

Account Enumeration Vulnerability: `forum.solnet.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.

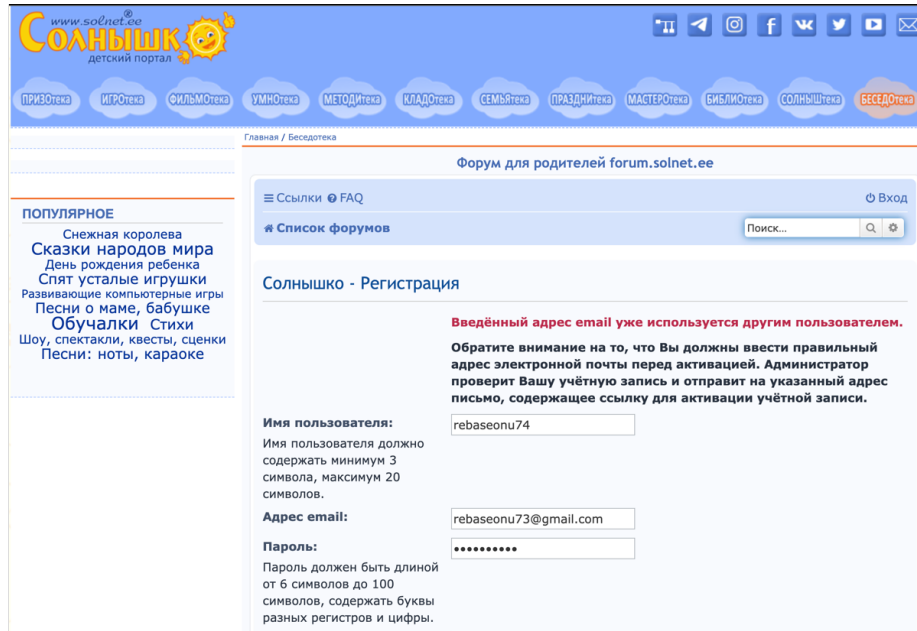
On 2025-01-08, we tested `forum.solnet.ee` and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific email address is registered with the service.** Disclosing such information to third parties constitutes a data breach, 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 account registration form of `forum.solnet.ee`. It was vulnerable to account enumeration. The vulnerabilities found are described in more detail in subsections below.

2.1 Account Registration Form



The screenshot shows the 'Солнышко' (Solnyshko) website, a children's portal. The main navigation bar includes links to various sections like 'ПРИВЕТКА', 'ИГРОТЕКА', 'ФИЛЬМОТЕКА', etc. The page title is 'Форум для родителей forum.solnet.ee'. The left sidebar lists 'ПОПУЛЯРНОЕ' (Popular) content. The main content area is titled 'Солнышко - Регистрация' (Solnyshko - Registration). It contains a registration form with the following fields and messages:

- Имя пользователя:** rebaseonu74. Below the field, it says: 'Имя пользователя должно содержать минимум 3 символа, максимум 20 символов.'
- Адрес email:** rebaseonu73@gmail.com.
- Пароль:** [masked]. Below the field, it says: 'Пароль должен быть длиннее от 6 символов до 100 символов, содержать буквы разных регистров и цифры.'

A red error message is displayed at the top of the form: 'Введённый адрес email уже используется другим пользователем.' (The entered email address is already used by another user). Below this, a note states: 'Обратите внимание на то, что Вы должны ввести правильный адрес электронной почты перед активацией. Администратор проверит Вашу учётную запись и отправит на указанный адрес письмо, содержащее ссылку для активации учётной записи.'

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).

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 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` [3] file was not found on `forum.solnet.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:

- No contact emails were found in a privacy policy of `forum.solnet.ee`.
- The email address `solnet-ee@yandex.ru` was found in the contact or help page of `forum.solnet.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] EdOverflow and Yakov Shafranovich. *security.txt - A proposed standard which allows websites to define security policies*. Accessed: 2025-01-26. URL: <https://securitytxt.org/>.