

# Account Enumeration Vulnerability: **geenius.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 2025-01-11, we tested **geenius.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 and account registration form of **geenius.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

Tundmatu e-posti aadress. Registreeri ennast Geeniuse lugejaks [siin](#)

### Logi sisse

[Sisene Google'i kontoga](#)

#### Sisene Geeniuse kontoga

E-posti aadress

rebaseonu76@gmail.com

Salasõna

\*\*\*\*\*

☐ Jäta mind meelde [Unustasid parooli?](#)

[Sisene](#)

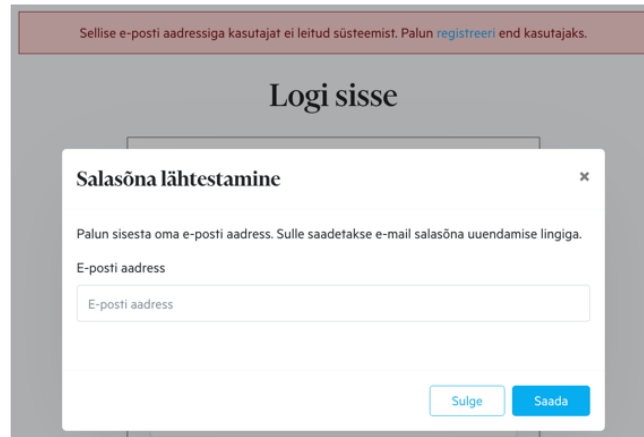
Figure 1: The vulnerability in the login form

The login form is susceptible to account enumeration attacks. This is because when a user with the provided email does not exist, the form shows a different error message 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 screenshot shows a web interface for logging in and resetting a password. At the top, a red banner contains the text: "Sellise e-posti aadressiga kasutajat ei leitud süsteemist. Palun registreeri end kasutajaks." Below this is a "Logi sisse" (Log in) section. A modal window titled "Salasõna lähtestamine" (Reset password) is open. It contains the instruction: "Palun sisesta oma e-posti aadress. Sulle saadetakse e-mail salasõna uuendamise lingiga." (Please enter your email address. You will receive an email with a link to reset your password). There is an input field labeled "E-posti aadress" (Email address) with the placeholder text "E-posti aadress". At the bottom right of the modal are two buttons: "Sulge" (Close) and "Saada" (Send).

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

The screenshot shows a web form titled "Registreeru Geeniuse kasutajaks". At the top, a pink banner reads "Vabandust, see e-postiaadress on juba kasutusel!". Below the title, the section "KONTO LOOMINE" is followed by "Geeniuse registreerunud kasutaja". A list of bullet points states: "• Piiramatult ligipääs Geeniuse tasuta artiklitele." and "• Igal argipäeval ülevaade päeva olulisematest uudistest." To the right is a cartoon illustration of a person standing on a stack of books. Below this, the "TASUTA" section contains "1. Nõustu kasutustingimustega" with a checked checkbox for "Nõustun veebilehe kasutustingimustega." and an unchecked checkbox for "Annan nõusoleku Geeniuse uudiskirjaga liitumiseks. Uudiskirjast saad alati loobuda, lingi selleks leiad saadetud kirja järele." This is followed by "2. Registreeru Google'i või Facebooki kontoga" with a button "Registreeru Google'i kontoga". Then, "3. Või loo uus konto" is shown with a text input field containing "rebaseonu73@gmail.com", two password input fields with masked characters and toggle icons, and a final blue "Registreeru" button.

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]

### 3 Security Contacts

A valid `security.txt` [4] file was not found on `geenius.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 `telli@geenius.ee` was found in the privacy policy of `geenius.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](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).
- [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/>.