

Account Enumeration Vulnerability: `cvkeskus.ee`

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

May 31, 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. For example, even without a direct message, small visual differences in responses, or slight variations in how the server behaves (like the exact data returned) for existing versus non-existing accounts, can still reveal if an account is registered.

On 2025-05-11, we reassessed `cvkeskus.ee` and found that **the service is still vulnerable to account enumeration**.

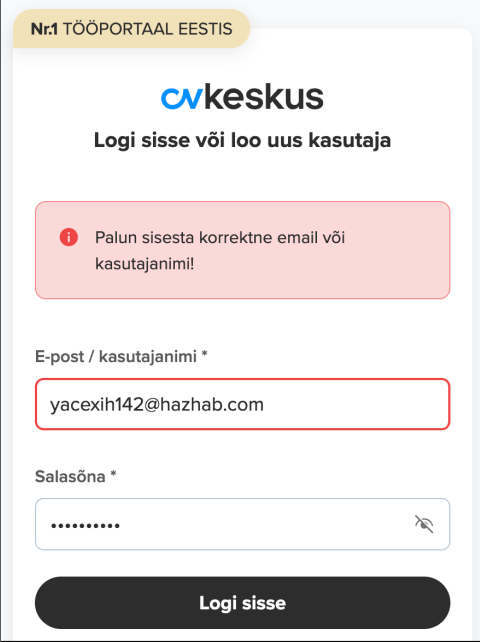
If the account identifier of an online service is personal data (e.g. email address, personal code etc), then the fact, whether it is associated to an account, is also considered personal data. Any disclosure of personal data to third parties without a legal basis constitutes a data breach [1].

We advise you to investigate the potential data breach, and notify the supervisory authority and the affected data subjects, if necessary. 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 `cvkeskus.ee`. We identified security issues in all of these functionalities. The vulnerabilities found are described in more detail in subsections below.

2.1 Login Form



The screenshot shows a login form for 'cvkeskus'. At the top, it says 'Nr.1 TÖÖPORTAAL EESTIS'. Below that is the 'cvkeskus' logo and the text 'Logi sisse või loo uus kasutaja'. A red error message box contains the text: 'Palun sisesta korrektne email või kasutajanimi!'. Below this, there are two input fields: 'E-post / kasutajanimi *' with the value 'yacexih142@hazhab.com' and 'Salasõna *' with masked characters. A black button labeled 'Logi sisse' is at the bottom.

Figure 1: The vulnerability in the login form

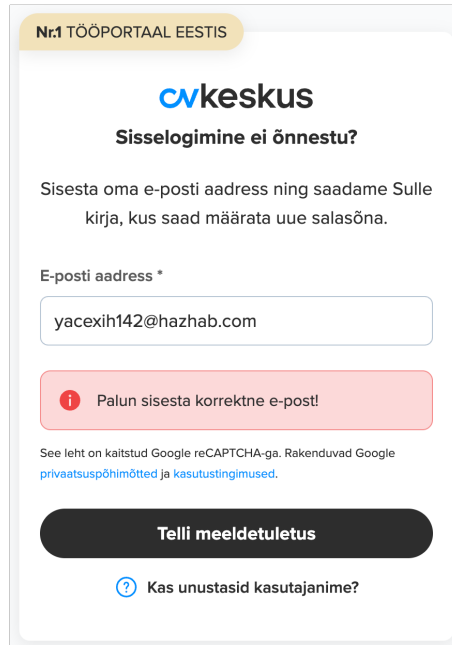
The login form is susceptible to account enumeration attacks. This is because when a user with the provided email does not exist, the form shows a different error message compared to when the password is incorrect (see Figure 1). Additionally, the form appears to lack anti-bot measures such as CAPTCHA, 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, the response must be uniform for both registered and unregistered email addresses. This uniformity must apply to the message displayed to the user as well as the underlying HTTP response details (like status codes, headers, and body content).

For example, the indistinguishable user-facing message could be: “Email or password is incorrect”. [2]

2.2 Password Reset Form



The screenshot shows a web form titled "Sisselogimine ei õnnestu?" (Login failed) from "cvkeskus". It asks the user to enter their email address to receive a password reset link. The email address "yacexih142@hazhab.com" is entered in the field. Below the field, a red error message box states: "Palun sisesta korrektne e-post!" (Please enter a correct email!). At the bottom, there is a button labeled "Telli meeldetuletus" (Request reminder) and a link that says "Kas unustasid kasutajanime?" (Did you forget your username?).

