

# Account Enumeration Vulnerability: **jysk.ee**

Gregor Eesmaa  
gregor.eesmaa@ut.ee  
University of Tartu

March 23, 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 2025-01-04, we tested **jysk.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 and account registration form of **jysk.ee**. No issues appeared on the login form and password reset form. However, we identified security issues on the account registration form. The vulnerabilities found are described in more detail in subsections below.

## 2.1 Account Registration Form

The screenshot shows the JYSK account registration page. At the top, there's a navigation bar with links like JÕULUDEKS, MAGAMISTUBA, VANNITUBA, KONTOR, ELUTUBA, SÕOGITUBA, HOIUSTAMINE, KÄRDINAD, SISEKIJUNDUS, and buttons for LOGIN and ORDER. Below the navigation bar, a red banner states: "Sama e-posti aadressiga klient on seotud veebisaidil juba olemas." (A client with the same email address is already linked on the website). The main heading is "REGISTREERUMINE" (Registration). There are two tabs: "Fraisk" (Selected) and "Juridiline isik" (Legal entity). The "Fraisk" tab contains a form with fields for phone number (+372) and email address (E-posti aadress\*). Below the form are checkboxes for terms and conditions, and a "SAADA KINNITUSKOOD" (Get confirmation code) button. To the right of the form, there's a section titled "REGISTREERI TÄITES ALLOLEV" (Register by filling in the following) with several promotional offers: "ERIHINNAD KLIENDIKAARDIGA" (Special prices with the client card), "120 PROOVIPÄEVA SINU GOLD MADRATSILE" (120 trial days for your Gold Mattress), "PIKENDATUD GARANTII KUNI 25 AASTAT SINU GOLD MADRATSILE" (Extended warranty up to 25 years for your Gold Mattress), "PIKENDATUD GARANTII KUNI 10 AASTAT SINU GOLD TERILE" (Extended warranty up to 10 years for your Gold Tiles), "ME SORBITUME MADALAIMA HINNAGA" (We will buy your goods at a low price), and "TÄHTAJATU TAGASTUSVÕIMALUS" (Return of the purchased goods). At the bottom, there's a footer with icons for a shopping cart, a flag, a checkmark, and a circular arrow, along with a small chat bubble icon.

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).

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 `jysk.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 `dpo@jysk.ee` was found in the privacy policy of `jysk.ee` and this report was sent to this email address on 2025-03-16, with no confirmation of receipt received to date.
- The email address `info@jysk.ee` was found in the contact or help page of `jysk.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] EdOverflow and Yakov Shafranovich. *security.txt - A proposed standard which allows websites to define security policies*. Accessed: 2025-01-26. URL: <https://securitytxt.org/>.