Security Vulnerability Report

No Rate Limiting Vulnerability in Password Reset Email

Vulnerable Domain: https://app.achievable.me

🔍 Summary

A **No Rate Limiting** vulnerability was identified in the password reset functionality of https://app.achievable.me. This issue arises from the lack of rate limiting on the password reset request, which allows attackers to repeatedly trigger password reset emails for any given email address.

An attacker could exploit this vulnerability to flood a victim's inbox with password reset requests, causing inconvenience, potential service disruption, and increasing the likelihood of other malicious activities such as phishing or social engineering.

⚠️ Security Impact

- **Email Flooding**: An attacker can overwhelm a victim's inbox by sending multiple password reset requests in a short period, causing frustration or service disruption.
- **Phishing Risk**: The repetitive nature of the emails may make the victim more susceptible to phishing attempts or other forms of social engineering.
- **Denial of Service (DoS)**: Excessive requests can lead to performance degradation, affecting the availability of the service.

📜 Observed Behaviour

The password reset functionality lacks any rate-limiting controls, allowing an attacker to continuously trigger password reset emails for the same email address. This results in **email flooding**, which could severely impact the user experience.

🛠️ Recommendations

- **Implement Rate Limiting**: Limit the number of password reset requests that can be made within a certain time frame (e.g., 5 requests per minute).
- **Captcha**: Integrate a CAPTCHA mechanism on the password reset form to prevent automated abuse.
- **Monitor and Alert**: Introduce monitoring to detect unusual request patterns or spikes in password reset requests.