

Account Enumeration Vulnerability: **city24.ee**

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

March 23, 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 **city24.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 **city24.ee**. We identified security issues in all of these functionalities. The vulnerabilities found are described in more detail in subsections below.

2.1 Login Form

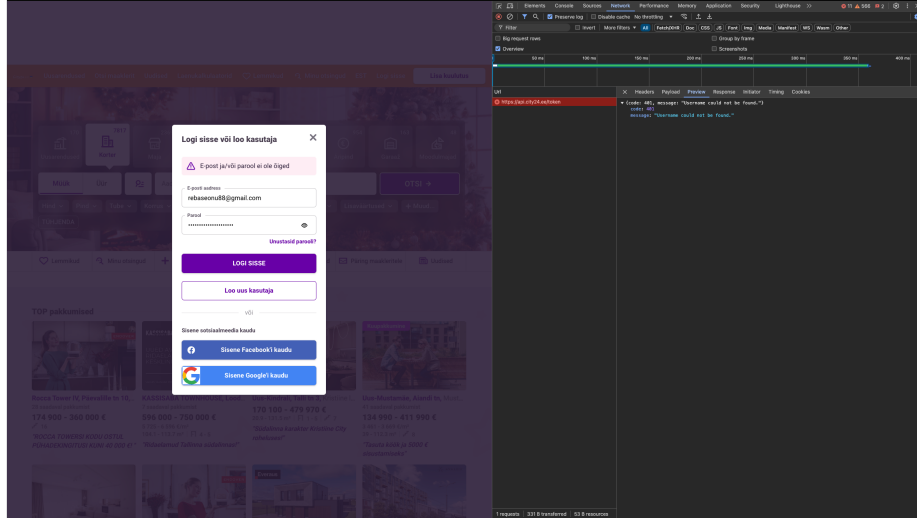


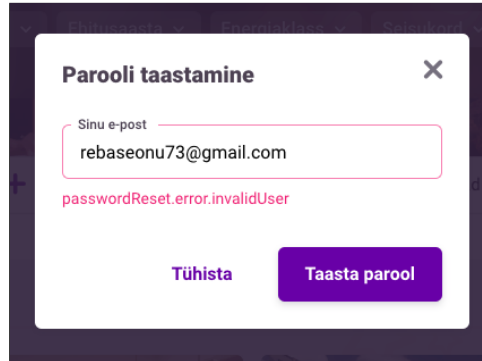
Figure 1: The vulnerability in the login form

The login form is susceptible to account enumeration attacks. This is because when a user with the provided email does not exist, there are subtle differences in the response received from the server compared to when the password is incorrect (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 error message whether the email is registered or not. For example, always return the message “Email or password is incorrect”. [2]

2.2 Password Reset Form



The image shows a web form titled "Parooli taastamine" (Password Reset) with a close button (X) in the top right corner. Below the title is a label "Sinu e-post" (Your email) followed by a text input field containing the email address "rebaseonu73@gmail.com". Below the input field, a red error message reads "passwordReset.error.invalidUser". At the bottom of the form, there are two buttons: a light blue button labeled "Tühista" (Cancel) and a dark blue button labeled "Taasta parool" (Reset password).

Figure 2: The vulnerability in the password reset form

The password reset form is also susceptible to account enumeration attacks. This is because when a password reset is requested for an email address that is not registered with the service, 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].

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: “A password reset link has been sent if an account with this email exists”. [2]

2.3 Account Registration Form

Uus kasutaja

E-posti aadress
rebaseonu73@gmail.com

See e-posti aadress on juba kasutusel

Ees- ja perekonnanimi
Rebase Onu

Telefon
+372 58632178

Parool
.....

Parool peab olema vähemalt 8 tähtemärki

☒ Nõustun City24.ee privaatsuspoliitika ja kasutustingimustega

☐ City24 uudiskiri

Veebileht on kaitstud reCAPTCHA-ga ja sellele kohanduvad Google Google Privaatsuspoliitika ja Kasutamistingimused.

Loo kasutaja

Figure 3: The vulnerability in the account registration form

The account registration 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 3). 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 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]

2.4 Email Change Form

The screenshot shows the 'Email' section of the City24.ee website. It contains three input fields, all with the value 'rebaseonu74@gmail.com':

- E-post**: The first field, with a grey border.
- Uus email**: The second field, with a pink border. Below it is a red error message: "See e-posti aadress on juba kasutusel".
- Korda emaili**: The third field, with a grey border.

Below the fields is a note: "* Kontaktemail on Sinu kasutajatunnus sisselogimiseks. Emaili muutes tuleb konto uuesti aktiveerida ja sisse logida uue aadressiga." At the bottom right are two buttons: "Tühista" (grey) and "Salvesta" (purple). At the bottom left is a link: "Minu tellimused".

Figure 4: 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 4). 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.

3 Security Contacts

A valid `security.txt` [4] file was not found on `city24.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 `klienditugi@city24.ee` was found in the privacy policy of `city24.ee` and this report was sent to this email address on 2025-03-16, with no confirmation of receipt received to date.
- The email address `Karin.Noppel@city24.ee` was found in the relevant business registry 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/>.