Báo cáo an toàn thông tin

# Demo Pentest Viettel Cyber Security

**Thông tin chung**

|  |
| --- |
| **Tên hệ thống** Hệ thống đăng ký tham dự Triển lãm quốc phòng Quốc tế 2024 |
| **Loại ứng dụng** Web |
| **Link truy cập** \* |
| **Thời gian** 2024-11-19 |
| **Đầu mối liên hệ** \* |
| **Hình thức đánh giá Blackbox** |
| **Nhóm đánh giá** Công ty An ninh mạng Viettel |
| **Số lượng lỗi**  1 1 0 0 0 |

# Danh mục lỗ hổng

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Khuyến nghị** | **Thấp** | **Trung bình** | **Cao** | **Nghiêm trọng** |

|  |
| --- |
| **Category Pass** |
| Other |
| Server Security Misconfiguration |
| Server-Side Injection |
| Broken Authentication and Session Management |
| Sensitive Data Exposure |
| Cross-Site Scripting (XSS) |
| Broken Access Control (BAC) |

|  |
| --- |
| **Category Pass** |
| Cross-Site Request Forgery (CSRF) |
| Application-Level Denial-of-Service (DoS) |
| Unvalidated Redirects and Forwards |
| External Behavior |
| Insufficient Security Configurability |
| Using Components with Known Vulnerabilities |
| Insecure Data Storage |
| Insecure Data Transport |
| Insecure OS/Firmware |
| Broken Cryptography |
| Privacy Concerns |
| Mobile Security Misconfiguration |
| Client-Side Injection |
| Automotive Security Misconfiguration |
| Lack of Binary Hardening |
| Network Security Misconfiguration |
| Indicators of Compromise |

**Danh sách lỗi**

|  |  |  |
| --- | --- | --- |
| **Mã lỗi** | **Tên lỗi** | **Mức độ nguy hiểm** |
| **BUG-1** | Không giới hạn số lần nhập mã số đăng ký | **THẤP** |
| **BUG-2** | Server trả về chi tiết thông báo lỗi | **KHUYẾN NGHỊ** |
| **BUG-3** | Input null trong phần tra cứu nhưng vẫn trả về tên và mã QR của người dùng khác | **KHUYẾN NGHỊ** |

