should not be faster for an existing account than for an email with which an account does not exist.

To mitigate the flaw, the response must be uniform for both registered and unregistered email addresses. This uniformity must apply to the message displayed to the user as well as the underlying HTTP response details (like status codes, headers, and body content).

For example, the indistinguishable user-facing message could be: "We have sent further instructions to the provided email address". Send an email in both cases, but differentiate the content based on account existence. For example, for new registration, provide means for account activation, and for existing accounts, provide means for account recovery. [2]

About This vulnerability report is part of an ongoing study on user enumeration vulnerabilities in Estonian online services. The study is conducted by the University of Tartu master's student Gregor Eesmaa (supervised by Arnis Paršovs - arnis.parsovs@ut.ee). The findings of this study will be published in a master's thesis scheduled for defence in August 2025.

References

[1] European Union. *General Data Protection Regulation (GDPR): Regulation (EU) 2016/679*. Official Journal of the European Union, L 119/1. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[2] OWASP. *Authentication Cheat Sheet - Authentication and Error Messages*. Accessed: 2025-01-26. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#authentication-and-error-messages.