

Account Enumeration Vulnerability: **eliis.eu**

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

April 27, 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 2025-04-27, we tested **eliis.eu** and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific account identifier is registered with the service.** 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 **2025-05-11**, 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 **eliis.eu**. 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

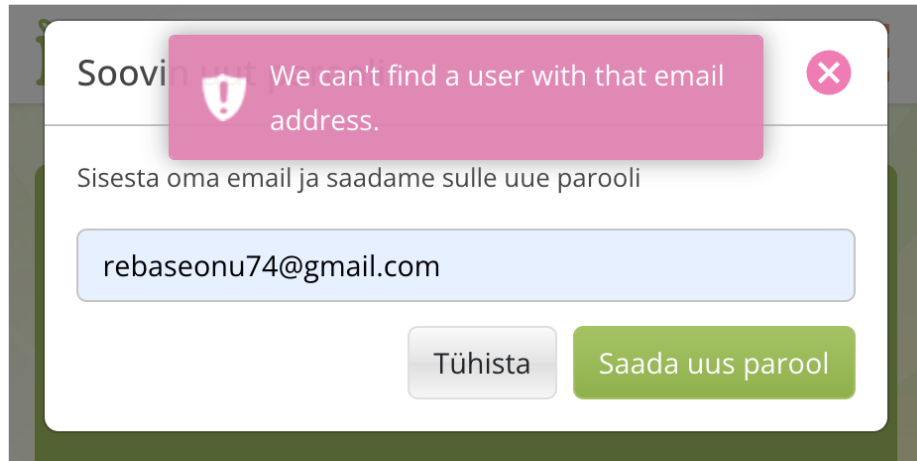
The image shows a web interface for a password reset form. At the top left, the word "Soovi" is partially visible. A pink error message box with a white shield icon and a close button (X) in the top right corner displays the text: "We can't find a user with that email address." Below the error message, the instruction "Sisesta oma email ja saadame sulle uue parooli" is shown. A light blue input field contains the email address "rebaseonu74@gmail.com". At the bottom, there are two buttons: a grey "Tühista" button and a green "Saada uus parool" button.

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, 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]

2.2 Account Registration Form



The screenshot shows a mobile application interface for account registration. At the top, there is a header with the 'ELII' logo and a red banner that reads 'The email has already been taken.' Below the header, the title 'Registreeri' is centered. A progress indicator shows four steps, with the second step 'Nõustun' (I agree) being the current step. The form contains several input fields: an email address field with 'rebaseonu73@gmail.com', a password field with masked characters '.....', a username field with 'Rebases', and a confirmation field with 'On'. Below these fields, there is a link for 'Nõustun Eliisi privaatsuspoliitika' (I agree to Elii's privacy policy). At the bottom, there are two buttons: 'Tagasi' (Back) and 'Nõustun ja liitun' (I agree and sign up).

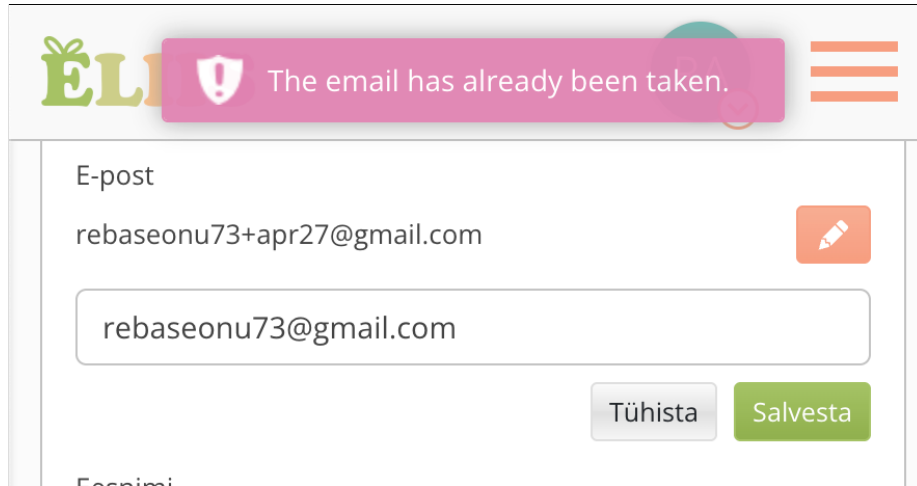
Figure 2: The vulnerability in the account registration form

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). 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]

2.3 Email Change Form



The screenshot shows a web interface for changing an email address. At the top left is a logo with the letters 'ELI' in green and orange. To its right is a pink banner with a white shield icon and the text 'The email has already been taken.' Further right is a hamburger menu icon. Below the banner, the form is titled 'E-post' and shows the current email 'rebaseonu73+apr27@gmail.com' next to an edit icon. A text input field contains 'rebaseonu73@gmail.com'. At the bottom right of the form are two buttons: 'Tühista' (grey) and 'Salvesta' (green).

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].

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 `eliis.eu`. 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 `info@eliis.ee` was found in the privacy policy of `eliis.eu` 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/>.