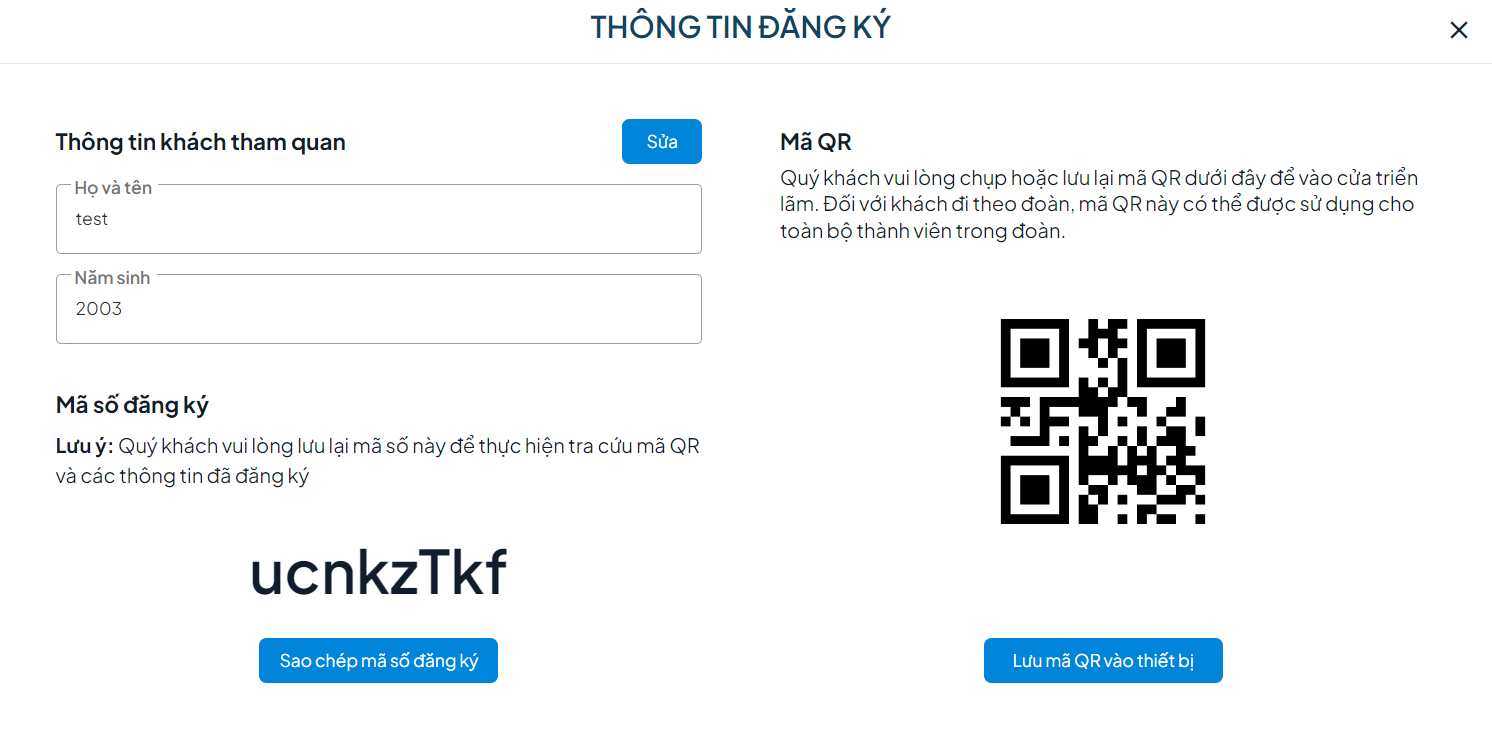
# Chi tiết lỗi

|  |
| --- |
| **[BUG-1](#_bookmark0) Không giới hạn số lần nhập mã số đăng ký** |

## Phân loại Server Security Misconfiguration > Brute Force

**Mô tả**

Khi người dùng đăng ký sẽ được cấp một mã số đăng ký. Mã này gồm 8 ký tự có thể là số, chữ cái thường hoặc chữ cái viết hoa và được dùng để sửa đổi thông tin cá nhân.



Ở chức năng tra cứu, nếu nhập mã số này người dùng có thể xem và sửa thông tin cá nhân của mình. Tuy nhiên người dùng không thể sửa đổi mã số đăng ký và ứng dụng cũng không giới hạn số lần nhập dẫn tới khả năng lợi dụng để brute force mã số đăng ký của người dùng. Vị trí lỗi:

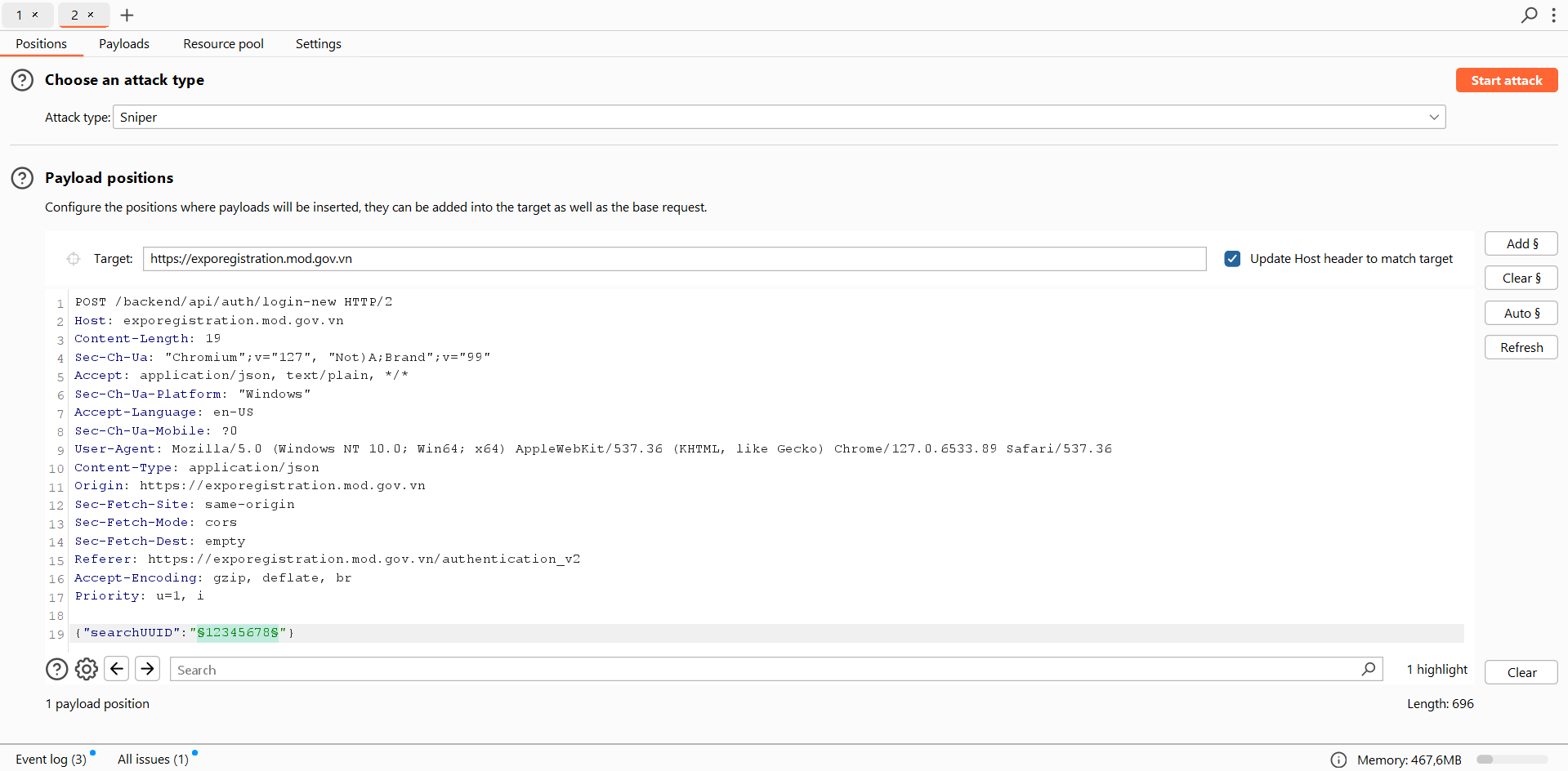
## Mức độ nguy hiểm: THẤP

**Ảnh hưởng**

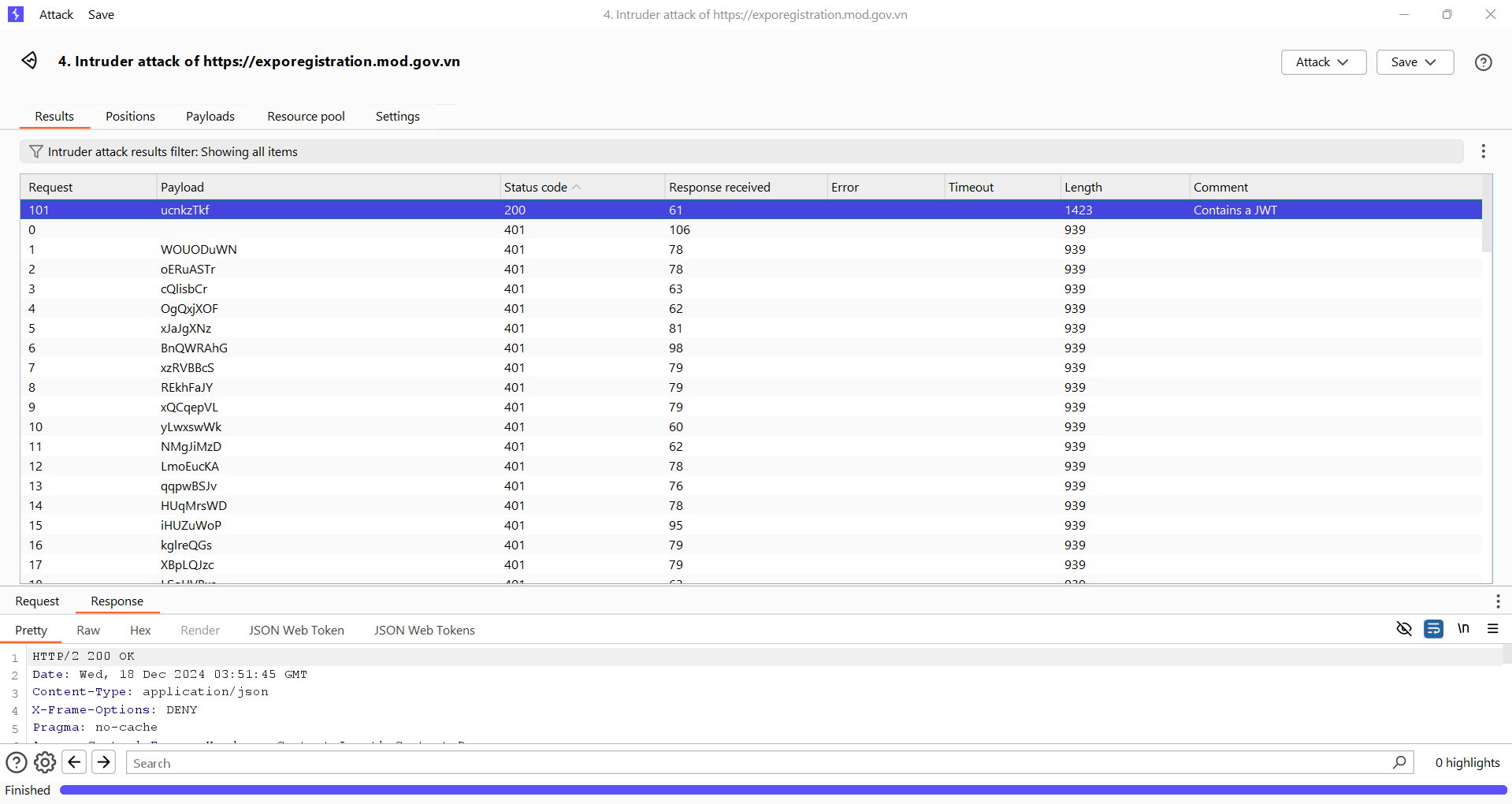
Kẻ tấn công brute force để tìm ra mã đăng ký của người dùng từ đó sửa đổi thông tin

## Các bước tái hiện Các bước để tái hiện

1. Truy cập url: <https://exporegistration.mod.gov.vn/authentication_v2>
2. Thử nhập các chuỗi 8 ký tự để tìm ra mã đăng ký của người dùng
3. Sử dụng công cụ Burpsuite để bruteforce mã đăng ký của người dùng



