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** https://exporegistration.mod.gov.vn |
| **Thời gian** 2024-12-19 |
| **Đầu mối liên hệ** \* |
| **Hình thức đánh giá Blackbox** |
| **Nhóm đánh giá** Công ty An ninh mạng Viettel |
| **Số lượng lỗi**  3 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** |
| **1** | Không giới hạn tần suất nhập mã số đăng ký | **THẤP** |
| **2** | Input rỗng trong phần tra cứu nhưng vẫn trả về tên và mã QR của người dùng khác | **KHUYẾN NGHỊ** |
| **3** | Server trả về chi tiết thông báo lỗi | **KHUYẾN NGHỊ** |
| **4** | Phiên bản web server hiện tại xuất hiện CVE mới | **KHUYẾN NGHỊ** |

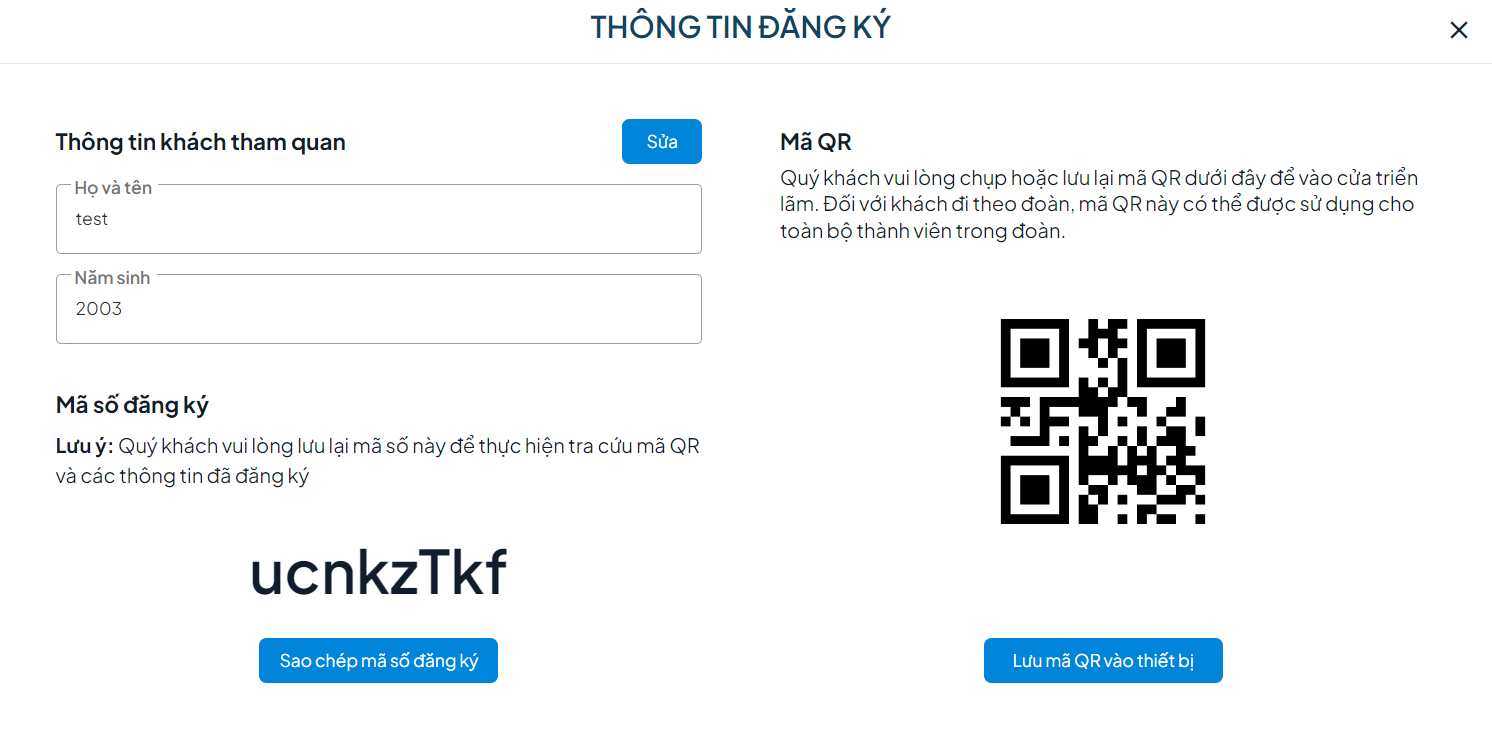
# Chi tiết lỗi

|  |
| --- |
| **[1](#_bookmark0) - Không giới hạn tấn suất 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:

|  |  |  |
| --- | --- | --- |
| STT | URL | Tham số |
| 1 | <https://exporegistration.mod.gov.vn/authentication_v2> | searchUUID |

