

Account Enumeration Vulnerability: **stena.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.

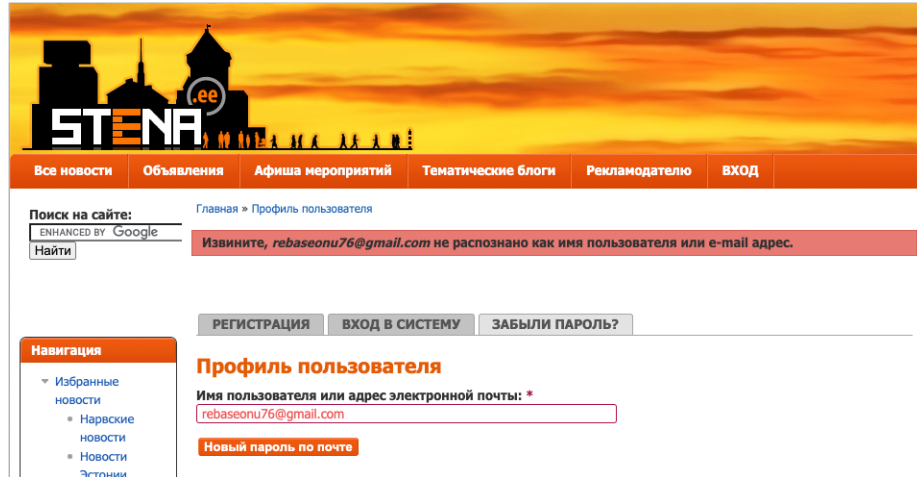
On 2025-01-12, we tested **stena.ee** and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific email address is registered with the service.** Disclosing such information to third parties constitutes a data breach, as 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 password reset form, account registration form and email change form of **stena.ee**. We identified security issues in all of these functionalities. The vulnerabilities found are described in more detail in subsections below.

2.1 Password Reset Form



The screenshot shows the STENA website interface. At the top is a navigation bar with links: Все новости, Объявления, Афиша мероприятий, Тематические блоги, Рекламодателю, and ВХОД. Below this is a search bar with the text "Поиск на сайте:" and "ENHANCED BY Google". To the right of the search bar is a link "Главная » Профиль пользователя". Below the search bar is a red error message: "Извините, rebaseonu76@gmail.com не распознано как имя пользователя или e-mail адрес." Below the error message are three buttons: РЕГИСТРАЦИЯ, ВХОД В СИСТЕМУ, and ЗАБЫЛИ ПАРОЛЬ?. On the left side, there is a "Навигация" section with a dropdown menu showing "Избранные новости" and "Нарвские новости". Below the navigation section is the "Профиль пользователя" section, which contains a form with the label "Имя пользователя или адрес электронной почты: *" and a text input field containing "rebaseonu76@gmail.com". Below the input field is a button labeled "Новый пароль по почте".

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 STENA website's account registration form. At the top, there is a navigation bar with links: "Все новости", "Объявления", "Афиша мероприятий", "Тематические блоги", "Рекламодателю", and "ВХОД". Below the navigation bar is a search bar with the text "Поиск на сайте:" and "ENHANCED BY Google". To the right of the search bar is a red banner that reads: "Адрес электронной почты rebaseonu73@gmail.com уже зарегистрирован. Забыли свой пароль?". Below the search bar is a "Найти" button. On the left side, there is a "Навигация" section with a list of links: "Избранные новости", "Нарские новости", "Новости Эстонии", "Песочница", "Добавить новость", "Тематические блоги", and "Все объявления". Below the navigation section is a "ВХОД" button. The main content area is titled "РЕГИСТРАЦИЯ" and "ВХОД В СИСТЕМУ". Below this is a section titled "Профиль пользователя" with a warning message: "ВНИМАНИЕ! Указывайте только реальный адрес электронной почты. Если Вам не приходят письма с нашего сайта - проверьте у себя в спаме. Либо выберите альтернативный способ регистрации используя любой из уже существующих Ваших аккаунтов ниже...". Below the warning message is a form with two fields: "Имя пользователя:" and "Адрес электронной почты:". The "Имя пользователя:" field contains the text "rebaseonu76". The "Адрес электронной почты:" field contains the text "rebaseonu73@gmail.com". Below the form is a checkbox with the text "я принимаю на себя всю ответственность за содержание моего комментария". At the bottom left, there is a "ВЫВОЗ И ПРИЕМ ОТХОДОВ" button. At the bottom right, there is a "Регистрация" button.

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].

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, 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



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, 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 `stena.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 `stena.ee`.
- The email address `stenaee@gmail.com` was found in the contact or help page of `stena.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/>.