

Account Enumeration Vulnerability: **example.com**

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

March 2, 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.

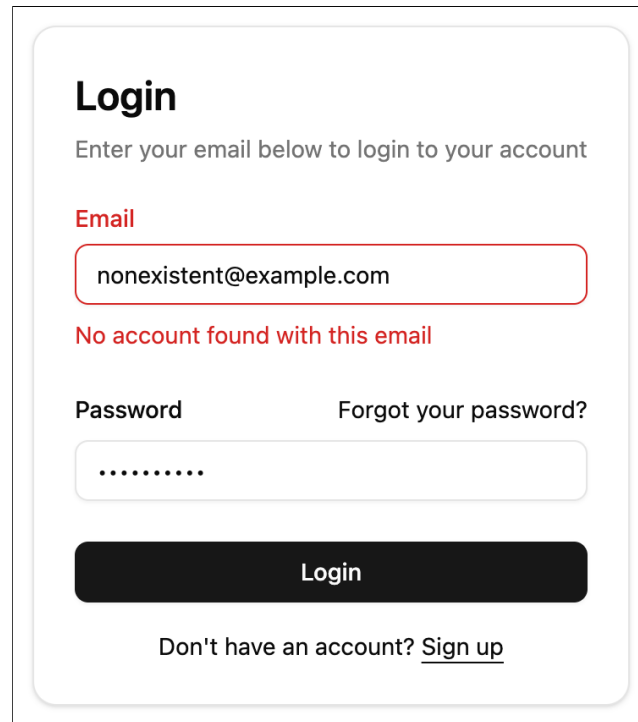
On 2025-03-02, we tested **example.com** and found that the service is vulnerable to account enumeration. **The vulnerability allows any party to test whether a user with a specific email address is registered with the service.** Disclosing such information to third parties constitutes a data breach, 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 **2025-04-11**, 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, password reset form, account registration form and email change form of **example.com**. We identified security issues in all of these functionalities. The vulnerabilities found are described in more detail in subsections below.

2.1 Login Form



Login

Enter your email below to login to your account

Email

nonexistent@example.com

No account found with this email

Password [Forgot your password?](#)

.....

Login

Don't have an account? [Sign up](#)

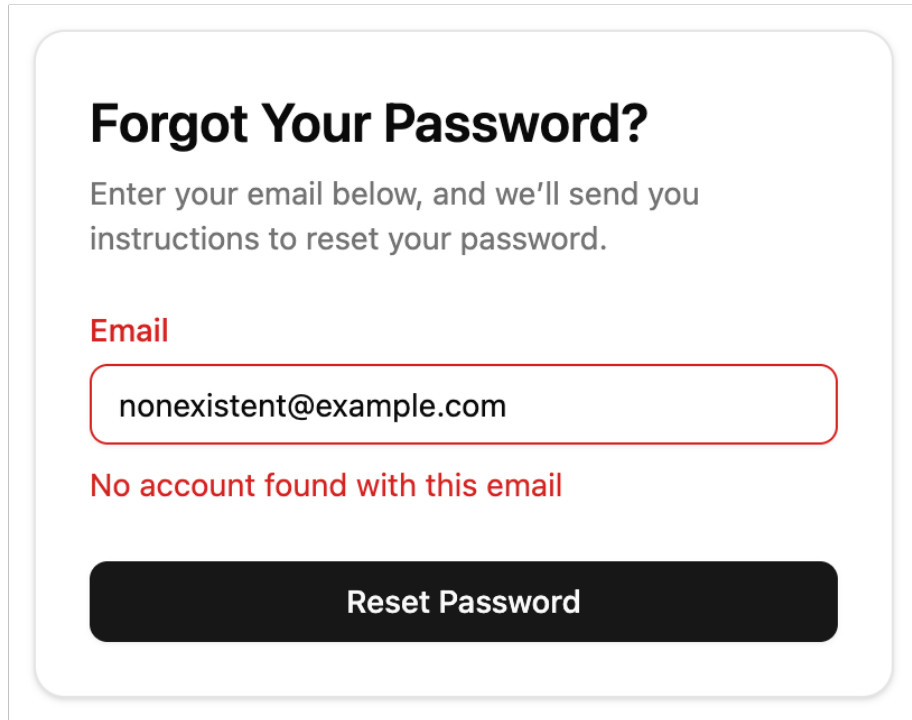
Figure 1: The vulnerability in the login form

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]

2.2 Password Reset Form



The image shows a web form titled "Forgot Your Password?". Below the title, it says "Enter your email below, and we'll send you instructions to reset your password." There is a text input field with the email "nonexistent@example.com". Below the input field, a red error message states "No account found with this email". At the bottom of the form is a dark button labeled "Reset Password".

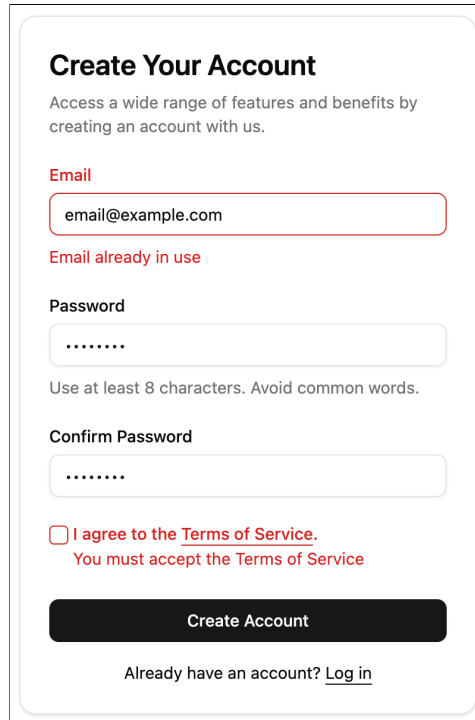
Figure 2: The vulnerability in the password reset form

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, return the same error 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]

2.3 Account Registration Form



Create Your Account

Access a wide range of features and benefits by creating an account with us.

Email

email@example.com

Email already in use

Password

.....

Use at least 8 characters. Avoid common words.

Confirm Password

.....

☐ I agree to the [Terms of Service](#).
You must accept the Terms of Service

Create Account

Already have an account? [Log in](#)

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].

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 error 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]

2.4 Email Change Form

The screenshot shows a web interface for account settings. On the left is a sidebar with links: Profile, Account (highlighted), Appearance, Notifications, and Display. The main content area is titled 'Settings' with the subtitle 'Manage your account settings and set e-mail preferences.' Below this is a section for 'Account' with the instruction 'Update your account settings.' The 'Email' field contains 'email@example.com' and is surrounded by a red border. Above the field is the label 'Email' in red. Below the field is the error message 'Email already in use' in red, followed by the text 'This is used for logging you in and sending offers you might be interested in.' Below the email field is a 'Confirm password' field, also with a red border, containing '.....'. Above it is the label 'Confirm password' in red, and below it is the error message 'Incorrect password' in red. At the bottom of the form is a black button labeled 'Update account'.

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].

No confirmation email is sent to the provided email address after this form is submitted. Additionally, by introducing validation errors in the form, the attacker can avoid submitting the form altogether. These shortcomings allow the attacker to verify unregistered email addresses, 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 error 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 `security.txt` [4] file was not found on `example.com`. 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 `example.com`.
- The email address `support@example.com` was found in the contact or help page of `example.com` and this report was sent to this email address on 2025-01-19, with no response received to date.
- The email address `domains@example.com` was found in the Estonian Internet Foundation WHOIS database and this report was sent to this email address on 2025-01-22, with no response received to date.
- The email address `john@example.com` was found in the relevant business registry 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/>.