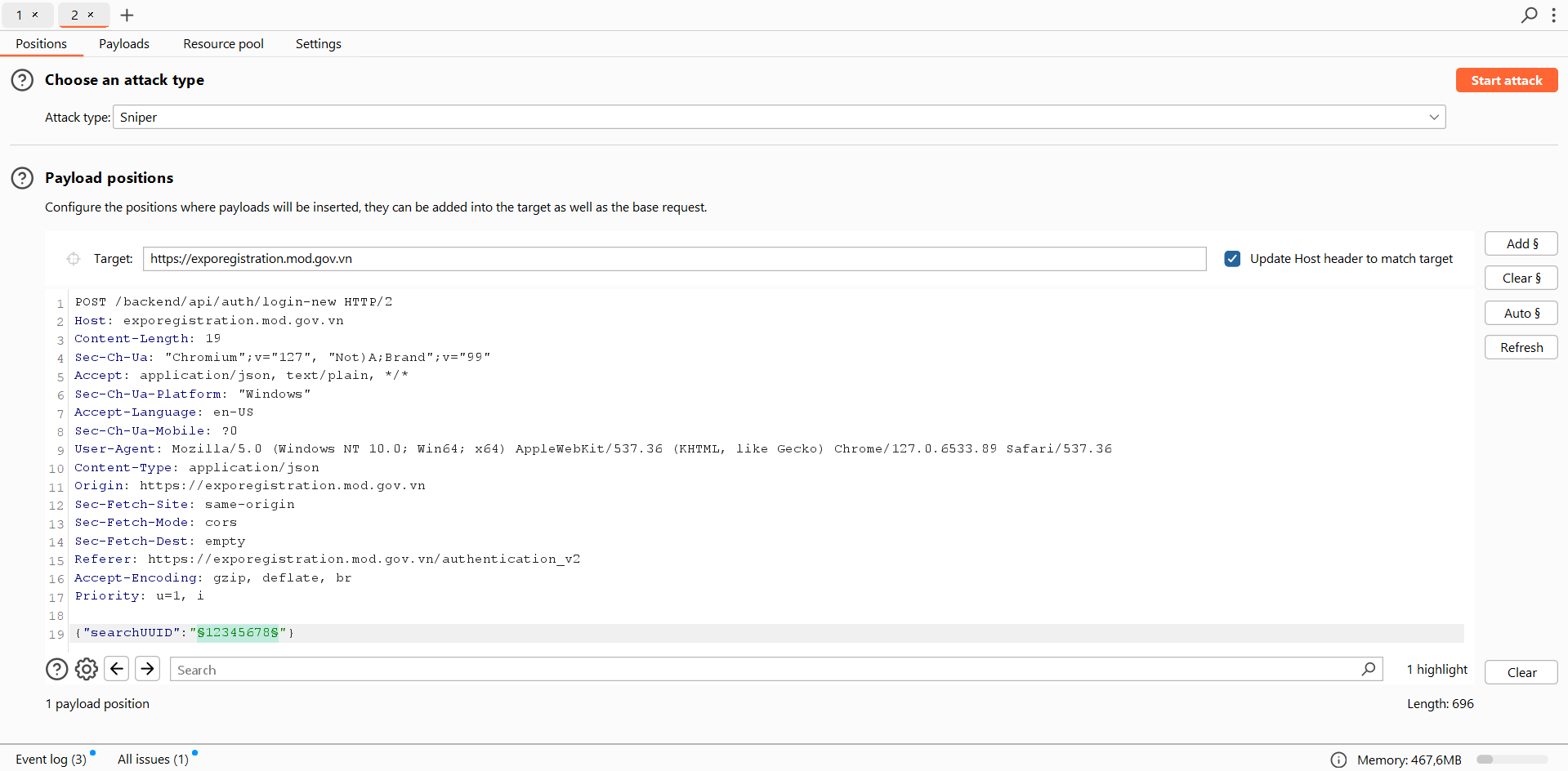
## Mức độ nguy hiểm: THẤP

**Ảnh hưởng**

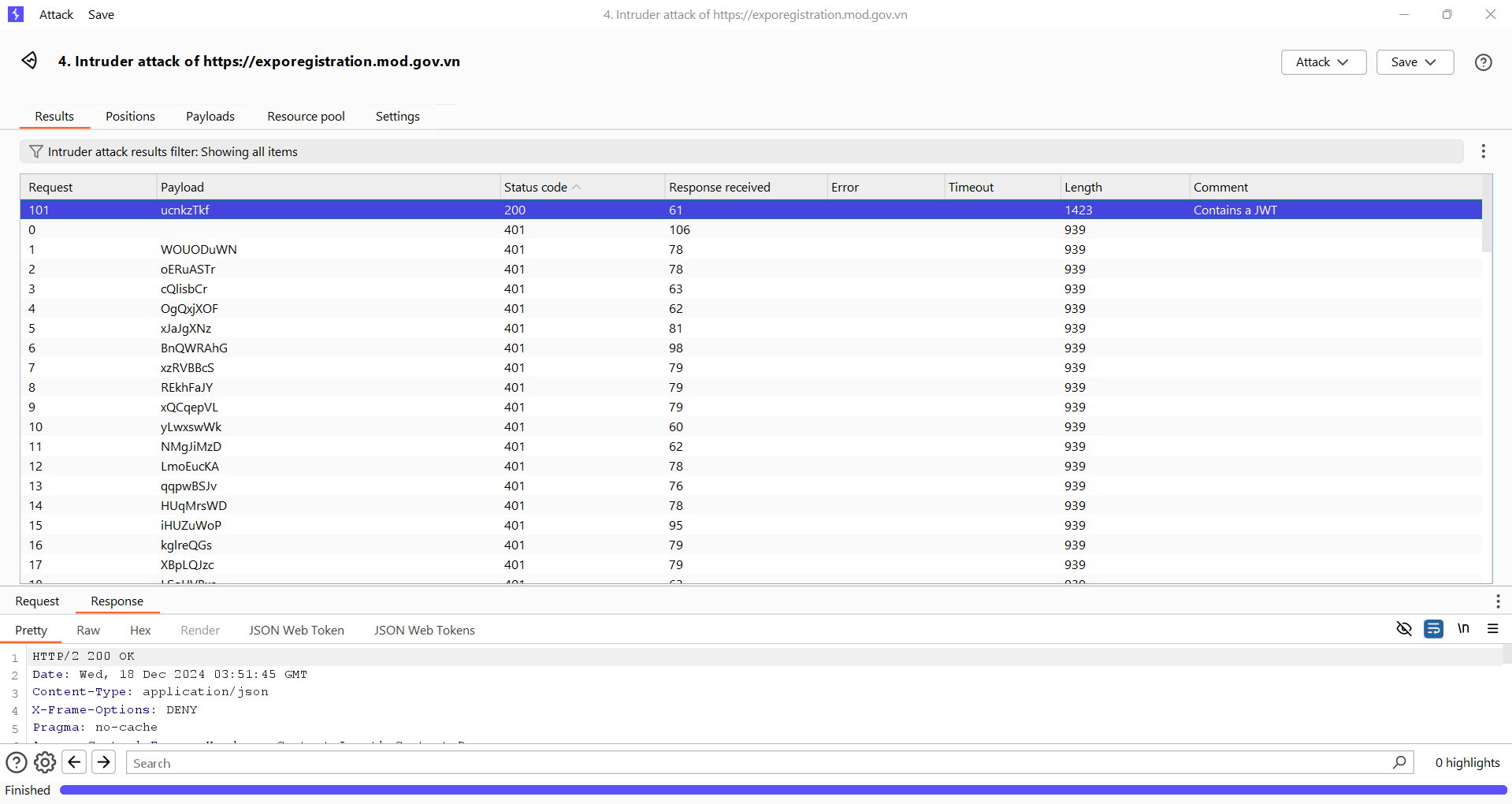
Kẻ tấn công brute force để tìm ra mã đăng ký của người dùng từ đó sửa đổi thông tin.