1. Nếu tìm được mã đăng ký khớp với người dùng nào đó web sẽ trả về phản hồi 200



## Cách khắc phục

- Giới hạn số lần nhập mã số đăng ký

- Yêu cầu nhập captcha mỗi khi tra cứu bằng mã số đăng ký

|  |
| --- |
| **BUG-2 Server trả về chi tiết thông báo lỗi** |

## Phân loại Server Security Misconfiguration > Information Disclosure

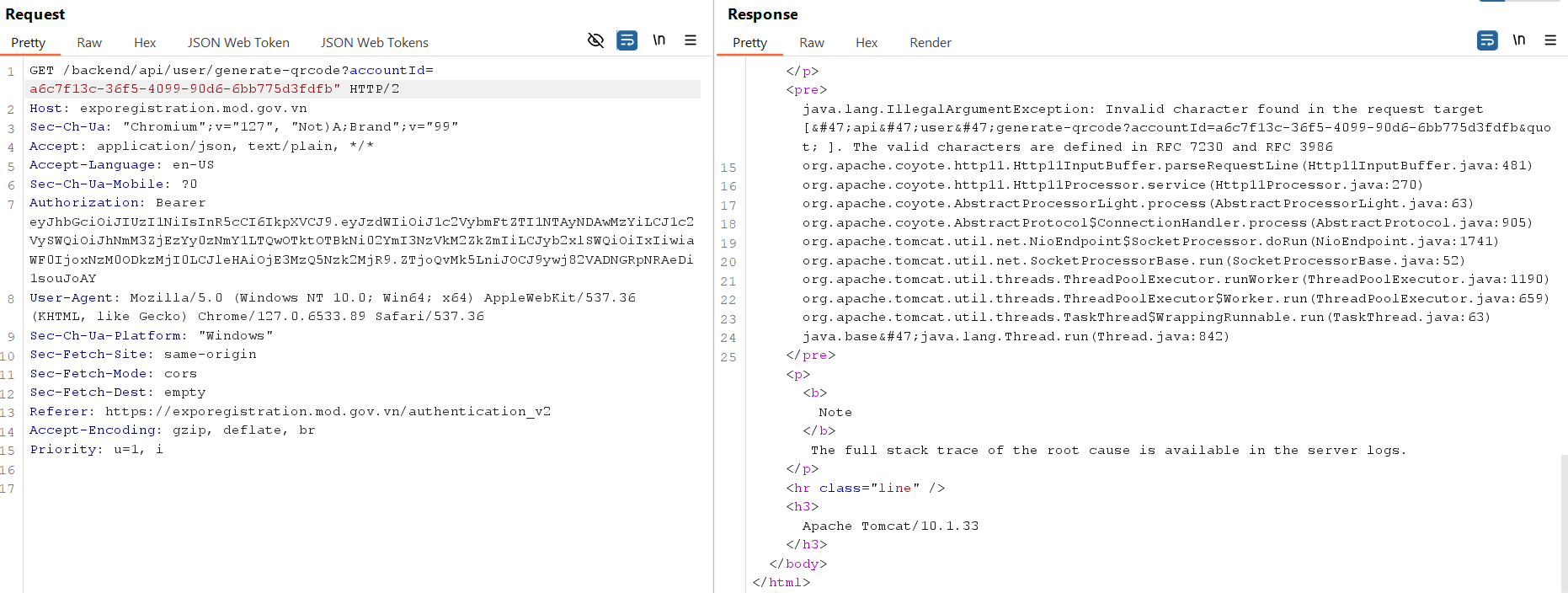
**Mô tả**

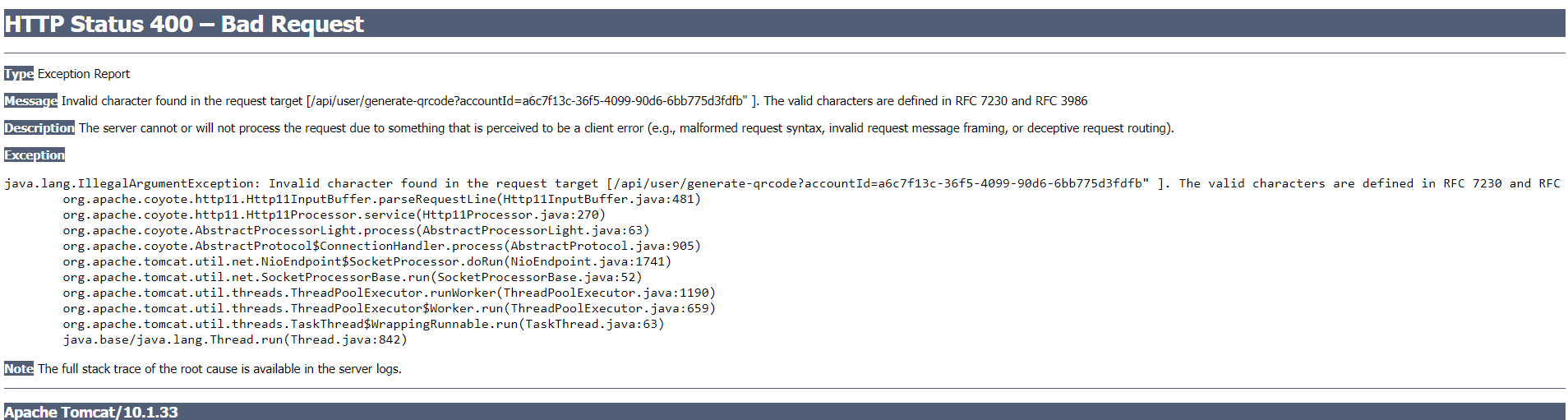
