

# Account Enumeration Vulnerability: `peaasi.ee`

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.

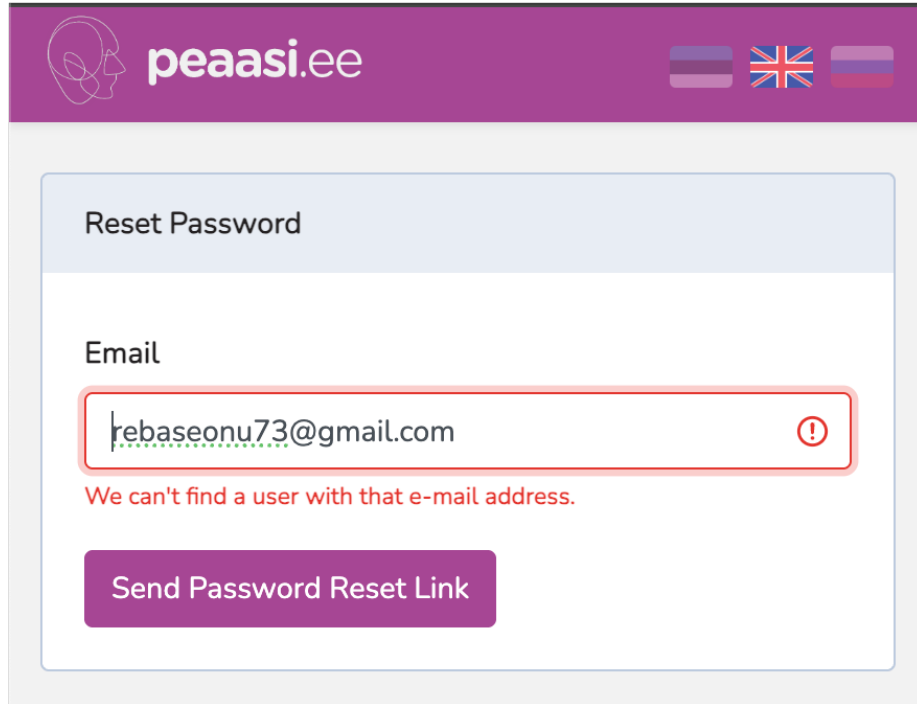
On 2025-04-27, we tested `peaasi.ee` and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific account identifier is registered with the service.** If the account identifier of an online service is personal data (e.g. 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 password reset form of `peaasi.ee`. It was vulnerable to account enumeration. The vulnerabilities found are described in more detail in subsections below.

## 2.1 Password Reset Form



The screenshot shows the 'Reset Password' form on the website 'peaasi.ee'. The form has a purple header with the logo and flags. The main form area is white with a light blue border. It contains a title 'Reset Password', an 'Email' label, a text input field with the email 'rebaseonu73@gmail.com', and a red error message: 'We can't find a user with that e-mail address.' Below the input field is a purple button labeled 'Send Password Reset Link'.

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]

### 3 Testing Limitations

The registration process was observed to require setting up a physical appointment with the service, so no test accounts were created on the service to avoid reducing resources available to people that need them. Because of the limitation, it was not possible to test the registration form, the login form or the email change form (if it exists).

Due to the testing limitations mentioned above, please ensure that the other authentication-related forms return indistinguishable responses regardless of account existence:

- In the login form, return the same error message whether the email is registered or not. For example, always return the message “Email or password is incorrect”. [2]
- In the registration form, 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]
- In the email change form (if such exists), 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.

## 4 Security Contacts

A valid `security.txt` [4] file was not found on `peaasi.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 `peaasi@peaasi.ee` was found in the privacy policy of `peaasi.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](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](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/>.