## 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

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

|  |
| --- |
| **2 - Input rỗng trong phần tra cứu nhưng vẫn trả về tên và mã QR của người dùng khác** |

## Phân loại Server Security Misconfiguration > Information Disclosure

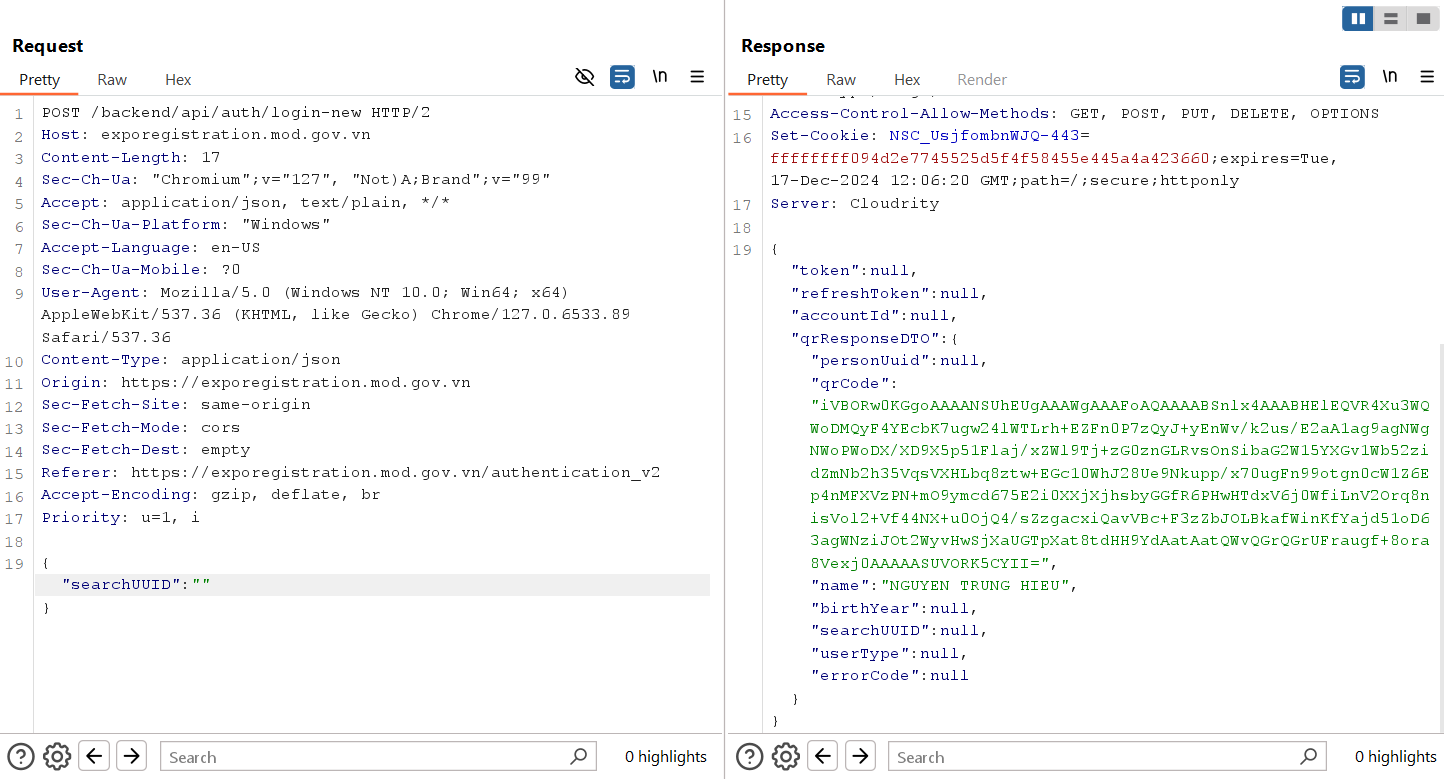
**Mô tả**

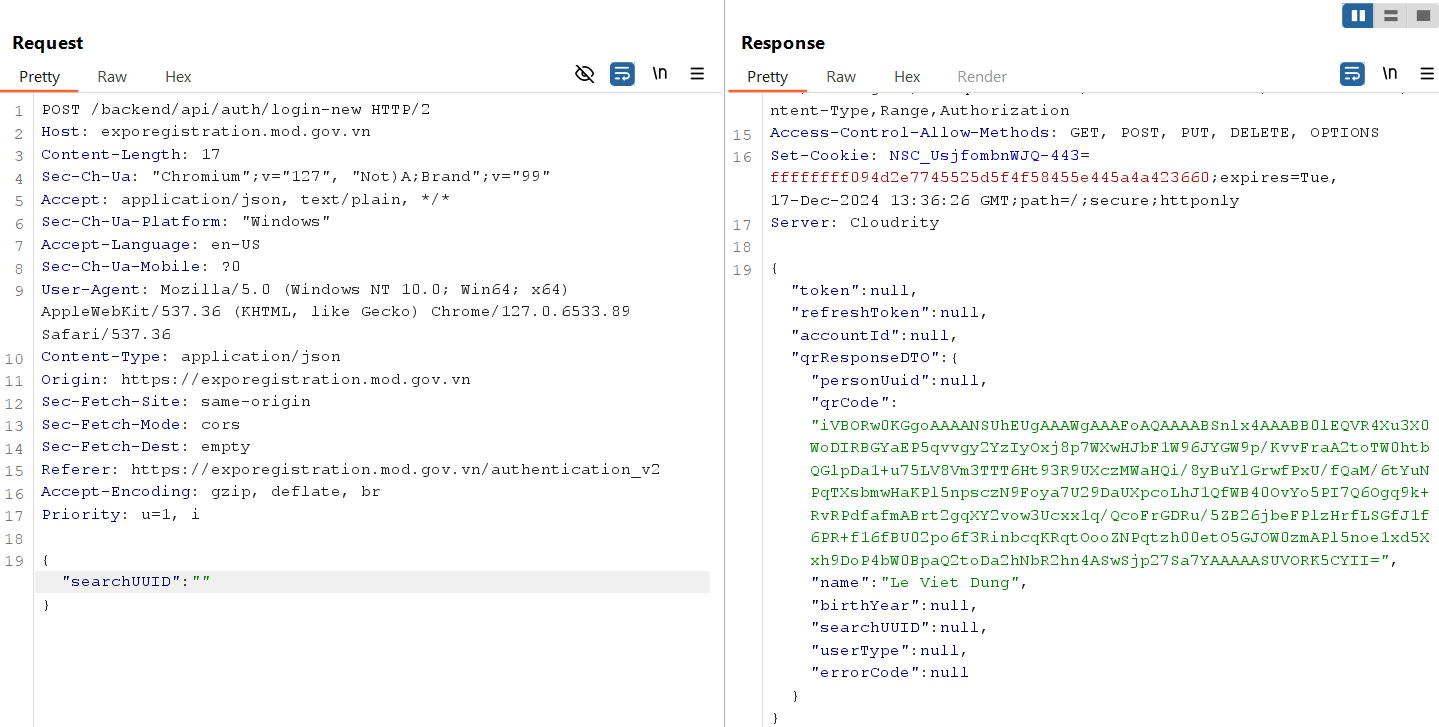
Tại chức năng tra cứu gửi đi một chuỗi rỗng nhưng server vẫn trả về tên và mã QR của người dùng khác.

## Mức độ nguy hiểm: KHUYẾN NGHỊ

## Các bước tái hiện Các bước để tái hiện

1. Thực hiện tra cứu người dùng, sử dụng công cụ như Burpsuite để sửa request và sửa tham số searchUUID thành giá trị rỗng.
2. Server vẫn trả về tên và mã QR của người dùng nào đó. Mỗi thời điểm cho ra một người dùng khác nhau.