## Mức độ nguy hiểm: KHUYẾN NGHỊ

**Ảnh hưởng**

Kẻ tấn công brute force để tìm ra mã đăng ký của người dùng từ đó sửa đổi thông tin

## Các bước tái hiện Các bước để tái hiện





## Cách khắc phục

-

|  |
| --- |
| **BUG-3 Nhập Input null trong phần tra cứu nhưng trả về tên và mã QR của người dùng khác** |

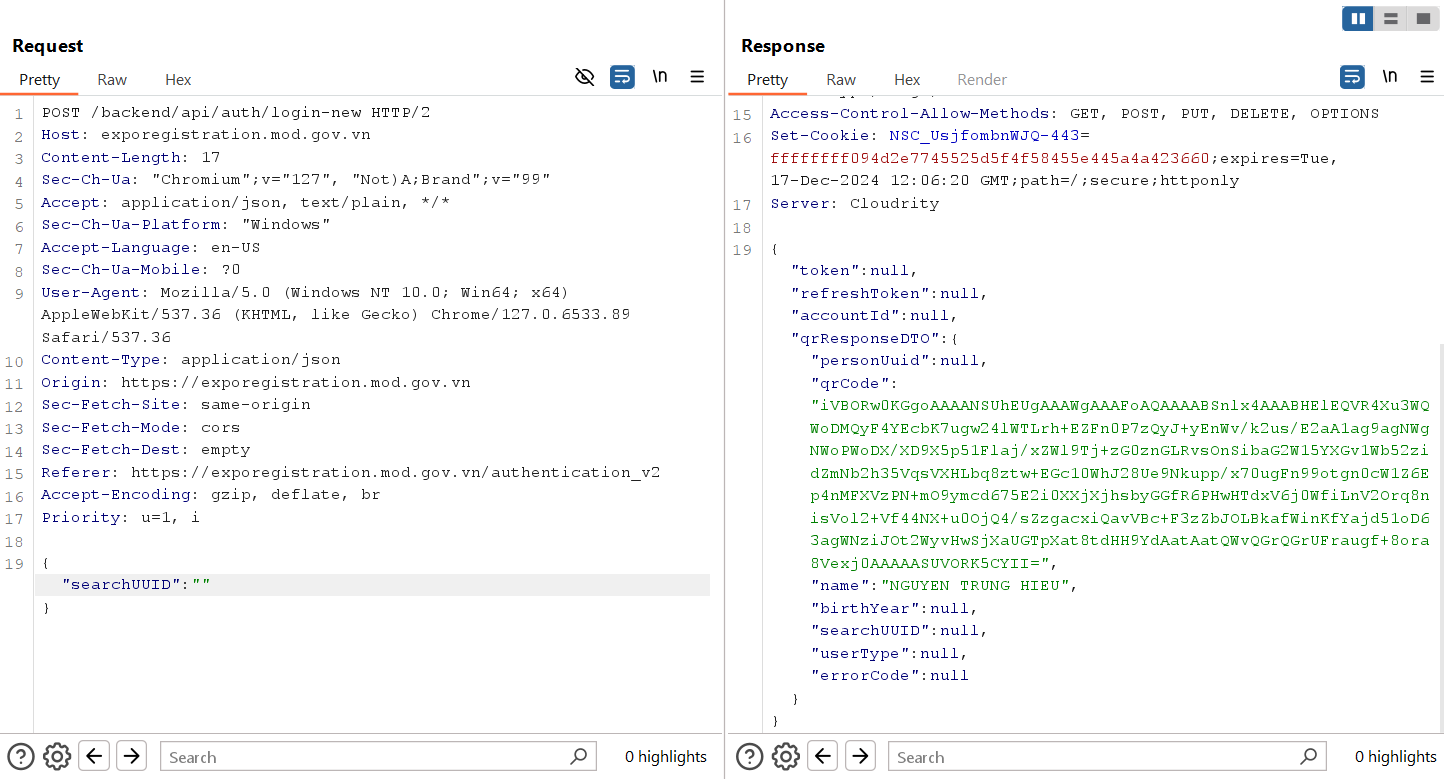
## Phân loại Server Security Misconfiguration > Information Disclosure

