

Account Enumeration Vulnerability: **elron.ee**

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

March 23, 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 2025-01-04, we tested **elron.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 **elron.ee**. No issues appeared on the login form. However, we identified security issues on the password reset form and account registration form. The vulnerabilities found are described in more detail in subsections below.

2.1 Password Reset Form

The screenshot shows the ELTRON 100 website's password reset interface. At the top, there is a navigation bar with the ELTRON 100 logo and links for Reisiotsing, Pileitiinfo, Sõiduinfo, and Elronist. A progress bar indicates the current step: 1 Sinu andmed, 2 Email, and 3 Uus parool. A contact number 06-24 kliendiinfo +372 616 0245 is displayed. A red error message box at the top states: 'Tähelepanu! Midagi läks valesti. Palun proovi uuesti.' Below this, the 'Muuda salasõna' section contains instructions in Estonian. The 'Sinu e-posti aadress' field contains the email 'rebaseonu71@gmail.com' and an 'Edasi' 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 the ELRON 100 website's account registration page. At the top, there is a navigation bar with links for 'Reisiotsing', 'Piletiinfo', 'Sõiduinfo', and 'Elronist'. On the right, there are links for 'Ostukorv', 'Minu konto', 'Eesti', and a search icon. Below the navigation bar, a progress indicator shows two steps: '1 Sinu andmed' (active) and '2 Emaili kinnitus'. A red banner at the top of the form area contains a warning icon and the text 'Tähelepanu! Sellise e-posti aadressiga konto on juba olemas. Kas soovid sisse logida?'. The form itself is divided into two main sections. The left section, titled 'Loo oma konto', explains that an Elroni account allows for easy purchase of train tickets, activation of services, and management of funds. It includes a link 'Kas Sul on juba konto? Logi sisse.' The right section, titled 'Sinu andmed', contains a label 'Kohustuslikud väljad on tähistatud sümboliga *'. It has an 'E-posti' field with the value 'rebaseonu73@gmail.com', a 'Salasõna' field with a masked password and a 'Näita' link, and a checkbox 'Olen lugenud ja nõustun kasutustingimustega' which is checked. At the bottom of the right section is a large orange button labeled 'Loo konto'.

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]

3 Security Contacts

A valid `security.txt` [4] file was not found on `elron.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 `info@elron.ee` was found in the privacy policy of `elron.ee` and this report was sent to this email address on 2025-03-16, with no confirmation of receipt received to date.
- The email address `klienditugi@elron.ee` was found in the contact or help page of `elron.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/>.