## Cách khắc phục

- Kiểm tra logic phần code

|  |
| --- |
| **3 - Server trả về chi tiết thông báo lỗi** |

## Phân loại Server Security Misconfiguration > Information Disclosure

## Tổng quan

## Các thông báo lỗi có thể xuất hiện trong nhiều trường hợp khác nhau. Chúng có thể xảy ra do mã nguồn lỗi logic hoặc khi hệ thống hoạt động bất thường dưới một tác động nào đó. Thông báo lỗi có thể để lộ thông tin loại công nghệ sử dụng, phiên bản,… Nếu đó là một phiên bản công nghệ đã cũ, kẻ tấn công hoàn toàn có thể tìm kiếm một số lỗ hổng (CVE) xảy ra đối với phiên bản đó và khai thác. Và sẽ càng nguy hiểm hơn nếu trang web sử dụng framework open source mà có thể tìm thấy toàn bộ source code qua github.

**Mô tả**

Tại một số endpoint khi truyền vào các giá trị đặc biệt để tạo tình huống ngoại lệ (exception). Server sẽ trả về chi tiết thông báo lỗi.

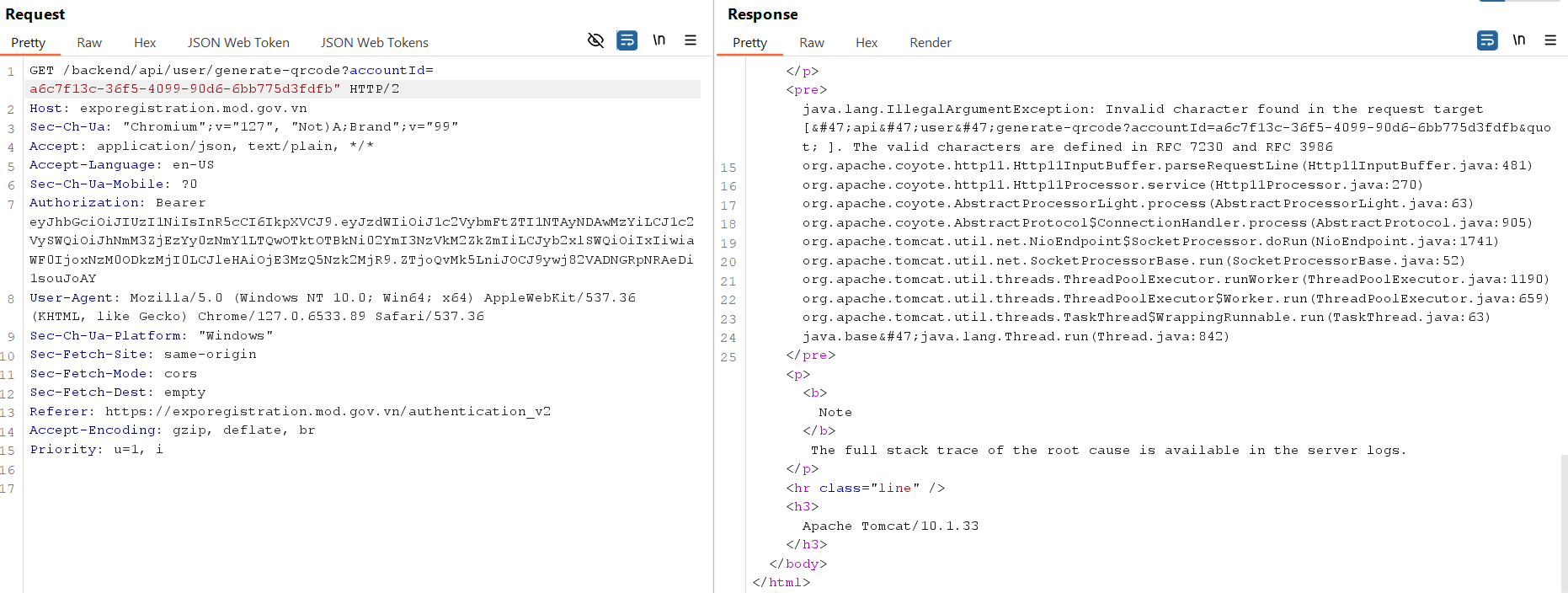
## Mức độ nguy hiểm: KHUYẾN NGHỊ

**Ảnh hưởng**

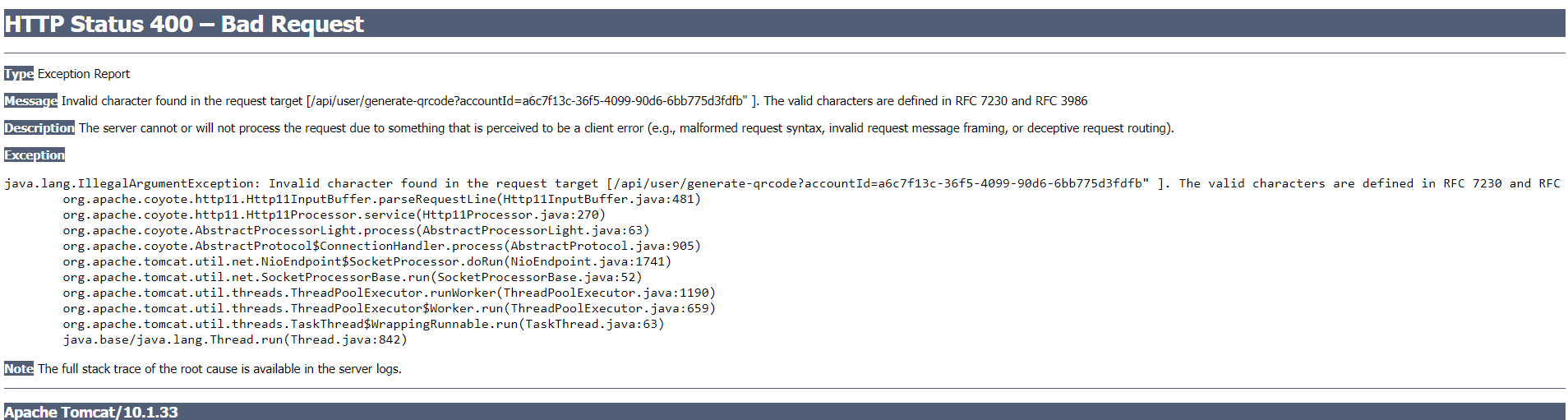
Gia tăng bề mặt tấn công và tạo điều kiện cho các cuộc tấn công khác

## Các bước tái hiện Các bước để tái hiện

1. Tại một số endpoint truyền vào các tham số với ký tự đặc biệt hoặc truyền vào một mảng để trigger lỗi.



1. Server trả về chi tiết thông báo lỗi chứa thông tin về web server và phiên bản.



