Account Enumeration Vulnerability: `zalando.ee`

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

March 16, 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 email address is already registered. However, an online service can also leak this information in other, more subtle ways, which are often overlooked by software developers.

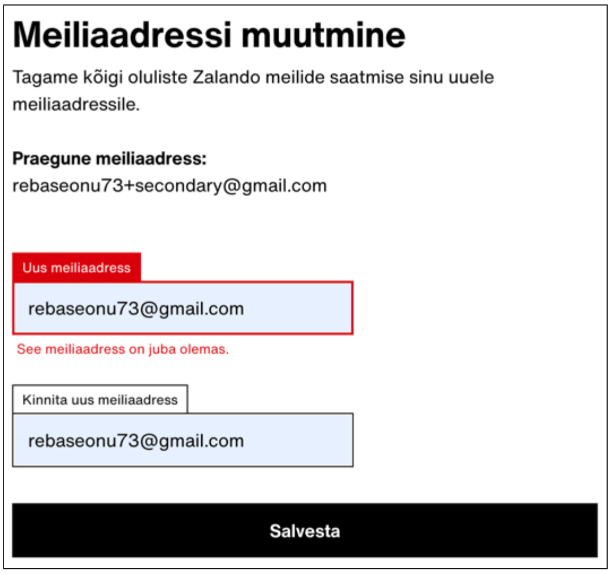
On 2025-01-04, we tested `zalando.ee` and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific email address is registered with the service.** Disclosing such information to third parties constitutes a data breach, as an email address and the fact of whether its holder has an account with an online service are considered personal data, and may be disclosed to third parties only if there is a legal basis for doing so [1].

We advise you to investigate the potential data breach, and notify the supervisory authority and the affected data subjects, if necessary. After **2025-04-15**, we will reassess the service and notify the Estonian Data Protection Inspectorate in case the vulnerability has not been mitigated. Detailed guidelines for mitigating this type of flaw are available in [2].

2 Vulnerabilities Found

We tested the email change form of `zalando.ee`. It was vulnerable to account enumeration. Additionally, we found that the first step of the combined authentication flow that directs forward to account creation and user login is also vulnerable to account enumeration. The vulnerabilities found are described in more detail in subsections below.

2.1 Email Change Form



Meiliaadressi muutmine

Tagame kõigi oluliste Zalando meilide saatmise sinu uuele meiliaadressile.

Praegune meiliaadress:
rebaseonu73+secondary@gmail.com

Uus meiliaadress: rebaseonu73@gmail.com

See meiliaadress on juba olemas.

Kinnita uus meiliaadress: rebaseonu73@gmail.com

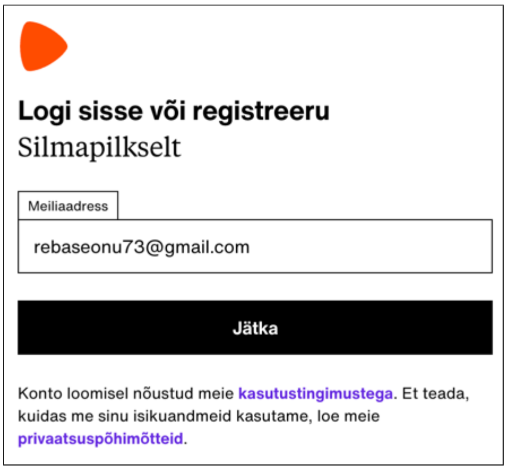
Figure 1: The vulnerability in the email change form

The email change form is susceptible to account enumeration attacks. This is because when the provided email address is already taken, the form shows an error message (see Figure 1). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these attacks [3].

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, return the same message whether the email is registered or not. For example, the message could read as follows: “We have sent further instructions to the provided new email address”. Send an email in both cases, but differentiate the content based on account existence. For example, if the email is unused, provide means for confirming the new email, but if the email is used, provide means for account recovery.

2.2 Authentication Flow



Logi sisse või registreeru

Silmapilkselt

Meiliaadress: rebaseonu73@gmail.com

Konto loomisel nõustud meie kasutustingimustega. Et teada, kuidas me sinu isikuandmeid kasutame, loe meie privaatsuspõhimõtteid.

Figure 2: The first step of the authentication flow

The first step of the authentication flow is also susceptible to account enumeration attacks (see Figure 2). This is because when an account with the email does not exist, the step directs the user to create a new account. However when an account with the email exists, the step instead directs the user to log in form.

Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these attacks.

The registration form normally sends a confirmation email to the email owner on complete successful submission. However, the first step of the flow relies on a separate request before the complete form could be submitted. This allows the attacker to verify registered email addresses, ensuring that the email owner remains unaware of the potential attack.

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, separate the login and registration flows. On the login form, ensure indistinguishable error messaging for both cases of unregistered email and incorrect password. For example, always return the message “Email or password is incorrect”. On the password reset page, ensure same messaging whether the email is registered or not. For example, the message could read as follows: “A password reset link has been sent if an account with this email exists”. [2]

On the registration form, ensure no errors are shown for already used emails. For example, the message after form submission could read as follows: “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]

3 Security Contacts

A valid `security.txt` [4] file was not found on `zalando.ee`. We recommend implementing a `security.txt` file to ensure any future security issues can be reported to the appropriate contact person. In its absence, we have taken the following actions:

- The email address `privaatsus@zalando.ee` was found in the privacy policy of `zalando.ee` and this report was sent to this email address.

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 May 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`.

[3] OWASP. *Authentication Cheat Sheet - Protect Against Automated Attacks*. Accessed: 2025-01-26. URL: `https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#protect-against-automated-attacks`.

[4] EdOverflow and Yakov Shafranovich. *security.txt – A proposed standard which allows websites to define security policies*. Accessed: 2025-01-26. URL: `https://securitytxt.org/`.