

Account Enumeration Vulnerability: **aboutyou.ee**

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

May 31, 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 2025-04-26, we reassessed **aboutyou.ee** 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 **aboutyou.ee**. No issues appeared on the login form. However, we identified security issues on the password reset form, account registration form and email change form. The vulnerabilities found are described in more detail in subsections below.

2.1 Password Reset Form

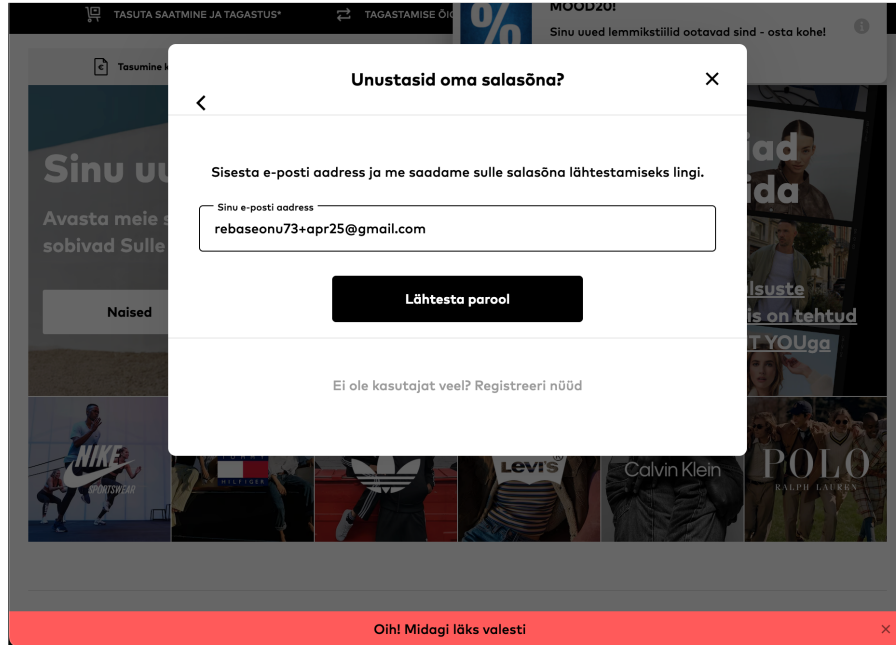


Figure 1: The vulnerability in the password reset form

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

2.2 Account Registration Form

The screenshot shows a web form titled "Logi sisse" (Login) with a close button (X) in the top right corner. The form has two main sections: a top section for login and a bottom section for registration. The top section contains a "Registreeri" (Register) button and a "Logi sisse" (Login) button. Below these are two buttons for social media login: "Registreeru platvormilt Apple" and "Registreeru platvormilt Facebook". The bottom section is for registration and contains several fields and options. It starts with a heading "Või kasuta oma e-posti aadressi" (Or use your email address). Below this are four input fields: "Eesnimi" (First name) with the value "Rebase", "Perekonnanimi" (Last name) with the value "Onu", "Sinu e-posti aadress" (Your email address) with the value "rebaseonu73@gmail.com", and "Salasõna (min. 6 tähtemärki)" (Password) with a masked value "*****" and a "näita" (show) link. Below the password field is a question "Kuidas sooviksid, et pöörduksime Sinu poole?" (How would you like us to contact you?) with four radio button options: "Pr." (selected), "Hr.", "Mitmesugust", and "Määramata". Below this is a checkbox "Soovin saada uudiskirju ABOUT YOU-lt praeguste trendide, pakumiste ja kupongide kohta vastavalt veebilehele Privatsuspoliitika. Te saate oma nõusoleku igal ajal... Näita rohkem" (I want to receive newsletters from ABOUT YOU about current trends, offers and coupons according to the website's Privacy Policy. You can revoke your consent at any time... Show more). Below the checkbox is a red error message "Selle e-posti aadressiga rebaseonu73@gmail.com on juba konto olemas." (An account already exists with this email address). Below the error message is a link "Unustasid oma salasõna? või liigu otse sisse logimis?" (Forgot your password? or go directly to login?). At the bottom of the form is a green "Success!" message with a checkmark icon and a "Registreeri nüüd" (Register now) button. The Cloudflare logo is also visible in the bottom right corner.

Figure 2: 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 2).

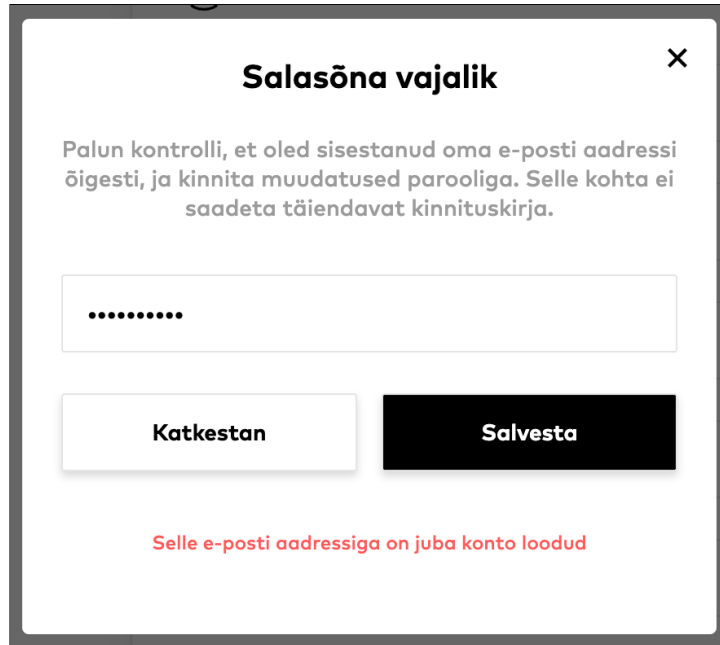
Moreover, no confirmation email is sent to the provided email address after this form is submitted. This allows the attacker to verify unregistered email addresses, ensuring that the email owner remains unaware of the potential attack.

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, 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]

2.3 Email Change Form



Salasõna vajalik ✕

Palun kontrolli, et oled sisestanud oma e-posti aadressi õigesti, ja kinnita muudatused parooliga. Selle kohta ei saadeta täiendavat kinnituskirja.

.....

Katkestan **Salvesta**

Selle e-posti aadressiga on juba konto loodud

Figure 3: 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 3). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these attacks [3].

Moreover, no confirmation email is sent to the provided email address after this form is submitted. This allows the attacker to verify unregistered 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, 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 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.

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.
- [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.