

# Account Enumeration Vulnerability: `postimees.ee`

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

May 18, 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.

On 2025-05-10, we reassessed `postimees.ee` and found that despite significant changes, **the service is still vulnerable to account enumeration**. Since the initial findings have been already addressed, this report will now highlight the more subtle residual hints of account existence that were identified. 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.

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. After **2025-06-17**, 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 `postimees.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. Additionally, we tested the subscription sharing form. The vulnerabilities found are described in more detail in subsections below.

## 2.1 Password Reset Form


Path	When email is registered:	Response
 /api/piano/reset-account	1	success
	When email is not registered:	
	1	error

Figure 1: The vulnerability in the password reset form

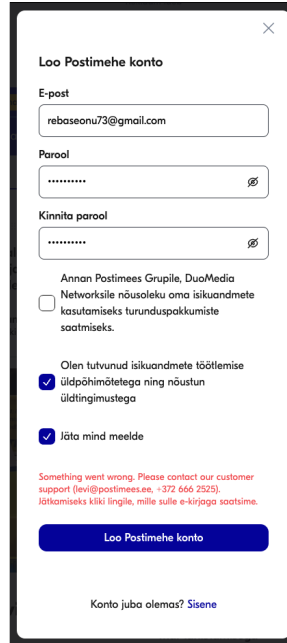
The password reset form is susceptible to account enumeration attacks. This is because when a password reset is requested for an email address that is not registered with the service, there are subtle differences in the response received from the server, compared to when the email is registered (see 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 mobile app interface for creating a Loo Postimehe account. The form includes fields for E-post (rebaseonu73@gmail.com), Parool (password), and Kinnitatu parool (confirm password). Below the password fields, there are three checkboxes: 'Annan Postimees Grupile, DuoMedia Networksile nõusoleku oma isikuandmete kasutamiseks turunduspakkumiste saatmiseks.' (unchecked), 'Olen tutvunud isikuandmete töötlemise üldpõhimõtete ja nõustun üldtingimustega' (checked), and 'Jäta mind meelde' (checked). A red error message is displayed: 'Something went wrong. Please contact our customer support (levi@postimees.ee, +372 666 2525). Jätkamiseks klikki lingile, mille sulle e-kirjaga saatsime.' At the bottom, there is a blue button labeled 'Loo Postimehe konto' and a link 'Konto juba olemas? Sisene'.

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).

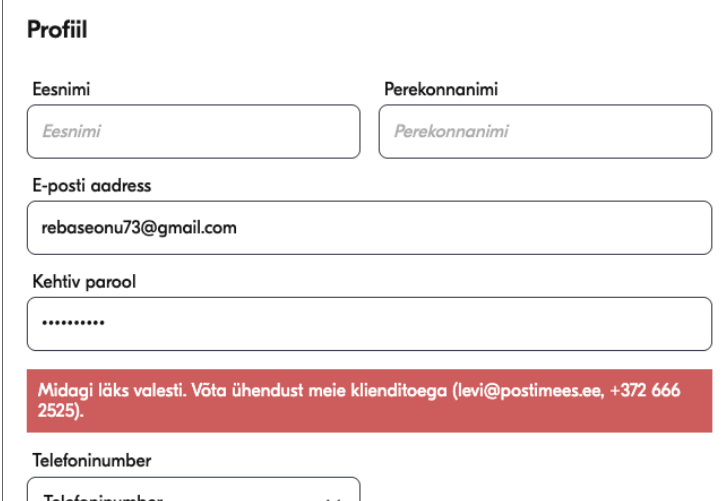
The form normally sends a confirmation email to the email owner on successful submission. However, by introducing validation errors in the form, an attacker can determine whether an email address is already registered, without successfully submitting the form. This allows the attacker to also verify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



**Profiil**

Eesnimi

Perekonnanimi

E-posti address

Kehtiv parool

Midagi läks valesti. Võta ühendust meie klienditoega (levi@postimees.ee, +372 666 2525).

Telefoninumber

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].

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**, 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.

## 2.4 Subscription Sharing Form

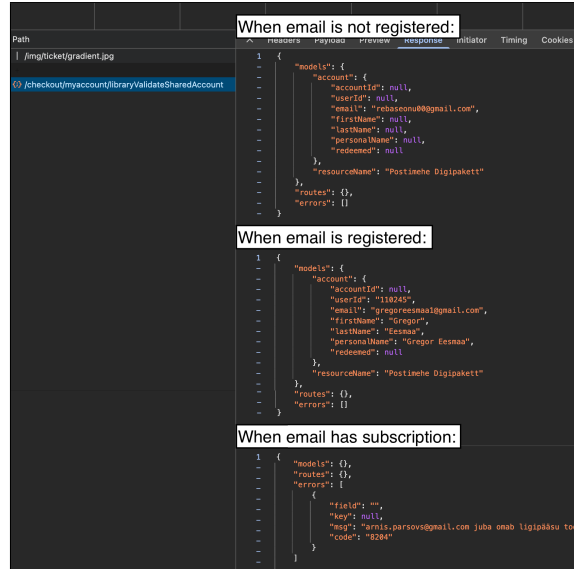


Figure 4: The vulnerabilities in the subscription sharing form

The subscription sharing form is also susceptible to account enumeration attacks, with additional data leaking about the existing accounts. This is possible due to subtle differences in the server’s validation responses to requests with unregistered emails, registered emails without a subscription, and registered emails that are already subscribed (see Figure 4).

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.

**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).

One way to achieve that would be to eliminate separate email validation requests. After user confirms their sharing preferences, 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(es)”. Send emails 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.

**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](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](https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#protect-against-automated-attacks).