## Cách khắc phục

- Chỉ hiển thị lỗi chung chung.

|  |
| --- |
| **4 - Phiên bản web server hiện tại xuất hiện CVE mới** |

## Phân loại Using Components with Known Vulnerability

**Mô tả**

Theo thông tin thu thập được hệ thống đang sử dụng Apache Tomcat phiên bản 10.1.33, phiên bản này nằm trong danh sách bị ảnh hưởng bởi lỗ hổng mới được công bố vào ngày 20/12/2024. Lỗ hổng thực thi mã từ xa (RCE) có mã CVE-2024-56337, chưa có điểm CVSS, ảnh hưởng đến nhiều phiên bản Tomcat, bao gồm 10.1.33. Lỗ hổng này xuất phát từ việc áp dụng biện pháp giảm thiểu chưa đầy đủ cho lỗ hổng trước đó là CVE-2024-50379. Kẻ tấn công có thể khai thác CVE-2024-56337 trên các hệ thống tệp không phân biệt chữ hoa chữ thường, khi servlet mặc định của Tomcat đã bật chức năng ghi. Bằng cách thao túng các đường dẫn cụ thể, kẻ tấn công có thể vượt qua các giải pháp an ninh, tải lên tệp chứa mã JSP độc hại và cuối cùng thực thi mã từ xa.

Người dùng đang sử dụng các phiên bản Apache Tomcat bị ảnh hưởng trên hệ thống tệp không phân biệt chữ hoa chữ thường, đặc biệt khi chức năng ghi của servlet mặc định được bật sẽ dễ bị tấn công.

## Mức độ nguy hiểm: KHUYẾN NGHỊ

## Cách khắc phục

- Kiểm tra lại cấu hình hệ thống và cập nhật Apache Tomcat lên phiên bản mới để giảm thiểu khả năng bị tấn công.