

Account Enumeration Vulnerability: **forum.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 **forum.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, account registration form and email change form of **forum.ee**. 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

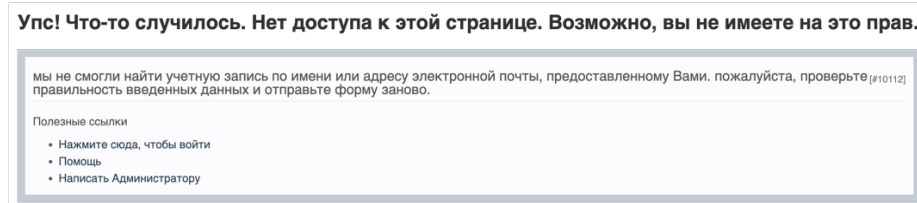


Figure 1: The vulnerability in the password reset form

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).

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

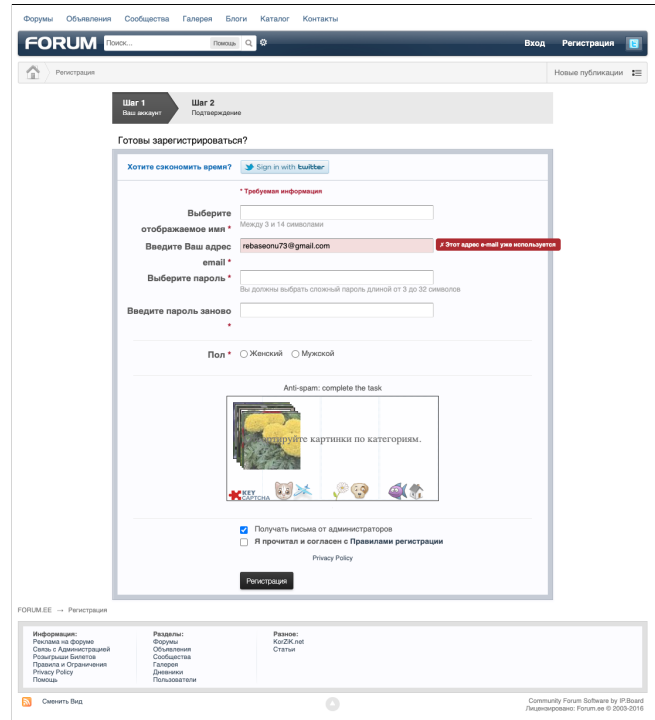
The image shows a web browser displaying a forum's registration page. The forum is titled "FORUM" and has a navigation bar with links like "Форумы", "Объявления", "Сообщества", "Галерея", "Блоги", "Каталог", and "Контакты". The registration process is divided into two steps: "Шаг 1: Вы выбрали" and "Шаг 2: Подтверждение". The current step is "Шаг 2". The form asks the user to "Выберите отображаемое имя" (Choose a display name) and "Введите Ваш адрес email" (Enter your email address). The email address "rebaseon73@gmail.com" is entered, and a red error message "Этот адрес e-mail уже используется" (This email address is already used) is displayed. Below the email field, there is a password field with the instruction "Вы должны выбрать сложный пароль длиной от 3 до 32 символов" (You must choose a complex password 3 to 32 characters long). There is also a checkbox for "Получать письма от администраторов" (Receive emails from administrators) and a checkbox for "Я прочитал и согласен с Правилами регистрации" (I have read and agree with the registration rules). The form also includes a CAPTCHA challenge with the text "Anti-spam: complete the task" and "Сопоставьте картинки по категориям" (Match the pictures by category). The footer of the page contains links to "Информация", "Правила на форуме", "Связь с Администрацией", "Рекламы", "Форумы", "Объявления", "Сообщества", "Галерея", "Блоги", "Каталог", "Контакты", and "Помощь".

Figure 2: The vulnerability in the account registration form

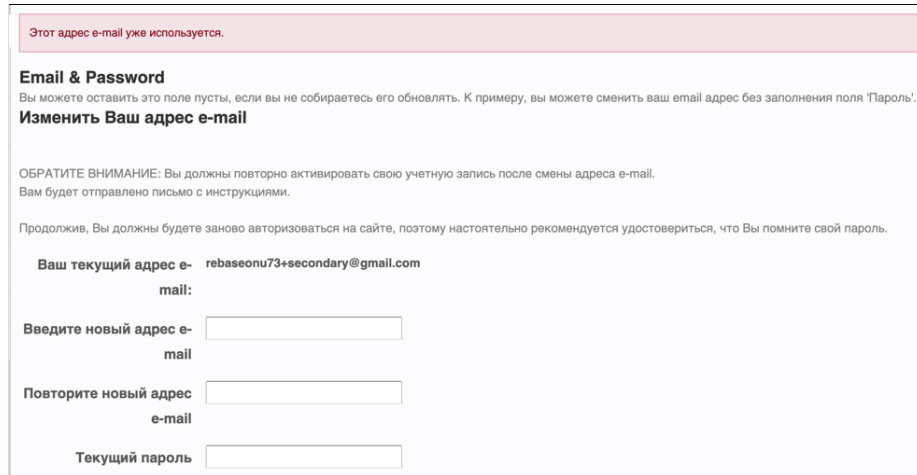
The account registration form is also susceptible to account enumeration attacks. This is because when the provided email address is already taken, the form shows an error message (see Figure 2). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, enabling attackers to easily automate these attacks [3].

The form normally sends a confirmation email to the email owner on complete successful submission. However, validation of the email address is done in a separate request before the complete form could be submitted. 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



Этот адрес e-mail уже используется.

Email & Password

Вы можете оставить это поле пустым, если вы не собираетесь его обновлять. К примеру, вы можете сменить ваш email адрес без заполнения поля 'Пароль'.

Изменить Ваш адрес e-mail

ОБРАТИТЕ ВНИМАНИЕ: Вы должны повторно активировать свою учетную запись после смены адреса e-mail. Вам будет отправлено письмо с инструкциями.

Продолжив, Вы должны будете заново авторизоваться на сайте, поэтому настоятельно рекомендуется удостовериться, что Вы помните свой пароль.

Ваш текущий адрес e-mail: rebaseonu73+secondary@gmail.com

Введите новый адрес e-mail:

Повторите новый адрес e-mail:

Текущий пароль:

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 `forum.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.ee`.
- The email address `info@forum.ee` was found in the contact or help page of `forum.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/>.