

Account Enumeration Vulnerability: `ope.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.

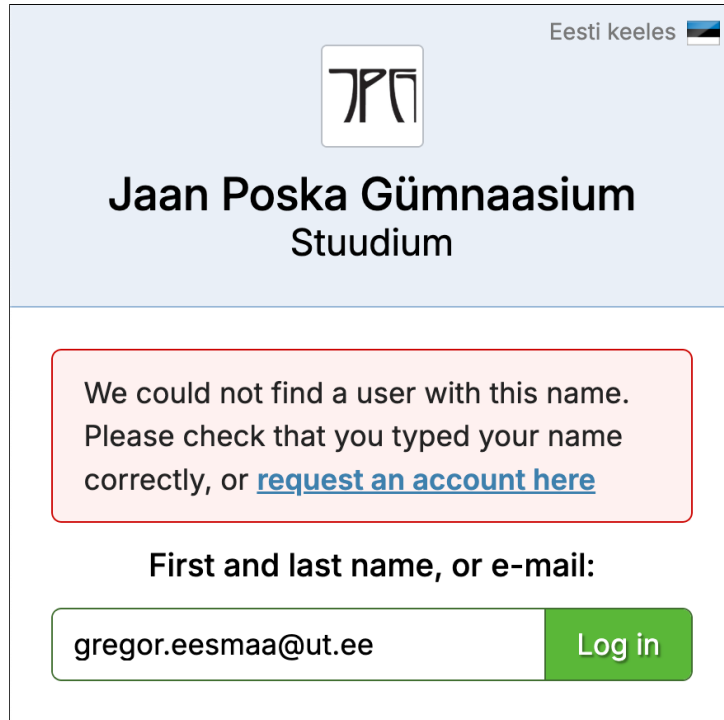
On 2025-04-27, we tested `ope.ee` and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific account identifier is registered with the service.** If the account identifier of an online service is personal data (e.g. email 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 login form and email change form of `ope.ee`. No issues appeared on the email change form. However, we identified security issues on the login form. The vulnerabilities found are described in more detail in subsections below.

2.1 Login Form



The screenshot shows the login interface for Jaan Poska Gümnaasium Stuudium. At the top right, it says "Eesti keeles" with a small Estonian flag. In the center, there is a logo consisting of stylized letters "JP" inside a square. Below the logo, the text "Jaan Poska Gümnaasium Stuudium" is displayed. A red-bordered box contains an error message: "We could not find a user with this name. Please check that you typed your name correctly, or [request an account here](#)". Below this box, the label "First and last name, or e-mail:" is shown. Underneath, there is a text input field containing the email "gregor.eesmaa@ut.ee" and a green "Log in" button.

Figure 1: The vulnerability in the login form

The login form is susceptible to account enumeration attacks. This is because when a user with the provided email does not exist, the form shows a different error message compared to when the password is incorrect (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 error message whether the email is registered or not. For example, always return the message “Email or password is incorrect”. [2]

Note: The same vulnerability allows for enumeration via personal codes or full names. Additionally, as distinct “clients” (institutions using Stuudium) seem to have distinct accounts, the vulnerability might also allow an attacker to estimate rough geolocation of the subjects. Both of these nuances greatly increase the risks imposed by this vulnerability.

3 Security Contacts

A valid `security.txt` [4] file was not found on `ope.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 `ope.ee`.
- The email address `info@stuudium.com` was found in the contact or help page of `ope.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/>.