

Account Enumeration Vulnerability: **kaup24.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.

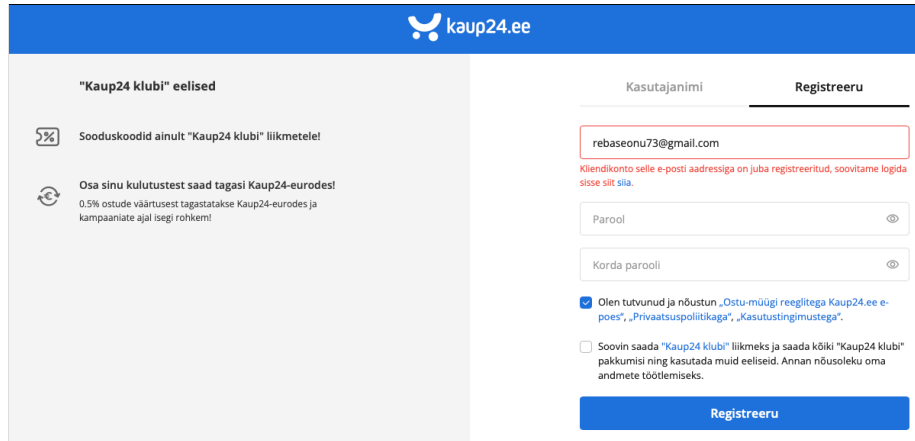
On 2025-02-03, we tested **kaup24.ee** and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific email address is registered with the service.** Disclosing such information to third parties constitutes a data breach, as 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 login form, password reset form, account registration form and email change form of **kaup24.ee**. No issues appeared on the login form and password reset form. However, we identified security issues on the account registration form and email change form. The vulnerabilities found are described in more detail in subsections below.

2.1 Account Registration Form



The screenshot shows the Kaup24 account registration page. On the left, there is a section titled "Kaup24 klubi" eelised (Kaup24 club benefits) with two bullet points: "Sooduskoodid ainult 'Kaup24 klubi' liikmetele!" (Discount codes only for 'Kaup24 club' members!) and "Osa sinu kulutustest saad tagasi Kaup24-eurodes!" (Part of your expenses will be returned to you in Kaup24 euros!). On the right, there is a registration form with the title "Kasutajanimi" (Username) and "Registreeru" (Register). The form contains a text input field for the email address, which has the value "rebaseonu73@gmail.com". Below this field, a red error message reads: "Kliendikonto selle e-posti aadressiga on juba registreeritud, soovitame logida sisse siit siia." (A client account with this email address is already registered, we recommend logging in here). Below the email field are two password fields: "Parool" (Password) and "Korda parooli" (Repeat password). There are two checkboxes: the first is checked and reads "Olen tutvunud ja nõustun „Ostu-müügi reeglitega Kaup24.ee e-poes“, „Privaatsuspoliitikaga“, „Kasutustingimustega“." (I have read and agree with the "Purchase-Sale rules on Kaup24.ee e-shop", "Privacy policy", "Terms of use"); the second is unchecked and reads "Soovin saada 'Kaup24 klubi' liikmeks ja saada kõiki 'Kaup24 klubi' pakkumisi ning kasutada muid eeliseid. Annan nõusoleku oma andmete töötlemiseks." (I want to become a 'Kaup24 club' member and receive all 'Kaup24 club' offers and use other benefits. I give my consent for the processing of my data). At the bottom right is a blue button labeled "Registreeru".

Figure 1: The vulnerability in the account registration form

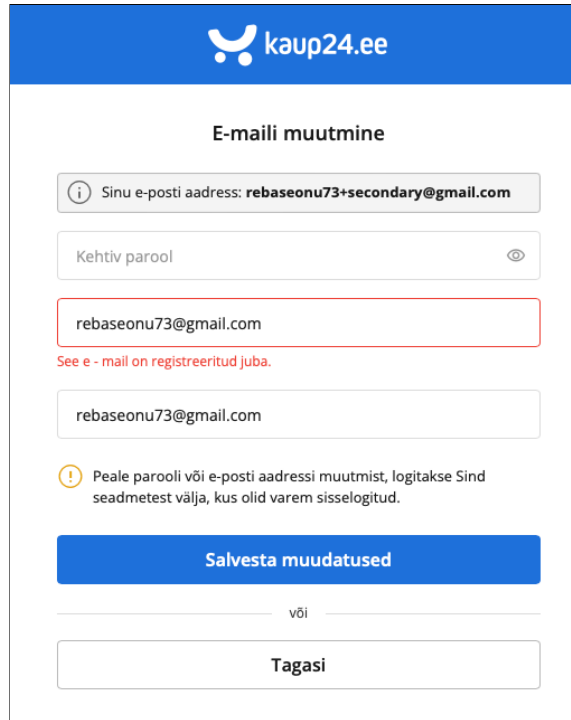
The account registration form is susceptible to account enumeration attacks. This is because when the provided email address is already taken, the form shows an error message (see Figure 1). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate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

The form normally sends a confirmation email to the email owner on successful submission. However, by introducing validation errors in the form, an attacker can determine whether an email address is already registered, without successfully submitting the form. This allows the attacker to also verify unregistered email addresses without triggering a confirmation email, thereby 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, 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 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]

2.2 Email Change Form



The screenshot shows the 'E-maili muutmine' (Email Change) form on kaup24.ee. At the top, the current email address is 'rebaseonu73+secondary@gmail.com'. Below it is a password field labeled 'Kehtiv parool'. The new email address field contains 'rebaseonu73@gmail.com' and is highlighted with a red border. Below this field, a red error message reads: 'See e - mail on registreeritud juba.' (This e-mail is already registered). Below the error message is a confirmation field containing the same new email address. A warning icon and message state: 'Peale parooli või e-posti aadressi muutmist, logitakse Sind seadmetest välja, kus olid varem sisselogitud.' (After changing the password or e-mail address, you will be logged out of the devices where you were previously logged in). At the bottom, there is a blue button 'Salvesta muudatused' (Save changes), a separator 'või' (or), and a button 'Tagasi' (Back).

Figure 2: The vulnerability in the email change form

The email change form is also susceptible to account enumeration attacks. This is because when the provided email address is already taken, the form shows an error message (see Figure 2). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these attacks [3].

The form normally sends a confirmation email to the email owner on successful submission. However, by introducing validation errors in the form, an attacker can determine whether an email address is already registered, without successfully submitting the form. This allows the attacker to also verify unregistered email addresses without triggering a confirmation email, thereby 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, 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.

3 Security Contacts

A valid `security.txt` [4] file was not found on `kaup24.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 `andmekaitse@kaup24.ee` was found in the privacy policy of `kaup24.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/>.