Figure 2: The vulnerability in the password reset form

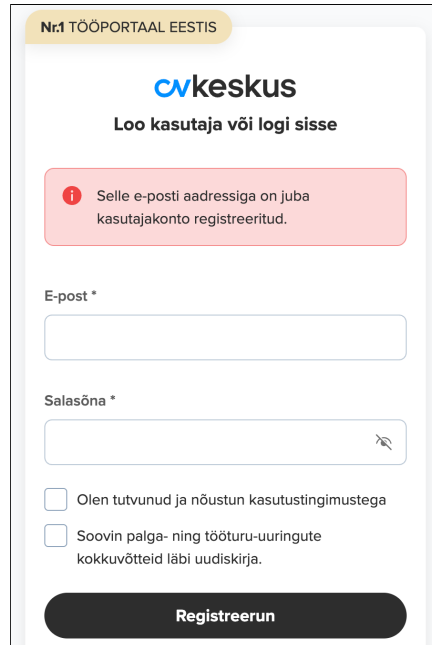
The password reset form is also susceptible to account enumeration attacks. This is because when a password reset is requested for an email address that is not registered with the service, the form shows an error message (see Figure 2). Additionally, the form appears to lack anti-bot measures such as 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, the response must be uniform for both registered and unregistered email addresses. This uniformity must apply to the message displayed to the user as well as the underlying HTTP response details (like status codes, headers, and body content).

For example, the indistinguishable user-facing message could be: “A password reset link has been sent if an account with this email exists”. [2]

2.3 Account Registration Form



The screenshot shows a web form for 'cvkeskus' with the header 'Nr1 TÖÖPORTAAL EESTIS'. The main heading is 'Loo kasutaja või logi sisse'. A red error message box states: 'Selle e-posti aadressiga on juba kasutajakonto registreeritud.' Below this are input fields for 'E-post *' and 'Salasõna *'. There are two checkboxes: 'Olen tutvunud ja nõustun kasutustingimustega' and 'Soovin palga- ning tööturu-uuringute kokkuvõtteid läbi uudiskirja.' At the bottom is a 'Registreerun' button.

Figure 3: 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 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, the response must be uniform for both registered and unregistered email addresses. This uniformity must apply to the message displayed to the user as well as the underlying HTTP response details (like status codes, headers, and body content).

For example, the indistinguishable user-facing message could be: “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]

2.4 Email Change Form

The screenshot shows a web form titled "E-maili aadress rebaseonu73@gmail.com on kasutusel." (Email address rebaseonu73@gmail.com is in use). The form is divided into two main sections: "Profil" (Profile) and "Kasutajanime või salasõna muutmine" (Change username or password). The "Profil" section contains fields for "Eesnimi" (First name) with value "Rebase", "Perekonnanimi" (Last name) with value "Onu", "Telefon" (Phone) with value "55577679", "Suhtluskeel" (Communication language) with value "eesti", "Sugu" (Gender) with value "Mees", "Päev" (Day) with value "1", "Kuu" (Month) with value "jaanuar", and "Aasta" (Year) with value "1970". There are also checkboxes for "Peidan info" (Hide info). The "Kasutajanime või salasõna muutmine" section contains a "Sinu kasutajanimi" (Your username) field with value "xahixap951@inkight.com", a "Uus salasõna" (New password) field, and a "Salasõna kordus" (Repeat password) field. A message in blue text says: "(Muutmiseks sisesta palun oma e-post, millest saab ühtlasi ka Sinu kasutajanimi)" (To change, please enter your email, from which you can also get your username). At the bottom, there is a checkbox for "Soovin kasulikkude tööteemalist infot oma e-postile" (I want useful work-related information to my email) and a "Salvestan" (Save) button.

Figure 4: 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 4). 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, the response must be uniform for both registered and unregistered email addresses. This uniformity must apply to the message displayed to the user as well as the underlying HTTP response details (like status codes, headers, and body content).

For example, the indistinguishable user-facing message could be: "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.

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 August 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.