

Account Enumeration Vulnerability: `ohtuleht.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 2024-11-18, we tested `ohtuleht.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 `ohtuleht.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. Additionally, we tested the subscription sharing form. The vulnerabilities found are described in more detail in subsections below.

2.1 Account Registration Form

Loo Õhtulehe konto

Õhtulehe konto on vajalik Õhtuleht Kirjastuse digipaketi ligipääsuks.

Facebook Apple Google

Või kasuta konto loomiseks e-posti:

rebaseonu73@gmail.com

Sama e-postiga kasutaja on juba registreeritud

.....

Jätkates nõustun, et olen tutvunud üldtingimustega ja andmekaitsetingimustega ning et minu andmeid kasutatakse konto loomiseks ja säilitamiseks.

☐ Annan Õhtuleht Kirjastus AS-ile õiguse töödelda minu e-posti aadressi ja telefoni pakkumiste ja uudiskirjade saatmiseks.

LOO ÕHTULEHE KONTO

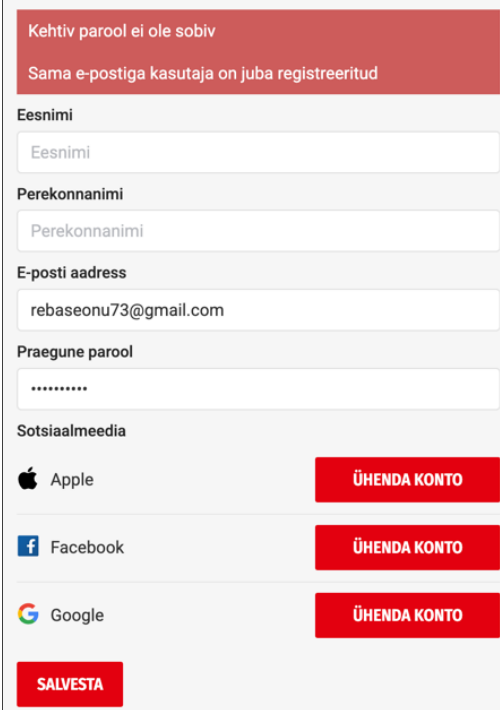
Figure 1: The vulnerability in the account registration form

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).

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 a web form for changing an email address. At the top, a red error banner contains the text: "Kehtiv parool ei ole sobiv" (Invalid password) and "Sama e-postiga kasutaja on juba registreeritud" (A user with the same email is already registered). Below this, the form has several input fields: "Eesnimi" (First name) with the placeholder "Eesnimi", "Perekonnanimi" (Last name) with the placeholder "Perekonnanimi", "E-posti aadress" (Email address) with the value "rebaseonu73@gmail.com", and "Praegune parool" (Current password) with masked characters "*****". Under the heading "Sotsiaalmeedia" (Social media), there are three options: Apple, Facebook, and Google, each with a corresponding icon and a red button labeled "ÜHENDA KONTO" (Connect account). At the bottom left is a red button labeled "SALVESTA" (Save).

Figure 2: The vulnerability in the email change form

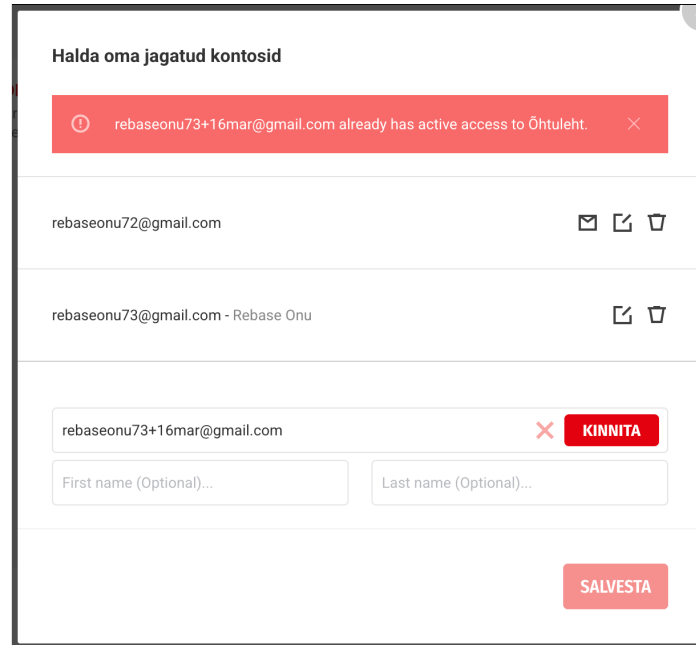
The email change form is also susceptible to account enumeration attacks. This is because when the provided email address is already taken, the form shows an error message (see Figure 2). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these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

No confirmation email is sent to the provided email address after this form is submitted. Additionally, by introducing validation errors in the form, the attacker can avoid submitting the form altogether. These shortcomings allow 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, 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.

2.3 Subscription Sharing Form



The screenshot shows a web form titled "Halda oma jagatud kontosid". At the top, a red error message states: "rebaseonu73+16mar@gmail.com already has active access to Õhtuleht". Below this, there is a list of email addresses with associated icons (envelope, share, trash). The list includes "rebaseonu72@gmail.com" and "rebaseonu73@gmail.com - Rebase Onu". A search input field contains "rebaseonu73+16mar@gmail.com", with a red "X" and a "KINNITA" button next to it. Below the search field are two optional text boxes for "First name (Optional)..." and "Last name (Optional)...". At the bottom right is a red "SALVESTA" button.

Figure 3: The vulnerabilities in the subscription sharing form

The subscription sharing form is also susceptible to account enumeration attacks, with additional data leaking about the existing accounts. This is because when an account with the email exists, the form shows their first and last names or an alert about them already having a subscription (see Figure 3).

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

Moreover, no confirmation email is sent to the provided email address after this form is submitted. This is because the email validation is done with a separate request for each email entered. Such behaviour 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, return the same information whether the email is registered or not, and whether they already have a subscription or not. For example, there could be a message that reads as follows: “We have sent further instructions to the provided email address”. Send an email in all cases, but differentiate the content based on account existence and existing subscriptions. For example, if the email is unregistered, provide means for creating an account; if the email is registered but has no subscriptions, provide means to activate the subscription; if the email is registered and has an active subscription, inform them of the existing subscription.

3 Security Contacts

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