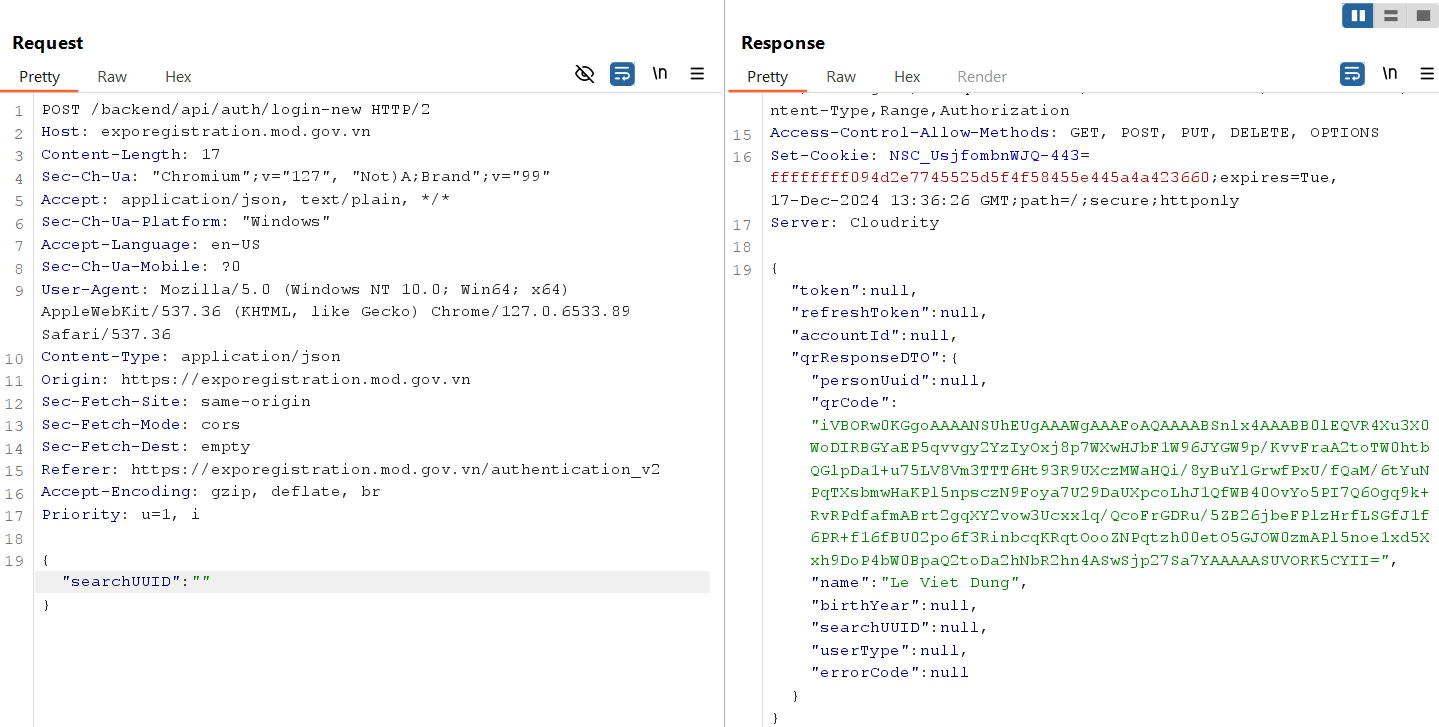
**Mô tả**

## Mức độ nguy hiểm: KHUYẾN NGHỊ

**Ảnh hưởng**

## Các bước tái hiện Các bước để tái hiện





## Cách khắc phục

-