

Account Enumeration Vulnerability: `amoremi.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 `amoremi.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 `amoremi.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

When email is registered:	When email is not registered:
<div><h3>Parooli meenusus</h3><div>Parooli meeldetuletus saadetakse mõne hetke pärast kontoga seotud e-posti aadressile. Abi: amoremi.ee/helpdesk</div><p>Kontrolli oma postkasti - saatsime sulle kirja kuuekohalise kinnituskoodiga. Sisesta see allolevasse kasti uue parooli määramiseks või kliiki kirja sees olevat aktiveerimise viidet</p><p>Tähelepanu!</p><ul style="list-style-type: none">Parooli muutmise kirja saamiseks võib sõltuvalt kirjaprogrammist minna kuni tund aega. Kontrolli ka vajadusel enda kirjaprogrammi Rämpsposti/Junk/Spam jms katalooge.<div>Kinnituskood</div><div>Jätka</div></div>	<div><h3>Parooli meenusus</h3><div>Parooli meeldetuletus saadetakse mõne hetke pärast kontoga seotud e-posti aadressile. Abi: amoremi.ee/helpdesk</div><p>Sisesta kasutajanimi või e-posti aadress, millelt registreerusid või mis on määratud Su peamiseks aadressiks ja me saadame Sulle viite, mille abil saad parooli muuta.</p><p>Tähelepanu!</p><ul style="list-style-type: none">Parooli muutmise kirja saamiseks võib sõltuvalt kirjaprogrammist minna kuni tund aega. Kontrolli ka vajadusel enda kirjaprogrammi Rämpsposti/Junk/Spam jms katalooge.<p>Kasutajanimi või e-posti aadress *</p><div>Kasutajanimi või e-posti aadress</div><div>Saada kiri</div></div>

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 'Konto registreerimine' (Account Registration) page. At the top, there is a header with the 'Amoremi' logo and a 'Logi sisse' (Log in) link. The main heading is 'Konto registreerimine'. Below this is a 'LOGIN INFO' section with a 'Menu' icon. The form contains three input fields: 'Kasutajanimi' (Username) with the value 'rebaseonu74', 'Parool' (Password), and 'E-post' (Email) with the value 'rebaseonu73@gmail.com'. An error message is displayed below the email field: 'Kasutaja 'rebaseonu73@gmail.com' aadressiga on juba registreeritud'. A red 'Registreeri' button is located below the form. Below the form, there are links for 'Kasutustingimused' (Terms of Use) and 'Liimetele sisselogimine' (Log in with email), and a section for 'Sisselogimise variandid' (Login options) with Facebook and Google icons.

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

The screenshot shows the 'Konto andmed' (Account Information) page. At the top, there's a navigation bar with 'KONTO ANDMED', 'PAROOL', and 'ALTERNATIIVNE LOGIMINE'. The main heading is 'Konto andmed'. Below it, a text block explains that changing the email address will automatically create a new one, which can be activated by clicking. It asks the user to confirm the change. The form has three fields: 'Kasutajanimi *' (Username) with the value 'rebaseonu74', 'E-post *' (Email) with the value 'rebaseonu73@gmail.com' and a red error message 'Sisestatud e-posti aadress on vigane', and 'Praegune parool *' (Current password) which is empty. A red 'Salvesta' button is at the bottom.

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].

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 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 `amoremi.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 `info@amoremi.ee` was found in the privacy policy of `amoremi.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/>.