Bypassing access controls using email address parsing discrepancies in a business website

Ref: CVE-2023-27043

Executive Summary

This report documents the discovery of a critical access control bypass vulnerability in the email registration mechanism of the target application. A discrepancy between the server's validation logic and the actual parsing behaviour of the email library allowed an attacker to bypass domain restrictions during account registration. Exploiting this flaw enabled unauthorized account creation and subsequent administrative access, leading to full user control, including account deletion.

Introduction

The goal of this security assessment was to evaluate the resilience of the application's registration mechanism against input validation bypasses and email domain restrictions. The assessment revealed a logic flaw in how the application parses and validates email addresses, resulting in an access control vulnerability.

Methodology

1. Used Burp Suite to intercept and modify registration HTTP requests.

2. Tested multiple encoded email formats (Q-encoding, UTF-8, and UTF-7) to evaluate parsing behaviour.

3. Observed server-side validation and error responses.

4. Confirmed a successful registration bypass via UTF-7 encoded email payloads.

5. Activated the account using the spoofed confirmation email.

6. Gained access to admin functionality and performed privileged actions.

Vulnerability Findings

- **Type:** Access Control Bypass via Email Parsing Discrepancy

- **Location:** User registration email domain validation

- **Severity**: High

Description

The application enforced email domain restrictions during user registration by validating the domain string of the email. However, the validation logic failed to properly decode or normalize certain encoded email formats, particularly UTF-7 encoded strings. This results in a mismatch between what the server validates and what the email parser interprets, allowing the attacker to register with an external email domain disguised as an internal one.

Proof of Concept (PoC)

1. Attempted to register with restricted email: → Blocked.
2. Attempted with various encodings (Q, UTF-8) → Blocked.
3. Registered using UTF-7 encoded email:

   ruby

   CopyEdit

   Result: Email was accepted and confirmation sent to `attacker@exploit-server.com`.
4. Confirmed account via email link
5. Logged in and accessed the admin panel.
6. Successfully deleted the user.

Impact Assessment

- Bypass of domain-based email restrictions.
- Unauthorized account registration and email confirmation.
- Full administrative access gained through spoofed account.
- Potential for user data manipulation, privilege escalation, and service abuse.

Recommendations

1. Normalize and decode all email input using the same parser used for actual email delivery.

2. Avoid relying solely on string-based domain validation. Use strict parsing libraries that enforce domain-level checks post-decoding.

3. Add logging and alerting for anomalous email formats during registration.

4. Perform regular fuzz testing and validation on input-handling logic.

Conclusion

The identified access control bypass represented a critical logic flaw due to inconsistent email parsing. This highlights the importance of robust and consistent validation mechanisms, especially when user input determines access control boundaries. Immediate remediation is essential to prevent exploitation in real-world deployments.